

Kommunikáció 2003

Nemzetközi szakmai tudományos konferencia anyaga



Zrínyi Miklós Nemzetvédelmi Egyetem
Budapest, 2003. október 15.

Szerkesztették a szervező bizottság tagjai:

Dr. habil. Sándor Miklós ezredes

Hamar Sándor mk. ezredes

Dr. Lehel György mk. ezds.

Fekete Károly mk. alezredes

Lektorálta:

Fekete Károly mk. alezredes

Fregan Beatrix

Felelős kiadó: Dr. Szabó Miklós, a Zrínyi Miklós Nemzetvédelmi Egyetem rektora

Megjelent a Zrínyi Miklós Nemzetvédelmi Egyetem Kiadó gondozásában

Igazgató: Veverka László

Készült a Zrínyi Miklós Nemzetvédelmi Egyetem nyomdájában, 200 példányban

Felelős vezető: Kardos István

ISBN 963 86229 6 2

TARTALOMJEGYZÉK

HÁTTÉR INFORMÁCIÓK	9
BEVEZETŐ	11
AGÁRDI Ferenc	
AZ MVM RT. TÁVKÖZLÉS FEJLESZTÉSÉNEK EREDMÉNYEI	13
ANTÓK Péter	
ÚJ KÁBELHÁLÓZAT LÉTESÍTŐ TECHNOLÓGIÁK	37
László BALOGH, Dr. Bertalan EGED	
PRECISION DIRECTION FINDING ALGORITHM OF RADIO SIGNALS	47
FEHÉR Gabriella	
ELEKTRONIKUS BŰNÖZÉS. HAZAI ÉS KÜLFÖLDI TAPASZTALATOK	57
Károly FEKETE	
EVOLVING POSSIBILITIES OF THE STRATEGIC MILITARY NETWORKS	65
Beatrix FREGAN	
STRATÉGIES ET TECHNOLOGIES SUR L'INFORMATION	69
Beatrix FREGAN – Zoltán RAJNAI	
TELECOMMUNICATIONS SPATIALES MILITAIRES ET INTEROPERABILITE	73
Roland GÉMESI - Balázs IVÁDY - László ZÖMBIK	
SECURITY AND RELIABILITY OF SENSOR NETWORKS	77
HÓKA Miklós	
A VÁROSHARC KOMMUNIKÁCIÓS JELLEMZŐI A 21. SZÁZADBAN	91
HÓKA Miklós	
A HARCTÉRI KOMMUNIKÁCIÓ EGYIK LEHETSÉGES JÖVŐKÉPE: A HARCÁSZATI INTERNET	103
JOBBÁGY Szabolcs - SEREGE Gábor	
AZ EGYSÉGES KÉSZENLÉTI DIGITÁLIS TRÖNKÖLT RÁDIÓRENDSZER, TETRA ÉS TETRAPOL JELLEMZŐI, SAJÁTOSSÁGAI	119
Kassai Károly	
AZ INFORMÁCIÓK, VALAMINT A HÍRADÓ ÉS INFORMATIKAI RENDSZER VÉDELME NEK SZABÁLYOZÁSA	133
KASZA Károly	
MODERN KATONAI TELEFONOK	141

KELEMEN Sándor	
ÚTVONAL OPTIMALIZÁLÁS ÉS SZEREPE A TŰZOLTÓSÁG MUNKÁJÁBAN.	153
KIS Lajos	
A MAGYAR HONVÉDSÉG HÍRRENDSZERÉNEK JELENE... ÉS JÖVŐJE?	157
Dr. KOCZKA Ferenc	
VÁLTOZÓ HONVÉDSÉG, ÁTALAKULÓ MÉRNÖKTISZT-KÉPZÉS	165
LADÁNYI – Turóczy Béla	
MELEG TARTALÉKOLT ANTENNARENDSZEREK	181
MIHÁLY Sándor - KELEMEN Sándor	
AZ ERDŐK TŰZVÉDELME T SZOLGÁLÓ, TŰZVÉDELMI KOCKÁZAT ELEMZŐ ÉS DÖNTÉSTÁMOGATÓ INFORMATIKAI RENDSZER.	193
MAROS Dóra	
RÁDIÓBERENDEZÉSEK MINŐSÉGI MEGFELELŐSÉGE	199
MICHELBERGER Pál	
INFORMATIKAI PROJEKTEK SAJÁTOSSÁGAI ÉS LEHETŐSÉGEI A VÉDELMI SZFÉRÁBAN (EGY KÍVÜLÁLLÓ VÉLEMÉNYE...)	203
MOLNÁR Kata- ZÖMBIK László	
DIGITÁLIS ALÁÍRÁS HASZNOSÍTÁSA	215
Dr. MRÁZ István	
A HADERŐ VEZETÉSE BÉKÉTŐL ELTÉRŐ (MINŐSÍTETT) IDŐSZAKOKBAN	221
Sandor MUNK	
INFORMATION INTEROPERABILITY AND COMMUNICATION	235
NÉMETH András	
ADAPTÍV ANTENNARENDSZER SZIMULÁCIÓJA	245
PÁNDI Erik	
A KORMÁNYZATI TÁVKÖZLÉS HELYZETE 1967-1989 KÖZÖTT	255
POÓR Zoltán	
KÉPÁTVITEL ÉS ADATÁTVITEL LEHETŐSÉGEI ÉS TAPASZTALATAI A VEZETÉKNÉLKÜLI HARCÁSZATI KOMMUNIKÁCIÓ TERÉN	281
Pinczésné KISS Klára - EGRI Gábor	
KRIMINOLÓGIAI JELENSÉGEK MÉRÉSE ÉS MÉRHE TŐSÉGE A KOMMUNIKÁCIÓ ÉS A MINŐSÉGBIZTOSÍTÁS TÜKRÉBEN	297

Zoltán RAJNAI	
SECURISATION DE DONNEES TEMPS REEL DANS UN SYSTEME DE COMBAT SUR ATM	321
Dr. Zoltán RAJNAI - Beatrix FREGAN	
FAUT-IL CHANGER LA STRATEGIE DE LA COMMUNICATION?	325
RÉVÉSZ Gyula	
HÍRADÓKIKÉPZÉS A NÉMET SZÖVETSÉGI KÖZTÁRSASÁG SZÁRAZFÖLDI HADERŐNEMNÉL	329
RÉVÉSZ Gyula	
PROFI HADSEREG HATÁSA A KIKÉPZÉSRE	338
Dr. habil SÁNDOR Miklós	
ÚJ KIHÍVÁSOKRA — ÚJ VÁLASZOK?!	343
SEREGE Gábor – JOBBÁGY Szabolcs	
GPRS: ÚT A MOBIL INTERNET FELÉ	348
SPRINGEL Zoltán	
INFOKOMMUNIKÁCIÓS SZOLGÁLTATÁSOK ÉS A BIZTONSÁG	354
SZABÓ Zoltán	
A RENDSZERINTEGRÁCIÓ ÉS A KAPSCH SZEREPE A KORSZERŰ KOMMUNIKÁCIÓS RENDSZEREK KIALAKÍTÁSÁBAN	356
SZÖLLŐSI Sándor	
AZ ÚJ TÍPUSÚ HADERŐ ÉS A SÚLYPONT-ÁTRENDÉZŐDÉS KÉRDÉSEI A TECHNIKAI STRUKTÚRÁBAN	364
Dr SZŰCS Gáspár	
A MH AGYAR HONVÉDSÉG INFORMATIKAI HELYZETE, FEJLESZTÉSI TERVEI, PROBLÉMÁI	370
TESSEDIK Tamás	
INFORMÁCIÓ SZOLGÁLTATÁS ÉS VÉDELEM A MINDENNAPI MUNKÁBAN	379
Tibor SÁNDORFI, Jácint LÁNCOS, Ferenc KUBINSZKY, László ZÖMBIK	
LOCATION HIDING ATTACKS IN IP NETWORKS	379

A nemzetközi tudományos konferencia kommunikációs partnere:

Magyar Távközlési Részvénytársaság

A tudományos konferencia kiemelt támogatói:



KONGSBERG

KONGSBERG Defence Communications



VT-Rendszertechnika Kft

A tudományos konferencia támogatói:

- ❖ Thales
 - ❖ Kapsch Telecom Kft
 - ❖ Fercom Kft
 - ❖ Antók Mérnöki Iroda
 - ❖ MM ENGINEERING Mérnöki tanácsadó Bt
-

HÁTTÉR INFORMÁCIÓK

A konferencia fővédnöke:

- Mikita János mk. vezérőrnagy, a Honvéd Vezérkar Törzsigazgatója

A konferencia védnökei:

- Prof. Dr. Szabó Miklós vezérőrnagy, akadémikus, rektor
- Halmai Ottó mk. dandártábornok, HVK híradó és informatikai csoportfőnök

A konferencia kommunikációs partnere:

- Magyar Távközlési Részvénytársaság

A konferencia támogatói:

- Kongsberg Defence Communications
- VT-Rendszertechnika Kft
- Thales
- Kapsch Telecom Kft
- Fercom Kft
- Antók Mérnöki Iroda

A konferencia rendezői:

- Zrínyi Miklós Nemzetvédelmi Egyetem Katonai kommunikációs rendszer-szervező tanszék
- Honvéd Vezérkar Híradó és Informatikai Csoportfőnökség
- Zrínyi Miklós Nemzetvédelmi Egyetem Katonai Műszaki Doktori Iskola
- Hírközlési és Informatikai Tudományos Egyesület Egyetemi Csoport

A szervező bizottság elnöke:

- Dr. habil. Sándor Miklós ezredes

A szervező bizottság titkára:

- Fekete Károly mk. alezredes

A szervező bizottság tagjai:

- Hamar Sándor mk. ezredes
- Dr. Lehel György mk. ezredes

BEVEZETŐ

A Tisztelt Olvasó a Zrínyi Miklós Nemzetvédelmi Egyetem katonai kommunikációs rendszerszervező tanszék, a HVK Híradó és informatikai csoportfőnökség, a Zrínyi Miklós Nemzetvédelmi Egyetem Katonai műszaki doktori iskola és a Hírközlési és Informatikai Tudományos Egyesület egyetemi csoportja által rendezett nemzetközi szakmai tudományos konferencia szerkesztett anyagát tartja a kezében.

Az immár negyedik szakmai tudományos konferencia célja volt áttekinteni a kommunikációval kapcsolatos változásokat. Különös figyelemmel kezelte az állandó versenyt túlélő és a kísérleti fázisban levő távközlési és informatikai megoldásokat. A konvergencia megjelenési formáit a konferencián kiállított és a konferencia résztvevők intézményeinél konkrétan megvalósított eszközökön és kommunikációs hálózatokon keresztül mutatta be.

További célja volt a katonai kommunikáció 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 szakmai konferencia egyben áttekintést adott a témakör elméleti tudományos kutatásának eddigi nemzetközi és hazai eredményeiről.

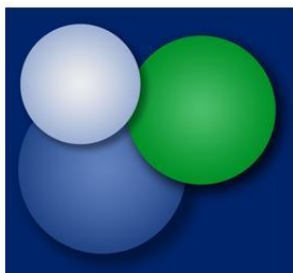
Az elméleti előadások mellett bemutatásra kerültek az MRR rádiók, egy többrendeltetésű, NATO szabványoknak megfelelő híradó és informatikai eszközökkel felszerelt konténer, speciális katonai antennák, kábelek, távbeszélő készülékek, valamint végül, de nem utolsósorban egy harcászati-hadműveleti szintű szárazföldi csapatok vezetését-irányítását támogató információs rendszer.

A szervező bizottság nem titkolt szándéka volt, hogy az előadásokon elhangzottak minél szélesebb körben ismertté váljanak, ezért a konferencia anyagát közreadjuk.

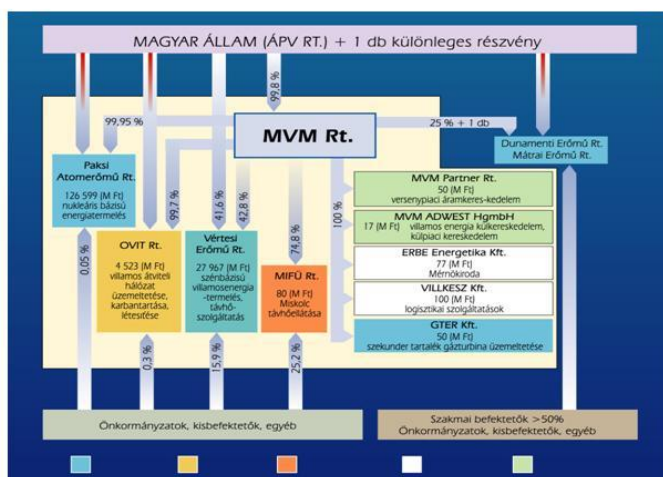
Dr. habil Sándor Miklós

AZ MVM RT. TÁVKÖZLÉS FEJLESZTÉSÉNEK EREDMÉNYEI

Kommunikáció 2003

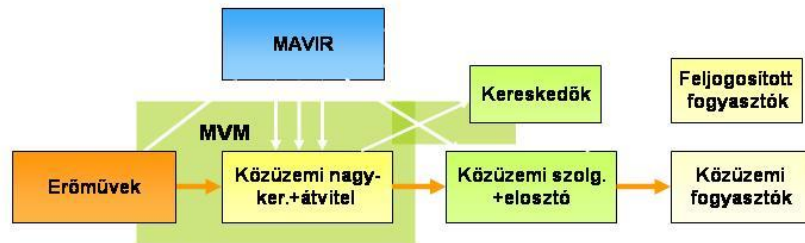


MVM Rt.
2003. október 15.



A liberalizált piac működése, az MVM szerepe

2003-tól:



Helyzetkép fejlesztés (TFP) előtt (1)

- Távközlési szolgáltatás az iparág-specifikus igények kielégítésére
- Kiszolgált kör
 - MVM Rt.
 - Leányvállalatok
 - Áramszolgáltatók
 - Erőművek

Helyzetkép fejlesztés (TFP) előtt (2)

- Szolgáltatás kínálat
 - Alaptevékenység ellátás
 - telemechanikai adatgyűjtés
 - Feszültség/meddő teljesítmény optimalizálás
 - Teljesítmény - frekvencia online szabályozás
 - Távadatgyűjtés, mérésadatgyűjtés
 - Védelmi jelátvitel, vagyonvédelem
 - Üzemirányító távbeszélő hálózat

Helyzetkép fejlesztés (TFP) előtt (3)

- Szolgáltatás kínálat
 - Alaptevékenység támogatás
 - Ügyviteli távbeszélő hálózat
 - Nem beszédcélú támogató szolgáltatások

Fejlesztés előtti technológia

- 67 telephely
- Mikrohullámú berendezések (PDH, 2 GHz, tipikusan 4x2 Mbit/s kapacitás)
- Üzemirányítási alközpontok
- ÜRIK projekt (SDH, optika)
- Összefoglalva: heterogén, néhol erkölcsileg elavult, kis kapacitású rendszer

Fejlesztés előtti technológia



Fejlesztés előtti technológia



Távközlés fejlesztési projekt (TFP)

- 2300 km optikai kábel, alapvetően OPGW
- 12-48 szálás kábelek
- SDH berendezések
- Projekt kezdete: 2000. szeptember 26.
- Projekt befejezése: 2003. április 10. (aug. 31.)
- Korszerű, nagy sávszélességű, országos gerinchálózati lefedés, gyűrűs topológia
- kiemelkedő biztonságú rendszer

Távközlés fejlesztési projekt (TFP)

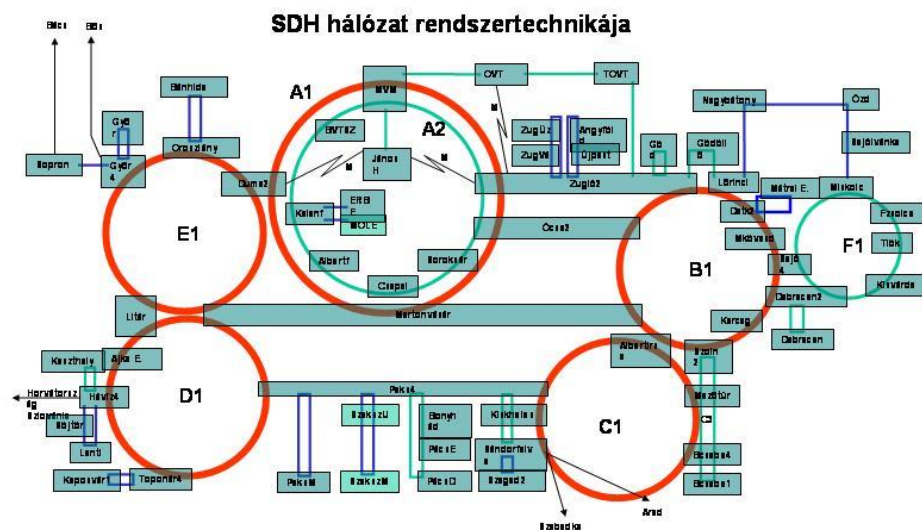


Az MVM célkitűzése a fejlesztéssel szemben

- **Átviteli biztonság szempontjából magas szinten versenyképes legyen**
- **Költség hatékony rendszer legyen, amely alkalmas:**
 - **Az energetikai iparág távközlési igényeinek teljes körű kielégítésére**
 - **A többlet kapacitások 'szabad piacon' értékesíthetők legyenek**

Rendszertехnikai elvárások

- **Üzembiztonsági megfontolások miatt a választott technológia: SDH**
- **Mind kapacitásban, mind védelmi megoldások tekintetében jelentős tartalékokat tartalmaz**
- **Biztosított a hálózat későbbi bővíthetősége: jövőbiztonság**



Beszállításra pályázó cégek

- OPGW kábelek
 - Alcatel
 - MKM
- Átviteltechnikai rendszer
 - Kapsch
 - ABB
 - Alcatel
 - NEC
 - Nortel
 - Sagem
 - Siemens
 - Synergon

A pályázat értékelési szempontjai

- **Műszaki szempontok**
 - **Ár**
 - **Referenciák**
 - **Kereskedelmi feltételek**
-
- **A fenti sorrend fontossági rangsort jelentett**
 - **Az üzembiztonság mind berendezés, mind rendszer szinten kiemelt fontossággal bírt**

Kábelhálózat

- **12/24/48 szálal optikai kábel**
- **OPGW (optical Ground Wire) technológia (a távvezeték védővezetőjébe integrált optikai kábel)**

Az OPGW kábel szerkezete



Kábelhálózat szerelési technológia

- Minimális föld feletti távolság: 30 m
- Kábel szakadás csak rendkívüli körülmények között lehetséges

Kábel szerelési technológia



Kábel szerelési technológia



Optikai kábelek kötési technológiája

- 4-5 kilométerenként kötés
- A kötésdoboz a feszítő oszlopokon 20 m magasságban helyezkedik el

Berendezés típusok

- Szünetmentes áramellátás (POWERSTAR)
- SDH rendszer (Nortel)
 - TN-1X
 - TN-4X
 - TN-16X
 - NTW048AB: EDFA optikai erősítő modul
 - DSCM-60: diszperzió kompenzáló modul
- PDH rendszer (Ascom)
 - UMUX 1500 család

Network management

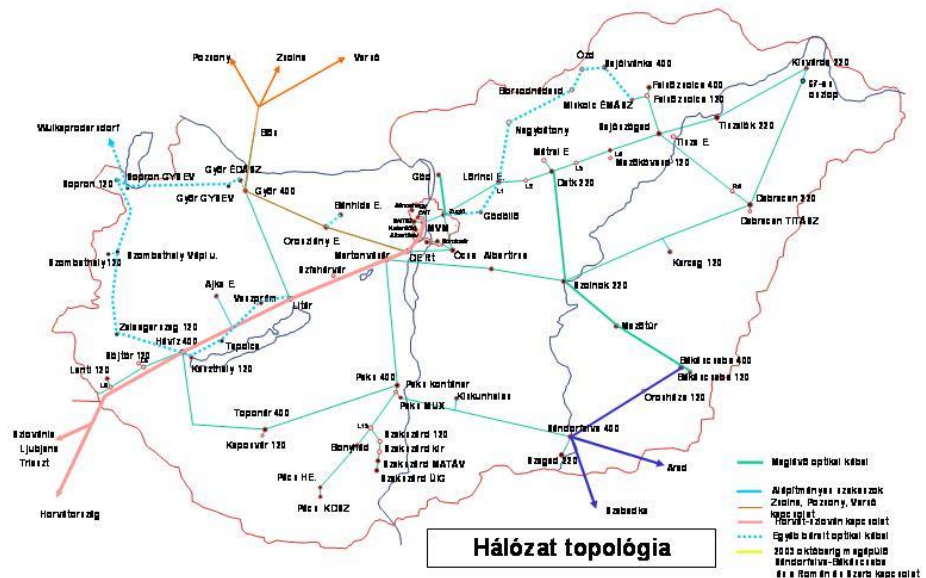
- Három független, de közös kommunikációval rendelkező rendszer (PDH, SDH, DWDM)
- Átlagon felüli megbízhatóság
 - redundáns, fizikailag elkülönített telephelyeken lévő két független hot-standby menedzsment állomás
 - UNIX operációs rendszer
 - HP eszközök
- OSI és IP kommunikációs protokollok
- Közvetve minden hálózati berendezés elérhető a hálózat minden pontjáról

Vizsgálatok

- Feltételek
 - Hiteles optikai, SDH és PDH műszerek
- Optikai mérések
- GPS és szinkron mérések, prioritások
- DWDM, SDH rendszer
 - Rendszer elméleti rendelkezésre állása:
$$R(\min) = ((RP - ((ES - SES) \times 0,3 + SES + US)) / RP) \times 100 = 99,95\%$$
(R(min) – mini máltis rendelkezésre állás, RP – rendelkezésre állási próba ideje (500 és 750 óra), ES – hibás másodpercek, SES – súlyosan hibás másodpercek, US – kiesett másodpercek)
 - RÁP mérések (2Mbit/s) $R(\min) = 99,997$
 - IRÁP mérések (2Mbit/s) $R(\min) = 99,995$
 - EOW
- PDH rendszer mérések
 - V.24, X.21, 4W+EWM
- MANAGEMENT szintű ellenőrzések (burst, alarm....)

Forgalomirányítás

- Áramkör igény felmérés, egyeztetés
- SDH trail tervezés (alternatív útvonal)
- PDH port kiosztás, útvonaltervezés
- MANAGEMENT konfigurálása, letöltések
- Paraméterek (szint, sebesség, paritás...)
- Ellenőrző mérések
- Átterhelés (lehető legrövidebb megszakadással)
- Új áramköri igények kiépítése
- Archiválás, nyilvántartás, számlázás
- Kapacitás gazdálkodás, távlati igényfelmérés, rendszerteknikai változások, hálózatbővítés



Villamos energia ipari üzembiztonsági sajátosságok

- Az üzemirányítási és folyamatirányítási távközlési hálózatok rendelkezésre állásának nagyobbak kell lennie, mint az irányított hálózat rendelkezésre állási előírása
- A1 csoport: kiesést nem tűrő rendszer
 - három, nyomvonalon is független összeköttetés
- A2 csoport: kiesést nem tűrő rendszer
 - kettő, nyomvonalon is független összeköttetés
- B1,B2 csoport: kiesést tűrő rendszer
 - a nyilvános közcélú szolgáltatásnak megfelelő rendelkezésre állás

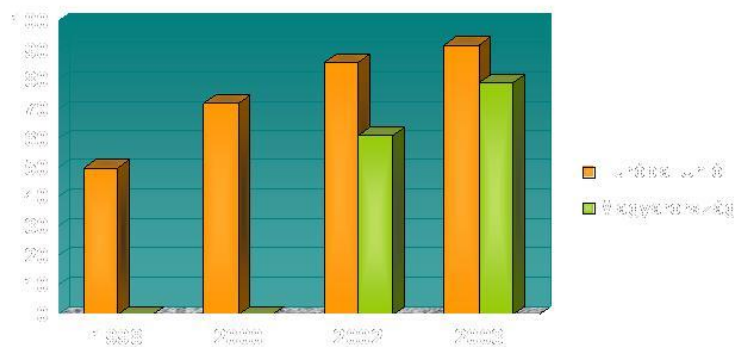
Üzembiztonsági előírások

- **Specifikáció: a hibaelhárítást 12 órán belül meg kell kezdeni**
- **Specifikáció: a tényleges hibaelhárítást 48 órán belül be kell fejezni**

A magyar távközlési piac jellemzői

- A piacra való belépés jogi korlátai elhárultak
- A piac már a liberalizáció előtt többszereplőssé vált
- Korlátozott területeken kialakuló verseny
- Koncentráció - néhány cégcsoport alakult ki, amelyek között a piaci versenyzés párhuzamosan egyre több szektorban folyik
- Az elmúlt években jelentős átrendeződés ment végbe az egyes szegmensek súlyát tekintve

Liberalizációs index



Forrás: IT-COM Kft. 2002.

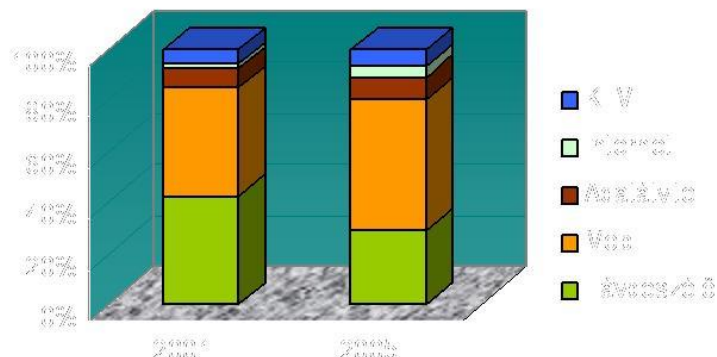
Részpiacok jellemzői (1)

- **Vezetékes távbeszélő piac** - az MVM számára nem célterület
 - kismértékben csökkenő piac
 - átstrukturálódás a bevételi arányokon belül
- **Mobil piac** - az MVM számára nem célterület
 - 16 % átlagos éves növekedés, csökkenő tendencia
 - élesedő verseny
 - bizonytalanság az UMTS körül
- **KTV és műsorszórás** - az MVM számára a szolgáltatók célpiacot jelentenek
 - 400 fölötti KTV szolgáltató, 1,7 millió előfizető
 - lassuló piaci koncentráció
 - folyamatosan növekvő számú visszirányra alkalmas hálózat

Részpiacok jellemzői (2)

- **Adatátviteli piac** - az MVM számára célpiac
 - 17 % átlagos éves növekedés
 - a részpiac aránya még kisebb, mint a Ny-Európában tapasztalható mérték
 - már jelenleg is erős, tovább fokozódó verseny
 - igények előtt járó alkalmazások

Részpiacok arányai



Miért jó partner az MVM az Önök számára?

- Kiemelt biztonsági és rendelkezésre állási paraméterekkel rendelkezik
- Konkurens távközlési cégek megkerülésének lehetőségét kínálja (összekapcsolási viták minimalizálása)
- Közvetlen nemzetközi csatlakozási lehetőségek
- A túlterhelt szakaszok tehermentesítésének lehetősége beruházás nélkül
- Magas rendelkezésre állási szinttel rendelkező alternatív útvonalak kialakításának lehetősége beruházás nélkül
- Versenyképes árak

Szolgáltatási kínálat: optikai szálak (sötét szálak) bérbeadása

- Átadási pont: optikai rendező
- Lehetőség berendezések elhelyezésére
- Lehetőség tápáram ellátásra
- Hozzáférési hálózat biztosítása
 - a hálózatot az MVM építi ki
 - a hálózatot az MVM bérli más szolgáltatóktól
 - a hálózatot a felhasználó építi ki
- Az optikai kábelek felügyelete biztosított az MVM által
- Igény esetén kicsatlakozási lehetőség bármely kötésből

Szolgáltatási kínálat: menedzselt bérelt vonali szolgáltatás

- ITU G.821 és ITU-T G.826-nak megfelelő minőségi jellemzőkkel rendelkező szolgáltatás
- Transzparens kapcsolat
- Az ügyfél által igényelt sáv szélességű és interfésszel végződött digitális pont-pont közti összeköttetés
- Folyamatos menedzselés
- Redundáns, gyűrűből felépülő, emelt biztonságú hálózat
- Hozzáférési hálózat biztosítása
 - a hálózatot az MVM építi ki
 - a hálózatot az MVM bérli más szolgáltatóktól
 - a hálózatot a felhasználó építi ki

Szolgáltatási kínálat: infrastruktúra bérlet

- **Mobil bázis állomás / vezeték nélküli Internet hozzáférés berendezéseinek elhelyezése**
- **Energia ellátás lehetősége**
- **Kapcsolódási lehetőség az optikai/SDH hálózathoz**
- **Igény esetén kulcsrakész kivitelezés**

Referencia mobil bázisállomás



A szolgáltatás minőségi paramétere

- Éves rendelkezésre állási mutató : **99,95 %**

A hálózaton jelenleg üzemelő áramkörök

- Összes áramkör: **1222**
- 2Mbit/s alatti áramkörök: **619**
- 2 Mbit/s-os áramkör: **391**
- Üzembe helyezésre előkészített: **212**

A szolgáltatás árát meghatározó tényezők

- Az igényelt összeköttetések száma, típusa
- Az előfizetői hozzáférés típusa
- A szerződés időtartama
- Igénybevett kapcsolódó szolgáltatások
- Egyedi tényezők

Minősegbiztosítás

- Célkitűzés: teljes körű európai minőségi modell megvalósítása
 - MSz EN ISO 9001 Minőségügyi rendszer
 - MSz EN ISO 14001 Környezetközpontú Irányítási Rendszer
- Irányítási politika alapkövetelményei
 - Elkötelezettség
 - Megbízhatóság
 - Etika
- Minőség tanúsító cég: IQNet
- Minőség tanúsítás időpontja: 2001.

A távközlési üzletág referenciái

- **Iparági vállalatok**

- MAVIR Rt.
- Paksi Atomerőmű Rt.
- Dunamenti Erőmű Rt.
- Mátrai Erőmű Rt.
- GTER Kft.
- Budapesti Elektromos Művek
- DÉDÁSz Rt.
- ÉDÁSz Rt.
- DÉMÁSz Rt.
- ÉMÁSz Rt.
- TITÁSz Rt.

- **Nem iparági partnerek**

- GTS
- GySEV
- Pantel
- Westel
- Pannon GSM
- VRAM
- ORFK
- OMSz

ÚJ KÁBELHÁLÓZAT LÉTESÍTŐ TECHNOLOGIÁK

Egy évtizeddel ezelőtt a vezetékes távközlési hálózat fejlesztésének az elsődleges feladata a teljes ellátás biztosítás feltételeinek létrehozása volt. A vezetékes hálózat tervezése, építése, szerelése a „hagyományos” rézkábel technológiával történt. A fényvezető kábelvonalak tervezése, építése beleillesszkedett a rézkábel környezetbe. Hasonlóan „hagyományos” módon épültek a kábeltelevíziós fényvezetős és koaxiális kábelhálózatok is.

A 2001. évi XL törvény a hírközlésről kereteket teremtett a távközlési piacon a vezetékes távközlési szolgáltatások területén is a verseny indítására. Az újonnan piacra lépő szolgáltatók esély egyenlőségét a törvényi keretek segítik, a korlátos erőforrások gátolják. A vezetékes távközlő hálózat nyomvonala lakott területen belül – építési szempontból – korlátos erőforrásnak számít. A keretet az MSZ 7487 – Közmű- és egyéb vezetékek elrendezése közterületen szabványsorozat adja. A szabvány szerint számítható ideális járdaszélesség, amely a szabványos közmű elhelyezést biztosítani tudja legalább 2,7 m széles kell, hogy legyen. Ahol ez a szélesség nem áll rendelkezésre, szabványtól eltérő megoldásokat kell alkalmazni.

Távközlési alépítmény-hálózat: Belterületen a járda alá beépített csőrendszer, melyre a kábel behúzás és a kábelkötések, vonali szerelvények elhelyezésére megszakító létesítményeket - beton szekrényeket, és kábelaknákat építenek. Az alépítmény-hálózat tervezett élettartama legalább 50 év.

Az alépítmény-hálózatnak két síkja alakult ki:

- néhány csőből, sekély mélységben épült elosztó-cső hálózat
- sok csőből, mélyen épült tömbcsatorna hálózat.

Az alépítmény hálózatban három építési stílus követi egymást:

- betoncsöves-alépítmény - 1975-ig
- műanyagcsöves alépítmény - napjainkban is épül
- vegyes réz-, optikai-, KTV alépítmény.

A betoncsöves hálózatra jellemző volt, hogy a 100 mm Ø-jű betoncsövekből, tömbcsatornákból 30-50 méter hosszú csőszakaszok. Az ólomköpenyű kábelek behúzása szakasz hosszokban, aknától-aknáig, vagy szekrénytől-szekrényig kézi erővel történt. Az alépítmény irányváltásait sarokaknák biztosították.

A műanyagcsöves építési stílus előnye, hogy a műanyagcső hajlíthatósága miatt a közműakadályok viszonylag könnyen elkerülhetők, a kábelaknák és szekrények a közművektől zsúfolt útkereszteződésekből elhúzhatók, az épületek bevezetései, a nyomvonal iránytörései íves csövekkel, szekrények építése nélkül megvalósíthatók. A műanyagcső kedvező súrlódási tényezője miatt a megszakító létesítmények távolsága 100-130 méterre megnőtt.

A fényvezető kábelek bevezetésével kezdődött meg a réz-optikai vegyes alépítménystílus építése. Ez egyrészt a műanyagcsöves alépítmény hálózatokban a fényvezető kábelek számára a PVC csövek béléscsővezetésével valósul meg, másrészt 40 mm és az 50 mm átmérőjű polietilén csövekkel megindult a fényvezető kábelek önálló alépítmény hálózatok építése.

A napjainkban a vezetékes távközlést biztosító hálózatok alépítményi szakaszai a közműszabvány által előírt szelvényt már megtöltötték. Az új hírközlő szolgáltatások és szolgáltatók esélyegyenlőségére a korlátok miatt szinte semmi remény sincs.

Ha a vezetékes távközlő hálózat egészét vizsgáljuk, és az egyes területeken kifejlesztett új technológiai megoldásokat összességében nézzük, és az ezekből kialakítható rendszerekhez a megfelelő építési- (létesítési-) stílust kialakítjuk, nem csak az esély egyenlőségre, hanem egyes területeken előny is létrehozható.

A hálózat egyes összetevőinek újdonságaiból kiragadunk néhány példát:

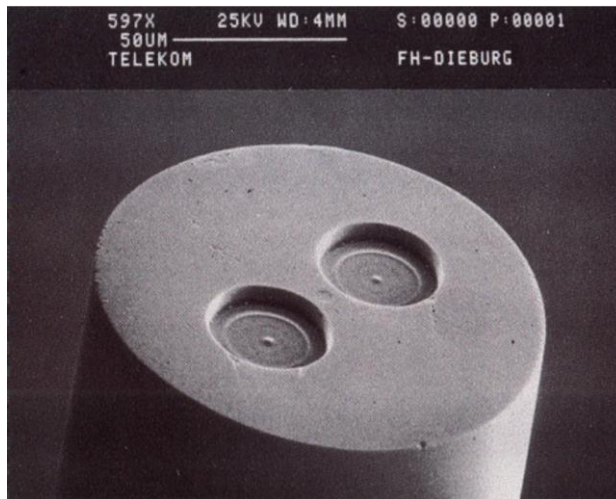
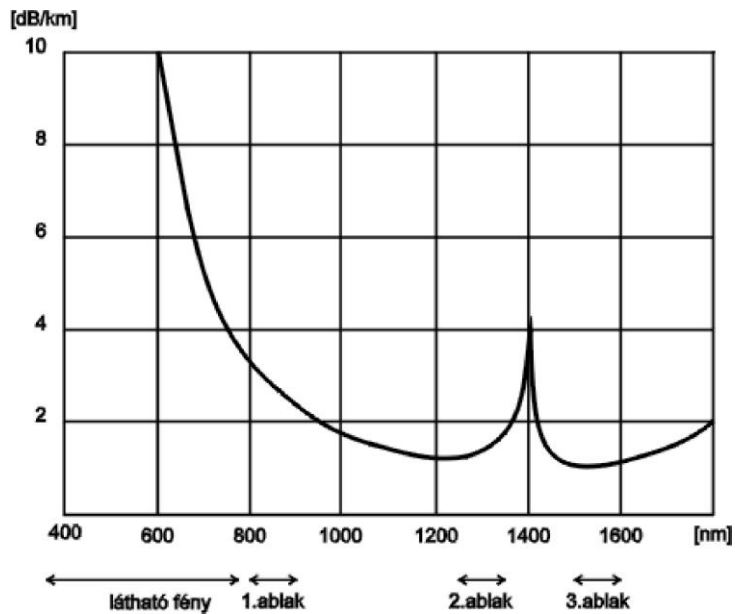
- új fényvezető száltípusok
- új fényvezető kábelstruktúrák
- új hálózati rendszerek
- új építési stílusok, technológiák
- új szerelési technológiák
- új tervezési- nyilvántartási rendszerek – tartalom és forma.

Új fényvezető száltípusok

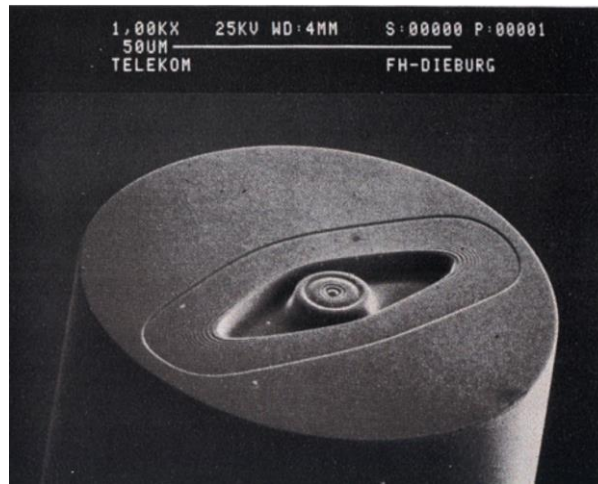
A fényvezető száltípusok fejlesztési irányai: a minél nagyobb távolságok áthidalása, ehhez egyre kisebb csillapítású és diszperziójú szálak gyártása, valamint a sáv szélesség növelését, a DWDM technika alkalmazását befolyásoló „vízcsúcs” eltüntetését a csillapítás/hullámhossz lefutásból.

A vezető szerepet játszó fényvezető szálgyártók a vízcsúcs nélküli szálakat tömegméretben gyártják és a kábelekbe általában már csak ezeket építik be. Az ilyen fényvezető kábelekkel épített hálózat már alkalmas Gigabit átvitelére is.

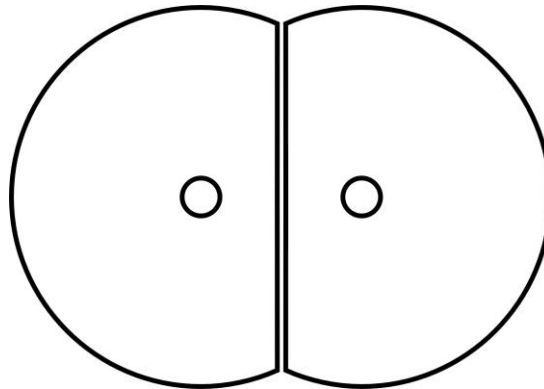
A csillapítás csökkentésére párhuzamosan kifejlesztették a fényvezető szál erősítőket. Ennek egyik példája a „Pandaszál”, amelyben a második mag a pumpáló lézer számára készül.



A nagytávolságú (50 km-nél hosszabb) és több hullámhosszú DWDM átvi-
telt a fényvezető szálak Polarizációs Módus Diszperziója korlátozza. Ennek
kiküszöbölésére új száltípusokat fejlesztettek ki. Ezek közé tartozik az ovális
szál.

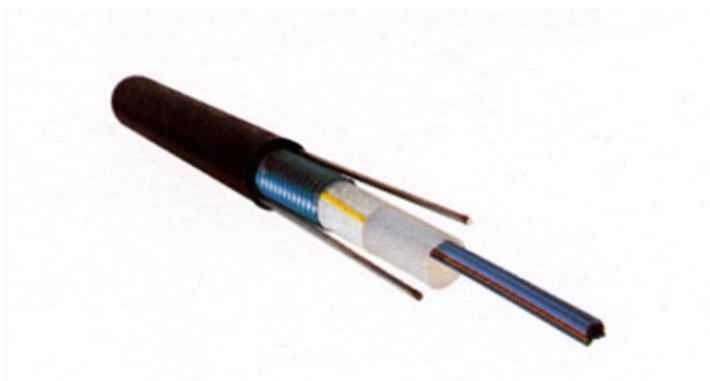


A fényvezető összeköttetések szálkapacitásának növelése érdekében az egy fényvezető szálon két hullámhossz átvitelét az 1x2WDM csatolókkal oldják meg. Ezeknek a csatolóknak a gyártásához fejlesztették ki a D típusú szálakat. 2 ilyen D típusú szál összeillesztésével oldják meg az iránycsatolást.



A szálfejlesztés mellett a kábelfejlesztés is eredményeket hozott.

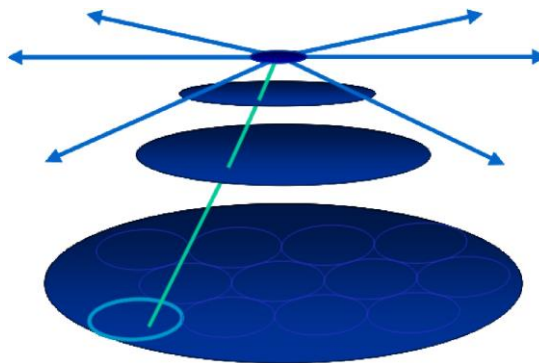
Az egyik kitűzött cél a minél kisebb átmérőjű, minél több fényvezető szálat tartalmazó és minél könnyebb fényvezető kábel gyártása, amely a mechanikai tulajdonságai alkalmassá teszik a fényvezető kábelt új építési körülmények közötti alkalmazására is. Ilyen például a 144 fényvezető szálalású ribbkábel.



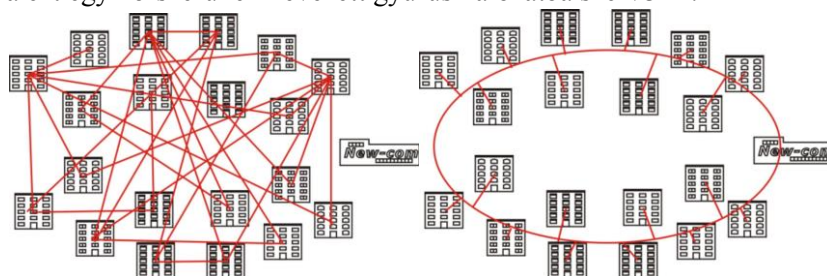
Új nyomvonal nyerését támogatja a nagyfeszültségű oszlopvonalak földelő vezetőibe integrált fényvezető kábel az OPRW is, valamint az ADSS és az AD-Lash kábelszerkezet. Ma hazánkban ezek a kábelszerkezetek a villamos elosztóhálózat belső informatikai céljait szolgálja, de magában foglalja az üzleti kommunikációs alkalmazás lehetőségét is.



Az új kábelfajtákkal egy időben kifejlesztésre kerültek új hálózat rendszerek és stílusok. A vezetékes távközlő hálózat hagyományos építési rendszere a telefonközpontból kiinduló, elosztós rendszerű, fa struktúrájú helyi, előfizetői hálózat. Ez a hálózat felcsatlakozott a primer és szekunder (körzeti- és országos-) hálózathoz és magába foglalja az elosztó- és az előfizetői síkokat.

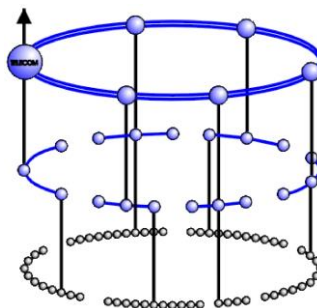


Az üzleti célú távközlési hálózat rendszerben az előfizetők (ügyfelek) összekötését pont-pont közötti, szövevényes hálózattal oldják meg. Még akkor is, ha ezt egy körszerűnek nevezett gyűrűs hálózatba szervezik.

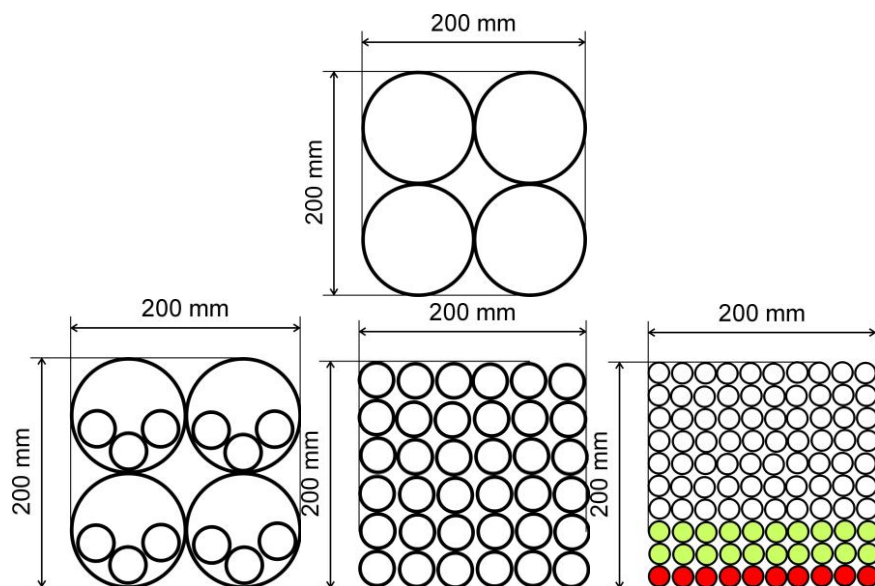


Az igazán rugalmas megoldást az adja, ha ebben a gyűrűs hálózatban is megvalósítják a három síkot, azaz, a trónk síkot, az elosztó síkot és az előfizetői síkot és a síkok közötti átmenetet.

A közmű zsúfoltság miatt, a korlátos nyomvonalai lehetőségek enyhítésére az alépitményi hálózatban az új kábelszerkezetekhez új építési elemek, rendszerek és technológiák alkalmazhatók.

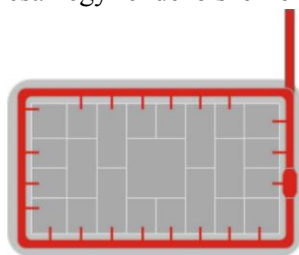


A hagyományos csőhálózat építésénél 100 mm átmérőjű PVC csöveket alkalmaznak. Ha megvizsgáljuk, hogy 4 db 100 mm átmérőjű cső által elfoglalt 200x200 mm-es szelvény helyére milyen cső beépítésekre van lehetőség és ezekbe a csövekbe milyen kábelek és milyen technológiával építhetők be, több megoldást is kapunk.



Az eredmény az mutatja, hogy ugyan abba a szelvénybe akár 100 db 20 mm-es csövet is el lehet helyezni. Ezek a csövek alkalmasak arra, hogy kábel-befűzésos módszerrel a mini kábeleket akár 600 méter távolságban is be lehessen juttatni.

Egy ilyen 100 csövet tartalmazó csőblokkal egy háztömböt úgy ellehet látni, hogy minden épületbe legalább 3-3 cső két irányból bemenjen és a háztömb körüli járdában mindössze csak egy rendező szekrény elhelyezés szükséges.

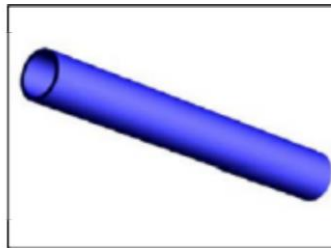


A háztömböket összekötő törzs csövekkel olyan rendszer is kiépíthető, ahol egye úttestek keresztezés mentesek lehetnek.

Az adathálózatok kezdetben irodák között, később épületen belül, majd telephelyek között, végül városon belül épültek ki. Ma már az országos kiterjedésű informatikai hálózatok létesítése is folyik. Ezek a hálózatok egyesíthetik magukban mindazokat a fejlesztési eredményeket amelyeket a fényvezető szálak, a fényvezető kábelek és a hálózati rendszerek terén elértek és már rendelkezésre állnak.



Az üzleti célú hálózatokban egyre gyakrabban jelentkezik az igény a 2 fényvezető szál kicsatlakoztatására. A szokásos fényvezető kábelek között a legkisebb kapacitásúak a 10 illetve 12 szálás kábelek. Ennek az igénynek a kielégítésére fejlesztették ki a fényvezető szál befűzési technológiát. Ennek az a lényege, hogy a szálmenedzselő fényvezető kábelkötésből erősfalú 3-6 mm átmérőjű csövet építenek ki az előfizetőid és ebbe a csőbe fűjják be az 1,2,...12 fényvezető szálát.



Új nyomvonal nyerésére ad reményt az utcai mikrokábel rendszer, amelynek a lényege az, hogy az úttestnek vagy a járdának, egy megfelelő szempon-
tok szerint kiválasztott vonalába 4-12 cm mély kb. 1,2 cm széles vágatot vág-
nak. Ebbe a vágatba fektetik le a különleges szerkezetű, rezgéscsillapított
mikrokábel. A rést bitumen öntéssel zárják le. A remélt építési sebesség kb. 1
km/nap. A fényvezető mikrokábel kötését a burkolatba süllyesztett kettősfalú
fazékkötéssel oldják meg. A mikrokábel hagyományos szerelvényekkel csatla-
kozhat a szabványos építésű fényvezető kábelhálózathoz.



Ennek az építési módnak további előnye, hogy a gyors és egyszerű építési módjából adódóan alkalmas arra is, hogy a katasztrófa sújtotta területen belül az ideiglenes hálózat viszonylag védetten, gyorsan kiépüljön.

PRECISION DIRECTION FINDING ALGORITHM OF RADIO SIGNALS

Sagax, LTD.

Haller u. 11-13. 1096 Budapest, Hungary

Phone: + 36-1-219-5455, FAX: +36-1-215-2126, email:
bertalan.eged@sagax.hu

Abstract

The direction finding problem based on interferometer principle has great accuracy in the angle of arrival estimation. To increase the accuracy there are two main ways. In the first one we add more antennas to the configuration, hence we get more measurement data, but it means that the physical configuration has to be changed. In the second method we design numerical algorithms which gives better estimations. The prize is the complexity and the increased computation time. In this paper a method from the second set is shown and analysed. The algorithm is based on the cross correlation technique.

1. Introduction

While radio direction finding for navigation purposes is losing in importance due to the availability of satellite navigation systems, the requirement for determining the location of emitter increases with the mobility of communication equipment. In the literature lots of situations can be found with respecting to direction finding. In these days one of the most focused application is the GSM system. The mobile phone industry uses the direction finding equipment on every base station. The reason is that using frequency-spreading techniques are increasingly used for wireless communication.

In literature and introduction papers of devices there are several methods according to different requirements. In this work one of the widely used direction finding method, namely the phased interferometer technique is discussed. This solution has some advantages: very high resolution can achieve, and conformal arrays are possible. But the disadvantages are the relative high cost and the larger size.

In this case a four element antenna array configuration is used. The signals of the output of the antenna elements are measured synchronisedly and

converted into digital domain after the corresponding down-converting. In the digital signal processing block the different estimation algorithms are realized with parallel computing, because of the strong computing time constraint.

This measurement configuration induces two separate statistical estimation algorithms. Firstly, the phase difference between two chosen antennas has to be estimated with very small error. Secondly, using the results of the delay estimations between antennas the estimated direction of the emitter is computed. As a matter of fact the first problem is a time delay estimation in the time-domain. In general without using any appropriate information about properties of the signal of emitter(s) it is a very hard problem with high accuracy requirement. Now, in the discussed situation there are radio frequency signals with different modulation methods, such as amplitude modulation (AM), frequency modulation (FM), phase shift keying (PSK), quadrature amplitude modulation (QAM), etc.

First of all this paper gives a brief description of the hardware configuration and the physical setup of antenna elements. Then the estimation problems are mentioned and analysed. In the last two sections a new method is published according to the assumed direction finding situation. In the end there is a brief conclusion section and some further research ideas are formulated.

2. Physical configuration and theory of direction finding

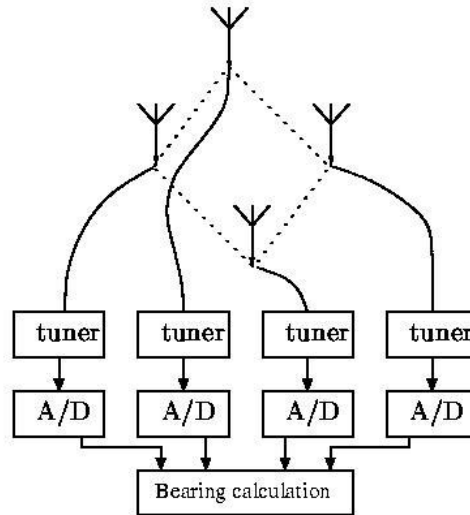


Figure 1: Configuration of direction finder

The direction finder setup can be seen in Fig. 1. We use four antennas in the array whose input signals are converted in the first IF band by the down converter block. The maximal frequency component of this frequency band is such that we can convert signals into digital domain with high frequency A/D converters. The direction estimator component (bearing calculation) of the configuration denotes a digital signal processing part. In this block the computing is in digital domain using DSP and FPGA processors. This kind of setup suits the so-called software radio architecture, thus the analog signals are sampled as soon as possible. Therefore we get high sampling rate and digital signals in pass-band.

The antenna configuration is such that the four antennas are at corners of a square. The minimal distance between two antennas determines the maximal frequency of the input signal. If λ denotes the wavelength of incoming signal and d denotes the distance of two antennas then the following inequality limits the highest frequency component:

Furthermore the physical realization of antennas causes that this setup can be used only in a typical frequency band. The filters in the down converter are specified to operate in this band, hence in digital domain we already know which interval of the time delay is valid.

The interferometer principle is the following. We originate the direction finding problem in time delay measurement. The Fig. 2. shows the basic geometry. The principle is that a plane wave arriving at an angle is received by one antenna earlier than the other due to the difference in path length.

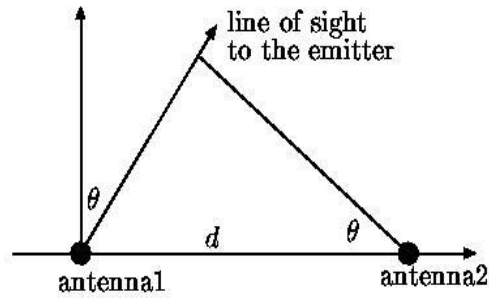


Figure 2: Principles of 2-element interferometer

If the distance of two antennas denotes d and the speed of light c then the time delay between signals of antennas is where q is the angle of the arrival. So with this analytical relationship we can obtain the directional information from the spatial position of the lines or surfaces of equal phase. Hence to solve the angle of arrival (AOA) determination problem we need estimate time

delays and from these results an angle. The details of these numerical algorithms are specified in the next sections.

3. Delay estimation

In our treatment the estimation of time delay suffers from a problem. The time grid (or the frequency grid) , i.e. the sampling time does not give enough resolution for the desired accuracy. Therefore the algorithm which seems to be usable at the first sight has to be refined, like the published, specialised ones in the papers. In the literature lots of possible methods can be found but all of these are valid only in special cases. In these paper the presented algorithms are also such, i.e. application of these limited for direction finding (delay estimation) for communication signals.

In this paper we are assuming that the type of the emitter signal is known, so the modulation method and the type of baseband signal are a priori informations in delay estimation problem. Furthermore, we assume that the emitter signal is a narrow-band one. In practice this condition is current because typically the frequency of carrier signal is 100 MHz and the bit-rate of baseband signal is 100 kHz. After the down-converting process we have maximum 5 MHz bandwidth with central frequency 10 MHz. It causes that with high sampling rate in the IF band the measure of changing of the baseband signal with respecting one segment is little. In the case of analogue baseband signal it means that the modulated signal has narrow-band spectra and in the case of digital modulations the bit rate should have to be slow.

Continuous-wave modulation

Firstly, let us study the case of analogue baseband signals. We consider two main types, namely the amplitude modulation (AM) and the frequency modulation (FM). The latter one as we mentioned is a narrow-band FM signal and since the properties of narrow-band FM signals can be derived from AM signals, in this paper it is enough to study the AM ones [1]. For example, an AM signal with carrier frequency 10 MHz (in the IF band) and an audio baseband signal pass the assumptions above.

If we are sampling such signal with sampling frequency $f_s=40$ MHz, then with conditions above in one segment there are lots of periods of carrier. And the amplitude of the carrier remains approximately constant because of the narrow band modulation.

Even so we cannot guarantee that the sampling is coherent, the result of FFT is approximately a line, because we get more periods. The problem is

that the frequency grid cannot guarantee desired resolution. And the determination of the maximum of a sine is not a well-conditioned problem especially with presented noise. To increase this we have to resample (interpolate) the spectra. This means that low-pass digital filters have to be designed. A more efficient method is to use analytical model. Obviously, the application is limited to the corresponding modulation method. But, if we use analytical model only in the case of part of cross-correlation function, then the computing time and complexity of model will be reduced. The background of this methods is that the cross correlation function has a local maximum at the true value of the delay.

With using the fact, that the auto-covariance function of a sinus function is also a sine, we can approximate the neighbourhood of the corresponding, global maxima with a parabola. Since the parabola fitting problem is an efficient and quick numerical algorithm, it takes short time to determine the local maxima. To fit a cosine function on the given time grid is not such easy problem, especially to determine the frequency is not an easy and quick algorithm. This is the reason, why the parabola fitting methods gives more acceptable result with respecting to computing time. Of course, if we consider a better model for communication signals and formulate a non-linear minimisation method then we can get better estimation for the time delay. The main problem is that solution of non-linear minimisation problem expect some cases has no predictable computing time and is too complex.

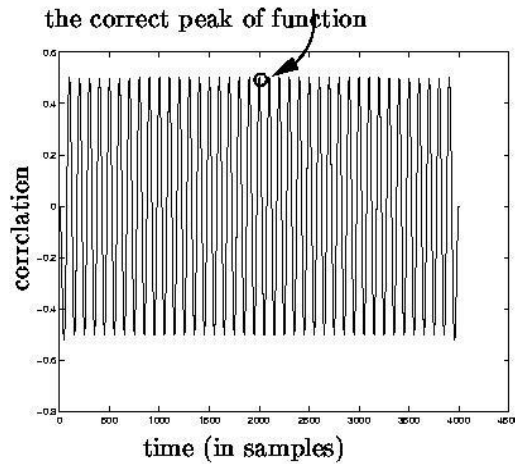


Figure 3: Correlation function of analog modulated signals

In the Fig. 3. a typical correlation function can be seen. It is approximately a sine function and has lots of local maxima. The correct one

can be selected by the known antenna distance d , the mixer frequency and the sampling rate. After the localisation of correct maximum of the correlation function we have to call the parabola fitting routine to determine the more precise the maximum of the sine function.

Digital modulation

Secondly, we study the digital modulations. The model of emitter can be seen in Fig. 4.



Figure 4: Model of emitter

The message source block emits pulse signals with given pulse rate. This signal is filtered by a Nyquist filter (in this case a raised cosine one) which is commonly used in communication system to avoid inter-symbol interference. And the result is up-converted to the desired frequency band by the mixer block. As we mentioned above we assuming that the bit rate is slow with respecting the carrier frequency. In our receiver we are processing segments of samples and we suppose that in one segment there is only fixed number (max. 10 pieces) of bit changing.

The impulse response $p(t)$ of a raised cosine filter is the following:

$$p(t) = (\text{sinc}(2Wt)) \left(\frac{\cos(2\pi\alpha Wt)}{1 - 16\alpha^2 W^2 t^2} \right)$$

.where the parameter α is the roll-off factor. The frequency parameter f_1 and bandwidth W are related by

$$\alpha = 1 - \frac{f_1}{W}$$

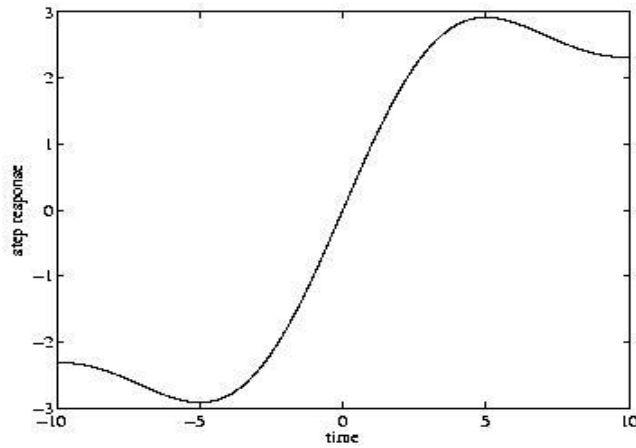


Figure 5: Filtered pulse by raised cosine filter

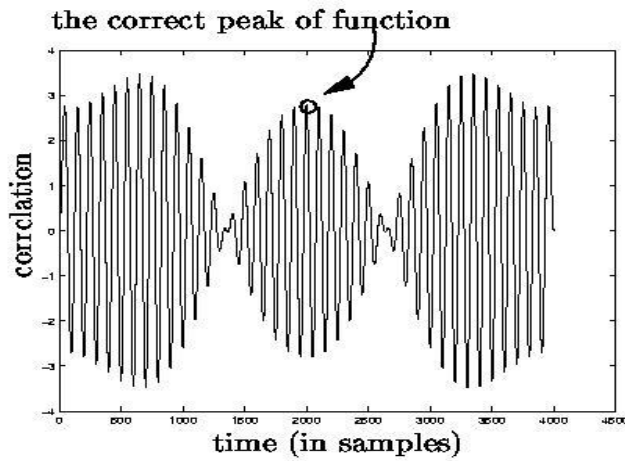


Figure 6: Correlation function of digital modulated signals

Fig. 5. depicts the step response of raised cosine filter. As a matter of fact it is a filtered pulse.

As in the previous subsection in Fig. 6. the correlation function can be seen. Because in the case of digital modulation we cannot state that the modulation signal is quasi constant, the cross correlation function is not a sine function. But, like in the figure to find the correct local maximum of the function we have to use the parameters of the receiver.

Parabola fitting

In this subsection we study the approximation of cross correlation function. Because of its symmetrical property in the neighbourhood of the true delay value the correlation function can be approximated with a parabola. It means that with a few points (samples) we get an approximation and its analytical maxima gives a good estimation. If we using the frequency domain identification method then statistically we get better result but if the segment of the signal consists at least one bit changing then using the cross correlation gives better estimation.

We suppose that the neighbourhood of the t value has M points. Then in the approximation problem we define the following norm that is the usually least squares norm.

$$\|a - b\| = \sum_{j=1}^M |a(x_j) - b(x_j)|^2$$

where x_j are the sampling points in the corresponding neighbourhood and a, b are two functions from this interval to the real line. Because these function space is a Hilbert space with respecting to the norm above, therefore the solution (which is a projection) is exists and unique. In our case a is the cross correlation function and b is a second-order polynom. The background of this kind of approximation is Taylor serie. Furthermore, since the cross-correlation function is a linear combination of sinus, this approximation sounds well.

Numerically the projection finding leads to solution of the following linear equations.

$$\begin{bmatrix} 1 & x_1 & x_1^2 \\ 1 & x_2 & x_2^2 \\ \vdots & \vdots & \vdots \\ 1 & x_M & x_M^2 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \end{bmatrix} = \begin{bmatrix} a(x_1) \\ a(x_2) \\ \vdots \\ a(x_M) \end{bmatrix}$$

with using that

$$b(t) = b_0 + b_1 t + b_2 t^2$$

4. Angle of arrival estimation

After for antenna pairs the delay estimations are finished, the angle of arrival can be computed from the propagation vector.

Now, the propagation vector k of target signal can be defined as

$$k = \frac{1}{c} \frac{x_0 - x_{\text{src}}}{\|x_0 - x_{\text{src}}\|}$$

where x_0 denotes the centre of the array. $\|\cdot\|$ denotes the L2-norm of a vector. Furthermore, the vector between the i th and m th antenna is denoted by

$$x_{im} = x_m - x_i$$

where x_i and x_m are two dimensional vectors representing the antenna locations in an orthogonal coordinate system.

Hence, the time delay t_{im} between the signals received by the i th and m th antenna can be calculated as

$$t_{im} = k^T x_{im}$$

Put it in matrix form, this equation for all antenna pairs can be represented by

$$V k = \hat{\tau}$$

with

$$V = [x_{i_1 m_1} \ x_{i_2 m_2} \ \dots \ x_{i_M m_M}]^T$$

$$\hat{\tau} = [\hat{\tau}_{i_1 m_1} \ \hat{\tau}_{i_2 m_2} \ \dots \ \hat{\tau}_{i_M m_M}]^T$$

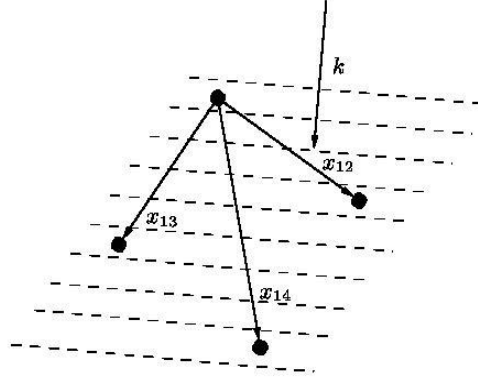


Figure 7: Propagation vector

Hence from k we can obtain the corresponding angle.

Proposed algorithms

Now, we give a compact description of the algorithms. In every step the corresponding computational algorithms can be run parallel, so the total processing time can be reduced significantly.

- Do the down conversion and sampling for every antenna.
- Calculate the cross-correlation function for the proper antenna pairs.
- Find the correct local maximums.
- After the parabola fitting estimate delays for antenna pairs.
- Calculate propagation vector and AOA from the obtained delay values.

5. Conclusions

In this paper we gave a brief description about the direction finding with interferometer principle. We described the main problems which arrived in the case of communication signals. The published algorithms is robust which can be explained by theoretical way. This algorithm has the advantage that it is easy to compute in parallel way. Of course, there are more work to develop better and more robust algorithm to different modulation methods, however the space and time are limited.

References

- [1] Simon Haykin, Communication System, John Wiley & Sons, Inc., 1994
- [2] Istvan Kollar, Signal Enhancement of nonsynchronized measurement for frequency domain identification, IEEE Transaction on Instrumentation and Measurement, no. 1. Pp. 156-159, 1992.

ELEKTRONIKUS BŰNÖZÉS. HAZAI ÉS KÜLFÖLDI TAPASZTALATOK

Ma az elektronikus adatfeldolgozás és –átvitel modern technológiája lehetővé teszi az információ nagysebességű áramlását, adatállományok gyors feldolgozását, továbbítását a társadalmi élt minden szférájában, valamint a privát életünkben is.

Az informatikai bűncselekmények számos fajtáját ismerjük. Ilyenek: a vagyoni haszonszerzés, hamisítás, adatkikémlelés, számítógép, a programok és az adatok ellen véghez vitt intellektuális és erőszakos támadások, a programok és információhordozók jogosulatlan megszerzése, másolása, kereskedése, bankkártyákkal való visszaélés. A legmodernebb jogsértések: a mobiltelefonokhoz tartozó SIM-kártya manipuláció, és az intra-, extra-, Interneten elkövethető, megjeleníthető jogellenes cselekmények.

Az informatikai bűncselekmények – kivéve a fizikai rongálást – intellektuális jellegűek. Igazi intellektust igényel a számítástechnikai rendszerekben hamisítást, vagyoni kárt okozó jogsértések. Ilyenek például a férgek, vírusok, logikai bombák gyártása és a rendszerekbe juttatása.

Fehérgalléros bűnözés egy gyűjtőfogalom, többnyire büntetlen előéletűek az elkövetők. (2) Ehhez a bűnözési formához tartozik az informatikai bűncselekmények elkövetései is. Az alábbi bűnözési formákat különítjük el egymástól:

- Foglalkozási (occupational): az elkövető munkakörét felhasználva saját magának szerez jogtalan előnyt, vagyoni hasznot számítógép felhasználásával. A magyar Büntető Törvénykönyv szerint ide tartozik a dematerializált értékpapírra (Btk. 333.§), lopás (Btk. 316.§), sikkasztás (Btk. 327.§), számítógépes csalás (Btk. 300/C.§). Tipikus elkövetők az operátorok, és számítógép kezelők.
- Szervezeti (corporate): a szervezet érdekében, a szervezet számára biztosítandó előny, vagyoni haszon elérését követnek el. A magyar Büntető Törvénykönyv szerint ide tartozik adó-, társadalombiztosítási csalás (Btk. 310.§.), az üzleti titok megszerzése a konkurens cégtől (Btk. 222.§.), az ügyfelek dematerializált értékpapír formájában megjeleníthető járandóságának elsikkasztása (Btk. 317.§.).(1)

A konkrét megjelenési formákat és magatartások külföldi szakemberek megpróbálták osztályozni, elkülöníteni egymástól. A szakirodalom szerint az alábbi osztályozások figyelhetők meg:

Gabriele Schmölzer és Peter Schich szerint:

1. támadás a hardver ellen
 - a. jogosulatlan belépés
 - b. gépidőlopás
 - c. a mikrochip jogtalan másolása
2. támadás a szoftver ellen
 - a. szoftverlopás
 - b. programmanipuláció
3. támadás az adat ellen
 - a. adatmanipuláció
 - b. adatlopás
 - c. visszaélés az adatfeldolgozási tevékenységgel(3)

Adler-Mueller-Laufer szerzőhármassal szerint:

1. számítógépes csalás
2. számítógépes kikémlelés
3. számítógépes szabotázs
4. számítógépes hacking
5. számítógépidő-, szoftver, és hardverlopás(4)

Az angol Martin Wasik szerint:

1. jogosulatlan hozzáférés a számítógépben tárolt adatokhoz vagy programokhoz;
2. számítógépes csalás;
3. adatok vagy programok jogosulatlan elvitele;
4. a számítógépidő és szolgáltatás jogosulatlan használata;
5. rombolás vagy károkozás.(5)

A **OECD** által kiküldött ad hoc bizottság 1983-1985 között feladata volt elemezni, és összegezni az európai judikatúra tapasztalatait. A bizottság a következőképpen rendszerezte a jogsértéseket:

a) számítógépes adatok és/vagy programok bevitele, módosítása, törlése vagy elmentése jogtalan vagyoni eszközök vagy más értékek megszerzése céljából;

b) számítógépes adatok és/vagy programok bevitele, módosítása, törlése vagy elmentése hamisítás céljából;

c) számítógépes adatok és/vagy programok bevitele, módosítása, törlése vagy elmentése, vagy a számítógépbe történő bármely más beavatkozás a számítógépes vagy telekommunikációs rendszerek funkcióinak megakadályozása céljából;

d) a védett számítógépes programok tulajdonosai exkluzív jogainak megsértése a program jogosulatlan hasznosítása vagy forgalomba hozatala révén;

e) a számítógépes vagy telekommunikációs rendszerbe az arra jogosult engedélye nélkül, vagy a biztonsági intézkedések megsértésével vagy más tisztességtelen, netán bűnös szándékkal történő belépés, vagy annak lehallgatása.(6)

Az **ET** ajánlást bocsátották ki 1989-ben abból a célból, hogy felmérje a számítógépes bűncselekmények realitását és valós veszélyeit, összegezze. Az ET (89) 9. számú ajánlásában szerepel egy minimumlista és egy fakultatív lista a javasolt szankcionálásokról. A következő valamennyi bűncselekmény büntetőjogi üldözésének feltétele az, hogy az elkövetés szándékosan történjen.

a) A számítógépes csalás: adatok, programok bevitele, megváltoztatása, törlése, elmentése, vagy más, az elektronikus adatfeldolgozási folyamat befolyásolását eredményező magatartás, amellyel az elkövető egy harmadik személynek gazdasági vagy vagyoni hátrányt okoz, illetve amelynek célja az, hogy az elkövető önmaga vagy más számára gazdasági vagy vagyoni előnyhöz jusson. (Alternatív javaslat: azzal a céllal, hogy az elkövető mást vagyontól megfossson.)

b) A számítógépes hamisítás: adatok, programok bevitele, megváltoztatása, törlése, mentése vagy más, az elektronikus adatfeldolgozási folyamat befolyásolását eredményező beavatkozás, amelynek révén megvalósul a hazai (nemzeti) jogban meghatározott hagyományos hamisítás bűncselekménye.

c) A számítógépes adatokban és programokban történő károkozás: az adatok és/vagy programok jogosulatlan törlése, rongálása, károsítása, mentése.

d) A számítógépes szabotázs: olyan adatok és/vagy programok bevitele, megváltoztatása, törlése, vagy a számítógépes rendszerek más befolyásolása, amelynek célja, hogy annak telekommunikációs funkcióját akadályozza.

e) A jogellenes behatolás: a számítógépes rendszerbe vagy hálózatba történő jogosulatlan bejutás a biztonsági intézkedések megsértése révén.

f) A jogellenes titokszerzés: a számítógépes rendszerből vagy hálózathoz jogosulatlan tudomásszerzés technikai eszközökkel.

g) Védett számítógépes programok jogellenes másolása: a jogi oltalommal bíró programok jogosulatlan reprodukálása és értékesítése.

h) A félvezető topográfiák jogellenes másolása: a jogi oltalommal bíró félvezető topográfiák jogosulatlan reprodukálása azok gyártása, kereskedelmi értékesítése és importja, valamint e termékek felhasználása céljából.

Az **ET fakultatív** listáján szereplő cselekmények:

a) a számítógépes adatok és/vagy programok megváltoztatása: ha jogosulatlan valósul meg;

b) a számítógépes kémkedés: kereskedelmi vagy üzleti titok jogosulatlan, vagy törvényes felhatalmazás nélküli megszerzése, nyilvánosságra hozatala, mással való közlése azzal a céllal, hogy a titok jogosultjának gazdasági hát-

rányt okozzon, illetve a titok megszerzésével önmaga vagy más számára jogtalan előnyt szerezzen;

c) a számítógép jogellenes használata: a számítógépes rendszerek és hálózatok jogosulatlan igénybevétele során az elkövető:

- jelentős kár okozását kockáztatja a jogosult sérelmére, vagy magát a rendszert, illetve funkciójának ellátását kockáztatja, vagy

- azzal a szándékkal cselekszik, hogy a jogosultnak, a rendszerben, illetve annak funkciójában kárt okozzon, vagy

- ténylegesen kárt okoz a jogosultnak a rendszerben, annak funkciójában;

d) védett programok jogellenes használata: a program olyan jogosulatlan használata, amely feloleli annak jogosulatlan megszerzését önmaga vagy más számára, továbbá minden olyan használat, amely a tulajdonos jogait sérti.(7)

A bűnözés története

Az 50-es évek végén az MIT nagygépek, amelyek katonai, illetve tudományos célokat szolgáltak, szűk memóriakapacitásúak voltak. Számítógépes szakemberek a programokból törekedtek "faragni", hogy minél több hely maradjon a feldolgozni kívánt adatok számára. Őket hívták "hackereknek", akik jó, és nemes szándékkal avatkoztak be az elektronikus adatfeldolgozás folyamatába.

Napjainkban szellemi kihívásként, "párbajként" fogják fel a számítógépet, a számítógépes rendszereket védő kódok megfejtését. A kiváltó okok többnyire: vonzza őket a kíváncsiság, az unalom, a játékoság, vagy hogy felvág hassanak a társak előtt. Ma a szervezett bűnözés szolgálatába szegődve, megbízásból, könnyű pénzszerzésért, kábítószerért vagy csupán fanatizmusból adják el tudásukat. A lengyel Andrzej Adamski felveti, hogy a "jó hacker" a rendszerbe történő illetéktelen belépésének is lehetnek direkt és indirekt jótékony hatásai. (8)

A jó hacker letörli a pornográf, a pedofil képeket bemutató oldalakat, a gyűlöletkeltésre alkalmas uszításokat, a szélsőséges politikai és vallási nézeteket tükröző, efféle szervezeteket hirdető irományokat, képeket, a kábítószer fogyasztását vagy a bombakészítést népszerűsítő oldalakat. A jó hacker a rendszer tökéletlenségeit is kijavíthatja (például gyorsabbá teheti, a leginkább használt könyvtárakat, fájlokat könnyebben elérhetővé teheti). Közvetetten pozitív eredménye az elektronikus adatfeldolgozó és -átviteli rendszer védelmi hiányosságainak felfedése, ami további biztonsági elemek alkalmazására ösztönöz. De ezzel védett rendszerbe lép be jogosulatlanul, és ezzel kárt okoz a helyi hálózat üzemeltetőjének. A weboldalak újraépítése, a jelszavak, kódok ismételt előállítás, a ráfordított munkaidő, az adatfeldolgozásból kiesett munkaórák stb. mind-mind akár vagyoni, akár pénzben ki nem fejezhető kárt okoznak.

Német országban a nyolcvanas évek végén, a skandináv országokban a kilencvenes évek elején, Olaszországban 1993-ban, Magyarországon 1994-ben követték el az első informatikai bűncselekményeket, amelyeket "első generációs informatikai bűncselekménynek" nevezünk.

A számítógépes bűnözés lehetséges motívumai

A számítógépet legálisan használók, olyan adatállományokhoz kívánnak hozzáférni, amelyekhez a belépési jogosultságuk nem elégséges.

Így az adatokról tudomás szerezhető, részben vagy egészben megváltoztathatók, törölhetők, kiegészíthetők, átrendezhető, az nem, vagy másképp értelmezhető. Ez vagyoni kárt okozhat, sértheti az adat tulajdonosának magánszféráját, vagy más jellegű hátrányt idézhet elő. Egy jogtalan törlése megbéníthat távközlést, gyártási tevékenységet, pénzügyi folyamatokat. Alkalmas lehet pornográf, gyűlölködő szövegek, ábrák stb. létrehozására. Tehát jellemző motívum a védett személyes adatok, és állam-, szolgálati, üzleti és banktitkok jogellenes megismerésére irányuló szándék.

Lássunk példát arra, hogy hogyan történ ez a nagyvilágban:

- „Az USA kormányzata 1999 tavaszán, a NATO Jugoszlávia ellen vívott háborúja idején olyan hackereket keresett, akiknek Milosevic jugoszláv elnök feltételezett görögországi, ciprusi, oroszországi bank-számláihoz kellett volna hozzáférniük, és azokról a pénzüsszegeket lehívni, hogy ily módon megakadályozzák a szökését.”(9)
- „A leghíresebb-hírhedtebb hacker, Kevin Mitnick (alvilági nevén Condor), aki az ezredfordulón volt 35 éves, és már többször elítélték a legkülönbözőbb elektronikai bűncselekményekért. 1988-ban egyévi szabadságvesztésre ítélték programsolásért, bankkártyák számainak kifürkészéséért. Szabadulása után továbbra is illegálisan "látogatja" a több tucat telefontársaság, szoftvergyártó cég hálózatát, ahonnan mobiltelefonok kódjait, szoftvereket szerez. Ezekért 46 hónapi szabadságvesztésre ítélték. Három évre eltiltották számítógép, mobiltelefon és egyéb technikai eszközök használatától.”(10)
- „Hátborzongató az egyesült államokbeli milwaukee-i "414-esek" (az ottani körzet hívószáma) esete. Az elkövetők a manhattani Sloane-Kettering Memorial Cancer Center számítógépes rendszerébe hatoltak be, és átprogramozták az ott kezelt rákbetegek adatait. A csoport egyik 17 éves tagja fedte fel a sajtónak cselekedetüket.”(11)
- „Az elektronikus adatfeldolgozó rendszerekben tárolt adatok vagy programok vagyoni haszonszerzési céllal történő manipulálása is tipikus motívum. A szintén egyesült államokbeli Kevin Poulson, betörve egy telefontársaság hálózatába, a nyereményjáték rendszerét úgy alakította át, hogy a sorsoláson egy autó "szerencsés" nyertese lett.”(12)

-
- A szervezett bűnözők is fantáziát látnak a könnyű pénzszerzés eme fajtájában. „Az orosz maffia megbízásából Vlagyimir Levin 1994-ben Szentpétervárról negyven alkalommal tízmillió dollárt hívott le az egyesült államokbeli Citibank számláiról, és a pénzüsségeket holland, finn stb. bankok számláin helyezte el. Angliába érkezésekor tartóztatták le, és az eljárás az USA-ban a mai napig tart.”(13)
 - Mind ez ideig a legtetemesebb kárt okozó bűncselekmény-sorozatot - amelyről a Guinness Rekordok könyve is beszámol – „1963-74 között követték el, amikor is az Equity Founding Corporation (az egyik egyesült államokbeli biztosítótársaság) számítógépeivel a cég munkatársai hamis kötvényeket készítettek, amelyekre fiktív kifizetéseket tettek. Hatvannégyezer fiktív biztosítási kéreletért kétfélmillió dollárt fizettettek ki a társasággal.”(14)
 - Stanley Mark Rifkin 1980-ban, elítélésekor csak 34 éves volt. „Számítástechnikai tanácsadóként dolgozott a Los Angeles-i Security Pacific Bankban. Itt az alkalmazottak az aznapi forgalmat az ügyfelek kódjaival egymásnak átkiabálják. Rifkin 1978. október 25-én egy utcai telefonfülkéből az egyik ügyfélszámlaszámra a hozzárendelt kódszám azonosításával 10,2 millió dollárt utaltat át a New York-i Serving Trust Bankba. A bűncselekményt nyolc nappal később észlelik, majd később a telefonhívás alapján azonosítják a telefonálót. Közben Rifkin az átutalt pénzből Svájcban egy fiktív cég nevében gyémántot vásárol. Visszatérve az Egyesült Államokba, ügyvédjének könnyelműen kérkedik gyémántjaival, aki azonban feljelenti. A bíróság az elkövető cselekményét lopásnak minősítve kilenc évi szabadságvesztés-büntetést szabott ki rá.” (15)
 - „A nyolcvanas évek elejéről származó egyik FBI-jelentés kiemeli, hogy míg a fegyveres bankrablással az elkövetők átlagosan tízezer dollárt zsákmányolnak, addig a komputeres elkövetés révén átlagosan egymillió dollárt.”(16)

Mi a motívum, a cél?

A haszonszerzés. A szoftverek jogosulatlan másolása, használata, forgalmazása, a félvezetők (chipek) tiltott másolása, kereskedése, a pornográf tartalmú képek felvitele, amelyek regisztrációs díj fejében érhetők el.

A legrosszabb amit elkövethetnek az elektronikus adatfeldolgozó és -átviteli rendszerek elleni támadások közül a vírust, férget és logikai bombát tartalmazó programok elhelyezése. Hatásuk lehet átmeneti (például dallamlejátszás, az adatfeldolgozás lassítása, továbbá ábrák, szövegek megjelenése a monitoron) vagy állandó (például fájlok tartalma megváltozik, megsemmisül).

A hálózatok világméretűvé válásával bármely ország állampolgára, akármilyen időpontban, akármilyen távolságra lévő intézmény adatállományához hozzáférhet. Ezt fémjelzi nemzetközi jellegét.

Nemzetközi példák:

„1985 márciusában a Los Angeles-i víz- és energiaügyi részleg számítógépeit a vírusok egyik fajtája, egy "logikai bomba" bénította meg.”(17)

„1988-ban Robert Morrison Cornell, akkor 24 éves egyetemi hallgató 6000(!) számítógépet fertőzött meg, köztük a féltve óvott NASA és a US Air Force legvédelettebb rendszereit.” (18)

„A katonai célú vírusok, a szembenálló fél védelmi rendszerének számítógépeit blokkolják.”(19) /Egyelőre nem lebbentik fel a fátylat arról a titokról, hogy az amerikaiak légi fölénye az Öböl-háborúban az iraki légvédelmi rendszert bénító vírusoknak köszönhető-e vagy sem./

Jellemzője még az elkövetés gyorsasága. Az elkövetés gyorsasága növeli a bűncselekmény veszélyességét, mivel a tettenérés nehézkessége gyengíti az eredményes nyomozást, tehát a büntetőjogi felelősségre vonást, végső soron a bűnmegelőzés esélyeit.

A magyarországi bűnözés aránya 1995-1998 között a kb. 500 ezerről közel 600 ezerre emelkedett, bár a mintegy 60 ezer rendbeli csalássorozat lerontja az 1998-as adatokat. 1999-ben ismét alig haladta meg az 500 000-es bűncselekményszámot. 1999-ben csökkent a számítógépes csalások száma, addig kárértékük jelentősen nőtt. 1998-ban a számítógépes csalással okozott kár 2,2 millió forint volt, 1999-re 7,1 millió forint lett. (20)

Felhasznált irodalom:

1. Büntető Törvénykönyv
2. Balogh Zsolt: Jogi informatika. Budapest-Pécs, 1998,266.o.
3. International Review of Penal Law. 1-2/1993,p.134
4. International Review of Penal Law. 1-2/1993,p.134
5. Matrin Wasik: crime and Computer. Oxford, 1991, pp. 2-3.
6. CD Computer-related Criminality: Analysis of Legal Police. Paris, 1986, p.
7. Council of Europe Legal Affairs: Computer-related Crime. Recommendation No. R (89) 9. Strasbourg 1990, pp. 36-39.; International Review of Penal Law 1-2/1993, pp. 673-680.
8. Andrzej Adamski: Crimes related to Computer Network (Bűncselekmények a számítógépes hálózatokkal összefüggésben) című előadásának szövegéből, 20-21. o. Az előadás elhangzott: VI. European Colloquium on Crime Policy and Criminal Policy, Helsinki, 1998. december 10-12.
9. Newsweek, 31 May 1999, p. 22.
10. [www.index.hu\cikkek0001\kevinm](http://www.index.hu/cikkek0001\kevinm) és www.kevinmitnick.com

-
11. Smith, A. N. - Alexander, W. J. - Medley, D. B.: Advanced Office Systems. Cincinnati-Ohio, 1986, p. 402.
 12. Ralph M. Stair: Computers in Today's World. Illinois, 1986, p. 502.
 13. www.spb.su/sppress/141/quilty.html;
www7.gratisweb.com/maganet/hacker9.htm
 14. Smith, A. N. - Alexander, W. J. - Medley, D. B.: Advanced Office Systems. Cincinnati-Ohio, 1986, p. 402.
 15. Ralph M. Stair: Computers in Today's World. Illinois, 1986, p. 502.
 16. Cunningham, W. H. - Aldag, R. - Swift, C. M.: Introduction to Business. Cincinnati-Ohio 1984, p. 445.
 17. Heti Világgazdaság, 1992. február 9., 39-40. o.
 18. Ulrich Sieber: The International Emergency of Criminal Information Law. Köln-Berlin-Bonn-München, 1992, p. 2.
 19. Heti Világgazdaság 1992. február 9., 39-40. o.
 20. A Belügyminisztérium Adatfeldolgozó Hivatal és a Legfőbb Ügyészség számítástechnika-alkalmazási és információs főosztály által évenként kiadott Tájékoztató az egységes rendőrségi és ügyészségi bűnügyi statisztikai adatokról című kiadvány. Budapest, 1995, 1996, 1997, 1998, 1999
 21. Nagy Zoltán András: Bűnözés Magyarországon, Informatikai Bűncselekmények. Magyar Tudomány, 2001/8

Károly FEKETE

EVOLVING POSSIBILITIES OF THE STRATEGIC MILITARY NETWORKS

Zrínyi Miklós National Defense University
Hungária krt. 9-11. 1058 Budapest, Hungary
Phone: + 36-1-432-9000/29153, FAX: +36-1-432-9025,
email: fekete@zmne.hu

Abstract

This paper presents an overview of the possible but not without fail practicable improving the infrastructure of the strategic military networks (SMN). Candidate infrastructure within the SMN is constructed from a variety of switching and routing technologies and transport systems. This paper describes those new and relevant technologies which will have to address interoperability, ease of use, legacy applications, bandwidth, IP and video transport. Nowadays the most popular application in hungarian SMN is TDM but we must pay attention to more flexible solutions as the ATM, IP, MPLS and optical networking.

Introduction

For the past few years, the Department of Military Communications System Management of Zrínyi Miklós National Defense University has been focused on how to implement the modern and powerful communication technologies. The main goal was achieve the solutions of new global infrastructure in areas of tactical and operational communications networks. The legacy technologies as analogue and time-division multiplexing are assimilated into the SMN but such a new applications as the multimedia and videoconference with special regard to network centric warfare¹ (NCW) compose the bandwidth bottlenecks. During the interim period, military network planners will need to provide solutions that will improve by offering increased bandwidth resources.

The NCW and bandwidth hungry applications are suppose:

¹ Network Centric Warfare (NCW): an information superiority- enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronisation. (Global Information Grid (GIG), JROCM 134-1, 30 August 2001 – unclassified-, p 77.)

-
- wire and wireless communications, to allow hungarian and joint forces to share information for both updating situations and receiving instructions;
 - processes information or data for use by separated facilities, hardwares and softwares;
 - real-time surveillance, for immediate assessment and response to actual events.

As we can see the data transfer or network link layer of open system interconnection (OSI) must be universally accessible by all command decisions and support to all who are connected to SMN.

Beginning the evolution

The networks within the SMN are constructed from a variety of analogue and digital switching and automated routing technologies. The communications traffic in the hungarian SMN have got three basic types: military user, control and management communications. Several military connections currently provide security services for user traffic too.

The other type of the traffic is control traffic which is indispensable for establishing user connections (f.e. signalling, naming, addressing and routing). The third type of the traffic is management traffic necessary to configure and monitor network components, inform to network infrastructure, network failure, handle auditing and handling, and provide to secure information flow.

Taking protocol-agnostic characteristics of TDM and plesiochronous digital hierarchy into consideration we must make it absolutely clear that TDM still fulfilling their mission. In Hungary this TDM equipments have been in stationer place for a long time (aprox. 20-25 years), good trained personnel available any time to operate and maintain these and –the most important think is- the communications application are designed on these systems.

The TDM based equipment have inability to support rapid communications evolution² of communications applications. By the way the TDM equipment is easy to set up but changes in configuration require addition hardware modules, transported and installed by trained personnel. Consequently the TDM based technology is a big challenge in front of developing a fast, modern and flexible hungarian fighting force.

What are the alternatives?

Asynchronous Transfer Mode (ATM)

The ATM was conceived to be a „universal” transport solution that could accept data streams by ATM Forum which was founded in 1991. ATM has got a serious advantage in contrast with TDM: ability to transport synchronous

² Communications evolution: relatively slow and gradual process of change that is initiated by a need to better adapt to a changing communications environment and ends with a mastery of the environment.

serial data, variable bit rate data, and packet data. These possibilities fits well to voice, Narrow Band ISDN, encrypted data and IP traffic of military users.

Beyond these advantages the ATM has a robust traffic management capability that supports several classes of service. As we know the ATM was evolved by control of International Telecommunication Union (ITU) and ATM Forum therefore the ATM has got a well standardised protocol set and have got a high level of interoperability across a complex set of different features and ATM can support a wide variety of vendors. Make a comparison between ATM and IP the measurement reflect that, for links that pass both voice and data, that ATM is more bandwidth efficient than IP services³.

Seen from the security aspects the ATM give a satisfaction to claim to:

- scalability (the support dynamic connectivity across large networks);
- compatibility (correct functionality and impose minimal performance penalties in networks);
- separability (possibility of individual applications and combinations, repeatability).

Internet Protocol (IP)

In the year of 2001 the Information Department of J6 of Hungarian General Staff announced a strategy to begin planning and realizing of an information backbone network (IBN) based on Internet Protocol. The IP resides in Layer 3 (Network Layer) of the OSI model, while the most common Layer 2 protocol is ATM. The version of IP in IBN is IPv4.

Recently, implementations of IP version 6 (IPv6) have become commercially off the shelf (COTS) available. The IPv6 protocol set extended compare with IPv4 from 32 to 128 bits satisfying a global demand for IP addresses. In addition the IPv6 have got an additive 8 bits traffic management extension which can help to assign a queuing priority to packets to facilitate quality of service (QoS).

On the other hand there is no traffic management standard in the IP. Even with the IPv6 features, the IP is still a „best-effort” protocol and can not give a guarantee for certain transport of data of a multi-hop military network.

Regarding evolution we can say: „The conversion from IPv4 to IPv6 will be a larger task for the industry than the penetration for Year 2000... Unlike the Year 2000 issue, the conversion to IPv6 has no specific timeline”⁴.

In point of view of security the IP suggests the infrastructure security, cryptographic integrity check and several security protocols.

³ Evolving the DoD Network: A Transition to Net-Centric Warfare, DNE Technologies, Inc., p. 8., 2003., www.dnetech.com

⁴ Microsoft's Objectives for IP version 6 (newsletter), Microsoft Corporation, October 6, 2000.

Multi-Protocol Label Switch (MPLS)

MPLS standards are being developed mainly by the IETF MPLS Working Group.

MPLS is a packet forwarding technique to improve throughput, QoS support, and communications traffic engineering of IP router-based networks⁵. Compare with IP, the MPLS in Label Switching Routers (LSR) in the core networks use Switching based on pre-assigned labels, which reduces the amount of packet handling. On the Table No. 1. we can see the comparison of different modern communications technologies in point of view of different information types.

Table No. 1.

	TDM, IPv4	MPLS, IPv6	ATM
Real-time communications	• Lowest latency • Permanent bandwidth assign.	• No deterministic networking and no delivery	• Comprehensive traffic management • QoS assign cell.
Accessibility	• Paths defined to support network layer	• IP address assigned to non-IP portals	• Paths defined to support network layer
Security	• Access managed by connections	• Access managed by firewalls	• Access managed by connections
Transparency	• Difficult to change	• Extensive planning for QoS	• Adm. must define two control plane

Conclusions

ATM protocol offers the most efficient multiplexing of all types of traffic. ATM is able to converge legacy data, voice, packet data. ATM has got a capability of QoS. While ATM is an immediate and a possible solution for the SMN, the strong move to an IPv6 core will gain good chance in the near future. Supposing the spreading of high-speed IP routers the QoS issues will become less important.

The final and better choice of future infrastructure of SMN may be a hybrid solution: the optical network based and ATM supported MPLS technologies.

⁵ Gary Buda, Don Choi, Richard F. Graveman: Security Standards for the Global Information Grid, IEEE Communications, p. 617-621., 2001

STRATÉGIES ET TECHNOLOGIES SUR L'INFORMATION

L'attentat du 11 septembre 2001 contre le World Trade Center a confirmé une donnée qui passe maintenant inaperçue tant elle est entrée dans les mœurs: l'instantanéité de l'information. Le premier impact de l'attentat a pu être filmé et diffusé quelques heures plus tard; c'est en direct que des centaines de millions de téléspectateurs ont pu voir le second. Prouesse rendue possible grâce à une révolution technique, le satellite a bousculé non seulement les notions de temps et d'espace, mais aussi les journalistes. Parfois dépassés, ils sont obligés de repenser leur métier fait d'un savant équilibre entre rapidité et recul.

La technologie permet de réaliser une des exigences journalistiques; rendre compte de l'événement au moment où il se déroule sinon le plus rapidement possible. Mais elle en met à mal une autre: rendre compte de l'événement avec suffisamment de distance pour lui apporter une valeur ajoutée qui s'appelle l'information, avec des éléments vérifiés, remis en perspective et expliqués. Entre l'événement et sa diffusion, le journaliste n'est plus seul. Le technicien a pris une place de plus en plus importante, à tel point que la fabrication de l'information est également structurée par la technique. En matière de sécurité intérieure, cela n'est pas sans conséquence.

Tout d'abord, la complexité et l'urgence des événements de sécurité font que toute augmentation de la vitesse de l'information risque de se traduire par une perte de qualité. Ensuite, l'amélioration des techniques a favorisé l'éclosion de nouveaux genres télévisuels dans le traitement de la sécurité.

Les exigences journalistiques: le temps et l'information

Toute la difficulté du métier de journaliste réside dans cette équation: produire un maximum d'information en un minimum de temps. Mais l'information n'est pas une donnée brute qu'il suffirait de collecter pour la diffuser. Il s'agit d'une donnée travaillée. Rendre compte „journalistiquement” du réel nécessite différentes opérations de base. Vérifier l'information pour en attester la véracité, en définir la source pour en connaître l'émetteur, l'expliquer qu'elle ait du sens auprès des lecteurs ou des téléspectateurs, la remettre en perspective pour juger de son importance et enfin la hiérarchiser car toutes les informations ne se valent pas. Toutes ces opérations requièrent du temps pour réaliser cette valeur ajoutée, mais aussi pour prendre du recul sur l'événement afin de le „dominer”. Mais le temps du journaliste est très particulier. Il est caractérisé par la rapidité et l'actualité.

La rapidité se situe dans l'enquête, la réalisation et l'exposition du sujet. Ce qui est déjà contraignant pour le journaliste de presse écrite ou radio devient structurant pour le journaliste TV puisque sa matière première c'est l'image. Il n'est plus seul. Pour réaliser son reportage, il va s'adjoindre des spécialistes tels que le cameraman, le preneur de sons et un monteur. Au temps de l'information s'ajoute donc le temps „technique” nécessaire à la réalisation imagée. Ainsi, un journaliste qui se voit confier un reportage à 8 heures du matin doit impérativement le „boucler” pour le journal de 12 heures. Il a 4 heures pour produire l'information, caler ses interview, tourner le reportage, le monter et le mixer. L'actualité est l'autre composante du temps journalistique. L'événement le plus récent, toute chose égale par ailleurs, chasse l'autre, car le journaliste n'est pas un historien, il travaille sur l'immédiat.

Alors, comment travailler rapidement sur l'actualité tout en gardant le recul nécessaire à la bonne production de l'information? Il s'agit d'une vieille problématique journalistique relancée par la révolution des techniques.

La révolution des techniques

Le premier bouleversement technologique concerne l'avènement du direct en matière d'informations télévisées. Les satellites ont inauguré l'ère de la mondialisation de l'information. Relayés sur le terrain par des petits cars Hautes fréquences (HF), il est possible à un journaliste d'établir un direct depuis n'importe quel lieu en moins d'une heure, ou du monde en 24 heures. Désormais, le direct aura la priorité sur „l'enregistré”.

Cette révolution a même donné lieu à un nouveau genre télévisuel: l'information continue, depuis Cable news network (CNN) jusqu'à La chaîne information (LCI), en attendant d'autres déclinaisons comme l'information continue locale, l'information continue par thèmes, etc.

Mais il n'y a pas que le direct qui a bénéficié du progrès technologique. Les reportages enregistrés aussi. Il y a 25 ans, avant de diffuser des images enregistrées, il fallait développer la bobine, à l'instar d'une pellicule photo. Maintenant, à peine rentré, le journaliste peut diffuser ses images immédiatement. Même les montages, grâce au numérique, sont plus rapides d'au moins 20 à 30 %. Toute la chaîne de production d'information télévisée peut ainsi travailler beaucoup plus rapidement.

Le deuxième bouleversement technologique concerne l'image. Les techniciens ont créé des caméras plus légères et surtout moins chères que le matériel traditionnel. Le résultat peut se constater sur chaque événement car les caméras se multiplient.

A côté de celles des chaînes nationales sont venues s'ajouter celles des agences d'images indépendantes. Ces dernières sont toujours plus nombreuses car le coût du matériel de reportage et de montage n'a cessé de diminuer, tandis qu'en parallèle, la multiplication des chaînes offre des débouchés croissants. Ces agences vendent leurs reportages „clefs en mains” aux diffuseurs. Là encore, une autre exigence journalistique est comblée. En effet, plus il y a de caméras, plus l'événement a de chance d'être filmé, sous des angles variés, par des reporters différents et plus l'information sera couverte en images.

Le premier impact contre le World Trade Center a été filmé par deux journalistes indépendants, avec des petites caméras, pour un reportage sur les pompiers de New York qu'ils comptaient revendre à une grande chaîne. Après la rapidité de diffusion et la multiplication des images, la troisième révolution technique a donné aux journalistes des outils performants pour enquêter plus rapidement.

Les plus anciens se demandent encore comment ils faisaient pour travailler en reportage, sans téléphonie portable. C'était la course aux cabines téléphoniques pour à la fois rester au plus près des dernières informations, et en même temps, vérifier les nouvelles. Le journaliste a aussi décuplé sa capacité d'enquête grâce à Internet où il peut maîtriser lui-même et rapidement toute la partie „documentation” ouverte de son travail.

Enfin ajoutez l'ordinateur personnel compact à ces deux outils et, incontestablement, la technique a apporté un vrai plus dans l'enquête journalistique. La difficulté du métier n'est plus de gagner du temps à tout prix, puisque la technique le permet, mais au contraire d'arriver à en rester le maître pour l'utiliser à bon escient. La véritable question est: que faire du temps gagné? Idem pour les images. La difficulté n'est plus la rareté, mais le trop-plein. La question n'est plus de savoir comment en obtenir mais plutôt quel sens leur donner, déterminer leur provenance et leur véracité. Le temps pour le temps, l'image pour l'image, voilà le danger qui guette le journaliste s'il se laisse dépasser par les nouvelles facilités que lui offre la technique car elles ne sont pas sans influence sur le traitement de l'information. Elles tendent même à la structurer. C'est particulièrement vrai pour la sécurité intérieure.

TELECOMMUNICATIONS SPATIALES MILITAIRES ET INTEROPERABILITE

Dans les années '70 et '80 il y a eu beaucoup de pays qui reconnaissait 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 radio-communication 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. Apte à véhiculer à très longue distance des débits élevés, à l'aide de terminaux 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 auquel les 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 oeuvre 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 Alliés⁶ 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).

⁶ EU (DSCS III) — GB (Skynet 5) — Otan (NATO IV) — France (Syracuse) — Espagne (Hispasat) — Italie (Sicral) — Turquie (Turcsat).

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.

SECURITY AND RELIABILITY OF SENSOR NETWORKS

Roland Gémesi*
gemesi@alpha.tmit.bme.hu

Balázs Ivády*
ivady@alpha.tmit.bme.hu

László Zömbik#
laszlo.zombik@ericsson.com

* Department of Telecommunications and Media Informatics (TMIT), BUTE

TMIT-BUTE; Ericsson Hungary

Abstract

The development of communication technologies and the growing level of integration allow the construction of mobile, autonomous devices that collectively serve a common goal. A self-organised sensor network is an active research area, but their applicability till rises serious questions of security. We analyse several security protocols and also simulate the effects of malicious activity in such a network.

Introduction

The development of compact, low-power wireless communication, sensor and actuators in the technology is giving rise to entirely new kind of embedded systems and a new genre of embedded software. Because of the ongoing miniaturisation, in the near future, advances in processor, memory and radio technology will enable small and cheap nodes capable of wireless communication and significant computation. The addition of sensing capability of such devices will make distributed micro sensing – an activity in which a collection of nodes coordinate to achieve a larger sensing task – became possible.

This new kind of embedded systems is distributed, deployed in environments where they may not be designed and configured for long; the scenario is often very dynamic. The collection of devices can communicate to achieve higher level coordinated behaviour. For example, wireless sensor nodes may be deposited in offices and corridors of buildings, to provide light, temperature and activity measurements. Wireless nodes may be attached to circuits or appliances to sense critical parameters and to actuate in particular situations. Sensor networks can be deployed in inhospitable environments such as remote geographic regions or toxic locations. They will also enable low maintenance sensing in less accessible environments: large industrial plants, aircraft interiors etc. [1]

Sensor network nodes form a self-organising, ad hoc network, where nodes create a multi-hop communication network. There are two common service architectures used in sensor networks. One of them is when nodes only make measurements and send information to a central processing and data storage point, which is often a more powerful entity in the network. In the other case,

such a central processor is not needed; all computation is done with the collaboration of network nodes.

From the security point of view ad hoc sensor networks need more attention. In an inhospitable environment malicious parties may disturb operation. To prevent this, security mechanisms should be used, although the limitations of resources (CPU, battery, etc.) and the absence of a central trusted entity classical security mechanism cannot be used. There are protocols designed for the use in sensor networks, although these have not been examined satisfactorily yet. The limitations of nodes also result in the uncertainty of network components. The overall operation of the system should tolerate such local breakdowns of the networks. The investigation of such mechanisms requires network simulations.

In the following section the threats of mobile ad hoc networks will be presented. After this, we introduce a framework for the analysis of security protocols. In this framework we examine security protocols proposed for sensor networks. In the following section the capabilities of the ns-2 network simulator will be explained that may be used for sensor network simulations. After this, the simulation of malicious parties in sensor networks and an object tracking simulation will be introduced.

Threats in mobile ad hoc networks

Sensor networks formalise a multi-hop network and operate as an ad hoc network. There are many issues with establishing proper security in a self-organising mobile ad hoc environment. The most important threats and bottlenecks will be highlighted in this section.

A mobile ad hoc network contains many resource-constrained devices. Those devices communicate with each other using a shared radio medium that is freely accessible even for malicious parties. Protection for confidentiality of sensitive information need to be realised, although algorithms used in large computer networks are mostly not usable here. The limited resources of nodes (CPU, Battery) do not allow the usage of hard security mechanisms, however information protected with only weak algorithms can be victims of brute force attacks.

A fully self-organised environment makes authentication much more difficult too. In traditional networks authentication algorithms are mostly based on a third trusted party (Certificate Authority). That is not available in ad hoc networks. Even authentication algorithms are usually based on PKI (Public Key Infrastructure) that has high computation demands. Without proper authentication impersonation and man-in-the middle attacks are possible. [2]

Although sensor networks are mostly deployed in untrusted location, sensor networks are usually involve a trusted base station. This base station collects sensor information or logs self-organised actuation. This can be used to run

harder algorithms or to provide authentication as well. In such environments we usually assume, that each node has a previously shared secret with this base station.

With this assumption, the aim of security protocol design is to apply computationally asymmetric mechanisms, where the base could have harder computation or storage tasks, but the sensors should not.

When the process of communication is well secured, a mobile ad hoc node is often threatened by physical attack. The availability of system services can become in danger if a large amount of participating nodes broke down. Small nodes could not afford hard physical protection; a local attacker can destroy any. The jamming of communication channel and the overloading of nodes may also block participants.

A self-organising distributed system works with the collaboration of individual nodes, although system services should be fault tolerant to node breakdown. System services should also remain functional even if attackers who do not collaborate and try to scramble services. The design and evaluation of such a self-organising and also fault-tolerant system is not trivial.

Security protocol analysis

Sensor networks are deeply distributed systems; their components are separated nodes running their own software concurrently. The analysis of distributed systems is much harder, than it was with sequential computers, because each component of the system can be in its individual state. A current state of the machine can be characterised with the states of all components. Such distributed systems can be given and analysed with process algebraic methods.

CSP (Communication Sequential Processes) is a language designed for the description of concurrent systems [3]. The CSP model of the concurrent system is built from processes that can participate named events, so can they get through a next state. There may exist a situation in a state of a process where a choice can be made between events by the process itself or the environment.

Processes can be put parallel, which means, that they can only participate an event together. The effect of parallelism can be imagined as a communication using a shared channel between two processes. It is also possible to isolate two processes by the interleave operator, that means that the two systems cannot take apart in the same events simultaneously.

Hiding is an operator of CSP that can be used to hide the visibility of events or processes. This may help when the modelling of complex systems are done by hiding internal mechanisms. After a set of events are hidden, they cannot be involved in any parallel structures, they cannot communicate outside.

There are more possibilities to give an actual state of the system. The easiest way is the traces model, where states of processes are given with the list of events (called traces) a process took part in. However there also exist failure and divergences models, but for the use of protocol analysis we only need the traces model.

An advantage of CSP is that the FDR (Failures Divergences Refinement) tool can be used to compare two systems. The base of FDR is refinement that is a fundamental engineering principle. We say, that a process B is traces refinement of process A, if each traces of process A are also traces of process B.

These are the main building blocks of CSP that makes possible the modelling of communication protocols. The participants of the protocol can be modelled as processes that communicate each other and get through their next state. Specifications of the protocol have to be formalised also in CSP when after traces refinement can be used.

In the case of security protocol analysis, CSP modelling has much more complex aspects. After modelling the processes of protocol participants, sensitive data terms and deduction systems, the malicious agent is also formalised. The state space of such a protocol may be quite large, and the goal is to check with refinement that for all states are in the secure set of states.

A CSP description of a security protocol is very long and difficult. The Casper compiler gets a simpler security protocol and specification description and creates the CSP model of that. The notation used by Casper and the detailed description of its keywords can be found in the Casper Manual [4].

Security analysis of Security Protocols for Sensor Networks (SPINS)

As we examined the threats of mobile ad hoc networks, we saw that establishing security in a self-organising environment is not trivial. We also mentioned that in ad hoc sensor networks often consists a trusted base station that has a previously shared secret with each node. This base station can make hard security computation, while the other nodes should be spared.

A possible solution for such an asymmetry is SPINS (Security Protocols for Sensor Networks), that consist of two secure building blocks: SNEP (Sensor Network Encryption Protocol) and μ Tesla (the “micro” version of Timed Efficient Streaming Loss-tolerant Authentication Protocol). SNEP provides data confidentiality, two-party data authentication, integrity and freshness, while μ Tesla provides source authentication for data broadcast [5].

SNEP

```
#Free variables
A, B : Agent
da, db : Message
nb : Nonce
f : HashFunction
kenc, kmac : Agent->Key
InverseKeys = (kenc, kenc), (kmac, kmac)

#Processes
SENSOR(A, B, da) knows kenc(A), kmac(A)
BASE(B, nb, db) knows kenc, kmac

#Protocol description
1.  -> B : A
2.  B -> A : nb, db
3.  A -> B : {da}{kenc(A)}, f(kmac(A), nb,
{da}{kenc(A)})

#Specification
Agreement(A, B, [da])
Secret(A, da, [B])
...
#Intruder Information
Intruder = Mallorv
```

Figure 1. SNEP protocol description

Figure 1 shows us the Casper description and the functionality of the two steps SNEP protocol. In the first step the base (B) finds out about the sensor node (A). In the second step the base station sends a request (*na*: nonce and *db*: message) to the sensor node. If the node receives this request, it creates the response. The response consists of two parts. The first part of the response contains an encrypted data: $\{da\}\{kenc(A)\}$, where *da* is the data, and the *kenc(A)* is the encryption key of the sensor. The other part of the response contains a MAC. The MAC is $f(kmac(A), nb, \{da\}\{kenc(A)\})$. If the MAC verifies correctly, node A knows that node B generated the response after it sent the request. The first message can also use plain SNEP if confidentiality and authenticity are needed.

Analysing this protocol we could say that this protocol is faultless. Neither *Agreement* nor *Secret* specification is broken in this setup. However enlarging the initial knowledge of the intruder (*IntruderKnowledge*), one after the other will be violated. For example with learning of key *kenc*, the *da* data can be read, so the *Secret* specification has to be violated. Moreover if by learning

```

#Free variables
A, B : Agent
ts1,ts2 : TimeStamp
na : Nonce
rootkey, tkey : TeslaKey
InverseKeys = (rootkey, rootkey), (tkey, tkey)

#Processes
BASE(B, na, rootkey, tkey)
SENSOR(A, rootkey)

#Protocol description
0.   -> B : A
    [A!=B]
1.   B -> A : {ts1}{rootkey}, {B, A, na}{tkey}%enc
    [ts1==now or ts1+1==now]
2.   B -> A : {tkey, ts2}{rootkey}
    [ts1<ts2 and decryptable(enc, tkey) and
    (nth(decrypt(enc, tkey), 1)==B) and
    (nth(decrypt(enc, tkey), 2)==A) ]

#Specification
Agreement(B,A,[B])
...
#Intruder Information
Intruder = Mallory
IntruderKnowledge = {Alice, Bob, Mallory, Nm}

```

Figure 2. μ Tesla protocol description

both the key *kenc*, and the key *kmac* (e.g. by hardware tampering), the intruder can read the whole communication, and also can modify it. In this case, either the *Agreement* or the *Secret* specification was violated.

μ Tesla

μ Tesla is a simplified version of the Tesla broadcast authentication protocol. Tesla achieves source authentication by the delayed disclosure of keys. The key of the message authentication will be revealed only when the message itself has been arrived to the destination. Only the provider of this key could be the source [6].

Frequent authentication requires a large number of keys, which is realised with a one-way key chain. This chain stands from the multiple application of a one-way hash function on a root key. Unfortunately the large number of those keys (called Tesla keys) requires significant storage capacity. In μ Tesla this storage is provided by the base station, while nodes can use authenticated broadcast with the help of this base.

Figure 2 shows us the Casper description and the functionality of the μ Tesla protocol. Our model do not use a hashed key chain, it uses two independent

keys. In the first step the base B finds out about the sensor node A . It is important, that the Base station and the sensor node may be not the same entity. In the second step the base station sends a time stamp encrypted with the root key to the sensor node $\{ts1\}\{rootkey\}$, and $\{B, A, na\}$ message encrypted with the Tesla key. The second part of the second message is not readable for the sensor, because it does not know the Tesla key, so the node put the message in a queue. In the third step, the node receives the Tesla key with the actual time stamp $\{tkey, ts2\}\{rootkey\}$. So the node can verify the currently of the Tesla key. If the key is correct, the node removes the previous message from the queue. So Tesla authenticates the packet with a Tesla key.

The analysis of this protocol description results that μ Tesla provides the specification and the authentication stands even in the presence of a malicious party.

Network simulator of sensor networks

Although we can analyse specified protocols with Casper and FDR, the operation of ad hoc sensor networks are often threatened by other effects. Sensor nodes are mostly small, battery-powered devices with a very limited life cycle. Moreover radio communication also introduces uncertainty; the system service should tolerate such errors.

The ns-2 simulator

To simulate such events, we use the ns-2 simulator [7]. Ns-2 is a flexible simulation environment widely used in the academic world. Ns-2 is capable of investigating how various protocols perform with different parameters, and also the effects of different topologies.

Ns-2 had already been used for wireless ad hoc network simulations. This occurs that many of the real world protocols are also implemented in ns-2. The simulation environment supports many of the communication paradigms. Many routing protocol implementations and node movements are also supported by the simulator and the investigation of energy constrained environments are also solved. In the following we review the capabilities of ns-2 that may be used for sensor network simulations.

In the physical layer, ns-2 includes radio propagation models with r^{-4} attenuation. Those are the free space, two-ray ground and shadowing models. The first two results a constant propagation distance, while the shadowing model gives a probabilistic channel that is much more realistic.

The radio range can be changed with the parameters of the physical layer. Many of those parameters can be altered, although we use only the transmission power parameter that determines the propagation range.

The ns-2 simulator implements a 1.6Mbps 802.11 MAC layer that is a CSMA based medium access control mechanism. Although there are energy efficiency reasons for selecting a TDMA style MAC for sensor networks, those are not really usable in the ns2 simulator.

In the network layer, ad hoc routing protocols had already been investigated in the simulator, the implementation of DSDV, AODV, DSR and TORA mechanisms are available. Moreover the directed diffusion routing paradigm is also available [8].

On top of the nodes, transport layer agents are placed those select incoming packets and route them to registered applications. A usable UDP and TCP agents are also available.

Finally, applications produce or consume packets, with a given traffic pattern. Available applications are CBR (Constant Bit Rate), PING, FTP, TELNET and others.

Ns-2 gives the possibility of wiring layers together and to schedule different actions. Any models may be changed, source codes are available, so arbitrary modifications can be made.

Phenomenon addition

Sensor networks are mostly used to detect some phenomena (e.g. CO or sound) and process them (e.g. simply report them to base station).

A phenomenon can be modelled as a special kind of network node [9]. This

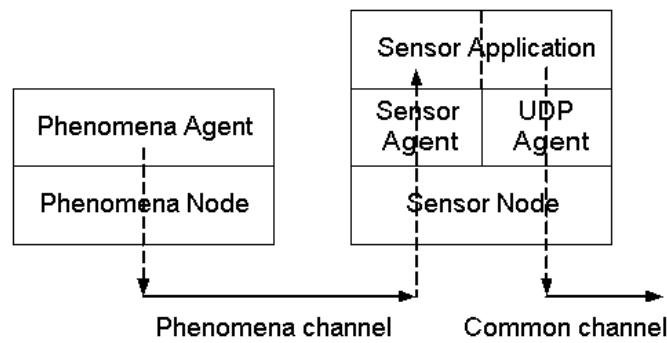


Figure 3. Model of phenomena sensing

node uses a separate communication channel wherein it broadcasts alarm messages. Sensor nodes use a special transport agent, that detects phenomena packages and notify the sensor application. That application then can utilise a

common agent of the node (e.g. UDP), to send packages to a base station (Figure 3).

With this modelling strategy, a phenomena triggered sensor field can be simulated.

Ad hoc On-Demand Distance Vector Routing (AODV)

AODV is a reactive ad hoc routing protocol, which means that it starts discovery of a route only when it is needed [10]. AODV relies on the dynamically established route table entries at intermediate nodes. Endpoints do not know the details of the whole path, and each intermediate node knows also only the direction of forwarding.

When a node starts to communicate, it initiates a Path Discovery process, which is a broadcasted route request message containing the destination's and originator's address. Each node receiving such a request message sets up a reverse route back to the source and rebroadcasts the request. The destination replies to the first incoming request with a route reply message on that way to the originator. This reply message runs back through the set up reverse route and also sets the forward route in the nodes. Each route entries have a specific lifetime, consequently unused reverse route entries will be deleted.

When a link error is detected a route error message is generated with the list of unreachable destinations and sent back to the sources. In AODV it is possible to repair a link locally, which is called local repair. If the local repair process succeeds, the endpoints will not be informed about the action at all.

AODV is a good example of a fully distributed routing mechanism, and it offers relatively low overhead.

Simulation of malicious node

Our goal is to simulate a sensor network and analyse its level of fault tolerance. We concentrate on the effects of node breakdowns to routing protocol. To achieve this, we set up a communication flow and we model a malicious node that denies routing.

We model a 8 x 8 grid of sensors in a 400 x 400m area, where a constant bit rate data flow is used in one direction. We use a two-ray ground propagation model and set the transmission power to result a range of a single hop. A modified 802.11 network interface model was used, because we do not concentrate on multiple access control and collision effects.

The AODV routing protocol was used, since it is included and tested in ns-2. Finally we use an UDP agent and a CBR (Constant Bit Rate) application. We use the packet size of 600 bytes and sending interval of 0.15 seconds. With this rate, the effect of collision due to data traffic is not significant.

To disturb this constant flow, we use a moving Phenomena node that destroys nodes getting near. The closure of phenomena is detected by the sensor agent also present on the nodes, and a modified sensor application removes all the remaining energy of a node. After this, the node will not be able to participate in any communication.

Metrics of service

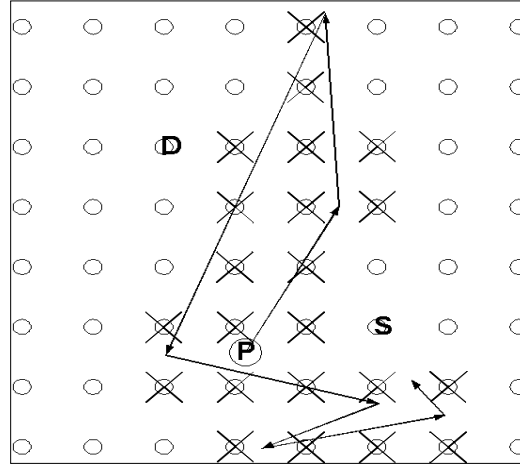


Figure 4. Simulation scenario

To evaluate service, we analyse the disturbed data flow. We can visualise the relocation of traffic flow with the network animator tool (NAM). The most important of our metrics is the delay of sent packets. Expectedly when new routes have to be found, delay may be longer and with node breakdowns, some packets may be lost.

The communication flow has the other important metric of hop count. The more intermediate nodes forward, the more hazardous the traffic is. We also investigate the forwarded number of packets for each node, which shows the load of individual nodes and also their importance in the service. The changes of routes and the variation of parameters may be comprehended with the examination of the distribution of routing messages.

Evaluation

In the base of our analysis a slowly moving attacker disorders the communication flow several times. The sensor nodes can be seen in figure 4, where *S* and *D* are the source and destination nodes and the movement of the attacker (*P*) can also be seen.

The delay of the communication flow can be seen in figure 5.a. One can see the steps where the communication route breaks down and a new one is requested. In those cases the packet currently at the killed node is lost. Although this kind of packet loss affects only a few packets, after the 123rd packet, none of the sent packets arrive. This is because after this point a new route cannot be found, the whole network become segmented.

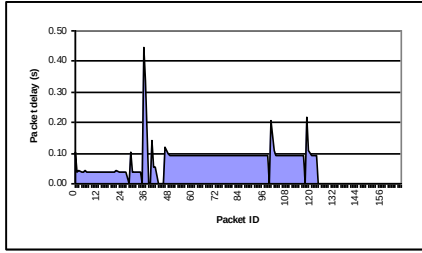


Figure 5.a. Packet delay

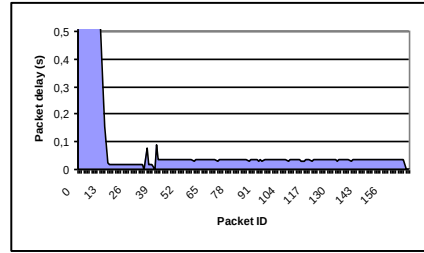


Figure 7.a. Packet delay

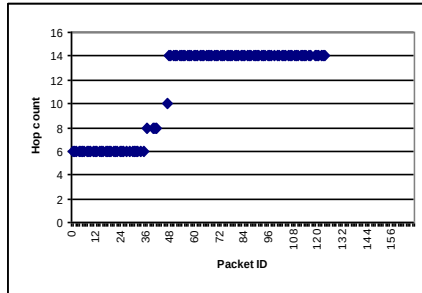


Figure 5.b. Hop count

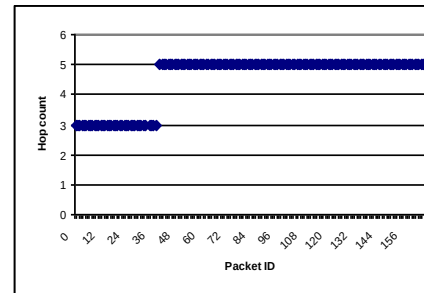


Figure 7.b. Hop count

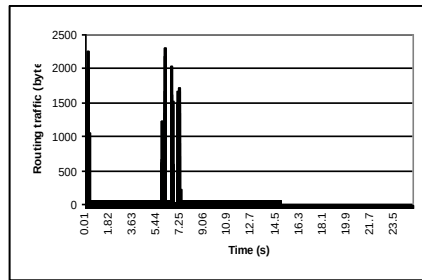


Figure 5.c. Routing traffic

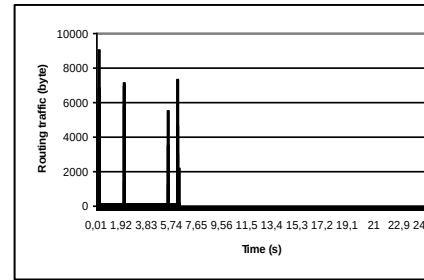


Figure 7.c. Routing traffic

The effects of new routes can also be seen in figure 5.b, which shows how hop counts increment. Although data packets often lost in those transitions, the large number of routing packets can be seen in figure 5.c. This happens, since the AODV protocol starts flooding requests to found the destination again.

In figure 6 we can see the graphical distribution of node usage during the simulation. We can see that some nodes of the networks were not used at all; most packets were found near the endpoints.

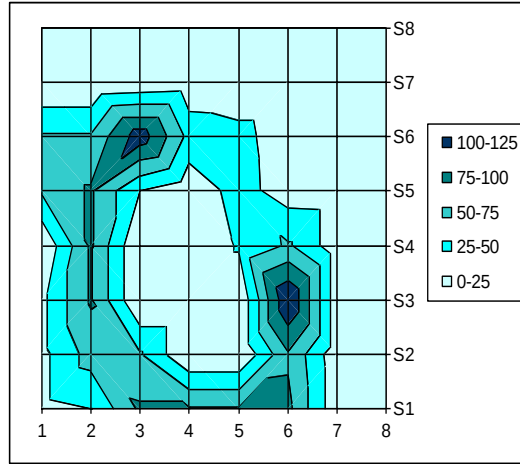


Figure 6. Node usage

In the previous analysis we used the transmission range of a single hop, which meant that each node had four neighbors. The fault tolerance of system availability is related with the redundancy of communication channels, so with the number of accessible neighbors. To achieve this, we modified the previous simulation to use the transmission range of two hops.

In this case, hop counts became significantly lower (figure 7.b). The number of steps occurred by route changes also decreased, the route became more fault tolerant. The peaks in the number of routing messages (figure 7.c) became also smaller. If we examine packet delays in figure 7.a, we can appoint the high starting delay.

The high starting delay is occurred by collision effects. Unfortunately AODV uses flooding for route request, which means that after the second level of broadcast a large number of packets appear in the network simultaneously. This occurs high lost rate of route request packets and makes such transient effects in each flooding. AODV is a general ad hoc routing mechanism and its route request flooding makes it problematic in such a dense topology.

Object tracking simulation

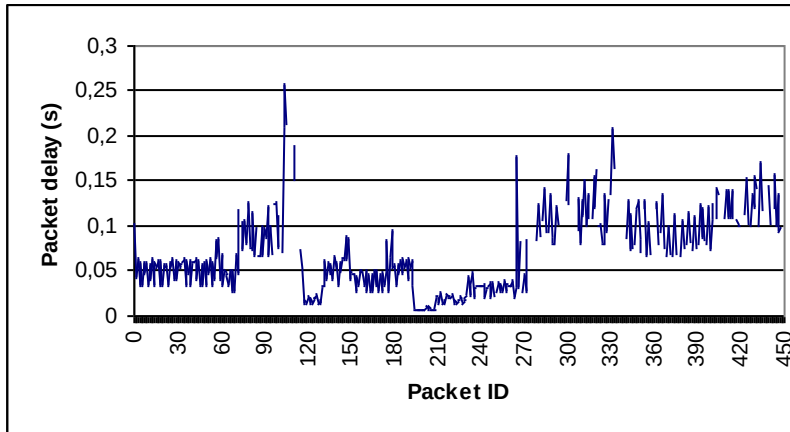


Figure 8. Packet delay

We also made an object tracking simulation, in which sensor nodes detecting the phenomena report it to a base station. We use the same environment, although the permanent sender is eliminated. Nodes near the phenomena send packets to the base station. In this case, routes or nodes do not break down, although with the movement of the phenomena new routes should be found.

We can see the packet delays in figure 8. delay varies a lot; as phenomena moves, new nodes detect it, so new routes have to be found. This generates route requests several times, so transient floods and collisions are present. Fortunately phenomena moves slowly, which results in that a neighbour of new route requesting nodes also has a cache entry.

In the animation of the network traffic, the changes of the traffic flow can be studied. The moving phenomena and also the reporting procedure can be seen when requesting new routes. Broadcast storms can also be examined.

Conclusion

We have presented that mobile ad hoc networks have serious security considerations. However in present day sensor networks with fully self-organised architecture is not used yet. With the help of a trusted base station satisfying security properties can be achieved with proposed security protocols. We have also investigated the simulation possibilities of sensor networks, because the fault tolerance of distributed algorithms has to be evaluated. We have shown that the ns-2 network simulator is capable to handle such networks. Thus simulations will have large importance in the design of self-organising networks.

References

- [1] Berkeley Nest Project - <http://webs.cs.berkeley.edu/nest-index.html>
- [2] Kata Molnár, László Zömbik. Security Issues in Mobile Ad hoc Networks, 2001
- [3] Peter Ryan, Steve Schneider, Michael Goldsmith, Gavin Lowe and Bill Roscoe. Modelling and Analysis of Security Protocols, 2001
- [4] Gavin Lowe, Philippa Broadfoot, Mei Lin Hui. A Compiler for the Analysis of Security Protocols, 2001
- [5] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar. SPINS: Security Protocols for Sensor Networks, 2001
- [6] Adrian Perrig, Ran Canetti, Dawn Song, J.D.Tygar. Efficient and Secure Source Authentication for Multicast, 2001
- [7] The Network Simulator ns-2 - <http://www.isi.edu/nsnam/ns/>
- [8] Chalermek Intanagonwiwat, Ramesh Govindan, Deborah Estrin. Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks, 2000
- [9] NRL's Sensor Network Extension to Ns-2 - <http://nrlsensorsim.pf.itd.nrl.navy.mil/>
- [10] Charles E. Perkins, Elizabeth M. Belding-Royer, Samir R. Das. Ad hoc On-Demand Distance Vector (AODV) Routing, 2002

A VÁROSHARC KOMMUNIKÁCIÓS JELLEMZŐI A 21. SZÁZADBAN

A beépített területek, a városok birtoklásáért folytatott katonai műveletek a hadviselés történetében mindig is központi szerepet játszottak. Az írott történelemben a legősibb városok, Úr, Uruk, Kis, Ninive, stb. a korabeli központi hatalmat hívatottak megvédelmezni, fallal körülvett központot biztosítva a vallási, gazdasági erő kiterjesztésének a környező, uralható területekre. A Homérosz által lejegyzett trójai háborútól kezdve napjaink városi hadviseléséig a cél a frekvenciált közlekedési csomópontokban fekvő városok megtartása vagy megszerzése, a város teljes körű irányítása. A városokban található a politikai, ipari, kulturális központok legtöbbször, itt összpontosulnak a kereskedelmi, szállítási ki- és berakodóhelyek, a légi, vízi és szárazföldi személyi közlekedés végállomásai. A lakosság egy jelentős része szintén ide tömörül, - a munkavállalás, a tanulás, az egyéni boldogulás vagy éppen a bűnözés lehetősége miatt -, így a felettük való „uralom”, irányítás is fontos stratégiai cél lehet.

A lakott települések méretüket tekintve a kb. 3000 vagy még kevesebb főt számláló falvaktól, kisvárosoktól a több százézes lélekszámú nagyvárosokig terjednek, de a különböző kutatások a 21. században már a *megapoliszok* kategóriáját is kénytelenek számbavenni. A világ lakosságának növekedése, az urbanizáció, vagyis a városiasodás trendje, új kihívások elé állítja a politikusokat, tudósokat, de ezzel együtt a katonákat is.

Az urbanizációs előrejelzések szerint, a világ számos régiójában 10 milliósnál nagyobb lélekszámú megapoliszok fejlődnek ki egy-két évtizeden belül. A 2000-es évben prognosztizált 6,1 milliárd földlakó száma 2015-re 7,2 milliárdra nő, és ezen belül is a népesség hat százaléka megapoliszokban fog lakni. Az ENSZ Népességi Hivatala (UN Population Division) adatai szerint a világ lakossága 2030-ra eléri a 8,27 milliárd főt és ebből 4,98 milliárd városlakó lesz [1]. Ez utóbbi előrejelzés 21, tízmilliósnál népesebb megapolisszal számol, már 2015-re⁷. Az európai kontinensen nem várható ilyen arányú fejlődés, de ha csak a mai London vagy Párizs lakosságát nézzük, az elővárosokkal együtt már közelíti a bűvös tízmilliós lélekszámot. Ugyancsak Európára jellemző leginkább, hogy a nagyvárosokban dolgozók előszeretettel költöznek a környező kisebb településekre, és ezzel nemcsak a nagyváros kiterjedését növelik,

⁷ A lélekszám millió főben: Tokyo – 27,2; Dhaka – 22,8; Bombay – 22,6; Sao Paulo – 21,2; Delhi – 20,9; Mexico City – 20,4; New York – 17,9; Jakarta – 17,3; Calcutta – 16,7; Karachi – 16,2; Lagos – 16,0; Los Angeles – 14,5; Shanghai – 13,6; Buenos Aires – 13,2; Metro Manila – 12,6; Peking – 11,7; Rio de Janeiro – 11,5; Kairo – 11,5; Istambul – 11,4; Osaka – 11,0; Tianjin – 10,3; [1]

hanem sokszor végeláthatatlan forgalmi dugókat is okoznak, különösen munkába menet. A lassan káoszba forduló urbanizációs trend a világon mindenhol egyre erőteljesebb problémákat vet fel már békeidőben is, de fennáll a lehetősége a totális káosz kialakulásának egy válsághelyzet megjelenésével, míg egy megapoliszban kialakuló háborús helyzetre jószerével forgatókönyvek sincsenek.

Katonai műveletek beépített területeken

Az i.e. 500 körül keletkezett Szun-Ce - A Hadviselés Törvényei című műben a következőt olvashatjuk: „Városfalak ostromlásának törvénye, hogy ilyesmit csak akkor csináljunk, ha más lehetőség nincsen”[2]. Már ekkor felismerték, hogy a „fallal körülvett városokat ostromolva erőnk megtörik”, és ez tükröződik napjaink legtöbb katonai doktrínájában és a legtöbb katonai szakíró munkájában.

Az emberiség írott történelmét vizsgálva ennek ellenére számos várostromról, ha úgy tetszik városharcról olvashatunk. A középkor igencsak bővelkedik a példákban: biztosnak tűnő védelmet jószerével csak a fallal körülvett települések, várak jelentettek, ahová a környező lakosság behúzódott a közeledő veszedelem elől. A falak szerepe a városok körül azonban napjainkra jószerével megszűnt, teret adva a közlekedés és a kereskedelem szabad áramlásának. A falak eltűnése viszont nem jelenti azt, hogy egy beépített területen könnyebben oldhatók meg a katonai műveletek, a hadviselés fejlődésére a városfalak megszüntetése csekély hatással volt.

A II. világháború kezdete óta a városharcok igen változatos formáit jegyezték le a történészek: gondoljunk csak a Sztálingrádi, Manilai, vagy Szöuli városharcokra, a Drezdai és Tokiói szőnyegbombázásokra, a Bejrúti polgárháborúra, a Managua-i és Budapesti forradalomra, a Belfastban folyó terroristaellenes harcra, a Bagdadi és Belgrádi precíziós bombázásokra vagy a Szarajevói békefenntartásra, a Groznij-i csatározásokra.

Csujkov tábornok jelentette ki a Sztálingrádi csata idején: „A városharc sokkal bonyolultabb, mint nyílt terepen harcolni. Városharcban a magas szintű vezetés kevésbé érvényesül, a legnagyobb feladat a szakaszparancsnokoké, a szétszabdalt alegységek vezetésében.” [3]

Nemcsak a csapatok közvetlen vezetésében való változtatásokkal kell számolni a beépített, városi és más területeken folytatott műveletekben, hanem számos, a korábbi hadviselési módoktól eltérő harcászati, és ezzel együtt híradási elv is felülvizsgálatra szorul. A harcoló felek változatos terepformák, különböző környezeti hatások között vívhatják meg harcukat, ennek néhány jellemzőjét tartalmazza a következő táblázat.

⁸ 1942. augusztus – 1943. február

Jellemzők	Város	Sivatag	Dzsungel	Hegyvidék
Civilek száma	Magas	Alacsony	Alacsony	Alacsony
Értékes infrastruktúra száma	Magas	Alacsony	Alacsony	Alacsony
Többdimenziós harc tér	Igen	Nem	Néha	Nem
Észlelés, megfigyelés hatótávolsága	Rövid	Nagy	Rövid	Közepes
Megközelítési útvonal	Számos	Számos	Kevés	Kevés
Járművek manőverező képessége	Alacsony	Magas	Alacsony	Közepes
Logisztikai szükséglet	Magas	Magas	Magas	Közepes
Híradás működése	Korlátozott	Akadálytalan	Korlátozott	Korlátozott

1. táblázat: A katonai műveletek jellemzőinek összehasonlítása különböző környezetben [3]

A város harc során általában a következő befolyásoló tényezőkkel kell számolni:

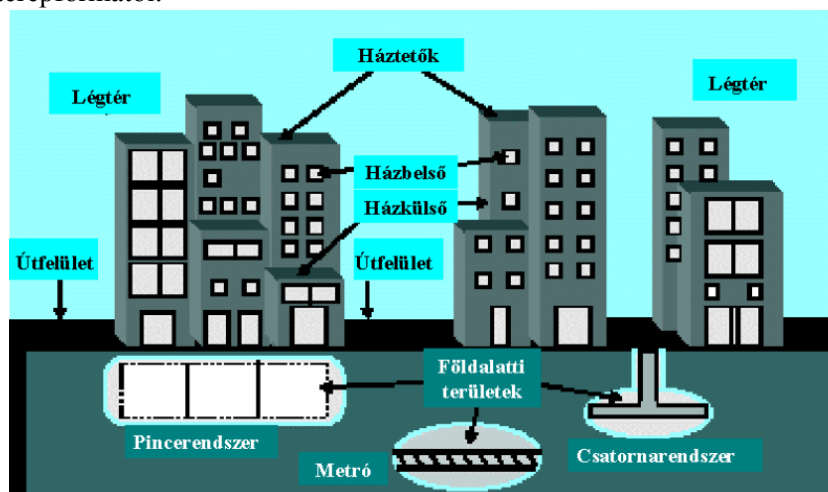
Terep, híradás, civil lakosság, tüzerő összpontosítás lehetősége, manőverezési és mobilitási lehetőségek, logisztikai támogatás, egészségügyi támogatás, emberi tényezők, kiképzettség. Alapvetően a terep jellege határozza meg a műveleti lehetőségeket: figyelembe kell venni, hogy egy kevésbé modellezhető, esetlegesen rombolt környezetben kell végrehajtani a feladatot, amely nehezen járható, a harc járművek mobilitási, manőverezési képessége kicsi és még ez is csökkenhet a hirtelen kialakított úttorlaszok, barikádok miatt. Beépített területen a technológiai fölény sem érvényesül kellő mértékben, a katonák arra kényszerülnek, hogy kis távolságon belüli tűzharcokban, kis csoportokban harcoljanak egy multidimenzionális környezetben rejtőzködő ellenséggel.[4]

Típus	Célok	Stratégiai fontosság	Katonai kockázat	Változatok	Valós példák a közelmúltból
1. Rendfenntartó műveletek	Elrettentés az erőszaktól	Alacsony	Alacsony	Nem katonai, humanitárius segítségnyújtás	Haiti, Bosznia, Szomália (korai)
2. Rajtaütés					
• Nagykövetségek kimenekítése	Behatolás, végrehajtás, kivonulás (vagy megtartás)	Közepes	Közepesen alacsonyabb	Nincs, minden helyzet egyedi, a célorientáltság a döntő	Libéria, Albánia, Sierra Leone
• Kulcsponctok és reptér elfoglalása		Közepesen nagyobb	Közepes	Más lehetőségek keresése	Panama
• Tömegpusztító fegyverek tárolóhelyei elleni		Közepesen nagyobb	Magas	A technológia, szállítás pusztítása; elrettentés	?
• Ellenséges vezetők elfogása		?	Alacsonytól magasig	Nincs, minden helyzet egyedi, a célorientáltság a döntő	Panama, Bosznia, Szomália (késői)
3. Hosszan tartó város harc	Az ellenség erőinek legyőzése	?	Nagyon magas	Más lehetőségek keresése	Grozni

2. táblázat: A beépített területeken folyó katonai műveletek kategóriáinak jellemzői [5]

Amerikai katonai elemzők, az érvényes doktrínákra támaszkodva megalkották a városi műveletek kategóriáit, amelyek jellemzőit a 2. táblázat foglalja össze.

Ahhoz hogy megértsük a beépített területek fizikai sajátosságait, célszerű azt modellezni, meghatározni, hogy miben tér el a többi, hadviselésben használt terepformától.



1. ábra. A városharc során multidimenzionális térrel kell számolni

Forrás: JP 3-06 Doctrine for joint urban operations I-5

Az ábra alapján jól látható, hogy az emeletes házak külső építményei, kiugró teraszok, erkélyek alkalmasak az orvlövészek, vagy mesterlövészek elhelyezésére, ugyanakkor a földalatti területek, csatorna és pincerendszerek egyrészt szintén megnehezítik az ellenség felderítését és leküzdését, a híradásról nem is beszélve, másrészt könnyen elhelyezhető és nehezen felderíthető robbanóanyag elhelyezési területtel szolgálnak. A magas házak közötti manőverezést nehezíti az úthálózat szélessége, így a nehézkes mozgású, alacsony manőverezési képességű harcjárműveknek csak a páncélvédőképessége hasznos, de számolni kell a háztetőkről történő sebezhetőséggel (pl. „Molotov koktélok”, stb.). A házak belsejében való célfelderítés megnehezül, és nagy az esély a szobáról-szobára történő harctevékenység kialakulására.

Ugyanakkor a korunkban egyre erőteljesebben jelentkező információs fölényre törekvés, az információk gyűjtése és elosztása, a kommunikációs technológiák alkalmazásának sajátosságai sem hagyhatók figyelmen kívül, ha sikert akarunk elérni egy ilyen típusú katonai műveletben.

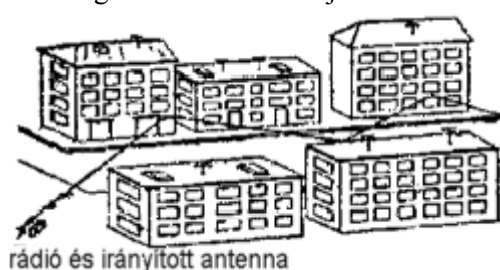
A városharc katonai híradásának problémái és lehetőségei

Az 1. táblázatban szereplő városharc híradásának értékelésekor a „korlátozott” jelzőt olvashatjuk. A leküzdendő problémák már a város ismereténél

kezdődnek, hiszen „a város birtoklásáért folyó küzdelemben jelentős előnyhöz jut az a fél, amelyik jobban ismeri a város területét, úthálózatát, közműveit és lakosságát, amely ismeretet a harc sikere érdekében tud felhasználni. A nagyváros lakosságának magatartása jelentősen befolyásolhatja a harcoló erők tevékenységét és annak sikerét. Jelentős problémát okozhat a harcoló alegységek tájékozódásában az, ha csak elavult térképek vagy vázlatok állnak a rendelkezésükre.”[6]

Ennek kiküszöbölésére alkalmazhatók a különböző pilótanélküli repülőgépekkel készített pillanatképek vagy videofelvételek készítése, illetve a katonai műholdak nagyfelbontású fényképei.

A magas építmények árnyékoló hatása miatt „a harcoló erők vezetése és híradása megnehezül, mivel a rádió- és rádiórelé-összeköttetések, különösen az URH-tartományban, gyakran használhatatlanná válnak.” [6] Némely esetben számolni lehet a városi környezet civil infrastruktúrájának, mobil vagy vezetékes telefonhálózatának használatával, ekkor azonban erős fenntartásokkal kell kezelni a kapcsolatok információvédelmét. A művelet jellegétől függően kiépülhet a vezetékes katonai híradás is, ez azonban sebezhetősége miatt csak kiegészítő alternatívaként jöhet számításba.



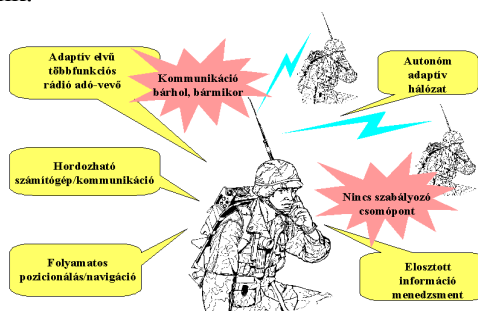
2. ábra. Többszörös átjátszás kialakítása épületek között.

A harcászati helyzetismeret kialakítására megalkotott új technológiájú híradóeszközök működését is behatárolják a fizika törvényszerűségei, így a gyakran vasbeton szerkezetű épületek a rádiófrekvenciás jelek szabad áramlását jelentősen gátolhatják. A terület ismeretében viszont lehetőség nyílik az épületekben elhelyezett többszörös átjátszóállomások elhelyezésére, egyfajta „elektronikus hírlánc” kialakítására, ahogy történt ez például Groznijban, az orosz csapatoknál.

Napjainkban a harcászati rádióhíradás alapvetően a 30-88 MHz-es frekvenciasávra korlátozódik, ahol az antennák egymásra való ráláthatósága az összeköttetés feltétele. A beépített területen történő műveletekben olyan irányított antennákkal célszerű megvalósítani a koncentrált jelkiszugárzást, amivel csökkenthető az épületek általi jelelnyelés, ugyanakkor besugározza a saját erők területeit. Az egymásnak ellentmondó elvárás megvalósítására új antenna típusok kikísérletezése szükséges, számításba vehető a fraktál-antennákkal történő kísérletek eredményei. A teljes frekvenciasávban fontos az antenna minél pontosabb illesztése a ki és bemeneti egységekhez, ezáltal csökken a káros álló-

hullám-reflexiók kialakulása, nő a hasznos jelkiszugárzás, akár fix, akár frekvenciaugratásos üzemmódban dolgozunk.

Városharcban elsősorban rádió-irányokkal kell számolnunk, de a támogató helikoptereken, földközeli pályájú műholdakon elhelyezett ájtátszóállomások segíthetik a rádióhálóközemetelését. Ezek hiányában törekedni kell az antennák ráláthatóságának biztosítására, például az épületek tetején történő elhelyezésről, a kiemelkedő épületek csúcsain (víztorony, templomtorony, stb.). Ugyancsak nem hagyható figyelmen kívül az antennák könnyű súlya, kis mérete sem, hiszen a gyalogosan mozgó harcosoknak a felszerelésen kívül ezt is hordozniuk kell.



3.ábra. Egy célszerű kommunikációs hálózat jellemzői a városharcra (Forrás: DARPA)[7]

A városharc végrehajtására a gyakorlatban komplex, integrált túlélőképeséget biztosító felszerelésekkel kell számolni. Tekintsük át ezek főbb jellemzőit az amerikai Land Warrior rendszer példáján, amely egyben a technológiai fejlesztés irányvonalának a bemutatása is.

Az amerikai Land Warrior rendszer

A 90-es években kezdték el fejleszteni a Földi Harcost (Land Warrior) [8], egy első generációs, moduláris felépítésű, integrált harcászati rendszert, amely biztosítja a katona számára a harcászati helyzetismeret kialakítását, a túlélőképeséget és a harci hatékonyságot. A rendszer öt alrendszert foglal magában: a fegyverzeti alrendszert, a sisak alrendszert, a komputer/rádió alrendszert, egy szoftver alrendszert, valamint a védőruházat és az egyéni felszerelés alrendszerét. Mindegyik alrendszer csatlakozik a digitális harcmező rendszeréhez, a sisakba épített kijelzőn megjelenik a terület digitális térképe, üzenetküldési és tűztámogatási funkciók könnyítik meg a kommunikációt. Videó és hőkép kamera csatlakozik a könnyített személyi lőfegyverhez, helyzetjelző és azonosító elektronikák segítenek a navigálásban, illetve segítenek felismerni a saját és az ellenséges erőket.

A tervek szerint kétfajta Land Warrior rendszerrel számolnak: az egyes harcos és a parancsnoki rendszerrel. A parancsnoki rendszer nagyobb kommunikációs lehetőségekkel rendelkezik: SINCGARS kompatibilis rádió, billentyűzet és komplex kijelző is megtalálható benne. Az egyes harcos rendszer üzemeltetése újratölthető akkumulátorokkal tervezett, de ahol nem oldható meg a harcjárműben vagy a városi környezetben az utántöltés, ott egyszer használatos, eldobható szárazelemekkel számolnak. A rádióhíradás megvalósí-

tását újfejlesztésű, kishatótávú szakaszrádiókkal tervezik, amelyek képesek az integrált hang és adatátvitelre, míg a parancsnoki rádiók hatótávolsága megnövelt, a kis egységek parancsnokaitól az előjáró század vagy magasabb szintű vezetőig terjedhet az információadáshoz. Mivel az egész rendszer moduláris felépítésű, a két alapváltozat tetszőlegesen variálható a feladat függvényében.



4.ábra. Land Warrior a 21. században

A fegyverzeti alrendszer az M-16/M-4 egyéni lőfegyverre épül, magában foglal elektronikai/optikai komponenseket, mint a videokamera, vagy a lézertáv mérő és a digitális tájoló, biztosítva a széles időjárási körülmények közötti vagy az éjszakai harcot.

Az integrált sisakra épített alrendszer egyrészt védelmet nyújt a repeszek ellen, másrészt a beépített számítógép és szenzor kijelző interfészt ad egyéb alrendszerekhez és a digitális harcmezőhöz. A kijelzőn az információk széles skálája jeleníthető meg: a számítógép-generálta grafikus adat, digitális térkép, felderítési információ, csapatelhelyezkedés, a fegyverre szerelt hőkamera vagy a videokamera képe.

A védőruha és egyéni felszerelés alrendszer a legmodernebb fejlesztésű, autóversenyeken használt védőöltözéken alapul, hátoldalán keretrendszerűen beépített vezetékek a számítógép/rádió csatlakozásokhoz. A ruházatba hatásnövelő védőbetéteket helyezve védőmellényként is funkcionálhat.

A számítógép/rádió alrendszer elemei egyszerűen felcsatlakozhatnak a védőruha keretrendszerére. A számítógép processzora fuzionál a rádiókkal és egy GPS lokátorral. Az alrendszer bankkártya méretű panelekből épül fel, de még annál is vékonyabb. Az egyéni rádió mobiltelefon méretű, míg a parancsnoki változat nagyobb, de teljesen kompatibilis a harcászati rádiókkal (SINCGARS). A hátra szerelt keretrendszer alsóbb régióiban kapott helyet a számítógép és a GPS rendszermodul. A menüvezérelt kijelző a katona által vezérelhető, a speciális kialakítású virtuális kesztyű ujjába épített érzékelőknek köszönhetően. Néhány funkció a tűzváltókar mellett került kialakításra, a célzási pontosság érdekében. A ruházat keretrendszerébe építik a GPS és a rádióantennákat, így nem zavarja a katonákat mozgás közben. Lényeges elvá-

rás, hogy a fejlett kommunikációs eszközök integrálásával megnőjön a katona túlélőképessége, valós idejű információk megjelenítésével, és a szakasztársakkal való folyamatos kapcsolattartással számolhasson. A kommunikációs alrendszer a nyitott felépítésnek (open system) köszönhetően mind hardveresen, mind szoftveresen egyszerűen továbbfejleszthető.

A Land Warrior szoftver alrendszere biztosítja a katonának, hogy egyfajta harctéri csomópontként funkcionáljon a rendszere. Szoftveres úton biztosított a kijelző vezérlése, a moduláris elemek feladat-orientált összekapcsolása és az egész rendszer áramellátása. Harcászati és feladat-specifikus támogató modulok, digitális térképrészletek, kimerevített videó állókép lehetősége is az alrendszer részét képezik, ugyanakkor teljes mértékű interoperabilitást biztosít más harctéri digitális rendszerekkel, a digitális harcmezővel.

A teljességhez tartozik, hogy a bár a rendszer tesztelése ütemterv szerint halad, a komplett, integrált funkciókkal bíró egybefüggő harcászati formátum azonban még várat magára. Részmegoldásként más modern technológiák felhasználása azonban napjaink szükséglete: így született meg az Összhaderőnemi Integrált Digitális Híradórendszer (JEDI), amely például a napjainkban is folyó afganisztáni harcokban jelentős szerepet játszik az összhaderőnemi egységek kommunikációjában. Ebben személyi zsebszámítógépek (PDA) biztosítják az összeköttetési kívánalmakat, - integrált GPS és kézirádió funkciókkal bővítve -, megteremtve a harcászati helyzetismeret kialakításának lehetőségét.



5. ábra. Harcászati PDA

A következő táblázatban összefoglaltam a jövő hadviselésére, kiemelten a városharcra kifejlesztett, illetve fejlesztés alatt lévő katonai személyi rendszereket, amelyek néhány éven belül rendszeresítve lesznek a fejlett haderőkben.

Rendszernév	Vezetés és irányítás	Kommunikációs rendszer	Fegyverzeti és szenzor rendszer	Navigáció	Egyéb
Nagy Britannia Future Integrated Soldier (FIST)[9]	Parancsnoki alrendszer (BOWMAN rendszer)	Hang és adat-kommunikáció (BOWMAN rendszer digitális rádiói)	Fegyver, lőszer és tűzszabályozó rendszer; Fegyverre szerelt felderítési és célmegjelölő funkciók (pl.: hőkép és szenzor)	GPS	Hordozható tápegységek, akkutöltő, stb. Fejlett védelmi képességű ruházat

			távírányítás)		
Francia-ország Fantassin à Équipements et Liaisons Intégrés (FELIN)[10]	IFF ⁹ rendszer	Megfigyelés és híradás; a személyi kom- munikáció csatlakozik a megfigyelési és IFF rendszerhez	Fegyverre szerelt pontlézeres célazono- sítás és éjjellátó készülék	GPS	Fejlett, könnyí- tett sisak és testfelület védő ruházat; hor- dozható támo- gató rendszerek (eü.csomag, stb)
Német- ország Infanterist der Zukunft (Idz) [11]	Harcászati helyzetismeret; IFF rendszer	Szakaszrádiók vizuális és akusztikai kiegészítéssel	Lézeres célmegjelö- lés; távolságmérő; digitális iránytű	GPS	Fejlett, NBC ellen védő ruházat és csökkentett felszerelés
Hollandia Kato- nai Modernizációs Program [12]	Integrált navigációs és érzékelő funkciókkal ellátott sisak	Felelősségi körzeten belüli híradás	Sisakra épített kijel- ző; többfunkciós éjjellátó; integrált személyi fegyver	A C3 rend- szerbe integrált navigá- ciós rendsze- rek	Integrált hatá- soknak ellenál- ló ruházat
Spanyol- ország Combatiente Futuro [13]	Vezetési irányítási eljárások	Felelősségi körzeten belüli híradás	Integrált fegyverzeti és szenzor rendszer; éjjellátó szemüveg	Navigá- ciós eljárás- sok	NBC véde- lemmel bíró felszerelés
Svédország Markus [14]	Vezetési irányítási eljárások	Kis hatótávú szakasz, vagy kézirádiók	Fegyverre szerelt IR, HDTV és videó kamera; integrált fegyverzeti és szen- zor rendszer; célzás- javító és lézer elleni védőszemüveg	GPS és elektro- nikus iránytű	Szél, víz, hideg és hőálló ruházat; bakte- riológiai és kémiai hadvise- lés elleni védelem

4. táblázat. Fejlesztés alatt lévő katonai személyi rendszerek

A városarc egyéb technológiai

A személyi integrált felszerelések mellett a túlélőképesség fokozására további lehetőségek nyílnak a robottechnológia fejlesztésével. A pilótánélküli mikro repülőgépek mellett megjelennek a városi robotok, amelyek lépcsőjáró-képességükkel, kiváló infra-, hő-, és videókép továbbítással növelhetik a speciális erők képességeit. 2025-re ezek a lehetőségek fogják meghatározni a jövő városarcát. [15]

⁹ IFF = Identification Friend or Foe – Idegen – barát felismerő, azonosító rendszer

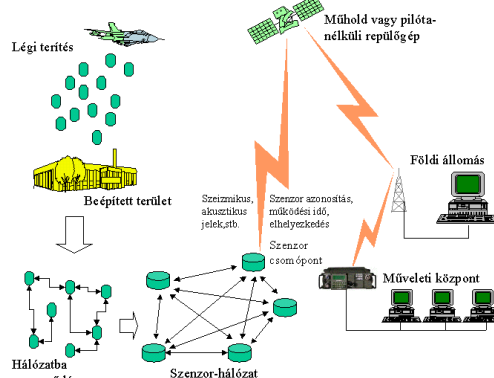


6.ábra. Pilótánélküli repülőgépek, harci robotok alkalmazása fogja jellemezni a jövő városharcát

Forrás: Future Combat System, Industry symposium, 2002.április 4, (USA)

A szenzorok alkalmazása a városharcban is kiemelt jelentőséggel bírhat a jövőben. Napjainkban is számtalan alkalmazási példa bizonyítja a különböző speciális érzékelők létjogosultságát, kezdve a környezet figyeléstől (szeizmikus, akusztikai zajok, infra-, hőkamera, stb.), a felderítésen keresztül, az atom, vegyi és biológiai fegyverek érzékelésére alkalmas típusokig.

Beépített területeken, a vizuális felderítés nehézségeit jelentősen kiegyenlítheti egy szenzorhálózat alkalmazása, amely például repülőről leszárt, intelligens, önállóan hálózatba szerveződni képes elemekből épülhet fel. Maguk a szenzorelemek fejlett jelfeldolgozási (DSP10), jeltevábbítási és helyzetmeghatározó (GPS) funkciókkal rendelkeznek, és valós idejű információkat, adatokat képesek közvetíteni meghatározott helyre.



7.ábra. Szenzorrendszer alkalmazása beépített területen Forrás: ARGUS11 Industry brief. 2000.március 14. (USA)

A műveleti sebesség biztosításához új, speciális képességű járművek tervezése ugyancsak a napjainkban folyó kutatás-fejlesztés része. A városharc kato-

¹⁰ Digital Signal Processing, digitális jelfeldolgozás

¹¹ Advanced Remote Ground Unattended Sensor, Fejlett Távvezérelt, Földfelszíni, Felügyelet nélküli Érzékelő

nájának a többdimenziós környezetben kell nagy mobilitási képességekkel rendelkezni, adott esetben 3-4 emeletes házak tetején hajt végre nagy távolságú ugrásokat a háztetőkön, így számításba veszik kisméretű személyi repülő szerkezetek megalkotását is. Ez csak könnyített felszereléssel lehetséges, viszont a logisztikai szállítás, utánpótlás biztosítása elengedhetetlen, hiszen a következő percekben merőben más körülmények között vívhatja harcát a katona. A városi járőrözési feladatok ugyancsak új vetületet kapnak, háttérbe szorul a járművek páncélvédettsége a manőverezés javára.



8. ábra. Speciális szállítójárművek jelennek meg a városharcban



9. ábra. Brit tengerészgyalogos járőr a dél-iraki Umm Qsar-ban (2003. március)

Összességében megállapíthatjuk, hogy a jövőben, a beépített területeken folytatott katonai műveleteket kis csoportokban végrehajtott feladatsorozatokként kell megtervezni és végrehajtani, amelyekhez a kommunikációs technikák közül ugyancsak a kis csoportok vezetékek nélküli híradását kell hozzárendelni. Az egyéni kommunikációs felszerelések fizikailag integráltak lesznek, az egyes funkciókat valós idejű megjelenítésre képes kijelzők biztosítják a katona számára, miközben saját túlélőképességét különböző védelmi felszerelések együttese növeli. Messzemenően számolhatunk a robot és szenzor technológia fejlesztési eredményeivel, jelentősen növelve a katona túlélőképességét. A jövő hadviselésének információcsere jellegében a bárhol, bármikor elv dominál, vagyis mindenfajta terepszakaszon, időjárás, napszak, évszak és egyéb körülményektől függetlenül biztosított az integrált harcászati kép kialakításának lehetősége.

A harcászati műveletek hatékonyabbá válása nemcsak a precíziós fegyverrendszerek fejlesztésének és alkalmazásának hatása nyomán lesz érzékelhető, ide tartozik olyan új műveleti elgondolások kialakítása is, mint a Hálózat Központú Hadviselés (Network Centric Warfare, NCW). A hálózatos képességekkel bíró katona, a maga fejlett kommunikációs képességeivel a jelenleg rendelkezésre álló legmodernebb, vezetékek nélküli hálózatok jellemzőit messzemenően kihasználó formában fog megjelenni a harctéren és a városharcban. Annak ellenére, hogy „napjainkban nem létezik olyan átfogó vezetékek nélküli kommunikációs technológia, mely egyidejűleg képes lenne kielégíteni a nagy

távolságú közvetlen összeköttetés, a nagysebességű adatátvitel, a multimédiás QoS-támogatás mellett, a kis méret és hordozhatóság igényeit”[16], úgy vélem a feltételek már adottak a kutatás-fejlesztés irányában. Bár egyes katonai szerzők megkérdőjelezzik a technológia alkalmazásának fontosságát¹², véleményem szerint az integrált technikai rendszer alkalmazása nélküli kiképzés meg sem közelíti a valóságos szituációt. Hazánkban sem ismeretlen az integrált technológiák használatára történő törekvés ezen a területen¹³. A kérdés, hogy a Magyar Honvédség dinamikus (és gyakori) átalakításában van-e létjogosultsága a jövő hadviselésére való felkészülésnek technikai vonatkozásban is.

Felhasznált irodalom:

- [1]. Future World population growth to be concentrated in urban areas of World <http://www.un.org/esa/population/publications/wup2001/WUP2001-pressrelease.pdf>.
- [2]. Szun-ce, a hadviselés törvényei; Balassi kiadó, 1998, 25.oldal, ISBN 963 506 194 3
- [3]. JP 3-06. Doctrine for Joint Urban Operations, 2002
- [4]. Porkoláb Imre: Műveletek végrehajtása beépített területeken, Kard és toll, válogatás a hadtudomány doktoranduszainak tanulmányaiból, 2002/2, 72-80.oldal, ISBN 963 7037 52 7
- [5] Urban Warfare conference, Hanscom Air Force Base Officer's Club, Bedford, Massachusetts, May 20, 1998
- [6]. Kőszegvári Tibor: Katonai műveletek a nagyvárosokban és a megapoliszokban, Hadtudomány 2001/3
- [7] DARPA Honlap – Small Unit Operations: Situational Awareness System; <http://www.darpa.mil/ato/programs.htm>
- [8] U.S. Army Soldier and Biological Chemical Command (SBCCOM), <http://www.natick.army.mil/soldier/WSIT/>
- [9] U.K. Ministry of Defence, <http://www.mod.uk/dpa/projects/fist.htm>,
- [10] Commandement de la Doctrine et de l'Enseignement Militaire Supérieure <http://www.cdes.terre.defense.gouv.fr/sitefr/materiels/CC/felin.htm>
- [11] Bundeswehr, http://www.bundeswehr.de/inhalt/06_02/artikel_1.html
- [12] Netherlands Institute of Applied Scientific Research, TNO, http://www.tno.nl/cases/defensie/soldier_modernization.html
- [13] Il Ministerio de Defensa, *Plan Nacional 2000-2003 Volumen II*.
- [14] Swedish Armed Forces homepage, MSS, <http://www.mss.mil.se/utbildning/article.php?id=3125>
- [15] Robert F.Hahn II-Bonnie Jezior: Urban Warfare and the Urban Warfighter of 2025, Parameters, 1999 summer, pp.74-86
- [16] Fekete Károly: A hálózatos harcos katona újszerű kommunikációs rendszere, Új Honvédségi Szemle, 2002/12, 84-99.oldal, ISSN 1585-4167

¹² Ackerman, Robert K. "Training, Not Technology Is Key to Urban Warfare." SIGNAL Magazin, May 2001

¹³ Modok Ferenc: A DIVAHR rendszer, MH EI Rt. 1997

A HARCTÉRI KOMMUNIKÁCIÓ EGYIK LEHETSÉGES JÖVŐKÉPE: A HARCÁSZATI INTERNET

A nem túl távoli jövőben, a katonák harci körülmények között fogják használni a személyi kommunikációs eszközeiket, amelyek egy olyan vezeték nélküli kommunikációs hálózathoz csatlakoznak, mely a szárazföldi dimenzióon túl lefedi a levegőt és a tengereket is. Személyi mikro-komputer fog választ adni arra, hogy hol, mikor és merre mozognak a csapataink, merre van az ellenség, és lehetővé téve a katona számára a személyes harctéri döntéseket.

A parancsnokok harcálláspontjai kilométerekre lesznek a valós harctól, a high-tech háborús „szobában”, és falméretű, nagyfelbontású térképeken követhetik a harctéri történéseket, vagy avatkozhatnak be valós időben. Egy *teljes harcászati képpel* fognak rendelkezni, és valós-idejű döntéseik nyomán, valós-idejű csapásmérést képesek vezényelni a kritikus helyeken. A teljes harcászati kép kialakítására szolgál a Harcászati Internet elnevezésű integrált kommunikációs hálózat, amely elsősorban a harcvezetés dimenzióit hivatott kitágítani.

Rendszertervezések

Meghatározó, hogy a legtöbb ország haderejének különböző szintjei közötti adatelosztás megszervezése elsőrendű feladat, a katonai műveletek sikeres végrehajtása érdekében.

Ország	USA	Kanada	Nagy-Britannia	Franciaország	Németország
Jelenlegi harcászati kommunikációs rendszer (szárazföld)	MSE TRI-TAC SINGGARS rádiórendszer	DARTS IRIS IRIS rádiórendszer	PTARMIGAN és MRS CLANSMAN rádiórendszer	RITA RITA2000 PR4G rádiórendszer	AUTOKO AUTOKO90
Harcmező digitalizálás utáni rendszer	WIN és MSE/TP SINGGARS és JTRS rádiórendszer	IRIS és BattleWEB IRIS rádiórendszer	PTARMIGAN BOWMAN BOWMAN rádiórendszer	RITA2000 és SIR progr. PR4G Fastnet Rádiórendszer (lehetőség)	AUTOKO90 +BIGSTAF Szoftverrádiók rendszere
Vezetési információs rendszer (dd. szinten és az alatt)	Force XXI battle command (FBCB2)	BattleWEB és MESHNET (adatelosztó rendszer)	BOWMAN és WAVE (adatfeldolgozó rendszer)	TACTIS, MESREG, FINDERS, (SIC-F)	HEROS (mobil C ³ I rendszer)
Harcászati Internet kialakítás	Tactical Internet	BattleWEB	Tactical Internet	Kidolgozás alatt	Kidolgozás alatt

1.táblázat: Egyes NATO tagországok kommunikációs rendszereinek fejlődése

forrás: Jane's Military Communications 2001-2002 [1]

A hatékony információ- és adatelosztás megvalósításához azonban végre kell hajtani a hadszíntér digitalizálásának programját, amely hozzájárulhat az információs fölény kialakításának képességéhez is. A digitális harcmező fejlett

információs képességei adják az alapját a modern harcvezetési eljárásoknak, amelyek a szövetség tagországainak napjainkban érvényes doktrínáiban jelennek meg. Az 1. táblázat vezetéstámogató rendszereiben rendre megjelennek ezek az elvárások, és a korszerű, digitális, nagysebességű kapcsolóelemek hálózatba szervezésében öltenek testet.

Miért Internet?

A válasz megadása előtt tegyünk egy rövid kirándulást a múltban [2]. 1957-ben az Egyesült Államok Védelmi Minisztériuma létrehozott egy kormányhivatalt, a Fejlesztési Kutatások, Tervezések Ügynökségét¹⁴, válaszul a szovjetek első műhold fellövésére. Az Ügynökségnél 12 év múlva, 1969-ben egy katonai számítógépes hálózat alapjait rakták le, amelyben az információk „csomagokra” darabolva mozogtak. Az ARPANET lehetővé tette az adatok szabad keringését a katonai hálózatban, és a gyakorlat bebizonyította, hogy ez a hálózati formáció hatásosan működik az adatátvitel, adatelosztás vonatkozásában. A hidegháborús szembenállás csökkenésével - a nyolcvanas évek közepére - a hálózat, a kutatási irányok változása miatt háttérbe szorult, így a katonai szféra kivonult a formációból, és ami megmaradt, abból fejlődött ki a ma Internet néven ismert világháló.

A meghálózattá fejlődés, a világ szinte minden részén kiépített hozzáférési lehetőség, az Internetes technológiák fejlődése és nem utolsósorban a mindezeket lehetővé tevő személyi számítógépek elterjedése, az (amerikai) katonai vezetők figyelmét ismét erre a területre irányította. Az adatátvitel előre nem prognosztizált megnövekedése miatt is szükség volt a „bevált” módszerekhez visszatérni, illetve az amerikai gazdasági, politikai, katonai érdekek mind hangsúlyosabbá válásával szóba került egy világméretű kommunikációs hálózat megvalósítása. Gazdasági megfontolásokból is célravezetőbb egy gyors adatáramlást megvalósító, fejlett infrastruktúrán alapuló, a civil szférában is beszerezhető alkatrészekből kiépíthető hálózatban gondolkodni, amihez a bárhonnan való csatlakozás előfeltétel. A hálózati biztonság kérdéskörének vizsgálata azonban megkívánta az elkülönülést a világhálótól, így a katonai változat közelebb áll egy nagykiterjedésű Intranet jellegű hálózathoz.

Alkalmazási szintek

Alapvetően a vezetés – irányítás részére kerül kiépítésre a Harcászati Internetnek nevezett digitális információs hálózat, amely támogatja a harcászati rendszerek működtetését és folyamatos figyelemmel kísérését. Ennek a hálózatnak elsősorban rugalmasnak kell lennie, toldás és hézagmentesnek, és megfelelő kommunikációs csatlakozást kell, hogy biztosítson az egész hadsereg harcászati felhasználói részére.

A Harcászati Internet leírható úgy is, mint egy integrált hadszíntéri kommunikációs hálózat, amely funkciójában hasonlóságot mutat a Nyilvános In-

¹⁴ Advanced Research Project Agency (ARPA)

ternettel¹⁵, annál is inkább, mivel infrastruktúrája az Internet technológián (IP)¹⁶ alapul. Kulcsfontosságú az a képesség, - csakúgy, mint a nyilvános Internetnél, - hogy az információ eljuthasson a hálózat bármely szegmensébe.

A Harcászati Internet kialakítását általában két, elkülönülő szintre tervezik és szervezik:

- Dandár szint fölött
- Dandár és az alatti szinteken

A dandár szint fölötti alkalmazásoknál a „Lövészároktól a Vezérkari Főnökig terjedő valós idejű kommunikáció” elgondolások¹⁷ szerint biztosíthatjuk az információkat, míg dandár és az alatti szinteken használva ezt a hálózatot, a hadsereg harcvezetési rendszerét terjeszthetjük ki a katonákhoz és a fegyverrendszerekhez.

A Harcászati Internet megvalósításával szembeni elvárások közül kiemelkedik a *mobilitási képesség*, a *kommunikáció folyamatosága* széles sávban, többféle üzemmódban, a hang és adatátvitel¹⁸ biztosítása, valamint az *automatikus útvonalválasztás*, de a *kerülő irányok biztosítása* is.[3]

A Harcászati Internet jellegű hálózatoknál a legmagasabb szinten általában a civil/üzleti szféra vezetékes hálózatain történik az információs rendszer kialakítása, és fix telepítésű műveleti központok között kerül megvalósításra az információ áramoltatás. A művelet-végrehajtói szinteken, a hadtest, dandár és ezek alatt megjelenő vezetési pontok összeköttetéseinek stabil biztosítására viszont egy tábori híradórendszer kerül kiépítésre, a veszélyeztetettség szintje szerinti nagyságban, és annak trónk¹⁹ kapcsolatai felhasználásával történik az információelosztás. Szükségessé válik az alacsonyabb szinteken keletkező információk megosztása a magasabb szintű elemek vezetési pontjaival, műveleti központjaival, illetve a különböző parancsok, műveleti előírások lejtuttatása a harcászati, végrehajtási szintekre. Ez az elvárás maga után vonja a két (ál-landó és tábori), funkcionálisan elkülönülő rendszerszint kapcsolódási lehetőségeinek stabil kiépítését.

A még alacsonyabb (zászlóalj, század) végrehajtói szinteken rádiókészülékek hálózatba szervezett elemei biztosítják az összeköttetést a harcjárművek között, és itt is stabil adatátvitelt kell megoldani a Harcászati Internet előnyeinek kihasználásához. A viszonylag keskeny sáv szélességben dolgozó har-

¹⁵ Célszerűnek tartom megnevezésben is elkülöníteni a civil használatú Internetet a katonai célútól

¹⁶ IP – Internet protokoll. A protokollok, a hálózati kommunikációt leíró szabályok rendszere. Protokollokat használnak a hálózatokban egymással kommunikáló számítógépek és programok is.

¹⁷ „Foxhole to the Whitehouse” és „C4I for the Warrior” koncepciók.

¹⁸ Amibe beletartozik az állókép és lehetőleg a mozgókép, a videó is.

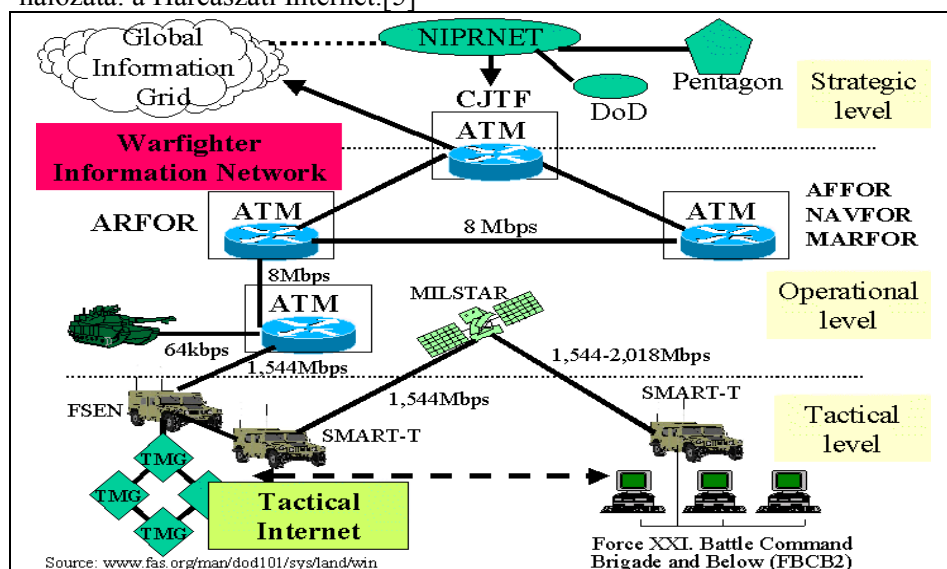
¹⁹ Csatornanyalábolás, csatornaösszefogás

cászati rádiók (jellemzően 50kHz, 25kHz vagy még ennél is kevesebb) viszont komoly gátját képezhetik a folyamatos, nagy adattömegek áramoltatásának.

Általánosságban egy olyan kombinált hálózati topológia kialakítása a cél, ahol a felhasznált szoftver és hardver elemek megfelelően működnek szinte bármilyen sávszélesség korlátozás között.

Az amerikai Harcászati Internet

Az amerikai Harcászati Internet [4] kialakítására azt a hipotézist állították fel a kilencvenes évek közepén, hogy ha egy alkalmi harci köteléken (Task Force [TF]) belül a digitális kommunikációs csatlakozásokat mind *függőlegetesen*, a parancsnoklási hierarchia szerint, mind *vízszintesen*, az együttműködés megvalósítására kiépítik, akkor megnövelhető az erők csapásmérő-képessége, túlélőképessége, és a műveletek végrehajtási sebessége is. Az amerikai hadseregben ma az egyik legfontosabb végrehajtandó feladat a hadszíntér digitalizálása. Az USA haderejében – többek között az Összhaderőnemi Elképzelés 2010, 2020 (Joint Vision [JV] 2010, 2020) hadművelleti koncepciók hatására és megvalósítására –, egy olyan kommunikációs rendszer, a Warfighter Information Network (WIN) alapjait alkották meg, amely a Pentagon és a Védelmi Minisztérium vezetését hívatott megvalósítani, kapcsolódva a Világméretű Információs Hálózathoz (Global Information Grid), illetve a műveletvégrehajtói szintekhez. A WIN szegmense a harcászati szint egyik információs hálózata: a Harcászati Internet.[5]



1.ábra: A Warfighter Information Network (WIN) felépítése [6]

A Harcászati Internet amerikai változata egy felső (Upper TI) és egy alsó (Lower TI), egymástól funkcionálisan elkülöníthető részből áll.

A felső szintű Harcászati Internet magában foglal:

- Egy számítógépes hálózatot (a Hadsereg Harcászati Vezetési és Irányítási Rendszerét²⁰)
- A hadsereg tábori híradó és informatikai rendszerének egyes szegmenseit (Mobil Felhasználók Hálózati Készülékei²¹)
- Valamint, az ITT gyártmányú Nagykapacitású Adatrádiók²² dandárszintű csatlakozási felületeit.

Az alsó szintű Harcászati Internet tartalmaz:

- Egy számítógépes hálózatot a 21.századi Erők Harcvezetésére, dandár szinten és az alatt²³ (FBCB2)
- Egy Földfelszíni Helymeghatározó és Jelentő Rendszert²⁴ (EPLRS)
- Egy harcászati rádióháló szegmenseit²⁵ (SINCGARS CNR)
- Gépjárműbe épített Harcászati Többfunkciós hálózati Átjárókat²⁶, valamint LAN routereket az üzenetkezelő rendszerhez

Az első csapatpróbák után, a gyakorlatban jelentkező adattovábbítási problémák kiküszöbölésére az alsó szintű hálózatban is alkalmazásra kerültek a NTDR-ek, a dandár és zászlóalj szintű harcászati műveleti központokban (Tactical Operations Center [TOC]).



2.ábra: FBCB2 számítógép terminál
A Helymeghatározó és Jelentő Rendszer kialakításánál az alábbi követelményeket vették figyelembe:



3.ábra: EPLRS egységek

²⁰ Army Tactical command and Control System (ATCCS)

²¹ Az amerikai tábori híradó és informatikai rendszer egyik alkotórésze a Mobil Felhasználók Hálózata, angolul: Mobile Subscriber Equipment (MSE), amely integrálja a felhasználók termináljait, a kapcsolóeszközöket, a rádiófelvevő pontokat, az információvédelmet és az összetett híradórendszer szabályozását.

²² Near Term Digital Radio (NTDR); jellemző adatsebesség: 288Kbps

²³ Force XXI Battle Command, Brigade and Below (FBCB2)

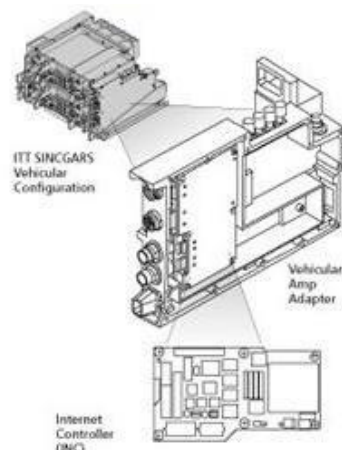
²⁴ Enhanced Position Location Reporting System (EPLRS)

²⁵ Az amerikai haderőben egy egycsatornás rádiórendszer van rendszeresítve a szárazföldi csapatok és a légierő részére, angolul: Single Channel Ground and Airborne Radio System (SINCGARS)

²⁶ Tactical Multifunction Gateways (TMG)

- Pontos helymeghatározás (GPS)
- Valós idejű adatbázis hozzáférés
- Korszerű digitális rádióháló
- Nagy jelsebességű adatkezelés
- Személyekre, járművekre meghatározott azonosító kódrendszer

Ez a rendszer információt biztosít az egységek azonosításához, helyzetük meghatározásához, illetve az egységek harcképességének meghatározásához. Az EPLRS az Időosztásos Többcsatornós Hozzáférés (Time Division Multiple Access [TDMA]) és a frekvenciaugratásos technológiákat felhasználva, magas fokú mobilitás mellett, nagy sebességű, automatizált adatcserét biztosít.²⁷



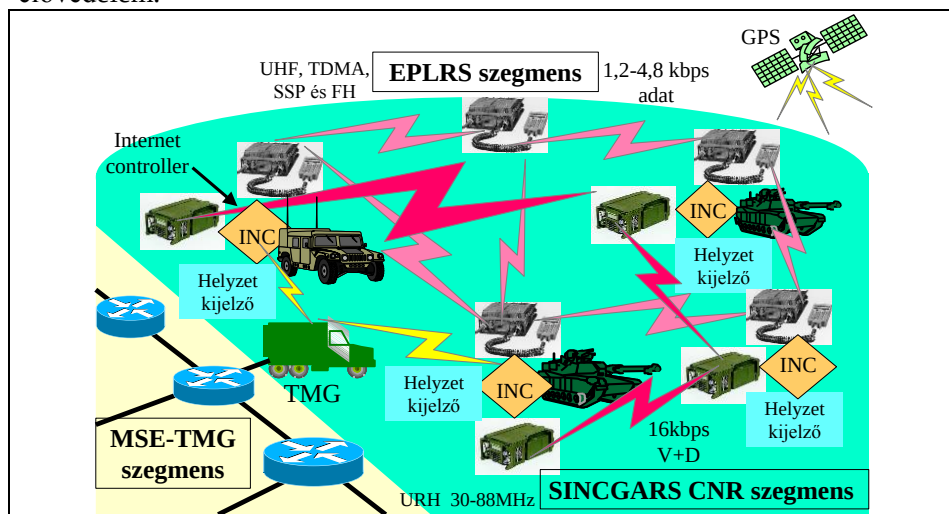
4.ábra: Az Internet Controller (INC) elhelyezkedése a rádiósketben

Az Egycsatornás rádiórendszer a szárazföldi csapatok és a légierő részére, vagyis a SINCGARS rádiócsalád elsődlegesen a lövész, páncélos és tüzér egységek, alegységek részére biztosítja a vezetést – irányítást. A moduláris felépítés kialakításánál figyelembe vették a szárazföldi csapatoknál és a légierőnél alkalmazott különféle egyéb rendszerek felépítését, alkalmazását (pl.: fegyver-irányítási rendszerek). Közvetlen GPS csatlakoztatásra képes, valamint hangadás – vételére, harcászati adatváltásra és a küldött üzenetek rögzítésére is a NATO interoperabilitási követelményeket kielégítve. Az URH sávban dolgozó, 30 – 88 MHz- es frekvenciatarományban mintegy 2320 csatornát lehet kiválasztani, amelyeken az információtovábbítás lehetséges nukleáris támadás esetén is.

Az amerikai *tábori híradó és informatikai rendszer* egyik alkotórésze az MSE, router protokollok alkalmazásával bővült a Harcászati Internet kialakítá-

²⁷ Szakasz és század szinteken jellemző a 1,2 – 4,8kbps, zászlóalj szinten ez már 16-28 kbps is lehet, míg dandár szinten elérheti az 58kbps jelsebességet is.

sára. Ennek hatására a rendszer szolgáltatásai között olyan új elemek jelentek meg, mint az elektronikus üzenetkezelés, hálózati könyvtár – létesítés, hatékonyabb hálózatmenedzselés, magasabb biztonsági fokozaton működő információvédelem.



5.ábra: Az amerikai Harcászati Internet alsó szintű felépítése

A Harcászati Internet alsó szintjének három fő szegmense: az FBCB2, az EPLRS, és a SINCGARS rádiók, valamint a NTDR adatrádiók és az MSE/TPN²⁸ -TMG alkalmazásával minden eddigénél hatékonyabban lehet megvalósítani a vezetési – irányítási információs rendszer alkalmazását a modern hadszíntéren. A továbbfejlesztett adatátvitel miatt megnövekedett az átviteli kapacitás, és az információ kevesebb kommunikációs trónkón fog átáramlani, mint a fix telepítésű, nyílt rendszereknél. A különböző szimulációs tesztek és összehasonlító modellezések során kialakultak az optimális paraméterek az Internet Protokollok (IP) használatában és ezek biztosítják a katonai szükségletek dinamikus és rugalmas megvalósítását a Harcászati Internet kommunikációs csatlakozásaiban.

Fontos szolgáltatás a Harcászati Internet információvédelme. Ez Magas Rejtjelzési Rendszer (Secret High System [SHS]) néven került kialakításra a kommunikációs hálózaton belül, biztosítva a vég – vég közötti rejtjelzést. A többszintre definiált rejtjelzési mechanizmusok magas szinten biztosítják a rugalmasságot.

Ugyancsak fontos szempont a rendszerirányítás technikai megvalósítása. A Rendszerintegrációt Szabályzó²⁹ programcsomag telepítése adja a hálózat

²⁸ Az MSE az újonnan programozott routerek hatására kibővülő lehetősége az adatátvitelben, ezt jelzi a Transmission Protocols to Network (TPN) rövidítése, magyarul: Átjátszási Eljárások a Hálózathoz

²⁹ Integrated System Controller (ISYSCON)

technikai irányításának lehetőségét a dandár alatti és a dandár fölötti Harcászati Internetnél. Míg alacsonyabb szinten a Harcászati Többfunkciós Átjárók (TMG) és Internet Szabályzók (INC) követelik meg a hálózat menedzselést, addig magasabb szinten az MSE/TPN, illetve a NTDR adatrádiók csatlakozásaiban kell ezt biztosítani, és az ISYSCON szoftver mindezt kiterjeszti automatikus hálózat menedzseléssé. A kommunikációs elemekre telepített Egyszerű Hálózati Menedzsment Protokollok³⁰ biztosítják a menedzser protokollokat proxy ügynökök (proxy agents) formájában az a Harcászati Internet működéséhez.



6.ábra: A Harcászati Internet harcjárműben

A harccsoportok járműibe épített SINGARS harcászati rádiók közös keretbe építve tartalmazzák az Internet Szabályozó Egységet (Internet Controller [INC]), amely integrálja az EPLRS kódjeleit a rádió adatforgalmával, és továbbítja azokat a helyzetkijelző monitorhoz, így a harctevékenység fizisaiban reális képet kap adott járműparancsnok a harctér helyzetismeretéhez, amelybe beletartozhat a műveleti térben mozgó járművek hovatartozása. Ehhez viszont az is szükséges, hogy a saját csapatok el legyenek látva a harci azonosító jeleket (Battlefield Combat Identification System [BCIS]) sugárzó berendezésekkel.

Az Internet Szabályzókra csatlakoztatott helyzetkijelzők, digitális, érintésvezérelt adatterminálok az FBCB2 rendszer tartozékai. Közös harcászati adatbázisokból (Joint Common Database [JCDB]) valós időben megjeleníthető adatok, harctéri azonosító rendszerek jelei, digitális térképek, időjárás előrejelzés stb. adják meg a valós Harcászati Kép kialakításának lehetőségét, amely egy integrált harctéri helyzetismeretet (Situational Awareness [SA]) kombinál az összhaderőnemi közös feladatokkal (Joint Common Operations [JCOP]). Új szervezetek ugyancsak integrálhatók a rendszerbe, erre a digitális eszközökkel való ellátottság egyre szélesebb köre a biztosíték.

Az angol haderő Harcászati Internete

Az angol elképzelések a Harcászati Internet kialakításának vonatkozásában a Bowman digitális híradó és informatikai rendszerre épülnek. A tervek szerint 2026-ig rendszerben lévő rendszer szívéét a harcászati rádiórendszer³¹ alkotja, amelyben szélessávú (1,6 - 512 MHz) szoftverrádiók kerülnek alkalmazásra, és ezek biztosítják a szenzoradatok, az álló – és mozgókép információk átját-

³⁰ Single Network Management Protocols (SNMP)

³¹ Az angol haderőnél napjainkban van a korábbi CLANSMAN rádiórendszer lecserélése

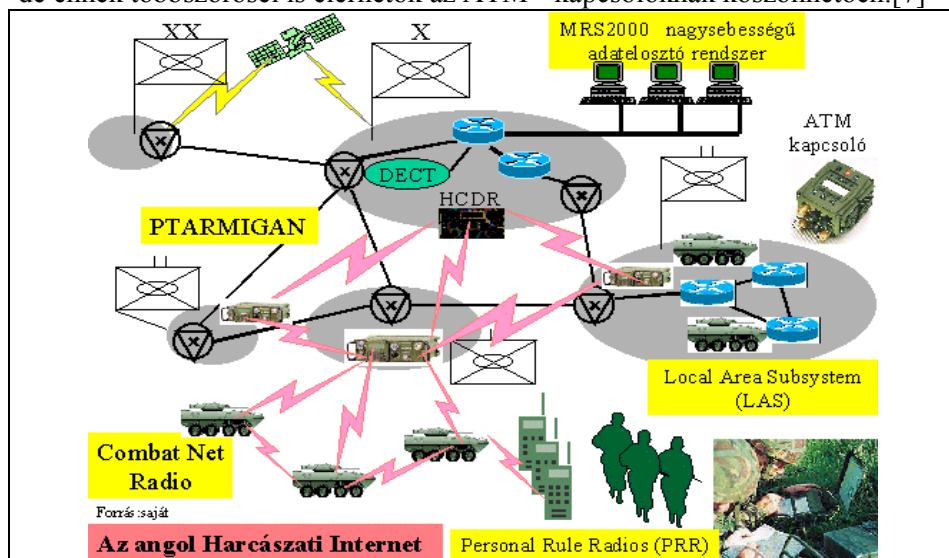
szását, a kombinált hang– és adatátvitel mellett. Minden rádió közvetlen, beépített GPS vevővel rendelkezik.

A harcászati rádiórendszer mellett, integrálva vannak a rendszerbe a Személyi Rádiók³², amelyek a harcosok felszerelésének tartozékai, és hatékony üzenetkezelő rendszert támogatnak.

Ugyancsak alrendszere a harcálláspontok belső kommunikációs hálózatainak kialakítása, amelyek akár vezeték-nélküli kapcsolatokon, akár optikai kábelekkal kerülhetnek kiépítésre, és a csatornák információ-bedugulása nélkül képesek üzemelni (a BOWMAN-LAS program szerint).

Jellemző a Bowman – re az erőteljes logisztikai támogatás, mivel hatékony hozzáférést biztosít a logisztikai adatbázisokhoz a különböző szervezeti szintekről, a műveletek minden fázisában.

A Nagykapacitású Adatrádiók³³ a megnövekedett információmennyiség átvitelét biztosítják, a rendszer összes viszonylatában, gyors és nagykapacitású kapcsolatokat alkotva a harcjárművek, a Harcászati Internet és az angol tábori területi hírrendszer (PTARMIGAN) között. Jellemző adatsebesség a 288 kbps, de ennek többszöröse is elérhető az ATM³⁴ kapcsolóknak köszönhetően.[7]



7.ábra: Az angol Harcászati Internet kialakítási lehetősége

A ma alkalmazott harctéri járművek legtöbbje rendelkezik egy belső beszélgető rendszerrel, amely szervesen kapcsolódik a harcászati rádióhálózathoz (CNR). A gép és harcjárművek mozgékonyága, sebességnövekedése képes biztosítani a hadműveleti harcászati támadások mélységének elérését, amelyet

³² Personal Role Radios (PRR)

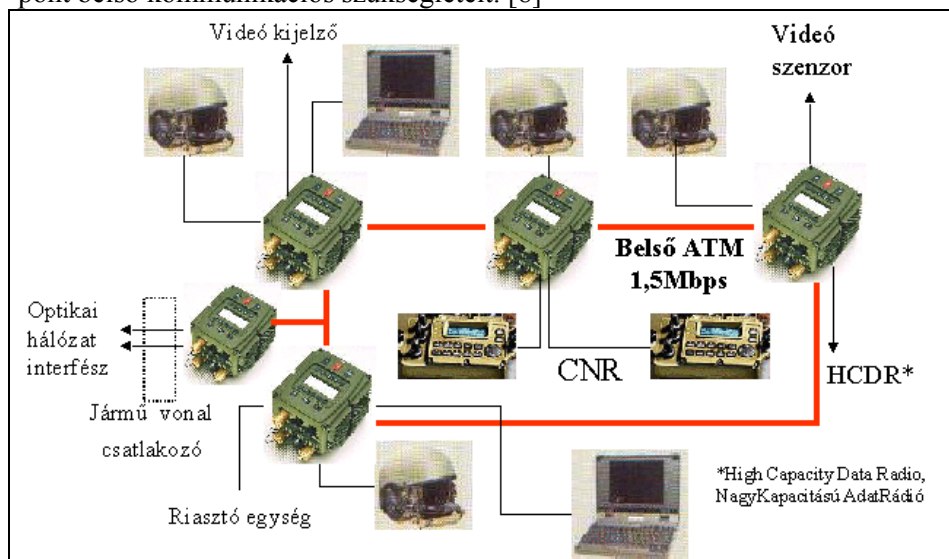
³³ High Capacity Data Radio,(HCDR)

³⁴ Asynchronous Transfer Mode

a harcolók részére meghatároz a parancsnok. A modern, gyors kapcsolóeszközök használata nélkül azonban a dinamika koordinációjához szükséges adatok, információk nem megfelelő szinten jutnak el a hálózat tagjaihoz.

A kor színvonalán álló harcjármű belső kommunikációs rendszere már teljes adatelosztásra képes, ami azt jelenti, hogy a rendszer Harcászati Hozzáfé-rési Egységei (Tactical Access Unit [TAU]) háromféle csatlakozást biztosítanak: számítógépeknek, adat/videó termináloknak és rádióknak vagy videó szenzoroknak. A harcászati szoftverrádiók mellett a Nagykapacitású Adatrádiók (HCDR) is használhatók.

Az angol haderő BOWMAN – LAS programjában³⁵ ilyen típusú kapcsolóeszközökkel oldják meg a járművek közötti kommunikációt, és a harcálláspont belső kommunikációs szükségleteit. [8]



8.ábra: Harcjármű belső kommunikációs rendszer multimédia lehetőséggel (SMARTNET)

A járművön belüli minden kezelőállomás számos rendszerinterfészt támogat, - például adatterminálok, rádiókészülékek, fejbeszélő egységek, számítógépek, szenzorok -, amelyek egymással is képesek kommunikálni a belső hálózaton keresztül. A rendszer elemei egyszerűen továbbfejleszthetők, szem előtt tartva a felhasználók számára a jövőben megjelenő lehetőségeket³⁶, valamint a kereskedelemben könnyen beszerezhető alkatrészeket (COTS³⁷).

³⁵ Local Area System (LAS), vagyis helyi, kis kiterjedésű vezetékes hálózat

³⁶ A szakirodalomban ezt PrePlanned Product Improvement (P³I) -nek nevezik, magyarul: előirányzott termékfejlesztés

³⁷ Commercial off-the-shelf , polcról levehető (civil) termék



9.ábra: Harcjármű belső kommunikáció

A francia Harcászati Internet

A franciák ugyancsak preferálják az információsükségletet a harcmezőn, és egészen szakaszparancsnoki szintig ellátják a harcolókat adatterminálokkal, de a nagy hálózatok megvalósításánál, a már rendelkezésre álló katonai (és esetenként civil) infrastruktúrára tervezik egy esetleges „Harcászati Internet” kialakítását. Mind több és több harcászati hálózat kialakítása a cél, bár a Harcászati Internet megnevezés nem szerepel a doktrínákban. Ennek ellenére az információelosztás a vezetési pont³⁸ „cellák” között a RITA³⁹ harcászati kommunikációs hálózat analóg és digitális vonalain, civil és katonai telefonvonalakon, műholdas csatlakozásokon (SYRACUSE⁴⁰), valamint a RITA-hoz (is) kapcsolható harcászati rádiórendszer viszonylatain valósul meg.

A francia haderő részére kifejlesztett, lehallgatás és zavarás elleni védelemmel ellátott, *többfunkciós*, ultrarövid hullámú sávon (jellemzően a 30 – 88 MHz frekvenciatartományban) üzemelő, negyedik generációs harcászati rádiórendszer a PR4G⁴¹. A PR4G rádiócsalád különböző teljesítményű (1W, 10-20W, 50-200W) és kialakítású (személyi, háti, járműbe építhető) rádióeszközökből áll. Megbízható működését az a tény is alátámasztja, hogy jelenleg 26 ország haderejében van rendszerbe állítva, - természetesen némi nemzeti változtatással -, és ebből 8 NATO-tagország.

A többfunkciós jelző jelen esetben 4 fő területet határoz meg:

- Harcászati rádióháló (CNR)
- Automatikus csatlakozás a tábori területi hírendszerhez
- Fegyverirányítási rendszerek kommunikációs szükségletei
- Harcászati Internet kialakításának szükségletei

³⁸ Command Post (CP)

³⁹ Réseau Intégrité de Tactique, francia tábori híradó és informatikai rendszer

⁴⁰ Nagytávolságú összeköttetésekre szolgáló, elsősorban rádiókommunikációt megvalósító francia műholdas rendszer

⁴¹ Le Poste de Radio 4ème Generation (rövidítve PR4G), vagyis 4. generációs rádióállomások

Egy Harcászati Internet jellegű hálózatban alkalmazva a PR4G rádiócsalád elemeit, - némileg továbbfejlesztve és kiegészítve az IP technológiát megvalósító számítástechnikai elemekkel -, alkották meg a PR4G Gyorshálózat (Fastnet) rádiórendszert.

A rádiórendszer interoperábilis a PR4G család valamennyi rádiójával (lévén, hogy azokból épül fel) és ugyanazokat a végkészüléket használja (harcászati számítógépek, adatterminálok, digitális faxok). A PR4G Fastnet-ben már modern, szoftverrel programozható rádiókat alkalmaznak a hullámformák széles körének használatához, és digitális jelfeldolgozó processzor⁴² biztosítja az előre-programozhatóságot és a többhullámformás működtetést.

A harcoló csoportok, szakasz és század szinten egy Harctéri Menedzsment Rendszert, a FINDERS-t használják Harcászati Internetként, amely beépítésre kerül minden harcjármű parancsnoki helyéhez és vezetési pont gép és harcjárműbe. Alkalmazásával elősegíthetik az akciók ütemének növelését, optimalizálhatják a harc hatékonyságát, illetve pszichikai erőként hatva növelheti a harcolók önbizalmát és összetartását, egymás segítését a művelet minden fázisában.



10.ábra: A FINDERS grafikus megjelenítője járműbe építve

A rendszer támogatja a szétbontakozást a terepen (harctéri azonosító jelek nyomon követésével és kijelzésével), valamint megóvás-támogatást biztosít (a fegyverrendszerekhez kapcsolódva) az ellenséges tűzérzési tűz és a légitámadások során.

A FINDERS minden pillanatban tiszta és megnyugtató válaszokat ad a jármű parancsnokának a következő feltett kérdésekre:

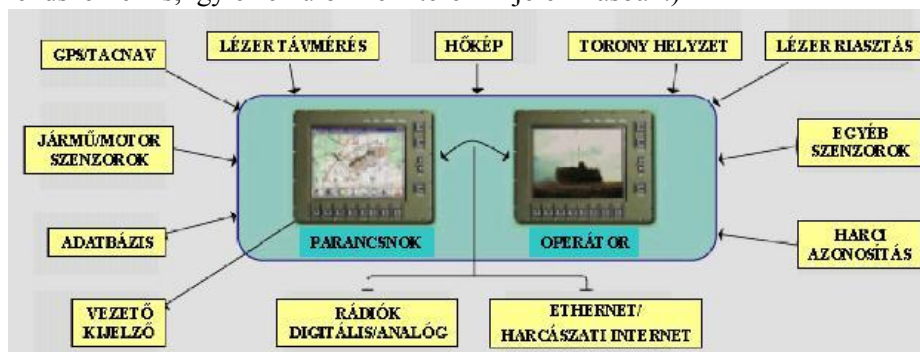
- Hol vagyok?
- Hol vannak a csapataink?
- Hol van az ellenség?
- Mit figyelhetek meg a belátható harcmezőn?
- Mi a feladatom?

Ezekon túlmenően a FINDERS támogatja a csoport parancsnoka részére:

- Az egyértelmű grafikus parancsok és jelentések adás – vételét;
- A csapat felszerelések technikai állapotának és logisztikai helyzetének menedzselését;
- Valós idejű harcmező ismeretet;
- Egy erőteljes, a harcászati helyzet analizálására szolgáló eszköz használatát;

⁴² Digital Signal Processor (DSP)

A harcászati vezetés számítógépes támogatásának hálózata jelenleg kiépítés alatt van a francia haderőben (SIR program), a számítógépeken futó SIC-F vezetési program viszont már rendszerben van a francia és a belga haderőben. (A SIC-F programcsomag képezi az alapját a kanadai BattleWEB információs rendszernek is, így erre külön nem térek ki jelen írásban.)



11. ábra: A FINDERS kijelző adatlekérdezési lehetőségei
(a kanadai BattleWEB is ezt használja)

A német Harcászati Internet

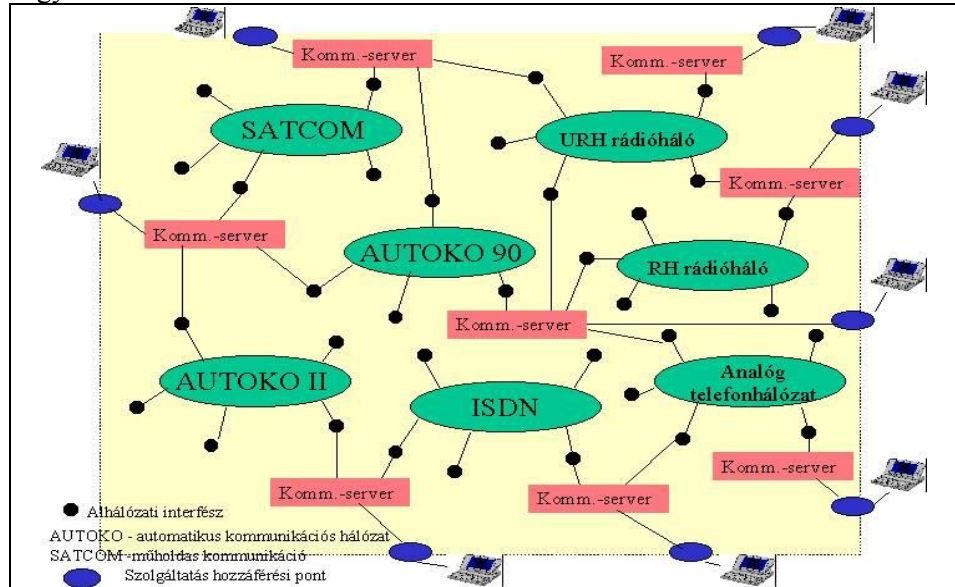
A német elvek szerint kialakításra kerülő Harcászati Internet-ben [9] alkalmazásra kerülő információtechnológia javítja és optimalizálja a harcászati vezetésképeséget. A Bundeswehr felső vezetése meghatározta, hogy az új technológiák bevezetésében az általános kereskedelmi termékeket (COTS) alkalmazzák (B-ISDN, ATM, WEB-technológia), a speciális katonai követelményekkel kiegészítve, és ezzel kerül kiépítésre egy globális, virtuális információs tér (hasonlóan az amerikai elgondolásokkal).

A mai német hadseregben, - hasonlóan számos ország haderejéhez -, heterogén, helyi hálózatokból áll a katonai kommunikációs rendszer. Ez részben elavult, túlnyomórészt rugalmatlan technikai elemekből épül fel, az interoperábilis hálózati elvárások csak speciális kimenetű eszközökön keresztül valósíthatók meg, gazdaságtalan üzemeltetéssel. A helyzetelemzés vezetett végső soron a Harcászati Internet (intranet) kialakításának szükségességéhez: az egyes helyi hálózatok közötti kommunikáció hatékony megvalósítása érdekében IP-n alapuló kommunikációs szerverek lettek telepítve.

Lényeges pont, a megfelelő sáv szélesség biztosítása, valamint a beszéd és adattovábbítás érdekében egységes, multifunkciós végberendezések alkalmazása. A harcászati elvárások közül a megnövekedett mobilitási képességet tartva elsődlegesen szem előtt, biztosított lesz a lehetőség, hogy a felhasználó bármilyen végberendezéssel, bárhol csatlakozhat a hálózathoz.

Az IP technológia jelentősége a harcászati kommunikációs hálózatokon belül óriási ütemben növekszik. A tesztek és ezek alapján a tervezett fejlesztések modellezhetőségével lehetővé válik az „Internet-telefon”, az IP alapú

beszédátvitel (Ipv6), és a hozzárendelhető beépített biztonsági funkciók (IPSec) folyamatos monitorozására, az áthallások csökkentése, az időbeniség megvalósítása és az elérhetőség növelésére. A katonai követelmények szerinti tesztelés alapján további elvárásokat fogalmazhatnak meg a felhasználók, a NATO és más országok kommunikációs rendszereinek interoperabilitását is figyelembe véve.



12.ábra: A német Harcászati Internet kialakítási lehetőségének vizsgálati hálózata

A Harcászati Internetek jövője

A Harcászati Internetekkel kapcsolatos kutatási területeken a legtöbb fejlett gazdasággal rendelkező nemzet kidolgozta, vagy napjainkban dolgozza ki elképzeléseit a jövőben kialakítandó mobil harcászati kommunikációs rendszereiről, a gyakorlatban azonban eddig kevés helyen került megvalósításra, szervezetszerűen pedig csak az amerikai hadseregben jutottak el a hadosztályszintű kialakításig. Az évek óta tartó alkalmazási próbák nem minden problémától mentesen zajlanak. Nehézkesen megvalósítható például a hívásadás a csomópontok között, és ez által a mobilkommunikációs bejelentkezési pont azonosítása. A hálózatba integrált statikus routerek, vagy a hozzájuk tartozó mobil Internet Protokollok nemegyszer használhatatlanok voltak, így a bejelentkező személy visszaellenőrzése nem volt lehetséges.⁴³

⁴³Ezt újonnan kifejlesztett, ad-hoc cellaformázási / üzenet routing rendszeralgoritmusok telepítésével küszöbölték ki.

Problémát okoznak a megnövekedett távolságok. A múltban a szakaszok hozzávetőleg 1km-es távolságon belül végezték a műveleteket, de mára az elkülönülés elérheti a 20 km-t is. A fegyverrendszerek hatótávolságának növekedése azt eredményezheti, hogy egy hadosztály egy több száz km-es kiterjedésű területen fog tevékenykedni. Egy dandár felderítő alegység pont-pont közötti összeköttetés igénye a 3-20 km távolságok között változhat, és a helyzetjelentéseknek „hosszú” kommunikációs utat kell megtenniük a vezetés híradási láncán, ami megnehezítheti a közel valós idejű döntéshozatalt. Nehézséggént merül fel, hogy a nagytávolságú összeköttetések (harcászati műholdas híradás, rövidhullámú rádiós kapcsolatok) jelenleg nem képezik részét a Harcászati Interneteknek, legalábbis az amerikai változatban. A nagytávolságon alkalmazott többutas átjátszás megbízhatóságának vizsgálata, a rendelkezésre álló sáv szélességek összehangolása az adatelosztás során megjelenő hatalmas fájl méretekkel (pl.: térképek, térképrészletek), az interoperabilitás biztosítása az egyéb összhaderőnemi / többnemzetiségű kötelékek kommunikációs, információszerezési rendszereivel, valamint a biztonsági eljárások precíz kidolgozása a rendszerek összehangolt információvédelméhez még a jövő feladatai közé tartozik. Az Információs, Vezetési és Elektronikai Hadviselés, vagy akár a Hálózat Központú Hadviselés hatásai a kialakított rendszerre ugyancsak a kutatási területek között kell, hogy szerepeljenek, csakúgy, mint a Harcászati Internet kritikus pontjainak meghatározása városharcban, magas hegyekben, vagy a dzsungel növényzetének dús lomboszata között.

Természetesen ez a vízió számos technikai és kulturális kérdést vet fel a katonák számára is. Mi történik, ha ebbe a high-tech hálózatba egy illetéktelen betör, vírussal fertőzi, hamis információt juttat be, működésképtelenné teszi? Az információhoz való hozzáférés ereje (vagy inkább mámora) nem fogja-e megváltoztatni a merev, katonai hierarchiát, az alá-fölé rendeltségi viszonyokat? Mi történik, ha minden szakaszparancsnok rendelkezni fog ugyanazzal az információval, mint a 2 – 3 szinttel magasabb parancsnoka? Ugyanez a szakaszparancsnok végre fogja-e hajtani a következő parancsot, kérdések nélkül, bízva az előljárója döntéshozatali képességében, a számára is nyilvánvaló információk alapján?

Ahogy az együttműködés mind magasabb, vagy még inkább mind alacsonyabb szintre terjed ki a közös műveletek végrehajtásában, a technológiák igyekeznek követni ezt az elvárást. Az információáramlás szabályozásával lehetővé válik, hogy a felsőbb szintű döntéshozó ne érdektelen vagy haszontalan információ tömeggel találkozzon, hanem a számára lényeges, olykor kritikus adatokat kapja. Felismert tény, hogy ezek a technológiák a dominóeffektus hatásait is magukban rejtik, különösen akkor, ha nem fordítunk kellő figyelmet a biztonsági kihívásokra, egy átfogó információvédelmi koncepció és eljárások formájában. Mindezen gondolatoknak meg kell jelennie a kiképzés, felkészítés területén is, ahol komplexitásában kerül oktatásra és begyakor-

lásra az új kommunikációs technológia használata, szerves részévé válva a katonai kultúrának is.[10]

Az információval kapcsolatos műveletek (gyűjtés, feldolgozás, tárolás, elosztás) mára már nem csak kizárólag az informatikai rendszerek feladata. A modern hadviselési elvekben rendre megjelennek a harcmező helyzetértékelésének elvárásai a műveletek vezetői, de végrehajtói részéről is. A bemutatott tipikus rendszerkialakítások az integrált híradó és informatikai rendszerek felé mutatnak, felismerve, hogy mindkét részterület a vezetéstámogatásban csúcsosodik ki. A műveletek sikere jórészt a vezetés hatékonyságán múlik, és a modern hadviselés elvárt mobilitási képessége ugyancsak megköveteli egy integrált, korszerű eszközökből álló kommunikációs rendszer vezetékes és vezeték nélküli kapcsolatait. A harctéri információszükséglet kielégítése minden hadviselési formában magas prioritást képez, és a modern technikák – technológiák alkalmazása ezt hívatottak biztosítani. A Harcászati Internetek megjelenése és elterjedése, a technikai fejlődés eredményeinek elegyítése az új típusú harc-eljárásokkal, vezetési metódusokkal, szoros összhangban van a nemzeti katonai doktrínákban vázolt kihívásokkal, az azokra adott válaszokkal – legalábbis kommunikációs vonatkozásban.

Források:

- [1] Jane's Military Communications 2001-2002, Jane's Information Group, 2001
Surrey CR5 2YU, UK, ISBN 07106 23 22 4
- [2] R.Zakon: Timeline of the Internet,
Internet: www.zakon.org/robert/Internet/timeline
- [3] Rupert Pengelley: Battling with tactical Internets, International Defence Review (IDR) 06/2000
Internet: www.idr.janes.com
- [4] The Tactical Internet, Internet: www.fas.org/man/dod-101/sys/land/internet-t.htm
- [5] The Warfighter Information Network – Terrestrial,
Internet: www.fas.org/man/dod-101/sys/land/win-ter.htm
- [6] The Warfighter Information Network – Tactical (WIN-T),
Internet: www.fas.org/man/dod-101/sys/land/win-t.htm
- [7] Bowman UK's revolution,
Internet: www.global-defence.com/Communications - Bowman
- [8] Rik Verhorst: From vehicle intercom to multimedia battlefield communications,
Defense Press of the Army (DPA), summer 1999
- [9] Walter Merker: Intranet-basierte taktische Kommunikation,
WTD 81 Kalvarienberg D-911171 Greding
- [10] Daintry Duffy: Information is a weapon ,
Internet: www.infowar.com/mil_c4i.shtml

AZ EGYSÉGES KÉSZENLÉTI DIGITÁLIS TRÖNKÖLT RÁDIÓRENDSZER, TETRA ÉS TETRAPOL JELLEMZŐI, SAJÁTOSSÁGAI

Bevezető

Cikkemben a Határőrségnél rendszerben lévő TETRA rendszert szeretném néhány szóban megvizsgálni, és fontosabb jellemzőit felvázolni a teljesség igénye nélkül. Ez a rendszer egy tervezett rendszer, amelyre kiírtak egy tendert, részletesen szabályozva ebben a támasztott elvárásokat a pályázó cégek irányába. A Határőrség Országos Parancsnokságán tett látogatás során betekintést nyerhettem ennek a rendszernek az összetételébe és sikerült néminemű ismeretet szerezni ennek a rendszernek az elvi és gyakorlati működéséről. Gondolok itt kialakulásának előzményeire, a különböző tervek, eszköztípusokra, melyekre néhány gondolatban kívánok kitérni. A cikk megírása óta mind a készülékekben, ind az alkalmazások területén minden bizonnyal történtek előrelépések. Az esetleges hiányosságokért szíves elnézésüket kérem.

Milyen előzmények vezettek ennek a rádiórendszernek a megalkotásához, milyen tényezők befolyásolták kifejlesztését. A vizsgálódások megkezdése előtt tisztáznunk kell mit is takar a megnevezés.

Mi is az a TETRA rendszer?

A TETRA egy angol mozaikszó, mely az alábbi eredeti angol kifejezést takarja: „Terrestrial Trunked Radio”. Ennek magyar megfelelője „földi trónkölt rádiórendszer”. Természetesen egy digitális, rendszerrel van szó, amely a mobil kommunikáció evolúciójának egyik még fejlesztésekre váró megoldása kecsegtető lehetőségekkel. Lényeg abban áll, hogy a GSM rendszerrel ellentétben sokkal nagyobb a megbízhatósága, a biztonság szempontjából jobb paraméterekkel rendelkezik, és becslések szerint alkalmazása során legalább háromszor gyorsabb összeköttetés felvétel valósítható meg a mobil rendszerhez képest, valamint lehetővé teszi a csoporthívást is. A hagyományos hangátvitelen kívül kiválóan alkalmas kép és adatátvitelre is, de sok esetben ez már az átviteli kapacitások felső határát súrolja többek között ez is az egyik lehetséges oka annak, hogy a fejlesztések elakadtak s nem fordítanak különösebb figyelmet a tényleges üzembe helyezésre. Nagy előnye, hogy a végfelhasználóknál elhelyezett eszközök különböző tartozékokkal egészíthetők ki, mint például elektronikus ujjnyom leolvasó, kamera, orvosi műszerek, stb., mely szolgáltatások véleményem szerint messzemenőig kihasználhatóak lehetnének. Ezt a mobil kommunikációs rendszert elsősorban a készenléti szervezetek számára fejlesztették ki, legalábbis ezen a felhasználói körön belül tervezik alapvető alkalmazását és szélesebb körű elterjedését. A TETRA-nak alapvetően két fajtája különíthető el: a civil és a készenléti. A lényegi különbség első-

sorban a felhasználói körben rejlik, de ez a megnevezésből is mindenki számára egyértelmű és világos. Ezen kívül a készenléti rendszer a sajátos felhasználói körből adódóan sokkal nagyobb megbízhatóságú, más funkciókkal rendelkezik, kellő mértékben titkosított és földrajzi lefedettsége is szinte 100%-os. A másik típusát elsősorban az üzleti szektor számára fejlesztették ki. Leszűkítve a felhasználókört, gondolok itt a biztonságtechnika, az energetika és az építőipar szektoraiban működő cégekre és vállalatokra. A TETRA rendszer fontos szerepét tovább hangsúlyozza, hogy egy adott vészhelyzet esetén a különböző készenléti szervek egységei akadály nélkül összekapcsolhatók, sőt lehetőség nyílik más országok kommunikációs rendszereivel történő együttműködésre is, fokozva így az általuk végrehajtandó tevékenységi kör még eredményesebb és hatékonyabb mivoltát, elősegítve a nemzetközi szinten történő együttműködést az érintett szervek között. A rendszerre kifejlesztett különböző típusú berendezések tökéletes együttműködését egy európai szabvány teszi lehetővé. Nem is olyan régen az Európai Unió tagországainak készenléti szerveinek együttműködése érdekében a NATO felszabadította a 380-400MHz tartományba eső frekvenciát hozzájárulva ebből adódóan egy a lehallgatással szemben kellő mértékben védett mobil kommunikációs rendszer kifejlesztéséhez. A cellaszerűen felépülő különböző nagyságú hálózatok révén lehetőség nyílik felhasználó csoportok kialakítására, reagálva az éppen kialakult szituációra. Természetesen mindez felügyelve és koordinálva egy központi diszpécser segítségével. Nagyvonalakban a könnyebb megértés érdekében talán ennyit. Néhány szóban szeretnék áttérni az előzményekre, melyek indokolták a rendszer kifejlesztését.

A megalkotáshoz vezető út

Mint minden esetben itt is az óriási mértékű fejlődés, a felhasználók újabb-nál-újabb igényei, a szolgáltatások minőségbeli emelése és az egyre magasabb szintű követelmények indokolták a változtatást. Ugyanis a belügyminisztérium számára pillanatnyilag rendelkezésre álló rádiórendszerek, melyeken keresztül a készenléti szervek, tehát a határőrség, rendőrség, vám és pénzügyőrség, a büntetés végrehajtás illetve a katasztrófavédelmi szervezetek, beleértve a tűzoltóságot, a polgári titkosszolgálatot, a mentőszolgálatot kommunikálnak, kezd elavulttá válni s már nem képes teljes mértékben eleget tenni a kor támasztotta követelményeknek. Gyökerei még az 1970-ben telepített infrastruktúrához nyúlnak vissza. Tettek ugyan bizonyos lépéseket a fejlesztések érdekében, de ezek nagyrészt csak felhasználóknál elhelyezett végkészülékeket érintették. Így jelentős részterületek maradtak érintetlenül vagy legalábbis nem sikerült megvalósítani a velük szemben támasztott elvárásokat, mint például a zavarással szembeni magasabb fokú védelmet, az illetéktelen személyek hozzáféréseinek kiküszöbölését, illetve a különböző szervezetek közötti zavartalan információcsere kérdésének megoldását. Másrészt jelentős problémát jelent, hogy az alkalmazott készülékek jelentős hányada technikailag jelentős mértékben le van amortizálódva. Ezek kicserélése mindamellett, hogy egy költséges dolog

lenne, azt eredményezné, hogy megint csak olyan berendezések kerülnének be a rendszerbe, melyek a régi kor színvonalának tesznek eleget, nem pedig korszerű, modern eszközök, melyek minőségbeli változást eredményeznének. Az új készülékek beszerzését indokolja a folyamatosan lezajló járműbeszerzés is, hiszen célszerűbb ezeket a gépkocsikat már az új technikával felszerelni idő és költségmegtakarítás tekintetében is. Továbbá, mint minden esetben itt is elmondhatjuk, hogy egyre inkább fokozódik a leterheltsége a csatornáknak, egyre nagyobb sávszélességre van igény, és a konvergencia élre törésének eredményeképpen már nem csak egyszerűen hangátvitelre van szükség, hanem képek átküldésére a hálózatokon keresztül, videó konferencia lebonyolítása, adatbázisokhoz való hozzáférés, azok lekérdezése, kezelése. Természetesen mindezeket a megfelelő állóképességgel, a kellő mértékben hitelesen, ha egy mód van rá „real time” módon, valamint megfelelő mobilitással és a környezeti viszonytárságoknak ellenálló képességekkel kell, hogy rendelkezzenek ezek a rendszerek,

Bármiben nyugodtan felvetődhet az a kérdés, hogy miért is van szükség a fent említett dolgokra. A válasz nagyon egyszerű és mindenki számára nagyon könnyen belátható. Az alkalmazásra kerülő rendszer meg kell, hogy feleljen ezeknek a követelményeknek abból a célból, hogy a korábban említett rend és területvédelmi szervek hatékonyan és eredményesen el tudják látni a hatáskörükbe tartozó feladatokat, képesek legyenek eleget tenni a velük szemben támasztott követelményeknek, zavartalanul együtt tudjanak működni. Ugyanakkor Magyarország is itt áll az Európai Unióhoz való csatlakozás küszöbén. A határok megszűnésével indokoltta válik nemzetközi szinten is a különböző rendészeti szervekkel történő még szorosabb kooperáció, például az embercsempészet visszaszorítása, a drog, a terrorizmus mindennemű formájának, csírájában történő felmorzsolása érdekében.

Az Európai Unióhoz való csatlakozás szinte megköveteli egy egységes digitális trónkölt rádiórendszernek a megalkotását és üzembe helyezését, természetesen úgy, hogy bármelyik tagország akadály nélkül kapcsolódni tudjon ehhez a rendszerhez, ne legyenek kompatibilitási, interoperabilitási problémák. Ebben a küzdelemben két, szinte hasonló rendszer veszi fel a versenyt: a TETRA és a TETRAPOL rendszer.

Melyek is a legfontosabb jellemzőik, melyek alapján megfelelnek a kiírt tendereknek? Felsorolásszerűen az alábbiakat említeném meg:

- Lehallgatás ellen védettek
- Hozzájárulnak az említett szervek hatékony és eredményes feladatteljesítéséhez
- Képesek kiszolgálni országos viszonylatban őket
- Nagy megbízhatóságúak
- Lehetővé válik a hang, kép, adat és egyéb kommunikációs módok egyidejű megvalósítása egymás zavarása nélkül

A tervek szerint ennek a rádiórendszernek a beszerzése az EU közbeszerzési pályázata alapján történik meg, és egy kormányrendelet eredményeképpen végrehajtották mind nálunk, mind az Európai Unión belül az együttműködéshez szükséges frekvenciaharmonizációt.

Kezdeti lépések

A gyakorlati megvalósítás első lépéseire 1998-ban került sor Budapesten. Ennek keretén belül a Belügyminisztérium egy kísérletet kezdett el az egységes digitális trónkölt készenléti rádiórendszerrel az Antenna Hungaria Rt. Részvételével bevonva a Budapesti Műszaki Egyetemet is. A TETRA szabványnak megfelelően alapvetően Motorola, Nokia, és Simoco típusú berendezéseket teszteltek. Az első 3db bázisállomással és mintegy 150 rádiókészülékkel, a második 1db bázisállomással és 30 db készülékkel, az utóbbi, pedig 2db bázisállomással és 80db készülékkel képviseltette magát. A TETRAPOL rádiórendszeren belül a francia érdekeltségű Matra Nortel vállalat 120db készülékkel és 1db bázisállomással járult hozzá a teszteléshez a Budapesti Műszaki Egyetem közreműködésével. Eltekintve az üzemeltetés során felmerülő kisebb problémáktól, egy kivételével mindegyik típusú berendezés megállta a helyét a nagyrészt éles körülmények között végrehajtott próbák során. A SIMOCO eszközök, mivel már induláskor sem működtek stabilan és megbízhatóan, így az éles helyzetben történő kipróbálásukra már nem is került sor.

A kísérletekkel szemben támasztott követelmények és az ezekből levonható tapasztalatok.

Kicsit tréfás formában mondhatnám azt, hogy a belügyminisztérium szakemberi szerettek volna meggyőződni arról, hogy valóban nem zsákhamacsát kínál számukra a másik fél, ezért az alábbi főbb célokat, kérdéseket tűzték ki, melyekre szerettek volna választ kapni a tesztelések végén:

- Műszakilag és szolgáltatás palettáját tekintve mennyire felelnek meg ezek a berendezések a velük szemben támasztott követelményeknek
- Azoknál a szerveknél, ahol alkalmazásra kerülnek milyen lehetőségek állnak rendelkezésre, és mennyire állnak készen a fogadásukra
- Milyen mértékben illeszthetőek a már meglévő kommunikációs infrastruktúrához
- A belügyminisztérium műszaki szerveinek megítélése az új technikával kapcsolatban
- Milyen következményeket hoz magával a rendszerbe állításuk, mire kell számítani a későbbi hosszú távú üzemeltetésükkel kapcsolatosan

Eredmények és következtetések:

- A kínált szolgáltatások széleskörűnek bizonyultak, a berendezésekkel együtt megfelelnek a szabványoknak, képesek biztosítani a szükséges adatátviteli képességet, megfelelnek az interoperabilitás követelményeknek

- Az egyes szervek felkészültek az új technika rendszerbe állítására, pozitívan vélekedtek ezekkel kapcsolatban, nem zárkoznak el a rendszerbe állítástól
- Ha néminemű nehézségek árán is, de megoldható a jelenleg rendszerben lévő eszközökről való áttérés az egységes készenléti digitális trónkölt rádiórendszerre kisebb-nagyobb nehézségek útján
- Ugyan ez elmondható a belügyminisztériumot kiszolgáló műszaki szervekről is, akik hasonlóképpen pozitívan vélekedtek a teszteléseket követően
- Nyilvánvalóvá vált azonban, hogy szükséges egy folyamatos rendszerfelügyelet, ugyanakkor lehetővé válik a felhasználók jogosultság szerinti nyilvántartása. Ennek a funkciónak a megvalósítását egy saját ügyfélszolgálatnak a felállításával tervezik megvalósítani, mely független a távközlési szolgáltatóktól. Ez biztosítaná a forgalmi felügyeletet, ellenőrzés alatt tartaná a rendszerhez való hozzáférést, kiutalná a felhasználók számára a különböző jogosultságokat

A rendszerrel kapcsolatban felmerülő elvárások

A cikk első néhány gondolata között általánosságban már említettem néhány fontosabb követelményt, mely köré körvonalazódik az alkalmazásra kerülő rendszerrel szemben támasztott követelményrendszer. Most néhány szóban ismét kitérnék erre. A digitalizáció térhódításából adódóan nem is lehet kérdés, hogy az egyik legfontosabb ilyen követelmény, mint azt az elnevezése is magában foglalja, hogy teljes mértékben kódolt és digitális legyen. Valamint nem utolsó szempont, hogy ezt a rendszert a már meglévő és használatban lévő belügyi távközlési infrastruktúrára kell tervezni és építeni.

A működtetéssel kapcsolatban két fő részterületet különíthetünk el. Az egyik a felügyelet, a másik pedig az üzemeltetés kérdésköre. A legfontosabb feladatok pedig, melyeket meg kell valósítani ennek a két szektornak, általánosságban az alábbiak:

- Kódolások és titkosítások végrehajtása és azok felügyelete
- Az adatbázisokhoz való hozzáférések biztosítása és azok felügyelete
- Szoftver fejlesztések végrehajtása
- A rádiórendszer tervezési és engedélyeztetési eljárásainak lefolytatása
- Egy közös összhang megtalálása a belügyminisztériumon belüli és kívüli szervezetek igényei és elvárásai között
- A szükséges gazdasági háttér biztosítása
- Az egyes eszközök beszerzése az igények, lehetőségek figyelembevételével
- Az együttműködés feltételeinek megteremtése

A felügyeleten belül azonban további három nagy kategória határolható el, a rendszer, a felhasználói és a forgalmi felügyelet.

A rendszer vagy más néven a műszaki felügyeletre háruló feladatok:

- Alapvetően a rendszer működésének biztosítása, üzemeltetése
- Forgalmi naplózás, forgalmi események nyilvántartása
- Hangrögzítés
- A hálózaton belüli routing kialakítása
- A rendszer paramétereinek meghatározása és beállítása
- A felhasználói csoportok kialakítása
- Kódkulcsok kialakítása
- A különböző prioritási szintek meghatározása
- Az egyes hálózati elemek beállítása
- A ki és belépő telefonkapcsolatok megvalósítása
- A központi adatbázisokhoz való hozzáférések biztosítása
- Levelezőrendszerekhez való csatlakozás biztosítása
- A rendszer időnkénti karbantartása
- A könnyebb áttekinthetőség érdekében a teljes hálózatnak és egyes részeinek, összetevőinek monitoros formában történő megjelenítése (mint tapasztalhattuk ezt a különböző szerveknél tett látogatásaink során a hálózatmenedzsmenttel kapcsolatosan)
- Riasztások kezelése, üzemi paraméterek felügyelete
- A felhasználói terminálok programozása, egyedi prioritások beállítása

A forgalmi felügyelet által ellátandó feladatok:

- Forgalmi naplózás ugyancsak
- Forgalmazás rögzítése és annak visszajátszási lehetősége
- A forgalmazások lehallgatása
- Különböző típusú hívások generálása (egyéni, csoportos, stb.) és azok fogadása
- Hangrögzítés szintén, mint az előbbi esetben
- Vészhívások kezelése
- Az analóg rádiórendszerekhez történő csatlakozás biztosítása és annak lebonyolítása
- Az egyes felhasználók tartózkodási helyeinek meghatározása

Végezetül pedig, a harmadik, a felhasználói csoport felügyelet által biztosítandó feladatok:

- A csoportok tetszőleges kialakítása, és bármikor történő átszervezése, átalakítása
- A felhasználói terminálok programozása a felhasználói csoportok igényeinek és a teljes rendszer igényének szem előtt tartásával
- Az egyéni prioritások beállítása, testreszabása
- GPS megjelenítése
- Különböző szintű jogosultságok beállítása

-
- Az egyes terminálok kiiktatása a rendszerből hosszabb rövidebb időre
Milyen rendszertechnikai követelményeknek megfelelően épüljön fel az alkalmazásra kerülő rádiórendszer

Magának a belügyminisztériumnak is vannak alapelvárásai, amelyeknek eleget kell, hogy tegyenek a pályázó cégek, de ezeket ki is egészíthetik az általuk kínált plusz lehetőségekkel, szolgáltatásokkal. Itt sok olyan dologra találhatunk, amelyeket az imént az ellátandó feladatokkal kapcsolatban már felsoroltam. Ez érthető is, hiszen a végrehajtandó feladatoknak, az elvárásokkal és a kívánt szolgáltatásokkal a rendszer eredményes működése érdekében szoros összhangban kell lennie. Ezek megvalósulása hiányában nem tudná betölteni alaprendeltetését.

Alappillérek:

- Ha a rendszerben bárhol meghibásodás lép fel vagy kiesnek tagállomások, akkor egyrészt legyen képes jelezni a meghibásodás helyét, annak mértékét, a további felhasználási lehetőségeket. Egy ilyen esetben sem legyen akadályoztatva az információáramlás
- Kiegyenlített jelszint legyen, ne legyenek jelentős mértékű ingadozások
- Egyaránt vezetékes és vezeték nélküli terminál esetében is megfelelő minőségű információtovábbítási lehetőséget biztosítson
- Teljes mértékben digitális úton történjen a hang, adat és egyéb információk átvitele
- Kódoltak legyenek ezek, megakadályozva az illetéktelen, hozzáférési jogosultságokkal nem rendelkező személyek betekintését illetéktelen
- A lefedettségi területen kívül eső tagállomások esetében az átvitel és a megfelelő minőség biztosítása érdekében legyen lehetőség a szükséges erősítők beiktatására, és az adatátvitel biztosítására is ezeken a területeken, a kommunikáció lehetőségének ez ne szabjon határt
- Biztosítva legyen a kódkulcsok kiosztása
- Képes legyen kapcsolódni a meglévő gerinchálózat eszközeihez hagyományos interfészen keresztül
- Legyen lehetőség a terminálok felhasználásának szervezésére és felügyeletére az elkülönült felhasználók esetében is
- A berendezéseket egy kormányrendelet alapján a 380-385MHz és 390-395MHz frekvenciasávra kell kalibrálni, ezen belül pedig, egy rádiócsatorna szélessége ne legyen nagyobb 25 kHz-nél
- Lehetőleg a frekvencia felhasználás független legyen az információcsere szolgáltatások fajtáitól, ha egy mód van rá, ne növekedjen azoknak megfelelően.
- Az egyes cégek előzetes felmérések alapján készítsenek számvetés arról, hogy az egyes területeken, különböző viszonyok között milyen szolgál-

tatásokat és milyen mértékben képesek szolgáltatni, figyelembe véve a rendszeresített gépkocsikat, antennákat

A tervezett, a rendszer által biztosítandó szolgáltatások

Itt szintén hasonló elvek érvényesülnek, mint a műszaki paraméterekkel kapcsolatban támasztott követelmények esetében. Ebben az esetben is a belügyminisztériumnak vannak alapvető kritériumai a szolgáltatások skáláját tekintve, de nem zárkózik el az adott cég által kínált többlétszolgáltatásoktól sem. Ezek alapvetően az alábbi elveknek kell, hogy eleget tegyenek:

- Legyen lehetőség az egyes paraméterek beállítására, ellenőrzésére
- Az egyes felhasználói csoportok együttműködésének biztosítása, felhasználói csoportok képzése, ezek módosítása
- Kódváltások zavartalan lebonyolítása
- Meghibásodás esetén a hatékony beavatkozás és hibaelhárítás érdekében azonnali, pontos riasztás jelzés
- Biztosítson lehetőséget a lefedett területen kívül elhelyezett terminálokkal való forgalmazásra is
- Ne legyen akadálya a különböző informatikai hálózatokhoz, számítógépes adatbázisokhoz való csatlakozásnak
- Közcélú telefonhálózathoz való csatlakozás megoldott legyen
- Képes legyen kommunikálni a meglévő analóg rádióhálózattal
- Csatlakozni tudjon a különböző levelező rendszerekhez, mint például az X400
- A központból le lehessen tiltani egyes terminálokat
- Kellő védelemmel rendelkezzen az illetéktelen behatolókkal szemben
- A berendezések rendelkezzenek megfelelő interfésszel az átviteli utak biztosítása érdekében
- Az eszközök biztosítsák az egyedi, csoportos hívás funkcióját
- Legyen mód a forgalmi események naplózására, híváskorlátozásra, vészhívásra, hívásátírányításra, hívófélazonosításra, hívásmegszakításra
- Képes legyen rövid szöveges üzenetek fogadására, küldésére
- Legyen egyaránt vonal, illetve csomagkapcsolt adatátviteli lehetőség is

Láthatjuk, hogy a rendszerrel szemben támasztott követelmények nem teljesíthetetlenek, hiszen az itt felsorolt műszaki vagy szolgáltatásbeli elvárások a civil életben is jelen vannak, gondoljunk csak például a különböző mobilszolgáltatókra és telefonkészülékeikre. Ezek nem mások, mint a civil életben jelenlévő, a mobil kommunikáció által jelentős mértékben alkalmazott technikai megoldások keveréke. Tulajdonképpen itt is hasonló elvek kell, hogy megvalósuljanak, mivel ennek a rendszernek is az egyik fontos alappillére a mobilitásban gyökeredzik.

Az eddig felvázolt elképzelések megvalósításához szükséges készülékek legfontosabb jellemzői

Azzal kapcsolatban, hogy a már korábban felvázolt technikai paramétereknek megfelelő készülékek konkrétan milyen formában jelenjenek meg, nagyon sokféle változat alakult ki. Itt is jellemző, hogy igyekeznek egy széles palettát rendszerbe állítani. Gondolok ezen belül az eltérő méretre, a különböző alaptartozékokra, stb.

Alapvetően három nagy kategóriáról kell beszélnünk, a kézi terminálokról, a mobil, általában gépjárművekbe épített berendezésekről és a fix telepítésű terminálokról. Ismét vissza kell térnem a „száraz” elvárások ismertetéséhez, mert a belügyminisztérium ebben a tárgykörben is elég alapos munkát végzett, és kemény feltételeket szabott a pályázókkal szemben a különböző rendeltetésű terminálok kialakításával, illetve az általuk kínált szolgáltatásokkal kapcsolatosan. Felsorolásszerűen szeretném ismertetni néhány mondat erejéig ezeket. Milyen kell, hogy legyen egy kézi terminál, mely alapvetően általános felhasználásra kerül rendszerbe állításra:

- Rendelkeznie kell alfanumerikus kijelzővel
- Minimum 1W kimenő teljesítményre legyen képes
- Megfelelő készenléti időt biztosító akkumulátorral rendelkezzen (a tervek szerint legalább 10 óra készenléti idő biztosításával)
- Legyen képes csatlakozni más adatátviteli eszközökhöz (pl. RS-232 csatlakozó segítségével)
- Rendelkezzen tasztatúrával
- Biztosítson lehetőséget csatornaváltásra
- Valamint nem is képezheti vita tárgyát, hogy megoldott legyen a hang-erő szabályozás

Alaptartozékként és kiegészítő eszközökként az úgynevezett „alapsomag-nak” tartalmaznia kell az antennát, az övcsipeszt, az akkumulátort, egyes vagy csoportos töltőt, gépjármű kihangosító szettet, GPS, tartalék tápegységet, különböző kezelő szerveket.

A készülékek rendelkezzenek az alábbi alapfunkciókkal: akkumulátor állapotának megjelenítése a kijelzőn, egyéni és csoportos hívás, beszélő azonosítása, vészhívás csak hogy a legfontosabbakat említsem.

Néhány szóban áttérnék a másik két termináltípus ismertetésére is. Már az első néhány sorban kísérteties hasonlóságot vélhetünk felfedezni az imént említett terminál jellemzőihez hasonlóan. Jelentős eltérésekre nem is kell számítanunk, hiszen ebben az esetben csupán a terminál telepítési helye változik. Maximum ez hordozhat magában némi különbséget. Természetesen kihangsúlyozva az „általános felhasználás” jelzőt, hiszen egy központban elhelyezett terminálnak jóval összetettebb feladatokat kell megvalósítania rendeltetéséből adódóan. Nézzük is meg ezeket: az előzőhöz hasonlóan itt is kell, hogy legyen egy megfelelő akkumulátor és tasztatúra, továbbá megoldott legyen a tetszőle-

ges csatornaváltás, hangerő szabályozás, GPS csatlakoztathatóság, a teljesítménnyel kapcsolatban itt már minimum 10W kimenő teljesítményre van szükség, szintén szükség van egy csatlakozási felületre más adatátviteli eszközök részére és ugyancsak egy alfanumerikus kijelző, aminek megléte nélkülözhetetlen.

Szolgáltatásait tekintve szinte teljesen equivalens a kézi terminállal: beszélő azonosítás, vészhívás, különböző típusú hívások, GPS jelek fogadása és továbbítása, adatbázisokhoz való hozzáférés, azok lekérdezése, kezelése, felolgozása, stb.

A fix telepítésű terminálokkal kapcsolatban a további redundáns információhalmaz elkerülése érdekében csak a felmerülő eltéréseket emelném ki, melyek az alábbiak: nélkülözhetetlen egy szünetmentes tápegység használata, a diszpécsernek legyen lehetősége jóváhagyni vagy elutasítani egy hívást, PSTN/PBX szolgáltatásokhoz való hozzáférés, hívások átirányításának lehetősége.

Azonban az csak egy dolog, hogy ezek a készülékek megvásárlásra kerüljenek, majd pedig rendszerbe állítják őket, ezek használatát egy viszonylag hosszabb időintervallumra tervezik. Ebből kifolyólag meg kell vizsgálni, és nem szabad figyelmen kívül hagyni az alkatrészekkel, csereegységekkel való utánpótlás kérdését sem vagy például a szerviz háttérét, a szükséges szoftverbázist, annak frissítési lehetőségét, kompatibilitását más szoftverekkel.

A tervezett rádiórendszer felállításával és az ennek kiépítéséhez szükséges készülékek beszerzésével az egyik nagy leküzdendő feladat megoldódni látszik, azonban mint tudjuk, legyen egy rendszer bármennyire is automatizált az emberi tényező jelenléte nem küszöbölhető ki. Véleményem szerint az ember az egyik legkritikusabb alkotóeleme ennek a struktúrának. Ebből adódóan még számos megoldásra váró feladatot kell megvalósítani.

A közeljövőben teljesítésre váró feladatok

Nagyon fontos a kezelői, kiszolgálói személyzetnek, az egyes személyekig lemenőleg a rendszer gördülékeny használatára való felkészítése, trainingek, kurzusok lebonyolításával. Meg kell vizsgálni a rendelkezésre álló lehetőségeket, a támasztott igényeket, közös nevezőre kell jutni ezzel kapcsolatban. Beleértve a gazdasági, pénzügyi, személyi háttérét. A már meglévő rendszer összehangolhatóságának, az új rendszer erre történő építhetőségének, ha szükséges új objektumok létrehozásának lehetőségét. Továbbá ki kell alakítani egy számkiosztási rendszert, egy egységes és közös ügyeleti rendszert és a hozzá kapcsolódó szintek meghatározását. A központi adatbázisokhoz való hozzáférés lehetőségeinek feltérképezése, prioritások kialakítása, stb. hasonlóan fontos és végrehajtandó feladat a közeljövőben.

Készülékek és jellemzőik

A kiírt tendernek megfelelő ismertetést követően szeretném megvizsgálnia dolognak egy kicsit a gyakorlati oldalát is, konkrét megjelenési formáját az

egyres készülékekkel kapcsolatban. Az alábbiakban néhány a Nokia által forgalmazott készüléket szeretnék bemutatni az internetes oldalakon talált képek, és az ott feltüntetett leírások segítségével. A tanulmányom első oldalain már korábban említettem, hogy a Nokia az egyik fontos résztvevője a TETRA fejlesztéseknek.

A THR420 rádió:

A készülék egy strapabíró alumíniumház borítást kapott, mely megvédi a külső behatásokkal szemben, és minden helyzetben magas szintű kapcsolat létrehozását teszi lehetővé. A rádió el van látva egy többfunkciós csatlakozóval, mely lehetővé teszi különböző tartozékoknak, például mikrofonos fejhallgatónak, fülhallgatónak vagy külső adatkommunikációs eszközöknek a rádióhoz való csatlakoztathatóságát. A megfelelő üzemidő biztosítása érdekében több fajta akkumulátorral látták el, a hozzá tartozó kiegészítők, mint például a gépjármű adapterek, a teleptöltők és a hordozótáskák pedig lehetővé teszik, hogy a THR420-at különböző helyzetekben használhassuk.



THR600 - A kompakt készülék:



A THR600 a Nokia egyik csúcsmodellje, professzionális szolgáltatásokkal felvértezve, ami a mobiltelefonokhoz hasonlóan egy hordozható kézi mobilkészülék, megtestesítve a kis méret és a modern tervezés kimagasló példáját. A duplex üzemmódban üzemelő THR600 ideális az egyéni rádiókommunikációhoz. Menürendszere könnyen kezelhető, nagymértékben segíti a széleskörű funkciók kihasználását és a készülék egyéni beállítását. A mindennapi életben forgalomban levő mobiltelefonokhoz hasonlóan itt is lehetőség van a billentyűk programozására, mely jelentős mértékben megkönnyíti, és gyorsabbá teszi a gyakrabban használt funkciók elérését. A kicsi, és praktikus THR600 egyaránt használható kézi készülékként, valamint gépjárműbe építve is. Ez nagyobb üzemelési területet biztosít, mivel a telep vezetés közben is feltölthető. A rendelkezésre álló tartozékok az alternatív telepek, a töltők, valamint a gépkocsi beszerelő vagy asztali kiegészítők.

TMR400 és TMR420 kapcsolata mozgás közben

A Nokia által forgalmazott TETRA mobilrádiók magas szintű kapcsolatteremtést és kommunikációt tesznek lehetővé mozgás közben is. Itt már megjelenik a konvergencia is a szolgáltatások palettáját tekintve, hiszen a beszédhang továbbításán kívül lehetőség nyílik a mobil alkalmazásokhoz szükséges adatok továbbítására, pl. helyzet-meghatározásra vagy adatbázisok lekérdezésére. A Nokia TETRA rádiók kétféle kezelőegysége közül lehet választani, a használat és a telepítés helyszínétől függően. Elsősorban gépjárműben való

használatra készültek és a rendelkezésre álló beszerelési csomagok és tartozékok széles köre révén gépkocsikban, hajókon, motorkerékpárokon és



különleges gépjárműveken is használhatók. Ezen kívül az asztali beépítő készlet révén fix irodai állomásként is alkalmazható. A **TMR400** egy olyan modern mobilrádió, melyet jelentős igénybevételre terveztek. A középen elhelyezkedő nagyméretű grafikus kijelző két oldalán találhatók a kezelőgombok, melyek egyszerű és gyors hozzáférést tesznek lehetővé a rendszer által kínált funkciókhoz.

A **TMR420** mobil rádióeszköz el van látva egy alfanumerikus billentyűzettel a könnyebb kezelhetőség és használat érdekében.



A csoportok kiválasztása és a hangerő szabályozása forgógombok segítségével történik, melyek a kiváló minőségű és viszonylag nagy kijelzővel együtt megbízható és könnyű üzemelést biztosítanak. Továbbá ha szükséges, akkor a berendezéshez mikrofon is csatlakoztatható.

A Nokia által forgalmazott TETRA terminálok legfontosabb jellemzői:

- Egyéni hívás
- PSTN (nyilvános telefonhálózat) hívás
- PABX (alközponti) hívás
- Csoportkommunikáció
- Közvetlen üzemmód
- Vészhívás
- Állapotüzenetek
- Rövid adatüzenetek
- IP csomag adatok
- Visszahívási kérés
- Sorba állítás
- Előfizetői és csoportprioritások
- Telefonkönyv

Táblázatos formában szeretném szemléltetni az imént felsorolt készülékek legfontosabb paramétereit a cég által megadott adatoknak megfelelően:

	TMR400/TMR420	THR420	THR600
Frekvencia-sávok	380-400, 410-430MHz	380-400MHz	380-400, 410-430MHz
Üzem módok	Félduplex, direkt és trónkölt	Félduplex, direkt és trónkölt	Félduplex, duplex, trónkölt és direkt
Kimenő teljesítmény	10W	1W	1W
Billentyűzet	TMR400: 29 billentyű, a vezérlő és programozható billentyűkkel együtt, BE/KI gomb, vész hívás billentyű TMR420: 23 billentyű a vezérlő és a programozható billentyűkkel együtt, BE/KI gomb, vész hívás billentyű, forgókapcsoló csoportválasztáshoz és hangerő szabályozáshoz	THR420: 20 billentyű a vezérlőbillentyűkkel együtt, BE/KI gomb, vész hívás billentyű, PTT (beszédváltó) billentyű, forgó kapcsoló csoportválasztáshoz és hangerő szabályozáshoz, 3 programozható billentyű	19 billentyű, BE/KI gomb, vész hívás billentyű, PTT (beszédváltó) billentyű
Kijelző	Dinamikus, nagy precizitású grafikus kijelző, térérő indikátorral, 7 ikon	Dinamikus, nagy precizitású grafikus kijelző, térérő és telepindikátorral, 7 ikon	Dinamikus, nagy precizitású grafikus kijelző, térérő és telep töltöttség szintjelző, 7 ikon
Méret	Rádiókészülék: 45 mm x 145 mm x 240 mm TMR400 kezelőegység: 90 mm x 175 mm x 40 mm TMR420 kezelőegység: 59mm x 185 mm x 30 mm	170 mm x 60 mm x 29 mm	152 mm x 54mm x 42mm
Súly	1,9 kg a kezelőegységgel	595 g a normál teleppel	370 g a normál teleppel
Telepek		1100 mAh, 1700 mAh (NiCd) 2500 mAh (NiMH)	900mAh (NiCd) 1200 mAh 1850 mAh (NiMH)

AZ INFORMÁCIÓK, VALAMINT A HÍRADÓ ÉS INFORMATIKAI RENDSZER VÉDELME NEK SZABÁLYOZÁSA

A fegyveres erők információs műveletei védelmének kialakítását különböző szintű szabályozók szerint kell kialakítani. A felülről lefelé kiépülő, egymásra támaszkodó alapelvek és rendszabályok a társadalmi és szervezeti hierarchiában lefelé haladva egyre részletesebb intézkedéseket írnak elő, amely rendszer ismerete támogatja a védelem rendszerszemléletű megközelítésének elsajátítását. Láthatóhatóvá válnak a különböző szintű rendszabályok közötti összefüggések, érthetőek lesznek a biztonság szempontjából lényeges környezeti elemek változásainak hatásai, és világossá válik a szükséges válaszreakciók kezdeményezésének szintje és hatásköre.

A stratégiai szint

A többszintű szabályozás legfelső szintjén a Magyar Köztársaság Biztonsági Stratégiában, a Katonai (Védelmi) Stratégiában, az Információvédelmi Stratégiában (esetleg még további funkcionális stratégiákban) foglaltaknak kell képeznie az elvi alapot az információk védelme érdekében szervezett tevékenységi rend kialakításához.⁴⁴ Ezekben a dokumentumokban úgy kell megfogalmazni a Magyar Köztársaság nemzeti és szövetségi információk védelmére vonatkozó alapelveit, hogy azok alapján levezethetők legyenek a szakterületet szabályozó jogszabályok és egyéb alacsonyabb szinten elhelyezkedő szabályozók.

A Magyar Köztársaság biztonság- és védelempolitikájának alapelveiről szóló országgyűlési határozat leszögezi, hogy hazánk a biztonságot több tényező együtteseként, átfogó módon értelmezi. Megállapítja, hogy hazánkra a tömegpusztító fegyverek és szállító rendszereik elterjedése mellett fokozódó kihívást és veszélyt jelent az információs rendszerek elleni támadás lehetősége.

A Magyar Köztársaság Nemzeti Biztonsági Stratégiája megállapítja, hogy a „lehetséges veszélyforrások összetettebbek, előre jelezhetőségük lehetősége csökkent, a belső és külső kockázati tényezők közötti határvonal elmosódott, valamint a különböző szintű kockázati tényezők egyszerre és egymással kölcsönhatásban jelentkeznek.”

Az „információs társadalom kihívásai” fejezet szerint a fejlett világ informatikai és telekommunikációs színvonalától való relatív lemaradás konzerválódása súlyos hatásokkal jár. A fejlett infrastruktúra kiépítése mellett fontos érdek a rendszerek védelme és a vészhelyzeti tartalékok biztosítása. A rendsze-

⁴⁴ Az utolsó két stratégia még nem készült el.

rek sebezhetősége olyan kockázati tényező, amelynek jellegzetessége, hogy kis erőösszpontosítás nagy távolságból is rendkívüli kárt képes okozni.

Formálisan nem stratégia, de mindenképpen említendő a védelmi felülvizsgálat első szakaszának lezárása után készített értékelés, amely számos új feladatot szab a Magyar Honvédség számára.

Az értékelés megállapítja, hogy a válságkezeléssel (békefenntartás-béketeremtéssel) kapcsolatos feladatok, a terrorizmus elterjedésének veszélye miatt az 1999. áprilisi washingtoni csúcstalálkozó döntései alapján a meglévő katonai kapacitások korszerűsítésre szorulnak. Újabb képességek kialakítására is szükség van, amelynek része a vezetés-irányítás és híradás (C3) modernebbé tétele (a szövetséges hadseregekkel interoperábilis korszerű, telepíthető és védett vezetési, kommunikációs és információs képesség). A haderőt modul rendszerűre kell alakítani (alapelem a zászlóalj erő, ennél kisebb harctámogató kötelékkel), a mobil műveleteket kell előtérbe helyezni, illetve a békefenntartást, mint alapfeladatot kell kezelni.

A tapasztaltak alapján megállapítható, hogy a hazánk fontosnak tartja az információk védelmét, de az ezzel kapcsolatos alapelveket nem alapozza meg részletesen ezekben a dokumentumokban.

A doktrínák szintje

Az összhaderőnemi, funkcionális és szakterületi doktrínákban az előbbi szint megállapításait a fegyveres erők működési sajátosságaival tovább kell bővíteni, és arra kell választ adni, hogy a nemzeti és szövetségi műveleteket milyen információvédelmi támogatással lehet megvalósítani.

A Magyar Honvédség Összhaderőnemi Doktrína nem teljes fogalmi letisztultsággal, de tartalmazza az információs műveletek/vezetési hadviselést, amely területen belül az információ biztonságot is megjeleníti. A feladatrendszer célja, összetevői nem a korszerű hadtudomány eredményeit tükrözik, illetve erőteljesen felismerhető a hagyományos, szervezeti hatáskörök mentén történő gondolkodás. Az Összhaderőnemi Vezetési doktrína (amely mint funkcionális doktrína egy szinten lejjebb helyezkedik el a doktrína hierarchiában) zömében csak felsorolásokra támaszkodik, és szakkifejezései, illetve megközelítése nem összehangolt az összhaderőnemi doktrínáival, ami felveti a kérdést: a felülről-lefelé építkező doktrína rendszerben a harmadik szinten ezek alapján milyen szakterületi doktrína fog születni?

A szabályzatok szintje

Ezen a szinten az előzőek részletes kimunkálására van szükség, amely már az összefüggő szakterületek szabályzatok formájában történő rögzítését jelenti. Itt ki kell térni minden olyan kérdésre, amelynek tisztázása szükséges a szakterületet szabályozó törvények, kormányrendeletek, intézkedések és utasítások, valamint az előző két általános alapelveket meghatározó szabályozó szint által meghatározottak betartása érdekében, nemzeti és szövetségi információk tekintetében egyaránt. A szabályzatok megfogalmazzák a katonai szervezetek

számára a vezetés felelősségét és feladatait, a védelmért felelős struktúrát és annak hatáskörét, illetve az összes olyan teendőt, amelyek szükségesek ahhoz, hogy a szervezetek ezen alapokon alakítsák ki és üzemeltessék saját információs rendszerüket.

Az általánosan nem szabályozott kérdések eseti jelleggel intézkedés formájában rendezhetők (de nagy számú intézkedés kiadása egy idő után megköveteli a szabályozókba történő bedolgozást).

A Magyar Honvédségen belül egységes információvédelmi szabályozás jelenleg nem áll rendelkezésre.

Az Általános Titokvédelmi és Ügyviteli Szabályzat az ügyviteli teendőkön túlmenően tartalmaz dokumentum biztonsági-, elektronikus védelmi (beleértve a rejtjelzést is) feladatokat, az objektumokba történő beléptetéssel kapcsolatos rendszabályokat. Az Informatikai Szabályzat foglalkozik a számítástechnikai eszközök védelmének egyes kérdéseivel (beleértve a helyi szintű szabályozás meghatározását is), valamint a különböző híradó szakutasítások is (pl. a rádióforgalmi szakutasítás) tartalmaznak egy-egy kérdés kapcsán védelmi feladatokat.⁴⁵

A szabályzatokra támaszkodva a következő lépcsőben a katonai szervezetek két részre választható helyi szabályozó mechanizmusa következik.

Elsőként az általános megfogalmazású szabályzatok bázisán a szervezet működési sajátosságai szerint meg kell határozni az összes alkalmazott információs művelettel kapcsolatos védelmi feladatokat, az alkalmazott rendszabályokhoz szükséges erőforrásokat, felelősségi köröket.

Ezek a szervezet egészére vonatkozó helyi szabályok dokumentum biztonság területén nemzeti esetben a Titokvédelmi Szabályzat, szövetségi dokumentumok esetében a Biztonsági Szabályzat és az Intézkedési Terv.

Az elektronikus információ biztonság rendszabályait nemzeti esetben Számítástechnikai Titokvédelmi Szabályzat-, szövetségi esetben a rendszereket támogató szervezeti elemek működési rendjét meghatározó Működési Utasítás szabályozza.⁴⁶

⁴⁵ Az elektronikus információvédelemmel foglalkozó szabályzatra az első kísérlet 2003. áprilisában megtörtént, de a feladat az első egyeztetés után megszakadt.

⁴⁶ Az informatikai területre szűkítve az Informatikai Biztonsági Kézikönyv (az ITB 12-es ajánlását idézve) a szervezetek számára *informatikai biztonságpolitika* és *Informatikai Biztonsági Szabályzat* (IBSZ) kialakítását tanácsolja. Amennyiben a szervezet mérete megköveteli, az IBSZ-t technikai okok miatt célszerű kétszintűvé tenni. A felső szinten a szervezet összes szabályozandó kérdését kell rögzíteni, majd ennek alapján a helyi IBSZ már csak az adott helyszíneken szükséges kérdéseket tárgyalja.

Az MSZ ISO/IEC 17799:2002 szabvány az előbbi forráshoz hasonlóan *informatikai biztonsági szabályzatot* javasol a szervezetek számára (ami szervezeti szinten tartalmaz egy biztonság politika és követelményrendszer együttese), majd ennek támogatására megemlíti az informatikai rendszerek részletesebb *biztonsági szabályzatát*.

A helyi, általános szabályozásra kell alapozni a rendszerfüggő szabályozást, amit összetett (vagy magasabb minősítésű adatokat kezelő rendszer) esetében először a szükséges „biztonság követelmények” kialakításával történik, majd annak jóváhagyása esetén az azok megvalósítását célzó „biztonsági utasítás”-t kell kiadni (ez szabályozási rend jelenleg a NATO elektronikus információk védelmére van meghatározva, de ennek a rendszernek bevezetése nemzeti területen is megfontolandó).

Míg a „biztonsági követelmények” a megvalósítás terén mozgásteret hagynak a biztonsági menedzsmentek, addig az „biztonsági utasítás” a védelmi teendők pontos és részletes leírása, ami a rendszerhez történő hozzáférés-, az üzemeltetéssel kapcsolatos feladatok kibontásával a rendszer üzembenntartásáért, biztonságáért felelős személyek és a felhasználók számára határoz meg feladatokat.

A továbbiakban e két rendszerfüggő biztonsági dokumentum fő területeit, feladatait mutatom be, mert gyakorlati tapasztalatom, hogy az üzemeltető szervezeteknek jelentős szabályozási problémái vannak.

A Biztonsági Követelmények

A Biztonsági Követelmények kialakulása egy folyamat eredménye, ahol az életciklus állomások lehető legkorábbi szakaszában az érintett felek között megkezdődik a rendszer létesítésével kapcsolatos feladatrendszer kialakítása, amelybe be kell építeni a biztonsági kérdéseket is.

A biztonság szempontjából lényeges kérdések így egy folyamat részeként a rendszer kifejlődésének ütemében bővülnek, és egyre részletesebbé válnak. A biztonsággal kapcsolatos felelősségeket és feladatokat a szabályozók (szabályozatlan esetben az illetékes nemzeti, vagy szövetséges hatóság állásfoglalásai) alapján, a következő üzemeltetési fázist előkészítve, előrehaladó módon kell kialakítani és az illetékes biztonsági hatóságok elé jóváhagyásra felterjeszteni.

A követelmények kialakításának olyan kockázatfelmérésre és elemzésre, illetve ezen alapuló kockázatkezelési rendszerre kell építkeznie, amely az aktuális helyzetnek megfelelő bemeneti adatokkal szolgál. Amennyiben ez nem így történik, előfordulhat, hogy egy beruházás, kommunikációs rendszer telepítése a minősítési szint szerinti követelményeket nem elégíti ki, és az utolsó pillanatban nem kapja meg a tervezett szintű működési engedélyt.

A Biztonsági Követelmény tehát egy teljes körű, pontos leírása azon biztonsági és együttműködési alapelveknek, amelyeket a rendszer kialakítása és üzemeltetése során az együttműködő feleknek (üzemeltető szervezet, biztonsági menedzsment, nemzeti és szövetségi biztonsági hatóságok) be kell tartani a rendszer rendeltetés szerinti felhasználása érdekében. Végleges formájában a Biztonsági Követelmény bemutatja, hogy mit jelent a rendszer számára a biztonság, annak elérése érdekében kinek, mit kell tenni, milyen hitelesítési és egyéb eljárásokkal (biztonsági jóváhagyás, vagy akkreditáció) lehet az üzemel-

tetési szakaszban a biztonságosnak mondható állapotot elérni és fenntartani (időszakos ellenőrzések és újra akkreditálás). Részletesen meg kell határozni, hogy a Biztonsági Utasításban milyen kérdéseket kell szabályozni, amelyek a következő területek köré csoportosíthatók:

- *A rendszer feladata.* Minden elektronikus információs rendszer valamilyen cél érdekében történő tevékenységet támogat, amelynek meghatározott résztevékenységei, sajátosságai vannak. Nagyon nehéz (illetve elképzelhetetlenül költséges) olyan kommunikációs rendszert tervezni, amely minden körülmények között minden igényt kielégít. A meghatározott tevékenységekhez információs műveletek rendelkeznek, amelyek ismeretében pontos védelmi rendszabályok alakíthatók ki, amelyek csak meghatározott biztonsági környezetben lehetnek hatásosak.
- *A rendszer határolása.* A vezetékelmélet oktatásakor már alapszinten tárgyalt kérdés, hogy mit kell a rendszer környezetének, elemeinek tekinteni, illetve ezek között hol húzódik a határ. Meg kell határozni az üzemeltetési környezet paramétereit, a személyi biztonsági tanúsítványok legalacsonyabb szintjét, a kezelt információk legmagasabb minősítési szintjét, a rendszer biztonsági üzemmódját és a felhasználókra vonatkozó követelményeket. A különböző funkcionális rendszerek használhatnak közös infrastruktúrát (áramellátás, fizikai védelem, technikai személyzet) ami szükségessé teszi a közös erőforrások igénylésének, karbantartásának Biztonsági Utasításban történő szabályozását, biztosítva, hogy semmilyen lényeges terület ne maradjon felelősség nélkül.
- *Felelősség a rendszer biztonságért.* Pontosan meg kell határozni a rendszer biztonságért felelős szervezeten kívüli és szervezeten belüli felelőségeket, a helyi biztonsági menedzsment felépítését (beleértve az összeférhetlenségek meghatározását is), az együttműködés rendjét a különböző hatóságokkal, illetve a különböző hatóságok együttes tevékenységének rendjét a rendszerrel kapcsolatos ügyek rendezése során.
- *A szükséges mértékű védelmi rendszer.* A védelmi rendszert az érvényben lévő szabályozók és a helyi sajátosságok alapján az arra jogosult hatóság által szükségesnek ítélt szigorításokkal, kiegészítésekkel integráltan kell kialakítani az általános alkalmazási területeken (fizikai-, személyi-, dokumentum- és elektronikus információ biztonság). Rögzíteni kell a biztonságot veszélyeztető eseményekről szóló tájékoztatás rendjét és követelményeit, valamint a kivizsgálás eljárási rendjét. Meg kell határozni, hogy a biztonsági követelmények alapján

kinek, milyen határidőre milyen tartalmú (rendszer) Biztonsági Utasítást kell elkészítenie, jóváhagyatnia, és időszakonként felülvizsgálnia.

- *A konfiguráció felügyelete.* A jóváhagyott rendszernek (és annak elemeinek) az illetékes hatóságok és a helyi menedzsment által folyamatosan felügyeltnek kell lennie. A korszerűsítés, rendszer kiterjesztése, vagy meghibásodás miatt bekövetkező változásokat, a tervezett és soron kívül szükségessé vált karbantartási, javítási feladatokat *jellegük, mértékük és jelentőségük* szerinti engedélyeztetési mechanizmusnak kell alávetni, végrehajtásukat – ha szükséges – egyedi eljárásokkal kell felügyelni, illetve a végrehajtás után az összes dokumentációban át kell vezetni a változtatásokat. Fontos feladat annak meghatározása, hogy melyek azok a rendszerben történő változtatások (funkciók, szolgáltatások, eszközök, szoftverek stb.), amelyek újraakkreditálást váltanak ki, vagy az illetékes hatóság előzetes jóváhagyását igénylik.
- *A vészhelyzeti és folytonossági tevékenység.* A védelmi rendszer a kockázatfelmérés, és értékelés alapján reálisnak tekintett külső és belső, szándékos vagy véletlen események hatásainak csökkentésére/elkerülésére szolgál. Ezen eseménytípuson kívüli helyzetekre a helyi sajátosságoknak megfelelő, a szükséges mértékig részletesen megtervezett és begyakorlott tevékenységre van szükség, amelyet az érintett személyek minden körülmények között képesek végrehajtani (pl. szabadságok idején, vagy téli időszakban) az illetéktelen megismerés, vagy egyéb formájú kihasználás elkerülése érdekében. Az adott munkahely sajátosságainak (kezelt eszközök, anyagok mennyisége, jellege, minősítése, rendelkezésre álló személyek száma, a környezet stb.) megfelelően meg kell határozni, hogy az illetéktelen megismerés megakadályozása milyen feladatrendszerrel oldható meg. Az erőforrások és a rendelkezésre álló idő figyelembe vételével három lehetséges megoldás közül lehet választani: a *védelmi rendszabályok megerősítése*, a minősített anyagok *biztonságos helyre történő szállítása* (mert van elég idő, szállítási kapacitás és biztonságos útvonal); vagy a *vétségmegsemmisítés* (mert nincs lehetőség az elszállításra).⁴⁷ A *folytonossági tervezés* (continuity planning; régebben contingency planning) feladata, hogy a szervezetnél az információs rendszerek működését negatívan befolyásoló katasztrófa (vagy egyéb kényszerítő hatás) elmúlása esetén vezérelje a normálisnak tekinthető információs szolgáltatások visszaállítását. Ehhez bemenő adatként meg kell határozni, hogy a szervezet vezetéséhez és a működéshez milyen minimális szolgáltatásokra van szükség. Ezután tervezhető a helyreállítás,

⁴⁷ A három megoldás kombinált alkalmazása is lehetséges.

amely támaszkodhat tartalék eszközökre, összeköttetésekre (pl. tartalék rejtjelző eszköz, kulcs, bélelt áramkör), helyi, vagy központi helyreállítási képességekre.

- *A Biztonsági Utasítás felülvizsgálatának, továbbfejlesztésének rendje.*
A rendszer környezetének változásai, az információkezelő rendszerek elleni támadási technikák fejlődése, a jogszabályok változtatása, vagy a védelmi rendszabályok esetleges elégtelensége megköveteli, hogy az utasítás időszakos felülvizsgálat alá essen és megtörténjenek a szükséges korrekciók. A felülvizsgálat rendjét, illetve a környezeti és egyéb változások figyelemmel kísérését időpontokhoz, felelősökhöz kell kötni és megfelelő ellenőrzési mechanizmus kialakításával meg kell követelni ennek a rendszernek a működését is.

A rendszer életciklusához kötötten meg kell határozni a Biztonsági Követelmények kialakításának, továbbfejlesztésének, változtatásának követelményeit, valamint azt, hogy a követelmények teljesítése érdekében milyen további szabályozó mechanizmus (szabályozók, utasítások stb.) határozzák meg a szükséges feladatokat és kik (milyen szervezet, vagy szervezetek) felelősek annak elkészítéséért.

A fentiek alapján jól felismerhető, hogy a szabályozási szint csökkenésével csoportosulnak, egyre részletesebbé válnak és a rendelkezésre álló technológiához igazodnak a biztonság érdekében hozott intézkedések. E tendencia hatása, hogy a szabályozási hierarchia alsó szintjein esetenként minősített szabályzatokra és szakutasításokra is szükség van, míg felső szinten még a rejtjelzésről is nyilvánosan megismerhető dokumentumok rendelkeznek.

A szabályozási rendszer elemei nem örök érvényűek. Minden szinten be kell építeni egy olyan mechanizmust, amely időről-időre, egy előre meghatározott rend szerint biztosítja az alapokat nyújtó tényezők felülvizsgálatát és szükség szerinti aktualizálását. Nem szabad tehát egy Magyar Honvédség szintű szabályzatban szervezeteket, beosztásokat megnevezni, illetve törvényekre és jogszabályokra szám szerint hivatkozni. Ugyanígy felesleges a törvények, kormányrendeletek szövegrészeinek, vagy fogalmainak szabályzatokban, szakutasításokban történő idézése, vagy ismétlése.

A szabályzatok által meghatározott képességeket biztosító szervezetek megnevezése, felelősségi körének és egyéb fontos tényezők meghatározása olyan intézkedésben (szakintézkedésben) szükséges, amelyek a szervezetek, esetleg feladatokból adódó változások esetén rugalmasan és gyorsan változtathatók.

A szabályzatoknak azt a területet kell szabályoznia, amire a hatáskör hivatalosan kiterjed, mert a szabályozásért felelős szervezetek munkarendje, a dokumentumok kiegészítései, felülvizsgálatai szakterületenként eltérő gyakoriságú lehet. Amennyiben a szervezetek egymás szabályzataiba helyeznek el rend-

szabályokat, feladatokat, azok aktualitásának figyelemmel kísérése egy idő után akadozhat, esetleg előfordulhatnak ismétlődések, illetve régi és új rendszabályok egyidejű szerepeltetése. Az információvédelem területén erre a legjobb példa a Titokvédelmi és Ügyviteli Szabályzatban a rejtjelzés, a számítástechnikai védelem, a megtévesztés feladatainak szerepeltetése.

További fontos feladat, hogy a szabályzatok - mintegy szabályozási infrastruktúraként - biztosítsák a rendszerfüggő szabályozáshoz szükséges háttérrel.

Összegzésként elmondható, hogy a NATO szövetségi doktrínától kezdve egy helyi szintű utasításig bezárólag csak akkor építhető fel logikus, ismétlődésektől és ellentmondásoktól mentes szabályozó rendszer, ha az összetartozó szakterületek saját rendszabályaikat és a más területekhez történő kapcsolódási pontokat feltérképezik, és szabályozórendszerüket tudatosan, előrelátóan alakítják ki. Ebben az esetben a jogszabályok módosulása, vagy a helyi biztonsági környezet egyes elemeinek változása esetén pontosan meghatározható a szabályozás azon szintje, ahol a szükséges átalakításokat meg kell tenni.

A szabályozás természetesen azonnal felveti a szervezeti elemek felelősségének kérdését, így kimondható, hogy az elmondottak csak akkor érvényesülhetnek, ha a megfelelő szervezeti keretek kialakítottak és működőképesek.

Felhasznált irodalom:

- 2144/2002. (V. 6.) Kormányhatározat a Magyar Köztársaság nemzeti biztonsági stratégiájáról
- 52/2002. (III. 26.) Kormányrendelet a Nemzeti biztonsági Felügyelet részletes feladatairól és működési rendjéről, valamint az iparbiztonsági ellenőrzések részletes szabályozásáról
- 56/1999. (IV. 2.) Korm. r. a nemzeti szerződés alapján átvett, vagy nemzetközi kötelezettségvállalás alapján készült minősített, valamint korlátozottan megismerhető adat védelmének eljárási szabályairól
- 94/1998. (XII. 29.) OGY határozat a Magyar Köztársaság biztonság-, és védelempolitikájának alapelveiről
- Informatikai Biztonsági Kézikönyv
- ITB 12-es ajánlás
- Király Imre: A helyi Titokvédelmi Szabályzat rendeltetése, elkészítésének tartalmi követelményei; ÚHSZ 2002/9
- MSZ ISO/IEC 17799:2002
- Tóth Ferdinánd: A doktrinális kiadványokról; ÚHSZ 2002/7
- Úton a XXI. század hadserege felé (védelmi felülvizsgálat 2003)

MODERN KATONAI TELEFONOK



IP-1000

Voice over IP USB Phone IP-1000

Features & Benefits:

- High Mobility
- USB Interface, just plug and play. No drive needed.
- Provided real-time volume adjustable button
- Can be mounted on your monitor or wall
- Microsoft Windows 98se/ME/2000/XP Operation System
- Provided H.323/SIP Internet telephony function by different Softphone software providers

- Free download keypad program from Web for different Softphone software using such as NetMeeting, Hicall ...etc.
- Free PC-to-PC calls over the Internet
- Provided API for Softphone software developer



September 29, 2003

PERYPHON
TELECOM ELECTRONIC INDUSTRY LTD

www.peryphon.co.il

10 Hamelacha St., block 209, New Industrial Park, Rosh-Ha'ayin 46061, Israel. P.O. Box 13204, Tel-Aviv. Fax: (972)3-9025684. Tel: (972)3-9025682. E-mail: sale@peryphon.co.il



PERYPHON is for more than a decade, a designer, promoter and manufacturer of the most modern and sophisticated telecommunications equipment and accessories. PERYPHON designs all its own products. Our greatest speciality is design of military telephones and other military products.

PERYPHON exports its products to Europe, South America, the Far East and Africa and supplies also to the Israeli PTT and Army Signal Corps. Due to its advanced technology and its knowledge and experience in the military and payphones fields, PERYPHON competes favorably with most manufacturers in the market.

PERYPHON manufactures its products with strict accordance to ISO 9002 and MIL standards.

PERYPHON operates a high level of quality control and designs its products with the highest level of technology on the market. All of products can be adapted or modified according to the demands of the customer.

***MILITARY LOUDSPEAKERS & HANDEST**

PERYPHON manufactures a large variety of different military products using the latest technology according to the request of different army signal corps worldwide. These include military field and military magneto telephones, military loudspeakers for different VRC models, various satellite telephones, military handsets and communication cables.

***MILITARY PHONES, P.O.S.T PHONS, IP-PHONES, PAYPHONES**

PERYPHON manufactures a large variety of telephones both for home use and for heavy-duty use & for military.



September 29, 2003



Combat Telephone

September 29, 2003

Military Telephones & Loudspeakers



TA-1088TP

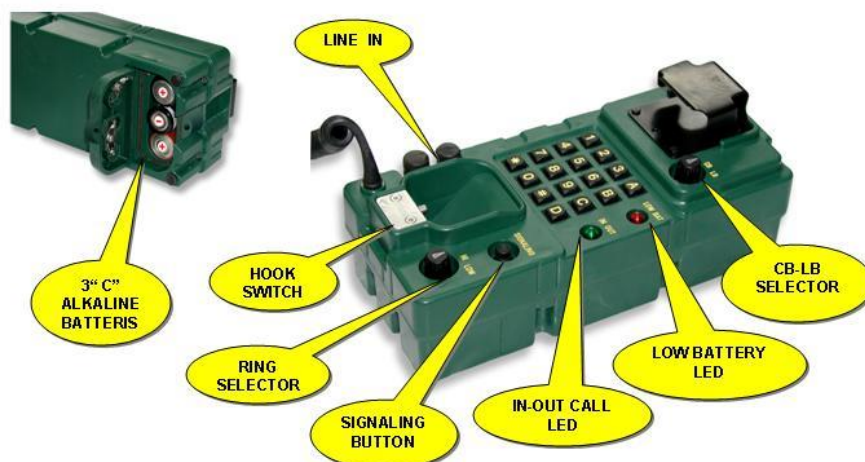
The TA-1088/TP Combat Telephone is a neatly styled lightweight. 2-wire local battery and central battery telephone, 16 buttons DTMF/PULSE dialing on CB. Technical Characteristics:

Voltage requirements :
LB 3.3 to 4.5 V dc, CB 24-60 V line, 20 to 60 mA.
Frequency range: 300-3400 Hz.
Signaling Electronic Generator:
25 or 50 Hz 45 to 80 V RMS 3W.
Station-to-Station range: using wire WD-1/TT
(loop resistance is 46 ohm per 1000 feet)
at distances of over 79 km performance is reduced.

Warning LED for "Low Battery".
LED Indicator, holding ring for 20 seconds, and outgoing warning ring.
Push button Electronic Signaling Generator.
DTMF/PULSE dialing with Redial and Flash button.
Piezo Ringer, adjustable.
Handset: H-189 with PTT switch.
Weight: Approx. 1.7 Kg excluding batteries.
Size: 240 x 95 x 110 mm.
Operation temp. -30 to +60 C.
Operates with AN/TTC 25, 38, 39 and SB-3614 switches Center.
Ring back LED.
4.5 V from standard "C" size cells



September 29, 2003



September 29, 2003

OPERATING FACILITIES:

Standard facilities include:

Magneto signalling by momentary switch operation (RING) ;

Audible / visual call indication; handset PTT switch, which enables the microphone. Warning Led for "Low Battery", Led for holding ring for 20 sec., and outgoing warning ring, Led for Ring Back.

Facilities include: Push button dial pad for loop disconnection or DTMF signalling. Two second timer for magneto ringer (battery saver). Last number re-dial, and two extra signalling Buttons (Flash) – (OPTIONAL).

COMPATIBLE EQUIPMENT:

The TA-1088/PT Tactical Field Telephone is compatible with all common types of magneto and central/battery switchboards including:

- RA2135 Auto Field switchboard
- SB130/GY Auto Field Switchboard
- SB3614 (V) TT Auto Field Switchboard
- 22A100 Series Eleven-Line Switchboard
- RA525 System Matel
- RA2100 Magneto Field Switchboard
- SB22 Series Magneto Field Switchboard.

September 29, 2003



TA-1088TP

ENVIRONMENTAL:

Dimensions

H – 120mm. W – 110mm. L – 240mm.

Weight not more than 1.7 Kg. $\pm 10\%$ Without Batteries.

Operating temperature:

-30C +60C

Storage Temperature:

-51C +71C

Immersion:

1m. for 2 hours

Vibration: 5 to 500Hz at 1.5g for 10 hours

Drop: 1.2 m. to concrete

General

The TA-1088/PT Combat Field Telephone will also pass the relevant MIL-STD-810E test for resistance to salt, fog, solar radiation, humidity, icing/freezing rain, pressure and shock.

September 29, 2003



TA-1088TP

ENVIRONMENTAL TEST RESULTS			
BUZZER ACOUSTIC LEVEL	MEASURED AT 1 METER FROM TELEPHONE WITH 35 VRMS 20Hz INCOMING CALL	70 dB SPL	75 dB SPL
SIDETONE	MINIMUM ATTENUATION AT 1000 Hz AND 600 OHM LOAD	13 db	18 db
RADIO FREQUENCY INTERFERENCE PROTECTION	MIL-STD-461		SATISFIED
HUMIDITY	MIL-STD-810-E		SATISFIED
ALTITUDE	MIL-STD-810-E		SATISFIED
LEAKAGE	3 FEET DEPTH FOR 60 MINUTES		SATISFIED
VIBRATION, BOUNCE AND SHOCK	MIL-STD-810-E		SATISFIED
SALT FOG	MIL-STD-810-E		SATISFIED
DUST	MIL-STD-810-E		SATISFIED

September 29, 2003

TA-1076P

TA-1076- P CB- LB "MAGNETO" Telephone Analyzer, multi- function and powerful performance analyzer either in PULSE or DTMF type , both auto swappable. The entire test Q.C. Limit Parameters can be set up by User and Indicated the by GO/ NO GO result quickly.

FEATURES:

1. Tone/Pulse Auto-Swap Testing
2. DTMF Testing
3. PULSE Test
4. Dial Testing
5. DTMF Distortion Test /Set
6. DTMF High/Low Group Level (dB) Rating Test /Set
7. High/Low Group Twist Test
8. H.F and L.F Mixed Signal Level Test
9. P.P.S Test (Pulse test)
10. Loop Current Test
11. 4 Groups of Bell Frequency Set
12. Dialing Total Number and Sequential Length Programmable
13. Transmit/Receive Test
14. Arti. Line Simulation
15. Sound Issuing Test
16. Flash Test
17. SIGNALING Test to distance 0-5 km.



Finally, the most outstanding feature of the TA- 1076- P MAGNETO Telephone Analyzer is its reliability, the equipment you have received has undergone rigorous and stringent tests to ensure you operate the equipment without any trouble

September 29, 2003

TA-1088TP

Transmit / Receive Test



Transmit / Receive Test



September 29, 2003

Immersion test method 512



Drop test method 516



Drop test method 516



September 29, 2003



September 29, 2003



TA-1089A

The TA-1089A Satellite Combat Telephone. Light weight.
Dialing on Satellite Network (IRIDIUM)

Technical Characteristics:

Voltage requirements:
3.3 to 4.5 V DC. from standard " C" size cells.
Frequency range: 1616 MHz, L-Band.
Signaling Electronic Generator:
01505 MOTOROLA Mobile Phone on CB.
Station-to-Station range:
All over the World.
Operates with:
IRIDIUM TDMA/ FDMA World Wide.
DTMF dialing with Redial & Flash Button.
Warning LED for "Low Battery".
Ring back LED, holding ring for 20 seconds, and outgoing warning ring.
Piezo Ringer, adjustable.
Handset: H-1189 with PTT switch.
Weight: Approx. 1.8 Kg excluding batteries.
Size: 290 x 95 x 140 mm.
Operation temp. -30 to +60 C.



September 29, 2003



TA-2088

FIELD ELECTRONIC MAGNETO TELEPHONE TA-2088 " MAGNETO-2000"

This indoor magneto telephone is specially designed for communication between two line points.
Manufactured with much strictness, to ensure many years of efficient and credible service.

Enables to call the second party without being related to the public telephone line, specially in cases where the public telephone exchanges are out of order, or the lines are busy, and there is an urgent need to call the second party.
Each phone can be connected in parallel to more than one set, and can also be connected to any telephone exchange for connection to the outside line.

This magneto telephone has an electronic ringer generator which replaces the old fashioned mechanical one .
The call to the second party is made by pushing a button, with a red LED indicatings the call is being made.
The magneto telephone is operated by two LR-"D" Alkaline batteries.



September 29, 2003

LS-108

Loudspeaker LS-108 is a two inch direct radiator, dynamic, permanent magnet type loudspeaker built in an armed housing, resistant to weather, water immersion, humidity, temperature extremes and bounce. It is intended for use with ground, airborne and seaborne service. Tactical equipment is mobile or fixed field communications equipment.

Characteristics :

Frequency Range :300 Hz-7000 Hz.

Power Rating :2 Watts RMS (nominal) and 4 Watts RMS to peak.

Input level : The input level for the following requirements is 3.15 V RMS.

Impedance : The input impedance of the LS-108 is between 40 and 54 Ohms.

Attenuation : The LS-108 output is attenuated at no less than 30 dB when using the volume control.

Temperature : -30 to +70 C

Dimensions : L = 110 mm; B = 62 mm; H = 32 mm.

Net weight : 0.280 kg.



September 29, 2003

LS-208

The LS-208 is a Military mobile cellular communication holder providing hands free functionality

with maintained sound quality for tactical vehicles. This is a hands free unit which reduces noise and echo that transmitters usually distribute. It also contains a Mil Handset H-189 to enable private conversation, not through the speaker. When not in use, handset is fully mounted and firmly held onto holder. This holder enables both an external connection to a Mil microphone through U-229 connector, and serial port through 9-pin Mil connector. The LS-208 can be mounted to any tactical vehicle and is protected against vibrations and RFI interference. It is housed in a dye-cast metal enclosure and is resistant to weather, water immersion, humidity, temperature extremes, vibrations and bounce. It is intended for use with ground, airborne and seaborne service.

Characteristics:

Frequency Range:

300 Hz-3500 Hz.

Power Rating:

5 Watts RMS (nominal)

and 8 Watts RMS to peak.

Temperature operation:

-30 to +70 C

Dimensions:

240mm x 140mm x 60mm

Net weight:

About 2 Kg.



September 29, 2003



MK-25

Military loudspeaker MK-25 is a 3 inch direct radiator, dynamic, permanent magnet type loudspeaker housed in a die cast enclosure and is resistant to weather, water immersion, humidity, temperature extremes and bounce. It is intended for use with ground, airborne and seaborne service. Tactical equipment is mobile or fixed field communications equipment.

Characteristics :

Supply DC: 10.5 - 12.5 V , 170 mA.
Frequency Range : 300 Hz - 3500 Hz.
Power Rating : 1 Watts RMS (nominal).
Input level : The input level for the following requirements is 0.05 - 3 V RMS.
Impedance : The input impedance of the MK-25 is between 8000 Ohms.
Temperature : -30 to + 70 C.
Dimensions : 118 mm x 73 mm x 110 mm.
Net weight : About 0.5 kg.



September 29, 2003



H-207/VRC

The H- 207/VRC Handset is designed for use with the AN-VBIC-1 vehicular intercom system.

Connected with the C-2296/VRC Control Box on the outside of the vehicle, the user of the H-207/VRC is permitted to communicate on radios connected to the AN/MC-1 inside the vehicle and to also communicate on the intercom circuit with vehicle crewmembers.

The handset features a push-to-talk switch for both transmission and a ground to light the external lamp on the C-2297/VRC Control Box to attract the attention of vehicle crewmembers and a 25 foot retractile cable assembly



September 29, 2003

IP- Telephone

September 29, 2003

AG-399

Peryphon's AG-399 Smart Phone contains many timesaving and advanced features including: * FSK compatible caller ID/Call waiting ID

- * Large Display Screen with Backlight
- * English Display
- * New Call/Ringing/Line in Use/New Message Indication
- * 8 Speed-dialing keys with direct dialing
- * Display name, number, date, time and sequence for new and waiting call
- * Store and display up to 50 name and telephone numbers
- * Call Log up to 50 incoming and outgoing calls
- * Separate ringing tones for special needs
- * Programmable DND
- * Indication and displayed list for not answered calls
- * Hands-free listening for voice messages
- * Speakerphone with Mute and Hold
- * Redial and Predial- prestore and editing phone number before dialing
- * Call duration display
- * Clock and calendar display
- * Displayed name and number for local customer in the On-Hook
- * Fixed feature keys for operation management



September 29, 2003

LAN Phone IP-101 is a full-featured IP-based telephone set for office telephony via Ethernet base communication. Over the office LAN connection, it provides IP-PBX solution such as station-to-station call, IP call and local PSTN/PBX extension call via PSTN Gateway.

The traditional PBX functionality is provided with H.450 features together with Gatekeeper or IP/PBX Call Manager. Two 10/100BaseT embedded switch/hub RJ-45 ports allow connect to office LAN and PC on your table. It is easily interface with ADSL/Cable Modem that is provided by ITSP, ISP or carrier company to provide VoIP services to residential and SOHO application. An integrated Analog Phone features provides IP call or PSTN call selection.

Or to be a Plain Old Telephone set (POTs) when external power is failure. It provides programmable keys and feature buttons, an internal high-quality speakerphone with microphone mute, HOLD function, FORWARD and TRANSFER feature buttons. The LAN Phone 101 also provides a dot matrix of two lines 24 characters LCD display each. The display provides features such as date and time, calling party name, calling party number, and digits dialed. An LED associated with each feature and line buttons provides feature and line status.

TELNET and LCD front panel provide local and remote configuration, Management and software download. By using this feature, ITSP/ISP provides centralized control, management and software upgraded remotely. Several examples are listed below: IP/Gatekeeper addressing setting, dial plan, voice coder, Gatekeeper and Peer to Peer mode selection, QoS and call progress tone setting.



September 29, 2003

ÚTVONAL OPTIMALIZÁLÁS ÉS SZEREPE A TŰZOLTÓSÁG MUNKÁJÁBAN.

Tűz, vagy káresetek elhárításának egyik igen fontos eleme a megközelítési útvonal meghatározása, azé az útvonalé, amelyiken a legrövidebb idő alatt lehet a kárhelyet megközelíteni. Nem biztos, hogy az úton méterben, kilométerben mért távolság a mérvadó, hiszen a vonulást számtalan tényező befolyásolja:

- Az útvonalon elérhető általában elérhető átlagsebesség (burkolat minősége meghatározza az elérhető átlagos sebességet),
- Az igénybevett utak szélessége,
- Kanyarodási sugár,
- Forgalom sűrűség, stb.

Megkülönböztető jelzést használó jármű a közúti jelzések jelentős részét figyelmen kívül hagyhatják (megengedett legnagyobb sebesség, egyirányú utca, járműforgalom elől elzárt terület, stb.) de a fizikai akadályok sajnos szűk korlátokat jelentenek. Olyan útvonalat célszerű választani, amely a legkisebb kockázatot jelenthet a kárhelyre igyekvő jármű akadálytalan továbbhaladása szempontjából.

Minden tényező figyelembevétele szinte lehetetlen vállalkozást jelent, hiszen pl. a forgalmi viszonyok dinamikusan változnak, a pillanatnyi út-optimum alkalmazása idővesztéssel is okozhat, tehát még azt is figyelembe kell venni, hogy mindig a kívánt cél felé haladjunk.

A sok, és dinamikus változót is tartalmazó probléma megoldását egy tűzoltóság nem tűzheti ki célként, hiszen nem ez a feladata. Az esetek döntő többségében pedig már az is célravezető, ha a fizikai akadályoktól mentes (útfelbontás, útelzárás) útvonalat meghatározzuk, figyelembe véve az útburkolat minőségét. A kidolgozás időszakában ez annál is indokoltabb volt, mivel a városban a szennyvízvezeték fektetése következtében időről-időre, új helyen képződött az utak mellett akadály.

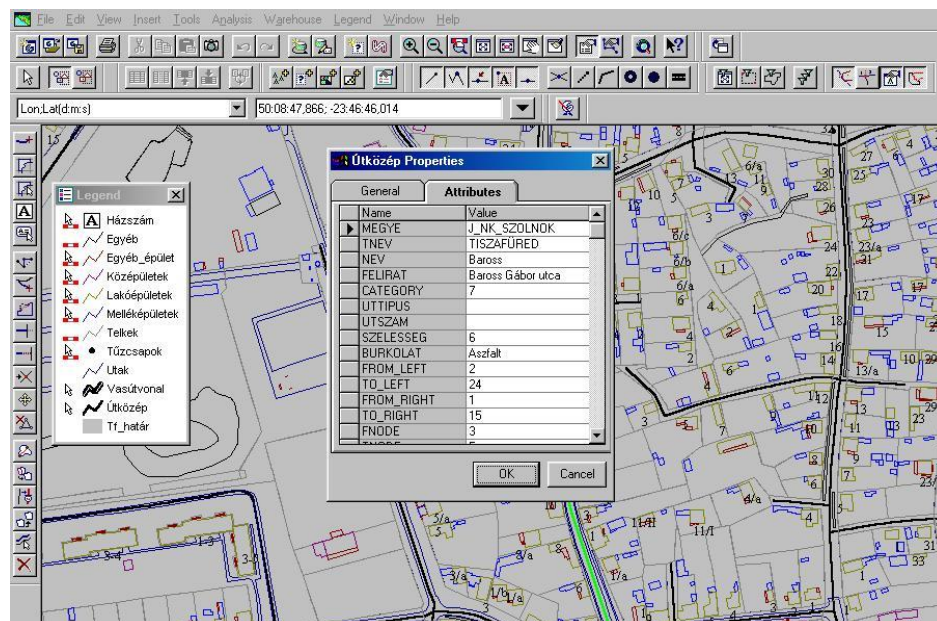
A feladat megoldásához a térinformatika eszközeit hívtuk segítségül, ami segít abban is, hogy a kárhely statikus környezetéről (építmények elhelyezkedése, vízszervezési helyek, útvonalak, stb.) információt kapjunk. A megoldás kidolgozásában nagy segítségünkre volt a GRAFIT KFT, ezúton is köszönjük munkájukat.

Az, hogy mintaterületként Tiszafüred városát választottuk, gondolom egyértelmű. Rendelkezésünkre állt a város 1:1000 léptékű digitális térképe, az adatfeltöltést mi végeztük. Olyan adatokat rendeltünk az épületekhez, útvonalakhoz, oltóvíz vételezési helyekhez, melyek több irányú elemzést tesznek

lehetővé, biztosítva a komplex hasznosítást, a GeoMedia térinformatikai alkalmazással.

Maradjunk csak az optimális útvonal meghatározásánál.

Az útvonal meghatározását a város útjainak képzeletbeli középvonalán végezzük, ami megközelítően pontos távolságmérést is lehetővé tesz. A képzeletbeli útközéphez az alábbi adatokat rendeltük:

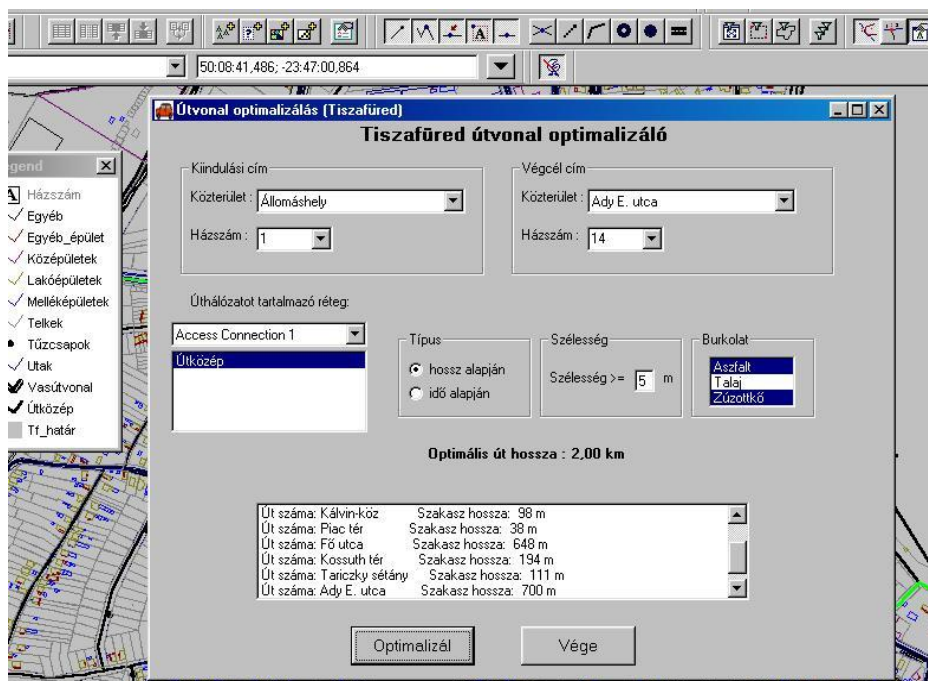


A város térképe, útdattal

- Utcanév,
- Kategória (átmenő főút, gyűjtőút, egyéb szilárd út, szilárd útalap, talajút),
- Szélesség,
- Burkolat minősége,
- Az utcában található kezdő és végső páros oldali házszám,
- Az utcában található kezdő és végső páratlan oldali házszám.

Az optimális útvonal meghatározásához a fenti adatok szükségesek, mely lehetővé teszi a város tetszés szerinti pontjáról, bármely részének időben, vagy távolságban mért legrövidebb idejű útvonalának meghatározását.

A kezelés (útvonalelemzés) az alábbi felülettel történik.



Az útvonal tulajdonságok (alapvetően a szélesség) adatbázisban történő változtatásával és az optimalizáláskor az aktuális szélességi paraméter beállításával, az igénybe vehető útburkolat megadásával, minden időben az optimális (olykor egyáltalán járható, legrövidebb) útvonal megtalálható.

A MAGYAR HONVÉDSÉG HÍRRENDSZERÉNEK JELENE... ÉS JÖVŐJE?

Bevezetés

A Magyar Honvédség híradás-szervezési elveinek megfelelően a következőképpen fogalmazhatjuk meg a hírendszer fogalmát: a hírendszer a csapatvezetési és fegyverirányítási rendszerek alapvető alkotórésze, mely egységes terv alapján; hely, idő szerint összekapcsolt és illesztett különböző rendeltetésű hírközpontok és híradó vonalak összessége. Természetesen ide kell értenünk az ezeket az eszközöket üzemeltető személyi állományt is. A hírendszer elemei a következők:

- vezetési pont hírközpontok;
- közvetlen összeköttetések híradó vonalai;
- alaphírhálózatok;
- híradás vezetési rendszere;
- futár- és tábori posta híradás;
- híradás logisztikai rendszere;
- híradó tartalék;

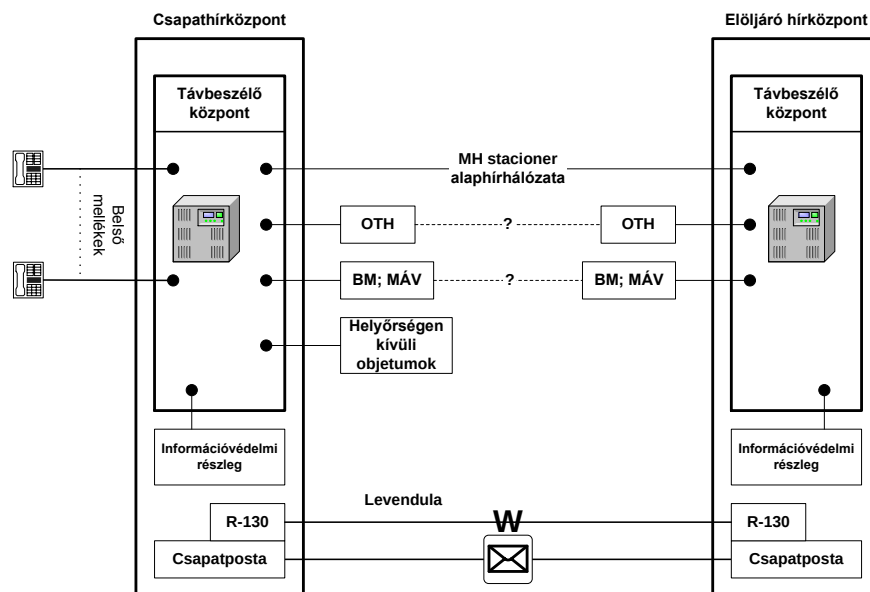
A következőkben az elemeket részleteiben is ismertetve rá szeretnék világítani a jelenleg üzemelő hírendszer elavultságára. Vagy a kor színvonalán állónak? Néhány szóban szeretnék arról a koncepcióról is szólni, amelynek végleges megvalósítása 2013-ra várható – természetesen kiegészítve az én véleményemmel is.

Vezetési pont hírközpontok

A jelenlegi vezetési rendszernek megfelelően a Magyar Honvédség (továbbiakban MH) katonai szervezetei mind békében, mind minősített esetben; mind békehelyőrségeikben, mind tábori körülmények között kötelesek vezetési pontjaikat üzemeltetni. Ezen szervezetek, illetve alárendeltjeinek vezetéséhez valamilyen szintű hírközpont szükséges, amely biztosítja az információk végződtetését és továbbítását.

Csathírközpontok

A csathírközpontok a katonai szervezetek békehelyőrségeiben települnek. Biztosítják a híradást az előjáróval, az alárendeltekkel, az együttműködőkkel, illetve a helyőrségen (laktanyán) belül. A következő ábrán egy csathírközpont elvi felépítését láthatjuk.



1. ábra: egy csathírközpont elvi felépítése

forrás: saját

Az ábrán láthatjuk, hogy egy csathírközpontnak milyen összeköttetésekkel kell rendelkeznie a folyamatos vezetés biztosítása érdekében:

- Magyar Honvédség stacioner hírhálózata; a későbbiekben ejtek róla szót;
- OTH: Országos Távközlő Hálózat; magába foglalja az összes közcélú szolgáltatót; részleteiben később;
- BM, MÁV: természetesen nemcsak a Magyar Honvédség üzemeltet saját zártcélú hálózatot, melyeket az együttműködés miatt több ponton összekapcsolnak. Az átjárás lehetősége általában nem automatikus, hanem egy „kezelő” közbeiktatásával történik;
- Információvédelmi részleg: feladata bizonyos közlemények információtartalmának rejtése, mellyel megakadályozza, hogy az illetéktelen előtt megismerhetetlen maradjon. Technikai eszközei a távbeszélő központok mellékeit használják (titkosító FAX). Néhány katonai szervezetnél még alkalmazhatnak géptáviró titkosítókat is.
- A helyőrségen kívüli objektumokkal (lehet például lőtér, gyakorlópálya, rádióadó pont, stb) való összeköttetés lehet saját tulajdonú vagy bérelt is. A mi szempontunkból az a fontos, hogy legyen összeköttetés!
- „Levendula”; Ez tulajdonképpen egy RH rádióforgalmi rendszer, ami azt a célt szolgálja, hogy ha egy katonai szervezetnek minden összeköttetése megszakad az előljáróval, akkor ezt a rendszert aktivizálva

álljon rendelkezésre egy csatorna, amelyen keresztül nem marad vezetés nélkül a katonai szervezet. Ez azt feltételezi, hogy az előjárónál állandó jelleggel vételkészen üzemel egy rádiókészülék, míg a katonai szervezetnél pedig elő van készítve!

- Csapatposta: Ez a nagyon kis szervezet biztosítja a katonai szervezet részére a hagyományos „postai” úton történő információtovábbítást.

Napjainkban az üzemeltetett berendezések nagy része már korszerűnek mondható digitális kapcsolóközpont (Siemens HICOM 300-as család), de sajnos egynéhány katonai szervezetnél még mindig a régi tárolt programvezérlésű berendezések (EPF család F-esített változatai) üzemelnek.

Tábori vezetési pont hírközpontok

Többféle tábori vezetési pont hírközpont létezik, attól függően, hogy milyen szintű katonai szervezet vezetését, irányítását végzik. A legkisebb a zászlóaljak vezetési pont hírközpontja (z. FIH HK), amely egy kis vonalkapacitású távbeszélő központból, a hozzá tartozó belső vezetékes hálózathoz (néhány km vezeték) és néhány páncélozott vezetési eszközökből (z. pk.-i, z. TÖF-i harcjármű, illetve harckocsi; annyiban különböznek, hogy több rádióeszköz van beépítve), illetve mobil rádióállomásból áll.

A következő szinten a dandár vezetési pont hírközpontjai állnak (dd. FH HK – Fő Harcálláspont Hírközpont, MH HK – Mögöttes Harcálláspont Hírközpont, EH HK – Előretolt Harcálláspont Hírközpont), melyeket a dandár híradó százada telepít. Felépítésüket tekintve a hírközpont a FH és a MH jól elkülöníthető, önálló része, melynek központi helyét egy maximum 40 melléket biztosító távbeszélő központ foglalja el. Itt már találhatunk olyan eszközt, amellyel a dd. képes felcsatlakozni a tábori alaphírhálózathoz (R-1406 állomás). Mindezekon kívül természetesen megtalálhatóak a páncélozott vezetési eszközök és rádióállomások is. Ki kell emelnünk, hogy a FH HK és a MH HK felépítése teljesen azonos, hiszen csak így módon képes biztosítani a vezetés átvételének feltételeit. Abban az esetben, ha a dd. parancsnoka közvetlen ráhatást akar gyakorolni alárendeltjei tevékenységére, akkor települ a dandár EH HK-ja (nem rendelkezik önálló szervezettel, a feladat függvényében rendeli el a parancsnok, hogy ki fog itt dolgozni), mely maximálisan 2-3 - a főharcálláspontból kikülönített - páncélozott vezetési eszközökből áll.

A következő szintű a gépesített hadtest FH HK, MH HK, EH HK. Ezeket a vezetési pont hírközpontokat a 43. Nagysándor József híradó zászlóalj telepíti. A hírközpontok felépítését tekintve hasonló a dandáréhoz, de az itt alkalmazott eszközök kapacitása alkalmazkodik a hírközponton áthaladó és végződött információk mennyiségéhez, illetve az ezeket felhasználó személyek számához.

A jelenleg rendszerben lévő eszközök miatt a vezetési pontok mobilitása (a gépjárművek és a híradó eszközök üzemképtelensége, a híradóállomá-

sok és azok antenna rendszereinek hosszú, nehézkes telepítési ideje) és információátersztő képessége (eszközök elavultak) rendkívül korlátozott, ezért a parancsnokoknak figyelembe kell vennie a vezetési pontok telepítési idejét a feladatok végrehajtása során.

Közvetlen összeköttetések híradó vonalai

A közvetlen összeköttetések híradó vonalai alatt azokat értjük, amelyek közvetlenül összekötik az előljáró és az alárendelt vezetési pont hírközpontjait, a tábori alaphírhálózat alaphírközpontjait, illetve a tábori alaphírhálózatot a stacioner (stratégiai) alaphírhálózzal vagy az Országos Távközlő Hálózzal.

Ezek a következők lehetnek:

- ✚ Rádió vonalak; általában közepes és nagy teljesítményű rádióállomásokkal alkalmaznak;
- ✚ Vezetékes vonalak; vagy bérelt, vagy saját tulajdonú (vagy tábori), amelyekre jellemző az egyre nagyobb az átviteli sávszélesség (ez inkább az új építésű sajáttulajdonú és az összes bérelt áramkörre vonatkozik);
- ✚ Rádiórelé vonalak; nagy csatornaszám, vagy nagy átviteli sávszélesség (a frekvenciamigráció keretében történt fejlesztés eredménye képpen $n \times 2$ Mbps sávszélességű átviteli utakról beszélnek);
- ✚ Troposzféra vonalak; jelenleg a MH-ben nincs rendszeresítve eszköz, de érdekes, hogy a NATO más tagországaiban ismét az érdeklődés előterébe került;
- ✚ Futár- és tábori posta vonalak;
- ✚ Kozmikus vagy műholdas vonalak; információim szerint nincs rendszeresítve ilyen eszköz a MH-nél, bár a műholdas híradás megjelenik a MH külföldön feladatot ellátó kontingenseinél (V-SAT, Inmarsat).

Alaphírhálózatok

Kétféle alaphírhálózzatot különböztetünk meg: stacioner és tábori alaphírhálózzat.

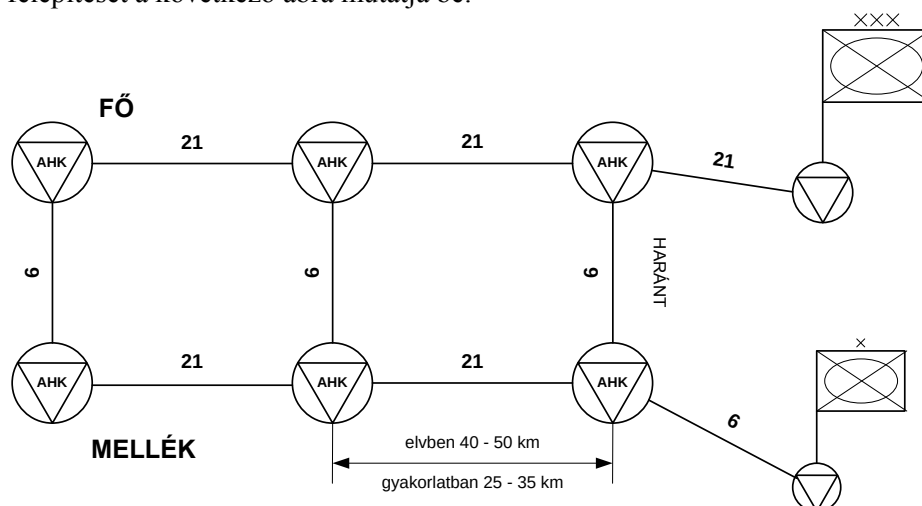
A stacioner (állandó telepítésű) alaphírhálózzatokhoz sorolhatjuk a MH Állandó Telepítésű Híradó és Informatikai Rendszerét (MHÁTHIR), az Országos Távközlő Hálózzat (OTH) részeit bérleményként és a NEKTÁR rendszert.

A MH ÁTHIR-ét a katonai szervezetek stacioner hírközpontjai, az azokat összekötő mikrohullámú rádiórelé és vezetékes (saját tulajdonú fémalapú és saját tulajdonú optikai) összeköttetései alkotják. Ezek biztosítják a MH távbeszélő és FAX híradását. Meg kell említenünk a MH informatikai rendszerét is, hiszen a mikrohullámú rendszeren biztosított sávszélesség szolgálja ki a MH Informatikai Gerinchálózzatát is.

Az OTH-ba beletartozik a Magyarország területén szolgáltatást nyújtó valamennyi vállalat, akiktől a távközlési és közbeszerzési törvény értelmében szolgáltatást vásárolhat a MH. Ezek a cégek lehetnek a MATÁV Rt., Vivendi Rt., Pantel Rt., Westel Távközlési Rt., Pannon GSM Rt., stb.

A NEKTÁR rendszer a MH URH rádió, rádiórelé és mikrohullámú rendszere.

A tábori alaphírhálózat – amelyet a 43. Nagysándor József híradó zászlóalj két alaphírközpont százada telepít – biztosítja a gépesített hadtest és alárendeltjei részére a híradást egy „területlefedő” rács segítségével, amelynek felépítését a következő ábra mutatja be.



2. ábra: a tábori alaphírhálózat felépítése

forrás: saját

Az ábrából a következőket láthatjuk:

- A tábori alaphírhálózat (továbbiakban TAHH) 6 darab alaphírközpontból (továbbiakban AHK) áll;
- Az AHK-kat a fő és a melléktengelyen 21 hadműveleti csatorna biztosítására képes R-414 rádiórelé eszközök kötik össze;
- Az AHK-kat a haránt irányokon 6 csatorna biztosítására képes R-1406 rádiórelé állomások kötik össze;
- A hadtest vezetési pontjait a TAHH AHK-jaival R-414 rádiórelé (21 csatorna) állomások kötik össze;
- A dandár szintű vezetési pontok R-1406 rádiórelé (6 csatorna) állomásokkal csatlakoznak a TAHH-ra.

Az itt felsorolt csupán elvek, illetve hogy hogyan is kellene kinéznie a TAHH-nak. Sajnos ez több ok miatt sem létesülhet teljesen:

- Az eszközök technikai színvonala és műszaki állapota (gépjármű és híradó szempontból), mely az utóbbi időben a karbantartások és javí-

tások nem megfelelő színvonala (a szakemberek hiánya, a karbantartó anyagok hiánya, a javító anyagok hiánya és a javító kapacitás hiánya okoznak, illetve az eszközök leamortizáltsága) rendkívül leromlottak;

- Nem áll rendelkezésre elegendő eszköz (információim szerint nem minden eszközből áll rendelkezésre a szükséges mennyiség az országban);
- Az R-414 rádiórelé állomás üzemi frekvenciája 2 GHz-es tartományba esik, ahonnan a katonai eszközöket kitiltották a frekvenciamigráció után, így a kiképzés nehézkessé vált (ez persze nem azt jelenti, hogy minősített esetben nem üzemelhetnek!).

Híradás vezetés rendszere

Ide tartoznak azok az erők és eszközök, amelyek biztosítják – békében és minősített esetben – a hírendszer megtervezését, megszervezését, a telepített hírendszer operatív vezetését, szükség szerinti átalakítását.

A hírendszer megtervezéséért és megszervezéséért a híradó és informatikai főnök (dd. és ö. z. szinten) vagy a híradó és informatikai főnökségek (hdt. szinten) a felelősök, melyet saját szakmai törzsével hajt végre.

A telepített hírendszer folyamatos, operatív vezetéséért a különböző hírközpontokban létrehozott Híradó Ügyeleti szolgálat a felelős. Ez nem más, mint egy 24 órás szolgálat, amelyet a hírközpont híradó beosztású tisztjeiből, tiszthelyetteseiből hoznak létre. Folyamatosan figyelemmel kísérik a hírendszer működését, begyűjtik az erre vonatkozó információkat és megteszik a megfelelő intézkedéseket.

Futár- és tábori posta híradás

A MH futár- és tábori posta (továbbiakban FTP) szolgálata békében csak Budapest helyőrségben, az ország területén pedig a BM futárszolgálata biztosítja a különböző írásos dokumentumok, térképek, levelek és egyéb küldemények címzetthez való jutását. Minősített esetben a MH FTP szolgálatának hatásköre az egész ország területére kiterjed.

A FTP híradásba beletartoznak a szervezetek (FTP főközpont, FTP állomások, FTP részlegek), a menetvonalak (földi, vízi és légi) és az eszközök (gépkocsik, motorkerékpárok, helikopterek, hajók és páncélozott harcjárművek)

Híradás logisztikai rendszere

Ez nem jelent mást, mint a híradó technikai eszközök és az azt üzemeltető állomány logisztikai kiszolgálását.

A híradó technikai eszközöknél a fejlesztéstől a rendszeresítésen keresztül a kivonásig tartó folyamat minden eleménél jelen van. Két legfontosabb eleme azonban a karbantartás (vagy technikai kiszolgálás) és a javítás. E

két elem nem megfelelő szintű végrehajtása rendkívül befolyásoló tényező lehet, mert akkor a hírendszerek üzemi mutatói leromlanak és nem képesek a vezetés feltételeinek biztosítására. Mindezeket – mint mindannyian tudjuk – nagyon nehéz végrehajtani a megfelelő szakember és anyagiány mellett!

A személyi állomány logisztikai biztosítása is ide sorolható, amelyhez hozzátartozik a kiképzés is.

Híradó tartalék

A híradó tartalék nem más, mint azon eszközöknek a csoportja, amelyek a rendszeresített mennyiségből a hírendszer telepítése során megmaradnak. Természetesen nem hatalmas mennyiségről van szó, hanem néhány dob vezetékről, esetleg egy-két hordozható rádióról. Ezeket az eszközöket a kiesett (meghibásodott, megsemmisült) eszközök pótlására vagy a már üzemelő hírendszer kiegészítésére használhatják fel. Ne feledjük el az üzemi tartalékot sem, amely a híradó állomások nem üzemelő berendezései, azért hogy szükség esetén felhasználhatók más csatornák pótlására vagy kiegészítésre.

A jövő?

A Vezetési Csoportfőnökség a „múlt század végén” elkészített egy koncepciót a MH TAHH-a korszerűsítésének megvalósítására. Az akkor kiadott koncepció véleményem szerint egy kissé elavult. Hogy miért, röviden vázolnám:

Az elképzelt területfedő rács 24 (12) darab AHK-ból állna, melyeket 4.5-5 GHz-es tartományban üzemelő 2 Mbps átviteli sávszélességű mikrohullámú eszközök kapcsolnak össze. A hadtest és dandár szintű vezetési pontok egyidőben két AHK-ra kapcsolódnak fel 14.5-15.5 GHz-es tartományban üzemelő 2 Mbps-os átviteli sávszélességű mikrohullámú eszközeikkel. A zászlóalj szintű alegységek egy AHK-ra csatlakoznak fel maximálisan 512 Kbps-os sávszélességgel a 220-450 MHz-es tartományban. A századok rádióikkal 64 kbps-os sávszélességgel csatlakoznak fel a TAHH AHK-k rádiófelvevő pontjaira. Az előjárók, az alárendeltek és az együttműködők között a TAHH biztosítja az összeköttetést. A rendszer fontos eleme a hálózatzfelügyeleti központ, amely irányítja az üzemelő TAHH-ot, a várható feladatnak megfelelően tervezi az új TAHH felépítését, ellátja adatokkal az állomásokat és végrehajtja a szükséges módosításokat.

Röviden felvázolnék néhány felvetődött kérdést:

- A teljes rendszerbe állítás várható időpontja 2013!!! Ez a rendszer hol fog állni az akkori fejlettségi szintnek megfelelően?
- Egyre alacsonyabb szinten jelennek meg (zászlóalj és század) azok a nagy átviteli sávszélességet igénylő multimédiás és egyéb (online adatbázishozzáférés, szenzor rendszerek) alkalmazások. Mindezek információigényét ki fogja tudni szolgálni?

-
- Nem ismeretes számomra, hogy a TAHH megtervezését és megszervezését milyen szervezet vagy technikai eszköz fogja majd elvégezni és milyen munkasorrendben?
 - A következő a hálózatzfelügyelet problematikája. Kik fognak itt dolgozni, milyen hatáskörük lesz (az összeköttetés felvételekor utasíthatnak egy dd. FH-t, hogy települjön arrébb, mert különben nem lesz összeköttetés), a tervezést is ők fogják végezni, vagy nem, mekkora létszámú lesz, milyen rendfokozatot fognak viselni (hadnagy vagy őrnagy), milyen szakmai végzettségűek lesznek (egyetem, főiskola)?

Befejezés

Az előbbieken megpróbáltam bemutatni néhány szóban a MH hírendszerét a fogalom értelmezésén keresztül. A bemutatottakon keresztül jól érzékelhető, hogy elindult egy folyamat a katonai híradás modernizálásában, de ez sajnos csak az ÁTHIR-t érinti. A tábori hírendszer (beleértve a TAHH-t is) elavult; mind híradó, mind gépjárműtechnikai vonatkozásban hatalmas javítási problémák mutatkoznak. Nincs elegendő technikai eszköz, az áttérés az önkéntes haderőre (lesz-e elegendő szerződéses katona és azok előképzettsége megfelelő lesz-e?) nagyban befolyásolják a hírendszerekkel szemben támasztott követelmények teljesítését. A MH híradó alakulatai és más katonai szervezetek híradó alegységei így is már teljesítőképességeik határán dolgoznak. Mindezek figyelembe vételével a következő kérdések merülnek fel bennem: Szabad-e ilyen remegő lábakon álló hírendszerral számolnunk? Képesek leszünk-e fenntartani a jelenlegi hírendszert az új rendszerbe állításáig? Ha az új rendszer egyes részeit hamarabb kell rendszerbe állítanunk, akkor azt össze tudjuk-e majd kapcsolni a régivel? Mi lehet a megoldás ebben a helyzetben?

Véleményem szerint a problémák megoldása csak akkor lehetséges, ha nem csak akkor veszik észre a híradókat, amikor „nem működik a telefon”. Ezt hogyan lehet elérni? Csakis azzal, ha a híradó katonák tudása és hozzáállása a jelenleginél jobb lesz. Ne feledjük, hogy ezzel kapcsolatban nekünk, mint oktatóknak feladatunk van. Mégpedig az, hogy széles látókörű, magasan képzett, az új ismeretekre is igényt tartó tiszteket és tiszthelyetteseket bocsássunk ki. Remélem, hogy ezzel a mondatommal nem sértettem meg senkit, ha igen, akkor elnézést kérek!

Felhasznált irodalom

[1] Kozák Miklós százados: A híradás alapvető fogalmai, jegyzet, Zrínyi Miklós Katonai Akadémia, Budapest, 1994, Nytsz.: 734/451;

[2] Dr. Rajnai Zoltán mk. őrgy. – Kis Lajos mk. szds.: Ábraalbum a „Katonai kommunikációs rendszerek szervezése” című tantárgyhoz, tansegédlet, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2002, Nytsz.: 932/504;

VÁLTOZÓ HONVÉDSÉG, ÁTALAKULÓ MÉRNÖKTISZT- KÉPZÉS

A katonai felsőoktatásban dolgozó, szolgálatot teljesítő középszintű vezető fő feladata, hogy az állandóan változó (kedvezőtlenebb) körülmények között is megtalálja a lehetőséget a felelősségi körébe tartozó képzés leghatékonyabb végzésére.

Úgy tűnik a HM HVK illetékesei is belátták, hogy a honvédség mérnöktiszti utánpótlását nem lehet és nem is célszerű a polgári életből megvásárolni. A katonai élet körülményei között, a Nemzetvédelmi Egyetemen szocializálódott hallgató, fiatal tiszt jobban teljesít csapatoknál, mint a polgári életből átvett társa. Ugyanakkor a mérnöktisztképző szervezeteknek is el kell fogadni, hogy a felére, harmadára csökkent haderő mérnöktiszti utánpótlás igénye a korábbi képzési struktúrával csak rendkívül gazdaságtalanul elégíthető ki, ami a védelmi felülvizsgálat után már kevésbé védhető.

A szerző az általános környezet felvázolásán túl a híradótiszt-képzés, a híradó szakmai felkészítés helyzetét, lehetőségeit vizsgálja a Zrínyi Miklós Nemzetvédelmi Egyetem változó képzési struktúrájának és szervezetének figyelembevételével.

Bevezető (a gondok)

A katonai felsőoktatás és a végrehajtó intézményhálózat átalakítása az 1990-es évek elejétől folyamatosan zajlik. A folyamat 1996-tól, a Zrínyi Miklós Nemzetvédelmi Egyetem megalakulásától intenzifikálódott, melynek eredményeképp az egykori tisztképző főiskolák folyamatosan beolvadtak, integrálódtak a egyetem szervezetébe. Ennek eredményeképp jött létre a jelenlegi három (két egyetemi és egy főiskolai) karos egyetemi szervezet.

Az egész folyamatra jellemző, hogy a szervezeti átalakításokat intézményen kívüli tényezők – a honvédelmi tárca oktatáspolitikai törekvései, az MH létszámcsoökkentése, a felsőoktatási integrációs törvény - generálták, amelyeknek természetes pénzügyi, finanszírozási okai voltak a fő mozgatói. Úgy tűnik, hogy az egyetem, illetve a jogelőd intézményei mindig kényszerhelyzetben voltak és belső – hatékonysági – megfontolásból nem igazán történt lényeges szervezeti változtatás.

Ezen időszak alatt mit sem változott a képzési struktúra. Önmagában ez nem is lenne probléma, hisz egy képzési rendszert többnyire hosszútávra alakítunk ki, 4-5 év szükséges a végzéshez és legalább 1-2 év kell ahhoz, hogy a képzés minőségét a „piac” visszaigazolja. Elégedettség töltött el minket, hogy

a szakjainkat a MAB 1999-ben akkreditálta, illetve feltételesen akkreditálta, az új szakokról általában kedvező állásfoglalást alakított ki [1]. A végzett tisztek döntő többsége megállta helyét csapatbeosztásokban, nemzetközi gyakorlatokon és koalíciós környezetben is elismerést vívnak ki.

Ugyanakkor megállapítható, hogy a Magyar Honvédségnél bekövetkezett létszámcsökkentések következtében jelentősen visszaesett egy-egy fegyvernem, szakcsapat tiszti szükséglete, melynek kielégítésére a megmerevedett képzési struktúra nem tudott adekvát választ adni. Így a megrendelő oldaláról bizonytalanná vált a tiszti utánpótlás tervezése, a másik oldalról viszont gyakran előfordult, hogy a végzett tiszteknek nem tudtak képzettségüknek megfelelő beosztást felajánlani.

Ebben a helyzetben a híradó szakmai felkészítés helyzetének megítéléséhez két terület vizsgálatát tartom kiemelten fontosnak:

- a mérnöktiszt-képzést, valamint
- a szaktanfolyami képzések feltételrendszerét.

1. Mérnöktiszt-képzés

1.1. A jelenlegi helyzet

A mérnöktiszt-képzés jelenleg a ZMNE Bolyai János Katonai Műszaki Főiskolai Karán folyik, 7 szakon és a szakokon belül 14 (6 gépész- és 8 villamosmérnöki) szakirányon. A szakok – építőmérnöki, gépésmérnöki, közlekedésmérnöki, vegyészmérnöki, villamosmérnöki, műszaki informatikai, biztonságtechnikai – és ennek megfelelően a képzés differenciálódása megfelel a műszaki felsőoktatás képesítési követelményeinek. Így megállapítható, hogy a főiskolai karon egyetlen szakmacsoportú (profiltiszta) képzés folyik, az ezzel járó oktatói, oktatásszervezési és infrastrukturális előnyökkel.

Ugyanakkor megállapítható, hogy a képzést végrehajtó szervezeti egységek leterheltsége – a megrendelő tiszti utánpótlás igényeinek függvényében – rendkívül differenciált. Ezt a helyzetet tovább rontja az utóbbi években beiskolázott hallgatók gyenge minősége és a lemorzsolódások magas aránya. A 2003. évi tisztaválasztás során két szakon illetve szakirányon is előfordult, hogy a képzési követelmények nem teljesítése miatt tancsoportonként csak 1-1 főt avathattunk tisztté. Ez a helyzet tartósan nem tartható fenn.

A híradótiszt-képzés a villamosmérnöki szak egyik szakirányán zajlik. A képzés végrehajtásáért a Katonai Távközlési és Telematikai Tanszék Híradó Szakcsoportja felel, amelynek alaprendeltetése a nappali és levelező képzési formákban tanuló főiskolai hallgatók képzése.

A karon folyó képzés eredményeképp végzett hallgatóink a tiszti kinevezési okmány mellett, híradó (távközlési) szakirányú villamosmérnöki oklevelet vehetnek át. A villamosmérnöki tudás a híradótiszti pálya megkezdésének szükséges, de nem elégséges feltétele. Ugyanakkor a polgári végzettség és a folyamatosan karbantartott tudás a fiatal híradótisztet a munkaerőpiac keresett

szereplőjévé teszi, biztosítva számára, hogy a Magyar Honvédségtől függetlenül is komoly egzisztenciát teremthet. Mindez a munkaadó (MH) számára folyamatos kihívást jelent és megfelelést a munkaerő piaci elvárásoknak.

1.2. A képzés struktúrájának és szervezeteinek átalakítása

1.2.1. Változó képzési struktúra, integrált képzés, hadmérnöki szak alapítása

Az egyetem korábban is kísérletet tett a képzési struktúra egyszerűsítésére, az egymáshoz szakmailag közel álló szakok, szakirányok képzésének összevonására, ezáltal a tiszti alapképzés gazdaságosságának javítására. Ez sikerrel járt azon szakokon, melyek teljes terjedelmükkel a katonai felsőoktatás képesítési követelményeinek hatálya alá estek. Így alakult ki az integrált képzést folytató katonai vezetői szak. Eredménytelen volt mindeddig a műszaki felsőoktatás képesítési követelményei által is meghatározott, mérnökképzést folytató szakokon és szakirányokon a képzés differenciáltságának csökkentésére irányuló erőfeszítés. A szakreferensek a végsőig ragaszkodtak a szakok, szakirányok részletes képzési követelményeinek teljesítéséhez, ami ugyan egybeesett a fegyvernem, szakcsapat érdekeivel, de a képzés gazdaságosságát radikálisan rontotta.

A megoldás – mely az integrált képzési szak, a hadmérnöki szak megalkotásában öltött testet – csak megrendelő és a képzést végrehajtó intézmény kölcsönös kompromisszumával, a probléma újszerű megközelítésével, egyfajta szemléletváltással volt lehetséges.

A hadmérnöki szak alapítása

Az előző pontokban is jelzett képzés-költséghatékonysági problémák az egyetem vezetését arra ösztönözték, hogy a jelenlegi – 7 szakon és 14 szakirányon folyó – mérnöktiszt-képzés alternatívájaként egy olyan integrált alapképzési szakot [3] hozzon létre, mely:

- a magyar és európai felsőoktatás harmonizációját elősegítő – Bolognai nyilatkozatban deklarált – elveknek megfelelően lineáris képzési szerkezetű, azaz a képzési folyamatnak egymásra épülő főiskolai (BSc) és egyetemi (MSc) kimenete van;
- kielégíti a Magyar Honvédség folyamatosan változó igényeit a mérnöktisztek utánpótlásában;
- a tanulmányi időszakon belül minél későbbre tolja ki a szakirány és specializáció választást annak érdekében, hogy optimálisan legyen tervezhető az MH mérnöktiszti utánpótlása;

hosszútávon fenntartható és költséghatékonyan működtethető az egyetem szervezésében.

A ZMNE erre a feladatra kiválasztott munkacsoportja kidolgozta a hadmérnöki szak létesítésére vonatkozó dokumentumokat.

Az új szak szerkezeti felépítését a következő oldalon látható ábra szemlélteti. A képzés első négy szemesztere közös alapozású. Az ötödik szemeszterben a képzés szétválik négy főszakirányra ezek: a haditechnikai-, a repülőműszaki-, a műszaki és közlekedési -, valamint a katonai elektronikai főszakirány. Az ötödik szemeszterben a főszakirány közös alapozása folyik. A hatodik szemesztertől kezdődik a szakirányú képzés.

Ez által biztosítható több jelenlegi szakirány hallgatóinak egy tancsoportban történő képzése az 5. félév végéig, mely jelentősen javítja a képzés költséghatékonyosságát, a képzési ciklus végén pedig jobban igazodik a csapatok tiszti utánpótlás igényeihez. Egy példával magyarázva: nem négy évenként indíthatnak elektronikai hadviselés osztályt, hanem a szakcsapat igénye szerint a rendszer évente, két évente is lehetőséget biztosít néhány fő beiskolázására, tisztté avatására.

Egyes szakirányokon a 7-8. szemeszterekben, megrendelő igényei alapján ágazati sajátosságokat tartalmazó tárgyak felvételére nyílik mód. Például a repülőműszaki főszakirány fedélzeti rendszerek szakirányán a megrendelő igénye alapján, repülőfedélzeti műszer- és automatikai ágazat, repülőfedélzeti rádióelektronikai ágazat vagy repülőfedélzeti fegyvertechnikai ágazat képzésére kerülhet sor. A képzés első ciklusa (BSc) a nyolcadik szemeszterrel zárul. A végzetek vagy folyamatosan, vagy néhány éves gyakorlati tapasztalat birtokában – a megrendelő igényének megfelelően – folytathatják tanulmányaikat a második ciklusban az MSc fokozat megszerzéséért. A megrendelő prognosztizált adatai szerint a képzés zöme az első ciklusra tevődik.

A második ciklusban a képzés elitképzés jellegű, a magasabb szintű mérnöki beosztások betöltéséhez szükséges képzettséget és végzettséget biztosítja. Az integrált katonai-, szakmai képzés tartalmazza a műszaki felsőoktatásban nélkülözhetetlen természettudományi ismeretek mellett az alkalmazott gazdaságtudományi ismereteket, a haderőnemek hadműveletének elméletét, az általános és szakmai menedzsment ismereteket és a komplex haditechnikai szakmai ismeretek megrendelő által szükségesnek ítélt ismereteit.

A hadmérnöki szak a műszaki szakcsoportra vonatkozó képesítési követelményeket követi. A szak főbb tanulmányi területeinek elosztása kielégíti a 77/2003 Korm. rendelet követelményeit, valamint 157/1996. Korm. rendeletben általánosan kialakított tantárgyi szerkezetet.

[illegible]

1. A fedélzeti rendszerek szakirány ágazatai: repülőfedélzeti műszer és automatika, repülőfedélzeti fegyvertechnika, repülőfedélzeti rádió-elektronikai.
2. A sárkány- hajtómű szakirány ágazatai: repülőgép, helikopter.

-
3. A műszaki szakirány ágazatai: fenntartási, építő, harcos műszaki, anyagi-technikai.
 4. A közlekedési szakirány ágazatai: szállító alegység-parancsnoki, közlekedéstervező.

Helytelen lenne a hadmérnöki szak alapításakor csak az előnyökről beszélni. A szak létrejötte egy kompromisszum eredménye, mely szükségszerűen engedményeket jelent a korábbi követelményekből, vívmányokból. A jelenlegi hét szakon folyó mérnöktiszt-képzés több mint 30 éves múltat tekint vissza, melynek során a képzés tapasztalatait visszaforgattuk és kialakult a megrendelő igényeinek megfelelő (de jelenleg gazdaságtalan) katonai-szakmai képzés.

A hadmérnöki szak tanterve erősíti ugyan a képzés katonai jellegét, de gyengíti a mérnöki alapozást. Ennek következtében a jelenlegi polgári követelményeknek is megfelelő képzés elmozdul, áttér a katonai követelmények fokozott kielégítésének szűkebb sávjába.

A hadmérnöki szakon végzettek nem rendelkeznek majd polgári végzettséggel, ami ugyan fokozza a szervezethez való (kényszer)kötődést, de nem biztos, hogy mindez jó a Magyar Honvédségnek és biztosan nem jó az egyénnek, aki egzisztenciálisan kiszolgáltatottabbá válik. Ez a változás nehezíti azon tisztek életpályáját akik idővel kiválnak a Honvédségből, a bennmaradókat pedig távolítja a magyar műszaki értelmiségtől.

Ezen hátrányok ellentételezéseként jelentkezik egy gazdaságosan, a Nemzetvédelmi Egyetem bázisain, katonai körülmények között végrehajtható hadmérnök-mérnök tiszt képzés, melyben megőrizhető, átmenthető az évtizedek alatt kialakult képzési kultúra.

1.2.2. Változó egyetemi szervezet

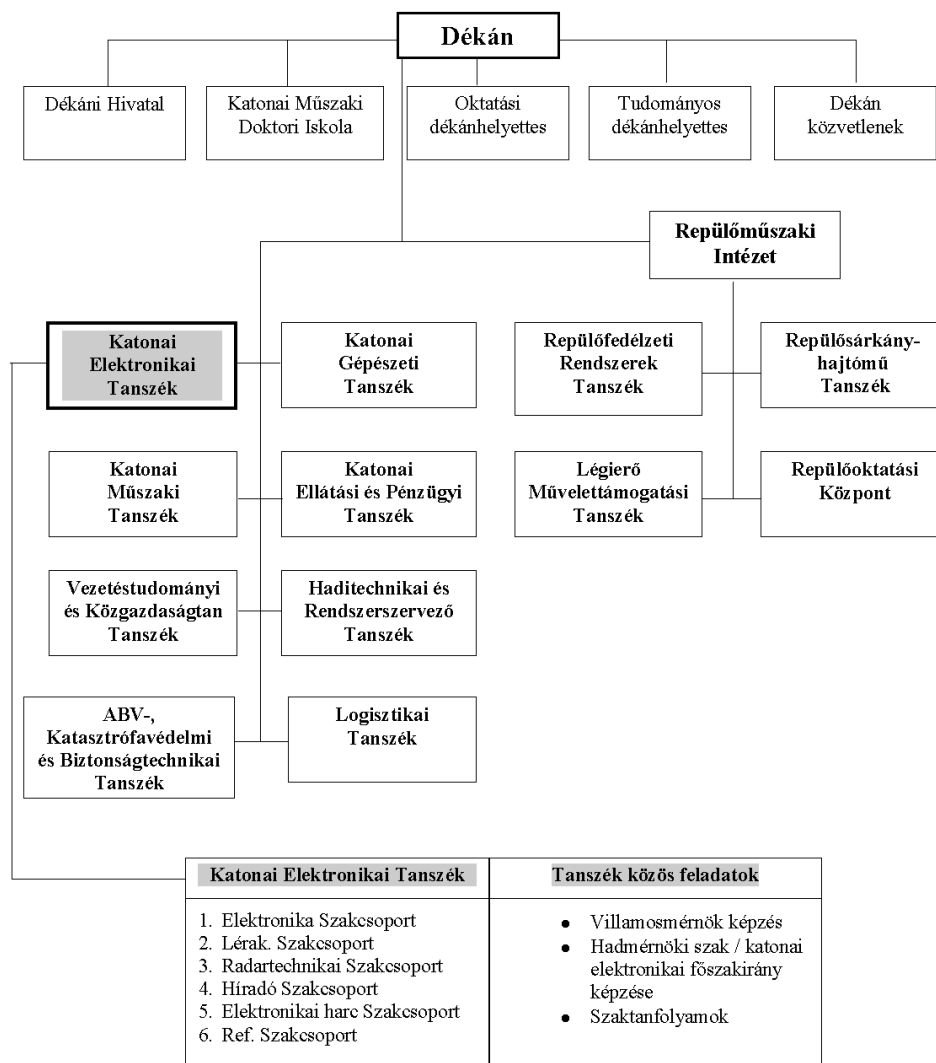
A ZMNE egyetértésben a megrendelővel, a képzés költséghatékonyságának javítását célzó szervezeti változásokat tervez, melynek eredményeképp – a jelenlegi két egyetemi és egy főiskolai kari szervezetek helyett – két egyetemi karos szervezetre tér át. Az áttérés magában foglal egy minimum 15 %-os létszámcsökkentést is. A mérnöktiszt-képzés a jelenlegi BJKMFK a és VSZTK szervezeteiből kialakuló Bolyai János Katonai Műszaki (egyetemi) Kar feladata lesz. Az új kar szervezete a következő oldalon látható [2]. A tanszékek száma a korábbi 28-ról 12-re csökken.

A híradótiszt-képzésért felelős szervezeti egység – a Katonai Elektronikai Tanszék – a villamosmérnök képzést folytató tanszékek összevonásával jön létre és ez lesz az egyik alaprendeltetés szerinti közös feladata is. A másik a hadmérnöki szak/katonai elektronikai főszakirány képzése. Az összevont oktatási szervezeti egység rövid idő alatt felkészül a képzési profiljába vágó szaktanfolyamok végzésére. Ez elemi érdeke lesz mindenkinek, hiszen a túlmunka díjazása csak a tanszéki óránorma teljesítése után lehetséges.

Az egyetem vezetésének elgondolása szerint az új integrált kari szervezet költséghatékonyan és a megrendelő igényeknek jobban megfelelően lesz képes feladatait ellátni.

A ZMNE Bolyai János Katonai Műszaki Kar szervezeti felépítése

/tervezet/



1.2.3. A híradótiszt-képzés helye az új képzési és szervezeti struktúrában

A híradótiszt-képzés alternatívái a következők:

-
- Amennyiben min. 15 fő/év mérnöktiszt igénye van a híradó szolgálatnak, úgy indítható a polgári (villamosmérnöki) végzettséget is biztosító híradó szakirány. (Ez a cikk leadásakor valós lehetőség, de ugyanakkor több irányból támadták a polgári végzettséget is biztosító képzés teljes felszámolását szorgalmazva.)
 - Ha az igényelt hallgatói létszám ennél kevesebb, úgy csak a gazdaságosabb képzést biztosító hadmérnöki szak / katonai elektronikai főszakirány / híradó szakirány indítható.

A híradócsapatok tiszti utánpótlás igénye jellemzően eléri ezt az irányszámot, így érvényesíthető a Híradó és Informatikai Csoportfőnökség elvárása, hogy a híradótisztek villamosmérnöki alapképzésben részesüljenek. A híradó szakirányú villamosmérnök képzés tananyagát, követelményeit a magyar műszaki felsőoktatás tradíciói alapozták meg és a mérnöktiszt-képzés több évtizedes tapasztalata igazította a megrendelő, a Magyar Honvédség igényeihez [4]. Szakmai színvonalát a folyamatosan ellenőrzött műszaki felsőoktatási követelmények biztosítják. Nem kizárt, hogy egyes években – a kisebb létszámú tiszti utánpótlás igény következtében – csak a hadmérnöki szak képzési rendszerében képezhetők híradótisztek. Ebben az esetben a következő oldalon ábrázolt szerkezetben vehetik fel a hadmérnöki szak / katonai elektronikai főszakirány / híradó szakirányának ismeretanyagát.

2. A szaktanfolyami képzés

A megrendelő Magyar Honvédség részéről – összefüggésben az önkéntes haderőre történő áttéréssel, az új haditechnikai eszközök rendszeresítésével, az új előmeneteli rend 2003 szeptember 1-vel történő bevezetésével – a hivatásos és szerződéses katonák tömeges át- és továbbképzési igénye jelentkezett, melynek részbeni kielégítését az egyetemnek fel kell vállalni. A tanfolyami képzés jelentős felfutása hónapok kérdése, de a működtetés szervezeti keretei máig nem alakultak ki. Tudomásul kell vennünk, hogy a képzés súlypontja eltolódik a tanfolyami képzések felé, mely egyidejűleg menekülési irány is lehet a tisztképzésben feleslegessé vált oktatók foglalkoztatására, a másutt csak drágábban megvásárolható képzések helyben történő végrehajtására. A főiskolai kar tanszékein végrehajtott 3 D-s radarkezelők, a Siemens HICOM 300 E rendszer üzemeltetők felkészítése is bizonyítja, hogy az egyetem bázisán megszervezett szakmai tanfolyamok gazdaságosan és hatékonyan elégítik ki a megrendelői igényeket.

Ez irányú feladatainkat a 17/1997., az 1/2000., a 10/2002., és a 20/2002. sz. HM rendeletek szabályozzák, melyek szerint az át- és továbbképzésekre vonatkozó előírásokat 2005-ig fokozatosan kell bevezetni.

Megjegyzések: nappali képzési formában heti 26 tanórával számolunk; szakmai, csapat (üzemi) -gyakorlat főiskolai szinten legfeljebb 12 hét; ösztöndíjas hallgatók, az első szemeszter előtt sorkatonai alpkiképzésen vesznek részt.

2.1. Meglévő és kialakítandó képességek a szaktanfolyami képzések végrehajtásához

A Katonai Távközlési és Telematikai Tanszék (és utódszervezete is) azonosul a megrendelő – HM HVK Híradó és Informatikai Csoportfőnökség, MH Elektronikai Szolgálatfőnökség – az irányú elvárásával, hogy tanszékünk vegyen részt a rendszerbe állításra tervezett és rendszerbe állított eszközök üzemeltetésére és üzemben tartására történő felkészítésben, működjön egyfajta szakmai továbbképző központként.

Tekintsük át azon képességeket, melyek már jelenleg is biztosítják az elvárásoknak történő megfelelést.

2.1.1. Siemens HICOM 300 E üzemeltetők felkészítése (haditechnikai céltanfolyam)



Képességek:

Oktatók: 3 fő

Infrastruktúra: távközlési mintahálózat szaktanterem négy, hálózatba kapcsolt digitális kapcsolóközponttal, optikai, mikro és hagyományos átviteli utakkal

Kiképzési programok:

1. Az alap nappali és levelező képzés tantárgyi programjai
2. HICOM 300 E/H szaktanfolyam (120 ó)
3. HICOM programozói tanfolyam (120 ó)

Gyakoriság: 3-4 tanfolyam/év

2.1.2. Kongsberg MP 300 és MH 300 rádió üzemeltetők felkészítése (haditechnikai céltanfolyam)



Képességek:

Oktatók: 2 fő

Infrastruktúra: Kongsberg URH rádiós szaktanterem, 10 klt. MP 300 hordozható, 10 klt. kézi rádióval és 2 klt. rádióteszt berendezéssel

Kiképzési programok:

1. Az alap nappali és levelező képzés tantárgyi programjai
2. Kézi rádió konfigurációs (30 ó)
3. Hordozható rádió konfigurációs (60 ó)
4. Kongsberg belső beszélgető rendszer üzemeltető (30 ó)
5. Kongsberg frekvenciamenedzsment (90 ó)

Gyakoriság: 4-8 tanfolyam/év

2.1.3. Mikrohullámú rádiórelé üzemeltetők felkészítése (haditechnikai céltanfolyam)



Képességek:

Oktatók: 2 fő

Infrastruktúra: Mikrohullámú szaktanterem, mérőműszerek a mikrohullámú és digitális jelátvitel paramétereinek mérésére

Kiképzési programok:

1. Az alap nappali és levelező képzés tantárgyi programjai
Gyakoriság: Tanfolyami képzés a mikrohullámú rádiórelék rendszerbe állítását megelőzően tervezett.

2.1.4. Információvédelmi szakállomány felkészítése (szakmai ismeret-kiegészítő felkészítés)



Információvédelmi szaktanterem

Oktatók: 5 fő (külső és belső előadók)

Infrastruktúra: információvédelmi szaktanterem nemzeti és NATO rejtjelző eszközökkel, informatikai hálózatok szaktanterem, kiegészítve az informatikai biztonság oktatásához szükséges hardver elemekkel és szoftverekkel

Kiképzési programok:

1. Az alap nappali és levelező képzés tantárgyi programjai
2. Információvédelmi alaptanfolyam (120 ó)
3. Információvédelmi technikai tanfolyam (120 ó)
4. Információvédelmi eszközismereti tanfolyamok (60-120 ó)
5. Információvédelmi szakügyviteli tanfolyam (120 ó)

Gyakoriság: 4 tanfolyam/év

2.1.5. Előmeneteli továbbképzés

Az előmeneteli továbbképzés

- az általános katonai és vezetői felkészülésből és vizsgából, valamint
- a tanszékünkön levelező formában végrehajtott szakmai felkészítésből és vizsgából áll.

A Híradó Szakcsoport együttműködve a HM HVK J-6-tal együttműködve kidolgozta a főhadnagyi és századosi előléptetéshez előírt követelményeket kielégítő képzési programokat és ez alapján 2003 júniusában vizsgáztattunk első alkalommal fiatal híradótiszteket. Felvállaltuk – külső munkaerő bevoná-

sával – az információvédelmi szakállomány előmeneteli továbbképzéseinek szervezését és végrehajtását is.

Oktatók: 10 fő (külső és belső oktató)

Infrastruktúra: a főiskolai kar, de kiemelten a Katonai Távközlési és Telematikai Tanszék szaktantermei

Kiképzési programok:

1. Híradó szakmai előmeneteli tanfolyam (százados)
2. Híradó szakmai előmeneteli tanfolyam (főhadnagy)
3. Rejtjelző szakmai előmeneteli tanfolyam (őrnagy)
4. Rejtjelző szakmai előmeneteli tanfolyam (százados)
5. Rejtjelző szakmai előmeneteli tanfolyam (főhadnagy)
6. Rejtjelző szakmai előmeneteli tanfolyam (törzssászlós)
7. Rejtjelző szakmai előmeneteli tanfolyam (főtörzsőrmester)
8. Rejtjelző szakmai előmeneteli tanfolyam (törzsőrmester)

Gyakoriság: 4-6 tanfolyam/év

A Híradó és Informatikai Csoportfőnökség az alábbi követelményeket [5] határozta meg a híradó (fhdgy., szds.) előmeneteli tanfolyamok résztvevői számára:

Ismerje meg

- a főiskolai tanulmányok befejezése - előző tanfolyami képzés - óta eltelt időben a híradó, villamosmérnöki, távközlési szakterületen bekövetkezett fontosabb jogszabályi, szervezési, szervezeti változásokat, az új technológiák alkalmazásának alapjait;
- az elmúlt években rendszeresített és a középtávon rendszeresítésre tervezett híradó eszközöket, működésük alapjait, szolgáltatási jellemzőiket, a hírendszerben történő alkalmazásuk rendjét;

Legyen képes

- alapképzettségére és a tanfolyamon megszerzett tudásra alapozva a polgári és katonai hírközlési környezet (távközlési szegmens) áttekintésére, a távközlési szolgáltatók hálózatainak igénybevételevel kapcsolatos feladatok értelmezésére, informatikai eszközök (személyi számítógép, e-learning hálózatok) alkalmazásával az új generációs híradó eszközök megismerésére, beüzemelésére, rendszerbe integrálására, üzemeltetésük és üzemben tartásuk szervezésére, informatikai és távközlő hálózatok együttes üzemeltetésére, az információ továbbítására az információvédelem követelményeinek teljesítése mellett.
- beosztásában a NATO előírások szerinti kidolgozói és törzsmunka végzésére

A felkészítést négy összevonással, az alábbi óraelosztásban [6] hajtottuk végre:

Tantárgyak megnevezése	Óraszámok		
	kontakt	önképzés	összesen
<i>A hírközlés szabályozása Magyarországon</i>	6	6	12
<i>Híradás (katonai kommunikációs hálózatok) szervezése</i>	12	12	24
1. Tk.: Kis- és közepes kiterjedésű műveletek híradása	6	6	12
2. Tk.: A NICS; A katonai híradás megszervezésének elvei a fejlesztések függvényében	6	6	12
<i>Elektronikai eszközök üzemben tartása</i>	4	4	8
<i>Információvédelem</i>	4	4	8
<i>Híradó eszközök típusismerete és üzemeltetése</i>	28	28	56
1. Tk. Komplex villamos rendszerek üzemeltetése és érintésvédelme	2	2	4
2. Tk. Mikrohullámú hálózatok és berendezések	6	6	12
3. Tk. Új generációs harcászati rádiók	6	6	12
4. Tk. HICOM 300 E/H ismeret	8	8	16
5. Tk. GPS ismeretek és kapcsolódó jártasságok	6	6	12
<i>Telematika</i>	10	10	20
1. Tk. Számítógépek felépítése és felhasználói szintű ismeretei	6	6	12
2. Tk. Informatikai hálózatok és azok csatlakoztatása távközlő hálózatokhoz	4	4	8
VIZSGA	6		6
Szóbeli vizsga	4		4
Gyakorlati vizsga	2		2
MINDÖSSZESEN:	70	64	134

Megjegyzés: A képzésben résztvevők számára 4 óra/fő konzultációt kell biztosítani, melyet személyesen vagy elektronikus formában vehetnek igénybe.

A tanfolyami képzésben széleskörűen alkalmaztunk informatikai eszközöket, de ezen a területen a csapatok ellátottsága jelentősen rontotta lehetőségeinket. A Zrínyi Miklós Nemzetvédelmi Egyetem törekszik arra, hogy a tisztek tanfolyami képzésében lényegesen nagyobb szerepet kapjon a távoktatás. En-

nek infrastrukturális feltételrendszere tanszékünkön kialakulóban van, egyetemi szinten Távoktatási Osztály koordinálja a szervezeti egységek munkáját. A csapatoknál ugyanakkor jelentős fejlesztés szükséges a fogadókészség biztosításához. Talán nem túl távoli elvárás, hogy minden (híradó)tiszt lappal és hálózati eléréssel rendelkezzen.

Befejezés

E rövid cikk keretében – felhasználva a konferencia által nyújtott publicitást – áttekintést kívántam adni a főiskolai karon, a Katonai Távközlési és Telematikai Tanszéken lezajlott és tervezett változásokról. A képzési struktúra átalakítása javítja a költséghatékonyságot, a tartalmi és infrastrukturális fejlesztések emelik a híradó szakkiképzés, a híradótiszt-képzés minőségét. Összességében megállapíthatom, hogy tanszékünk felkészült az új híradó eszköz rendszerbe állításából egyetemünkre háruló képzési feladatok teljesítésére.

A felhasznált irodalom jegyzéke:

- [1] Czimmer István László: A hadmérnökképzés kialakításának körülményei, szükségessége, célja Hadmérnökképzési konferencia, ZMNE, 2003. 06. 18.
- [2] A Zrínyi Miklós Nemzetvédelmi Egyetem helyzete és szervezeti átalakítása, Honvédelmi Minisztérium vezetői információs értekezlet Budapest, 2003. 05. 12. [3] Hadmérnöki szakbizottság: Szaklétesítési kérelem (munkaanyag), ZMNE, 2003. 07. 04.
- [4] 157/1996 (X. 22.) kormányrendelet a műszaki felsőoktatás alapképzési szakjainak képesítési követelményeiről
- [5] A híradó századparancsnoki (százados) képesítés szakmai követelményei HM HVK Vezetési Csoportfőnökség, 2003. 03. 11.
- [6] Híradó szakmai előmeneteli tanfolyam (százados) képzési programja, ZMNE, 2003.

MELEG TARTALÉKOLT ANTENNARENDSZEREK

GRANTE Antenna Fejlesztő és Gyártó Részvénytársaság
2509 Esztergom - Kertváros, Dorogi út 5-7., 2501 Esztergom, Pf.: 84.,
Telefon: 06-33-435-268, 06-33-512-468, 06-33-435-271, Fax: 06-33-435-
265
E-mail: grante@grante.hu, ladanyi@grante.hu, Honlap: www.grante.hu

BEVEZETÉS

A távközlési igények ugrásszerű növekedése két alapvető technológiai feladatot állít a gyártók elé:

- a kapacitások növelése
- a megbízhatóság fokozása

Ezeket az igényeket lényegében a GSM gyors térnyerése és az internetes forgalom növekedése generálja.

A kapacitások növelésére a mikrohullámú hálózatok esetében többféle lehetőség van:

1. nagyobb frekvenciasáv
2. bonyolult modulációs eljárások alkalmazása
3. a frekvencia újra felhasználása (frequency reuse)

ad 1. A spektrum végeessége és az igények folyamatos növekedése miatt ez az út nem járható.

ad 2. A bonyolult modulációs eljárások realizálása növeli a meghibásodás valószínűségét és drágítja a berendezéseket.

ad 3. A frekvencia újra felhasználása optimális megoldás (kétpolarizációs antenna) egy antenna dupla kapacitás.

MEGBÍZHATÓSÁG

A mikrohullámú összeköttetés megbízhatóságának fokozása.

A berendezés rendelkezésre állása:

$$A = \text{MTBF} / (\text{MTBF} + \text{MTTR})$$

MTBF – két meghibásodás között eltelt átlagos időtartam

MTTR – a hiba kijavításáig eltelt időtartam

Általánosságban a rendelkezésre állás: (készenléti együttható)

$$A = \text{működési idő} / (\text{működési idő} + \text{állási idő})$$

Pl.: Ha egy rendszer 10.000 órát működik és 10 órát áll, akkor a készenléti együtttható

$$A = 10.000 / (10.000 + 10) = 0,999$$

azaz 99,9%

A kiesési együtttható:

$$U = 1 - A$$

Az adott példában:

$$U = 1 - 0,999 = 0,001$$

azaz 0,1%

Ha egy kétutas csatornában a kiesési együtttható 0,02% és feltételezzük, hogy a két út egymástól független, akkor a kiesési idő 105 perc/év.

Ez az érték a gyakorlatban elfogathatatlan.

A készenléti együtttható növelésének legjobb módszere a meleg tartalékolt rendszer alkalmazása.

A készenléti együtttható 10.000 óra MTBF esetében tartalékolt rendszere

$$(MTBF = 10.000 * 10.000 = 10^8 \text{ óra})$$

$$A = \frac{MTBF}{(MTBF + MTTR)} = 0,999999$$

Azaz 99,999999%

A kiesési együtttható:

$$U = 1 - A = 10^{-7}$$

A kiesési idő: 3,2 mp/év

A mai korszerű berendezések esetében az MTBF $\cong$ 400.000 óra.

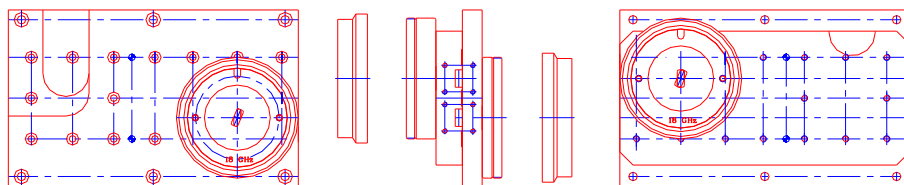
Tartalékolt rendszer esetében a kiesési idő (MTTR= 10 óra feltételezés esetében)

$$U = 0,00093 \text{ mp/év}$$

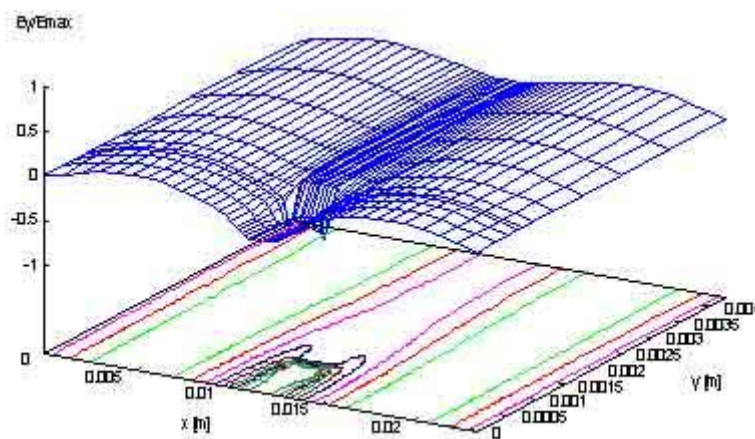
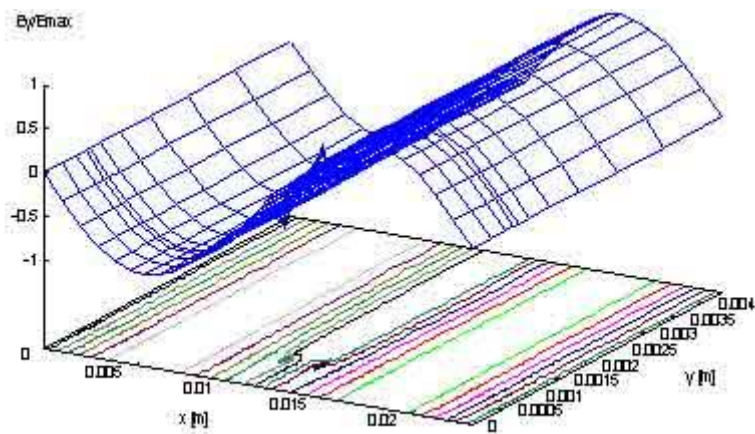
Feltételezés: MTTR=1 hét=168 óra (mostoha időjárás)

Ekkor $U = 0,0315 \text{ mp/év}$.

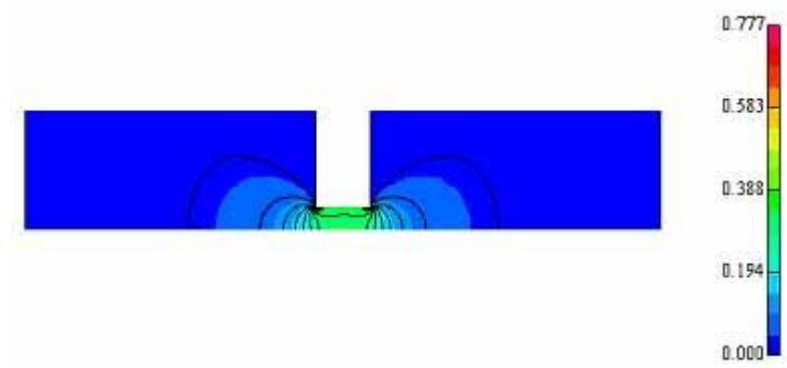
A rendszer kiesési ideje gyakorlatilag nem érzékeny a javításig eltelt időtartamra.



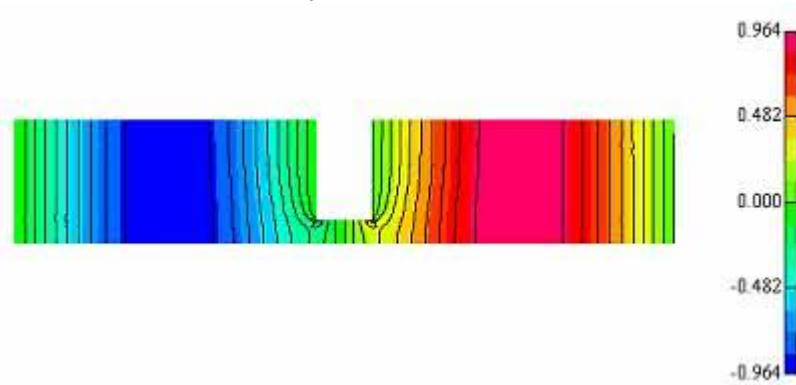
Iránycsatoló sematikus ábrája



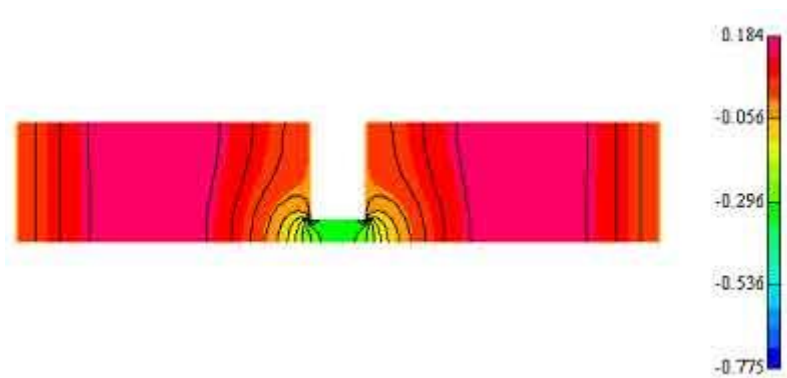
Térerősség-eloszlás a három alap módusra:
(R220/2 iránycsatoló, $s=2\text{mm}$, $d=0.8\text{ mm}$, $\beta=600/\text{m}$)



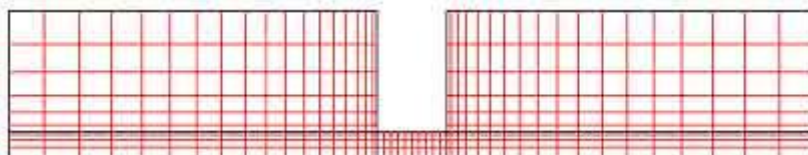
TE10 módus, E_y eloszlása a keresztmetszet mentén



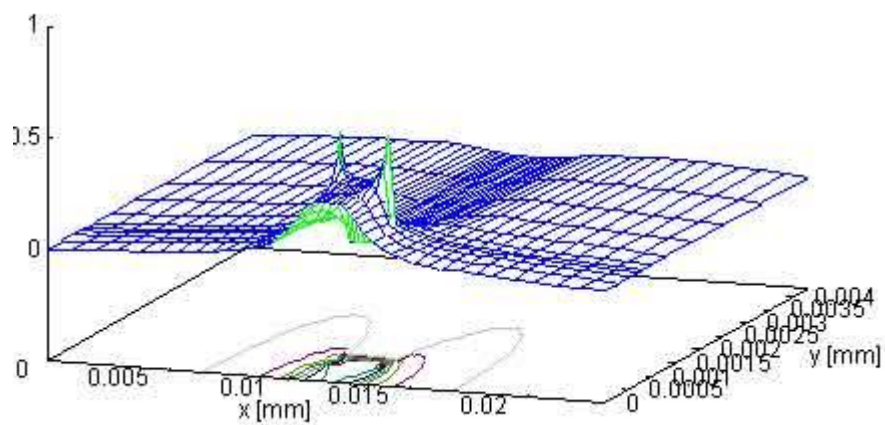
TE20 módus, E_y eloszlása a keresztmetszet mentén



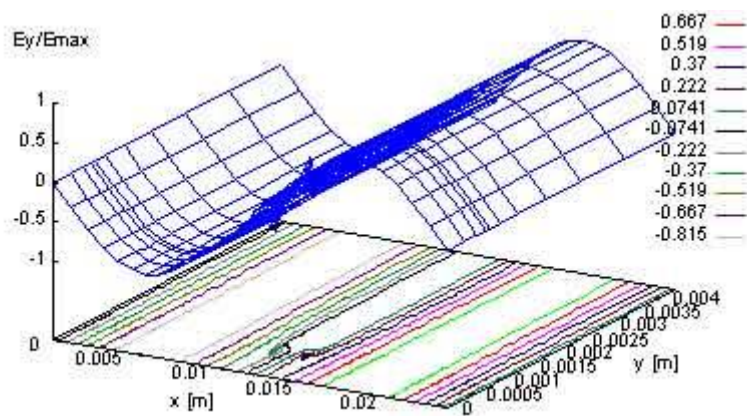
TE30 módus, E_y eloszlása a keresztmetszet mentén



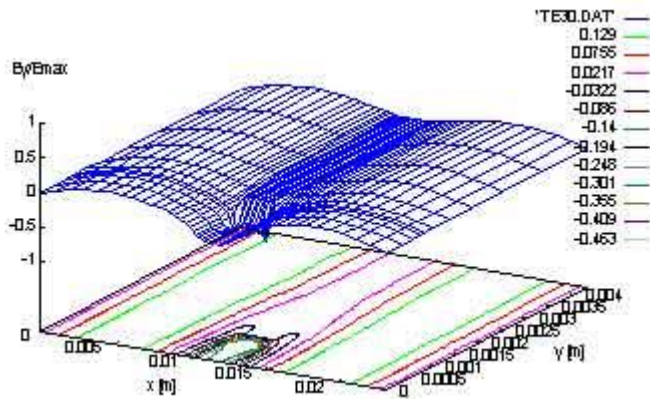
A számításhoz használt véges elem struktúra



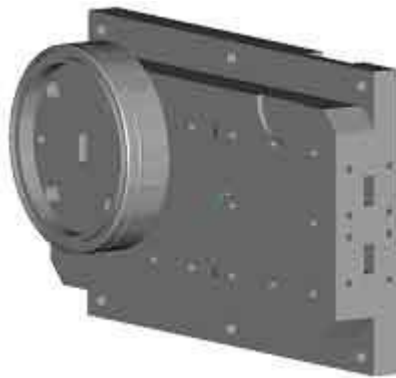
TE10 módus, E_y eloszlása a keresztmetszet mentén



TE20 módus, E_y eloszlása a keresztmetszet mentén



TE30 módus, E_y eloszlása a keresztmetszet mentén



Íránycsatló adapterekkel szerelve

A KÖZVETLENÜL SZERELHETŐ 1+0 RENDSZER ELŐNYEI

- A konstrukció rendkívül kompakt
- Külön tartószerkezetre nincs szükség
- Flexibilis hullámvezetőre nincs szükség
- A csatlakozók száma minimális
- A beiktatási csillapítás zérus
- A reflexiós csillapítást az antenna szabja meg
- A rendszer mechanikailag jól védett
- A kültéri egység nagyon egyszerűen és gyorsan kicserélhető

-
- A balos-jobbos szerelhetőség biztosítja az optimális telepítést

MELEG TARTALÉKOLT (1+1) EGYPOLARIZÁCIÓS DIREKT SZERELT ANTENNARENDSZEREK ELŐNYEI

- Nagyon kompakt konstrukció
- Drasztikusan csökkentett szerelési idő
- Kis beiktatási csillapítás (a hullámvezetők hossza minimális)
- Kis reflexiós csillapítás (a csatlakozók száma minimális)
- Kis súly (nincs szükség külön tartószerkezetekre a kültéri egységekhez és a flexibilis hullámvezetőkhez).
- Kis térfogat (nagyon kompakt tartószerkezet)
- Rendkívül nagy megbízhatóság (a csatlakozók - karimák- száma minimális, a teljes hullámvezető rendszer védett).
- A konstrukció univerzális (opció). Egy darab kültéri egység felszerelhető a T alakú tartószerkezet helyére (1+0 rendszer az 1+1 rendszer helyett vagy fordítva).
- Az antenna polarizációja változtatható és finoman beállítható a reflektor mögött (opció) elhelyezkedő polár rotor (PR) segítségével. (a kültéri egységeket nem kell leszerelni!)
- A hibás kültéri egység néhány percen belül kicserélhető.

KÉTPOLARIZÁCIÓS (DUPLEX) (2+0) DIREKT SZERELT ANTENNARENDSZEREK ELŐNYEI

- Nagyon kompakt konstrukció
- Drasztikusan csökkentett szerelési idő
- Kis beiktatási csillapítás (a hullámvezetők hossza minimális)
- Kis reflexiós csillapítás (a csatlakozók száma minimális)
- Kis súly (nincs szükség külön tartószerkezetekre a kültéri egységekhez és a flexibilis hullámvezetőkhez).
- Kis térfogat (nagyon kompakt tartószerkezet)
- Rendkívül nagy megbízhatóság (a csatlakozók - karimák- száma minimális, a teljes hullámvezető rendszer védett).
- Az antenna polarizációja finoman beállítható a reflektor mögött (a kültéri egységeket nem kell leszerelni!)
- A hibás kültéri egység néhány percen belül kicserélhető.

MELEG TARTALÉKOLT KÉT POLARIZÁCIÓS (DUPLEX) [2X(1+1)] RENDSZER MŰSZAKI LEÍRÁSA

Antennacsatlód

Előnyök:

- A kapacitás kétszerezhető az antennák számának növelése nélkül
- Az antenna helyfoglalása minimális (1 db antenna kettő helyett)
- A szélterhelés kb. 50%-kal kisebb
- Egy antennát két szolgáltató is használhat (pl. templomtorony, ahol nem fér el több antenna)
- Mindkét polarizációban meleg tartalékolt rendszer üzemel (a megbízhatóság jelentős mértékben nő)
- A rádió adó-vevő berendezések könnyen felszerelhetők és cserélhetők (meghibásodás)
- A négy berendezés az antenna mögött minimális helyet foglal (rendkívül kompakt konstrukció)
- Célszerű ezt rendelni, mert a jövőben bármikor kétszerezhető a kapacitás utólagos engedélyek megszerzése nélkül
- Rendszertechnikai megfontolások alapján választani lehet 3 dB, 6 dB illetve 10 dB csatlósú iránycsatló rendszerek közül (ezek a rendszeren belül tetszőlegesen kombinálhatók)

Pl. HPA 0.8 D 180 FR-4P-3V-6H antenna esetében egy High Performance, kétpolarizációs, két iránycsatlóval (egy 3 dB-es és egy 6 dB-es) rendelkező antenna, amely 4 db 18 GHz-es frekvenciasávú berendezés közvetlen felszerelésére alkalmas.

Lehetséges fejlesztési forgatókönyv

Fázis	Berendezések száma	Kapacitás (Mbps)	Kiesési idő/év	Polarizáció
1.	1	34	8,4 perc	V
2. (hot-standby)	2	34	0,003 mp	V
3.	3	2x34	8,4 perc	H
4. (hot-standby)	4	2x34	0,003 perc	H

A számításoknál a következő feltételekkel éltünk:

$$MTBF = 2,5 * 10^5 \text{ óra}$$

$$MTTR = 4 \text{ óra}$$

A berendezések közötti átkapcsolást végző áramkört tökéletesen megbízhatónak vettük.

A kiesési idő számításánál a tápegységek és az antenna meghibásodását figyelmen kívül hagytuk, és nem foglalkoztunk a terjedési viszonyok változása

következtében fellépő jelenségekkel és egyéb okokkal (fading, eső csillapítás, a torony összeomlása, szándékos rongálás stb.).

Egy jól megtervezett összeköttetésnél a kiesési idő valószínűleg alapvetően a rádió berendezés megbízhatóságától függ.

Az MTTR értéke jelentős mértékben befolyásolja az egy berendezéssel üzemeltetett összeköttetés megbízhatóságát, hot-standby rendszer esetén azonban hatása elhanyagolható.

pl. MTBF = 2,5 - 105 óra

MTTR = 100 óra

Egy rádióberendezés: U (kiesési idő) = 3,5 óra/év

Hot-standby rendszer: U (kiesési idő) = 0.05 mp/év

MELEGTARTALÉKOLT, KÉTPOLARIZÁCIÓS 2X (1+1)

RENDSZER MŰSZAKI LEÍRÁSA

A rendszer részei

High Performance kétpolarizációs antenna típus, téglalap keresztmetszetű hullámvezető könyök (2db)

- Iránycsatoló (3 vagy 6 dB csatolás) (2db)
- Adapterek a rádióberendezésekhez
- Tartószerkezet (alakú)
- Beállító szerelvények (azimut + eleváció)
- Polarizációs finombeállító (a teljes tartószerkezet a berendezéssel együtt az antenna sugárzási tengelyen kívül $\pm 2,55^\circ$ os szögtartományon belül finoman beállítható)

A rendszer műszaki előnyei

Kétszeres kapacitás (pl. 2x34 Mbps) 5 nagyságrenddel nagyobb megbízhatóság:

- Különlegesen kompakt konstrukció
- Drasztikusan lecsökkentett szerelésidő
- Kicsi beiktatási csillapítás (a hullámvezetők hossza minimális, nincs szükség flexibilis hullámvezetőre)
- Kis reflexiós csillapítás (a csatlakozások száma minimális)
- Könnyű tartószerkezet (nincs szükség a 4 db berendezéshez külön tartószerkezetekre)
- Kis térfogat
- Rendkívül nagy mechanikai bízhatóság

- (a csatlakozók száma minimális, a hullámvezető rendszer védett)
- Univerzális konstrukció is rendelkezésre áll, 2+, rendszer szerelhető a T alakú tartórendszer helyére (2+0 rendszer a 2 x (1+1) rendszer helyett).

Bármely meghibásodott berendezés percekben belül kicserélhető.

MELEG TARTALÉKOLT (3+1) VAGY TARTALÉKOLATLAN (4+0) RENDSZEREK MŰSZAKI LEÍRÁSA

A rendszer részei

- High Performance antenna
- Polarizáció forgató rendszer
- Polarizáció forgató szerelvény (a polarizáció forgató lemez helyett)
- Iránycsatolók (1db 3 dB-es, 2db 3 vagy 6 dB-es)
- H-síkú könyökök (2db)
- Adapterek a rádióberendezésekhez (4db)
- Tartószerkezet
- Beállító mechanikus (eleváció, azimut)



HPA 0.6 S ... FR-2V3-3 (6)

0.6 m átmérőjű High Performance Antenna Pasolink V3 kültéri egységekkel

Ez a konstrukció rendelkezésre áll a
7, 13, 15, 18, 23, 26, 38 GHz frekvenciasávokban



HPA 1.2-D -130 FR-4V3-3

1.2 m átmérőjű High Performance Antenna 4db Pasolink V3 kültéri egységgel

Ez a konstrukció rendelkezésre áll a
7, 13, 15, 18, 23, 26, 38 GHz frekvenciasávokban

**AZ ERDŐK TŰZVÉDELME SZOLGÁLÓ, TŰZVÉDELMI
KOCKAZAT ELEMZŐ ÉS DÖNTÉSTÁMOGATÓ
INFORMATIKAI RENDSZER.**

Az erdőtűzek hazánkban évről-évre több százmilliós forintos, természeti és gazdasági kárt okoznak. Az erdőtűzek alkalmával az erdőterületek elpusztulásából eredő kárérték és a tűz oltására fordított költség a kifejlődött tűlevelű erdők esetében a legmagasabb. Egy-egy kiterjedt erdőtűz oltása a megközelítés nehézségei, a nagy erő-eszköz és oltóanyag igény következtében több hétig is eltarthat. Költségigénye rendkívül magas és jelentős hatással van a környező lakosság életvitelére. A tűzkárt szenvedett erdőterület rehabilitációja hosszú éveket igényel és költségigényes.

2002. évben a Kormányzati Koordinációs Bizottság Titkársága által vezetett projekt keretében olyan kockázat elemző, előrejelző és döntéstámogató informatikai rendszert javasoltunk megvalósítani, amely megfelelő támogatást nyújt az erdők védelmére, adott időszakban jelzi az erdőterületek tűz-veszélyeztetettségének mértékét, javaslatokat ad az intézkedésekre, támogatja a beavatkozások koordinálását.

Tekintsük át hogyan alakul ki erdőtűz?

Az erdőtűz keletkezésében közrejátszanak:

- **Gyújtóforrás jelenléte;**

A vizsgálatok eredményei azt mutatják, hogy az erdőtűzek keletkezéséhez az esetek döntő többségében az emberi tényezők (gondatlanság, felelőtlenység, szándékosság) vezetnek. Kétségtelenül előfordul, hogy meteorológiai tényezők (pl. villámcsapás) is okoznak erdőtűzet, de ezek aránya igen alacsony, 1-2 %, hiszen a zivatarfelhőkhöz társuló csapadék a legtöbb esetben hamar kioltja a lángokat.

- **Elegendő mennyiségű, természetes eredetű, éghető anyag;**

Az éghető anyag mennyiségét nagyobb mértékben befolyásolják az erdészeti tényezők. Így többek között a telepítés, a művelés módja, a fafaj biológiai jellemzői, az állományszerkezet, fenológiai fázis és az erdő szerves hulladéktól való megtisztítottsága.

- **Az éghető szerves anyag nedvességét befolyásoló meteorológiai tényezők;**

Ide sorolandó a levegő hőmérséklete, növényzet-, a talaj-, a levegő víz, illetve páratartalma, szélerősség. Hazánkban az erdőtüzek kialakulásához kedvező feltételek többnyire hosszantartó csapadékszegény időszak után állnak fenn.

Az erdőtüzek esetében a gyújtóforrás jelenléte (emberi tényező) intézkedésekkel befolyásolható, visszaszorítható, valamint az éghető anyag mennyisége egyrészt szabályozható, másrészt az intézkedések kialakításánál figyelembe vett adat (tűzvédelmi besorolás).

A fentiek alapján látszik, hogy a meteorológiai tényezők azok, amelyek mérhetők, de nem befolyásolhatók, de nagy szerepük van az erdők tűzvédelmi veszélyeztetettségének kialakulásában.

Az Országos Meteorológiai Szolgálatnál korábban készített tanulmányban (Bussay Attila – Szinell Csaba – Szentimrey Tamás: Az aszály magyarországi előfordulásainak vizsgálata és mérhetősége 1999.) megállapították a meteorológiai tényezők jelentős befolyásoló hatását.

A tanulmány a hazánkban 1931-1998. közötti időszakban keletkezett erdőtüzeket vizsgálta, abból a szempontból, hogy az ebben az időszakban, a tüzesetek közelében mért meteorológiai adatok milyenek voltak, a meteorológiai tényezők hogyan befolyásolhatták a tüzesetek kialakulását. Öt, a külföldi gyakorlatban használt ún. erdőtűz index magyarországi alkalmazhatóságát vizsgálták elemezve, hogy az egyes számított indexek a megtörtént tüzesetek területére milyen értékeket mutattak, milyen mértékben hathattak közre a meteorológiai tényezők a tűz kialakulásában. Az indexek „jóságának” vizsgálatánál két feltételt szabtak. Az egyik, hogy lehetőség szerint minél kevesebb legyen a „vakriasztás”, azaz a magas veszélyeztetettségi kategória előfordulása minimális legyen, ugyanakkor a bekövetkezett tüzesetek magas indexű napokon következzenek be a maximális számban és az éves statisztika is a magasabb erdőtűz indexű években legyen magasabb.

A tűzvédelmi kockázat-elemző és döntés-támogató rendszer projektjének kidolgozása során a francia erdőtűz index adatot (input), a tűzvédelmi besorolásból származtatott számadatot (output) használtuk. Ezzel megvalósíthatjuk azt a rendszert, mely a vonatkozó jogszabályok szerint kezelt, de a nem befolyásolható tényező (meteorológiai viszonyok) hatásának kitett védendő erdőterület (éghető anyag) tűz általi veszélyeztetettségének mértékét meghatározva, intézkedések megtételét ajánlja fel arra, hogy a gyújtóforrás jelenlétének lehetőségét csökkentsük, ezáltal a leggyakoribb befolyásoló körülményt (emberi

közrehatás) távol tartsuk. További szolgáltatásként jelentkezik, hogy egy, a megtett intézkedések ellenére keletkezett tűz oltásához az adatbázisból az információk (megközelítés, eszközök, oltóanyag, stb.) kinyerhetők.

A számítás menete:

Az un. francia index 0 és 5 körüli értéket vesz fel, ahol 1,5 alatti értékek nagyon alacsony, 1,5 és 2 között alacsony, 2,01 és 3,50 között közepes, 3,51 feletti értékek nagyon magas tűzveszélyt mutatnak. Az index csak a terület nedvességének értékét mutatja, de nem veszi számításba az adott területen lévő vegetáció és terület jellemzőit, amelyet a 12/1997. (II.26.) BM rendelet alapján készített veszélyeztetettségi besorolás tartalmaz.

A tényleges veszély mértékének meghatározásához rendelkezésre álló, felhasználható adatokból (francia index és a veszélyeztetettségi besorolás) kell olyan adatot származtatni, mely egy széles tartományban ad eredményt.

A projekt kidolgozásában résztvevők a 0-1000 skálát tartották a legmegfelelőbbnek, mivel az, ezen kapott eredmény alkalmazható differenciáltságot eredményez és biztosítja azt, hogy az egyes veszélyeztetettségi kategóriákhoz tartozó párolgási index értékek széthúzhatók és megfelelően adják vissza a tényleges veszélyeztetettséget, de minimálisra csökkenti a un. vak-riasztások számát, amikor alacsony index érték is magas tűzveszély értéket ad.

Az adatok kitűzött skálára történő feszítésénél azt az elvet alkalmaztuk, hogy a legnagyobb értékű párolgási index (3,51 felett), a legnagyobb veszélyeztetettségű területen (1) a legmagasabb veszélyeztetettséghez tartozó intézkedéseket indukáló számadatot határozza meg, de alacsony párolgási index értéknél se javasoljon aránytalanul magas beavatkozást kiváltó számértékeket.

A számítás az alábbi képlettel történik: $T_v = I \times V + M$, ahol

T_v : tűzveszélyesség

I : francia index

V : veszélyeztetettségi normáló tényező

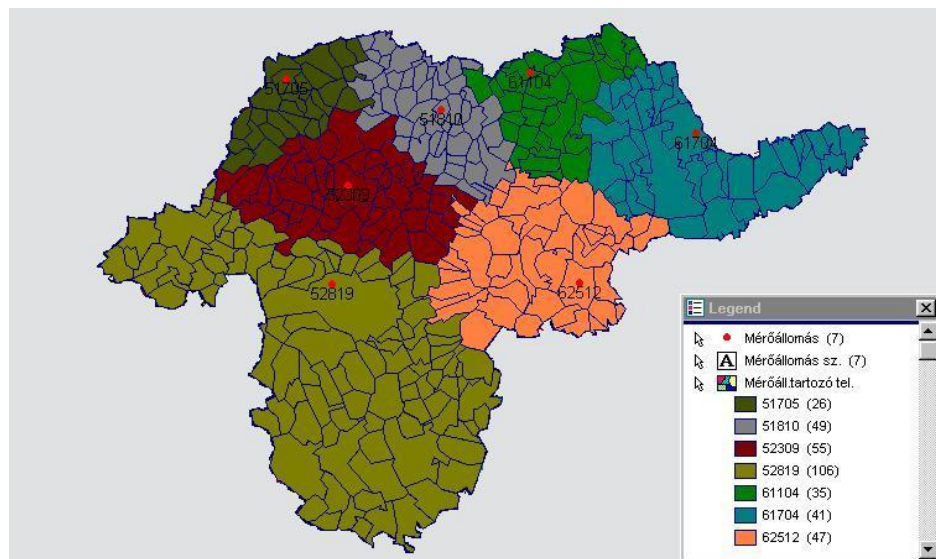
M : veszélyeztetettségi módosító tényező

A számításhoz használt adatok származása:

Erdők veszélyeztetettségi adatai: az Állami Erdészeti Szolgálat által szolgáltatott adatokat használtuk fel. Az egyes erdőterületek besorolása az Országos Erdő Adattárban még nem áll rendelkezésre, az egyes települések

közigazgatási területének besorolását tudták rendelkezésünkre bocsátani, így ezt használtuk fel.

Francia index adat: megállapodás alapján az Országos Meteorológiai Szolgálat szolgáltatja, az általa működtetett állomások mérései alapján. A projektnél mintaterületként használt Borsod-Abaúj-Zemplén megyében 7 meteorológiai állomás működik. Az ezek által szolgáltatott adatokat területi, domborzati tulajdonságok alapján rendeltük hozzá az egyes településekhez.



A meteorológiai mérőállomások és a hozzá tartozó területek

A felhasznált alkalmazások:

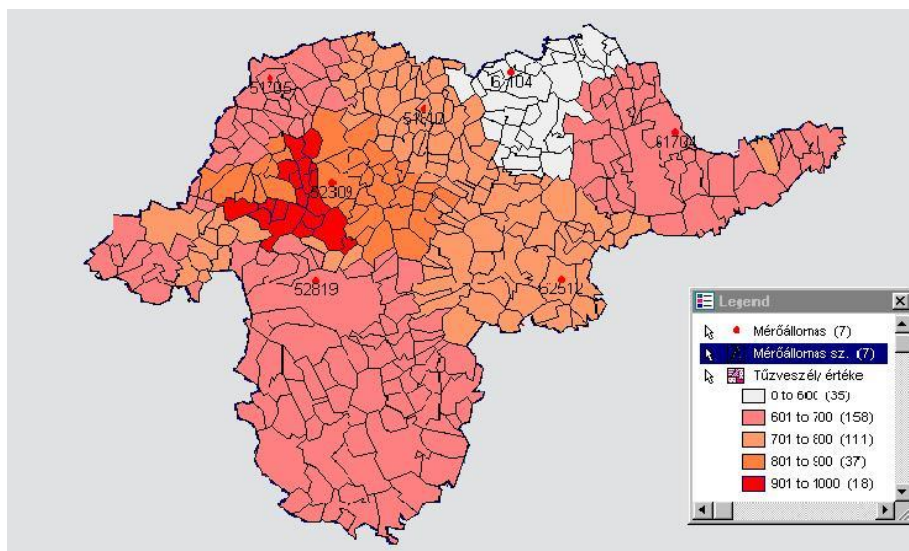
A rendszer elé támasztott követelményekhez igazodva (vizuális megjeleníthetőség, nyomtathatóság), valamint a mintaterület domborzati tagoltsága miatt figyelembe véve, hogy az erdők besorolási adatai településekhez rendelve készült el, térinformatikai alkalmazást a GeoMedia Professional 4.0 alkalmaztuk, mely alkalmas MS Access adatbázis kezelésre és képes együttműködni más térinformatikai alkalmazásokkal. Így az esetlegesen más alkalmazásokkal dolgozó adatszolgáltatók (Országos Meteorológiai Szolgálat, Állami Erdészeti Szolgálat) adatainak közvetlen használhatósága megoldott. Az alkalmazás mind képernyős megjelenítésre, elemzésre, mind azok nyomtatott formátumú elkészítésére alkalmas.

Az elkészített adatbeviteli felülettel az adatbázis megfelelő mezőjébe rögzített, számított tűzveszélyességi érték alapján automatikusan készült tematikus térkép adja a vizuális információt, a beépített lekérdezések biztosítják az egyes tűzveszélyességi érték-sávokhoz tartozó rekordok lekérdezését, az adatok, a javasolt intézkedések megjelenítését, nyomtatását.

A rendszer működtetése:

A rendszer napi működtetést igényel, így biztosítható a folyamatok követése.

A kezelő a rendelkezésre álló beviteli mező segítségével rögzíti a meteorológiai állomásokról érkező adatokat. Ez – a mintaterületen – 7 adat bevitelét jelenti. A nyugtázás után futtatja az 5 lekérdezést, a kívánt adatokat, intézkedési sorokat megtekinti, szükség esetén nyomtatja, továbbítja azokat. A vezető az adatok alapján elrendeli az intézkedések megtételét. Az intézkedések megtételére jogosultak az adatbázisban, a kinyert adatokban szerepelnek.



Az adatok alapján készült tematikus térkép.

Térinformatika alkalmazása a projektben:

Az alkalmazással szemben támasztott egyik igény a vizuális információ szolgáltatás, tehát kézenfekvő volt, valamilyen térinformatikai alkalmazás felhasználása volt. Univerzalitása miatt esett a GeoMedia-ra a választás. A

tematikus térkép (tűz megelőzési feladatok segítése) készítésén túlmenően a tűzoltói beavatkozásokhoz értékes adatok gyűjtésével is tud segítséget adni, megfelelően feltöltött adatbázisok esetén:

- A tűz által érintett terület jellemzői (fa fajták, domborzat, települések adatai)
- Felvonulási útvonalak kijelölése,
- Vízszerzési helyek, kapacitás gyűjtése,
- Szerszámbázisok, és azok felszereltsége,
- Erő-, eszköznyilvántartás, stb.

A projekt az elmúlt év nyarán elkészült. Kipróbálásra a Borsod-Abaúj-Zemplén megyei Katasztrófavédelmi Igazgatóság részére került átadásra. További sorsáról nincs információnk.

RÁDIÓBERENDEZÉSEK MINŐSÉGI MEGFELELŐSÉGE

Európai uniós követelmények

Az Európai Unióba való belépésünk folyamatában elengedhetlenné vált, hogy a magyar jogalkotásban EU-konform szabályozások jelenjenek meg.

A rádiós végberendezések alapvető követelményeinek műszaki jellemzőit többek között az ún. harmonizált szabványok határozzák meg, de ezek használatát nem tették kötelezővé. A harmonizált szabványok és az azokhoz kapcsolódó egyéb európai szabványok betartása elősegíti a rádiós berendezések EU tagországokon belüli kereskedelmi forgalmazását.

A harmonizált szabványok a gyártók, forgalmazók számára olyan műszaki előírásokat tartalmaznak, amelyeket előírnak, hogyan kell a rádiós berendezést megtervezni, legyártani, letesztelni és a műszaki követelményeknek való megfelelést igazolni (megfelelőségi igazolás).

Az EU tagállamaiban 2000. áprilisában lépett érvénybe a rádióberendezésekről és távközlő végberendezésekről szóló R&TTE irányelv, amely közös alapokra helyezte a berendezések piacon való megjelenésének, szabad forgalmazásának és üzembe helyezésének elveit.

Magyar jogszabályi környezet

Az R&TTE irányelvet kisebb eltérésekkel a *rádióberendezésekről és a távközlő végberendezésekről, valamint azok megfelelőségéről* szóló 3/2001 MeHVM rendelet tartalmazza. A rendeletben leírtak szerint a berendezések piacra vitelének alapvető feltétele nem egy bonyolult és költséges engedélyezési eljárás lefolytatása, hanem annak igazolása, hogy forgalmazott rádióberendezés megfelel az előírt alapvető követelményeknek.

A megfelelést a gyártónak kell garantálni, illetve igazolni, amelyet egy megfelelőségi nyilatkozatban kell közzétennie. A berendezések piaci forgalmazásának további feltételeit az alábbi magyar jogszabályok és szabványok határozzák meg:

- 79/1997. IKIM rendelet az egyes villamosági termékek biztonsági követelményeiről és azoknak való megfelelőség értékeléséről;
- 208/1999. Kormányrendelet az egységes megfelelőségi jelölés használatáról;
- 31/1999. GM-KHVM rendelet az elektromágneses összeférhetőségről;
- 24/2001. MeHVM rendelet a hírközlési hatóság piacfelügyeleti tevékenységéről;
- 27/2001. MeHVM rendelet egyes rádióberendezések alapvető követelményeinek megállapításáról;
- MSZ 25051 Szabvány a megfelelőség igazolási modulokról

Alapvető követelmények

Minden forgalmazásra kerülő rádióberendezésre a következő követelmények vonatkoznak:

- A berendezések nem veszélyeztethetik az emberi életet, a felhasználók egészségét és testi épségét (79/1997. IKIM rendelet);
- A berendezéseknek meg kell felelnie az elektromágneses összeférhetőség követelményeinek (31/1999. GM-KHVM rendelet);
- A fentieken túlmenően a berendezést úgy kell kialakítani, hogy az a lehető leggazdaságosabban használja fel a korlátozott frekvenciaspektrumot.

A frekvenciaspektrum felhasználása a nemzeti és nemzetközi spektrumok részletes leírása alapján történhet. A sávok felhasználása esetén biztosítani kell, hogy a felhasználók egymást ne zavarják. Ennek egyik biztosítója a harmonizált szabványok alkalmazása.

A harmonizált szabványok magyarországi bevezetése csak kis késéssel követi az európaiakat. Jelenleg több mint 150, a 3/2001 rendelet hatálya alá tartozó harmonizált szabvány került Magyarországon nyilvántartásba. Egyes rádióberendezések esetében lehetőség van egyszerre több harmonizált szabvány, vagy egy harmonizált szabvány egyes részeinek a használatára is.

Abban az esetben, ha egy adott berendezéstípusra nincs harmonizált szabvány, egyéb szabványok alkalmazására kerülhet sor. Különleges esetekben – a berendezés felhasználásától függően - a fent leírtakon kívül további követelmények írhatók elő. Ilyenek alkalmazások lehetnek például a készenléti és segélyszolgálatok, a berendezések használata hátrányos helyzetűek számára (pl. hallás- és látássérültek), stb.

A megfelelés igazolása

Az európai irányelvek és a bevezetett magyar jogszabályok kötelezően előírják a CE megfelelési jelölés használatát, amit a gyártó akkor helyezhet el a termékén, ha az megfelel az alapvető követelményeknek. A szabályozások ugyancsak előírják a berendezés osztályba sorolásának feltüntetését a berendezésen, amennyiben ez szükséges.

A rádióberendezéseket és távközlő végberendezéseket az R&TTE direktíva szerint jelenleg két osztályba sorolják. Az első osztályba azok a berendezések tartoznak, amelyek CE jelöléssel és megfelelési nyilatkozattal forgalomba hozhatók és üzembe helyezhetők. Erre az osztályra nem kell osztályazonosítót alkalmazni. A második csoportba tartozó berendezések esetében a terméken osztályazonosító jelet, egy körbe foglalt felkiáltójelet (alert jelet) kell elhelyezni. A jelet fel kell tüntetni a használati/kezelési útmutatóban, valamint a termék csomagolásán is.

A rádióberendezés megfelelési nyilatkozatában a gyártó kinyilvánítja, hogy az megfelel az alapvető követelményeknek. A nyilatkozatot a Magyaror-

szágon forgalmazott termék esetében magyar nyelven, írásban kell megtenni, és annak másolatát minden forgalomba lévő termékhez mellékelni kell. A nyilatkozatot és a nyilatkozat alapját képező dokumentumokat az utolsó forgalomba hozott berendezés piacra vitelének időpontjától számítva a gyártónak 10 évig kell megőriznie.

A megfelelőségi nyilatkozat elkészítéséért, és a CE megfelelőségi jel berendezésen való elhelyezéséért a gyártó vagy annak meghatalmazott képviselője a felelős. A 3/2001 MeHVM rendelet alapján gyártónak számít az a gazdálkodó szervezet, amely felel a készülék tervezéséért, gyártásáért, csomagolásáért, jelöléséért és forgalomba hozataláért, függetlenül attól, hogy ezeket a feladatokat saját maga vagy megbízásából más végzi. Gyártónak tekintendő az is, aki ugyancsak forgalomba hozatal céljából jelentős, az alapvető követelményeket befolyásoló változtatásokat vagy bővítéseket végez meglévő készülékeken, vagy azokból új készüléket állít elő (például a berendezéshez nem az előírt antennát csatlakoztatja). Ha a gyártó székhelye nem Magyarország területén van, a készülék importálója tekintendő gyártónak.

A megfelelőségi nyilatkozatnak a következőket kell tartalmaznia:

- gyártó megnevezése és címe;
- berendezés rendeltetése, típusa, egyedi azonosításra alkalmas jelölése ;
- alkalmazott jogszabályok, szabványok felsorolása, amelynek a berendezés megfelel;
- ha volt közreműködő tanúsító szervezet, annak megjelölése;
- a gyártó hiteles aláírása.

A megfelelőség értékelése

A gyártó által tett megfelelőségi nyilatkozat és a berendezésen elhelyezett CE jelölés nem minden esetben fogadható el a megfelelőség igazolására. A megfelelőség értékelési eljárásokat a 3/2001 MeHVM rendelet mellékletei írják le. A megfelelőség értékelése az MSZ 25051 szabvány alapján történik, amelyben az értékelés alapját az „A”, „Aa” és „H” modulok, valamint a műszaki konstrukciós dokumentáció („TCF”) képezik..

1. Az „A” modul minden vezetékes és rádióvevő berendezés esetén alkalmazható. Ebben az esetben a gyártó gondoskodik a CE megfelelőségi jel és az osztályjel elhelyezéséről, a használati/kezelési útmutató és a megfelelőségi nyilatkozat elkészítéséről, valamint a berendezés dokumentációinak és alapvető mérési eredményeinek elérhetőségéről.
2. Az „Aa” modult olyan esetekben kell alkalmazni, amikor a rádióadó berendezések harmonizált szabványokat alkalmaznak.
 - a.) Ha a szabvány leírja az alapvető rádiós méréseket, a gyártó a méréseket maga is elvégezheti és az „A” modulhoz hasonló módon nyilatkozhat a megfelelőségről.

-
- b.) Abban az esetben, ha a szabvány nem írja elő az alapvető méréseket, akkor egy tanúsító szervezet (Notified Body) beavatkozása szükséges, aki előírja az alapvető méréseket, és azok elvégzésének módját. A gyártó ilyenkor a berendezésen köteles feltüntetni a tanúsító szervezet számát is.
3. A „TCF” alkalmazása esetén az „Aa” modul b.) pontjában leírtak az érvényesek, és olyan esetekben lehet alkalmazni, amikor a rádióadó-berendezés nem harmonizált szabványok alapján működik. Ilyenkor a berendezésre vonatkozó műszaki konstrukciós dokumentációt (TCF) egy vagy több tanúsító szervezetnek kell benyújtani.
4. A „H” modult (teljes minőségbiztosítás) minden fenti esetben lehet alkalmazni. Ebben az esetben a gyártónak tanúsított minőségügyi rendszert kell működtetnie (pl. ISO) a tervezés, a gyártás, a tesztelés és ellenőrzés folyamataira és a megfelelőségi értékelést tanúsító szervezet felügyelete alatt kell elvégezni. A gyártói kötelezettségek az 'A' modulnál leírtak szerint érvényesek, de a CE jelölés után fel kell tüntetni a tanúsító szervezet számát is.

INFORMATIKAI PROJEKTEK SAJÁTOSSÁGAI ÉS LEHETŐSÉGEI A VÉDELMI SZFÉRÁBAN (EGY KÍVÜLÁLLÓ VÉLEMÉNYE...)

*A rendszerváltozás után történt haderő átalakítások, a kormányzati takaré-
kossági intézkedések miatt a védelmi szféra egyes ágai szinte alig rendelkeznek
saját, professzionális informatikai fejlesztő kapacitással. Ez azt jelenti, hogy –
előre kidolgozott stratégiák alapján – külső erőforrásokat kell igénybe venni
az információs rendszerek fejlesztéséhez. A rendszerelemek kiválasztásánál, a
rendszerek kialakításánál, életre keltésénél kiemelt szerepet kaphatnak a pro-
jektmenedzsment ismeretek.*

*A profitorientált vállalatok nagy része is külső megoldás-szállítótól szerzi
be vállalat számára szükséges informatikai megoldásokat. Az itt felhalmozott
projektvezetési ismeretek (módszertanok, ajánlások) egy része a védelmi szfé-
rában is felhasználható. A cikk megpróbálja áttekinteni a két terület informati-
kai projektjeinek hasonló és eltérő elemeit és vizsgálja, hogy milyen tapaszta-
latok vehetők át az üzleti életből.*

1. Lehetőségek az informatikai projektmenedzsmentben (az üzle- ti szféra által használt „eszközök”)

„**Informatikai projekt** alatt az adott szervezet stratégiai céljainak megvaló-
sítása érdekében kialakított projektet értünk, amely az elérendő projektered-
mény tekintetében informatikai megoldások bevezetését, fejlesztését, illetve
továbbfejlesztését valósítja meg...” (Görög-Ternyik, 2001, p.25.)

Egyre gyakoribb, hogy a profitorientált vállalatok a profiljukba nem illő te-
vékenységeket külső vállalkozókkal végeztetik el. Igaz ez az információs
rendszerek kiválasztására és bevezetésére, sőt sok esetben a működtetésére is.
Gondoljunk csak az egyre terjedő informatikai outsourcing-ra vagy az on-line
alkalmazásszolgáltatásra (Application Service Providing). Az informatikai
projektek célja – a bevezetésben idézett definíció alapján is – működő infor-
mációs rendszerek létrehozása vagy továbbfejlesztése.

Mit értünk **információs rendszer** alatt? A Magyar Nagylexikon meghatáro-
zása a következő:

„Információs rendszer azoknak az információs egységeknek az összetartozó
együttese, amelyek szakmailag, területileg vagy más szempontok szerint egy-
séges elvek, munkamódszerek alapján együttműködnek, működő szervezetet
alkotnak. Az információs rendszer az információ megszerzésével, rögzítésével
létrehozásával, tárolásával, kikeresésével, feldolgozásával, átalakításával, to-

vábbításával, megjelenítésével és megsemmisítésével foglalkozik.” (Magyar Nagylexikon, kilencedik kötet, 1999, p. 870.)

Halassy Béla ezzel összecsengően, de rövidebben adja meg az információs rendszer fogalmát.

„Az információs rendszer

- adatoknak (információknak);
- a velük kapcsolatos információs eseményeknek;
- a rajtuk végrehajtott információs tevékenységeknek;
- az előzőekkel kapcsolatos **erőforrásoknak**;
- az információk felhasználóinak;
- ill. a fentieket szabályozó szabványoknak és eljárásoknak szervezett együttese.” (Halassy, 1996, p. 43.)

A védelmi szférában ennél részletesebb meghatározás született. „Az **információs rendszerek** szűkebb értelemben funkcionálisan összetartozó, egységes szabályozás hatálya alá tartozó, szervezett információs tevékenységek, folyamatok. Tágabb értelemben az egyes információs rendszerek részét képezik az általuk kezelt információk, az információs tevékenységeket végrehajtó szereplők és a végrehajtás során felhasznált erőforrások is. Egy szervezetben folyó információs tevékenységek összessége, a szervezeti információfeldolgozás számos, egymással összekapcsolódó információs rendszerbe szerveződik.” (Munk, 2002, p.140.)

Az információs rendszerek **erőforrásainak** a hardver és a szoftver eszközök, a rendszer felállításához, bevezetéséhez szükséges szervezési ismereteket (orgver) valamint az azt kezelő személyzetet és az információs rendszerbe kerülő adatokat tekinthetjük (Kacsukné – Kiss, 1999, p.74.). Az előbbieket (hardver, szoftver, orgver) „megvásárolhatók”, az utóbbiakat a szervezet általában saját maga biztosítja.

Vannak, akik az erőforrásokat csak működő információs rendszerekre értik és feldolgozott adatokat nem sorolják ebbe a körbe. Véleményem szerint a most következő definíció ettől függetlenül nincs ellentétben az előző meghatározással. „Az **információs erőforrások** közé az információszerzést, tárolást, továbbítást, feldolgozást és megjelenítést végző – számítástechnikai, híradástechnikai és más – eszközrendszerek, eszközök; a tevékenységekhez szükséges segédanyagok; valamint a különböző információhordozók tartoznak. Az egyes információs erőforrások az információs szintér különböző szereplőinek birtokában, kezelésében, működtetésében vannak és jellegükből, valamint képességeikből következően általában több – akár egy időben végbemenő – információs tevékenység végrehajtása során használhatók fel.” (Munk, 2002, p.142.)

A vállalatok is úgy szeretnék jól működő információs rendszerekhez jutni, hogy ehhez ne kelljen hosszú távra nagy számú informatikai szakembert,

valamint projekt menedzsert alkalmazni. Ezért „kulcsrakész” megoldásokat⁴⁸ vásárolnak vagy az informatikai projekt idejére külső tanácsadókat alkalmaznak, akik koordinálják a bevezetést. Ennek célja, hogy a vállalat a lehető legkisebb fennakadásokkal lássa el profiljába tartozó termelő és/vagy szolgáltató tevékenységét.

A piacon beszerezhető vállalati információs rendszerek megvásárolható részei⁴⁹ általában a legjobb vállalati gyakorlatot („best practice”) tükrözik. A cégek – nem túl nagy kockázatot vállalva – ennek megfelelően alakítják át belső és külső folyamataikat, szervezeti felépítésüket. Az ún. standard verziók alkalmazása azért is érdekük, mert így lényegesen kevesebb karbantartási, ill. verzióváltási díjat kell fizetni a megoldás szállítójának.

1.1. Projektmódszertanok

Az informatikai projektet vezető szakember (akár vállalati, akár független tanácsadó...) számos egymáshoz hasonló projektmódszertan közül választhat.

A **PRINCE** (Projects IN Controlled Environments) szabványosított lépéssorozat, amely felöleli egy informatikai projekt irányításának egészét, a projekt kialakítástól a projekteredmény operatív működésének kezdetéig. Az eljárást az 1980-as évek végén a brit kormány információs rendszerekkel foglalkozó központja (**CCTA** – Central Computing and Telecommunications Agency) dolgozta ki, majd a 90-es években továbbfejlesztések révén más jellegű projektek irányítására is alkalmassá vált (Görög-Ternyik, 2001, p.199-205.) Az eljárás használata révén elkerülhető, hogy a projektkialakítás tevékenységét is

¹ Külső forrásból beszerezhető szoftvertermékeknel (esetleg hardvereszközöknél) négy „típus” különböztethetünk meg:

- COTS (Commercial Off The Shelf) – könnyen installálható megoldások, amelyek a kereskedelemben megvásárolhatók. Erre a legjobb példát az ún. „dobozos” szoftverek (operációs rendszerek, szövegszerkesztők, levelező programok stb.) jelentik.
- MOTS (Modified or Modifiable Off The Shelf) – a megoldást a beszerző, a szállító vagy akár egy harmadik fél módosítja a beszerző igényeinek megfelelően. Ezeknél a szoftvereknél a fejlesztés és a speciális céloknak megfelelő adaptáció elválik egymástól. Néhány esetben a rövidítés elején található „M” betű katonai (military) megoldást rejt.
- GOTS (Government Off The Shelf) – ezeket a termékeket a kormányzat ilyen céllal létrehozott szervezeti egységei készítik, ill. készítetik általában speciális kormányzati célokra (pl. népszámlálás nyilvántartás).
- NOTS (NATO Off The Shelf) – a NATO konzultációs, vezetési és irányítási feladatainak (C3 – Consultation, Command, Control) támogatására kifejlesztett megoldásokat takarja. Bizonyos szövegkörnyezetben az „N” betű (niche) szűk piaccal rendelkező, speciális igényeket kielégítő termékekre utal.

⁴⁹ ERP (Enterprise Resource Planning system) – vállalatirányítási információs rendszer, MIS (Management Information System) – vezetői információs rendszer, DSS (Decision Support System) – döntéstámogató rendszer, e-Business megoldások stb.

a megoldás szállítója végezze, gyakorlatilag sajátmagának szabva meg a „szükséges tevékenységeket”.

A PRINCE részletes ajánlást tartalmaz a kialakítandó projektszervezetre, a projekttervek készítésére és az ellenőrző tevékenység végzésére.

Nagyon fontos szerepet kapnak az eljárásban a minőségpolitikai kérdések:

- minőségre vonatkozó szabványok és szabályozások megadása,
- minőségellenőrzés módja,
- minőségi felülvizsgálók kiválasztása.

Az **Euromethod** információs rendszerek beszerzésével, fejlesztésével és adaptációjával foglalkozó módszertan. Gyakorlatilag kommunikációt segítő közös nyelv a „vevő” és a szállító között. A módszer a bevezetési projekt során is használható (elsősorban az előrehaladás ellenőrzésénél és a szerződés lezárásánál), hiszen mindkét fél számára érthetően fogalmazza meg a fogalmakat és követelményeket. A módszer kialakítását és fejlesztését az Európai Unió is támogatja az 1990-es évek elejétől. Magyarországra az MTA Információtechnológiai Alapítvány révén került.

Az ERP rendszereket készítő cégek közül soknak, saját, jogilag védett bevezetési projekt módszertana van.⁵⁰ Tehát nem egyszerűen szoftverrendszert árulnak, hanem komplett üzleti célú megoldást, amelybe beletartozik az implementáció is.

Az Intentia, mint a Movex gyártója svéd egyetemi szakembereket is bevont az Implex ciklus kidolgozásába. Az együttműködés egyik eredménye egy több mint 200 „kötelező” és „ajánlott” tevékenységet tartalmazó projekt-ellenőrző lista lett. Az információs rendszer bevezetését ez alapján követik, garantálva a sikeres bevezetést. A módszertan további erőssége, hogy a világ különböző pontjain zajló, ill. befejezett Movex bevezetések tapasztalatait összegyűjtik és feldolgozzák. Ez az informatikai projektekkel kapcsolatos, folyamatosan megújuló tudásbázis a jövőbeni partnerek számára jelent segítséget. A „rendszer-specifikus” projektmódszertanok felhasználása, ill. alkalmazása más informatikai projektek estében azonban szinte lehetetlen, hiszen a részletes dokumentációkat a cégek üzleti titokként kezelik. Bemutatók rendszerleírásaikban csak felületesen, a reklám miatt érintik ezt a témát. A korábban ilyennel dolgozó szakemberek azonban sok hasznosítható tapasztalattal rendelkezhetnek.

Az Interneten számos ingyenesen vagy kis költséggel letölthető általános projektmódszertan leírásra lehet bukkanni.⁵¹

⁵⁰ **SAP** – Accelerated Systems Applications and Products, **J.D. Edwards-One World** – Rapidly, Economically and Predictably Methodology, **Scala** – Signature Implementation Methodology, **Infor:corvex-infor:Com** – infor:solution Concept, **proAlpha** – goLive, **Intentia Ab-Movex** – Implex ciklus.

⁵¹ Project Management Body of Knowledge, Ten Step, Method 123 stb.

Ezek felhasználásánál figyelembe kell venni, hogy az informatikai projektek sajátosak. Technológiai, folyamatszerkezeti és emberi erőforrás kezeléssel kapcsolatos elemek egyaránt megtalálhatóak benne.

1.2. Projekttervező és kezelő szoftverek

Az informatikai projektek esetében is megfogalmazható egy valamilyen elérendő műszaki vagy szervezeti cél és megadhatók az erőforrás- és időkorlátok. Ezek kezelésében jó szolgálatot tehetnek a projektmenedzsment megoldások. A „dobozos” szoftverek⁵² nem csak hálótervezésre használhatók. Képesek több, párhuzamosan futó projekt azonos erőforrás felhasználásait is figyelemmel kísérni, illetve koordinálni. A korszerű, hálózatokon is futtatható szoftverek a projekt munkában résztvevő szakemberek számára óriási segítséget jelentenek, hiszen támogatják a projekt adminisztrálását és a legkisebb végrehajtási zavar esetén is az egész tevékenységláncolat azonnal újratervezhető.

1.3. Projektszervezet

Az informatikai projektek lehetséges végrehajtására alkalmas szervezeti formákat, azok előnyeit és hátrányait a szakirodalom részletesen tárgyalja (Görög-Ternyik, 2001, p. 157-170.). A három alapvető választási lehetőség a következő:

- projekt koordinációs szervezeti forma (hagyományos, de bővített lineáris vagy funkcionális szervezet),
- mátrix szervezeti forma,
- projektorientált szervezeti forma.

A választás mindig az adott informatikai projekt körülményeinek és sajátosságainak valamint a szervezet és az abban zajló folyamatok függvénye. Ennek elemzése jelen tanulmány határain túlmutat.

A gyakorlatban van egy sokszor alkalmazott megoldás, ha az információs rendszer olyan külső szállítótól érkezik, aki vállalja a bevezetést is. Az alkalmazó vállalatnál működő projektszervezet mintájára a megoldás szállítója is kialakít egy hasonló szervezeti struktúrát. Ez azt jelenti, hogy minden projekt tevékenységet, problémát közösen hajtanak végre, ill. oldanak meg. A két – legfelső vezetői szintről delegált – projektvezető együttesen felel az informatikai projekt sikeréért.

1.4. Szervezeti változás, változtatás

Már az információs rendszer bevezetés során gondolni kell az üzemeltetésre is. Ez befolyásolja az azt használó szervezetet is. Strukturált szakembergár-

⁵² MS Project 2000., Sciforma PS Suite, OPX2, Artemis Project View stb.

dára van/lesz szükség a napi működés közben jelentkező zavarok kezeléséhez. A vállalatnál – hacsak nem a teljes szolgáltatás külső kézben van – megjelennek a **rendszergazdák**. Igazán nagy rendszerek esetén külön a hardveres és külön a szoftveres... Ha az információs rendszer integrált és több funkcionális területet is felölel, akkor szükség lehet ún. **modulgazdákra**. A következő szinten megjelennek a „**kulcsfelhasználók**” (key users) akik egy-egy részfolyamatot (pl. raktári tranzakciók követése, ki- és bevételezések) ismernek tökéletesen és képesek az adott területre érkező „egyszerű” **felhasználókat** betanítani, illetve munkájukban támogatni.

A bevezetés és a működés során jelentkező problémákat e szerint a struktúra szerint, alulról fölfelé továbbítják vagy próbálják megoldani, úgy, hogy minél kevesebb drága, külső erőforrást kelljen igénybe venni. Ez a „hierarchia” a védelmi feladatokat ellátó szervezeteknél is átvehető. Természetesen a projekt ideje alatt vannak olyan „munkakörök”, amelyeket a csoportmunkában dolgozó projektszervezet egy-egy tagja ideiglenesen tölt be, az adott feladatnak megfelelően (pl. adatbázisok áttöltése előtti ellenőrzés...).

1.5. Harmadik fél bevonása

Külső, harmadik fél bevonása katalizátorként meggyorsíthatja az adott információs rendszer bevezetését. Több lehetőség is adódik a közreműködésre.

A **tanácsadó** segíthet abban, hogy a rendszer szállítói ne erőltessék rá a szervezetre az egyszerűbb, de kevésbé hasznos megoldásokat.

A projektmenedzser biztosíthatja a projektszerűséget, és sokat segíthet az itt nem tárgyalt pályázati anyag összeállításában és a rendszer kiválasztásában. A módszertani szabályok betartásával, betartatásával és a folyamatos projekt ellenőrzéssel keretet ad a bevezetésnek.

A független minőségbiztosító (vagy minőségirányító) más, mint a projektmenedzser. Igaz, hogy rendszeresen vizsgálja a projektszerűséget, szakértőként segíti a szakmai egyeztetéseket, és felhívja a figyelmet a kockázatokra, de nem jelöl ki felelősöket, nem avatkozik be a bevezetési folyamatba és nem kéri számon a feladatok végrehajtását. Nem a megbízó vagy a megbízott érdekeit képviseli, hanem a projekt céljait. Segíti a résztvevők közötti kommunikációt, ill. együttműködést. Minőségi szempontok alapján vizsgálja és értékeli a keletkező dokumentumokat (szerződések, tervek, jegyzőkönyvek stb.) és tájékoztatja a projektvezetést és a megbízó felső vezetőit.

Az alkalmazásszolgáltatók (ASP - Application Service Provider) bérleti szerződés keretében teljes körű informatikai szolgáltatást nyújtanak (hardver- és rendszerszoftver üzemeltetés, információs rendszerek tervezése, telekommunikációs szolgáltatások, rendszer bevezetés és változás-menedzselés, oktatás stb.). Gyakorlatilag egy előkonfigurált – az esetek nagy részében költségta-
karékos – megoldást bocsátanak a felhasználó rendelkezésére. Az így kialakuló stratégiai szövetség miatt a felhasználó azonban kiszolgáltatottá válhat.

Harmadik fél bevonásának ellenzői mind a bevezetést elindító szervezetben, mind az informatikai megoldás szállítójánál megtalálhatóak. Indokaik a következők:

- az eltérő projekt módszertanok alkalmazásai konfliktushoz vezethetnek,
- a külső szakemberek sem a rendszert, sem a befogadó szervezetet nem ismerik,
- költséges a megoldás szállító mellett egy külső szakembert vagy szakértői csoportot is fizetni.
- Ezek az indokok valós veszélyeket hordoznak. Ezért a projekt kialakítás kezdeti szakaszában tisztázni kell a projektben résztvevők szerepét, feladatait és jogkörüket és legfőképpen a bevezetésnél jelentkező kiadásokat.
-

2. Védelmi szféra speciális igényei

A védelmi szféra informatikai projektjei sok szempontból speciálisnak tekinthetők.

- A legritkább esetben vásárolnak integrált, minden szervezeti folyamatra kiterjedő információs rendszereket. Sokkal gyakoribb a funkcionális elemekből történő „építkezés”. Emiatt viszont kiemelt szerepet kap a rendszerek nyitottsága és együttműködési képessége. A védelmi tevékenységgel foglalkozó szervezetek is szerezhettek be – a vállalatoknál megszokott – folyamatokat követő és döntéstámogató megoldásokat a logisztika, pénzügy, számvitel, kontrolling, karbantartás, eszközgazdálkodás és emberi erőforrás gazdálkodás területeire, de túlsúlyban vannak a speciális, csak a honvédségnél és rend- és katasztrófavédelemben használt rendszerek (pl. helyzetismeret alkalmazások).
- A fejlesztések a korlátozott pénzügyi források miatt valószínűleg szakaszosak lesznek. Ez azt jelenti, hogy nem egy projektről beszélhetünk, hanem egymással összefüggő, időben elhúzódó projektek láncolatáról.
- A kereskedelembe megvásárolt vagy más külső forrásból (pl. NATO) átvett programrendszerek mellett elképzelhető informatikai fejlesztő cégek és a védelmi szféra közös, speciális célú alkalmazásfejlesztése is. Ez a projektben résztvevőktől rendszerfejlesztési ismereteket is igényel (pl. SSDAM módszertan, Bana, 1995.).
- A terület sajátosságai és a biztonsági kérdések miatt a projekt irányításáért felelős vezetőnek általában belső szakembernek kell lennie.
- Nehezen kérhető teljes körű, nagyszámú és az adott feladatnak teljesen megfelelő referencia a megoldás-szállítóktól, hiszen az információs rendszerek nagy része egyedi jellegű és máshol nem alkalmazható (pl. országos gépjármű nyilvántartás...).

-
- Általában a megvásárolt rendszer, illetve részrendszer bevezetésével valamint működésével kapcsolatban nincs tapasztalat. Nem mindig lehet másik szervezet eredményeit, bevált ötleteit átvenni.
 - Sokkal nagyobb szerepet kap a távközlés, mint a hagyományos polgári alkalmazások esetében. Az információs rendszereknek itt egyik legfontosabb eleme a kommunikációs alrendszer. A vezetési rendszereknek minden körülmények között biztosítani kell a szükséges információk áramlását. Minősített helyzetekben az adatátvitellel szembeni elvárások (valós idejű átvitel, információvédelem, más hálózatokhoz történő kapcsolódás stb.) emelkedhetnek. A mobil kommunikáció ilyenkor lényegesen nagyobb szerepet kap, mint egy „statikus” termelő vagy szolgáltató vállalat információs rendszerében.

3. Stratégiai gondolkodás

A védelmi szféra szervezeteiben megvan a hajlandóság a stratégiai gondolkodásra. A Belügyminisztérium ágazati szintű informatikai stratégiát készített. A Magyar Honvédségnél is többen ráébredtek arra, hogy az itt használt információs rendszerek nagy része elavult. Szükség van tehát átfogó rekonstrukciónak. Az 1995-ben elkészült magyar Nemzeti Informatikai Stratégiához kapcsolódóan a Magyar Honvédség Informatikai Intézete tanulmányokat dolgozott ki informatikai fejlesztésekre vonatkozóan (vezetést és irányítást támogató rendszerek...) Ezeknek az elgondolásoknak, ill. fejlesztési stratégiának a karbantartása azóta is folyamatos.

Komplex fejlesztést csak megfelelő informatikai stratégia alapján lehet hatékonyan megvalósítani. Eltérő alapokon fejlesztett „szigetmegoldásokkal” – még ha azok a legkorszerűbbek is – nem lehet megfelelni a kihívásoknak.

Az informatikai projekt akkor tekinthető projektnek, ha van célja, végrehajtásához megszabott időtartama és erőforrás korlátja (Papp, 2002, p.22.) Az erőforrások közül ma Magyarországon a legszűkösebb a pénz. Ennek hatékony felhasználása csak úgy lehetséges, ha a fejlesztési stratégiát széles műszaki, gazdasági és szakmai alapokon készítik elő és ezt az adott területek felsőszintű vezetői tartják kézben és elemeit (infrastruktúra, kommunikációs hálózat, alkalmazások) egységes egésként kezelik. Az információs rendszer létrehozásához az előbbi három elemen kívül beruházásokra, az új folyamatoknak megfelelő szervezeti változtatásokra és oktatásra, képzésre van szükség (Gorza, 2001, p.14.). Ehhez nyújthatnak segítséget a megfelelően összeválogatott – esetleg más területen már bevált – projektmenedzsment eszközök, ismeretek.

4. A projektirányítás szakaszai

A védelmi szféra szervezeteinél is léteznek projektirányításra vonatkozó szabályzatok (pl. 22/2002. (HK9.) HM utasítás, MH vezérkari főnökének

98/1999 számú intézkedése a MH informatikai fejlesztéseinek végrehajtási rendjére). Ettől függetlenül vagy e mellett is érdemes áttekinteni egy informatikai projekt menetét.

A már korábban tárgyalt projektmetódusoknál is megfigyelhető, hogy három nagyobb szakaszra bonthatók a projektek. (Hice – Turner – Cashwell, 1983. p. 347-413.)

4.1. Projekttervezés

A rendszerek bevezetésével, implementációjával foglalkozó informatikai projektek, bár sok szempontból hasonlóak egymáshoz, mégis mindegyik egyedi tervezést igényel. Az első magától értetődő lépés a **projekt meghatározása**. Ebben a projektvezető megpróbál szakmailag alátámasztott projektcélokat definiálni a jövőbeni **felhasználói elvárások** alapján. Természetesen figyelembe kell venni a rendelkezésre álló időt és az anyagi és személyi erőforráskorlátokat is. Mivel a választott rendszereket vagy annak bizonyos elemeit külső szállítóktól szerzik be, fontos az **átvételi kritériumok** megadása. Itt vissza lehet nyúlni az információs rendszer kiválasztásnál már meghatározott és lehetőség szerint számszerűsített „kizáró” és „soroló” szempontokra (Michelberger, 2003.).

A projektvezetésnek vannak jó értelemben vett adminisztrációs kötelezettségei. A feladatok végrehajtásával párhuzamosan folyamatosan tájékoztatni kell a projekt sikerében érdekelt vezetőket, felhasználókat és a csoportmunkába munkatársakat delegáló szervezeti egységeket. Az ún. **állapotjelentések** gyakoriságát, tartalmi és formai követelményeit (terv és tényállapot összevetése, korábbi problémák megoldása, jelenlegi problémák leírása, tervmódosítások indoklása stb.) még a jóváhagyott projektterv előtt tisztázni kell.

A projekt dokumentáció első darabja egy felsőszintű vezető által ellenjegyzett **nyilatkozat**, amely alapján a projekt-team elkezdheti a munkáját. Gyakorlatilag megadja projekt célját és határait.

A tervezés a céloktól és a végrehajtandó munkától függően több lépcsőben is történhet. A projekt vezetője egy becsült, **kezdeti tevékenységlista és ütemterv** alapján válogatja össze a **projekt-team tagjait**, akik segíthetnek a részletes projektterv kialakításában is. fontos, hogy a csoportmunkában résztvevő tagok rendelkezzenek a megfelelő szaktudással, és képesek legyenek együtt dolgozni. A vezető mindenkori felelőssége jelezni, ha úgy érzi, hogy a projekt adott feltételek mellett megvalósíthatatlan. Ebben a kezdeti fázisban is jól használhatók a már tárgyalt projekttervező és kezelő szoftverek. A projekt kezelését, átláthatóvá tételét segítik a **„mérőkövek”** megadása. Ezek egy-egy pontosan megfogalmazott részfeladat vagy kritikus sikertényező teljesülését jelzik, esetleg mutatják a projekt-team összetételének a szakmai követelmények miatti változását.

A **projekt dokumentáció** jelentős részét képezik még a projekttel kapcsolatos levelezések, az értekezletek jegyzőkönyvei, mérőföldkövek utáni átadás-átvételek dokumentumai, a különböző felhasznált szakmai ajánlások, módszertanok és szabványok, valamint a szállító által biztosított rendszerleírások.

A **részletes projektterv** minden egyes tevékenységéhez meg kell adni a végrehajtáshoz szükséges időt, a megfelelő szaktudással rendelkező személyzetet (felelősök és végrehajtók) és a tevékenységek és feladatok közötti logikai kapcsolatokat (egymásutániség, átfedések, párhuzamosságok). A projekt végrehajtása csak a jóváhagyott részletes projektterv alapján kezdődhet.

4.2. Projektellenőrzés

Ennél a lépésnél történik a teljes projekt végrehajtásának ellenőrzése, ill. követése. Az előrehaladás áttekintését külső, „projektől független” ellenőrök is segíthetik. Ezek a személyek, csoportok időszakonként vagy jelentős mérőföldkövek elérése után szakmailag értékelik az elvégzett munkát, tájékoztatva a projektet elindító, ill. jóváhagyó felsővezetőket. Ettől függetlenül működik egy „belső ellenőrzés” is, amelyet a projektvezető(k) koordinálnak (ld. állapotjelentések). Az előrehaladást sokkal jobban lehet követni egy részletes, folyamatosan aktualizált projektterv alapján. A szakmai célok teljesülése mellett figyelni kell az erőforrások (elsősorban projekt ráfordítások) és a rendelkezésre álló idő felhasználására is.

A projekt ellenőrzésében kiemelt szerepet kap az adminisztráció, hiszen a „kívülálló” (pl. minőségbiztosító) és az új team-tagok a világosan leírt, „projekt szabványon” alapuló jelentések alapján tudnak bekapcsolódni a közös munkába.

A projekt előrehaladásával folyamatosan szükség lehet különböző képzésekre (módszertanok, alkotótechnikák, felhasználói betanítás stb.). Ennek módjait, módszereit (külső tanfolyamok, informális képzések, projektorientált szemináriumok) teljesítését szintén rögzíteni kell.

4.3. Projekt lezárása

A projekt akkor tekinthető befejezetnek, ha valamennyi tevékenysége lezárult, a végső értékelő jelentések (sikerült a kitűzött célt megvalósítani és az előírt költség- és időhatárok között maradni?) elkészültek és ezt az átvétellel megbízott szakemberek is elfogadták. Nagy információs rendszerek elhúzódo bevezetése esetén gyakran előfordul, hogy a felhasználók a jövőbeni rendszert jobban megismerve különböző kiegészítéseket, változtatásokat szeretnének. Ezek figyelembevétele nem minden esetben lehetséges. Sőt, jelentős igény módosulás esetén még a projekt befagyasztására esetleg újratervezésre is sor kerülhet. A projektvezető feladata ezeknek az igényeknek a kezelése.

A projekt-teamet mindaddig nem szabad felosztatni, amíg az üzemeltetést végző szervezet fel nem áll és a felhasználók meg nem tanulják a rendszer kezelését.

Az új rendszer indítása történhet szakaszosan vagy teljes körűen is. Ezt az adott szervezet teherbíró képessége dönti el.

Gondot jelenthet a régi rendszerek leállítása. A hirtelen váltás nagy kockázatot jelent, hiszen az új rendszernek az alapos tesztek ellenére is lehetnek gyermekbetegségei. Ezért a szervezetek nagy része biztonsági okokból egy ideig párhuzamosan működteti az új és a régi rendszert. A megszokás, néha indokolatlan biztonsági igények miatt létrejövő „kettős” terhelés megviseli a felhasználókat. Az információs rendszer bevezetésének eredményei egyébként sem mindig jelentkeznek a felhasználók szintjén. Egy-egy munkahelyen lehet, hogy a megszokottól eltérő jellegű, vagy többletmunka jelentkezik.

A középszintű vezetők, jövőbeni kulcsfelhasználók gyakran idegenkednek az új rendszertől. Az idősebb generáció nehezebben fogadja az új „munkakörnyezetet” (képernyők, bizonylatok, kimutatások, jelentések, megváltozott folyamatok...).

Egy jól működő on-line információs rendszer sokszor „sérti” a középvezetők érdekeit. Az új rendszer bevezetésének nem megfelelő támogatásával és a régi információs rendszer sziget megoldásainak erőltetésével fenntarthatják az információ birtoklásából származó előnyös helyzetüket.

Összefoglalás

A cikk nem akart új informatikai stratégiák kiindulópontja lenni. Csupán a várható és elkerülhetetlen fejlesztések előtt akarta felhívni a figyelmet arra, hogy megfelelő eszközök és módszerek nélkül a legjobb tervek is megbukhatnak.

Az üzleti életben lényegesen nagyobb számban indítanak és zárnak le informatikai projekteket (általában sikerrel...). Az itt összegyűlt módszertani tapasztalatok – természetesen a védelmi szféra sajátosságait figyelembe véve – felhasználhatók és átvehetők.

Irodalom:

BANA István: Az SSADM rendszerszervezési módszertan. LSI Oktatóközpont, 1995.

-
- GORZA Jenő: A szervezeti informatikai stratégia készítésének szükségessége, idő-szerűsége, a stratégia elemei. VIII. Vállalati Informatika Konferencia, 2001. november 20-21. Balatonfüred, 9-17. oldal
- GÖRÖG Mihály – TERNYIK László: Informatikai projektek vezetése. Kossuth Kiadó, Budapest, 2001.
- HALASSY Béla: Ember – Információ – Rendszer. IDG Magyarországi Lapkiadó Kft., 1996.
- G.F. HICE – W. S. TURNER – L.F. CASHWELL: Számítógépes rendszerek fejlesztésnek módszertana. Műszaki Könyvkiadó, Budapest, 1983.
- KACSUKNÉ BRUCKNER Livia – KISS Tamás: Bevezetés az üzleti informatikába. Akadémiai Kiadó, 1999.
- MUNK Sándor: Információs szintér, információs környezet, információs infrastruktúra. Nemzetvédelmi Egyetemi Közlemények, ZMNE, 2002/2. (133-154. o.)
- MICHELBERGER Pál: Integrált információs rendszerek összehasonlító értékelése. ZMNE, Bolyai Szemle, 2003. 1. szám
- PAPP Ottó: Projektmenedzsment a gyakorlatban. LSI Oktatóközpont, 2002.
- TÁTRAI Tibor: MS Project 2000, MS Project Central. Computerbooks, 2001.
- A Belügyminisztérium ágazati szintű informatikai stratégiája 1999-2002. Magyar Nagylexikon. Kilencedik Kötet, p.870. Magyar Nagylexikon Kiadó, 1999.
- www.aisc.com (Artemis Project Management)
- www.itb.hu/ajanlasok (Bevezetés a PRINCE projektirányítási módszertanba és Euromethod dokumentáció)
- www.method123.com (Method 123)
- www.planisware.com (OPX2 Enterprise-Wide Project Control)
- www.pmi.org (Project Management Body of Knowledge)
- www.prince2.com (PRINCE 2)
- www.sciforma.com (Sciforma PS Suite)
- www.tenstep.com (Ten Step)

DIGITÁLIS ALÁÍRÁS HASZNOSÍTÁSA

1. Bevezetés

Napjainkban az elektronikus adatrögzítés és kommunikáció korát éljük. Leveleink megírásához, adataink rögzítéséhez és tárolásához, a munkánk megkönnyítését végző programok futtatásához számítógépet használunk. Viszont mindannyian tudjuk, hogy ennek a kényelemnek az ára a biztonság. Rendkívül sok időt és energiát takarítunk meg például az elektronikus levelezéssel, de minden egyes elküldött levélért aggódhatunk, hogy nem kerül-e illetéktelenek kezébe, vagy azok a levelek, amelyeket mi kapunk tartalmaznak-e vírust és valóban az küldte-e aki feladóként szerepel? Rengeteg ilyen és ezekhez hasonló kérdés van még, amelyekre a biztonsági szakemberek a lehető legjobb megoldásokat próbálják kidolgozni. Egy ilyen viszonylag új, vagy legalábbis még nem túl elterjedt biztonsági megoldás a digitális (vagy elektronikus) aláírás.

De mit is jelent a digitális aláírás és miért van szükség rá a katonaságnál? Ahhoz, hogy erre a kérdésre választ kapjunk, először nézzük meg mire jó a hagyományos aláírás. Amennyiben egy levelet, vagy iratot valaki a kézjeggyel ellát, ezzel igazolja, hogy az tőle származik, teljes tartalmát ő írta (vagy legalábbis egyetért a benne foglaltakkal) és az aláírás óta – aminek időpontját általában tartalmazza a dokumentum – senki sem módosította azt. A digitális aláírás sok egyéb funkciója mellett ugyanazt biztosítja felhasználója számára, mint a hagyományos aláírás. Vagyis a digitális aláírással ellátott dokumentumról eldönthetjük, hogy hiteles és sértetlen, valamint aláírója nem tagadhatja le, hogy az adott dokumentum tőle származik.

Egy ilyen megoldással rengeteg időt és energiát lehet megtakarítani. Nem szükséges a bizalmas leveleket és dokumentumokat kinyomtatni, majd manuálisan aláírni, hanem mindez elektronikus formában bonyolítható és ugyanolyan biztonságos.

3. Az elektronikus kommunikáció kockázatai

Az elektronikus kommunikációt érő támadásokat alapvetően két nagy csoportra oszthatjuk: aktív és passzív támadásokra. Aktív a támadás, amennyiben az üzenet tartalmát egy arra nem jogosult – rosszindulatú – fél megváltoztatja, vagy aktívan befolyásolja a kommunikációt. Ebbe a csoportba tartozik a megsemmisítés, az üzenetmódosítás, a visszajátszás, az üzenetlopás vagy eltérítés és az üzenetkésleltetés. Passzív támadásról akkor beszélünk, amikor a tá-

madó aktívan nem befolyásolja a kommunikációt. Erre példa a forgalomelemzés, és az üzenettagadás.

A megszemélyesítéses támadás esetén a támadó fél valaki más nevében küld üzenetet, így téveszti meg a fogadó felet. Ehhez nagyon hasonló az üzenetmódosításos támadás, amelynek során egy illetéktelen személy az általa elfogott üzenetet megváltoztatva küldi tovább a címzett félnek. Az üzenetlopásos vagy eltérítéses támadás lényege az, hogy a támadó elfogja az üzenetet és ezt saját céljára használja fel, vagy valaki másnak továbbítja. Visszajátszásról akkor beszélünk, ha az elfogott üzenetet a támadó többször is elküldi a címzettnek. Az üzenetkésleltetés pedig azt jelenti, hogy a támadó fél a birtokába került üzenetet visszatartja és csak bizonyos idő elteltével küldi tovább a címzettnek.

A forgalomelemzésnek, mint passzív támadási módszernek nem a kommunikációba való aktív beavatkozás a célja. Ebben az esetben a támadó csak figyeli a kommunikációt, és így információt szerez a felekről. Üzenettagadásról akkor beszélhetünk, ha a küldő fél letagadja, hogy az adott üzenet tőle származik, vagy a címzett nem ismeri el azt, hogy megkapta az adott üzenetet.

Ezen támadások mindegyike ellen önmagában egyetlen biztonsági eljárás sem nyújthat védelmet. A kommunikáció különböző szintjein más és más protokollok gondoskodnak arról, hogy üzeneteink ne essenek támadók áldozatául. Csak akkor érezhetjük biztonságban magunkat, ha a különböző biztonsági megoldásokat megfelelően és lehetőleg egymással kombinálva alkalmazzuk.

A digitális aláírás is csak bizonyos biztonsági problémák megoldására jó és célszerű valamilyen más eljárással – például titkosítással – együtt használni.

3. A digitális aláírás működése

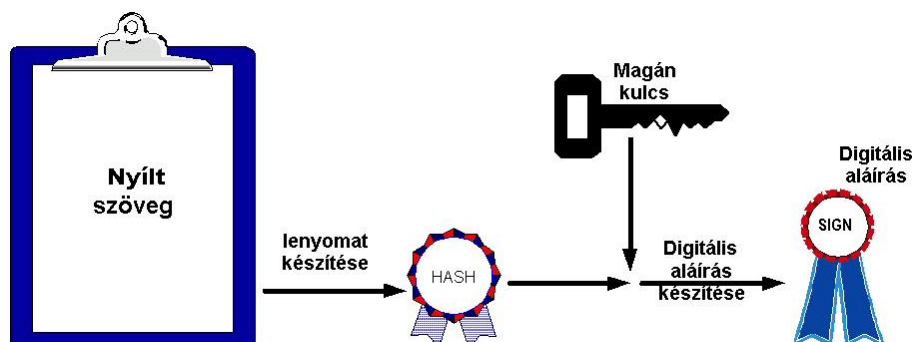
A digitális aláírással szemben tehát ugyanazok a követelmények, mint amik a hagyományos aláírással szemben. Egyértelműen kell azonosítania az aláíró, ezzel biztosítva a hitelességet. Garantálnia kell a sértetlenséget vagyis, hogy a dokumentum az aláírás óta nem változott. Valamint letagadhatatlannak kell lennie a digitális aláírással ellátott dokumentumnak.

Ezekből az elvárásokból következik, hogy a digitális aláírásnak ugyanolyan egyedinek kell lennie, mint az emberek kézjegyeknek. De hogy lehet ezt az egyediséget technikailag kivitelezni? Hogy is működik a digitális aláírás?

Szükségünk van először is egy úgynevezett nyílt szövegre, amely tetszőleges hosszúságú még nem titkosított és nem hitelesített dokumentumot jelent. Ezen kívül kell még valamilyen lenyomat [3] (HASH) és aláírás készítő eljárás valamint az aláíró magánkulcsa.

A folyamat a következő. Először vesszük a nyílt szöveget és a HASH készítő algoritmus segítségével egy lenyomatot készítünk belőle, ami általában 160 bites (SHA-1 [2] esetén). Ezután ebből a lenyomatból és a magánkulcsból

(private key) egy aláíráskészítő eljárás segítségével előállítjuk a digitális aláírást [1].



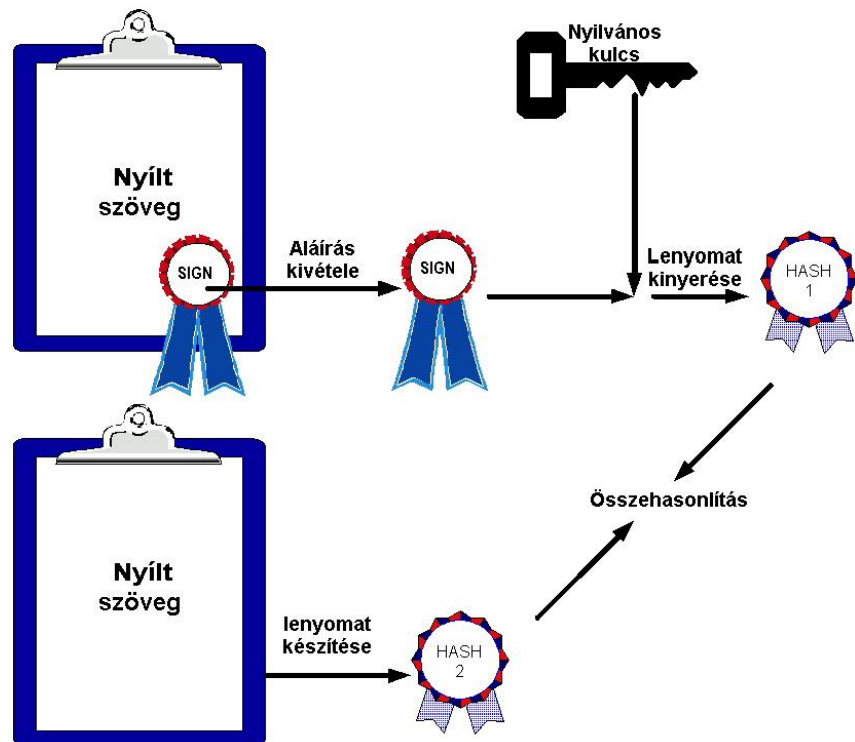
1. ábra: A digitális aláírás létrehozása

A digitális aláírás ellenőrzése sem sokkal bonyolultabb folyamat, mint annak létrehozása [5]. Ebben az esetben azonban az aláíró nyilvános kulcsát használjuk fel és lenyomat ellenőrző eljárást lenyomat készítő eljárás helyett. Amennyiben kapunk egy digitális aláírással ellátott dokumentumot (vagyis az állítólagosan eredeti nyílt szöveget és egy aláírást) nagyon egyszerűen megbizonyosodhatunk annak eredetiségéről és hitelességéről. A nyílt szövegből ugyanazzal a HASH készítő algoritmussal előállítunk egy lenyomatot, amelyet az aláíró is használt. Ezután az aláírásból és az aláíró nyilvános kulcsából az aláírás ellenőrző eljárás segítségével “visszafejtjük” az eredeti lenyomatot. Ha az általunk gyártott lenyomat megegyezik az aláírásból nyert lenomattal, akkor elfogadhatjuk, hogy az általunk vizsgált aláírással ellátott szöveg hiteles és nem változtatták meg az aláírás óta.

Most térjünk ki arra, hogyan keletkeznek a fent említett magán- és nyilvános kulcsok.

Alapvetően kettő fajta titkosítást különböztetünk meg. Az egyik a szimmetrikus (vagy titkos) kulcsú titkosítás, a másik pedig az aszimmetrikus (vagy nyilvános) kulcsú titkosítás.

Szimmetrikus kulcsú titkosítás esetén a küldő és a fogadó fél ugyanazt a kulcsot használja. A küldő a közös kulccsal betitkosítja az információt, amit a fogadó fél vissza tud fejteni. Ehhez a kommunikációt megelőzően a két félnek meg kell egyeznie a mindkettőjük által használt kulcsban. Vagyis legalább egyszer személyesen kell találkozniuk, vagy egy teljesen biztonságos csatornán keresztül kapcsolatot teremteniük.



2. ábra: A digitális aláírás ellenőrzése

Az aszimmetrikus titkosítás esetében nincs szükség a kommunikálni kívánó felek előzetes biztonságos csatornán történő kulcscseréjére. Mindkét fél rendelkezik egy magán és egy nyilvános kulccsal. A magán kulcsát mindenki maga tárolja és rajta kívül azt senki nem ismeri. A nyilvános kulcsot viszont bárkinek elküldheti, ha azt akarja, hogy az illető titkosított dokumentumot tudjon küldeni számára. A titkosítás ugyanis úgy történik, hogy az a fél aki egy titkosított szöveget akar küldeni fogja a címzett nyilvános kulcsát és azzal betitkosítja az általa küldendő dokumentumot, amelyet visszafejteni csakis a nyilvános kulcs magánkulcs párjával lehet, amit a címzett birtokol.

4. Hitelesítő központok (CA)

A fentiekben leírtak alapján egyértelmű, hogy digitális aláíráshoz csak aszimmetrikus kulcsú titkosító algoritmust lehet alkalmazni. Hiszen kizárólag ez a módszer garantálja azt, hogy az adott kulcs egyetlen személyhez tartozik

ugyanúgy, mint a manuális aláírás. Viszont az aláírás annyiban tér el a titkosítástól, hogy bárkinek vissza kell tudni fejteti (vagyis ellenőrizni) egy adott aláírást, de csakis egyetlen ember tudja azt generálni. Ez pedig pontosan az aszimmetrikus titkosítás folyamatának ellentéte. Tehát digitális aláírás esetén a saját magánkulcsunkkal titkosítjuk be az aláírni kívánt szövegből előállított lenyomatot és ezt utána a nyilvános kulcsunkkal bárki ellenőrizni tudja.

Ezen a ponton viszont felmerülhet a nyilvános kulcsok elhelyezésének kérdése. Mert, ha azt akarjuk, hogy bárki ellenőrizhesse az aláírásunk valódiságát, akkor mindenki által elérhetővé kell tennünk a nyilvános kulcsunkat. De mi van akkor, ha valaki az én nevemben ír alá valamit és hozzá a saját nyilvános kulcsát elküldi ellenőrzés végett arról azt állítva, hogy az én kulcsom? Ebben az esetben a címzett megnyugszik, hogy az aláírással minden rendben, hiszen ellenőrizte azt. Csak egy probléma van, hogy az nem annak az embernek az aláírása volt, akinek ő tulajdonította. Erre az igencsak markáns problémára nyújtanak megoldást az úgynevezett CA-k (Certificate Authority). A CA-k hasonló szerepet töltenek be, mint a rendőrség. Garantálják számunkra, hogy az a nyilvános kulcs, amelyet ők aláírnak [4] valóban hiteles. Ahhoz az emberhez tartozik, akiről ők azt állítják. Ezután pedig már tényleg megbízhatóan lehet digitális aláírást használni. Természetesen a CA-k bizalmi alapon működnek. Bizonyára egy zárt katonai hálózat esetében nem fognak egy civil CA-ban megbízni. De ha saját katonai CA-t állítanak fel, amelyben a nekik megfelelő szintű biztonsági elvárásoknak megfelelően azonosítják és írják alá a nyilvános kulcsokat, akkor teljesen megbízható digitális aláírásokat tudnak létrehozni.

5. Konklúzió

Láthatjuk, hogy ma már technikailag szinte tökéletes biztonsági megoldások állnak rendelkezésünkre. Ez azonban senkit ne tegyen könnyelművé, hiszen minden biztonsági rendszer leggyengébb pontja maga az ember. Saját figyelmetlenségünk, felszínességünk vagy csupán sietségünk nagy hibákat eredményezhet. Elég csak egyetlen alkalommal kihagyni a digitális aláírás hitelességének ellenőrzését és máris belesétálhatunk egy csapdába. Ráadásul mindezt hamis biztonságérzettel tesszük, hiszen meg vagyunk győződve arról, hogy az aláírás hiteles. Pedig az igazság az, hogy az elektronikus világban jobban kell ügyelnünk adataink biztonságára, mint a mindennapi életben, hiszen sokkal inkább ki vagyunk téve a támadásoknak.

Referenciák

-
- [1] Digital Signature Standard (DSS) FIPS PUB 186-2, 2000.
 - [2] Secure Hash Standard (SHA-1) FIPS PUB 180-1, 1995
 - [3] The MD5 Message-Digest Algorithm. R. Rivest. 1992, RFC 1321.
 - [4] ITU X.509 Public Key and Attribute Certificate Frameworks, 2000.
 - [5] Almási János: Elektronikus aláírás és társai

A HADERŐ VEZETÉSE BÉKÉTŐL ELTÉRŐ (MINŐSÍTETT) IDŐSZAKOKBAN

Vázlat a HM HVK hadműveleti és kiképzési csoportfőnök előadásához

"Az 1992. évi LXIII. tv. 19.§ (5) bekezdése alapján

NEM NYILVÁNOS

2003. szeptember 30-ától számított 5 évig."

Az előadás témájának a *haderőátalakítás* időszerű feladatai adnak aktualitást. Azok a törekvések, amelyek a megváltozott biztonsági helyzethez, a kormányzati szándékokhoz és a szövetségi vállalásainkhoz igazodó magyar haderő kialakítására irányulnak. Amelyek eredményeként átalakul a honvédség állománya, az összetétele és a feladatai éppúgy, mint az alkalmazás, a tevékenység és működés valamennyi lényeges eleme. Fontos színtere a változásoknak *haderő vezetése*, ahol az átalakítás egyaránt kiterjed a béke- és a békétől eltérő (minősített) időszakok katonai vezetési rendszerére. Az előadás a békétől eltérő időszakok vezetésének fontosabb jellemzőiről ad egy vázlatos tájékoztatást.

Az előadás *három fő kérdés* köré csoportosítja a mondanivalóját. Értelmezi a honvédség vezetésének néhány időszerű kérdését, majd bemutatja a felsőszintű vezetés, ezt követően pedig a közép- és csapatszintű vezetés főbb sajátosságait.

1. A honvédség vezetésének néhány időszerű kérdése

A Kormány a honvédelemről szóló 1993. évi CX. törvény (8. §-a (3) a) felhatalmazása alapján az egységes irányítás és vezetés követelményének fokozottabb érvényre juttatása érdekében, a Magyar Honvédség irányításának és felsőszintű vezetésének rendjét *kormányhatározatban* rögzítette.⁵³ A határozatban foglaltaknak megfelelően a Kormány az MH működésének irányításával kapcsolatos tevékenységét a *honvédelmi miniszter útján* gyakorolja.

Kormányzati irányítás, vezetés

A katonai vezetés vizsgálata, tartalmi elemeinek taglalása és rendszerének átalakítása nem lenne teljes értékű a néhány alapfogalom értelmezése, elemzése nélkül. Különösen nem napjainkban, amikor a HM és a HVK integrációja kapcsán minden korábbinál időszerűbbé vált az *irányítás és vezetés* ismételt értelmezése. Mindezekről azért sem tekinthetünk el, mert a katonai

⁵³ 2204/2001. (VIII. 8.) Korm. Határozat a Magyar Honvédség irányításának és felsőszintű vezetésének rendjéről.

vezetés mozgásterét mindenkor a *kormányzati irányítás és vezetés* közjogi hatásköre határozza meg.

Előzetesen egy lényeges jogszabályi megállapítás, amely felszínre hozza az *irányítás és vezetés* fogalmi párosát: "*A honvédelmi miniszter irányítja és vezeti a honvédséget.*"⁵⁴ Az előadás ennek szem előtt tartásával törekszik bemutatni a katonai vezetés elemeit.

A kormányzati *irányítás és vezetés* a honvédség eredményes működtetésére irányuló államigazgatási tevékenység egy konkrét formája. Összetett jellegénél fogva ötvözi magába mind az *irányítás*, mind pedig a *vezetés* sajátos jegyeit.

Az *irányítás* a honvédség működésének legfelső szintű és alapvető befolyásoló eszköze. Az államigazgatási hatalomgyakorlás hierarchikus tevékenységfajtája, egymás alá- és fölérendelt felek közötti jogviszonyt testesít meg. Az irányítás közjogi jogosítványok alapján folyik, benne a honvédelmi miniszter a kormány irányító hatáskörét képviseli az MH felé.

Az irányítás és vezetés fogalompáros ebben az összetételben (és sorrendben) a *honvédelmi miniszter hatásköréhez* kötődik. Az igazgatástudomány általános értelmezésével összhangban mindkét tevékenységi forma a honvédség eredményes és jogszerű működtetésére irányul. Célja a Magyar Honvédség befolyásolása a kormányzati célkitűzések (követelmények, feladatok) eredményes teljesítése érdekében.

Az irányítás, mint miniszteri hatáskör, *kormányzati funkciót* jelöl.⁵⁵ Közjogi jogosítványok talaján áll, tartalmát, kereteit jogszabályok állapítják meg.

A tartalmi meghatározottság mellett viszonylag kötött az irányítás alkalmazható *eszköztára* is, amely *jogi és nem jogi irányítási eszközöket* foglal magába. Az igénybe vehető eszközöket jogszabályok határozzák meg. Közös sajátosságuk, hogy alkalmazásuk jogi hatással és következménnyel jár.

Az irányítás *célját* legáltalánosabban a honvédség eredményes, jogszerű működésének átfogó és teljes körű biztosítása, továbbá a működéshez szükséges feltételekről való gondoskodás adja.

Az irányítás lényege tehát a *miniszteri akaratérvényesítés* a haderő *működése* fölött. Az irányítás *tartalmát* a honvédelmi miniszter által rendszeresen ellátott feladatok összessége képezi. Hatáskörét jogszabályok rögzítik. Az irányítás kiterjed a honvédség katonaszakmai és szervezeti tevékenységeire. Funkciói felölelik a szervezetek létrehozásával és felszámolásával, a személyügyi munkával, a finanszírozással és a szakmai feladatok meghatározásával kapcsolatos területeket.

⁵⁴ 2204/2001. (VIII. 8.) Korm. Határozat 2. pont.

⁵⁵ Lényeges tehát annak hangsúlyozása, hogy a kormányzati *irányítás* fogalma (és hatásköre) közel nem azonos a katonai *irányítás* fogalmával.

A miniszter irányítási hatásköre olyan jogosultságokat foglal magába, mint:

- a működés alapvető viszonyainak *szabályozási joga* az általa kiadott kötelező normatív aktusok keretében (szabályozási vagy normaalkotási jogosultság);
- a konkrét *utasítás joga* a honvédség, annak részei vagy vezetői számára;
- *döntés és határozathozatal joga* a honvédség konkrét ügyeiben;
- a honvédségi vezetési aktusok *felülvizsgálatának joga* (aktus-felülvizsgálat) jogszerűség vagy célszerűség alapján;
- a honvédség *ellenőrzésének joga*.

Az irányítás szempontjából a honvédség működésének két összetevője van. Úgymint a *katonai-szakmai* és a *szervezeti tevékenység*.

A *katonai-szakmai* tevékenység a honvédség alapvető kötelességéhez kapcsolódik. Elsődleges érdek, hogy a honvédség működése és helyzete katonai-szakmai szempontból feleljen meg a törvényi előírásoknak.

A honvédség csak akkor képes teljesíteni az elé tűzött szakmai célokat és követelményeket, ha az azokhoz nélkülözhetetlen *szervezeti tevékenységet* is folytat. Olyanokat, mint a belső szervezeti formák kialakítása, az állomány felkészítése, összetételének a feladatok szempontjából kedvező alakítása, az ellátás és fenntartás feladatai, a működési feltételek stb. A szakmai tevékenységnek prioritása van minden mással szemben. Ez azonban nem jelentheti a szervezeti oldal háttérbe helyezését, hiszen hiánya vagy elégtelen volta megkérdőjelezi a szakmai tevékenység eredményességét.

A haderő ilyen tagoltságú tevékenysége megjelenik az igazgatási irányításban is. A miniszter irányítási hatásköre törvényben nincs egyik vagy másik területre korlátozva, így jogosult befolyást gyakorolni az MH szakmai és szervezeti működésére egyaránt. Ez alapján beszélhetünk a miniszter *szakmai és szervezeti irányítói tevékenységéről*. Abból eredően, hogy a honvédség katonai-szakmai célokat szolgál, a közjogi irányítás elsősorban ugyancsak erre irányul.⁵⁶

Az irányítás és vezetés közti alapvető különbséget az igazgatástudomány abban hangsúlyozza, hogy az irányítást végző személy az irányított *szervezeten kívül* – a hierarchikus kapcsolatból eredően fölötte – áll, addig a vezető az adott szervezet csúcán és mindenképpen *azon belül* helyezkedik el. A vezető a szervezet részeként gyakorol hatást annak helyzetére és tevékenységére.

⁵⁶ Ezt a teljes körű irányítást nevezi a szakirodalom esetenként "totális" vagy "hatósági" igazgatásnak. (LŐRINCZ Lajos: A közigazgatás-tudomány alapjai. Rejtjel Kiadó Kft. Budapest, 1997. 112. oldal.)

Katonai vezetés, katonai irányítás

A *katonai vezetés* (továbbiakban: vezetés) az alárendeltek befolyásolásának folyamata a parancsnokok részéről a katonai tevékenység sikere, a feladat eredményes végrehajtása érdekében.⁵⁷ Jogot és kötelezettséget, hatáskört és felelősséget testesít meg, amelyeket az egyszemélyi vezetőre ruháznak a célkitűzések és követelmények meghatározására, a szervezeti struktúra és az állomány kialakítására, hatékony működtetésére, az alárendeltek tevékenységének szabályozására, irányítására és ellenőrzésére. Lényeges eleme a törvényileg biztosított és ellenőrzött jog (a vezetői hatalom) a vezetői akarat és szándék megfogalmazásához, kinyilvánításához és végigviteléhez a küldetés teljesítése érdekében. Magába foglalja az alárendelt erők (egységek) alkalmazásának jogkörét és felelősségét.⁵⁸

A *katonai irányítás* jelenti azt a hatáskört és felelősséget, amelyet a parancsnok az alárendelt szervezetek tevékenységének egyes összetevői (egy része, egy szakasza) vagy a megerősítő erők felett gyakorol. Vezetési tevékenység, melynek révén a törzs bevonásával szervezi, koordinálja az alárendeltjei és a megerősítő erők tevékenységét.⁵⁹

Az irányítás általában *tipizált* (tipizálható) *eljárásokat* jelent az információs, a kommunikációs, a híradó, az informatikai és más vezetéstechnikai rendszerek, eszközök széles körű alkalmazásával.

A vezetés folyamat-szemléletű megközelítésében az irányítás olyan elem, mellyel a katonai szervezet funkcióit a vezető (parancsnok) az alárendelt vezetők, illetve a *törzsén keresztül* koordinálja. Kiterjed a feladat végrehajtásához szükséges struktúra létrehozására, feltételek megteremtésére és fenntartására, az erőforrások felkészítésére, elosztására és pótlására.

A *vezetés és irányítás* (ebben a sorrendben) egymással szoros kapcsolatban lévő fogalmak, de nem szinonimák. A vezetés szélesebb és komplexebb tevékenység, magába foglalja az irányítás funkcióit. A vezetés szorosan kötődik a *vezető személyéhez*, az irányításban nagyobb a súlya a *törzs tevékenységének*. A vezetői szándék és akarat lényegében az irányítás feladatmeghatározó, szervező és koordináló funkciói révén realizálódik.

57 „A vezetés joghatóság és egy személyre van ruházva. Úgy lehet leírni (de nem meghatározni), mint egy folyamatot, amelynek során a parancsnok az akaratát és szándékát keresztülviszi az alárendeltre abból a célból, hogy egy konkrét tevékenység megtörténjen.” (Szövetséges Összhaderőnemi Doktrína AJP-01B. A HVK hadművelleti csoportfőnökség kiadványa 2003. 0402. pont.)

58 „A vezetés ...magába foglalja a jogkört és a felelősséget a csapatok kijelölésére és felvonultatására a küldetés teljesítése céljából...” (AJP-01B, 0402 pont).

59 „Az irányítás a parancsnok által gyakorolt jogkör ...folyamat, amelyen keresztül a parancsnok a törzs segítségével megszervezi, utasítja és koordinálja a hozzá beosztott kötelek tevékenységét.” (AJP-01B, 0402 pont).

Az előadás a vezetés fogalmát szélesebb értelemben, a tartalmi teljességére utalóan használja. Érti alatta annak valamennyi funkcionális elemét, azonos tartalommal a NATO-ban általánosan elfogadott *"command and controll"* vagy a *"full command"*⁶⁰ fogalmakkal.

Katonai felső szintű vezetés

A előadás alkalmazásában a *"katonai felső szintű vezetés"* az MH katonai tevékenységének egyszemélyi vezetőjét, a *Honvéd Vezérkar főnököt*, annak felelősségi és hatáskörét, valamint vezetői tevékenységét jelöli a szervezeti és támogató elemeivel együtt.

Az előadás alapnak tekinti azt a jogszabályi előírást, miszerint „A honvédelmi miniszter a Kormánynak az ország honvédelmi feladatai végrehajtásáért, valamint a honvédség irányításáért és vezetéséért felelős szakminisztere. A honvédelmi miniszter ...a honvédség vezetését ...a Honvéd Vezérkar főnöke útján látja el.”⁶¹

A HM Honvéd Vezérkar főnök vezeti tehát a Honvéd Vezérkart és a Magyar Honvédség katonai tevékenységét. Szakmai előljáróként végzi a HM hivatalok és háttérintézmények katonai tevékenységével (készenlét, mozgósítás, felkészítés, kiképzés stb.) kapcsolatos szakirányítást.

Vezetési funkciók, a vezetés folyamata és rendszere

A vezető funkcionális feladatai – a vezetési funkciók – közül az információigény és a működési követelmények szempontjából *tervezés és szabályozás*, a *szervezés*, az *irányítás* és az *ellenőrzés* tekinthető alapvetőnek és jellemzőnek.⁶²

A *tervezés és szabályozás* a helyzetadatok értékelésére, a célok és követelmények megfogalmazására, a feladatok előírására, a környezettel való kapcsolatra, az erőforrások előteremtésére és alkalmazási, felhasználási módjára vonatkozó döntések sorozata. Lényege: a szándékolt állapot megvalósítása,

⁶⁰ *Full command* – teljes körű vezetés. Egy szolgálati előljárónak az alárendeltek felé történő parancsadási jogköre és felelőssége. Átfogja a katonai tevékenységek és adminisztráció összes kérdését. Csak a nemzeti haderők viszonylatában, azok keretein belül létezik.

A vezetés szövetségi szinten (nemzetközi értelemben) a jogok lényegesen szűkebb körét jelenti. Egyetlen NATO parancsnok sem rendelkezik teljes körű parancsnoksággal az alárendeltségébe utalt többnemzetiségű erők felett. Az erőket a NATO alárendeltségbe utaló államok csak a hadműveleti vezetést vagy irányítást adják át. (AJP-01B, A fogalmak és meghatározások gyűjteménye).

⁶¹ 2001. évi XLIII. törvény a Honvédelmi Minisztérium és a Honvéd Vezérkar integrációjával érintett törvények módosításáról, 4. § (1) bekezdés és 12. §.

⁶² Dr. KÓTHAY János: A vezetéstudomány helye, szerepe, nézetrendszere. és Dr. MEZEY Gyula kandidátus: Folyamatok, biztonság, adatminőség. Az MH új békevezetési rendszere c. tudományos konferencia anyaga. Hadtudományi Tájékoztató 1998/4. szám 51-63. és 178-185. o.

a kitűzött helyzet elérése érdekében a vezetői célkitűzések feladatokra, részfeladatokra, szervezetekre, időre, helyre történő kibontása, elrendelése és tervbe foglalása.

A tervezés során vázolják és végiggondolják a kitűzött cél elérésének lehetséges változatait, elemzik azokat és kiválasztják a legkedvezőbb változatot. A tervezésnek viszonylag kötött rendje, ebből eredően sajátos információ-igénye van. Többnyire a döntés-előkészítéssel egy-időben kezdődik, lényegi szakasza a döntés után és annak révén, a tervek jóváhagyásával fejeződik be.

A *szervezés* a katonai szervezetek létrehozására, működésük feltételeinek megteremtésére és összehangolására irányul. A szervezés ennek megfelelően legalább két részre tagolható: a szervezetek és a tevékenység szervezésére. Mindkét terület a szervezés központi elemével, a munka- és feladatmegosztással kapcsolatos. Az állandó jellegű és az alkalmi szervezetek létrehozása vagy a feladatokhoz történő igazítása közvetlenül szolgálja a szervezeteken belüli munkamegosztást. A tevékenység szervezése pedig a szükségleteknek megfelelően, a helyzethez igazodva teremti meg a célszerű erőforrás-elosztás feltételeit.

A szervezés egyrészt a mindennapos tevékenység feltételeinek biztosításával kapcsolatos általános teendőket, másrészt a szervezeti struktúrák alakításával kapcsolatos szervezési szakfeladatokat jelenti. A mindennapos operatív szervezői tevékenység a munka összehangolását foglalja magában, eredménye a tervszerűség és a szervezettség. A szakfeladatok a szervezeti elemek harmóniájának biztosítására, a szervezetek külső és belső körülményekhez történő igazítására irányul.

Az *irányítás* központi eleme a valós tevékenység, annak tervszerű megvalósítását szolgálja. Összetett funkció, magába foglal olyan elemeket, mint a koordinálás, a feltételek biztosítása, a részfolyamatok célirányosságának ellenőrzése, valamint a szükséges korrekciók bevétele.

Az irányítás, a koordináció lényege az egyeztetés és összehangolás a tevékenységek tervszerűsége, szervezettsége és eredményessége érdekében. Az erőforrások, a tennivalók és a feltételek összehangolására irányul. Célja, hogy a közösen végzett feladatok a legkisebb ráfordítással, kellő időben, a közös cél érdekében megfelelően, eredményesen kerüljenek végrehajtásra. A koordináció elsősorban a résztvékenységek összehangolását szolgálja.

Az *ellenőrzés* általános célja a vezetés tájékoztatása a kitűzött és a tényleges helyzet/tevékenység egybeeséséről vagy eltéréséről és a kialakult állapotokról. Fontos a szerepe a vezetői szándékok megvalósításában, a döntések helytállóságának igazolásában, a tevékenység hatékonyságának mérésében, a követelmények és az elért eredmények egybevetésében. Eszköze a hibák, a tévedések, mulasztások visszajelzésének, megállapítja azok okait, és javaslatot tesz kijavításuk módjára.

Az ellenőrzés fontos információforrás. Nélküle a vezető nem rendelkezne elegendő és kellően objektív információval a szervezet helyzetéről, az abban zajló folyamatokról. A szervezet tagjai, a munkacsoportok, az egyes szervezeti egységek az ellenőrzés értékelő része nélkül felszínesebb visszajelzést kapnának munkájuk eredményességéről és hiányosságairól.⁶³

A vezetés folyamata

A vezetési funkciók a gyakorlatban folyamatjelleggel jutnak érvényre. Olyan főbb tevékenységek sora jelzi a folyamat teljes ciklusát, mint a *célok kitűzése*, az *információgyűjtés*, a *helyzetértékelés*, a *döntés*, valamint a *feladat meghatározása*. Valamennyi vezetési funkcióban a folyamatelemek láncolata és többnyire együttes eredménye jelentkezik.

Minden vezetési folyamatelem *döntés-centrikus*. A vezető feladatai között az egyik legfontosabb és legnagyobb felelősséggel járó feladat a döntések meghozatala. Megalapozása *hatékony információs rendszert* igényel teljes körű, naprakész adatokkal, információkkal és korszerű döntés-előkészítő eljárásokkal.

A döntés a vezetés *egyik legjellemzőbb*, egyben legkockázatosabb *funkciója*. A döntés lényege a lehetőségek közötti választás, amely utasítás, intézkedés, jóváhagyás, egyetértés, kiadmányozás vagy más formában jelenhet meg. Döntési jogosultsággal a vezető rendelkezik, akinek joga és kötelessége a hatáskörén belül döntéseket hozni.

A döntések *kötelező* (cselekvési és magatartási szabályok) vagy *ajánlás* (irányelv) jellegűek lehetnek. Legfontosabb típusai a döntésnek az *általános* (normatív) szabály és az *egyedi* (konkrét) rendelkezés.

A vezetés rendszere

A vezető tevékenységét, feladatainak ellátását és a vezető szervezetek (törzsek) működését a vezetési rendszer támogatja. Az előadás alkalmazásában jelenti a vezetési feltételek létrehozásához és működtetéséhez szükséges *szervezeti, erőforrás- és eszközrendszereket*, működési (alkalmazási, eljárási) rendjük *elméletét és gyakorlatát*. Ide sorolja a katonai vezető szerveket és azok tevékenységét, a kialakított munkahelyeket (vezetési pontokat) és a feladatokat támogató híradás, informatika és más, pl. a kiszolgálás, a logisztikai támogatás elemeinek szerves egységét.

Az MH béke vezetési és irányítási rendszere többoldalúan meghatározott, azt elvi alapjaiban és gyakorlati feltételeiben a *háborús vezetési rend* alapján kell kialakítani. Struktúrájánál, működési rendjénél és kapcsolatainál

⁶³ A tárgyalt funkciókkal kapcsolatban lényeges hangsúlyozni: külön-külön történt felsorolásukból úgy tűnhet, hogy azok a valóságban is elkülönültek. A tagolásuk azonban csupán a vizsgálatuk szempontjából engedhető meg, a gyakorlatban a funkciók szorosan összekapcsolódnak és átmennek egymásba. Így például, valamennyi funkció az információra épül; a tervezés lényegére nézve döntések sorozata.

figyelemmel kell lenni a csak békében megoldandó feladatokra, valamint a rendszer bővítésének lehetőségére a háborús feladatoknak megfelelően.

A *háborús vezetési és irányítási rendszer* a minősített időszakokban – veszélyhelyzetben, a szükségállapotban, illetve a rendkívüli állapotban – működő rendszer az ott megoldandó sajátos feladatok vezetésére és irányítására.

Viszonylag újszerű fogalma a témakörnek a *békétől eltérő időszak* vezetési és irányítási rendszere. A jogszabályi (alkotmányos) alapjai napjainkig nem kerültek rögzítésre, azok továbbra is az előkészítés fázisában vannak.⁶⁴ Annak az időszaknak és feladat-együttesnek a vezetésére és irányítására kerül kialakítására, amely még nem éri el a minősített időszakok szintjét, de amelyek már lényegesen eltérnek – fajsúlyosabbak, fontosabbak, sürgetőbbek – a béke-időben megszokott rutin feladatoktól. Amikor katonai erők vagy eszközök igénybevételével kell a kialakult helyzetre reagálni. Amikor az adott feladat jellege, súlya nagyobb hatáskört, operatívabb beavatkozást, szélesebb együttműködést követel meg, ami mindenképpen túlmutat a béke állapotra kialakított vezetési rendszer keretein.

A *békétől eltérő időszak* kapcsolódhat pl. a katasztrófa-védelem súlyosabb eseteihez. Kötődhet alacsony, illetve magasabb intenzitású (fegyveres) válság-helyzetekhez, amelyek ugyan a határainkon kívül alakulnak ki, de hatással lehetnek hazánkra és végső soron átnőhetnek háborús konfliktusba. Ide tartozhatnak az országhatáron kívüli 5. cikkely és a nem 5. cikkely (békeműveletek) szerinti műveletek.

Általános követelmények

A békétől eltérő (minősített) időszakok vezetési és irányítási rendszer kialakításával és működésével szemben az alábbi általános követelmények határozhatók meg:

- a meglévő béke-irányítási és vezetési rendre épüljön, alapjait egységes követelmények képezzék;
- vegye figyelembe a háborús (minősített) időszaki rendszert, az abba való átmenet legyen fokozatos, ne követeljen meg drasztikus beavatkozást;
- legyen gyorsan aktivizálható;
- a felépítése a kihívásoknak megfelelően fokozatosan, illetve egy lépésben (azonnal) bővíthető és csökkenthető legyen;
- belső szervezete (a bevont szervekkel, személyekkel) minden lehetséges feladatot le tudjon fedni;
- egy időben biztosítsa a tervezés, szervezés, valamint a katonai szervezetek más vezetési és irányítási feladatainak végrehajtását,
- rendelkezzen a feladatokat segítő adatbázissal;

⁶⁴ Az Alkotmány módosításáról szóló törvényjavaslat és indoklása. Kézirat. HM Igazgatási és Közjogi Kodifikációs Főosztály 2003.

- több csatornán tartson kapcsolatot az előljáró, az alárendelt és az együttműködő szervekkel;
- rendelkezzen tartalék vezetési pontokkal (működési helyekkel);
- legyen a híradás, az informatikai és a más biztosítási fajta tekintetében korszerűen támogatott és információ védett,
- rendelkezzen a szükséges mobil szállító és vezetési eszközökkel;
- legyen kellően begyakorlott és felkészült;
- legyen képes hosszú ideig működni, ezért biztosítsa a váltásos munkarendet,
- feleljen meg a törvényességnek (hatáskörök, jog- és felelősségi körök, járandóságok jogszabályok szerinti biztosítása).

A békétől eltérő (minősített) időszak vezetési rendszere a *felső*-, a *közép*, valamint a *csapat szintű* rendszer-elemekből épül fel.

2. A felsőszintű vezetés sajátosságai

A felsőszintű vezetési rendszer *rendeltetése*: a kialakult helyzet elemzése és értékelése, a Honvédelmi Tanács, a Kormány, a honvédelmi miniszter és a HVKF döntéseinek előkészítése és ennek megfelelően a fegyveres erőkre és a rendvédelmi szervekre vonatkozó feladatok megtervezése, a tevékenységet támogató polgári vonatkozású igények megfogalmazása, valamint a katonai szervezetek vezetése és irányítása.

Feladatai:

- a háborús, az 5. és a nem 5. cikkely (békeműveletek) szerinti tevékenységek, valamint a válságkezelés során a Honvédelmi Tanács, a Kormány, a HM és a HVKF döntéseinek katonaszakmai előkészítése, a tervezési, szervezési folyamat végrehajtása mind honi, mind a határon túli területeken;
- katasztrófa-helyzet kezelése;
- intézkedés a kijelölt erők felkészítésére és kiképzésére, műveleti tevékenységük megtervezésére és azok végrehajtására;
- átcsoportosítások, szállítások megtervezése mind honi, mind külföldi területen;
- adatok gyűjtése, elemzése, értékelése, jelentések összeállítása;
- a veszteségpótlás, utánpótlás megtervezése;
- a Befogadó Nemzeti Támogatás feladatainak kezelése;
- kapcsolat és összeköttetés fenntartása az előljáró, az alárendelt és az együttműködő szervekkel;
- a végrehajtó szervezetek és a tevékenységük ellenőrzése;
- a végrehajtó szervezetek támogatása;
- a tevékenységek felső szintű vezetése és irányítása.

A felsőszintű vezetési és irányítási rendszer kialakításának lehetőségei

A jelentkező feladatok kezelésére a HM Honvéd Vezérkar csoportfőnökségeiből, az érintett minisztériumi szervek, a háttérintézmények, a HM közvetlen irányítása és felügyelete alá tartozó szervek, a haderőnemi parancsnokságok, az MH Összhaderőnemi Hadművelési Központ (MH ÖHK), az MH Budapesti Helyőrség-parancsnokság, valamint az együttműködő szervezetek bevonásával HVK *Vezetési Operatív Csoport* (VOCS) kerül aktivizálásra, illetve alkalmazásra.⁶⁵

A VOCS-on belül a funkcionális feladatok koncentrációja és megosztása, a tervező, szervező, valamint az irányító, vezető funkciók szétválasztása érdekében különböző *munkacsoportokat* célszerű megalakítani. (A VOCS-ba be nem osztott állomány a békefeladatait végzi, illetve szükség esetén pótolja a VOCS állományát, vagy más feladatokat hajt végre).

Külön *összekötő (munka-) csoportokat* célszerű kialakítani az összeköttetés fenntartása, a kimenő és bejövő adatok, információk feldolgozására.

A kiszolgáló, biztosító és *támogató csoportok*, illetve személyek szorosán véve nem képezik ugyan a VOCS állományát, azonban a tervezés és feladat-végrehajtás szempontjából fontos azok megjelenítése is. A csoportok kialakítása során, valamint a létszámok meghatározásánál a végrehajtandó *feladatokból kell* kiindulni. A folyamatos működés érdekében a 24 órás *váltási rendet* célszerű alkalmazni. Ez azt jelenti, hogy békeidőszakban három (a törvényi járandóságok biztosítása érdekében), minősített időszakban kettő váltás működik úgy a vezető, mint a törzs és támogató állományból.

A vezető szervek, munkacsoportok *elhelyezéséhez* fel lehet használni a HM I objektum munkahelyeit (a tervező csoport részére), az MH ÖHK elhelyezési körletét (irányító csoport részére) és vezetési objektumait (a vezetési pontok operatív része), valamint más HM objektumokat és munkahelyeket.

Veszélyeztetettség esetén, illetve minősített időszakokban a vezetés folyamatosságának, a vezető szervek életképességének biztosítása érdekében *fő és tartalék vezetési csoport* létrehozása célszerű.

A *híradó, az informatikai* és más *támogatás* alapja a békében is működő rendszer lehet, kiegészítve a szükséges eszközökkel és anyagokkal, valamint bevezetett rendszabályokkal.

A vezetési (munka-) csoportok *aktivizálását* a békében működő 24 órás szolgálatokon keresztül célszerű megoldani.

A VOCS, a munkacsoportok, illetve a szolgálati személyek részére a *feladatokat* Szervezeti Működési szabályzatban (SZMSZ) és munkaköri leírásokban szükséges rögzíteni. A feladatok megjelennek a szervezetek készenlét-fokozási terveiben. A személyek, munkacsoportok felkészítéséért, az adatok

⁶⁵ Az együttműködő szervezetek bevonásának lehetőségét és rendjét a Kormány 3053/1998. sz. határozata szabályozza.

naprakészen tartásáért a biztosító szervezet, illetve a munkacsoport vezetője felelős.

3. A haderőnemi, valamint a csapatszintű vezetés sajátosságai

A középszintű vezetés a szárazföldi csapatok, a légierő, valamint a logisztikai és támogató csapatok haderőnemi sajátosságokkal rendelkező vezetési rendszerére épül.

Szárazföldi Csapatok

Az MH Szárazföldi Parancsnokság (SZFP) az egész szervezetével nem old meg békétől eltérő (minősített) időszaki feladatokat (hadművelati vezetést).

A parancsnokság állományából kijelölt Vezetési Operatív Csoport feladatai:

- az Alkotmány 19/E §-ban meghatározott feladatok tervezése, szervezése és vezetése;
- az alárendelt katonai szervezetek alaprendeltetése ellátására való folyamatos felkészítés és kiképzés, a művelési alkalmazásának tervezése, szervezése, vezetése és ellenőrzése a HVKF követelményei és a HM HVK által kidolgozott alapelvek szerint;
- a határbiztosításra (Honvédelmi Törvény 22. §. (1) bek. b) pont) kijelölt erők tevékenységének tervezése, szervezése és közvetlen vezetése kijelölt mozgó VOCS –csal;
- a tevékenységek eszkalálódásának kezdeti időszakában a művelet közvetlen vezetése a HVK irányításával;
- a magas készenlétű parancsnokság beérkezésekor, szárazföldi komponenssel vagy a szükséges elemekkel annak kiegészítése;
- a Magyar Köztársaság fegyveres védelme érdekében az ország határain belül nemzeti vagy NATO vezetés alatti összhaderőnemi műveletekben való részvétel biztosítása;
- összekötő csoport működtetése a NATO parancsnokság mellett mind hazai, mind külföldi területen a magyar erők tevékenységének koordinálása céljából;
- felkészülés a külföldön tevékenykedő dandár vezetésének rotálása érdekében egy dandárnyi erőhöz szükséges vezető szerv létrehozására;
- az alárendelt csapatok készenlét fokozásának és fenntartásának, mozgósítási feladatai végrehajtásának tervezése, szervezése, ellenőrzése, az elrendelés és a végrehajtás feltételeinek biztosítása;
- a szárazföldi haderőnemtől kijelölt készenléti és szárazföldi fegyveres készségi alegységek felkészítésének, kiképzésének, alkalmazásának tervezése, szervezése és vezetése;
- a szolgálati alárendeltségébe tartozó nemzetközi válságkezelő műveletekben résztvevő katonai szervezetek felkészítésének, alkalmazásuk

-
- esetén átcsoportosításának, telepítésének, a Befogadó Nemzeti Támogatásának, váltásának tervezése, szervezése, koordinálása és irányítása;
- a Katasztrófavédelmi Rendszer keretében az ipari és természeti katasztrófák elhárításában, illetve humanitárius segítségnyújtásban résztvevő katonai erők közvetlen vezetése;
 - a szárazföldi haderőnemnél a harcászati felmérő és értékelő program (OPEVAL) tervezése, szervezése és végrehajtásának irányítása.

A békétől eltérő időszak feladatainak végrehajtására létrehozott csoportokat folyamatosan, a várható alkalmazásuknak megfelelő célirányos *felkészítésben, kiképzésben és összekovácsolásban* kell részesíteni, amely módszerében kiterjed az egyéni felkészüléstől a CAX gyakorláson keresztül a nemzetközi gyakorlatokig. Az SZFP VOCS *működési helye*: stacioner vezetési pontként Székesfehérvár, mobil VOCS -csal a szükséges szállító és híradó, informatikai eszközökkel az alkalmazás körzetében a közvetlen vezetés biztosítása a HVK irányításával.

Légierő

A Magyar Honvédség Légierő Parancsnokság (MH LEP) a Magyar Honvédség középszintű haderőnemi parancsnokságaként, a Magyar Honvédség alkotmányos rendeltetésének teljesítése érdekében a légierő részére meghatározott feladatok végrehajtásával, a szövetséges fegyveres erőkkel együttműködésben biztosítja a Magyar Köztársaság *légterének szuverenitását*, valamint a szövetségi kötelezettségeknek történő megfelelés érdekében részt vesz a légierő hadműveleti feladatok megoldásában.

Az MH LEP feladatait mind béke, mind békétől eltérő időszakban a NATO *egységes légvédelmi rendszerének* keretein belül, annak részeként hajtja végre. A vezetési struktúrája a NATO egységes vezetési rendszerének megfelelően épül fel. A nemzeti érdekű feladatok a NATO déli szárnyának légierő parancsnokságával egyeztetve kerülnek végrehajtásra. A MH Légierő Parancsnokság és alárendelt katonai szervezetei számára a nemzeti vezetési rendszerben a *HM HVK*, míg a NATO vezetési rendszerében közvetlenül a *Déli Régió Légierő (Komponens) Parancsnokság* illetékes szervezeteinek vezetői jogosultak a vezetésre vonatkozó intézkedések, utasítások kiadására.

A NATO parancsnokság alá tartozó illetve NATO számára *felajánlott erők* számára külön intézkedésben meghatározott esetekben (TOA - Transfer of Authority = jogok átadása után), az illetékes NATO szervezet felelős vezetője *közvetlenül*, a felelősségi köréhez tartozó tárgyban jogosult a megfelelő intézkedések meghozatalára.

Fő feladatai:

- honi területen, az államhatár mentén a válságkezelés feladatainak vezetése érdekében – a szárazföldi erők légi támogatásnak irányítására – a megalakításra kerülő MH SZFP VOCS-hoz összekötő csoport kiküldése;

-
- külföldi részvétel esetén a kiküldésre kerülő összekötő csoporthoz a megfelelő szakmai felkészültséggel rendelkező kiegészítő létszám biztosítása;
 - a haderőnemhez tartozó katonai szervezetek alaprendeltetés ellátására való folyamatos, a NATO hadműveleti eljárások szerinti felkészítésének tervezése, szervezése;
 - a haderőnem csapatai felkészítésének és kiképzésének tervezése, szervezése és ellenőrzése a HM HVKF követelményei és a HM HVK által kidolgozott alapelvek, valamint a Szövetséges Hatalmak Európai Legfelsőbb Parancsnoksága ajánlásai alapján;
 - légi készenléti szolgálat működtetése Magyarország fegyveres védelme érdekében, az ország határain belül, nemzeti vagy NATO vezetés alatt;
 - felkészülés az ország határain kívül, a Washingtoni Szerződés V. cikkelye szerinti hadműveleti feladatokban, valamint – nemzetközi szervezetek vezetése alatt – békétámogató műveletekben való részvételre;
 - a MK légi riasztása megszervezése és biztosítása;
 - részvétel a Honvédelmi Katasztrófavédelmi Rendszer keretében az ipari és természeti katasztrófák elhárításában, illetve humanitárius segítségnyújtásban;
 - a légierő erőinek és eszközeinek közreműködése az ország határain kívül – az ország működőképességét, lakosságának életét, vagyonát és rendjét veszélyeztető – különböző katasztrófák következményeinek felszámolásában való részvétel esetén;
 - a HM HVKF felhatalmazása alapján együttműködés a haderőnemen kívüli szervezetekkel;
 - az MH LEP és az alárendelt katonai szervezetek tevékenységének mindenoldalú biztosítása.

A LEP *működési helye*: stacioner vezetési pontként Veszprém. Az MH SZFP VOCS-hoz kiküldésre kerülő *összekötő csoportot* mobil vezetési eszközökkel felszerelt, bárhol telepíthető szervezetként szükséges kialakítani.

Az MH Összhaderőnemi Logisztikai és Támogató Parancsnokság

Fő feladatai:

- a HM HVK követelményei alapján részt vesz az MH békétől eltérő (minősített) időszaki logisztikai támogatási terveinek kidolgozásában, valamint az MH közép- és hosszú távú fejlesztési terveinek összeállításában;
- vezeti és szakmailag irányítja a fogyasztói logisztika vonatkozásában a fejezet gazdálkodási szakterületeit;
- integrált ellátó központok működtetésével biztosítja az MH haditechnikai eszközeinek, anyagainak és hadfelszereléseinek tárolásával,

-
- üzembentartásával, valamint a személyi állomány ellátásával kapcsolatos feladatok végrehajtását;
- ellátja az ország közlekedési rendszere hadművelleti követelmények szerinti honvédelmi felkészítésének szakmai felügyeletét, szabályozza a külföldi és hazai katonai csapatmozgások közlekedési biztosítását, szállítmányok kísérését, együttműködik a polgári közlekedési szervekkel;
 - ellátja az ország területén talált lőszeres és robbanóanyagok felkutatásának, hatástalanításának, a lőterek, gyakorlóterek tűzszerész mentesítésének felügyeletét;
 - végzi az MH szintű meteorológiai és térképészeti támogatás, valamint a nyomdai szolgáltatások végrehajtásának irányítását;
 - felügyeli és irányítja az MH-ban folyó mérésügyi tevékenységet;
 - működteti a Kormány és a HM HVK speciális erősítési létesítményeit;
 - tervezi, szervezi és ellenőrzi szolgálati alárendeltjei vonatkozásában a munkavédelmi és tűzvédelmi tevékenységgel kapcsolatos feladatokat;
 - a HM GTH-tól átveszi az erőforrás tervezés kapcsán a logisztikai gazdálkodási és információs rendszer rendszergazda szerepkörét, továbbá a minősített időszakos MH szintű feladatok kezelését és a kodifikációs feladatokat;
 - megalakítja és végzi a civil-katonai és együttműködési központ feladatait.

Az ÖLTP működési helye: stacioner vezetési pontként Budapest. Az MH SZFP VOCS-hoz kiküldésre kerülő összekötő csoportot mobil vezetési eszközökkel felszerelt, bárhol telepíthető szervezetként célszerű kialakítani.

A csapatszintű vezetés jellemzői

A Magyar Honvédség szervezetében a jövőben lényegében *kettő dandárnyi* erővel számolunk. Az egyik dandár az 5. cikkben foglaltaknak megfelelő feladatokra való készenlétben tartásra, valamint különböző hadművelti-harcászati feladatok végrehajtására készül fel. A másik dandár a nemzeti érdekből történő feladatok megvalósítására, határbiztosítási feladatok ellátására áll készen.

A fentiekkel összhangban a dandároknak olyan mobil eszközökkel kell rendelkezniük, amelyek biztosítják egy *fő és egy tartalék vezetési* pont folyamatos működtetését honi és külföldi területen. A feladatokhoz a rotációt biztosító dandár szintű vezetési csoportot, az EH-nak megfelelő operatív csoportot és az összekötő csoportot mobil vezetési eszközökkel felszerelt, bárhol telepíthető szervezetként kell kialakítani. Az alegységeknek (zászlóaljoknak) a harc vezetésére szolgáló *mozgó harcállásponttal* kell rendelkezniük, amely biztosítja az előjáróval és az alárendeltekkel történő folyamatos összeköttetést.

INFORMATION INTEROPERABILITY AND COMMUNICATION

*Department of Informatics, National Defence University Miklós Zrínyi
Budapest, Hungary. e-mail: munk@zmne.hu*

1. Introduction

From the end of the 20th century, in the emerging Information Age, information and infocommunication capabilities possessed by different actors are increasingly significant resources used to effectively and efficiently fulfil their activities. The actors usually don't act alone, they can only achieve their goals in cooperation, coordinated with other actor's. Role of information capabilities necessary to cooperation is especially significant in execution of those complex operations that require coordinated actions of a mission-oriented and in many cases dynamically changing group of several actors.

Information interoperability is one of the most important components of operational interoperability, and its significance is continually grows. It has three – technical, syntactical, and semantical – levels, that are built on each other. Communication is a basic condition of cooperation, and without it there is no even information interoperability. Military publications practically have payed no attention so far to the role of communication in information interoperability.

The objective of this publication is to summarize the basic concepts and characteristics of information interoperability, to analyse the levels of information interoperability and to describe their main features, and finally to study the role of communication in ensuring information interoperability, and the potential changes of this role.

2. Basics of information interoperability

Interoperability in general is a relation between/among two or more objects, a mutual capability necessary to ensure successful and efficient interoperation, supporting cooperation.⁶⁶ Subjects of interoperability are active objects that can be organised groups of humans acting consciously (forces, groupings, organisations, etc.), or technical systems operating purposefully (equipments, functional units, etc.). Accordingly we can differentiate interoper-

⁶⁶ Details can be found in MUNK: An analysis of basic interoperability related terms, system of interoperability types.

erability between/among actors, and between/among equipments. In the military literature these two types are most frequently called operational interoperability, and technical interoperability.⁶⁷

Fundamental condition of successful and efficient operation of complex organizations, organizational systems, groupings is the sufficient level of information exchange between components, the sharing, and coordinated exploitation of information necessary for cooperation. In case of heterogeneous components there is an additional condition, the information interoperability of the cooperating forces that in our opinion, in its broader sense can be defined in the following way:

Information interoperability is a mutual capability of different actors necessary to ensure exchange and common understanding of information needed for their successful cooperation.

Information interoperability can be interpreted in partly different, but analogue manner in case of individual persons, and organizations. Concepts of information, and knowledge in our interpretation are connected to human mind.⁶⁸ The previous is a reflection, an inner, mental representation of a delimited aspect of the world, and the later is the mental representation of the whole world. In the course of information exchange between people one party (the sender) transforms a piece of his/her knowledge into a representation appropriate for transmission, and this outer representation gets to the other party (the receiver), who interprets it, and develops an own inner, mental representation, and inserts it into his/her knowledge. Thus eventually not the information itself is transmitted, but it is represented, the representation is transmitted, and an "other" information created on the basis of this representation.

Common understanding means, that parties of information exchange perceiving identical items of communication, interpreting identical outer representations develop an appropriately identical mental representation (in this case appropriately identical for the purposes of cooperation). In other words common understanding means that the interpreted meaning of the given representation developed by the receiver corresponds with a required level to the intended meaning, determined by the sender.

In case of information exchange between organizations, organizational information is interpreted – analogously to the concept of personal information – as a reflection, inner mental and/or outer representation of a delimited aspect of the world, in the organization. So organisational information can simultaneously exist in both form, in the mind of members of the organization, and in the form of some outer, recorded representation. These later can be recorded

⁶⁷ See for example in "Realizing the Potential of C4I", Chapter 2.

⁶⁸ Details can be found in MUNK: Információs színtér, információs környezet, információs infrastruktúra.

on traditional media, and stored in information systems, devices, and applications in "informational" formats.⁶⁹

Basic model of inter-organisational information exchange consists of the following tasks:

- ☐ - some piece of information in the human mind represented in an appropriate representation (if required);
- ☐ - representation resulted from the previous step, or already existing in recorded format is transformed to an intermediary representation appropriate for transmission (if required);
- ☐ - intermediary representation is transmitted to the receiver;
- ☐ - intermediary representation received is transformed (back) to a representation appropriate for the receiver (if required);
- ☐ - the resulted representation is interpreted, transformed to information, i.e. to an inner mental representation (if required).

As it can be seen from the above, almost all steps of the information exchange process – except for transmission of the intermediary representation – are representational transformations, where the basic requirement of the information interoperability (the information exchange based on common understanding) is to preserve the intended (planned) meaning carried by representations.

3. Levels of information interoperability

Information interoperability requires different components, and capabilities, that are almost uniformly classified into three groups, into three levels. These are: the technical level of the physical representations; the syntactical level of the intermediary (non-physical) representations, and the semantical level related to the interpretation (meaning) of the representations. In the following we will discuss the basic concepts and features of these levels and their interrelationships.

The technical component of information interoperability (technical level information interoperability, shortly technical interoperability) is the group of capabilities to handle – create, transmit, and present – physical (material) representations carrying information. In broader sense this component can be interpreted in case of information exchange without use of devices, but in the following we will discuss only capabilities related to organizational information exchange supported by technical systems.

Physical (technical) condition of information exchange is the existence and purposeful operation of "interoperable" devices, or systems, appropriate for the given representation. Interoperability of devices means, that the physical representation, or material medium created by one device can be received, processed by the other device. In the framework of division of labour an inde-

⁶⁹ In our days this format is typically, but not exclusively electronic and digital.

pendent functional area (communication, telecommunication), and a specialized system of technology (communication systems) evolved, that took over most of the tasks of ensuring technical interoperability, from the parties involved in information exchange.

During information exchange end-devices (interfaces) of the communication system receive information in predefined formats of physical representations, and transmit it to an other end-device (interface), to the receiver. Inside the communication system there can happen other representational transformations, but these are unimportant and transparent for the parties involved in information exchange. The communication system guarantees secure transmission of this representation without any modifications, according to an agreed quality of service (QoS) level. The concept of technical interoperability with respect to information interoperability can be defined in the following way:

Technical level information interoperability is a mutual capability of different actors to exchange physical representations carrying information necessary for efficient cooperation (with the help of the available communication infrastructure, and appropriate communication devices).



The syntactical component of information interoperability (syntactical level information interoperability, shortly syntactical interoperability) is the group of capabilities to handle intermediary representations built on top of physical representations. In practice these capabilities related to knowledge about languages, message- and data formats used in information exchange.

Syntactical interoperability capabilities necessary for traditional information exchange include knowledge and application of rules on format of spoken, and written languages, or symbolic representations (mathematical formalisms, technical drawings, military symbols of situation, etc.). Syntactical knowledge of representations used in traditional devices are built into the devices itself as embedded knowledge.

In case of information systems, and devices syntactical interoperability in first approach can be interpreted as a capability to exchange and application of different representations of information. Requirements of syntactical interoperability are primarily determined by the information categories, individual information necessary for cooperation, since transmission, exchange of these information are preconditions of successful cooperation.

Information exchanged by the parties are handled in predetermined representations, that can be the same, and can be different. In the first case eventually there are no any difficulties during information exchange, but in the second case it is necessary to make intermediate transformation, or transformations. So the concept of syntactical interoperability can be defined as follows:

Syntactical level information interoperability is a mutual capability of different actors to exchange intermediary representations of information necessary for efficient cooperation (with optional transformations if required).

So information interoperability on the syntactical level can be reached in two fundamental ways: with the standardization of information representations, ensuring their sameness, or with development of conversion capabilities between different formats. Information exchange between systems with syntactical heterogeneities (with different representations) can be done using the representation of one of the systems, or using an intermediary, mediator representation, different from the primary representations.



The semantic component of information interoperability (semantical level information interoperability, shortly semantic interoperability) is the group of capabilities related to exchange of different representations preserving their intended meaning. Meaning, that humans assign to environmental effects, messages, and data, is basically subjective, strongly connected to individuals. Identical (if it is possible at all), or similar reflection can be reached only in the course of cooperation, or with communication. Common interpretation, developed and confirmed in practice, is a prerequisite of successful cooperation, and communication.

Concepts used with common understanding in a group of people, and information based on these concepts is no longer dependent on subjectum of individual members of the group. All members of the group perceive, and interpret the environmental effects, things and phenomena of the world in the same way⁷⁰, so they can also provide and receive information about these objects with (sufficiently) identical content and meaning. These concepts, and information are group-subjective (or inter-subjective), because they depend on the common, agreed interpretation of the group. In this sense we can talk about the meaning of an environmental effect, message, or data, pertaining to a given group.

For the purposes of storage and transmission, or operation of automated devices, different components of human knowledge can be recorded, stored, and utilized using traditional or electronic media, or systems. Knowledge components objectified in different forms (text, data, program, rules, drawing, picture, audio, video, etc. and any combinations of these) usually are available for other people to use. Information storage, and processing devices obviously are not able to interpret data stored, or processed, they 'do not know' their meaning. Only people utilizing these devices can assign meaning to data.

⁷⁰ To be more precise, as we have said earlier: in a way similar enough for cooperation.

So only an intended meaning, planned interpretation can be assigned to knowledge components stored on information media, or in information systems (and any devices with information functions), and it should be connected to users of these systems (devices), or to information providers. The intended meaning, agreed intentions, and interpretation of the primary users are usually determined in the purpose and functional requirements of the given system. Conditions of common interpretation suitable to purpose of the given system can be ensured partly by direct communication with primary users, partly by different documentations supporting application of the given system.

According to the discussions done above, the concept of semantic interoperability can be defined in the following way:

Semantic interoperability is a mutual capability of different actors to exchange representations of information necessary for efficient cooperation, in a way that preserves meaning (with optional transformations if required).

4. Ensuring information interoperability in communication systems

In this section we discuss the role, and new possibilities of communication in ensuring information interoperability. Communication is transmission, receiving, or exchange of (in narrower sense) information, or (in broader sense) information, values, behavioural patterns and ideas. According to the appropriate NATO glossary communication is "information transfer according to agreed conventions"⁷¹. Communication can be direct (such as in case of speech, gestures, etc.), that requires simultaneous participation of the parties and ensures bidirectional information exchange, and can be indirect (such as writing, data, etc.), where the simultaneous participation is not required, but as a consequence, continuous feedback is not possible. There are also intermediate forms, e.g. electronic mail, that can be considered a quasi-direct communication.

Media, carriers, intermediary representations used in information exchange, can be classified into three broad groups. These are the following: "carriers" used during interpersonal communication (speech, metacommunication); traditional media used in indirect information exchange, that can be created and interpreted without technical devices; and finally media that require technical devices. In this latter group we can distinguish media related to traditional devices, and media related to modern, infocommunication, or information technology equipments. Finally telecommunication is communication by technical (wire, radio, optical or other electromagnetic) systems.⁷²

⁷¹ AComP-01(A) NATO Communications Glossary, 701.01.04 Communication [2-701-1.o.].

⁷² AComP-01(A) NATO Communications Glossary, 701.01.05 Telecommunication [2-701-1.o.].

From the different versions mentioned above, due to the revolution of information technology, the traditional media are continuously pushed into the background, specifically they are replaced by functionally fully equivalent IT-based representations⁷³, that have even better features and can be handled more efficiently. As a consequence of this process, most and a continually growing part of communication between organizations is realized using infocommunication systems, and devices.



Communication is a basic condition of information interoperability between different actors of the infosphere, because successful information exchange, cooperation in general is impossible without communication. Communication technologies, communication infrastructure, and communication systems for a long time have supported elimination of different kinds of heterogeneity, have helped to hide these heterogeneities from actors participating in information exchange. The first task was to manage the differences between end-devices of the same network, and this was followed by the task to connect dissimilar networks, with different protocols, and parameters. Nevertheless these were only heterogeneities inside the communication system, that are not in direct connection with the information exchange between parties, but with the technical solutions of it.

Traditional forms of communication support information exchange only in a content- and meaning-independent way. After a given end-device transforms the information intended to send, into an appropriate intermediary representation, the communication system guarantees secure transmission of this representation without any modifications, according to an agreed quality of service (QoS) level. In broadest sense the same happens in case of courier and postal services, where mails, and other postal parcels in physical form are transported from senders to receivers. The 'without any modification' attribute is valid only from the point of view of the communicating parties, inside the communication system any transformations can happen transparently for them.

This means that up to the present, in case of communication interoperability issues basically have not arisen to solve heterogeneity problems between the parties involved in information exchange, but to overcome heterogeneities inside the communication system itself. Traditional communication systems, as a matter of fact, were not able to transform the content, or format of messages transmitted: e.g. to selectively transmit a part of a telegram; to translate a message into a different language; to deliver a telegram in form of facsimile, or a short message system (SMS) in form of a telegram.

⁷³ Texts, drawings, pictures, sound- and video materials, etc. represented mainly, but not exclusively in electronic digital format.

In modern infocommunication systems, based on the integration of information processing, and communication functions, have already evolved the basic conditions of handling other kinds of heterogeneity of information exchange. This enables that in the future communication can mean not only transmission of intermediary representations, but to some extent transfer of content, and meaning. Since communicating parties want to give, or exchange knowledge, information (irrespective of their appearance, or representation), and not to transmit telegram, SMS, e-mail, or letters.

A digital communication infrastructure having information processing capabilities can provide a lot of services in the future, that support information interoperability. These services first of all could support the handling of syntactical differences. Based on these services communication systems can get information from the sender in a given format, and after transmission and optional transformation(s) deliver it in an other format to the receiver. This will probably happen first in case of audio-visual, and textual representations.

These new services enable, for example, seamless linking of videoconference terminals, videophon devices that use different formats, or transmission and presentation in required format of still, and motion pictures acquired by videocameras working in different formats. It would be possible to handle different textual formats, and transform one to the other too, so it frees users from the task of transformations. All these can be implemented similar to a situation, where traditional analogue, and newer, ISDN telephones are connected to the ISDN network through the same ISDN equipment.

Services supporting information interoperability based on software components implemented in communication end-devices, and switches. Earlier these software components were able to work only in computers, but nowadays information processing and storage capabilities have already appeared in almost every communication devices. Software components originally supported the effective implementation, and flexible development of primary communication functions, so it was "only" a new technical solution for an old problem. The next step was the implementation of different value-added services (more comfortable user interfaces, address lists, etc.). Finally the complex functions necessary to ensure interoperability were made possible by the continuous growth of processing and storage capabilities.

In summary we should come to the conclusion, that communication systems of the XXI. century must have the appropriate capabilities to support information interoperability. In addition to secure transmission of messages, they must be able to make necessary conversions between heterogeneous representation formats used by different users, in order that make easier the information exchange between cooperating parties.

References

1. AComP-01(A), NATO Communications Glossary. English and French. – NATO Military Agency for Standardization, Brussels, 2000.
2. Munk, Sándor: An analysis of basic interoperability related terms, system of interoperability types. – Academic and Applied Research in Military Science, 2002/1. (pp 117-132)
3. Munk Sándor: Információs színtér, információs környezet, információs infrastruktúra. – Nemzetvédelmi Egyetemi Közlemények, 2002/2. (pp 133-154)
4. Realizing the Potential of C4I: Fundamental Challenges. Chapter 2. Interoperability. – National Academy Press, Washington, 1999.
5. [<http://books.nap.edu/html/C4I/ch2.html>]

ADAPTÍV ANTENNARENDSZER SZIMULÁCIÓJA

A technikai, technológiai, és még inkább az információs robbanás lökéshullámai napjainkban sem látszanak veszíteni intenzitásukból. Sőt... Az információra éhes fejlett, és egyre inkább a fejlődő társadalmak növekvő igényei folyamatos versengésre készítetik a kutató-, tervező- és fejlesztőmérnököket, újabbnál újabb látványos, hasznos, vagy akár csak hasznosnak tűnő megoldások kidolgozásában. Lassan befejeződik (vagy már be is fejeződött) a telekommunikáció és informatika teljes integrációja (telematika), gondoljunk csak a mobiltelefon társaságok GPRS (a jövőben UMTS) alapú Internet hozzáférést biztosító szolgáltatásaira, vagy az IP telefóniára. Az információk megszerzésére és birtoklására irányuló, rohamosan növekvő kereslet kielégítése („az információ hatalom”) sok fejtörést okoz a szolgáltatóknak.

Hasonló helyzetben van a Magyar Honvédség is azzal az apró különbséggel, hogy „információs robbanásról” még nemigen beszélhetünk. A fejlesztés ugyan folyamatos (MH digitális távközlési hálózat, MH zártcélú mikrohullámú hálózat, Kongsberg URH harcászati rádiók), azonban ennek sebességét a lehetőségekhez képest fokozni kellene. Igazság szerint, míg a fejlett nyugati államokban a katonai alkalmazások fejlesztése megelőzi a polgári fejlesztéseket, addig nálunk csak kullog utána. Csak remélni lehet, hogy a korszerűsítésre irányuló törekvések a reformok következtében felgyorsulnak, és néhány éven belül egy technikailag fejlett, európai színvonalú Magyar Honvédség oltalmazhatja az ország szuverenitását, képviselheti Hazánkat a NATO-ban.

Írásomban egy olyan témával foglalkozom, amelyben mind a katonai, mind a polgári célú alkalmazások területén számos lehetőség rejlik. Ez pedig nem más, mint az adaptív antennarendszerekkel történő iránybecslés.

Adaptív antennarendszerekben rejlő lehetőségek

Ha egy rendszerben az antennákkal szemben támasztott követelmények nem elégíthetők ki egyszerű eszközökkel, lehetőségünk van összetett, elektronikusan vezérelt antennarendszerek alkalmazására. Ezek adaptív jelfeldolgozó algoritmusok segítségével alkalmassá válnak a kívánt iránykarakteristikák kialakítására. Alkalmazásuk lehetőséget nyújt a térben tetszőlegesen mozgatható tűnyalábok létrehozására anélkül, hogy maga az antennarendszer a helyzetét fizikailag megváltoztatná. Az adaptív módszerekkel történő iránymeghatározás mind a polgári-, mind a katonai mobil hírközlésben fontos szerepet tölthet be. Néhány példa a teljesség igénye nélkül:

Katonai célú alkalmazási lehetőségek:

1. A zavaró rádióadók bemérésére: A hadszíntéren, az ellenség csapatainak kommunikációját megnehezítendő gyakran működtetnek zavaró rádióadókat. Ezek hatása csökkenthető oly módon, hogy az antennarendszer karakterisztikájában nullhelyet illesztnek a zavaró források irányára.
2. Felderítés elleni védelem: A rádióforgalom lehallgatása megnehezíthető, ha az adóoldalon egy tűnyalábbal sugározunk a vevő irányába, ezáltal lehetetlenné téve az egyéb irányokból történő vételt.
3. Célkövetés: A rádióforgalmat bonyolító járművek (helikopterek, páncélosok stb.) ill. személyek helyzete felderíthető, mozgása követhetővé válik, sőt adott esetben akár a fegyverek célravezetésében is hasznos segítséget jelenthet a megfelelően kialakított adaptív antennarendszer. (Jelenleg korszerű vadászgépek (F-15, SZU-27) fedélzeti radarjai működnek ezen az elven, melynek segítségével egyszerűen több cél ellen is képesek rakétát indítani)

A polgári életben leginkább a mobil kommunikáció területén alkalmazhatók nagy hatékonysággal az adaptív iránymérő módszerek. A bázisállomás egy-egy tűnyalábbal követi a forgalmat bonyolító mobil készülékeket, ezáltal:

1. A hálózat kapacitása növelhető: A keskeny nyalábnak köszönhetően csökken az azonos frekvenciát alkalmazó cellákból érkező interferencia. Ez lehetőséget teremt adott területen a frekvenciakihasználtság javítására, ezáltal növelve a kiszolgálható felhasználók számát. (Az elektronikusan vezérelt nyalábok lehetővé teszik továbbá a dinamikus cellakiosztást)
2. A kisugárzott rádiófrekvenciás energia csökkenthető: A sugárzási irány jelentős korlátozásának köszönhetően lényegesen kisebb teljesítményű energia elegendő egy adott távolságra lévő mobilkészülékkel való kommunikációhoz.
3. Az elektromágneses környezetszennyezés az előző pontban leírtak egyenes következményeként jelentősen csökken.

A fentiekén kívül további lehetőségeket rejlenek még az űrkutatás, műholdas személyi hírközlés és műholdas műsorszórás területén is, ezek alapján azonban elmondható, hogy az adaptív antennarendszerek felhasználásának igazán csak a képzelet szab határt.

Antennarendszerek [2, 4, 5]

A térben egymáshoz képest valamilyen rendszer szerint elhelyezett antenákat antennarendszernek nevezzük. Az elemek lehetőség szerint azonos tulaj-

donságokkal rendelkező egyszerű felépítésű antennák (pl. dipólusok). Az antennarendszer geometriája az 1. ábrán látható. Feltételezve, hogy a $Q(r)$ megfigyelési pont távolsága sokkal nagyobb az antennarendszer lineáris méreténél, a referencia pontban elhelyezett antennaelem térerőssége:

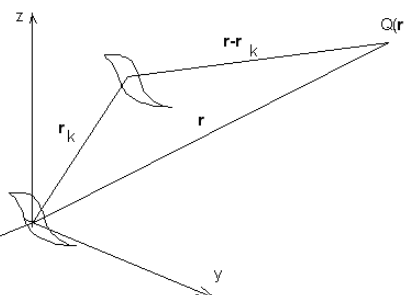
$$\mathbf{E}_0(\mathbf{r}) = U_0 \mathbf{F}(\vartheta, \varphi) \frac{e^{-j\beta r}}{r}$$

ahol:

$$U_0 = \sqrt{60 P_A G_A}$$

továbbá:

$$\mathbf{F}(\vartheta, \varphi) = F(\vartheta, \varphi) \cdot e^{j\Phi(\vartheta, \varphi)} \cdot \mathbf{p}(\vartheta, \varphi)$$



a komplex vektor iránykarakterisztika. **1. ábra:** Antennarendszer geometriája [2]

A k -adik pozícióban elhelyezett antenna térerőssége:

$$\mathbf{E}_k(\mathbf{r}) = U_0 \mathbf{F}(\vartheta, \varphi) \frac{e^{-j\beta |\mathbf{r} - \mathbf{r}_k|}}{|\mathbf{r} - \mathbf{r}_k|}$$

Ha a megfigyelési pont elegendően távol van, az $|\mathbf{r}|$ és $|\mathbf{r} - \mathbf{r}_k|$ párhuzamosnak tekinthető, azaz a fázis szempontjából alkalmazható az $|\mathbf{r} - \mathbf{r}_k| \cong |\mathbf{r}| - \mathbf{r}_k \cdot \mathbf{e}_r$ míg az amplitúdóra a $|\mathbf{r} - \mathbf{r}_k| \cong |\mathbf{r}|$ közelítés.

Ezek alapján az N elemű antennarendszer eredő térerőssége:

$$\mathbf{E}(\mathbf{r}) = U_0 \mathbf{F}(\vartheta, \varphi) \frac{e^{-j\beta r}}{r} \cdot \sum_{k=0}^{N-1} I_k \cdot e^{-j\beta \mathbf{r}_k \cdot \mathbf{e}_r}$$

$$F_i(\vartheta, \varphi) = \sum_{k=0}^{N-1} I_k \cdot e^{-j\beta \mathbf{r}_k \cdot \mathbf{e}_r}$$

az antennarendszer iránytényezője:

$$E_0(\mathbf{r}) = U_0 \mathbf{F}(\vartheta, \varphi) \frac{e^{-j\beta r}}{r}$$

egyetlen elem térerőssége:

A fő sugárzási irány $\mathbf{r}$ elektronikus beállítása illetve mozgatása az I_k táplálási áramok fázisával történhet. A fő sugárzási irányban az iránytényező maximális, tehát:

$$F_i(\vartheta, \varphi) = \sum_{k=0}^{N-1} |I_k| \cdot e^{j\delta_k} \cdot e^{-j\beta \mathbf{r}_k \cdot \mathbf{e}_r} \quad \text{maximális, ha} \quad \delta_k = -\beta \cdot \mathbf{r}_k \cdot \mathbf{e}_r$$

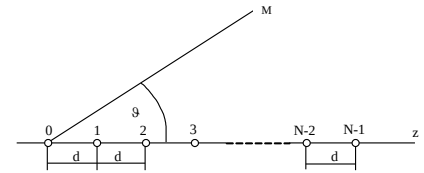
Az antennák táplálását tehát úgy kell megoldani, hogy az antennák közötti távolságkülönbségből adódó fáziskülönbséget a tápláló áram fázisa kompen-

zálja (haladóhullámú táplálás). Ekkor a fő sugárzási irányban ($\mathbf{e}_M$) az iránytényező:

$$F_i(\vartheta_M, \varphi_M) = \sum_{k=0}^{N-1} |I_k|$$

Tételezzünk fel egy lineáris antennarendszert (antennasor), melyben az elemek a z tengely mentén helyezkednek el egymástól d távolságra. A fő sugárzási irány z tengellyel bezárt szöge legyen ϑ (2. ábra). Ebben az esetben a k -adik antennaelem gerjesztő fázisa:

$$\delta_k = -\beta \cdot k \cdot d \cdot \cos \vartheta.$$



2. ábra: Antennasor modellje

két szomszédos antennaelem közti fáziskülönbség:

$$\delta_k - \delta_{k-1} = -\beta \cdot d \cdot \cos \vartheta$$

Ezt a táplálást progresszív fáziseloszlású táplálásnak nevezzük, mert a szomszédos elemek közti gerjesztés fáziskülönbsége állandó. A képletből látszik, hogy oldalsugárzó ($\vartheta_M = 90^\circ$) kialakításakor azonos fázisban, orrsugárzó ($\vartheta_M = 0^\circ$) esetén pedig ellenfázisban kell táplálni az antennaelemeket.

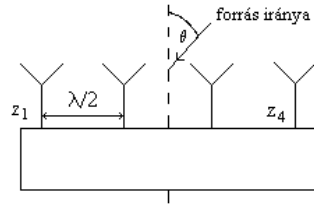
Mivel az antennaelemek tulajdonképpen nem mások, mint térbeli mintavételi pontok, ezért távolságukat (d) úgy kell megválasztani, hogy teljesüljön Shannon mintavételi tétele (időbeni és térbeni frekvencia analógia). Ha d nagyobb $\lambda/2$ -nél, átlapolódás jön létre a térbeli spektrumban azaz, több főirány keletkezik. Iránymérés és interferenciaszűrés esetén ez megghamisítaná a mérést, ezért az antennaelemek távolsága nem lehet nagyobb a hullámhossz felénél.

Íránymérés és interferenciaszűrés [1, 3]

Az íránymérés és interferenciaszűrés egymással szoros kapcsolatban álló műveletek. Interferencia szűrés csak a zavaró jelforrások (interferenciák) irányának ismeretében lehetséges és fordítva, hiteles írányméréshez gyakran van szükség a zavaró adók elnyomására

Az antennarendszerek elektronikusan változtatható iránykarakterisztikája, valamint a ma már gyors digitális jelfeldolgozás, illetve az ennek kapcsán alkalmazható adaptív algoritmusok jelentősen megkönnyítik a zavarforrások kiszűrésének mechanizmusát.

Tekintsünk példaként egy négyelemű antennarendszert, ahol az elemek távolsága a hullámhossz fele (3. ábra).



3. ábra: Négyelemű rendszer modellje

A fázisközéppont, az antennarendszer geometriai közepe, míg a mért irány, az ebbe a pontba állított merőlegeshez viszonyított szögeltérés. Az elmélet alapján, egy N-elemű sor iránytényezője felírható egy (N-1)-ed fokú polinommal, ami N-1 nullhelyet jelent. Ennek megfelelően a négyelemű antenna sor maximálisan három irány becslésére alkalmas. Feltételezzük továbbá: a vizsgált források elegendően távol vannak az antennáktól ahhoz, hogy a beeső hullámok az egyes elemekhez párhuzamosan érkeznek, így köztük csak az úthosszkülönbségből adódó fáziskülönbség lesz.

Az egyenlő távolságra elhelyezett antennaelemek mintavételezik az őket körülvevő elektromágneses teret (amplitúdó, fázis), ebből előáll a mintavett vektor, ami tartalmazza a fenn említett fáziskülönbséget. A számítások alapját az autókorrelációs mátrix képezi, amely a $\mathbf{z}^T = [z_1 \ z_2 \ z_3 \ z_4]$ mintavett vektorból a következő összefüggés alapján számítható:

$$\mathbf{R} = E\{\mathbf{z}\mathbf{z}^H\} = \lim_{k \rightarrow \infty} \frac{1}{k} \sum_{i=1}^k \mathbf{z}(t_i) \mathbf{z}(t_i)^H$$

ahol E a halmazátlagot jelenti.

Szimuláció esetén, amikor figyelembe kell venni olyan valós problémákat, mint például az additív zaj, különböző források közti fáziseltérés, vagy a

moduláció okozta fáziseltérés, azok hatása átlagolással kiejthető. Ez azt jelenti, hogy a mintavételezést egymás után többször elvégezzük, és a kapott vektorok átlagát vesszük. Az M minta alapján becsült autokorrelációs mátrix tehát a következő:

$$\hat{\mathbf{R}}_M = \frac{1}{M} \sum_{i=1}^M \mathbf{z}_i \mathbf{z}_i^H$$

Az iránymeghatározást ezen mátrix alapján különböző algoritmusokkal végzik, melyek pontosságban, dinamikatarományban, felbontásban, zavarállóságban térnek el egymástól.

A három legalapvetőbb módszer spektruma a következő:

$$S_{\text{BARTLETT}}(\omega) = E\{|\mathbf{s}^H \mathbf{z}|^2\} = \mathbf{s}^H(\theta) \mathbf{R} \mathbf{s}(\theta)$$

$$S_{\text{CAPON}}(\omega) = \frac{1}{\mathbf{s}^T(\omega) \mathbf{R}^{-1} \mathbf{s}^*(\omega)}$$

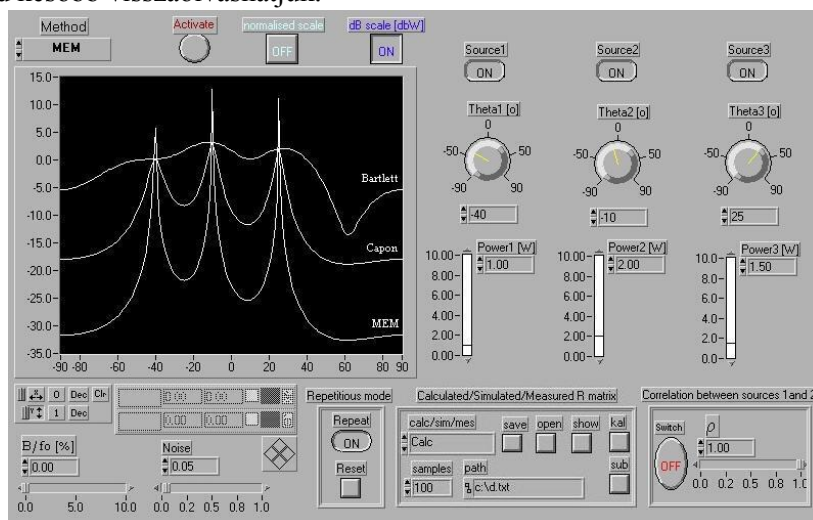
$$S_{\text{MEM}}(\omega) = \frac{1}{|\mathbf{s}^H(\omega) \mathbf{R}^{-1} \delta|^2}$$

Az első konvencionális módszer (Bartlett becslés vagy Fourier módszer), míg a második és harmadik adaptív algoritmus (Capon vagy MSINR, azaz maximális jel/zaj viszony módszer és MEM, azaz maximális entrópia módszer). Az adaptivitás leegyszerűsítve azt jelenti, hogy az antennarendszer karakterisztikája követi a vizsgált tér változásait, azaz a vizsgált irányba fordítja az iránykarakterisztika maximumát, míg a zavaró források irányára nullhelyet illeszt. Fizikailag az iránymérés a következőképpen történik: a fentiek alapján kialakított iránykarakteristikával végigpásztázza a félteret, és a mérési eredmények alapján becsli a vizsgált források irányát.

Szimuláció

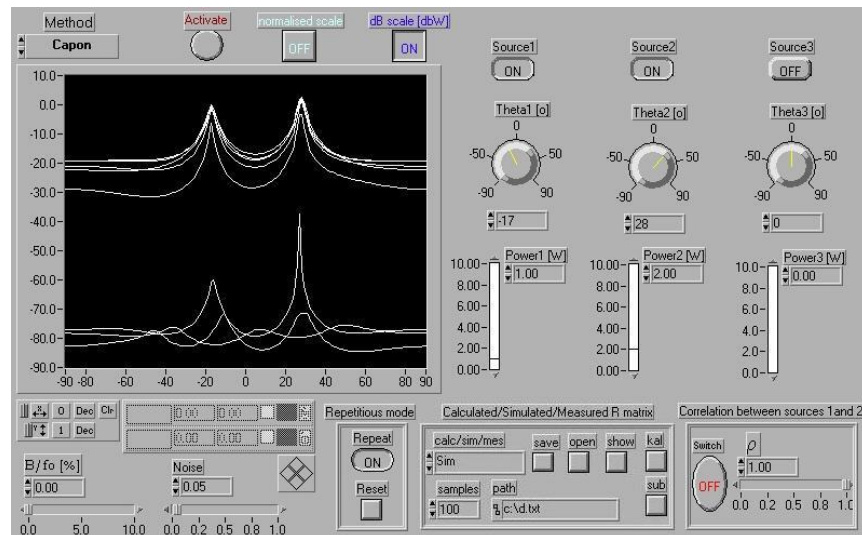
Most bemutatásra kerül egy szoftver, ami a bemutatott rendszerben alkalmas számítás, szimuláción alapuló iránybecsléshez szükséges számítások végzésére, az eredmények grafikus megjelenítésére. A kezelőfelület a 4. ábrán látható. A felhasználó megjelenítheti az eredményeket lineáris, logaritmikus vagy normalizált skálán, továbbá lehetőség van összehasonlítás céljából a görbék egymásra rajzolására, a pontosabb leolvasás elősegítése érdekében pedig markerek használatára. Négy antennából álló rendszer, legfeljebb három irány becslésére alkalmas, így ennyi áll rendelkezésünkre számítás és szimuláció esetén. Ezek iránya és teljesítménye egymástól függetlenül folyamatosan, lineáris skálán beállítható. Szimuláció esetén tetszőlegesen beállíthatjuk a minta-

számot, zajt adhatunk a jelekhez, beállíthatjuk a sávszélességüket, valamint az első és második forrást korrelálttá tehetjük. A kapott eredményeket tárolhatjuk, majd később visszaolvashatjuk.



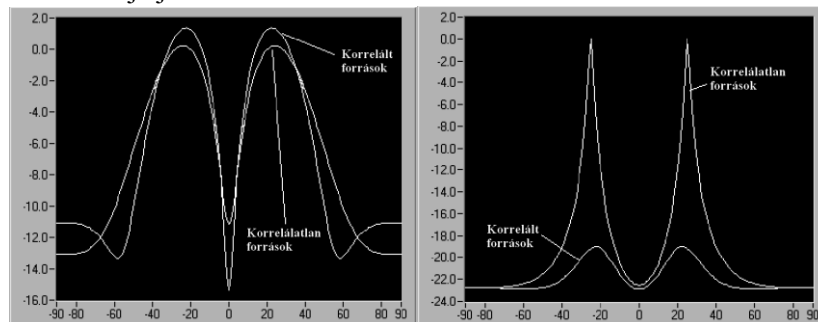
4. ábra: A program kezelőfelülete

A 4. ábrán ezek alapján a következő beállítások láthatók számítási üzemmód esetén a források tulajdonságai sorrendben a következők: -40° , 1W; -10° , 2W ; 25° , 1.5W. A kijelzőn megfigyelhető a különböző algoritmusok két leg-
alapvetőbb tulajdonsága, a dinamika és felbontás. Steril körülmények között tehát az adaptív modellek messze fölülmúlják mindkét paraméter tekintetében a konvencionális módszert. Csekély zavarálló képességük miatt azonban valós körülmények között kevésbé meggyőző eredményt adnak. Az 5. ábra a mintaszám növelésének hatását mutatja be Capon módszer szimulációja esetén (lentől fölfelé a mintaszám nő). Megállapítható, hogy a megbízható méréshez 100 minta már elegendő. (A mintaszám az átlagolt mérések számát jelenti.)



5. ábra: Capon módszer hatékonysága a minták számának függvényében

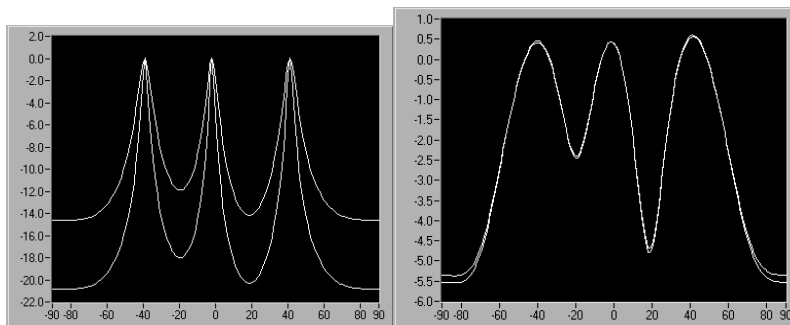
A korrelált források hatása az alábbi ábrákon figyelhető meg (Bartlett - balra, Capon - jobbra). Megállapítható, hogy míg a Bartlett becslés esetében a korreláció alig befolyásolja a mérést, addig az adaptív algoritmusok pontossága és dinamikája jelentősen romlik.



6. ábra: Bartlett

7. Ábra: Capon

A 8. és 9. ábrán a sávszélesség hatása vizsgálható ($B/f_0 = 0\%$ és $B/f_0 = 10\%$). Ez alapján szintén az adaptív algoritmusok gyengesége látszik: a Bartlett becsléssel kapott eredmény gyakorlatilag érzéketlen a spektrum kiszélesedésére, a Capon módszer esetén viszont jelentősen csökken a dinamika (6dB).



8. ábra: Bartlett

9. ábra: Capon

Összességében látható, hogy az adaptív algoritmusok ideális esetben messze fölülmúlják a Bartlett becslést, a valós körülmények azonban, mint a zaj, moduláció, reflexiókból adódó korreláció jelentősen rontják azok hatékonyságát.

Természetesen végtelen azoknak a beállításoknak a száma melyek a főnti módon a programmal vizsgálhatók, ezáltal alkalmas különböző vizsgálatok elvégzésére, új algoritmusok kifejlesztésére és tesztelésére.

A bemutatott programot Folkmann Viktor mérnök úrral valósítottuk meg, továbbfejlesztése folyamatosan zajlik a Budapesti Műszaki és Gazdaságtudományi Egyetemen.

Irodalomjegyzék:

1. *Alfonso Farina*: Antenna-Based Signal Processing Techniques for Systems Artech House, Norwood, 1992.
2. *Szekeres Béla, Nagy Lajos, Petre Péter*: Antennák és hullámterjedés jegyzet (BME)
3. *Varga Zoltán*: Rádió iránymérés (Diplomaterv) Budapesti Műszaki Egyetem 1999.
4. *Simonyi Károly, Zombori László*: Elméleti villamosságtan Műszaki Könyvkiadó 2000.
5. *Istvánffy Edvin*: Tápvonalak, antennák és hullámterjedés Műegyetemi kiadó 1997.

A KORMÁNYZATI TÁVKÖZLÉS HELYZETE 1967-1989 KÖZÖTT

1.2. Kezdeti időszak

A kormányzati távközlés egységesítése és annak más kommunikációs rendszerekre gyakorolt hatásai vizsgálatának szándéka három dolgot feltételez:

- hazánkban nem szerveződött kormányzati kommunikációs rendszer;
- a meglevő rendszer átalakításra, illetve továbbfejlesztésre szorul;
- a kormányzati szervek igényeit a rendészeti-, katonai- és közigazgatási kommunikációs rendszerek szolgálják ki, de az igények kielégítésének szervezetek közötti koordinációja nem megfelelő.

Ahhoz, hogy a fenti felvetésekre sikerüljön kielégítő válaszokat kapni, meg kell határozni – *amennyiben lehetséges* – a kormányzati kommunikációt kiszolgáló rendszer megszervezése időpontját és kialakulásának körülményeit, meg kell vizsgálni fejlődésének folyamatait és a környezetére²⁷ gyakorolt hatásokat.

A kutatásokat a II. világháborút közvetlenül követő időszaknál kellett megkezdeni, amikor is Budapesten helyreállították az erős háborús pusztítások miatt megsérült távbeszélő infrastruktúra jelentősebb elemeit [11]. A működőképes hálózatra alapozva a '40-es évek végére került kialakításra a „K” távbeszélő hálózat⁷⁴, mely a kormányzati felsővezetők közötti kommunikációt tette lehetővé. [12]. E ténymegállapítástól függetlenül azonban a kormányzat igényeit kiszolgáló rendszer megszervezését először, dokumentált formában a Magyar Forradalmi Munkás-Paraszt Kormány⁷⁵ 1967. október 19-én kelt, **3343/1967.** számú határozata írja elő.

²⁷ elsősorban más kommunikációs rendszerek

⁷⁴ a „K” jelentése: közigazgatási. Mai szakmai fogalmainkkal élve zárt felhasználói csoportot kiszolgáló hálózat. A zárt felhasználói csoport tagjai tartós szakmai vagy gazdasági-üzleti kapcsolatban állnak egymással, illetve közös üzleti tevékenységet végeznek, és akiknek egymás közötti kommunikációs szükséglete ezen kapcsolaton alapuló közös érdekből ered

⁷⁵ Magyarország kormányának hivatalos megnevezése 1956-1989 között

A rendszer és környezete kezdeti szakasza fejlődésének vizsgálatát és elemzését tehát 1967-től kezdem. A vizsgált szakasz 1989-ben zárul, mely során célszerű áttekinteni a következő témaköröket is:

- az igénybe vehető kommunikációs szolgáltatások;
- szolgáltatási követelmények;
- a szolgáltatás nyújtásában közreműködők és az igénybevevők köre.

1.2.1. A nem kormányzati szektor

A bipoláris világrend⁷⁶ időszakában hazánk a jelenlegitől eltérő politikai és gazdasági berendezkedésű állam volt. A Varsói Szerződés⁷⁷ és a KGST⁷⁸ tagállamként a szocialista országokhoz hasonló belső államhatalmi struktúrával és tervgazdasággal rendelkezett, ami jelentősen befolyásolta a távközlési szektor helyzetét⁷⁹ is. A kormányzati távközléssel kapcsolatos kép megismeréséhez így szükségszerű röviden áttekinteni az állami irányítás és felügyelet alá tartozó, de nem a kormányzatot kiszolgáló rendszerek⁸⁰ viszonyait is.

Az 1960-as években a kommunikáció technológiai alapjait döntően az **analóg** távközlési rendszerek képviselték, melyek közül csak néhány elem került digitalizálásra⁸¹ a '80-as évekre, ezért a kommunikációs szolgáltatások **típusai** nem bővültek jelentősen. Összességében már a II. világháború előtt is alkalmazott fő fajtákról van szó, vagyis az élőbeszéd továbbítására alkalmas **távbeszélő**⁸², valamint az írott szöveg átvitelét biztosító **géptávíró**⁸³ szolgálta-

⁷⁶ 1945-1990 közötti történelmi időszak

⁷⁷ Varsói Szerződés (VSz): 1955-1990 között funkcionáló politikai és katonai szövetségi rendszer, melynek elsődleges célja volt a NATO-val szembeni – elsősorban katonai jellegű – súlypontképzés

⁷⁸ Kölcsönös Gazdasági Segítség Tanácsa, mely a szocialista országok gazdasági tevékenységének összehangolása érdekében jött létre. 1949-1990 között funkcionált

⁷⁹ ebben az időszakban a távközlési szektor teljes vertikumára jellemző volt, hogy a stratégiai döntésektől kezdődően a gyakorlati megvalósításig állami irányítás alatt állt

⁸⁰ elsősorban itt a lakossági és gazdasági szereplőket kiszolgáló rendszerekről, a civil szféráról beszélhetünk

⁸¹ lényegében a PCM átviteltechnikai rendszerekről és a tárolt programvezérlésű (TPV) kapcsolástechnika megjelenéséről beszélhetünk

⁸² a Német Szövetségi Köztársaságban 1952-ben kezdenek hozzá a Siemens cég által technikailag már 1923 óta előkészített országos automata telefonhívás bevezetéséhez. A minden országrészt átfogó távhívó hálózat csak két évtizeddel később került átadásra

tásokról. A fő szolgáltatások mellett a számítástechnika térhódításával párhuzamosan a '70-es évek közepétől igény jelentkezett **adatátviteli**⁸⁴ kapcsolatok kialakítására, mikortól is világszerte megkezdődött a távközlés és számítástechnika határainak összemosódása. Ezzel egyidejűleg, a nyolcvanas évek közepétől jelenik meg a géptáviró vetélytársa a **telefax**⁸⁵ készülék.

Természetesen, a szolgáltatásfajták csekély mértékűnek nevezhető bővülése nem jelenti azt, hogy egy közel fél évszázados intervallumban nem történt semmilyen érdemi technikai fejlesztés. Ki kell hangsúlyozni, hogy jelentős lépések történtek a távbeszélő és géptáviró szolgáltatások automatizálására, vagyis a manuális kapcsolás kiküszöbölésére, az igénybe vehető távközlési kapacitások bővítésére, valamint – *mai fogalmainkkal élve* – a minőségbiztosítás⁸⁶ fokozására. Hazánk távközlési infrastruktúrájában – *melynek legnagyobb szereplője a Magyar Posta*⁸⁷ volt – a '60-as évek végéig a 7A2 mechanikus, rotary rendszerű automata távbeszélő központok⁸⁸ voltak a jellemzők, melyeket az ARM 202/2 és ARF 102 crossbar⁸⁹ távhívó központok, valamint az ARK 511 crossbar végközpontok váltottak fel. 1980-ban a Magyar Posta távközlő rendszerében 2.543 db főközpont (238 db gépi, 209 db CB és 2.096 db LB⁹⁰), 617.243 db távbeszélő fővonalat⁹¹ (282.542 db különvonalú és 334.701

⁸³ a géptáviró, távgépíró és telex elnevezések fogalmilag egyformának tekinthetők. Az Egyesült Államokat követve, Európában először Németország épít ki és helyez üzembe országos telexhálózatot (1933)

⁸⁴ a németországi IBM 1961-ben mutatta be *Tele-Processing* eljárását, amivel a telefonon közvetített adatok számítógéppel való tovább feldolgozása lehetővé válhatott. Ezzel a lehetőséggel az elektronikus adatfeldolgozás új határt lépett át

⁸⁵ az első síkgyazású távmásoló készüléket (telefaxot) 1971-ben a Rank Xerox vitte piacra

⁸⁶ minőségbiztosítás: mindazok a tervezett és rendszeres intézkedések, amelyek szükségesek ahhoz, hogy a termék vagy szolgáltatás a megadott minőségi követelményeket kielégítse

⁸⁷ a Magyar Posta elődje távközlési szolgáltatásokkal a XIX. század végén kezdett el foglalkozni. Baross Gábor a posta és a távírda egyesítésével (1887), valamint a távközlési szolgáltatások államosításával (1888) a magyar távközlést Európa élmezőnyébe helyezte

⁸⁸ Rotary rendszerű központ: automata elektromechanikus központ, melyben a kapcsolást a hívott kapcsolási száma alapján forgógépek végezték

⁸⁹ crossbar központ: automata, elektromechanikus központ, melyben a kapcsolást keresztrudas kapcsológépek végezték

⁹⁰ LB / CB: Local Battery – helyi telepes / Central Battery – központi telepes

⁹¹ távbeszélő fővonal: előfizetői hozzáférési pontot a közcélú távbeszélő hálózat előfizetői központjával összekapcsoló áramkör, amely a központban egyéni kapcsolási számmal rendelkezik

db ikervonalú⁹²⁾ szolgált ki, melyből 404.303 db működött lakáson, 197.169 db volt közületi és 15.771 db nyilvános helyen üzemelt. Ebben az évben az ország területén 40 db géptávíróközpont funkcionált 11.200 db állomáskapacitással, összesen 8.132 db előfizetői géptávíró állomással. Az adatátviteli állomások száma 738 db volt [13].

A géptávíró rendszer fejlesztése 1953-1963 között zajlott le, melynek eredményeképp az teljesen automatizálttá vált. Az első nemzetközi géptávíró központ 1961-ben került átadásra [14]. 1989-ig az országos távközlőhálózat kapcsolástechnikai elemeinek teljes automatizálását nem sikerült megoldani, így az említett távbeszélőközpontok mellett az LB és CB manuális központok is használatban maradtak egészen 1999-ig [15].

Törekvések történtek a belföldi és nemzetközi viszonylatok bővítésére is, azonban a világ politikai és gazdasági rendszerében országunk által elfoglalt hely nem tette lehetővé a technológiai fejlettség tekintetében magasabb színvonalon álló technikai rendszerek és eszközök beszerzését, illetve gyártási eljárások megismerését⁹³⁾. A fennálló viszonyok hatására (a kormányzati szektort is beleértve) a távbeszélő ellátást tekintve 1990-re 9,62 db távbeszélő főállomás jutott 100 lakosra vetítve. Ez azt jelenti, hogy a nyolcvanas évek végére hazánk átlagos távbeszélő ellátottság tekintetében alulmaradt a nyugat-európai országokhoz képest, mivel az ilyen típusú mérőszám a fejlett régióban 32-es értéket mutatott [16]. A következő táblázat az egyik fő szolgáltatásfajta 1980-1990 közötti kvantitatív fejlődését ábrázolja, aminek alapján megállapítható, hogy egy évtized alatt a távbeszélő ellátottság, mint a társadalmi fejlettség egyik fokmérője több mint 60%-kal nőtt [17].

év	1980.	1985.	1988.	1990.
db távbeszélő fővonal/100 lakos	5,8	6,94	8,1	9,62

1.1. számú táblázat: a távbeszélő fővonalak sűrűsége Magyarországon
(forrás: Magyar Válasz az Információs Társadalom kihívásaira)

⁹²⁾ kapacitáshiány miatt a fővonalakat különvonalakra és ikervonalakra osztották fel. Az ikervonal két előfizetői hozzáférési pontot szolgált ki úgy, hogy azok virtuális különvonalként működtek, de egyidejű hívás kezdeményezésére, illetve fogadására nem volt lehetőség

⁹³⁾ 1950-ben alakult meg a NATO tagországok és Japán részvételével működő COCOM-bizottság (Coordinating Committee for Multilateral Export Controls – Többoldalú Exportellenőrzést Koordináló Bizottság), melynek célja volt, hogy ellenőrzésével megakadályozza egyes termékek (főként katonai felszerelések és fejlett technikájú műszaki berendezések) exportját a szocialista államokba

A távbeszélő rendszerek fejlődése mellett 1989-ig folyamatosan bővült a géptávíró, illetve az adatátviteli szolgáltatások igénybevételének lehetősége is. 1989-ben 38 db géptávíró és adatkapcsoló központ működött 18.270 db állomáskapacitással. A 13.480 db géptávíró állomás mellett 7.551 db adatállomás működött, melyből távbeszélő hálózaton 5.343 db, vonalkapcsolt hálózaton 463 db, közvetlen összeköttetésen 1.745 db üzemelt [18].

1990-ig a teljes hazai távközlési szektor állami monopóliumban volt, melyet igazol a postáról és távközlésről szóló 1964. évi II. törvény⁹⁴ is, mely lezögezi, hogy a postai és távközlési kérdések teljes vertikuma állami tevékenységi körbe tartozik [19]. A hírközlési szolgáltatásokat,⁹⁵ valamint a frekvenciagazdálkodást kizárólagossággal a Magyar Posta, az egyik legnagyobb állami vállalat biztosította.⁹⁶

A vizsgált időszakra vonatkoztatva elmondható, hogy a lebonyolított technikai fejlesztések révén a lakossági és gazdasági szereplők távközlési lehetőségei folyamatosan bővültek, azonban a kilencvenes évekig az ország életének részét képezték a várakozói listákkal jellemzett, kielégítetlen mennyiségi igények.

1.2.2. A kormányzati szektor

A kormányzati szektor áttekintése előtt célszerű visszakanyarodni a kormányzati távközléssel összefüggésben az 1.1. alfejezetben tett megállapításhoz, miszerint a kormányzati távközlés hatóköre az Országgyűlésre, a Kormányra, a központi államigazgatási szervekre (Miniszterelnöki Hivatal, minisztériumok, országos főhatóságok), valamint az államigazgatás területi- és helyi szerveire terjed ki. E konkrét meghatározás mellett azonban tisztázni kell, hogy az 1967-1989 közötti időszakban a kormányzati távközlés megvalósulásában mely szervek működtek közre, milyen paraméterekkel rendelkező saját⁹⁷ kommunikációs rendszerrel rendelkeztek, illetőleg milyen igényeket szolgálták ki az állami szektorban.

⁹⁴ e jogszabály teljes hatálytalánítása csak 1993-ban, a frekvenciagazdálkodásról szóló 1993. évi LXII. törvény 27. § (1) bekezdése alapján történt meg

⁹⁵ távközlési- és postai szolgáltatások, valamint a rádió- és televízió műsorszórás

⁹⁶ a Magyar Posta szervezete 1990. január 1-jén módosult. A korábbi fő feladatokat a Magyar Posta Vállalat, a Magyar Távközlési Vállalat, valamint a Magyar Műsorszóró Vállalat vette át

⁹⁷ mai foglmaink szerint ezeket az 50/1998. (III. 27.) Korm. rendelet alapján zárt-célú távközlő hálózatként foghatjuk fel

Az időszak sajátja volt az államrendszer egyközpontúsága [20]. A centralizált államvezetésben a honvédelmi és belügyi ágazat kiemelt szerepet töltött be, az előbbi a VSz katonai kötelezettségeiből adódóan, míg az utóbbi a belső rend, az állam biztonságának garantálása okán volt annak tekinthető [21]. Ez a modell a politikai-katonai szövetségi rendszert vezető ország⁹⁸ belső hatalmi struktúráját képezte le a hazai viszonyoknak megfelelően. A szektor domináns képviselőiként a mindenkor kormányzat⁹⁹, a fegyveres erők¹⁰⁰, valamint a fegyveres testületek¹⁰¹ számítottak, így a kormányzati távközlés egyrészt az e szervezetek által fenntartott és működtetett kommunikációs rendszerek útján, valamint az egyetlen távközlő szervezet, a Magyar Posta rendszerén keresztül valósult meg.

A kormányzat, a honvédelmi és a belügyi ágazat távközlési szolgáltatások igénybevételével, azok fejlesztésével kapcsolatos lehetőségeit jellemzően a következő főbb tényezők befolyásolták:

- az ország távközlési alpinfrastruktúrájának helyzete, fejlettségi szintje, vagyis a Magyar Posta hálózatainak minősége;
- a szövetségi feladatokból származó együttműködési kötelezettségek;
- az államvezetés és az ágazati szervek jogszabályokban meghatározott feladatai;
- a tervutasításos gazdasági rendszer.

A kormányzati szektor rendszerei a vizsgált időszakban fenti tényezők alapján fejlődtek, mely fejlődési szakaszok főbb jellemzőinek – *ágazatonkénti* – rövid áttekintésére kerül sor a következőkben.

⁹⁸ Szovjetunió

⁹⁹ itt meg kell említeni, hogy a kormányzat, mint szervezet, valamint a vezető politikai párt integrált egységben tevékenykedett. A kormányzat tagjai sok esetben a vezetői politikai párt tagjai voltak. E kapcsolatot azonban a továbbiakban nem veszem figyelembe, így az államigazgatás legfelsőbb vezetőjeként a Kormányt tekintem

¹⁰⁰ fegyveres erők: az Alkotmányról szóló 1949. évi XX. törvény 40/A § (1) bekezdése alapján a Magyar Honvédség és a Határőrség. A tárgyalt időszakban e két szerv megnevezése: Magyar Néphadsereg és BM Határőrség

¹⁰¹ a vizsgált időszak szempontjából fegyveres testületnek az állambiztonság, rendőrség, tűzoltóság, vám- és pénzügyőrség, büntetés-végrehajtás, valamint a munkásőrség számít. E szervek közül azonban jelentős kommunikációs rendszerrel csak a Belügyminisztérium alárendeltségébe tartozók rendelkeztek, mely rendszerek képezték az ágazati infrastruktúrát

1.2.2.1. A honvédelmi ágazat

A honvédelmi tárca a '70-es évek közepén döntött a Magyar Néphadsereg önálló, állandó jellegű hírhálózatának kiépítéséről, mivel nyilvánvalóvá vált, hogy a Magyar Posta által üzemeltetett országos távközlő hálózat nem képes kiszolgálni a katonai vezetés országos és nemzetközi, békeidejű és háborús vezetési igényeit. A korszerűsítési folyamat során mind a tábori hírendszer, mind a stacioner (állandó) hírendszer elemei a kor technikai színvonalán, a szövetségi keretek lehetőségein belül modernizálásra kerültek [22]. A fejlesztési koncepciók kidolgozása, majd a végrehajtás centralizáltan, a vezérkar Híradó Főnöksége útján került megszervezésre.

Az állandó hírendszer kiépítésével lényegében véve 1976-1989 között megvalósult a fővárosban és – *a területi hírközpontok kiépítésével* – a vidéken diszlokált katonai szervezetek folyamatos távhívó-távbeszélő, valamint géptávíró szolgáltatással való ellátása. Az önálló, analóg rendszer hozzávetőleg 100 db különböző típusú, automata távbeszélő kapcsolóelemből,¹⁰² valamint 20 db géptávíró központból állt, összesen mintegy 30 ezer db távbeszélő mellékállomást, 65 ezer db alközponton végződött távbeszélő mellékállomást, valamint 500 db géptávíró állomást foglalva magába. Ezen időszakban épült ki a mikrohullámú hálózat alapja is 1.200 távbeszélő és 600 géptávíró csatorna kapacitással [23].

A fejlesztési ciklus végeztével az ágazat országos kiterjedésű, egyenszilárd-ságú állandó hírendszerrel rendelkezett, mely a területi hírközpontok, a vezetési pontok hírközpontjai és a különböző vezetékes és vezeték nélküli összeköttetések útján biztosította a békeidejű vezetés távközlési feltételeit. Együttműködve a Magyar Postával és a társ fegyveres testületekkel ez a hírendszer képezte a minősített időszak¹⁰³ (háborús) híradás alapját is.

A Magyar Néphadsereg állandó hírendszere a Magyar Postához hasonló arányban tartalmazott analóg és digitális rendszertechnikai elemeket tekintettel arra, hogy mind a tervek elkészítésében,¹⁰⁴ mind – *az akkor beszerezhető eszközök és berendezések felhasználásával* – a kivitelezési, telepítési és beüzemelési eljárásokban a Posta szakemberei részt vettek. Képességeit tekintve a

¹⁰² többek között: ARF-102/A, ARK, 511, ARK-511/A, ARK-522, ARM-503, EPF-128, EPF-512, EPK-128/Z

¹⁰³ az Alkotmányban meghatározott, az ország normális működésétől eltérő időszakok összefoglaló elnevezése

¹⁰⁴ az „MN Távhívó Hálózat Rendszertechnikai Terve” 1980-ban került összeállításra és jóváhagyásra. A tervet a Posta Tervező Iroda készítette

rendszer elsősorban a vezetéknélküli (rádiós)¹⁰⁵ és információvédelmi rendszerek által nyújtott szolgáltatásokban különbözött a civil szektor által használt hálózatoktól. A rendszer a kapcsolóközpontok szintjén összekapcsolható volt mind a Magyar Posta, mind a társ fegyveres testületek hálózatával, de jellemző volt egy-egy távbeszélő szolgáltatás-hozzáférési pont¹⁰⁶ államigazgatási szervekhez történő kihelyezése is.

A kormányzati távközlés szempontjából az állandó hírrendszer megléte elsődleges fontosságú volt, tekintettel arra, hogy minősített időszakokban az állami és katonai felsővezetés közötti kommunikáció döntően e hálózat útján valósulhatott meg. A rendszer elemei természetesen megtalálhatók voltak a „K” vezetési rendszer¹⁰⁷ védett objektumaiban, azonban a hálózati topológia a katonai egységek diszlokációjához igazodott, mely a főváros és néhány megyeszékhely¹⁰⁸ kivételével nem egyezett a közigazgatási egységek működési területével.

Összességében véve a honvédelmi ágazat katonai kommunikációs rendszere az ország, illetve a honvédség gazdasági lehetőségeinek függvényében, illetve a szövetségi elvárásoknak megfelelően került fejlesztésre. A nem kormányzati szektorhoz viszonyítottan szolgáltatási színvonala magasabb volt, hiszen a fejlesztések eredményeképp új minőség jött létre.

1.2.2.2. A Kormány és a belügyi ágazat

A kormányzati távközlés és a belügyi ágazat kommunikációs rendszerének logikai összekapcsolása nem tűnhet indokoltnak, azonban a vizsgált időszakban a belső rend biztosításával, valamint az állambiztonsággal¹⁰⁹ kapcsolatos feladatokat a kormányzati munkamegosztás értelmében a Belügyminisztérium látta el. A hazai biztonsági szervek egy szervezetben való egységes

¹⁰⁵ e körbe sorolható az MRKB rádiótelefon rendszer, az állandó telepítésű troposzféra hírközpontok, a riasztást biztosító Orfeusz, illetve a vezérkar híradását biztosító állandó telepítésű rádióközpontok, a digitális mikrohullámú rendszerek (RP)

¹⁰⁶ szolgáltatás-hozzáférés: egy távközlő végberendezés fizikai és logikai csatlakoztatása valamely távközlési hálózathoz vagy annak részéhez azért, hogy a hálózati funkciók és a hálózaton nyújtott szolgáltatások igénybevehetővé váljanak

¹⁰⁷ a „K” vezetési rendszer biztosítja az állam minősített időszakai vezetésének alapvető feltételeit

¹⁰⁸ ez alól csak a megyei hadkiegészítő parancsnokságok képeznek kivételt

¹⁰⁹ az állambiztonsággal kapcsolatos teendőket ma a belügyi ágazatról leválasztott polgári és katonai nemzetbiztonsági szolgálatok látják el

irányítása és vezetése a baloldali blokk¹¹⁰ országaiban általánosan alkalmazott szervezési koncepcióhoz hasonlóan történt, ami egyúttal feltételezte az államhatalmi ágazaton belüli kiemelt szerepkört is [24].

A Belügyminisztérium¹¹¹ szerteágazó, az államigazgatást teljes vertikumban kontrolláló szerepére építve a Magyar Forradalmi Munkás-Paraszt Kormány 3343/1967. számú határozata alapján a kormányzati felsővezetés utasította a belügyi ágazatot, hogy építse ki, és üzemeltetésre vegye át a békeidejű nemzetközi párt- és kormány szintű titkosított¹¹² távbeszélő összeköttetési rendszert¹¹³. A feladat 1969-ben került teljesítésre [25].

A feladatrendszer átvételének közvetlen előzménye a VSz tagállamok miniszterelnökeinek és a pártok¹¹⁴ Központi Bizottságai első titkárainak Budapesten lefolytatott értekezlete volt, melyen határozat született a nemzetközi kormány-összeköttetések kialakításáról. A határozatok gyakorlati végrehajtása érdekében az érintett országok állambiztonsági képviselői 1967. augusztus 15-17. között Moszkvában meghatározták a résztvevő országok¹¹⁵ közötti titkosított távbeszélő hírszervezési technikai, forgalmi, üzemeltetési és együttműködési feladatait [26].

¹¹⁰ a baloldali blokk elnevezés a szocialista társadalmi berendezkedésű országok gyűjtőneve volt

¹¹¹ mai fogalmainkkal élve a Belügyminisztérium inkább rendészeti (és biztonsági) minisztériumként funkcionált, ugyanis a közigazgatás szervezése és irányítása 1989-ig a Minisztertanács közvetlen alárendeltségébe tartozó Tanács Hivatal tevékenységének köréhez tartozott

¹¹² az államtitokról és szolgálati titokról szóló 1995. évi LXV. törvény 4. § (1) bek. szerint a szolgálati titok az az adat, amelynek az érvényességi idő lejártá előtti nyilvánosságra hozatala, jogosulatlan megszerzése és felhasználása, illetéktelen személy részére hozzáférhetővé tétele, továbbá az arra jogosult részére hozzáférhetlenné tétele sérti vagy veszélyezteti az állami vagy közfeladatot ellátó szerv működésének rendjét, akadályozza a feladat- és hatáskörének illetéktelen befolyástól mentes gyakorlását, és ezáltal közvetve a Magyar Köztársaság törvényben meghatározott érdekeit hátrányosan érinti. A rendszer a mai fogalmaink szerint is csak a szolgálati titok kategóriájába sorolt információk védelmére volt tervezve. Ehhez azonban mindenképpen hozzá kell tenni, hogy aktív információvédelem csak a kapcsolóeszközök között volt, vagyis a központ-végberendezés viszonylatban csak az átviteli közeg (kábel) mechanikus védelme jelentette a biztonságot

¹¹³ a rendszer „VCS” néven, az alkalmazott orosz „Высокая Частота” (magas frekvencia) technológiára utaló elnevezésen vált ismertté

¹¹⁴ a pártokon itt az adott európai szocialista ország vezető pártját kell érteni (pl.: Szovjetunió Kommunista Pártja, Magyar Szocialista Munkáspárt, stb.)

¹¹⁵ Bulgária, Csehszlovákia, Lengyelország, Magyarország, Német Demokratikus Köztársaság, Románia és Szovjetunió

A békeidejű üzemeltetési feladatok gyakorlati átvételét követően a Honvédelmi Bizottság¹¹⁶ a 2/212/1970. számú határozatában előírta, hogy a minősített időszakok idejére a hírhálózat bővítésével az akkori K-I. vezetési ponton a békeidőszak titkosított távbeszélő szolgáltatásaival azonos szintű ellátást kell biztosítani.

A nemzetközi kormány-összeköttetési rendszer¹¹⁷ távközlési szolgáltatásainak további bővítését a Kormány 3023/1971. számú határozata rendelte el, ami alapján – *ugyancsak titkosított* – géptávíró kapcsolatok jöttek létre a már együttműködő országok meghatározott vezetői írásos kommunikációjának biztosítására.

Az összeköttetések¹¹⁸ biztosításáért és fenntartásáért a Közlekedés és Postaügyi Minisztérium¹¹⁹, míg a kapcsolástechnikai és végberendezési elemek közvetlen üzemviteléért, a forgalmi feladatok ellátásáért a BM III/V. Csoportfőnökség¹²⁰ felelt. Ez a szervezési megoldás az egykori Szovjetunióban is alkalmazott volt, mivel a szovjet kormányzati kommunikációs rendszert üzemeltető szolgálat a KGB¹²¹ szervezetében került elhelyezésre [27].

A kormány-összeköttetési rendszer szolgáltatásait 1980-ban csak alig valamivel több, mint száz – *többnyire a fővárosban üzemelő* – szolgáltatás-hozzáférési pontról lehetett igénybevenni, mellyel kapcsolatosan a BM III/V. Csoportfőnökség jelentése megjegyzi, hogy a párt- és kormány felsővezetői

¹¹⁶ Honvédelmi Bizottság: 1990-ig a Minisztertanács (MT) a honvédelemmel kapcsolatos egyes feladatait – az általa megállapított körben – az MT Honvédelmi Bizottsága útján látta el. A kormánybizottság határozatait a miniszterek, az országos hatáskörű szervek vezetői és egyéb szervek kötelesek voltak végrehajtani

¹¹⁷ a továbbiakban kormány-összeköttetési rendszer, a Belügyminisztérium terminológiája szerint kormányhíradás

¹¹⁸ itt mind a géptávíró, mind a távbeszélő szolgáltatások igénybevételére alkalmas átviteltechnikai infrastruktúrát kell érteni hazai, illetve nemzetközi viszonylatban egyaránt. A fővárost tekintve a helyzet felemás volt, mivel a központokat a végberendezéssel összekötő fizikai kábelek biztonsági és üzembiztonsági felügyeletét az állambiztonsági szolgálat látta el

¹¹⁹ ami a gyakorlatban azt jelentette, hogy az üzemviteli feladatokat a Magyar Posta látta el

¹²⁰ BM III/V. Csoportfőnökség: az állambiztonsági szolgálaton (III. Főcsoportfőnökség) belül azon szervezeti egység volt, mely az állambiztonsági munkához szükséges technikai feltételeket (többek között kormányhíradás) biztosította

¹²¹ KGB (КГБ): Комитет Государственной Безопасности – az egykori Szovjetunió Állambiztonsági Bizottsága

titkosított távbeszélő rendszer a baráti szocialista országokhoz képest szűk kiépítettségű [28].

A Honvédelmi Bizottság – *a belügyi tárca javaslata alapján* – a VI. ötéves terv¹²² összeállításánál, három ciklusra (VI-VIII. ötéves tervidőszakra) lebontva előirányozta a rendszer jelentős bővítését. Az 1994-re kialakításra tervezett hálózat több meglevő kommunikációs rendszer integrálásával jött volna létre, azonban kiépítésére nem került sor. A kormány-összeköttetési rendszer egy olyan integrált kommunikációs rendszer képét vetítette fel, mely béke- és minősített időszakokban egyaránt képes kiszolgálni a párt- és kormány felsővezetőinek, az államigazgatás központi szervei vezetőinek, valamint a területi szervek vezetői jelentős részének kommunikációs igényeit.

Az integrálásra tervezett elemek kiválasztása koncepciójának értelmezéséhez azonban tudni kell, hogy a Belügyminisztérium a kormányhíradás témakörét 1967-1989 között állambiztonsági kérdésként kezelte. A BM III. Főcsoportfőnökség szakmai állásfoglalása a „kormányhíradó” rendszerrel kapcsolatos legfőbb követelményről nem volt más, mint, hogy a rendszer minden eleme rendelkezzen valamilyen típusú információvédelmi képességgel. Ennek hiányában az adott elem nem képezhette a rendszer részét.

E követelmény ismeretében érdemes áttekinteni az integrálásra tervezett alrendszerek távközlési struktúra területén 1980-ban elfoglalt helyét és állapotát, mivel azok üzemeltetése és fenntartása nem volt egy kézben. A helyzet megállapítása a tárgyidőszakban alkalmazott dokumentálási rendszer miatt¹²³ nem jelent könnyű feladatot, azonban a fennmaradt információk alapján a rendszer-elemek a következők szerint csoportosíthatók:

- „MK” (minisztériumi közigazgatási) távbeszélő hálózat¹²⁴;
- kormányzati védett „PB” távbeszélő hálózat¹²⁵;
- „ALTÁJ” országos mobil rádiótelefon hálózat;
- kormányzati titkosított „VCS” távbeszélő hálózat¹²⁶;

¹²² VI. ötéves terv: az 1981-85 közötti időszakot öleli fel

¹²³ a témakörrel kapcsolatos dokumentumok nagy része „SzT” kategóriájú volt és 1989-ben, illetve a VSz megszűnése időszakában megsemmisítésre kerültek. A csekély mennyiségben megmaradt anyagok nehezen hozzáférhetők, mivel azok szétszórta, az ágazati szervek különböző irattáraiban kerültek archiválásra

¹²⁴ a rendszer a minisztériumok és az államigazgatás felsővezetőit szolgálta ki budapesti hatókörrel

¹²⁵ a rendszer az MSZMP Politikai Bizottság tagjainak kommunikációs igényeit szolgálta ki. Elnevezése a '90-es évek első felében módosult „KV” (kormányzati védett) megnevezésre

-
- nemzetközi kormány-összeköttetési géptáviró hálózat.

Az „MK” távbeszélő hálózat fővárosi hatókörrel a „K” távbeszélő hálózat analógiájára épült fel. Kialakításának szükségességét az indokolta, hogy a „K” távbeszélő rendszer túlságosan is nyitottá vált a felhasználói létszám növekedésével¹²⁷, így a Kormány és az államigazgatás központi szervei vezetőinek, mint zárt felhasználói csoport zavartalan kommunikációjának biztosítása már nem volt megoldott. A nyílt rendszert¹²⁸ egyetlen, a Magyar Posta által üzemeltett automata kapcsolóelem szolgált ki, tekintettel a felhasználói létszám alacsony szintjére. A távbeszélő központot a szolgáltatás-hozzáférési pontokkal összekötő hálózat szintén a Magyar Posta sajátja volt. A hálózat tehát információvédelmi képességekkel nem rendelkezett.

A kormányzati védett „PB” távbeszélő hálózat kiépítésére a „VCS” rendszerrel egyidőben került sor és a Kormány meghatározott tagjainak igényeit szolgált ki automata távbeszélő¹²⁹ központ közreműködésével. A szolgáltatás-hozzáférési pontok telepítési helye kizárólag Budapest közigazgatási területére korlátozódott. A központot és a végberendezéseket összekötő fizikai szakaszokon túlnyomósan „HH” kábelek¹³⁰ biztosítottak védelmet, ezért az egykori jelentések titkosított hálózatként említik. Az üzemeltetést a BM III/V. Csoportfőnökség végezte. Információvédelmi képessége a „HH” kábeleken alapult.

Az „ALTÁJ” országos automata mobil rádiótelefon hálózat¹³¹ a '70-es évek közepén létesült a Kormány vezeték nélküli kommunikációs igényeinek

¹²⁶ a rendszer elnevezése 1990 után megszüntetéséig „KT” (kormányzati titkosított) megnevezésre módosult

¹²⁷ a felhasználói létszám fokozatos bővülése a rendszer folyamatos fejlesztésének eredménye volt

¹²⁸ a rendszer információvédelmi eszközöket nem tartalmazott

¹²⁹ a központ a BM III/V. Csoportfőnökség Országházban kialakított hírközpontjában működött. A rotary típusú kapcsolóelemet a '80-as években ARF távbeszélő központ váltotta fel. A hívószámok e hálózatban háromjegyűek voltak

¹³⁰ „HH” kábel: ólomköpenyes kábel. Belső szerkezetét úgy alakították ki, hogy lehetőség legyen a rézvezető és a külső burkolat között állandó légnyomás kialakítására és fenntartására. A levegő nyomásának folyamatos ellenőrzésével lehetőség volt a mechanikus beavatkozások azonnali észlelésére. A kábelviszonylatokon fehérzaj generátort alkalmaztak, míg a szolgáltatás-hozzáférési pontoknál kialakított csatlakozófelületeket nyitásérzékelővel szereltek fel, mely az illetéktelen behatolás tényét a hírközpontban jelezte. HH kábelhálózat csak a fővárosban került kiépítésre, melynek tulajdonkezelője és fenntartója a BM III/V. Csoportfőnökség volt

¹³¹ ALTÁJ: a rendszer szovjet fejlesztésű volt, nevét a Szovjetunióban levő „Алтай” hegység után kapta. Elméletileg országos kiépítettségű volt, azonban – ha-

kielégítésére. A hálózat alkalmas volt a Belügyminisztérium és a Honvédelmi Minisztérium távbeszélő hálózatához – *kezelői közreműködés útján* – történő csatlakozásra. Az országos központ a Belügyminisztérium épületében üzemelt, regionális központjai Hármashatár-hegyen, Kabhegyen, Pécs-Misina-tetőn, Kiskunfélegyházán és Galyatetőn kerültek kiépítésre. A rendszer fenntartásáért a BM I/2. Osztály¹³² felelt, mivel információvédelmi eszköz a hálózatban nem került rendszeresítésre. A rendszer kezelői közreműködéssel a „K”, a BM, a HM és a Magyar Posta távbeszélő hálózatával volt összekapcsolható.

A „VCS” távbeszélő szolgáltatás igénybevétele manuális központ útján, csak kezelői közreműködéssel volt lehetséges, ami az erősen korlátozott létszámú felhasználói kör folytán nem okozott forgalmi torlódást. Aktív információvédelem nemzetközi kapcsolóközpontok viszonylatában valósult meg, míg a hírközpont és a szolgáltatás-hozzáférési pontok között „HH” kábelek biztosítottak védelmet. A kézi központ – *hasonlóan a „PB” rendszer kapcsolóközpontjához* – az Országházban kialakított speciális hírközpontban került telepítésre.

A felvázolt tervekkel ellentétben a kormány-összeköttetési géptávíró szolgáltatásokhoz hazánkban mindösszesen két állandó alkalmazásban álló, stacioner telepítésű¹³³ és egy alkalmi felhasználású, mobilizálható szolgáltatás-hozzáférési pont létesült. A géptávíró szolgáltatás kapcsoló- és információvédelmi eleme szintén az Országházban települt. A géptávíró központot a végberendezéssel összekötő fizikai átviteli közegként „HH” kábel került felhasználásra. Információvédelmi szempontból a géptávíró hálózat működése teljesen megegyezett a „VCS” rendszer működésével.

A fejlesztési elképzelések alapján az integrált rendszer szolgáltatásait tekintve komplex lett volna, mivel a vizsgált időszakban használatos jelentősebb szolgáltatásfajta (távbeszélő és géptávíró) valamint a mobil rádiótelefon szolgáltatás nyújtása képességének megvalósítását célul tűzte ki. A tervben a BM III/V. Csoportfőnökség felügyelete alatt egységesül a Magyar Posta által üzemeltett „MK” távbeszélő rendszer, valamint a „PB” távbeszélő rendszer. Az „MK” hálózatban üzemelő szolgáltatás-hozzáférési pontok kiszolgálása a „PB” rendszer automata központja, illetve „HH” kábelek útján valósul meg.

sonlóan a GSM rendszerek magyarországi közvetlen megjelenését követő időszakhoz – a besugárzási területet illetően mindvégig fehér foltok maradtak

¹³² BM I/2. Osztály: a BM Anyagi-Pénzügyi-Technikai Főcsoportfőnökség (I. Főcsoportfőnökség) önálló osztálya, közismertebb nevén BM Híradástechnikai Osztály

¹³³ az egyik az Elnöki Tanács elnökét, míg a másik az MSZMP KB első titkárát szolgálta ki

Az összevont rendszer „VCS” távbeszélő hálózattal történő összekapcsolására csak kezelő útján van lehetőség.

A terv felvázolja az „ALTÁJ” mobil rendszer információvédelmi eszközökkel történő ellátását is, mely teljesülésekor a rendszer üzemviteli szempontból a BM III/V. Csoportfőnökség alárendeltségébe kerül. Szűkebb körben számoltak azonban a titkosított géptávíró szolgáltatások bővítésével, mivel az elsősorban a „K” vezetési rendszer korszerűsítéséhez kötődött.

Az integrált rendszerrel kapcsolatos elképzelések nem valósultak meg, melynek okát elsősorban a költségvetési források¹³⁴ hiányában látom. A VI. ötéves tervben minőségi változást a csak a nemzeti hírközpontok közötti információvédelmi eszközök¹³⁵ cseréjének, valamint a „PB” távbeszélő hálózat automata központja kiváltásának lebonyolítása jelentett. E fejlesztések mellett a Belügyminisztérium igyekezett szervezési oldalról is biztosítani a nemzetközi híradás mindenidejű működését, ezért 1981-ben megállapodást kötött a hazánkban állomásozó szovjet Déli Hadseregcsoporthoz mellett működő kormányhíradó osztállyal a különleges időszakok kormányhíradása megszervezésének közös feladatairól [29].

1989-ig, a VII. ötéves terv időszakában érdemi, dokumentált rendszertechnikai változás már nem következett be. A kormányhíradás egészéhez hozzátartozik, hogy a vizsgált időszakban nem sikerült megoldani a szolgáltatáshozzáférési pontok közötti teljes, elektronikus technikai eszközön alapuló információvédelmet,¹³⁶ vagyis a speciális – *ennél fogva költségesebb beruházást és fenntartást igénylő* – „HH” kábel kiváltására sem volt mód. A kábeltípus rendszerben tartása eredményezte azt, hogy a felhasználói kör jelentős bővítésével az integrált rendszer tervezői sem számolhattak.

A BM III/V. Csoportfőnökség által alkalmazott terminológia miatt a Magyar Posta által üzemeltetett „K” távbeszélő hálózat nem tartozott a kormányhíradó rendszerek körébe. A folyamatos fejlesztések eredményeképpen

¹³⁴ a BM III/IV. Csoportfőnökség a kapcsolódó költséget a VI. ötéves terv időszakában 213, 4 millió forintban állapította meg, míg a VII. ötéves terv időszakára 234, 7 millió forinttal tervezett

¹³⁵ a „Korall” trónkitkosító eszközök „Delfin” trónkrejtjelzőkre, vagyis államtitok kategóriájába tartozó információk forgalmazását lehetővé eszközökkel kerültek kiváltásra. Ez a technikai váltás azonban nem oldotta meg a távbeszélő központ és a végbe-
rendezés közötti információvédelem problematikáját

¹³⁶ a kormányhíradás információvédelmi rendszerét a tagországok nemzeti közti egyezmények alapján működtették, tehát a végpontok közötti elektronikus információvédelem megoldása csak közös erőfeszítés útján lett volna megoldható

országos méretűvé vált, melyben a hálózat fő kapcsolóelemét a fővárosban¹³⁷ elhelyezett távbeszélő főközpont alkotta. A szolgáltatás-hozzáférési pontok közvetlenül vagy alközpontokon¹³⁸ keresztül kapcsolódtak a főközpontoz.

A hálózat jelentősége abban állt, hogy a bekapcsolt felhasználók¹³⁹ minden időben azonos minőségi paraméterekkel bíró nyílt távbeszélő szolgáltatást vehetett igénybe az ország bármely pontján. A rendszert a Magyar Posta tartotta fenn, a teljes hálózat távközlési infrastruktúrájának alrendszereként működött, budapesti és vidéki automata kapcsolóközpontjait a biztonsági ágazat üzemeltette.

Függetlenül a Belügyminisztérium által képviselt állásponttól, a „K” távbeszélő hálózat kormányzati távközlésben betöltött szerepe igen jelentős, és ennek megítélését erősítheti az is, hogy az írásos kommunikációt támogató géptávíró szolgáltatásokat a Magyar Posta biztosította – *a honvédelmi és belügyi ágazatok kivételével* – az államigazgatás teljes szektorában.

A kormányhíradás biztosításán túl a belügyi ágazat saját szervei kommunikációs igényének kiszolgálására a következő távközlő rendszereket¹⁴⁰ hozta létre:

- BM távhívó-távbeszélő hálózat;
- BM országos géptávíró hálózat;
- BM országos mozgószerelési rádióhálózat;
- BM MRKB mobil rádiótelefon hálózat.

Az ágazat távközlő rendszerei jellemzően stacioner telepítésűek voltak (távhívó-távbeszélő hálózat, országos géptávíró hálózat, az országos mozgószerelési¹⁴¹ rádióhálózat, MRKB mobil rádiótelefon hálózat), és elsősorban a rendészeti szervek igényeinek kielégítésére voltak hivatottak. A fenntartás és üzemeltetés megszervezését és irányítását a Híradástechnikai Osztály és a

¹³⁷ a Magyar Posta Schweidel utcai erősítőállomásán

¹³⁸ melyek a Magyar Posta megyeszékhelyeken üzemelő területi szerveinél, valamint a „K” vezetési rendszerbe kapcsolt objektumokban kerültek telepítésre

¹³⁹ elsőként a Kormány, azt követően az államigazgatás központi és területi vezetői, majd a '80-as években már a fontosabb állami vállalatok, társadalmi szervek vezetői is bekapcsolásra kerültek

¹⁴⁰ e fejezetben ezek összességét tekintem rendészeti kommunikációs rendszernek

¹⁴¹ mozgószerelések: olyan feladatot ellátó személyek vagy szervezetek, melyek tevékenységük ellátása során (irányítás, vezetés, információval való ellátás, stb.) kommunikációs igényeiket mobil távközlő rendszerek útján elégítik ki

Határőrség Országos Parancsnokság végezte. A fejlesztési kérdéseket a BM centralizáltan, a Híradástechnikai Osztály felelősségi körébe utalva¹⁴² kezelte.

A szaktárcák közötti folyamatos együttműködésnek köszönhetően a Belügyminisztérium a honvédelmi ágazat rendszereihez hasonló képességekkel rendelkezett, természetesen ez alól kivételt képeznek a katonai tábori hírend-szer által nyújtott szolgáltatások, melyek egyes elemeiben voltak csak felfe-dezhetők a határőrizeti szerveknél.

A vezetékes távbeszélő rendszerek technikai fejlesztése a '60-as évek végén kezdődött meg a kapcsolóközpontok gépesítésével és ennek eredmé-nyeképp a távhívás az 1970-es évek elejére automatizálódott.¹⁴³ Gyakorlatilag ebben az időszakban alakult ki a *helyi központi – gócközponti – gyűjtő-gócközponti – főgyűjtő-gócközponti* struktúra, ami egészen 2001-ig meghatá-rozta a BM digitális távbeszélő hálózatának topológiáját is teljesen igazodva a közigazgatás területi rendszeréhez [30]. A távbeszélő rendszer legfőbb gyen-geségét az önálló (helyközi) átviteltechnikai hálózat hiánya okozta, mely ösz-szeköttetéseket a Magyar Posta biztosított.

A rendszer a kapcsolóközpontok szintjén összekapcsolható volt mind a Magyar Posta, mind a Magyar Néphadsereg hálózatával, de jellemző volt egy-egy távbeszélő szolgáltatás-hozzáférési pont államigazgatási szervekhez törté-nő kihelyezése is.

A honvédelmi ágazattól eltérően a géptávíró kapcsolástechnika auto-matizálása teljesen elmaradt. Ennek egyik oka, hogy a '80-as évek második felében bevezetésre került az egységes gépi prioráló rendszer¹⁴⁴, mellyel a saját távbeszélő hálózat útján létesülő, rejtjelzett¹⁴⁵ modemes adatkapcsolatok révén lehetett ellenőrzési és információvédelmet igénylő adatforgalmi tevékenységet

¹⁴² e körbe gyakorlatilag nem tartozott bele a kormányhíradással összefüggő lénye-gi fejlesztési tevékenység. E téma 1990-ig a – Belügyminisztérium struktúrájának átalakításáig – BM III/V. Csoportfőnökség hatáskörébe tartozott

¹⁴³ a belügyi ágazat távbeszélő hálózatában ugyan azon eszközök kerültek alkalma-zásra, mint amelyeket a Magyar Posta, illetőleg a honvédelmi tárca is alkalmazott

¹⁴⁴ priorálás: a személyes adatok ellenőrzését jelenti, mely a bünyügyi és különböző adatárak felhasználása útján, szigorú dokumentálási kötelezettség mellett történik

¹⁴⁵ a végberendezések között kialakított rejtjeles kapcsolatokon a továbbiakban le-hetőség nyílt államtitkot képző információk áramoltatására is. A belügyi ágazat nyílt modemes adatkapcsolati hálózatai 1986-ban kerültek rendszeresítésre, míg a rejtjelzettek 1987-ben

végezni, kikerülve a géptáviró szolgáltatások¹⁴⁶ igénybevételét. Másik ok a külön infrastruktúrát nem igénylő telefax berendezések megjelenése és viszonylag gyors elterjedése volt, mely eszköz szolgáltatásai révén képes volt kiváltani a géptávirót.

A mozgószerelési rádiórendszerek fejlesztése az állam- és közbiztonsági érdekek¹⁴⁷ figyelembevételével kezdődött meg az 1960-as évek közepén. A hálózatok kezdetben lokális jellegűek voltak, majd a fokozatos fejlesztési folyamat hatására a '80-as évek elejére országos lefedettségű, önálló megyei rendszereket képeztek. A megyei szinkronrendszerek kialakításának megkezdése csak a '80-as évek legvégén kezdődött meg. Természetesen a határőrizeti tevékenység biztosítása érdekében az államhatár mentén került telepítésre önálló rádiórendszer [31].

A belügyi ágazat az „ALTÁJ” mobil rádiótelefon rendszerével egyidejűleg hozta létre az MRKB1¹⁴⁸ mobil hálózatát, amelynek hatóköre csak a főváros területére terjedt ki, felhasználói elsősorban a rendészeti szervek voltak. A Belügyminisztériumban elhelyezett központja útján lehetséges volt a honvédelmi tárca távbeszélő rendszerének, illetve a közületi hálózat irányába hívást kezdeményezni, illetve onnan fogadni. Az igények bővülése miatt a '80-as évek végén került átadásra az MRKB2¹⁴⁹ hálózat, melyet a honvédelmi tárca is rendszeresített.

A belügyi ágazat kommunikációs alrendszereinek összességét áttekintve megállapítható, hogy a Kormány kommunikációs igényeinek meghatározó részét a belügyi ágazat üzemeltetésében levő kommunikációs hálózatok elégítették ki. A tárgyalt időszakban a Magyar Postával együttműködve folyamatos fejlesztés folyt – a „VCS”, „PB”, „ALTÁJ”, valamint géptáviró rendszerek kivételével – az összes ismertetett hálózaton, ami azt eredményezte,

¹⁴⁶ a géptáviró hálózat végleges felszámolására 39 évvel rendszerbe állítása után, 2000. november 25-én került sor. Ekkor kerültek kivonásra a géptáviró szolgáltatásokhoz kapcsolódó rejtjeltechnikai anyagok is

¹⁴⁷ Európai viszonylatban az 1960-as években kezdődnek meg a rendészeti munka támogatását célzó állandó telepítésű URH rendszerek kiépítése. Magyarországon a Belügyminisztérium által felügyelt szervek esetében, így az állambiztonság, rendőrség és határőrség tekintetében is közös infrastruktúrára épülő rádióhálózatok jönnek létre, melyen a felhasználói csoportokat külön rádióhálókba szerveztek

¹⁴⁸ 8 csatornás analóg mobil rádiótelefon rendszer (170 MHz, 9 MHz duplex távolság)

¹⁴⁹ szintén 8 csatornás analóg mobil rádiótelefon rendszer (451 MHz, 10 MHz duplex távolság). Mind az MRKB1, mind az MRKB2 rendszer a BM Híradástechnikai Osztály üzemeltette

hogy a honvédelmi ágazathoz hasonló egyenszilárdságú távhívó-távbeszélő, mobil rádiótelefon és mozgószolgálati rádiórendszer jött létre.

1.2.2.3. Közigazgatás

Az 1.1. alfejezetben leírtak alapján *a közigazgatás az államigazgatás, amely központi, területi és helyi szervek hierarchikus rendszere, valamint az önkormányzati szervezetrendszer is, amely alá-fölérendeltségi viszonyban nem álló területi és helyi szervek együttese.* E megállapítás mentén a közigazgatási szervek által igénybevehető távközlési szolgáltatások egy része már áttekintésre került.¹⁵⁰

A közigazgatás fennmaradó szegmense – *főként a tanácsi testületek*¹⁵¹ – kommunikációs igényeit kizárólag csak a Magyar Posta által a lakossági és gazdasági szereplők részére biztosított infrastruktúra igénybevételevel oldhatta meg. Lényegében e szervek távközlési lehetőségei a civil szektor lehetőségeivel voltak teljesen azonosak, vagyis számukra e lehetőség egyértelműen megnyitási és minőségi hiányt jelentett mind a távbeszélő, mind a géptáviró szolgáltatásokat illetően. A közigazgatás tekintetében minden további vizsgálódás nélkül kijelenthetem, hogy az 1967-1998 közötti időszakban önálló közigazgatási kommunikációs rendszer létezéséről és működéséről nem beszélhetünk.

1.2.2.4. Minősített időszaki távközlés

A normális működésétől eltérő időszakokban (katasztrófhelyzet, külső hatalom fenyegetése, háborús helyzet, illetve egyéb hasonló helyzet) az állami irányítás és az intézményrendszerek fenntartása, illetve folyamatos működtetése létfontosságú feladat, melynek célja, hogy az eredeti helyzethez való visszatérés mielőbb megvalósuljon.

A bipoláris világrend fennállása során a minősített időszakokra történő felkészülés elsősorban a koalíciós háború sikeres megvívása lehetőségének feltételeit akarta megteremteni. Ennek érdekében az állami és gazdasági élet minden szereplőjének várható feladat- és tevékenységrendszerét előre ki kellett dolgozni¹⁵². A sikeres végrehajtás alapját a különböző jogszabályok és ágazati normarendszerek biztosították.

¹⁵⁰ Kormány, minisztériumok, fegyveres és rendészeti szervek, az államigazgatás területi szervei

¹⁵¹ a mai önkormányzatok funkcionális jogelődjei

¹⁵² a mai fogalmaink szerint e tevékenység a gazdaságmozgósítás része. A hadtudományi lexikon a szerint a gazdaságmozgósítás – az országmozgósítás részeként – az

A kormányzat, valamint az állami vezetés és irányítás folyamatosságának biztosítására került megszervezésre és kiépítésre a „K” vezetési rendszer, melynek egyik eleme volt a K-600-as hírrendszer. A hírrendszer a tervekben meghatározott objektumok, körletek és egyéb helyiségek közötti kommunikáció érdekében előkészített összeköttetések rendszeréből állt. Ennek teljes, illetve részbeni üzembe helyezése adott esetben kiadandó intézkedés alapján történhetett, korlátozott idő alatt. Az összeköttetések alapját a Magyar Posta távközlési infrastruktúrája jelentette.

A K-600-as hírrendszer megtervezéséért, megszervezéséért és pénzügyi finanszírozásáért a kormánysszervek, ezen belül a közlekedési és postaügyi, illetve a pénzügyi tárca felelt, melyekkel szorosan együttműködött a honvédelmi és belügyi tárca.

A „K” vezetési rendszeren túl mind a honvédelmi (K-300 és K-500), mind a belügyi tárca (K-400) rendelkezett előkészített összeköttetésekkel. Tehát mindkét tárca számára a minősített időszak feladatainak függvényében lehetősége nyílt a K összeköttetések és saját stacioner, illetve tábori hírrendszerei átviteli útjainak legmegfelelőbb kombinálására.

A K-300, K-400 és K-500-as rendszerek szintén a Magyar Posta alapinfrastruktúrájának részét képezték.

1.3. Összegzés, következtetések

Megítélésem szerint javaslatot dolgozni ki a kormányzati távközlés rendszere valamely jellemzőjének minőségileg új átalakítására és kiegészítésére a komplex rendszer fejlődéstörténetének ismerete nélkül nem lehetséges.

Miután egy-egy rendszer múltbeli továbbfejlesztésének iránya a tudományos kutatások objektív eredményei mellett mindig is függött a végrehajtók, illetve a környezet szubjektumától, ezért a történeti áttekintés elvetése könnyen teremthet olyan helyzetet, ahol egy folyamat ok-okozatának értelmezése, magyarázata lehetetlen lesz, ezáltal a kitűzött cél elérése is kérdésessé válik.

ország békegazdaságának a háború követelményei szerinti áttérése a hadigazdálkodás rendszerére. Célja a gazdaság összes (termelő, közlekedési, hír- és távközlési, gyógyító és szolgáltató) erőforrásának átállítása a háborús feladatok megoldására. A gazdaságmozgósítás előkészítését célszerű a korszerű háború figyelembevételével már békében előkészíteni

Jelen témakör esetében pedig a múlt lehetőségek adta legteljesebb megismerése és rendszerezése egyenesen elkerülhetetlen mivel a forrásanyagok kvantitatív és kvalitatív hiányának ténye feltételezi, hogy a fejlődésben többszeri törések következhetnek be, mely körülmények behatóbb ismerete elősegítheti a fejlesztési javaslatok objektivitását.

A fejezetben leírtakat összegezve, valamint a kormányzati távközlést 1989-ban megvalósítók körét áttekintve az alábbi megállapítások tehetők:

- 1., létezik a Magyar Néphadsereg által fenntartott *katonai kommunikációs rendszer*, amely elsősorban a honvédelmi ágazat igényeit elégíti ki. A rendszer a kapcsolóközpontok szintjén csatlakozik a rendészeti kommunikációs rendszerhez, a civil szféra részére fenntartott infrastruktúrához. A honvédelmi tárca a kormányzati távközlést elsősorban a minősített időszakokban, a „K” vezetési rendszerben való szerepvállalás révén szolgálja, mely azt jelenti, hogy rendszerével csatlakozik a Magyar Posta által fenntartott K-300, K-500 és K-600-as hálózatokhoz. Másodsorban saját rendszere útján biztosítja a Honvédelmi Minisztérium és a minisztérium felügyelete alá tartozó államigazgatási szervek egymás közötti kommunikációját. Ezen túlmenően egy-egy szolgáltatás-hozzáférési pont kihelyezésével az államigazgatás különböző szerveivel létesít kapcsolatot;
- 2., a Belügyminisztérium alárendeltségében funkcionál egy *rendészeti kommunikációs rendszer*, amelynek fenntartói különböző belügyi szervek. Lényegében a katonai kommunikációs rendszerrel kapcsolatosan tett megállapítások – *az ágazati sajátosságok figyelembe vétele mellett*¹⁵³ – e rendszerre ugyanúgy érvényesek;
- 3., szintén a Belügyminisztérium alárendeltségébe utalva működik a „*kormányhíradás*”-t kiszolgáló kommunikációs rendszer, melynek fenntartója az állambiztonsági szolgálat. A területi és ellátottsági hatókör szűk, a Kormányt és a központi államigazgatás szerveinek egy részét szolgálja ki. Más hazai kommunikációs rendszerekkel nincs összekapcsolva, tehát teljesen zárt. Kapcsolódik a „K” vezetési rendszerhez, vagyis a minősített időszak vezetési feltételei biztosítani igyekezik;
- 4., hírközlési alpinfrastruktúrája kiterjedtségének révén a Magyar Posta jár élen a kormányzati távközlés gyakorlati megvalósításában.

¹⁵³ az ellátottak körét, illetve a minősített időszaki távközlést tekintve

Üzemeltetési körében van a „K”, és „MK” távbeszélő hálózat, illetve a honvédelmi és belügyi ágazat tekintetében a kormány-összeköttetési távbeszélő és géptávíró hálózat nemzeti központok közötti fizikai kapcsolatainak hazai szakaszai, a katonai és rendészeti kommunikációs rendszerek távbeszélő és géptávíró központjait összekötő helyközi átviteli utak jelentős része¹⁵⁴, valamint közreműködik a „VCS”, „PB” és a titkosított géptávíró rendszert kiszolgáló „HH” kábelek fenntartásába. Infrastruktúrájára támaszkodva biztosítja továbbá a K-300, K-400, K-500 és K-600-as hálózatokat, vagyis a minősített időszakos kommunikációs igények kielégítésében vállal szerepet.

Az 1-3. pontban felsorolt kommunikációs rendszerek hatókörén kívül eső államigazgatási szerveket, valamint az Országgyűlést a lakossági és gazdasági szereplőkkel egy minőségi szinten szolgálja ki;

- 5., önálló közigazgatási kommunikációs rendszer nem létezik.

Fentiek alapján rögzíthető, hogy 1989-ben a kormányzati távközlés megvalósulásában a honvédelmi tárca, a belügyi tárca, valamint a Magyar Posta játszotta a legfőbb szerepet.

Függetlenül attól, hogy hazánkban a gyakorlatban is megkezdődött a különböző adatátviteli célú kapcsolatok kialakítása és a telefaxok elterjedése, úgy gondolom, hogy a vizsgált időszakban a kormányzati távközlést érintően a legfőbb kommunikációs szolgáltatásfajta a távbeszélő szolgáltatás volt, melyel párhuzamosan az írásbeliség igényeit a géptávíró szolgáltatás elégítette ki. Ez elsősorban abból adódott, hogy a szereplők igyekeztek az analóg technikai megoldásokat alkalmazó alpinfrastruktúrájukat oly módon korszerűsíteni, hogy azok elsőként mennyiségileg teljesítsék a szolgálati igényeket. Természetesen a mennyiségi növekedés magában hordozta az infrastruktúra olyan irányú technikai átalakításának kényszerét is, mely végül is oda vezetett, hogy a főbb kommunikációs fajták igénybevétele könnyebbé vált,¹⁵⁵ illetőleg előkészítette a korszerűbb szolgáltatások (pl.: adatkapcsolatok) igénybevételét lehetővé tevő műszaki alapokat. A korszerűbb szolgáltatások elterjedését az országot érintő importkorlátozások is gátolták, ennek ellenére elmondható, hogy a katonai- és rendészeti kommunikációs rendszerek, valamint a „K” és „MK” távbeszélő hálózatok egyenszilárdá váltak, vagyis a szolgáltatás-hozzáférési

¹⁵⁴ a honvédelmi tárca országos mikrohullámú rendszer kiépítésével kezdte függetleníteni magát a Magyar Postától

¹⁵⁵ például: tárcsahangra való várakozás megszűnése, kezelő nélküli távhívás, automata géptávíró szolgáltatások

pontok bármelyikéről ugyanolyan minőségű szolgáltatás igénybevételére volt lehetőség.

A felhasználói kör viszonylagos állandósága miatt mennyiségi jellegű problémák nem jellemezték a kormány-összeköttetési, valamint a „PB” távbeszélő rendszereket. Mivel a rendszerek üzemvitelét állambiztonsági kérdéskörként kezelték, így azok a telepítésük időszakában az alkalmazott legmagasabb minőségi követelményeknek feleltek meg. A működés folyamán történtek kisebb fejlesztések, illetve készültek bővítési elgondolások, de a biztonsági szempontok¹⁵⁶ érvényesítésének aránytalan pénzügyi terhei miatt ezek nem valósultak meg. Ennek esett áldozatául az „ALTÁJ” mobil rádiótelefon-rendszer, mivel a források hiánya megakadályozta, hogy a „kormányhíradás” kritériuma szerint kerüljön átalakításra.

Az a tény, hogy 1967-1989 között önálló *közigazgatási kommunikációs rendszer* nem létezett annyit jelent, hogy az államigazgatási szervek helyi- és területi szervei kommunikációs igényeiket kénytelenek voltak a Magyar Posta lakossági és gazdasági szereplők részére fenntartott infrastruktúráján keresztül, szolgáltatási alapon megoldani. Ez számukra egyértelműen mennyiségi és minőségi hiányt jelentett mindkét kommunikációs szolgáltatást illetően, azonban maga az állam engedélyezett kevesebb prioritást az e szerveket érintő fejlesztések területén, élve a tervutasításos gazdasági rendszer jellegéből adódó lehetőségeivel. Ezt a mesterséges beavatkozást természetesen képes volt kompenzálni azzal, hogy teljeskörű felügyeletet gyakorolt a Magyar Posta, mint állami vállalat felett, így működési folyamatait is igényeinek megfelelően irányíthatta.

A tárgyalt időszakra vonatkoztatva elmondható, hogy a honvédelmi és belügyi tárca fejlesztései, illetve a kommunikációs rendszereikkel kapcsolatos irányítói tevékenységek centralizáltan folytak, szakmai szervezeteik – *fejlesztési és üzemeltetési szinten történő* – együttműködése a Magyar Postával szoros volt.

Leírtakat mérlegelve azt a következtetést vonom le, hogy a 3343/1967. számú kormányhatározat volt az első olyan dokumentum, amely előírta egy, a kormányzat kommunikációs igényeit kiszolgáló rendszer kialakítását. A határozat alapján ténylegesen megvalósult rendszer 1967-1989 között a kormányzati távközlés fogalma szerinti funkciót csak részlegesen töltötte be, mivel a „kormányhíradással” kapcsolatban következetesen alkalmazott biztonsági

¹⁵⁶ itt az információvédelmi kérdésekre kell gondolni

követelményrendszer a kommunikációs szolgáltatások igénybevevői körének kiterjesztését folyamatosan meggátolta.

Annak ellenére, hogy a korszerű nyugati technológiákat illetően Magyarország importja szigorú ellenőrzés és korlátozás alatt állt, mind a katonai- és rendészeti kommunikációs rendszerek, mind a Magyar Posta különböző távközlő hálózatai minőségi fejlesztéseken estek át, így az állambiztonsági korlátok miatt szűk kapacitású kormányhíradó rendszer mellett a kormányzati távközlés technikai megvalósulásában a honvédelmi, a belügyi, valamint a közlekedés és postaügyi tárca által felügyelt más szervek üzemeltetési körében levő rendszerek is szerepet kaptak.

E kombinált, sokszereplős megoldást elsősorban a korlátozott infrastrukturális lehetőségek indokolták, de a kormányzati távközléssel összefüggő érdekeket nem csorbította, hiszen az állami tulajdon túlsúlyából, valamint a centralizált államvezetés gyakorlatából adódóan ezek érvényesíthetők maradtak. E módszer alkalmazása mellett az 1967-1989 között hivatalban levő Kormányok mindegyike fontosnak ítélte meg, hogy az állam saját kommunikációs igényeit kiszolgáló technikai és szervezeti struktúrák fejlesztése és ellenőrzése kormányzati kézben maradjon, így a tradicionálisan meglevő rendszerek mellett az újonnan létesítettek mindegyikét az államigazgatási szervek irányítása alá helyezte.

Mindezek alapján kimondható, hogy Magyarországon 1967-1989 között a kormányzati távközlést önálló kormányzati kommunikációs rendszer nem szolgálta ki. A kormányzati szervek igényeit különböző államigazgatási, illetve állami szervezetek kommunikációs rendszerei együttesen elégítették ki az állam koordinációs tevékenysége mellett.

Hivatkozások:

- [11] Gyurgyák Béla: A helyközi és a József távbeszélő központ újjáépítése, Híradástechnika, 1-4. oldal, 1947/1., kiadva: a Híradástechnika 1999/1. számában, 35-38. oldal, ISSN 00182028
- [12] Dr. Király Béla: Honvédségből Néphadsereg, Budapest, Conexus Printer, ISBN 963 02 6860 4, 168. oldal, 1989.
- [13] A Magyar Posta Statisztikai Évkönyve 1979-1980., Budapest, Közlekedésügyi és Postaügyi Minisztérium Postafőosztály, Szerk.: Petőczy Istvánné, ISSN 0209 6587, 69-91. oldal, 1980.
- [14] Horváth Károly: A Magyar Posta ezer éve, Budapest, Pallas Stúdió, ISBN 963 9207 20 9, 51. oldal, 1999.

-
- [15] Hírközlés-statisztikai évkönyv 2000., Budapest, Hírközlési Főfelügyelet, Főszerk.: Dr. Juhászné Huszty Katalin, ISSN 1586 7226, 46. oldal, 2001.
- [16] Hungarian Telecommunications Regulatory Environment and Authority: by Communication Authority, International Directorate, Hungary, Budapest, pp. 5, November 1997.
- [17] Magyar Válasz az Információs Társadalom kihívásaira (tanulmány), Miniszterelnöki Hivatal, 15. oldal, 1999., <http://www.iif.hu/~lengyel/valasz/>
- [18] A Magyar Posta Statisztikai Évkönyve 1989., Budapest, Magyar Posta Központja, Szerk.: Petőczy Istvánné, ISSN 0209 6587, 72. oldal, 1990.
- [19] Magyar Közlöny
- [20] Dr. Tóth Zoltán: Akarjuk-e és képesek vagyunk-e a közigazgatás reformjára?, Magyar Közigazgatás LIII. évf. 7. szám, ISSN 0865 736 X, 387. oldal, Budapest, 2003.
- [21] Magyarország rendvédelme a második világháború utáni években, A magyar rendvédelem története, Budapest, Szemere Társulás, Főszerk.: Dr. Parádi József, ISBN 963 04 7958 3, 136-171. oldal, 1996.
- [22] Dr. Lindner Miklós: A híradó szolgálat félévszázada a híradástechnika fejlődésének tükrében, „A kommunikáció (híradás) helye és szerepe a vezetés rendszerében” tudományos konferencia, Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, 13-18. oldal, 2000. október 04.
- [23] Hamar Sándor: A katonai híradás fejlődésének és fejlesztésének lehetséges útjai, „Kommunikáció 2002.” Nemzetközi szakmai tudományos konferencia, Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, ISBN 963 86229 2 X, 245-117. oldal, 2002. október 30.
- [24] Dr. Kiszely Gábor: Állambiztonság: 1956-1990., Budapest, Korona Kiadó, ISBN 963 9376 13 2, 192-195. oldal, 2001.
- [25] Belügyminisztérium, Előterjesztés a Honvédelmi Bizottsághoz, Budapest, BM Távközlési Szolgálat irattár, Iktatási szám: M-36-10-5/1981., 1981. május 11.
- [26] BM III/V. Csoportfőnökség, Jelentés a párt és kormány felső vezetői titkosított távbeszélő hírendszereinek továbbfejlesztéséről a VI. és VII. ötéves terv időszakában, Budapest, BM Távközlési Szolgálat irattár, Iktatási szám: 36-60-21/1980., 1980. november 3.
- [27] Andrew, Christopher; Mitrohin, Vaszilij: A Mitrohin archívum, Budapest, Talantum Kiadó, ISBN 963 645 076 5, 565. oldal, 2000.
- [28] BM III/V. Csoportfőnökség, Jelentés a „K” vezetési rendszer, a párt és kormány felső vezetői titkosított távbeszélő hírendszereinek VI. ötéves terv időszakában, Budapest, BM Távközlési Szolgálat irattár, Iktatási szám: 36-10-5/4-1/1981., 1981. február 4.
- [29] BM III/V. Csoportfőnökség, Megállapodás a Déli Hadseregcsoporthoz mellé működő állambiztonsági kormányhíradó osztály és a Belügyminisztérium kormányhíradó osztálya között a különleges időszakok kormányhíradása megszervezésének közös feladatairól, Budapest, BM Távközlési Szolgálat irattár, Iktatási szám: M-36-10-5/3-1/1981., 1981. június
- [30] Pándi, Erik – Dr. Sándor, Miklós: Modernisation trends in the branch communication supporting system of the Ministry of the Interior, Budapest, Bolyai Szemle X. évf. 3. szám, ISSN 1416 1443, 64. oldal, 2001.

-
- [31] Pándi Erik – Vörös Szabolcs: A belügyminisztériumi ágazati távközlés fejlesztésének néhány kérdése, Tudomány Napja 2000. pályázat, földíjnyertes pályamű, Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, Egyetemi Könyvtár Kézirattára, N° KV 252, 22-27. oldal

Felhasznált irodalom:

1. Paturi, Felix R.: A technika krónikája, Officina Nova, ISBN 963 7836 44 6, Budapest, 1991.
2. Kennedy, Paul: A huszonegyedik század küszöbén, Napvilág Kiadó, ISBN 963 9082 09 0, Budapest, 1997.
3. Sallai Gyula, Aranyosné Börcs Janka (szerk.): A távközlés és információtechnológia jogi szabályozása, Hírközlési Főfelügyelet, ISBN 963 03 6663 0, Budapest, 1998.
4. Sallai Gyula, Vácziné Takács Zita, Aranyosné Börcs Janka (szerk.): A távközlés és információtechnológia jogi szabályozása – kiegészítő kötet, Hírközlési Főfelügyelet, ISBN 963 00 4343 2, Budapest, 2000.
5. Dr. Polyák Gábor: Az elektronikus közigazgatás néhány szabályozási kérdése, Magyar közigazgatás LIII. évf. 7. szám, ISSN 0865 736 X, 405-412. oldal, Budapest, 2003.
6. Dr. Szücs Ervin: Rendszer és modell I., Egységes Jegyzet, Eötvös Loránd Tudományegyetem TTK, Budapest, 1990.
7. Dr. Lajtha György: Az információs társadalom előzményei, „A Hírközlési Főfelügyelet országos fóruma”, Budapest, Hírközlési Főfelügyelet, ISBN 963 02 9961 5, 26-38. oldal, 1995. szeptember 14.

KÉPÁTVITEL ÉS ADATÁTVITEL LEHETŐSÉGEI ÉS TAPASZTALATAI A VEZETÉKNÉLKÜLI HARCÁSZATI KOMMUNIKÁCIÓ TERÉN

Más HARRIS rövidítések



- JTRS - Joint Tactical Radio System
- SDR - Software Defined Radio
- MMI - Man – Machine Interface
- CSSCS - Combat Service Support Control System
- BCB - Battle Command Brigade
- Sincgars - Single Channel Ground and Airborne Radio

HUTS One rule w. 852

next level solutions

25-Oct-99



**Harris Wireless
Messaging Products**



HUTS Overrule No. #1

next level solutions

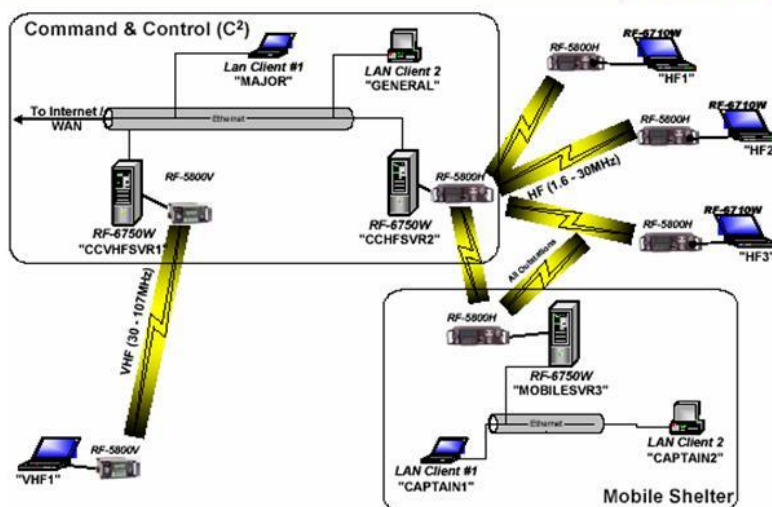
26-Oct-99

- Probléma az ismert SMTP protokoll HF rádiós átvitele
 - a protokoll csevegős volta miatti számos adásirányváltás nem hatékony a HF modemeken
 - A nagy fejlécek a HF kapcsolatot feleslegesen terhelik
 - TCP/IP problémák HF rádión:
 - a TCP/IP protokollt nagysebességű, kis hibaaarányú vezetékess médiára optimalizálták
 - Nagyon hatástalan a hibahajlamos csatornákon
 - Kis megbízhatóságú
 - Tovább növeli az SMTP fejlécek méreteit
- Probléma mind HF, mind VHF átvitel – HF problémásabb
- A megoldás a levelet file-ként küldeni, rádiós átvitelre való protokoll használatával

- E-mail és file átvitelt biztosít
- Fizikailag elkülönülő LAN-ok között működik különböző médiákon keresztül
 - Harris rádiók
 - Különböző típusú HF/VHF/UHF rádiókon
 - INMARSAT
 - Vezetékes összeköttetések
- A HF rádió teljesen automatikus kezelése
 - MIL-STD-188-141A ALE rádiós kapcsolatot létesít igény alapján
 - MIL-STD-188-110A/B Serial Tone / QAM 75 – 9600 bps
 - HF adatátviteli protokoll hibamentes e-mail átvitelt biztosít
 - STANAG 4838
 - STANAG 5066
 - FED-STD-1052
 - HF átviteli képesség maximalizálva teljes e-mail továbbításokkal
 - Üzenetek automatikus ütemezése, prioritás szerint sorba állítása

- RF-6750W Wireless Gateway, vezeték nélküli átjáró
 - Interface a TCP/IP LAN POP3, SMTP alkalmazások felé
 - Win2000 rendszeren fut
 - Exchange Servert használ
 - Hálózati adaptert, szinkron és aszinkron kártyákat használ
- RF-6710W Wireless Messaging Terminal
 - Adott az RF-6750W minden funkciója, kivéve a LAN interface
 - Végkészülékként, HF kliensként használható
 - Win2000 rendszeren fut

- Számos módszer van a hálózat átbocsátóképesség növelésére
 - Automatikus üzenettömörítés
 - Azonos címre küldött üzenetek összegyűjtve, együttküldve
 - Foglalt végpont automatikus újrarahívása
 - Időzített átvitel
- Alternatív útvonal választás
 - más csomópont(ok)on keresztüli küldés
 - más médian (pl. vezeték) keresztüli átvitel
- Adásismétlés előtt belehallgatás a csatornába véletlenidejű késleltetéssel
- Fontossági sorrend
 - Üzenetek érkezés ideje és fontosság szerint sorba állítva
 - A sorban a legfontosabb elemek átvitele történik elsőként



- A harctéri felhasználásra tervezett egyszerű kezelés
- Kompatibilitás és együttműködés szabvány formátumokkal és protollokkal
- Outlook User Interface integráltság
- Az ipari szabványnak számító HUITS-on alapul



Magasszintű tömörítés

Harris Wavelet

JPEG

Fontos képrészlet kiemelése

Képnézegető és konvertáló

JPG, TIF, BMP, MAC, IMG

- Harris folyamatosan fejleszti az eszközt már több mint 10 éve
- Lépést tart:
 - Operációs rendszerekkel
 - E-mail szerver és kliens alkalmazásokkal
 - Az üzleti hálózatok fejlődésével
 - Számítástechnikai platformokkal
- Tervek
 - további STANAG 5066 fejlesztések
 - beleértve az IP klienst
 - további STANAG 4538 fejlesztések
 - folyamatos fejlődés és karbantartás
 - a Harris rádiók változásainak és újításainak követése

- Többsávú
- Átvitel más csomópontok felé irányítása automatikusan
- Átvitel jellemzői
 - átbocsátó kapacitás
 - megbízhatóság
 - üzenetkezelés
- Csatorna-hozzáférés
- A termék érettsége és megbízhatósága
- Outlook integráltság (nem feltétlenül RF6750W-vel)
- Beépített képkezelés
- Elsőbbségek kezelése
- Konfigurációs eszközök
- Terméktámogatás



Harris Universal Imaging Transmission Software (HUITs)

HARRIS
RF-3700H

HUITs Overview, #10

next level solutions

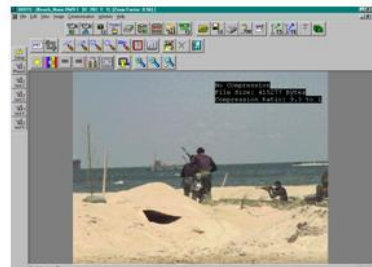
28-Oct99

A képátvitel fejlődése

Több mint 12 éves tapasztalat a képátvitelben



1989

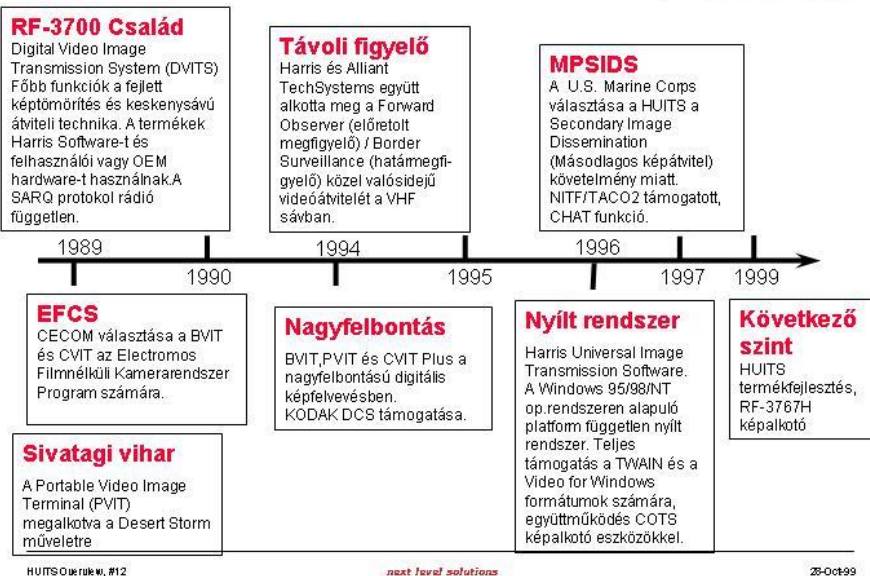


2001

HUITs Overview, #11

next level solutions

28-Oct99



- Nagyfelbontású képek átvitele szűkös rádiócsatornákon
- Interface nagyszámú rádió, titkosító és kamera számára
- A harcosok számára tervezett egyszerű működtetés
- Kompatibilitás és együttműködés szabványos formátumokkal és protokollokkal
- COTS hardware és software platform



- Prioritized Image Transmission (PIT)
- Magasrendű tömörítés
 - JPEG
 - Harris Wavelet
 - Érdekes részletek
- Élőbeállítások
- Free Image Viewer a formátumkonverzióhoz
- Nem csak állóképek
 - adatfileok
 - rövid mozgóképek
 - chat
- Egyszerű hálózat a frekvencia-megosztás miatt

- Légi felderítés
- Gépjármű felderítés / Csata értékelés
- Shipboard Interdiction-**Fedélzeti tiltás/zárótűz !?**
- Mobil és fix harcálláspont
- Határmegfigyelés / Határsértés ellenőrzése
- Vészhelyzeti reagálás / Gyorstelepítés
- Katasztrófa és Kárfelbecslés
- Rendfenntartás
- Orvosi esetek kiértékelése

- Hardware
 - Standard PC platforms
 - ≥ 300 Mhz PII, 64 MB RAM, 4GB H/D
 - Asztali gépek, laptopok, robosztus taktikai PCk
- Software
 - Windows® 98SE, NT 4.0
 - Windows® 2000 & XP
 - Standard Windows applikációk
 - Standard install/uninstall

- Digitális kamerák
 - TWAIN
 - SCSI
 - PCMCIA RAM disk vagy harddisk
 - Soros vagy párhuzamos
- Analóg kamerák
 - Video for Windows
 - Standard frame grabbers
 - NTSC vagy PAL
- Scannerek
 - TWAIN
 - Bármilyen, amihez van Windows driver

Image Formats	➤ NITF, JPG, TIF, BMP, TGA, PSD, & HW ➤ Plus 12 others
Image Capture (Scanner/Camera)	➤ 16 and 32 bit TWAIN ➤ Video for Windows ➤ PCMCIA
Protocol	➤ TACO2 (NITFS) ➤ SARQ (EFCS)
Operating System	➤ Windows 98SE/NT ➤ Printer support
PC Hardware	➤ Platform Independent ➤ PCMCIA Technologies
Communications Interface	➤ Synchronous RS-232 ➤ Asynchronous RS-232 ➤ COTS Landline Modem ➤ INMARSAT

HUIITS Kommunikációs Interface

- HUIITS szinte minden adatátviteli rádiót támogat
- Standard rádiós beállítások

AN/PRC-150	AN/PRC-137	AN/PRC-119
RT-1523(C)	AN/PSC-3	AN/PSC-5
LST-5C	AN/PRC-138	AN/PRC-117A/D
MST-20	AN/WSC-3	AN/PRC-117F
RF-5800M/U	RF-5800V	RF-5800H

- Titkosító beállítások

KY-57	KY-58	KG-84
KY-99	KY-68	KIV-7

- Egyéb kommunikációs beállítások

STU-III	Land line modem	Inmarsat
---------	-----------------	----------

- A protokoll a rendszerműködés legfontosabb összetevője
- Taktikai rádió protokoll hatékonysága
 - Gyors adatátvitel a jó csatornákon
 - Megbízható adatátvitel rossz minőségű csatornákon
 - Harris szaktudás
- SARQ
 - Packet alapú
 - Adaptív FEC
 - Burst Mode
 - Optimalizált képátvitel a taktikai rádiókon
- TACO2
 - NITFS együttműködő-képesség

- 100+ kamera integrálva felhasználói hordozható eszközökbe
- 300+ HUITS integrálva Litton HTU készülékekbe
- 100+ HUITS integrálva Panasonic CF-25 készülékekbe
- 50+ HUITS integrálva standard asztali PC-kbe
- 20+ HUITS integrálva más felhasználói platformokon
 - Litton Rugged Notebook
 - PW Lite
 - PGI
 - Toshiba Libretto



- HUITTS méretezhető képfelvevő és továbbító mag
- Harris közel 40 éves tapasztalata a katonai rendszerek és 12 éves tapasztalata a képátviteli rendszerek terén
- Harris kulcsrakész, testreszabott taktikai és stratégiai rendszereket szállít
 - Felhasználói nagyfelbontású légi fényképezés
 - COTS és OEM hardware/software felhasználói integrálása
 - HÁP rendszerek

- A Harris szaktudása biztosítja a méretezhető képalkotó rendszereket.





- Alkalmazás
 - Határmegfigyelés
 - Vészhelyzeti reagálás
 - Környezeti reagálás
- Érzékelő bemenet
 - Digitális kamerák
 - Video kamerák
 - I.R. kamerák
- GPS
 - kommunikáció
 - VHF/UHF LOS
 - UHF TACSAT/INMARSAT
 - BLOS
- HUITTS előnyei:
 - Állóképek és videó klipek
 - hordozható terminálok
 - közel valós idejű képtovábbítás
 - kapcsolat bármilyen adatátviteli rádióhoz

- Software alkalmazások
 - Windows® NT 4.0 és 98
 - teljesen automatizált e-mail különböző médiákon
 - TCP/IP LAN kapcsolódás rádiókhoz
 - megbízható protokoll a rosszminőségű csatornákhöz



- MS Outlook felhasználói felület
- Két termék:
 - Server: RF-6750W - interface LAN felé
 - Client: RF-6710W - végkészülék
 - standard PC hardware felhasználásával
- Média: HF, VHF, UHF, Tacsat, vezetékes, INMARSAT

Integrálható a HUITTS-hoz teljes hálózati képátvitelt biztosítva

A képátvitel
tömörítést igényel.
Tömörítés nélkül a
képek túl nagyok a
keskenysávú
csatornákon való
átvitelhez.



Ez a kép 55x
gyorsabban
továbbítható
így, mint
tömörítés
nélkül.



A nagy tömörítés
eredménye igen
kis képméret, de
a képminőség is
romlik.



PIT (Prioritized
Image
Transmission)
használatával
kiválaszthatóak
fontos
képterületek,
melyeken csak
kis tömörítés
történik.



- A Harris megoldása a katona számára készült
- A kezelés egyszerűsége
 - Rádió előbeállítások
 - Egér működtetés
 - Felhasználói kezelőfelület
- Együttműködőképesség
 - Platform függetlenség
 - Univerzális kamera/scanner interface
 - Katonai rádió interface
 - Standard protokollok és képformátumok
- Teljesítmény
 - Gyors, megbízható protokollok a taktikai rádiókapcsolatok számára
 - Már bizonyított az US és tengerentúli hadseregekben

- COTS - Commercial Off-The Shelf
- LOS - Level Of Sight
- PIT - Prioritized Image Transmission
- FEC - Forward Error Correction
- SARQ - S Automatic Repeat Request
- TACSAT - Tactical Satellite
- TACO2 -
- NITFS -

KRIMINOLÓGIAI JELENSÉGEK MÉRÉSE ÉS MÉRHETŐSÉGE A KOMMUNIKÁCIÓ ÉS A MINŐSÉGBIZTOSÍTÁS TÜKRÉBEN

Bevezető

A Belügyminisztérium, mint a Magyar Köztársaság egyik legnagyobb intézménye az ország igazgatásában a belső ügyek minisztériumaként működik. A jogszabályokban és az állami irányítás egyéb jogi eszközeinek megfelelően vesz részt a kormányzati munkában, irányítja a szakigazgatással és a közbiztonsággal, a katasztrófák elleni védekezéssel, egyéb rendészeti feladatokkal kapcsolatos tevékenységet, valamint többek között az önkormányzatokkal kapcsolatos feladatokat. Közreműködik a bűnmegelőzési tevékenységek ellátásában és végzi az általános közigazgatás-szervezési és fejlesztési feladatokat.

A munka közben a munkatársak egy sor olyan társadalmi jelenséggel kerülnek szembe, amely során felmerül a kérdés, hogy a norma-követés vagy éppen a norma-sértés milyen mértékű. Ezekre a kérdésekre akkor adható egzakts és (közel) objektív válasz, ha a mértéket meg tudjuk "mérni". A kriminológiai jelenségeknél azonban ez a "mérés" nem olyan egyszerű és egyértelmű, pedig a normák rendszerében azok egy része jól definiált sablonokat is ad, amikor egy-egy tényállásnál – ahhoz illeszkedő módon – a büntetési tételre vonatkozó sávot (től – ig határt) is meghatároz. Azonban éppen a büntetés mértékének kiszabásához meg kell tudni mérni a normasértés mértékét és ahhoz illeszkedően kell alkalmazni azt. Példaként egy egyszerű sebességtúllépés közlekedési szabálysértés esetén a jól meghatározható és könnyen mérhető fizikai mennyiség miatt az eljárás viszonylag jól kezelhető, azonban a valóságban előforduló esetek többsége ennél lényegesen összetettebb.

1.1. A kriminológiai jelenségek és a kommunikáció összefüggései

A kriminológia vizsgáldási köréhez tartozó jelenségekkel kapcsolatosan a kommunikáció kérdésköre két, eltérő aspektusból merül fel. Ez tulajdonképpen a jelenségekhez való kapcsolat alapján jellemezhető külső, illetve belső kommunikációként.

A külső kommunikáció alatt a kriminológiai eseménnyel összefüggő és a kívülvilág (a társadalom) felé irányuló információ-szolgáltatást értjük. A belső kommunikáció pedig a kriminológiai jelenséggel összefüggő munkatevékenység során alkalmazott és szükséges információ cserét jelenti.

A kommunikáció fejlesztése szempontjából elsőrendű tényezőt jelent az emberi viselkedés és kifejezőképesség, azonban a belső kommunikáció esetén jelentős szerepet kap az infrastruktúra, mint kiszolgáló eszközrendszer megléte, vagy hiánya is.

1.2. A belügyi munka és a minőségbiztosítás összefüggései

A belügyi szakmai tevékenység során olyan társadalmi jelenségekkel összefüggő kérdések merülnek fel, amelyek többek között a kriminológia vizsgálódási köréhez tartoznak. Az ezekre adandó válaszok során azt is vizsgálni célszerű, hogy az események milyen mértékben változnak, fejlődnek-e egyáltalán, illetve milyen minőségű munkavégzés folyik ezen a területen.

A belügyi szakmai munka minőségének megítélésénél is a klasszikus "minőség" definíciót érdemes alapul venni. E szerint a minőség nem más, mint a vevő, illetve a partner megelégedettsége. A BM szakterületére vonatkoztatott jelenségek esetében azonban már a *vevő*, illetve a *partner* is legalább 2 féle módon értelmezhető:

- vevő-elégedettség az individuum (egyén) síkján
- vevő-elégedettség a társadalom (helyi vagy szélesebb közösség) síkján.

Ennek megfelelően egy adott kérdést (pl. milyen mértékű a bűnözés?) két-féle formában lehet (és kell) feltenni:

- a) hogyan értékeli az egyén a bűnözést? {a lakóhelyén, vagy lakókörnyezetében, illetve munkahelyén}
- b) hogyan értékeli a közösség, vagy önkormányzat, illetve a társadalom a bűnözést a körzetben?

Az elégedettség ráadásul teljes mértékben szubjektív kategória és így ennek megítélése kizárólag a szóban forgó személytől függ. Ha az értékítéletet több személyből álló csoport alkotja, abban az esetben is a különféle módszerrel történő felmérés esetén (eltérő kérdések feltevésével) általában más-más, többé-kevésbé eltérő, illetve csak részben egyező, egymást átfedő eredményt kapunk. Így a munkavégzés minőségének megállapítása tulajdonképpen komplex mérhetőségi problémát vet fel.

1.3. A rendőrségi minőségfejlesztés

A fejlett nyugati társadalmakban a 80-as évek óta zajlik a közigazgatási-kultúra váltása. Ennek lényege, hogy mindenütt a lakosság, az állampolgár igényeit helyezik a működés középpontjába. A közigazgatás-fejlesztési programok központi kérdésként kezelik a közigazgatási szervek ügyfél-centrikus működését, a közintézmények hatékonyságának és eredményességének, valamint az állampolgárok elégedettségének javítását.

Magyarországon a 90-es években indult el – kezdetben a gazdasági szférában – a minőségfejlesztési tevékenység, mely egyben a szervezeti kultúra tudatos megváltoztatását jelenti. Napjainkban a magyar közigazgatásban is óriási az igény az egyszerűbb és olcsóbb munkamódszerek, illetve a minőségi meg-

oldások alkalmazására. A rendőrség – mint speciális közigazgatási szervezet – sem mentes ettől az igénytől.

Ezek után óhatatlanul felmerül a kérdés, hogy miért van szükség rendőrségi minőségfejlesztésre? A lehetséges válaszoknak csupán egy részét adjuk meg az alábbiakban, a teljesség igénye nélkül.

- A közelgő EU csatlakozás miatt az európai minőségi normák meghonosítása nemcsak a versenyszférában, hanem a közszférában, ezen belül a rendőrségen is elengedhetetlenül szükséges.
- Egyre növekvő társadalmi elvárások jelennek meg a rendőrséggel szemben. A hatékonysági és a minőségi mutatók itt sem hagyhatók figyelmen kívül, mivel a piactgazdasági környezetben működő közszolgálati szektorban is egyre szigorúbbak a követelmények. Az állampolgároknak egyre szigorúbbak a követelményei a közszolgálat és a szolgáltatások színvonala iránt, amelyeknek a hagyományos munkamódszerekkel, szervezeti kultúrával és alkalmazotti hozzáállással már nem lehet megfelelni.
- Az országban a foglalkoztatottak közel egyharmada a költségvetési szféra szervezeteinek alkalmazásában áll. Megélhetésük, szakmai előmenetelük a jövőben egyre inkább intézményük eredményességétől, társadalmi megítélésétől, a gazdaságra gyakorolt hatásától függ. Az alkalmazottak teljes mértékű bevonása lehetővé teszi képességeik kihasználását a szervezet számára, egyben lehetőséget teremt a dolgozók önmegvalósításának kibontakoztatására.
- A rendőrség hatékony működését csak folyamatszemléletű megközelítéssel, a „vevői igények” felismerésével és kielégítésével, a vezetés és szabályozás áttekinthetővé tételével lehet elérni.
- A rendőri tevékenység változásokon megy keresztül, de a teljesítménymérés, a hatékonyság, az eredményesség, a minőség értékelése és javítása területén lemaradás tapasztalható.

Ezek az okok vezettek ahhoz, hogy a rendőrségen is megindult a minőségfejlesztés. 1999-2001. között a Miskolci Egyetem irányításával 6 északkelet-magyarországi megye rendőri vezetői PHARE támogatással egy EU konform programot indítottak, melynek folytatásaként 4 megyében indult meg először az egységes szemléletű rendőrségi minőségfejlesztési program. Az e program keretében javasolt modell a teljes közszolgálat, és köztük a rendvédelmi szolgálatok egészére is értelmezhető, összhangban áll az eddigi eredményekkel, és megteremti a kapcsolatot az egyéni és szervezeti teljesítményértékelés és fejlesztés több éve folyó kísérleti próbálkozása és a minőségirányítás között.

A Rendőrségi Kiválósági Modell (RKM) a minőség társadalmazításának európai alapmodelljéből, az EFQM (European Foundation for Quality Management) modellből alakult ki, amely a minőség fejlesztését a társadalom biz-

tonsági igényéből vezeti le és a partneri együttműködésre helyezi a fő hangsúlyt a lakossággal, valamint a rendőrség tagjaival.

A modell kidolgozása közben sikeres minta-értékelések zajlottak (1999-től), és több konkrét önértékelés megvalósítása tökéletesítette egészen mostanáig a modell tartalmát. Ezek bebizonyították, hogy a BM különböző szervei különböző minőségirányítási rendszereket tartanak követendőnek.

Méréselméleti alapok

2.1. Természettudományi megalapozás

Az emberiség korai történelmétől fogva a természeti jelenségek értékelésénél szembe találkozott a mérés problémájával. Ez először a különböző, többnyire fizikai mennyiségek esetében merült fel (hosszúság, tömeg, súly, idő, sebesség stb.). Maga a mérés tulajdonképpen egy etalonnal való összehasonlítást jelent. A mérés pontosságát tehát két dolog befolyásolja, magának az etalonnak a pontossága, valamint az összehasonlításnak, mint folyamatnak a pontossága.

A tudomány előrehaladása során mindkét pontossági elem fejlődött és így alakult ki napjainkra a természettudományok terén az SI mértékegység rendszer, amelyben a mai fizikai ismeretek összes mérőszáma 4 alapegységből származtatható {méter (m); kilogramm (kg); másodperc (s); és áramerősség (A)}.

A fizikai összefüggések elemzésekor olyan technikák is kialakultak, amikor a végeredményként dimenzió nélküli mennyiség („csupán” viszonyszám) adódik. (Ezzel tulajdonképpen önálló tudományterület, a dimenzióanalízis foglalkozik.)

Egyes fizikai mennyiségeknél még ennek a lényegében dimenzió nélküli viszonyszámnak is „dimenzió”-szerű elnevezést adnak, például, amikor azt mondjuk, hogy egy repülőgép sebessége 2 „mach”, akkor ezzel azt fejezzük ki, hogy a hangsebességnél kétszer gyorsabban repül.

2.2. A kriminológiai jelenségek mérése

A kriminológiai jelenségek mérésénél szinte kizárólag ilyen dimenzió nélküli viszonyszámok használatosak, azaz az események mértékét a legtöbb esetben azonos, vagy hasonló (illetve hasonlóknak vélt) elemmel vetjük össze. Éppen ebből fakad a „mérés” nehézsége, hiszen a majdnem azonos jelenség nem jelenti ugyanazt a jelenséget, ami óhatatlanul bizonyos torzításokat eredményez. (Természetesen ez a torzítás, amennyiben tisztában vagyunk vele, akár elfogadható is lehet, illetve figyelembe vehető és az eredményeknél korrigálható is.)

A természettudományok vizsgálódási körébe tartozó jelenségeknél a legtöbb esetben a törvényszerűségek egzakt módon, közvetlen ok – okozati összefüggések megjelenésével érvényesülnek. A társadalomtudományi kérdéseknél azonban a törvényszerűségek többnyire csupán tendenciaszerűen, statisztikai

úton kimutatható módon fejeződnek ki. Ennek megfelelően a jelenségek vizsgálata, mérése is speciális módszereket igényel.

A kriminológiai jelenségek mérésénél ezért mind az „etalon”, mind az összehasonlítási lehetőség nehézségbe ütközik. Az etalon kérdését az írott és íratlan normák rendszere viszonylag jól megoldja. Azonban a természettudományok terén alkalmazott egzakt és jól megfogalmazható definíciókkal szemben egy egyszerű jogi norma is bonyolult relációkat határoz meg annak érdekében, hogy a gyakorlati életben előforduló számtalan körülmény esetében is kellő módon alkalmazható legyen.

Az olyan jelenségek esetén – mint pl. a bűnözés mértéke, vagy az ügyfélkihasználás a közigazgatásban – a viszonyítási alap kiválasztása nem köthető valamilyen emberi cselekedetnek vagy észlelésnek, érzékelésnek *kívüli*, független és stabil állandó mértékhez. Ebből adódóan az eredmény óhatatlanul szubjektív lesz. Az összehasonlítási folyamat során ezután szinte fel sem tűnik az ember által végzett értékelés objektivitást torzító hatása. Ezekre a felvetésekre a jelenlegi rendszerek elemzése után kísérelünk meg jövőbeni kitérési pontokat és irányokat felvázolni.

2.3. A rendőrség tevékenységét meghatározó események mérése

A rendőrségi tevékenység döntő mértékben reaktív módon reagál valamilyen társadalmi eseményre. Ezen események mérésére rendszerint a különféle rendőrségi statisztikák szolgálnak.

A magyarországi kriminológiai vizsgálatok kezdete egy statisztikus nevéhez, Földes Bélához kötődik. Ő volt az, aki először elemezte statisztikai tények alapján a magyarországi bűnözési helyzetet. 1889-ben jelent meg „A bűnügy statisztikája” című munkája.

Napjainkra a statisztikáknak és az ezekhez kapcsolódó tanulmányoknak a száma jelentősen megnőtt. A kriminálstatisztika a társadalomstatisztikai rendszer része, jelenleg három, egymástól jól elkülöníthető részre tagolódik:

- az egységes rendőrségi-ügyészségi rendszer (ERÜBS)
- a bírósági statisztikai rendszer
- a büntetés-végrehajtási statisztika.

Az egységes rendőrségi-ügyészségi statisztikai rendszer 1963-ban a belügyminiszter és a legfőbb ügyész közös utasítására jött létre. 1964. január 1-től működik, azóta folyamatosan alakították, korszerűsítették. Alapvetően két részre osztható: egyik része a bűnözéssel, mint jelenséggel, a másik része a rendőri-ügyészi tevékenységgel, mint jogalkalmazó munkával, ennek hatékonyságával foglalkozik.

A bűnözésre vonatkozó részben regisztrálják egyrészt a bűncselekményeket, másrészt a bűncselekmények elkövetőit, külön-külön lapokon. A bűncselekmény regisztrálásánál feltüntetik annak valamennyi fontos kriminológiai,

kriminalisztikai jellemzőjét. A bűnözés személyi oldalán az elkövetőre jellemző adatokat rögzítik, lehetőséget biztosítva ezzel a bűnösségi körülmények feltüntetésével a társadalmi-gazdasági jellemzők vizsgálatára is.

A rendőrségi szakasz a nyomozás elrendelésétől a nyomozás befejezéséig, míg az ügyészségi szakasz a rendőrségtől vádemelési javaslattal történő érkezéstől az ügyészségi szakasz befejezéséig (vádemelés, eljárás megszüntetése) terjed. Rendőrségi használatnál ezek az ERÜBS adatok számítanak „etalonnak”. Megyéenként, illetve eljáró rendőri szervenként találhatók az adatok a már jelzett csoportosításokban.

Egészen részletes elemzésre adnak lehetőséget például a befejezett ügyek száma (a rendőri nyomozásokban), az ismertté vált bűncselekmények (az elkövető helye szerint), a 100.000 lakosra jutó bűncselekmények, az ismertté vált bűnelkövetők (a lakóhely szerint), a 100.000 lakosra jutó bűnelkövetők, a külföldi bűnelkövetők (az eljáró szervek szerint), stb. statisztikái.

A bírósági ill. a büntetés-végrehajtási statisztikák kevésbé használatosak a rendőri tevékenység mérésénél. A bírósági statisztika rendszere több mint száz éves múltra tekint vissza. Két részre osztható, az egyik rész a bírósági ügyforgalom és munkateher alakulását jelző adatokat tartalmazza, a másik a jogerősen befejezett büntetőügyek vádlottainak adatain alapul. Ez a statisztika tartalmazza azoknak a büntetőügyeknek, illetve azon eljárásban szereplő vádlottnak az adatait is, amelyeknek rendőrségi-ügyészségi előzménye nincs.

A büntetés-végrehajtási statisztika a büntetés-végrehajtási intézetben fogva tartottak számáról, megoszlásáról, bűncselekményeinek kategorizálásáról, a büntetés-végrehajtási fokozatról, a büntetés tartamáról és a befogadások, illetőleg szabadítások számáról ad képet.

A bűnügyi statisztikák szükségképpen kétarcúak. Egyrészt bemutatják az ismertté vált bűnözést, másrészt következtethetünk belőle az azt készítő szerv leterheltségére, hatékonyságára, áteresztő képességére. A statisztikai adatok számtalan kedvelt hivatkozási, viszonyítási és illusztrálási lehetőséget kínálnak, de egyúttal korlátokat is hordoznak magukban. A felhasználóknak ezért mindig tekintetbe kell venni a valóságtükrözési fokukat is, melyek időnként erősen relativizálják használhatóságukat.

Természetesen számos más mérési módszer is lehetséges, melyekkel ritkábban élnek a kutatók. Ilyen például a megkérdezés módszere, amely lehet lakossági, illetve szakértői megkérdezés. Megfigyeléssel, kísérlettel szintén mérhetünk rendőri tevékenységet és ezeknek szintén több válfajuk ismert.

Fontos az is, egyáltalán hogyan, milyen módon kívánják hasznosítani a felhasználók ezeket a méréseket? Ilyenek lehetnek:

- prognózisok gyártása,
- stratégiai feladatok megfogalmazása,
- bűnözési térkép összeállítása, stb.

A módszerek megválasztásánál ezért igen fontos a felhasználás céljának kellő időben történő megfogalmazása.

Jelenlegi mérési rendszerek és főbb hiányosságaik

A jelenlegi skálák az események kapcsán azok pusztán mértékére igyekeznek választ adni. Fő módszerük, hogy a jelenséget számszerűsíteni kell, és ez által lehet azokat összemérni. Ezekre az (eddig) legjobb módszernek a különféle statisztikai összehasonlítások bizonyultak. Főbb torzítások legfőképpen abból származnak, hogy a társadalmi jelenségek, általában olyan bonyolultak, hogy minden aspektusuk nem ragadható meg egy vagy néhány adat számszerűsítésével. Ráadásul ezek a jelenségek (pl. megyék bűnözési helyzete) a térben és az időben rendkívül heterogén módon változnak.

Emiatt a jelenségeket valamilyen – rendszerint összetett – szempont alapján össze kell hasonlítani. A legegyszerűbb összehasonlítások akkor adódnak, amennyiben pusztán a térbeli megoszlás szerint, illetve az időben önmagunkhoz viszonyítunk.

3.1. Viszonyítás a térben

Ezen módszerek szerint az adott jelenséget azonos időben, illetve időszakban, de hasonló, vagy mellérendelt szervezetek között vizsgáljuk. Jó példa erre, amikor egy bizonyos időszakban, pl. a különféle közigazgatási egységek, megyék helyzetét vetjük össze (bűnügyi statisztika, közlekedési balesetek száma, ügyfélforgalom, stb.). Természetesen az adott vizsgálat pontosságát, illetve a torzításokat jelentősen befolyásolja, hogy egymással milyen relációban lévő alanyokat választunk ki. Szomszédos megyék vonatkozásában a bűncselekmények között nyilván több összefüggés fedezhető fel, mint az ország két vége közti esetben. Autópályás balesetek összevetésénél is lényeges, hogy melyik megye adatait vizsgáljuk, hiszen pl. Békés megyében – feltehetően még a jövőben is jó ideig – nem következik be autópályás közlekedési baleset. Az ilyen jellegű összevetések esetén mindig figyelemmel kell lenni a különböző befolyásoló körülményekre, a peremfeltételekre.

Ugyanakkor a térben való szemléletes összehasonlítás nagyon szemléletes, illetve jól „eladható”/ábrázolható eredményt szolgáltat. Számtalan publikációban találunk olyan ábrákat, amelyek valamilyen térképen jelölik az eltérő területekhez tartozó különféle adatokat. Ezek a – többnyire színes – ábrázolások valóban áttekinthetően és jól kiértékelhető formában mutatják az információt. A kiértékelésnél azonban nagyon körültekintően kell eljárni, mert az eltérések valódi okainak feltárása nélkül az eredmény tévútra vezethet. Önmagában egy rosszabb statisztikai mutatóval rendelkező szervezet nem feltétlenül végez alacsonyabb színvonalú, vagy rosszabb hatásfokú tevékenységet.

3.2. Viszonyítás az idő dimenzió mentén

Az összehasonlítás másik igen elterjedt és (talán) reális(abb) képet nyújtó módja, amennyiben az adott szervezet múltbeli és jelenidejű helyzetét elemez-

zük és hasonlítjuk össze. Ekkor általában jól kimutatható a szervezet működésének változása, a korábbi tevékenységek végrehajtásának módosulása. Az összevetés eredményeképpen adódó eltérésekből lehet ezután levonni a következtetéseket és tervezni a jövőbeni cselekvési programokat, irányokat.

Amennyiben az idősíkon való összehasonlítást több alkalommal rendszeresen elvégezzük, akkor ez a tevékenység az adott szervezet jobb működésére is ösztönzően hat. Az ismétlődő „mérések” eredményes visszacsatolást jelenthetnek a szervezetnél bevezetett változtatások következményeit illetően.

A következtetések levonásakor azonban igen részletes elemzéssel kell feltárni a változások valódi okait. A feltételezett okok hatásmechanizmusát is célszerű feltárni, tekintettel arra, hogy előfordulhat olyan eset, amikor a feladat megoldására javasolt, illetve bevezetett módszer az eredeti jelenséget ugyan megoldotta, azonban újabb – esetleg súlyosabb – problémát okoz.

Az adott szervezet korábbi önmagával való összevetése általában azért is jó módszer, mivel alkalmazkodik az alany speciális működési körülményeihez, adottságaihoz. Az összehasonlítás rendszerint jobban ösztönöz, amennyiben nem valamilyen elméleti ideális helyzethez képest viszonyítunk és ezáltal a jövőben kitűzésre váró célok is teljesíthetővé válnak.

3.3. A látencia hatásai

A kriminológiai jelenségek egyik legsajátosabb velejárója és lényegéből fakadó tulajdonsága a látencia. Ennek mértékét csupán becsülni lehet, ami a jelenségek vizsgálatát jelenősen torzítja. Ebben az esetben igen széles határok között változhat a valóság és a „mért” jelenség eltérése, vagyis a hibahatár is igen nagy mértékben jelentkezik. Ráadásul ezt a hibahatárt is csak becsülni lehet.

A látencia mérésére a feladat bonyolultsága okán ebben a dolgozatban nem vállalkozunk. A jelenség említése is csupán a mérhetőségi problémával való kapcsolata miatt történt.

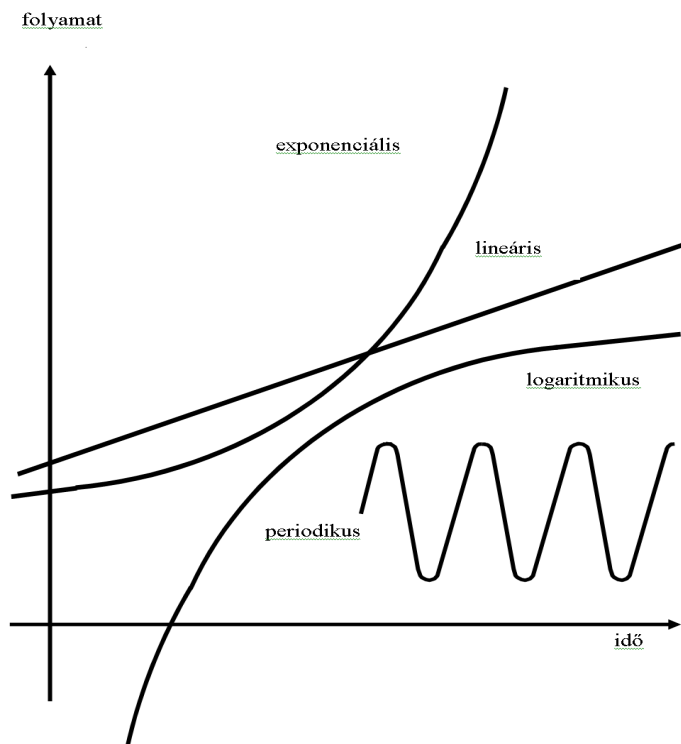
Mérési technikák a belügyi munka minőségfejlesztése szemszögéből

A természettudományi jelenségek mérése esetén alaptételt jelent, hogy a mérés, mint a megfigyelési folyamat egyik eleme ne okozzon beavatkozást magába a vizsgálni kívánt folyamatba. E követelmény analóg módon jelentkezik a kriminológiai jelenségek vizsgálata esetén is. (A látencia vizsgálatok során például a tettesi illetve áldozati megkérdezések, illetve a kísérleti megfigyelő módszerek, és ezek kombinációja éppen ennek az elvnek is megfelelően veszik figyelembe az eredményeket a kiértékelés során.)

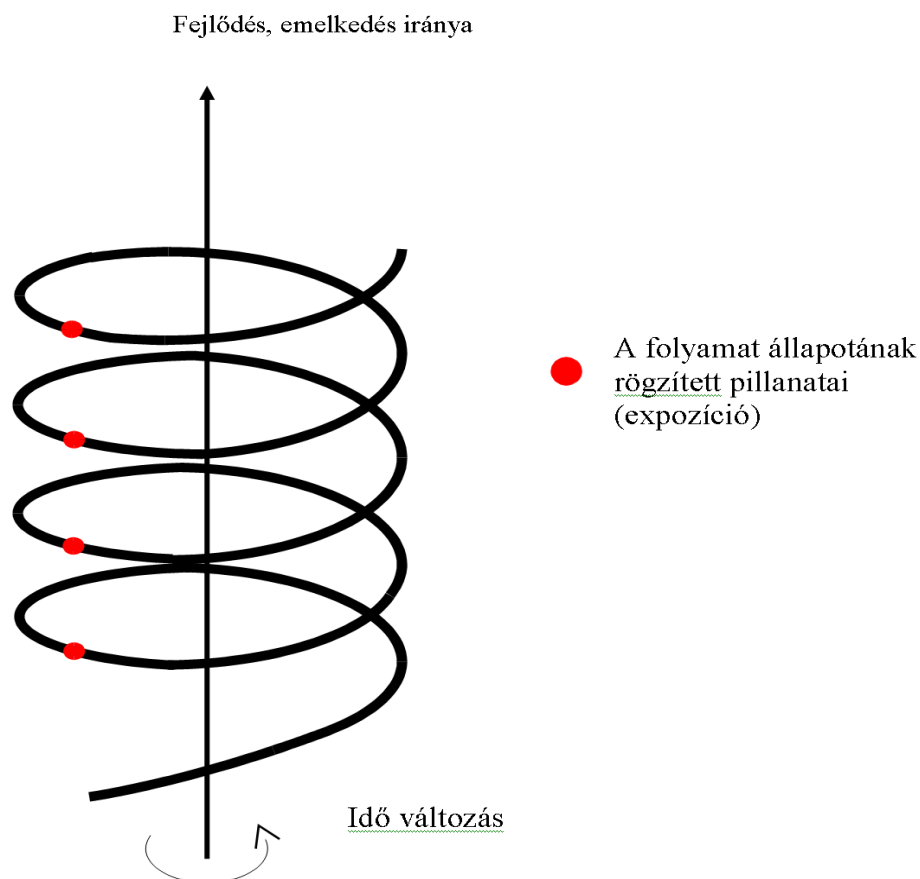
Ugyanilyen kiindulópontot jelent, hogy a mérni kívánt folyamatot (valamilyen szinten) ismerni kell ahhoz, hogy megfelelő mérőeszközt lehessen készíteni. (Például a hőmérséklet mérésére szolgáló legáltalánosabb eszközök a folyadékok hőtágulásának ismeretében készülnek.)

A mérési technikák továbbfejlesztése érdekében a vizsgálni és mérni kívánt jelenségek minél jobb megismeréséből célszerű kiindulni és ezzel egyidejűleg a jelenségek minél részletesebb megismerését kell célul kitűzni. Ezt az önmagában való ellentmondást az időben való változások figyelembe vételével lehetséges feloldani oly módon, hogy az idő dimenziót nem csupán statikus módon, lineáris egyenesként vetítjük, hanem egy spirálszerű kiterjedésként. Ez a módszer szemléletesen ábrázolja a folyamatok önmagába való visszatérését, megismétlődését és ugyanakkor az emelkedő színvonalat, fejlődést is.

A folyamatok időbeni változásának statikus, illetve komplex ábrázolását vázolják az 1. és 2. számú ábrák.



1. számú ábra folyamatok statikus ábrázolása



2. számú ábra folyamatok komplex ábrázolása

(Az ábrák természetesen csupán néhány önkényesen kiragadott formát szemléltetnek. A valóságban számtalan ezektől eltérő lehetőség is adódik.)

Az ábrázolásoknak leginkább a mérések kiértékelésekor van jelentősége, amikor a mérési adatokat valamilyen grafikonra illesztjük és ezzel szemléltetjük azokat. Ezekben az esetekben gondot kell fordítani arra, hogy kellő módon, szemel jól láthatóan kiderüljenek a folyamatokban rejlő statisztikai változások fő irányai.

4.1. Kérdőíves felmérések

A kriminológiai jelenségek értékelésének egyik legáltalánosabban elterjedt módszerének az – akár interjúval együtt végzett – kérdőíves felmérés számít. Természetesen ez a módszer nem automatikusan és önmagától hatékony, hanem csupán megfelelő és sok munkával végzett előkészítő tevékenység után.

Ennek során úgy célszerű összeállítani a kérdések tematikáját, amely számol a lehetséges, akár ellentétes válaszokkal is. A megfelelően összeállított kérdőívet ezután – a vizsgálni kívánt jelenséggel összhangban – a társadalmi környezet egy részében kell kitölteni (illetve kitöltetni). A kérdőívek kitöltése történhet a vizsgált terület valamennyi résztvevőjének körében, illetve valamilyen kiválasztott minta alapján.

A teljes halmaz vizsgálata általában nem lehetséges, csak speciális esetekben, amikor a teljes megkérdezni, illetve vizsgálni kívánt személyek számát technikailag is lehetséges kezelni. (Pl.: adott megyéhez tartozó összes önkormányzat megkeresése még elméletileg kezelhetőnek tűnik, de az egész ország esetében a több mint 3000 szervezeti egység esetében ez már általában kivitelezhetetlen.)

A mintavételezési technikák alkalmazása általánosan elfogadott módszernek számít, amennyiben jó eséllyel feltételezhető, hogy a minta összetétele (jó közelítéssel) megegyezik a teljes vizsgált területtel. Ekkor a minta kiválasztása során figyelemmel kell lenni annak reprezentatív jellegének biztosítására.

A mintavételezéssel, a minta kiválasztásával a matematikai statisztika tudománya foglalkozik, azonban a különféle események eloszlásának meghatározásakor kevésbé veszi számba a társadalmi jelenségekre vonatkozó mintavételi becsléseket. Mivel ezen jelenségek, különösen a kriminológiai események ok-okozati összefüggései sokkal bonyolultabbak, ezért a sok esetben jól használható és matematikailag kezelhető (például geometriai) eloszlások nem alkalmazhatók automatikusan. Például a megyék bűnözési statisztikáinak elemzésénél – a térképes szemlélet alapján – szinte önmagától adódik egy olyan feltételezés, amely szerint a terület nagysága egyértelműen és *kizárólagosan* meghatároz bizonyos eseményeket, azaz a megyékben bekövetkezett bűncselekmények száma (illetve azok előfordulási valószínűsége) egyenesen arányos a megyék területének nagyságával. Ez az állítás természetesen a valóságban nem állja meg a helyét.

Tekintettel arra, hogy a matematikai statisztika idáig döntő többségben a természeti jelenségek vizsgálatából, illetve a gazdaság anyagi folyamatainak elemeiből, a termelésből merítette a kutatási adatokat, a felállított és bizonyított tételei is többnyire ezekre vonatkoznak. A társadalmi jelenségek esetében a teljes halmaz és a minta megfelelésének vizsgálata és összevetése, azok megfelelően kezelhető matematikai statisztikai leírása még nem kellő mélységben kidolgozott.

4.2. Komplex kiértékelés

A kérdőív összeállításakor, illetve a felmérés lebonyolításakor figyelemmel kell lenni a kiértékelés komplex jellegére.

4.2.1. Szempontokra bontás

Első lépésben a jelenséget a vizsgálat szemszögéből külön-külön kiértékelésre váró szempontokra bontjuk. A kérdésfeltevés ekkor a következő módon alakul:

Értékelje az **A** jelenséget az **s1** szempont alapján.

Értékelje az **A** jelenséget az **s2** szempont alapján. Stb.

Konkrét kérdéssel szemlélítve például:

Értékelje az okmányiroda működését

- a várakozással eltöltött idő alapján;
- az ügyintéző szakszerű munkavégzése alapján;
- az ügyintéző udvarias, ügyfélbarát viselkedése alapján;
- az egyes okmánytípusok kiállítása alapján;
- stb.

A szempontok összeállításánál a jelenséget részleteiben elemezni szükséges és ezek alapján meg kell ragadni (lehetőleg) a folyamatot befolyásoló valamennyi lényeges momentumot. Ezek összessége adja meg a teljes szempont halmazt.

4.2.2. Súlyozás

A szempontok összeállítása után célszerű átgondolni azok fontosságát, valamint esetlegesen az egymásra épülésük hierarchiáját.

A fontosabb szempontokhoz nagyobb, a kevésbé fontosakhoz kisebb súlytényezőt célszerű hozzárendelni. Ezen tényezők kellő megválasztásával alakul ki az egész értékelési rendszer lényege, ugyanis a szempontokhoz eltérő fontosságot választva végeredményül más és más eredményt kapunk. Az előző – okmányirodai – példát továbbgondolva a hivatal szemszögéből valószínűleg a másodikként felsorolt **szakszerűség** szempontja a legfontosabb, azonban adott esetben az ügyfelek lehet, hogy a **várakozást**, mint figyelembe venni kívánt tényezőt fontosabbnak ítélik.

A súlyozásnál nem csupán rangsort kell felállítani, hanem azt is rögzíteni kell, hogy az adott szempont milyen mértékben fontosabb a másiknál. Az egyik módszer szerint a legkevésbé fontos szemponthoz célszerű egyszeres tényezőt rendelni és ehhez viszonyítva lehet a többiekhez különféle szorzókat meghatározni. Lehetséges több szemponthoz is azonos súlyozást megállapítani, azonban az lényeges, hogy a számértékeket még az előkészítés időszakában rögzítsük és a későbbiekben csupán kisebb mértékben módosítsuk. (A módosítás sokszor elkerülhetetlen, hiszen a folyamat során a bővülő ismeretek alapján esetleg újabb szempont, vagy aspektus merülhet fel. A lényeg, hogy a felállított rendszer konzekvens és egyben kellően rugalmas legyen.)

Másik módszer szerint a súlytényezőket úgy is meg lehet választani, hogy az összegük egységnyi legyen. Ebben az esetben is a kívánt arányokat kell kialakítani, azonban ekkor a konkrét értékelés után – a következő pontban ismertetett százalékos skála alkalmazása esetén – a kapott végeredmény valamilyen százalékos formát mutat, ami sok esetben szemléletes lehet.

A súlytényezőket a továbbiakban ξ_i – vel jelöljük.

4.2.3. Értékelés az egyes szempontok szerint

Az egyes szempontok szerinti értékelést többféle skála alkalmazásával hajthatjuk végre. Ezek általában egymással egyenértékűnek tekinthetők, de mégis adott szempontok esetén, ahhoz illeszkedő módon kell közülük választani. A skálákat általában az értékelési sávok finomsága szerint különböztetjük meg.

- Bináris (kétlépcsős) skála: az adott értékelési szempontot csupán a *teljesül* – *nem teljesül*, *megfelel* – *nem felel meg*, *igen* – *nem*, stb. válasz-párokkal fedjük le. Jól alkalmazható általában kizáró rész-szempontok értékelésénél, ahol a feltétel meglétét, vagy hiányát elegendő megállapítani, annak teljesülési mértéke nem fontos. Ez a skála a 0 – 1 szám-párokkal jól kifejezhető, ráadásul az összegzés során a szorzási művelettel igen szemléletes eredményt szolgáltat.
- Többlépcsős skálák: az értékelés finomítása érdekében további lépcsőfokot (fokokat) vezetünk be. Ezek legáltalánosabb megjelenését láthatjuk az iskolában is alkalmazott osztályozás során.
3 lépcső esetén szokásos alkalmazást jelent például a *kiváló* – *megfelelt* – *nem felelt meg* értékelési skála.

5 lépcső használatára a legismertebb, hétköznapi iskolai osztályozás szolgál (*kitűnő – jó – közepes – elégséges – elégtelen*).

További finomabb – 7 vagy 10 fokozatú – skálák is alkalmazhatóak, amelyre vonatkozóan felső határt lényegében csupán a józan ész szab. Ilyen magasabb lépcsőszámot alkalmaznak sok esetben a rendezvények szervezői, amikor a résztvevőket kéri fel az adott rendezvény értékelésére. A viszonylag sok lépcsőfok esetén az értékelést végző személy úgy érzi, hogy igen jó szabadsági fokkal nyilváníthat véleményt.

- Százalékos skála: lényegében a többlépcsős skála speciális esetét jelenti, hiszen itt a finomításra 100 lépcsőfok is adott. Amennyiben a százalékos skálát a 0-tól 100-ig terjedő tartományban értelmezzük, akkor bizonyos szempontból a bináris skála kizáró (*nem teljesült*) funkcióját is beépítettük a 0-s számérték alkalmazásával. Ebben az esetben ugyanis, ha valamilyen szempontra a zérus értéket adjuk, akkor az azt fejezi ki, hogy az adott szempont kategorikusan nem teljesült.

4.2.4. Összegzés a különféle szempontok tekintetében

A súlytényezők meghatározása és az értékelés végrehajtása után egyszerű, formalizált matematikai eljárással kell elvégezni az összegzést.

Első lépésként az egyes szempontokra adott értékelő válaszokat számszerű (numerikus) formára alakítjuk az alkalmazott skálák értékének megfelelően. Értelemszerűen a százalékos skála már önmagában számértéket szolgáltat. Ezeket a számértékeket jelöljük e_i – vel.

Második lépésben az adott értékelési számot össze kell szorozni a megfelelő súlytényezővel, amely így már súlyozott értékelési számot, mint részeredményt ad.

$$\Psi_i = \xi_i * e_i$$

Harmadik lépésben a végeredményt a súlyozott részeredmények összege adja.

$$\Psi = \sum \xi_i * e_i$$

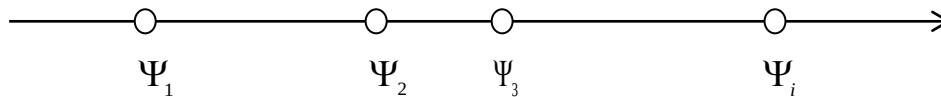
A százalékos skála és az összességében egységnyre normált súlytényezők alkalmazása esetén a végeredményt szintén százalékos skálán kapjuk, ami adott esetben jól szemléltethető.

4.2.5. Ábrázolás

Végezetül célszerű az eredményeket valamilyen módon ábrázolni.

Lineáris ábrázolás

A legegyszerűbb esetben az eredményül kapott számokat csupán egymás mellé helyezve növekvő vagy csökkenő sorrendben, lényegében egy szám-egyenesen ábrázoljuk. Ezt a módszert akkor indokolt alkalmazni, amikor egy összesített mérőszámmal kívánjuk jellemezni az összehasonlított jelenségeket. Egy mintaábrázolást mutat a 3. számú ábra.



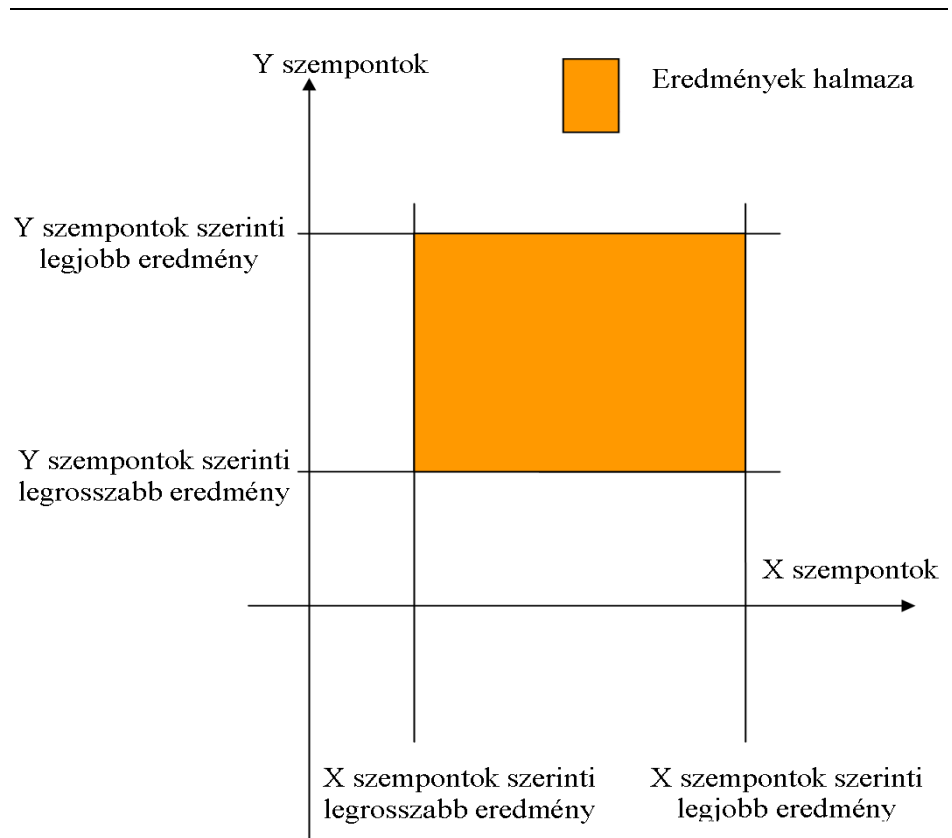
3. számú ábra az eredmények egydimenziós ábrázolása

Síkbeli (térbeli) ábrázolás

A valóságban azonban a legtöbb esetben érdemes a szempont halmazt megosztani. Amennyiben a szempontok valamilyen rendező elv szerint 2 részre csoportosíthatóak, akkor igen szemléletes ábrázolásra nyílik lehetőség a kétdimenziós síkban. Például a szempontokat be lehet sorolni

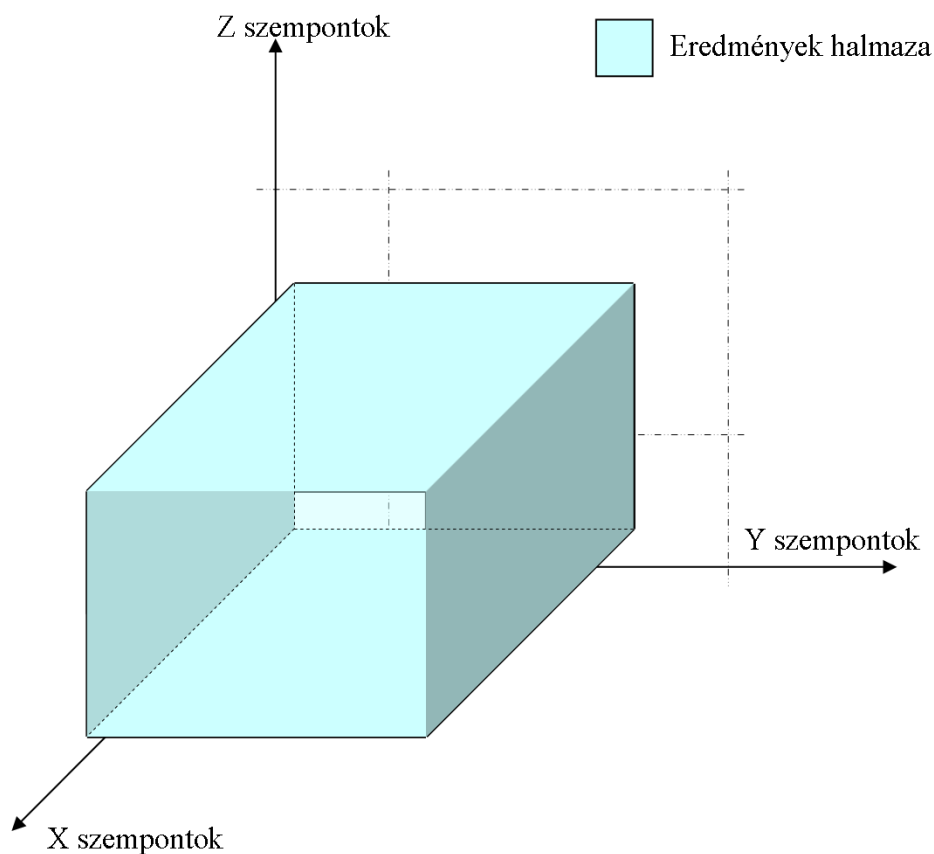
- szakszerűséget kifejező csoportba, illetve
- gazdaságosságot kifejező csoportba.

(Természetesen ez a megosztás jelen esetben teljesen elméleti és önkényes.) Ekkor a kétféle szemponthalmaz összesített részeredményei a síkban egy téglalap alakú mezőben ábrázolhatók a 4. számú ábra szerint.



4. számú ábra az eredmények kétdimenziós ábrázolása

Az ábrázolás 3 dimenziós esetben analóg módon kiterjeszthető a térbe, azonban ez lényegesen nehézkesebb és nehezebben áttekinthető eredményt szolgáltat. (5. számú ábra)

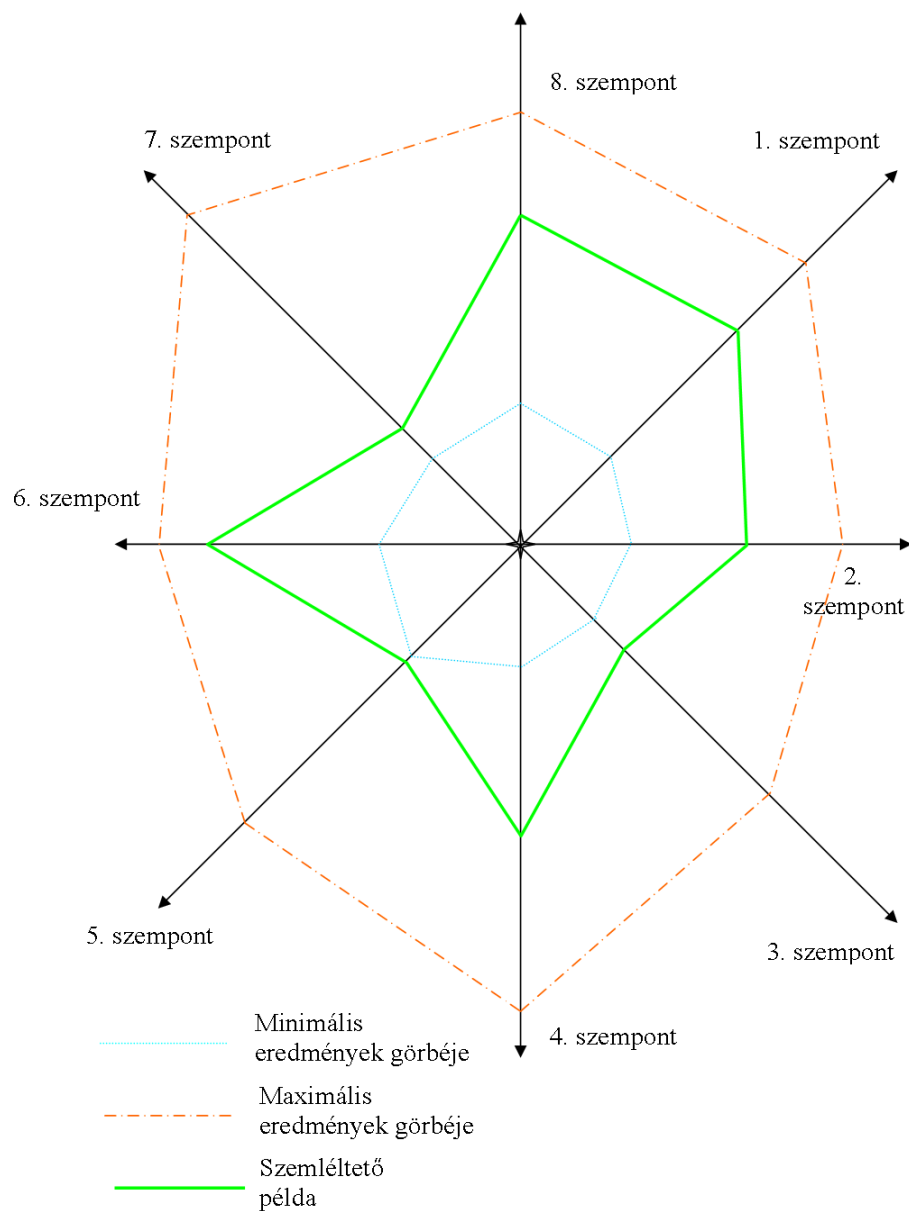


5. számú ábra az eredmények háromdimenziós ábrázolása

n dimenziós ábrázolás (csillagábra)

Amennyiben a szempontokat háromnál több csoportba indokolt besorolni, akkor az előzőekben vázolt ábrázolási módok már nem alkalmazhatóak. Ebben az esetben egy origóból kiindulva a szempont-csoportoknak megfelelő számú (n darab) félegyenest indítunk – lehetőleg szimmetrikusan $360/n$ fokra osztva az egymással bezárt szöget.

A következő lépésben a félegyeneseken ábrázoljuk az adott szemponthoz tartozó eredményt, amely így az origótól való távolságként értelmezhető. Az adott folyamathoz tartozó értékelési pontokat összekötve kapjuk annak értékelő sokszögét (érékelő csillagját). A csillagábrás szemléltetés akkor indokolt, ha az értékelési szempontok közel azonos súlyozásúak és ezért indokolt azokat egyenként szerepeltetni. Az n dimenziós ábrázolást a 6. számú ábra szemlélteti ($n=8$ esetére).



6. számú ábra az eredmények ábrázolása csillagábrán

A minimális és a maximális eredmények görbéje közötti terület adja az értékelési mezőt.

4.3. Rendőrségi mérési technikák

4.3.1. Külföldi gyakorlat

Joggal vetődhet fel a kérdés, hogy máshol hogyan, milyen módszerekkel végzik a rendőrségi munka minőségének mérését. Kitekintve a tőlünk valamivel előbbre tartó fejlett nyugat-európai országok gyakorlatára, megállapíthatjuk, hogy máshol sincs erre egységes recept. E fejezet kidolgozójának holland és német kollégákkal volt szerencséje ebben a témában konzultálni.

A hollandok kb. 5-6 éve nagy hangsúlyt fektetnek a rendőrségi minőségfejlesztésre. A tőlük mintaként kapott – dolgozói önértékelésre vonatkozó – kérdőív világos, egyértelmű kifejezésmódjával, lényegre törő kérdéseivel nagyon megnyerte tetszésünket. Kísérletképpen ki is próbáltuk az egyik nógrádi kapitányság dolgozói körében, s egy-két kérdéstől eltekintve a „tesztelők” is kielégítőnek tartották, olyan kérdőívnek, amit nem dob félre senki és nem automatikusan karikázzák a kitöltők, hogy minél előbb készen legyenek vele.

A hollandok úgy vélik, hogy a folyamatos értékelések miatt sok év után egyre nehezebb az érdeklődést szinten tartani. Az elején még lázba hozta a rendőröket, hogy hogyan értékelik őket, mit tudnak tenni ennek javítása érdekében, mára azonban nehéz ezt fenntartani.

A németországi rendőrségi minőségfejlesztés hasonló egy kicsit a magyar helyzethez. Több tartományban kísérleteztek TQM, CAF, Balanced Scorecard (BSC) programokkal, számos eredményt tudnak ennek kapcsán már felmutatni. Összefogott rendszer nincs, úgy vélik: mindenki tapossa ki a számára megfelelő utat.

4.3.2. Itthoni kezdeményezések

A magyar rendőrségen eddig is mértünk, voltak statisztikák, amelyek segítségével folyamatokat tudtunk elemezni, értékelni. Ezekről részletesen beszámolnak az irodalomjegyzékben hivatkozott publikációk. A minőségfejlesztést szolgáló mérésben az jelenti az újdonságot, hogy ezekben a modellekben például különböző alapelveket vizsgálunk a kérdőívek segítségével.

- *Ügyfélközpontúság.* Ez azt jelenti, hogy ismerni kell, mit várnak el tőlünk azok, akik majd igénybe veszik szolgáltatásainkat, ők a rendőrség „vevői”. (Függetlenül attól, hogy esetlegesen intézkedés alá vontak lesznek, vagy bármilyen más rendőrségi „szolgáltatást” vesznek figyelembe.)

-
- *Vezetés.* A vezetők kötelessége a célokról, főbb irányokról, a szervezet belső egységéről való gondoskodás.
 - *Az emberek bevonása a folyamatokba.* A szervezetet dolgozók, emberek alkotják és az ő bevonásuk elengedhetetlenül szükséges a minőség megvalósulásához.
 - *A folyamatok szerinti megközelítés.* Az erőforrásokat és a tevékenységeket a folyamatok részeként fogjuk fel, ezzel növelhetjük a hatékonyságot.
 - *Rendszerszemlélet.* Az egymással összefüggő folyamatokat rendszerként kezeljük, majd megtalálva az összefüggéseket, mindent a cél elérésének lehet alárendelni.
 - *Folyamatos tökéletesítés.* A bizalmat jelentősen növelheti, ha tudják rólunk azt, hogy a folyamatok tökéletesítésén fáradozunk és egyre jobb eredményekre törekszünk.
 - *Tényeken alapuló döntéshozatal.* Az egyre bővülő információk és ismereteink elemzése és értékelése alapján hozhatunk hatásos döntéseket.
 - *Kölcsönösen előnyös kapcsolat a segítőkkel, együttműködőkkel, beszállítókkal.* Ezáltal javul az értékteremtő képesség, mert mindenkinek érdeke lesz a jobb minőség.

A modell segítségével az adottságok oldaláról (vezetés, dolgozók, üzletpolitika és stratégia, partnerkapcsolatok és erőforrások, folyamatok), valamint az eredmények oldaláról (dolgozói eredmények, vevői eredmények, társadalmi eredmények, kulcsteljesítmény eredmények) közelítjük meg a tevékenység mérését.

4.3.3. Az első hazai rendőrségi sikerek

- Az ORFK Kutyavezető-képző Iskola (Dunakeszi) ISO 9000-es sorozatú minősítéssel rendelkezik, az első rendőrségi szerv volt, amely minőségfejlesztési tevékenységbe kezdett.
- Az ORFK Bűnügyi Szakértői és Kutatóintézetben számos speciális szakmai minőségbiztosítási rendszerhez csatlakoztak. Folyamatosan újabb és újabb területek kapcsolódnak be:

-
- ❖ 1992 – a véralkohol vizsgálatok nemzetközi minőségtanúsítása (DGKC)
 - ❖ 1995 – textil elemi szálak és a DNS minőségi kontrollja (ENFSI és GEDNAP)
 - ❖ 1996 – a DNA és az ENSZ kábítószer-laboratóriumi kontroll (DCP) kezdődött el.
 - ❖ Jelenleg az ujjnyomat, az írásminták és okmányok, valamint a fegyverszakértői vizsgálatok nemzetközi minőségbiztosítási rendszeréhez való kapcsolódás zajlik.
- A Fejér Megyei RFK 2001. áprilisától kezdte el az ISO 9001:2000 szabvány alkalmazását, tanúsítvánnyal rendelkezik.
- A Hajdú-Bihar Megyei RFK a Debreceni Egyetem TQM centerével közösen megkezdte a TQM vezetésfilozófia bevezetését. Ehhez kapcsolódva az EFQM modell felhasználásával önértékeléseket hajtottak végre. Csatlakozott hozzájuk a Borsod-Abaúj-Zemplén Megyei RFK, ahol szintén végrehajtották az önértékelést.

4.4. A további kutatások lehetséges irányai

Tekintettel arra, hogy a felvetett kérdéskör bonyolultsága meghaladja a jelen dolgozat kereteit, ebben a témában további lehetséges kutatási irányokat vetünk fel. Ezek közé adott esetben különböző tudományágakhoz, vagy területekhez tartozó gondolat is tartozik.

- Lehetségesnek tartunk a matematikai statisztika terén olyan elméleti vizsgálódásokat, amelyek igyekeznek kideríteni a különböző társadalmi folyamatok esetében alkalmazható mintavételi elveket és összehasonlítási eljárásokat. Ezzel arra a kérdésre igyekezünk választ találni, hogy milyen (mértékű, összetételű stb.) minta fedti le adott esetben például a bűnözés jelenségét, továbbá egy ilyen minta milyen pontossággal írja le a teljes halmazt. Véleményünk szerint például a látencia felderítését jelentősen elősegítené a kriminológiai jelenségek matematikai statisztikai elméleti megalapozása.
- Véleményünk szerint további erőfeszítéseket érdemes tenni abba az irányba, hogy egy – egy jelenségről alkotott társadalmi megítélés vizsgálatára milyen lehetséges felmérő ív(ek) alkalmas(ak). Ennek érdekében minta – kérdőívek összeállítását és gyakorlati ellenőrzését is indokoltnak véljük.

-
- További vizsgálatokat tartunk célszerűnek abban az irányban, hogy a dolgozatban bemutatott értékelési módszert milyen további területen lehetne hasznosítani – akár a Belügyminisztériumhoz tartozó egyéb szakterületeken is (Pl.: logisztikai feladatok esetén).

Összefoglalás

A dolgozatban bemutatottuk a belügyi szakterületen a minőségfejlesztés terén is alkalmazható mérési módszerek elvi alapjait. Rövid bevezető után indokoltuk a minőségfejlesztés belügyi területen való szükségességét, majd általános méréselméleti megalapozást tettünk.

Vázoltuk a jelenleg legáltalánosabban alkalmazott statisztikai módszereket és összehasonlításokat. Ezekben alapvetően kétféle, hozzávetőlegesen horizontálisnak, illetve vertikálisnak tekinthető módszer terjedt el, amelyek a térben, ill. az időben való összevetést jelentik.

A tanulmány fő részében ismertettük egy jól használható komplex eljárás lépéseit a szempontokra bontás, súlyozás, értékelés, összegzés és ábrázolás folyamataként. Ezeket a lépéseket – adott esetben – szemléltető ábrákkal kiegészítve tettük teljesebbé. Végezetül vázlatosan beszámoltunk a rendőrségnél elindult hazai gyakorlatról.

A dolgozat végén további – a témához kapcsolódó – lehetséges kutatási irányokat vázoltunk.

Irodalomjegyzék:

- | | |
|-------------------|--|
| Balogh Albert: | Az új ISO 9000-es és ISO 9004-es szabvány szemlélete
Minőség és Megbízhatóság, 2001/1. sz. 21-29. p. |
| Dudás Ferenc: | Közigazgatás-fejlesztési tendenciák a minőség és a teljesítmény tükrében (I. rész) Műveltség és Minőség
2002/5. Sz. 243-249. p. |
| Dudás Ferenc: | A közigazgatási minőségpolitika a kihívások tükrében
Minőség és Megbízhatóság 2003/3. 163-170. l. |
| Havellant Ferenc: | Rendőrségi minőségfejlesztés
Belügyi Szemle, 2002/8. sz. 32-56. p. |
| Ishikawa, Kaoru: | Introduktion to Quality Control
3A Co. Tokyo, 1994. |
| Ishikawa, Kaoru: | What is Total Quality Control?
The Japanese Way, Prentice-Hall Inc. 1985. |

-
- Juran, J. M. Ifj. Gryna, F. M.: A minőség tervezése és elemzése
Műszaki Kiadó, Bp. 1966.
- Kertész Imre: A rendőrség laboratóriumok integrált minőségirányítási rendszere
Belügyi Szemle, 2002/8. sz. 26-31. p.
- Kopasz Árpád: A magyar rendőrség minőségfejlesztési programja
Belügyi Szemle, 2002/3. sz. 3-25. p.
- Korinek László: A bűnözés visszatükröződése. Látens bűnözés, bűnözésábrázolás, félelem a bűnözéstől - Tanulmány
Kriminológiai ismeretek. Bűnözés. Bűnözéskontroll (Szerk.: Gönczöl Katalin – Korinek László – Lévai Miklós
Corvina 1999. 75-92. p.
- Mikó György: Az EFQM-modell és az ISO 9000-es szabványok a sikeres vezetésért. Minőség és Megbízhatóság 2003/3. 152-155. l.
- Szirtes Thomas: The High Art of Dimensional Analysis and Modelling
Toronto, Ontario, Canada M2H 1E7
- Varga Sándorné: A személyzet felkészítése a közszolgálat irányítására
Minőség és Megbízhatóság 2003/2. 94-96. l.
- Vavró István: A bűnözés mérésének módszerei; a magyarországi kriminalitás általános jellemzői – Tanulmány
Kriminológiai ismeretek. Bűnözés. Bűnözéskontroll (Szerk.: Gönczöl Katalin – Korinek László – Lévai Miklós
Corvina 1999. 53-74. p.
- Varga Lajos: Az EOQ harmonizált rendszere szerinti szakemberképes hazai tapasztalatai Minőség és Megbízhatóság 2003/2. 77-79.
- Vetier András: Szemléletes mérték és valószínűségelmélet
Nemzeti Tankönyvkiadó, 1995.
- Vincze István: Matematikai statisztika ipari alkalmazásokkal
Műszaki Könyvkiadó, 1975.

SECURISATION DE DONNEES TEMPS REEL DANS UN SYSTEME DE COMBAT SUR ATM

De plus en plus, les réseaux de télécommunication utilisent des architectures, des protocoles et des matériels issus du monde civil. Les réseaux militaires ont de par leur nature même des exigences propres en terme de survivabilité. Il est fondamental de prendre le maximum de précautions possibles en regard de la technologie utilisée: dans le cas d'ATM, à laquelle on s'intéresse ici, on utilisera de la fibre optique insensible aux perturbations électromagnétiques, on concevra une architecture comportant un grand nombre de noeuds et aussi maillée que possible, on utilisera les techniques de préconfiguration de VP/VC (Virtual Path, Virtual Channel) et, au niveau application, on dupliquera les serveurs qui seront physiquement éloignés (de manière à assurer un minimum de sécurité par redondance).

En plus des défaillances usuelles (panne d'équipement, coupure „accidentelle” de câbles) on doit ici se protéger contre des destruction multiples, simultanées, non „franches”, consécutives à des impacts directs d'armes (destruction instantanée d'un ou plusieurs noeuds, d'un ou plusieurs liens) ou induites par un milieu naturellement hostile (tangage/roulis, chocs, incendies, voie d'eau). Dans ces cas extrêmes et pour des applicatifs temps réel de type système de combat, les techniques classiques ne suffisent pas:

- toute retransmission d'information erronée ou perdue est inutile du fait de la durée de validité très courte des informations tactiques;
- toute solution basée sur le basculement d'un VP (Virtual Path) sur un autre et se traduisant par des pertes de cellules ou une détérioration de délai n'est pas assez satisfaisante.

Cela étant, on considère à l'heure actuelle, qu'un Poste de commandement est constitué d'une plate-forme et d'un système de combat (comprenant les senseurs, les aides au commandement et le système de direction de combat (SdC)¹⁵⁷.

De nombreux travaux visent à améliorer encore les performances intrinsèques d'ATM pour adapter cette techniques qui ne tolèrent ni pertes ni délais.

Pour répondre aux exigences des communications temps réel à l'intérieur du système de combat, on propose ici un mécanisme de protection sur deux chemins physiquement disjoints. On présente et décrit un algorithme possible pour la récupération des cellules issues des flux dupliqués. On étudie une

¹⁵⁷ P.PRAIDER:Architecture des systèmes de combat
(L'Armement N° 63, octobre 1998.)

implémentation de cet algorithme au niveau de la couche AAL (ATM Adaptation Layer) de sorte qu'aucun des deux flux ne soit à priori considéré comme nominal. La disparition d'un des flux ne nécessite ainsi aucune détection ni traitement particulier.

Le besoin de protection des communications critiques

Certaines communications à très fortes contraintes nécessitent de mettre en oeuvre des protections très fortes, parfois spécifiques. Ainsi, par exemple, existe-t-il des contraintes explicites pour les applicatifs type messagerie opérationnelle ou diffusion d'ordre:

- des spécifications opérationnelles imposent qu'un message d'urgence donnée („flash”, „immédiat”) ait été „traité” (par exemple visualisé sur une console dédiée au PC opération) en un temps donné à partir du moment où sa réception commence sur une antenne de réception du Poste de Commandement (en fonction du débit de la chaîne réception et de la longueur du message). Il est ici hors de question de perdre un seul caractère (message texte) ou que le réseau induise des pertes ou erreurs bit (sur des messages formatés utilisés par les systèmes informatiques) et ceci dans les „pires” cas.
- Des spécifications opérationnelles imposent également que des ordres vocaux („engagement”, „halte au feu”...) soient recus par les destinataires dans les pires cas de destruction ou de pannes. Ces ordres à la voix, en fonction de l'endroit d'où ils proviennent, peuvent par ailleurs être diffusés spécifiquement dans certaines zones et/ou couper une diffusion en cours de priorité moindre.

Des solutions partielles sont déjà implémentées pour certains systèmes de télécommunications actuels:

- duplication des liaisons inter-équipements de concentration;
- mécanismes de priorité entre les flux de données;
- multiplication des noeuds d'accès;
- duplication des équipements sensibles.

Une des tendances actuelles (en partie pour raisons de coût) est de fédérer sur un réseau unique des applicatifs ayant des contraintes fortes (messagerie opérationnelle (data) et diffusion d'ordres (voix)) et des applicatifs non opérationnels comme la phonie de distraction.

Les possibilités d'ATM

ATM est une technique intrinsèquement conçue pour le transport indistinct de la voix, de la vidéo et des données, avec la qualité de service (QoS) appropriée et toute la granularité requise (choix de débits de nx64 kbit/s au Gbit/s). Basée sur la communication de paquets, orientée connexion, cette technique a pris en compte les progrès effectués sur la technologie des

supports physiques et a repoussé le contrôle d'erreur aux couches hautes des protocoles. La commutation à l'intérieur du réseau ATM de cellules de petite taille (53 octets) est alors très rapide et cette technique est particulièrement bien adaptée au transport d'informations isochrones. De plus, et contrairement aux réseaux de type IP, ATM permet d'affecter une qualité de service appropriée à chaque type de trafic véhiculé en fonction des exigences propres de trafic¹⁵⁸.

Les communications entre ces équipements seront principalement de type point à multipoints bidirectionnelles. De nombreuses solutions exploitant les caractéristiques d'ATM ont été développées. Elles consistent en général à déterminer une stratégie visant à établir aussi vite que possible les Virtual Path et /ou Virtual Channel „détruits” par incident.

Cette stratégie peut être centralisée: de nouveaux Virtual Path sont établis au cas par cas par l'administration centrale qui a une vue complète du réseau et peut optimiser les ressources restantes lors de la reconfiguration. Pour autant, on ne peut considérer que des solutions programmées: tous les scénarios de destruction sont prévus et une solution adéquate déjà prête. Cette solution assez lourde est cependant moins pénalisante en temps qu'une reconstruction dynamique du réseau.

A l'opposé, on trouve de nombreux algorithmes à base de solutions prédéterminées décentralisées: pour chaque Virtual Path établi, on établit systématiquement un Virtual Path propre de secours. On peut également effectuer un pool de „x” Virtual Path „à la redondance de „y” Virtual Path ce qui permet d'économiser des ressources en bande passante mais n'assure plus une redondance complète. Les solutions exposées jusqu'ici ne sont pas satisfaisantes puisque, pour des sources haut débit, elles impliquent toutes des pertes de cellules durant la restauration: ces sources ne sont pas contrôlables nature (pas de contrôle de flux possible) et la bufferisation temporaire en un point du réseau est antinomique du contexte temps réel¹⁵⁹.

¹⁵⁸ voir: M.C.PONS, F.X. ARQUES: Réseau locaux embarqués:nouvelles architectures, nouveaux services (Revue Scientifique et Technique de la Défense, No 45, 1999-3.)

¹⁵⁹ voir: D: KOFMAN, M:GAGNAIRE: Réseaux haut débit (Dunod, 1999)

FAUT-IL CHANGER LA STRATEGIE DE LA COMMUNICATION?

Le monde des systèmes d'information et de communication est en total bouleversement. D'une part, sous la pression du monde civil très innovant, et d'autre part, sous la contrainte des opérations extérieures à caractère multinational durant lesquelles le SIC¹⁶⁰ est confronté et comparé aux SIC OTAN surtout américains. La barrière entre système civil et système militaire est en voie de disparition, au profit de notions telles que dualité, interopérabilité, banalisation ou spécificité limitée.

Toutes les évolutions technologiques que l'on constate dans le monde civil sont ou seront transposées dans les SIC militaires. Ces innovations modifieront le fonctionnement des états-majors, ainsi que la structure des SIC opérationnels. Néanmoins, la spécificité du métier militaire engendra toujours une organisation spécifique, à la fois freinant les évolutions mais aussi garantissant la cohérence et l'efficacité de l'action militaire.

Il est très difficile de dresser une liste exhaustive des nouvelles technologies introduites dans les SIC opérationnels. C'est donné plus en éclairage dans quelques domaines proposés, avant d'essayer de tirer quelques enseignements de ces évolutions dans le domaine de l'organisation et du fonctionnement.

Le premier aspect que nous mettrons en valeur est relatif à l'interconnexion des réseaux.

Nous n'en sommes aujourd'hui qu'au début du processus, mais l'application des savoir-faire des grands opérateurs, l'utilisation de l'ATM et des technologies issues du monde Internet sont en train de faire passer d'une logique de réseau dédié et séparé à une logique de réseaux interconnectés multiservices.

Ce mouvement a commencé par l'établissement du réseau de transport interarmées, fédérant les réseaux des armées, et se poursuivra par la mise en place d'un Intranet Défense permettant aux abonnés de la Défense d'échanger

¹⁶⁰ Système d'information et de commandement

tout type d'informations classifiées ou non, et dans un cadre formel ou informel.

La similitude avec les réseaux civils est évidente, c'est pourquoi il est possible d'envisager de confier à un opérateur civil la responsabilité de mettre en oeuvre tout ou partie des réseaux fixes des armées. C'est ce que l'on appelle « l'externalisation ».

Cependant, le processus d'interconnexion des réseaux s'avère très délicat à mettre en oeuvre, notamment avec les Alliés de l'OTAN où les problèmes de sécurité rendent toute interconnexion très difficile, dès que l'on s'écarte de la téléphonie classique.

Au niveau des déploiements extérieurs, on a appris cela des retours d'expériences des déploiements en Bosnie, on constate que l'on passe systématiquement après la mise en place initiale d'une architecture SIC, militaire à près de 100%, à une architecture majoritairement à base de systèmes civils. Ainsi, après le mouvement de transfert, le noyau dur militaire minimal est complété par des moyens civils loués ou achetés, et calibrés pour acheminer les hauts débits.

Il faut donc concevoir dès l'origine cette relève des systèmes qui doivent fournir les mêmes services aux utilisateurs. Système militaire ou système civil, il devient donc, aujourd'hui, très difficile de faire la différence.

Quant aux utilisateurs, ils entendent disposer en opérations extérieures des mêmes services qu'au bureau ou bien qu'à leur domicile.

Mais c'est au niveau des systèmes d'information opérationnels que l'on assiste aux changements les plus importants.

En effet, les systèmes développés sont de plus en plus communicants. Ils permettent un vrai travail coopératif par l'utilisation de la visio-conférence, des forums, de l'e-mail, du tableau blanc ou du travail sur document partagé.

Par ailleurs, ils sont de plus en plus ouverts, en permettant l'accès à des bases de données localisées ou distantes, notamment par le biais de guichets d'information.

Le deuxième aspect que nous mettrons en valeur a trait au système de commandement.

En effet, on assiste à la prise de conscience de la nécessité de développer de réels systèmes d'aide au commandement intégrant des outils d'aide à la décision, qu'il s'agisse d'un système d'élaboration de la vision globale opérationnelle ou bien des outils utilisant les capacités de simulation.

Ce domaine de la simulation est en pleine mutation. La politique de simulation interarmées traduit la ferme volonté d'accorder à cette discipline une importance toute particulière, tant cet outil offre des perspectives de meilleure efficacité et de créativité accrue. Point n'est besoin d'insister sur la réelle plus-value que l'ensemble de la communauté militaire attend de la simulation en ce qui concerne la planification, la conduite d'opérations, les études et les évolutions de doctrine, sans oublier bien évidemment, l'entraînement à moindre coût des PC¹⁶¹ interarmées ou de composante.

Les conséquences de l'arrivée des nouvelles technologies sont multiples. Néanmoins, et cela peut paraître paradoxal, l'organisation du commandement est encore peu touchée par les évolutions en cours. Le respect du principe hiérarchique, où chaque niveau de commandement synthétise et "valide" les informations transmises au niveau supérieur, et les principes de confidentialité et de besoin d'en connaître limitent les possibilités de changements profonds de l'organisation du commandement. Dans ce domaine, les positions sont en opposition avec les conceptions américaines prônées dans la doctrine *Joint Vision 2010*.

Par contre, dans le fonctionnement des états-majors, à tous les niveaux, de même qu'au niveau des forces elles-mêmes, les évolutions sont réelles. On constate ainsi:

- une circulation accélérée de l'information entre les différents acteurs.
La numérisation croissante des informations associée aux capacités des réseaux permet un accès de plus en plus important au temps réfléchi voire au temps réel;
- un accès élargi à l'information, favorisant notamment la compréhension des situations et les prises de décisions.
L'information n'est plus cloisonnée;
- une augmentation du nombre des échanges dans des modes beaucoup plus souples, notamment grâce à l'e-mail;
- des modes de travail nouveaux, par la création de groupes d'intérêt virtuels permettant de travailler ponctuellement sur des problèmes

¹⁶¹ Poste de commandement

-
- communs, à partir de structures dispersées géographiquement;
 - un décloisonnement des niveaux hiérarchiques. L'accès direct aux niveaux les plus bas de commandement, indépendamment de la chaîne hiérarchique est un souci constant du haut commandement national.

Ce sont autant de conséquences au niveau du fonctionnement des états-majors. Il semble que la règle soit: puisque cela existe, nous devons en disposer. Cependant, sans que les conséquences en soient tirées complètement dans le domaine de l'organisation.

Pour ce qui est des matériels, ceux-ci sont de plus en plus banalisés et, seules quelques fonctionnalités militaires spécifiques les différencient des produits civils du commerce. Ainsi, pour les officiers d'état-major, il s'agit avant tout d'acquérir une bonne maîtrise des outils bureautiques standards, indispensables pour une utilisation optimale du système mis à leur disposition.

Enfin, au niveau du développement des SIC, il s'avère très difficile de suivre le rythme des évolutions du marché civil dans la mise en œuvre d'un programme. Il faut pouvoir faire évoluer en permanence le système, autant en lui adjoignant de nouvelles fonctionnalités qu'en le faisant évoluer, afin de répondre le mieux possible aux besoins des utilisateurs.

En conclusion, et pour répondre clairement à la question posée, il est clair que des évolutions importantes sont en cours. Néanmoins, l'organisation du commandement dans ces principes reste identique, même si le fonctionnement des états-majors et le commandement des forces sont en profonde modification par l'apport des nouvelles technologies.

On peut imaginer une organisation comprenant des structures réticulaires, ou chaque individu possède une grande autonomie dans la phase de réflexion, qui doivent cohabiter avec des structures classiques "pyramidales" plus aptes à l'action, l'ensemble de ces structures étant intégré dans une boucle de rétroaction.

Il reste de nombreux problèmes à résoudre en ce qui concerne la formation des personnels, la gestion de l'information ou bien la conduite des programmes. Il reste notamment à engager la réflexion sur les impacts des nouvelles technologies sur l'organisation du commandement.

HÍRADÓKIKÉPZÉS A NÉMET SZÖVETSÉGI KÖZTÁRSASÁG SZÁRAZFÖLDI HADERŐNEMNÉL

A Német Szövetségi Köztársaságban a haderőnemek részére a kiképzés nem egységes a sajátosságok miatt. Az általános érvényű képzés azonban nem mutat eltéréseket. Dolgozatomban a szárazföldi haderőnem híradó állományának képzési rendszerét mutatom be.

Kiképzési rendszer

Kiképzés (1. ábra)

A Német Szövetségi Köztársaság katonai képzési rendszerében támaszkodik a civil környezetre, a civil életben megszerzett szaktudásra, képzésre.

A sorkatonai szolgálat 10 hónap időtartalmú 1996 óta. A 18-28 év közötti hadköteles férfiak kerülnek kiképzésre a Bundeswehrben.

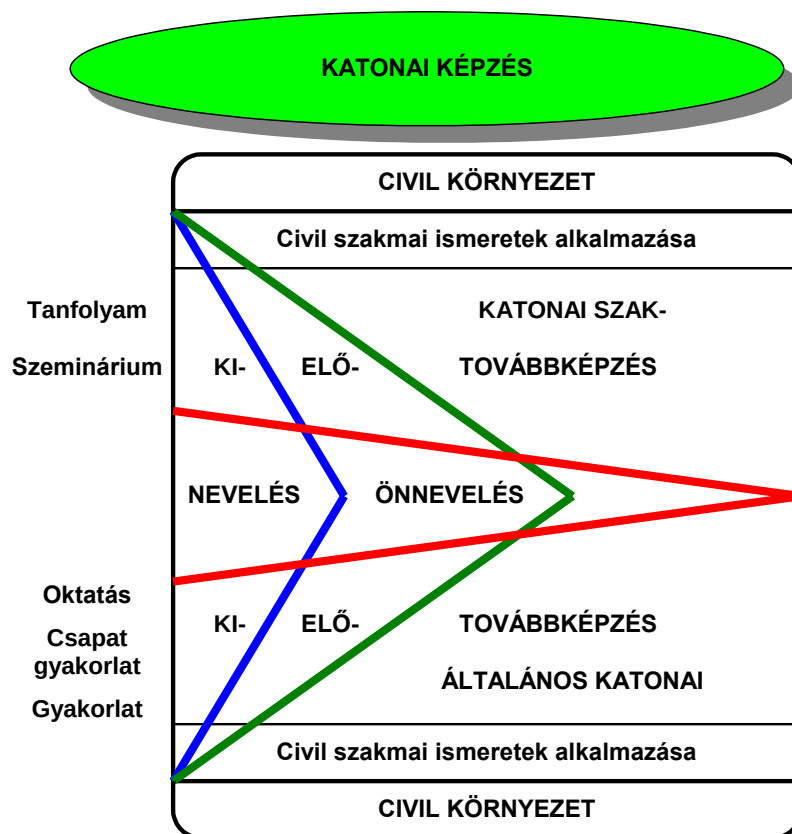
A sorkatonai szolgálat letöltése után a tartalékos hadkötelezettség időtartalma legénységi állomány esetén maximum 9 hónap, tiszthelyetteseknél 15, tiszteknél pedig 18 hónap. Önkéntes tartalékos szolgálat esetén időkorlátok nem kerültek meghatározásra.

A hadkötelezettség legénységi állománynak 45 éves korig, tisztek-tiszthelyettesek esetében pedig 60 éves korig kötelező.

Általános alapkiképzés 2 hónap. A szolgálati helyének megfelelő képzés (szakkiképzés) 1-2 hónap. Alegység szintű kiképzés 4 - 7 hónap.

Az önkéntes tovább szolgálat 2 - 13 hónapig tart, amely letöltése után a szerződéses szolgálati viszonyt választhatja a jelentkező.

Lehetősége van a szerződéseseknek karriertanfolyamra, tiszthelyettesi tanfolyamra, valamint tiszti tanfolyamra.

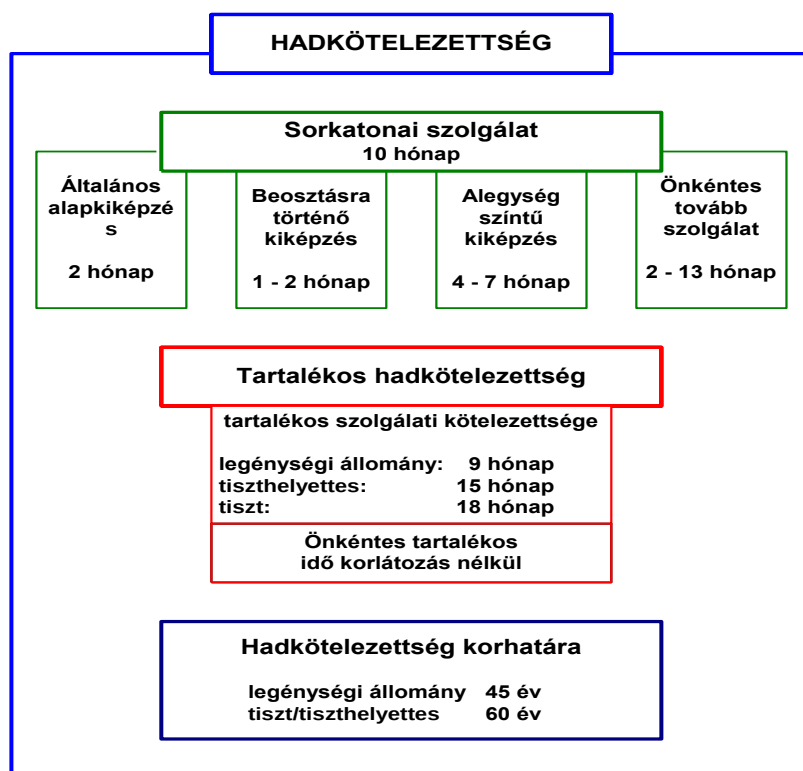


Sorállomány kiképzése (2. ábra)

A tiszthelyettes és tisztképzés rendszerének bemutatására az alábbi táblázatokban található adatok segítik a könnyebb megértést.

A képzés rendszere az előírt időintervallumnak megfelelően történik, ez gyakorlatilag az alap tiszti (hadnagyi), valamint az alap tiszthelyettesi (őrmester) rendfokozat eléréséhez szükséges képzési rendszert mutatja be.

A rendfokozati rendszer nem hasonlítható össze tiszthelyettesek esetén a magyar rendfokozatokkal.



Tiszthelyettes képzés

Év	Hó	Mód	Időtartam	Kiképzés
24		HUS	2 2 hét	Előképző szeminárium
17		HUS	1 2 hét	Előképző szeminárium
8-10		HUS/TrS	3 hónap	Szakasziparancsnoki tanfolyam
5 őrmester		FAKp	2-12 hó- nap	Szakkiképzés A fokozat
4 törzsaltiszt		TrS	3 hónap	Zászlósi tanfolyam
2 altiszt		FAKp	2-11 hó- nap	Szakkiképzés
		HUS	9 hónap	Altiszti felkészítő tanfolyam
1	12 6	Tr/TrS Tr	5 hónap 3-4 hónap	Altiszti alaptanfolyam Általános alapkiképzés és szakbeosztásra való felkészítés

HUS: Tiszthelyettes képző iskola
 TrS: Csapat (fegyvernemi) iskola
 Tr: Csapat (fegyvernem)
 FAKp: Szakkiképző század

Tisztképzés

H	Egyetemi képzés 3 év			
ó	Felkészülés 3 hónap			
3	Hadnagy	Tr	3 hó	Szakaszparancsnoki vezetői gyakorlat
9				
8				
3	Törzszászlós	Tr	9 hó	Szakaszparancsnok helyettesi vezetői gyakorlat Egyéni képzés (pl: idegen nyelv, sportvezetői, gyakorlatvezetői)
7				
6				
3				
5				
4				
3				
3				
2				
3				
1				
3				
0				
2		OSH	6 hó	Tiszti tanfolyam
9				
2				
8				
7				
2				
6				
2				
5		Trs	1 hó	Szabadság
4				
2				
3				
2				
2				
2	Zászlós	Trs	1 hó	Szabadság

1				
2	Zászlós- jelölt	TrS	5 hó	Tisztjelölt tanfolyam II. rész (szakasparancsnoki képzés, magában foglalva 4 hetes speciális túlélőtanfolyamot)
0				
1				
9				
1				
8				
1				
7				
1				
6				
1		Tr	3 hó	Rajparancsnoki vezetői gyakorlat (általános és szakkiképzőként)
5				
1				
4		TrS	4 hó	Tisztjelölt tanfolyam I. rész (rajparancsnoki képzés)
1				
3				
1				
2				
1				
1				
0				
9				
8	Tisztje- lölt	Tr	2 hó	Gépjárművezetői alapkiképzés
7		Tr		Alegység szintű kiképzés (szabadság)
6				
5		Tr	1-2 hó	Szolgálati kiképzés
4				
3	Őrvezető	Tr	2 hó	Általános alapkiképzés
2				
1				

OSH: Tisztképző iskola
TrS: Csapat (fegyvernemi) iskola
Tr: Csapat (fegyvernem)

Iskolák

A BUNDESWEHR új vezetési struktúrájának kialakítása során az iskolai rendszerű képzés koordinálása érdekében a katonai iskolák vezetésére létrehoztak osztályvezetői állást a Heeresamt-ban.

Az iskolák tagozódása a következő rendszer szerint került meghatározásra:

- 2 tiszti iskola (OSH)
- 3 tiszthelyettesi iskola (HUS),
- 16 fegyvernemi iskola (TrS).

A híradó kiképzéssel és szakkiképzéssel foglalkozó iskolát Feldafingen hozták létre, melynek elnevezése Fernmeldeschule des Heeres/Fachschule des Heeres für Elektrotechnik. A továbbiakban ezen híradó kiképző központ oktatási tevékenységét ismertetem.

A tisztek és tiszthelyettesek fegyvernemi képzése, valamint szakkiképzése, speciális híradó eszközök alkalmazására való felkészítése, illetve karriertanfolyamai találhatóak ebben az intézményben.

Itt különböző technikai beosztásokra, valamint a parancsnoki funkciók betöltésére szolgáló tanfolyamok kerülnek megtartásra, ebben az intézményben található a BIGSTAF, a HEROS, AUTOKO rendszerek elemeinek híradó felkészítése.

Az intézményben a szakképzés mellett nagy hangsúlyt fektetnek a fizikai felkészítésre. A tiszteknél általában az alaptanfolyamon szakaszparancsnoki beosztásig kerülnek felkészítésre, karriertanfolyamként a századparancsnoki, zászlóaljparancsnoki, törzstiszti beosztásra történő felkészítésre, melyek 1-3 hónapig tartanak, tiszthelyettesek esetében különböző szakbeosztásokra, technikai ismeretekre és a vezetési rendszerek üzemeltetésére készíti fel az állományt.

Híradó szervezetek

Legfelsőbb katonai vezetés híradásának biztosítására

2 híradóezred (1 híradással, 1 híradó technikai biztosítással)

Légierő vezetésnek biztosítására

törzs- és híradóezred

Szárazföldi haderőnem vezetésének biztosítására

törzs- és híradóezred

Hadtestek

törzs- és híradóezred (vezetési pontok, valamint a hadtest felelősségi területének híradó üzemeltetése)

híradózászlóalj (AUTOKO rendszer üzemeltetése)

Hadosztály

törzs- és híradózászlóalj (vezetési pontok, valamint a hadosztály felelősségi területén a csapatok vezetésének biztosítása)

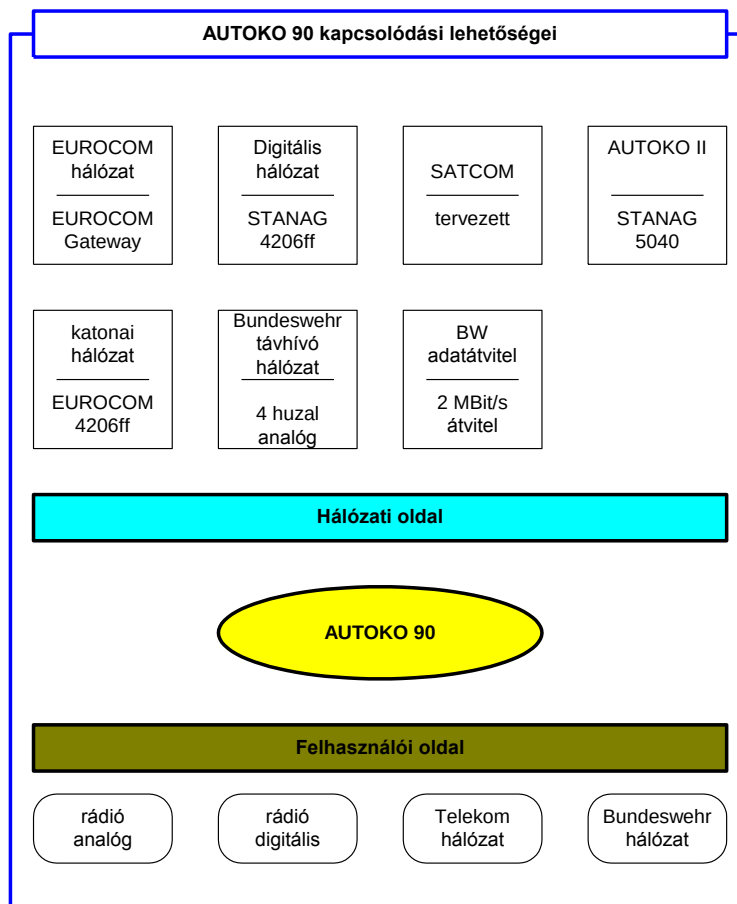
Dandár

híradószakasz (a dandár vezetési feltételeinek megteremtése, AUTOKO végpont üzemeltetése a vezetési ponton)

A felsorolt vezetési szintek, azok híradó erői is megmutatják, hogy a híradó ki-, illetve továbbképzés milyen fontos terület a Bundeswehren belül.

Az AUTOKO rendszer kapcsolódási lehetőségei, mind a felhasználói, mind a hálózati oldalon megfelelő technikai, szabályzat ismeretet igényelnek, melyre a Bundeswehr híradó kiképzési rendszere a megfelelő szintű felkészítést tudja biztosítani.

Az alábbi táblázaton az AUTOKO rendszer, kapcsolódási lehetőségeit vázoltam fel.



Összhaderőnemi Információtechnológiai gondolkodás

A Német Szövetségi Köztársaság Védelmi Minisztériuma létrehozott 2000. augusztus 1.-től egy Információtechnológia igazgatói (IT-Direktor) posztot és az alatta dolgozó stábot, amely a Bundeswehr információtechnológiai feladataiért felelős.

Egy új projekttel, elnevezése KINTOP (Interoperabilität der Krisenreaktionskräfte), az azonnali (gyors) reagálású erők interoperabilitási problémájának megoldásával foglalkozik.

Feladata, hogy az „alkalmazási területen” lévő Bundeswehr alakulatok, parancsnokságok és Németország között javítsa az együttműködési képességet a kommunikációs rendszeren belül, műholdas összeköttetések által.

Az igazgatóság másik feladata, megoldást keresni a szárazföldi, a légierő, a hadi tengerészet vezetési rendszerei (RUBIN, JASMIN, VERIS, HEROS, stb.) együttműködési lehetőségére minősített esetben. Eddig nem volt lehetséges az összhaderőnemi vezetés. Ennek megoldása „Összhaderőnemi Vezetési Információs Rendszer” (Streitkräftegemeinsames Führungs-Informationen-System).

Harmadik feladat egy program kidolgozása (HERKULES), „az együttműködés új formája az iparral”, az innováció, инвестиáció és gazdaságosság a Bundeswehrben jegyében.

Természetesen a felsorolt feladatoknak való megfelelés eredményeképpen a képzési rendszerben is várhatóak a változások

FELHASZNÁLT IRODALOM

1. Klaus Hahnenfeld, Neuordnung im IT-Bereich, (Sodat und Technik, 2002. Január 19-23. o.)
2. <http://www.bundeswehr.de>
3. Bundesministerium der Verteidigung Inspekteur des Heeres, Führungsgrundgebiet 6 (Védelmi Minisztérium Szárazföldi Inspektor, 6. Vezetési Terület (Szolgálati használatra))
4. FmS/FSHEIT Oktatási Segédanyagok: AUTOKO 90, BIGSTAF, AUTOKO II

PROFI HADSEREG HATÁSA A KIKÉPZÉSRE

Az 1989-ben megkezdődött társadalmi és politikai átalakulás jelentős hatást gyakorolt az ország védelmével és a fegyveres erők funkciójával foglalkozó politikusok és katonai szakemberek gondolkodására. Még korábban a szovjet vezetés alatt álló Varsói Szerződésben elfoglalt helyünk és a magyar fegyveres erőknek szánt szerep határozta meg a gondolkodás témáit és határait, 1989-től kezdve egyre inkább a saját erőkre való támaszkodás, illetve ezzel párhuzamosan egy másik katonai szövetséghez, a NATO-hoz történő mielőbbi csatlakozás gondolata vált a szakemberek legfontosabb feladatai közé.

Az 1955-től 1991-ig tartó Varsói Szerződés tagság során egyértelmű volt az, hogy a Szovjetunió világuralmi terveinek megvalósítása céljából létrehozott katonai szövetségen belül nincs helye és lehetősége az önálló magyar katonai elméletének és az erre épülő önálló nemzeti fegyveres erőnek. Az emberek, katonák nevelése megakadályozta új, emberközpontú feladatrendszer, kiképzés bevezetését. A meghatározó nézet még mindig a tömeghadsereg, az elrettentő demonstráció megjelenítése volt. Ezt megelőzően az 1945-55-ös évek alatt sem lehetett szó önálló magyar honvédelemről és gondolkodásról, hiszen a Magyarországot megszállva tartó szovjet fegyveres erők, majd az 1948-tól nagy ütemben épített Néphadseregben jelen lévő szovjet tanácsadók meggátolták a nemzeti célok érdekében történő gondolkodást, valamint az ezek alapján elképzelt haderőfejlesztést.

Az 1980-as évek végi Magyar Néphadsereget még mindig az úgynevezett ipari társadalomnak megfelelő „tömeghadsereg” sajátosságai jellemezték. Úgy mint a túl magas békelétszám, a régi és új hadi8technikai eszközök együttes hadrendben tartása, a túlzott költség, a szovjet hadászat, hadművelleti művészet és harcászati elveinek- módszereinek alkalmazása, valamint a nemzetgazdaság különböző ágazataiban végzett idénymunka.

A változás elkerülhetetlenné vált, ahogy a politikai szemlélet is átalakulásba kezdett. Megkezdődtek a Magyar Néphadsereg megreformálásai, átszervezései. Az új szervezeti rendszertől a létszámgondok enyhítését, az ütőerő lényeges növekedését várták. Az évek folyamán végrehajtott átalakulás jelentős szemléletváltást hozott, mely hatására előtérbe került a kiképzés jelentősége, a folyamatosság megtartása. A gyorsan változó nemzetközi (számunkra kedvező) átalakulási folyamatai, a fokozatosan javuló hazai gazdasági helyzet teremtették meg az alapját annak, hogy a Magyar Honvédségben kezdetét vegye egy eddig példa nélkül álló haderőreform, haderő-átalakítás. Ez a folyamat a mennyiségi változásokon túl a minőségi átalakításnak és a modernizációnak ad prioritást, meghaladja az előző időszak reform- és átalakítási kísérleteit.

A haderő-átalakítás eredményeként az átalakuló, kisebb létszámú, korszerűbb, finanszírozhatóbb, társadalmilag elfogadott, megbecsült, vonzó pályaképet felmutató magyar haderőnek alaprendeltetésével összhangban biztosítania kell a szövetségi kötelezettségek teljesítését, a szövetségi rendszer keretei közötti együttműködés, a nemzetközi béketámogató és válságkezelő erőfeszítésekhez való hozzájárulásokhoz megfelelés képességét.

Az átalakítás kiterjed a haderő életének minden területére, így a Magyar Honvédség hadrendjére, szervezeti felépítésére, vezetési rendjére és alkalmazási elveire, a harckészültség és mozgósítás, a hadkiegészítés, a felkészítés és kiképzés rendszerére.

Az átalakítás eredményeként létrejön a jelenleginél kisebb létszámú tartósan finanszírozható, feladatainak ellátására alkalmas haderő, amely képes:

- reális visszatartó erő megjelenítésére,
- az ország katonai védelmének biztosítására, valamint a kollektív védelmi feladatok végrehajtására,
- a nemzetközi szerződésekben vállalt katonai kötelezettségek teljesítése keretében béketámogató és humanitárius műveletekben, valamint szövetséges csapatok manővereinek, szállításainak biztosításában való részvételre,
- alkotmányosan kihirdetett szükségállapot idején a rendvédelmi szervek támogatására,
- elemi csapás, katasztrófa esetén segítségnyújtásra, közreműködésre a polgári védelmi feladatok ellátásában.

Első ütemben megvalósul az új szervezeti rendre történő áttérés, az új diszlokáció, az indokolt létszámarányok kialakítása, a fenntartási és működési költségcsökkentés megalapozása, a munka- és életkörülmények javítása, a NATO-kompatibilitás és interoperabilitás legalapvetőbb feltételeinek biztosítása.

A második ütemben a hadrafoghatóság és a kiképzési szint növelése a cél.

A harmadik ütem a haditechnikai modernizáció képességi igényeknek megfelelő kialakítását öleli fel.

Az átalakítás során jelentősen változtak, módosultak a békében rendszeresített beosztási arányok. A sorállományú beosztások csökkentésével párhuzamosan növekedett a szerződéses állomány létszáma. A cél egyértelműen a professzionális haderő elérése, melynek alapja az önkéntes, szerződéses állományú katonák alkalmazása. Ehhez minőségi változásnak kellett beállnia az oktatás, felkészítés, kiképzés területén is.

A tisztképzés a Zrínyi Miklós Nemzetvédelmi Egyetemen és fakultásain, a tiszthelyettes-képzés a Központi Tiszthelyettes Szakképző Iskolán folyik.

Az oktatásban kiemelt figyelmet kapnak a speciális szakmai, a nyelvi és a számítógépes ismeretek, a szellemi kompatibilitás megvalósítását célzó területek.

A hivatásos állomány megújult oktatási, felkészítési, kiképzési rendszere magasabb átjárhatóságot biztosít a civil és a katonai képzés között. A felkészítés, kiképzés folyamatában különös hangsúlyt kapnak az önállóság, a fizikai erőnlét fokozására, az alegység, az egyes katona harcának, tevékenységének támogatására irányuló formák, módszerek.

A harctéri siker alapját a jól szervezett kiképzés képezi. A jól kiképzett és fegyelmezett katonák jelentős pozitív változást eredményeznek a katonai szervezetek hatékonyságában még annak ellenére is, hogy azok nincsenek a legkorszerűbb fegyverzettel, technikai eszközzel felszerelve. A kiképzés területén a reformkoncepciók tisztán, világosan megfogalmazzák azokat a követelményeket, célkitűzéseket, amelyeket az újonnan kialakítandó haderő igényei a kiképzéssel szemben támasztanak.

A szerződéses állomány folyamatos elterjedésével (a teljes átállást követően) meghatározó könnyebbtséget jelent a kiképzés színvonalának, hadrafoghatóságának kialakításában. A besorozott állomány szolgálati idejének leteltével folyamatosan cserélődött, így meghatározott időnként kezdődhetett előlről a teljes kiképzés. A szolgálati idő drasztikus lecsökkentésével a sorozott sorállomány kiképzése sok kívánnivalót hagyott maga után, általában csak az alapok megteremtésére volt idő biztosítva a különböző szakterületen. A profi haderő folyamatos megteremtése a szerződéses állományra való átállás nagy lehetőségeket biztosít a kiképzés területén. A kiképzésre fordítható időt nagy mértékben lehet növelni, így költséghatékonyabbá, realizitkusabbá, a kiképzendők motiváltságának növelésével egyidejűleg intenzívebbé, az egyének és elsősorban az alegységek teljesítményének mérése objektívabbá, a gyakorlatok tervezése egyszerűbbé, szakszerűbbé válhat. Rugalmas cél- és feladatorientált kiképzési rendszer kialakításával, valamint a kiképzés belső tartalmának, arányainak megváltoztatásával gyorsabban reagáló, részben önálló szerződéses (profi) katonák kerülnek a Magyar Honvédség állományába.

Az önkéntes szerződéses állomány kiképzése a Kiképző Központokban folytatott kiképzéssel veszi kezdetét, amely magában foglalja a szerződéses állomány egyéni alap- és szakalapozó kiképzését. Szakmailag a Kiképző Központ lehet az első szűrő, amely a katona egyéni felkészültségét, alkalmasságát megállapítaná. Ez hatalmas lépés, hiszen a profi hadseregben olyan katonákra van szükség, akikkel el lehet végezni a kijelölt feladatot, önálló gondolkodásra alkalmasak.

A kiképzés belső tartalmának kialakítása a rugalmasság, az erőforrásokkal összhangban lévő cél-, és feladatorientált kiképzés megteremtésének a záloga. Bizonyos állandóan visszatérő kiképzési feladatok kivételével mindig változó (tehát nem ismétlődő) a kötelék számára megszabott feladattól, az

adott parancsnok kreativitásától, felkészültségétől és a rendelkezésre álló erőforrástól függően változik. Így a szerződéses katona folyamatosan tovább képezhető, felkészíthető. Az önkéntes haderőt az állományváltás szempontjából állandóság jellemzi- az állomány feltöltése után – és csak az időközben szolgálatot vállalók alap kiképzését kell végrehajtani, amely lényegesen kisebb leterheltséget jelent a kiképző központok számára. A kiképzésre fordítható idő jelentősen meghatározza annak hatékonyságát. A sorozott sorállomány kiképzésében fő probléma volt, hogy mire elért egy kiképzettségi szintet, vagy az alegységek összekovácsolása befejeződne már le is szerelt, így a hadrafoghatósági szint állandóan változik. Ugyanakkor a szerződéses katonákkal felöltött alegységek hadrafoghatósági szintje csaknem folyamatosan állandóan egy meghatározott szint elérése után fokozatosan tovább fejleszthető. Ezen képzési formák alapján megfelelnek azon képességeknek, amelyek minden területen, az egyes szervezeti egységeket, alegységeket minimális rákészítéssel alkalmassá teszik az összes akcióformában eredményes tevékenységre.

A kiképzésnek arra kell törekednie, hogy növelje az egyén vagy alegység szakértelmét, ezzel erősítve az önbizalmat, a tudást, a feladat végrehatási képességeket. Ennek elérése érdekében biztosítani kell egy olyan kiképzési környezetet, légkört, amely elősegíti a tanulást és a fejlődést. Profi katonák közösségében ez könnyen megvalósítható, hiszen minden egyén célja a fejlődés, a jelenkori kihívások magas szintű megfelelése. Egy olyan környezetben, ahol a katonák hivatásuknak választották a honvédségi életpályát, kevésbé kell szembenézni olyan visszatartó erővel, mely szétzilálná a fegyelmet, a kiképzést.

A kiképzésnek alávetettek teljesítményét rendszeresen és minden egyes szakaszban értékelni lehet a követelményekhez viszonyított teljesítménymutatók, valamint a kiképzési elvekért és a tervezésért felelős személyek által meghatározott szintek alkalmazásával. Amennyiben lemaradás vagy elfogadható hibák hátráltatják a katona fejlődési szintjének növekedését, mindig van lehetőség annak kiküszöbölésére.

A teljesítmény ilyen mérése segítséget nyújt a parancsnoknak az egységek, katonák értékeléséhez. Ez azon eszközök egyike, amely által a jövőbeni kiképzési követelmények ebből adódóan az erőforrás-szükségletek meghatározhatók. A profi haderő kialakítása szakaszában alapvető elem, hogy egy szerződéses katonára meghatározóan több kiképzési idő jut, mint korábban egy sorozott katonára. Így előtérbe helyezhető a szakmai kiképzés, az általános kiképzés, amely hozzájárul a személyes fejlődéshez. Ez utóbbi főleg ismeretalapú és magába foglalja az oktatást. Néhány jártasságot alapvetőnek vagy kötelezőnek tekinthetünk, amellyel mindenkinek rendelkeznie kell. Az alapvető jártasságokat és azok mindegyikében elérendő követelményeket rendszeresen felül kell vizsgálni.

A jártasság minden fajtája kopik, ha nem alkalmazzák rendszeresen. Ennek mértéke az egyéntől és a speciális jártasságtól függ. Ezt a kopást megelőzhet-

jük, ha ezeket a jártasságokat a kiképzés más kategóriáiba építjük be. A jártasságok megerősítésének gyakoriságát az elfogadható működési szint fenntartása érdekében elsősorban a felejtés, a működési hatékonyság, az idő és költség kiegyensúlyozásával kell irányítani és nem valamely meghatározott időkerettel. A szerződéses profi idejéből kitelik, hogy a meghatározott feladatokra koncentrálni, ismétlődő foglalkozásokon, képzésen vegyen részt.

A kisebb, de nagyobb képességű, rugalmasabb haderőnek biztosítani kell, hogy az általa folytatott kiképzés járuljon hozzá az alkalmazási feladatok szélesebb skálájának végrehajtásához. Alapvető fontosságú, hogy az új (profí) katonák valamennyi szinten átítatódjanak a harcos erkölccsel. A hozzáértő és gondos parancsnokok által kiképzett és vezetett minőségi katonák a siker kulcsai maradnak a jövő harcmezőjén is. Gondosan kiválasztott, egyéni feladatokra képzik ki őket az alapkiképzés során, így biztosítva harckészségüket beosztásukba áthelyezésüktől kezdve. Ismerni fogják a velük szemben támasztott változatos jellegű feladatokat és követelményeket, továbbá ismerni fogják az általuk használandó felszerelést.

Valamennyi szinten a megnövelt rugalmasság és alkalmazkodóképesség a követelmény.

A szerződéses katonai kiképzés válik a legfontosabb feladattá a haderő számára, ezért mindent megtesz azért, hogy szolgálati idejük alatt a szerződéses katonák a lehető legjobban sajátítsák el a katonai mesterséget. Így azután a pszichikai és fizikai terhelések következtében a szolgálati idejük lejártát követően a társadalom aktív tagjaivá válnak.

Források:

- | | |
|-------------------|--|
| Dul Sándor. | Adalékok a kiképzési rendszer kialakításához |
| Kőszegvári Tibor: | A magyar katonai gondolkodás a 90-es években |

ÚJ KIHÍVÁSOKRA — ÚJ VÁLASZOK?!

Napjainkban a sajtó — az írott és az elektronikus is — hangos a politikai pártok egymásnak feszülésétől. A kormány három nagy területen reformintézkedéseket jelentett be. Ezek közül számunkra a legfontosabb, amelye minket közvetlenül érint, a haderőreform kérdésköre. Mint amikor az állóvízbe dobott kő hullámokat vet, úgy jönnek sorban, egymás után a kérdések.

Én nem a reformmal magával, hanem csak azokkal a minket, engem állandóan foglalkoztató kérdéscsokorral, a felvetődő megválaszolandó kérdésekkel akarok foglalkozni, amelyekkel nap mint nap találkozom. Igen nap, mint nap, mert különböző híreket hallunk a karcsúsításról, az összevonásokról, a költségmegvonásokról stb. Hallottunk már kisebb, de erősebb, ütőképesebb hadseregről. Arról, hogy nincs ellenségképünk és arról is, hogy belátható időn belül nem kell a haderő komplex alkalmazásával számolnunk. Mindezek jól képzett, tanult emberek véleményével alátámasztva, a számsorok hosszú, hosszú kilométereivel.

Az ilyen nagy ívű kérdések mellett teljesen eltörpülnek azok a problémák, felvetések, amelyekkel foglalkozni akarok. Tulajdonképp ezek nem különálló kérdések, hanem egy téma különböző aspektusú vizsgálata. Nem, nem vizsgálat. Kérdéscsokor, egy gondolatsor, egy fájó, de megoldásra váró, ha úgy tetszik sürgősen megoldandó kérdéskör. Hogy milyen kérdésekről? Az iskola-rendszerű képzésről.

Eddig is tudtunk róla, eddig is éreztük a jelentését annak, hogy a beiskolázásra váró, felvételre jelentkező tisztek, miután befizették a felvételi eljárás díját és beküldték jelentkezési lapjukat, a felvételi vizsgára már nem érkeznek be. Nem jelennek meg, mert nincs parancsnoki támogatásuk. Az állományilletékes parancsnok nem járul hozzá, nem javasolja továbbtanulásukat. Ergo olyan jól állunk kiművelt emberfőkkel, hogy nem szükséges fiatal, tehetséges emberek számára lehetővé tenni a tudás, a magasabb szakmai és általános műveltség megszerzését. Érdekes egy felfogás, szerintem fordítva ülünk a lovon, azon a képzeletbelin.

Azért, hogy a helyzet ne legyen ilyen egyszerű, egyértelmű, valaki, vagy valakik bedobták a köztudatba azt a gyűlölt kifejezést, hogy túlképzés. Mi ez? Csak nem arról van szó, hogy nincs szükség művelt, gondolkodni tudó embe-

rekre? Vagy talán az a baj, hogy túl sokan, sokat fognak gondolkodni? Netán más véleményük lesz, mint a kontraszelekcióval fölénk tett főnököknek?

Mert mondjuk meg őszintén, — ha azok akarunk lenni egy gyenge pillanatunkban — ez kontraszelekció! Mármint az, ha csak azt lehet beiskolázni, akit a parancsnoka javasol, mert kiszemelte őt egy egyetemi végzettséghez kötött munkakör betöltésére. És itt a parancsnok is kutyaszorítóban van! Mert én a 2001. XCV. törvényben nem olvastam olyan kitételt, hogy az egyetemi és főiskolai végzettségű tiszteket, ilyen végzettséghez kötött beosztásba **kell** helyezni. Parancsnokaink erre hivatkozva tagadják meg az aláírásukat a jelentkezni, a tanulni, többet tudni akarótól.

A törvény 1. számú melléklete szerint a főtisztek: őrnagy, alezredes, ezredes. Az őrnagy tehát főtiszt. Akkor miért nem végezhet egyetemet? Az őrnagyi beosztás miért nem egyetemi végzettséghez kötött? Mert ez a gyakorlat Nyugaton és Keleten is? Ha már főtiszt az őrnagy, miért nem tanulhat, miért nem végezhet egyetemet?

Az előmeneteli tanfolyam nem pótolhatja az egyetemi diplomát! De erről majd később szólok.

Három törvényi helyről szeretnék idézni csak, a teljesség igénye nélkül, ezek ismeretében vonja le mindenki a következtetéseit.

80§ „A magasabb beosztás betöltéséhez szükséges iskolai végzettség megszerzését hazai vagy külföldi ... iskolarendszerű, vagy iskolarendszeren kívüli oktatás (képzés) keretében kell biztosítani. A beiskolázásra pályázat, vagy kijelölés útján kerül sor. Emellett **lehetőséget kell adni** a szolgálat tagjának a szolgálati érdek sérelmével nem járó, saját elhatározáson alapuló továbbtanulásra is.”

81§ „Ha a továbbtanulás nem kapcsolódik közvetlenül a beosztáshoz, vagy a tervezett előmenetelhez, a képzéssel összefüggő támogatás csak tanulmányi szerződéssel biztosítható.”

Ezekben nincs semmilyen megkötés, tiltás, tilalomfa, diszkrimináció. Pláne akkor, ha a tiszt saját szakmájában kíván fejlődni. Tudást és nem papírt szerezni.

És álljon még itt a sorban a 2003. évi XLV. törvény, amely módosítja a fegyveres szervek hivatásos állományú tagjainak szolgálati viszonyáról szóló 1996. XLIII. törvényt.

52. § a HSzt. 98§-ának (1) bekezdése helyébe a következő rendelkezés lép:
„(1) A hivatásos állomány tagja saját elhatározása alapján iskolarendszerű oktatásban/képzésben csak az állományilletékes parancsnok felé tett előzetes **bejelentés!** alapján folytathat tanulmányokat. Az állományilletékes parancsnok **csak** abban az esetben korlátozhatja az oktatásban/képzésben való részvételt, ha az a szolgálati érdek aránytalan sérelmével járna. A képzésben részt vevő részére a tanulmányok folytatásához szükséges szabadidőt biztosítani kell.

Ez megtalálható a Honvédelmi Közlöny 2003. augusztus 22-i 15. száma 1070-1104. oldalain.

A törvényi oldalról véleményem szerint tiszta a kép. Most már csak a fejekben kellene rendet tenni.

A polgári egyetemekre, főiskolákra jelentkezők, ha levelező képzésre nyertek felvételt sok esetben a szabadságuk terhére, minden engedély nélkül folytathattak, folytattak és folytatnak tanulmányokat olyan területeken, amelyekből az MH-nak semmilyen „haszna” nem származott. És aki katonaként akar „katonául” tanulni?

Arról nem is beszélve, ha marad ez a jelenlegi gyakorlat, akkor az oktató állomány is dilemma elé kerül. Ha valakit beiskoláztak, akkor azt egy magasabb beosztás betöltésére tervezték. Várnak rá. Várják. Az oktató mindent megtesz azért, hogy elsajátíttassa vele az anyagot. És ha nem megy? Könnyű a válasz, megbukik. És ha akkor sem tud majd levizsgázni? Kegyelem kettes? Vezető beosztásban? Szelekció? Kontra!

Nem lenne jobb az a megoldás, hogy aki tanulni akar az tanulhasson? 52. §! És az azonos felkészültséggel rendelkezők közül kiválasztani azt, aki alkalmas a magasabb beosztás betöltésére?

El kellene gondolkozni — a véleményem szerinti — helytelen gyakorlaton. Ezt követeli a tiszti állomány csökkentése, a tudományos-technikai színvonal emelkedése, a hadsereg érdeke. A kiművelt emberfők fogják a tisztállomány társadalmi presztízsét, elismertségét megalapozni.

A haderőreform nem hagyja érintetlenül az oktatási intézményeket, így egyetemünket sem. Mielőtt a kérdés érdemi részéről szólnék, meg szeretném említeni, hogy amit a Nemzetvédelmi Egyetemen el lehet sajátítani, azt nem kellene a polgári felsősokú intézményekben megrendelni. Mert ezek csak hangulatot keltenek, rontják az állomány közérzetét.

Az egyetem állományának csökkentése, a karok összevonása, a szakmai műhelyek, a szakmai kultúrák megőrzése jelentős terhet rakott, rak az állományra.

A beiskolázási keretszámok csökkentése, illetve a parancsnoki engedéllyel rendelkezők csekély száma sürget mindenkit arra, hogy új utakat, új alapokat keressen az oktatás/képzés számára.

Azt tudjuk, hogy kinek képezzünk. A megrendelőnek. A megrendelő a Magyar Honvédség. A megrendelő igénye elsődleges. Viszont, ha a megrendelő érdeklődése csökken, akkor választékbővítéssel, síppal-dobbal, nádihegedűvel fel kell kelteni érdeklődését.

Különböző tanfolyamok szervezésével, posztgraduális képzéssel, esetlegesen a zászlósi és tiszthelyettesi képzésben való részvétellel.

Ez nem új dolog. Nem mi találtuk ki. Pl. Franciaországban, Rennesben a Híradó iskolán folyik a francia haderő számára a híradók képzése. A katonától a tiszthelyettesen, a tiszten át a főtisztig.

Nem egy eretnek gondolat az, hogy a képzést egy kézbe kellene adni! A szakképzést. A pincétől a padlásig. Egy vezérlő akarat, egy elgondolás mentén. Így egyívű képzés lenne, a központi elképzelésnek megfelelően. Persze ennek is lennének szakaszai, de minden a cél elérése irányába hatna.

Ebben a tanévben megkezdődtek a különböző előmeneteli tanfolyamok. Ezek beindítását, megvalósítását csak üdvözölni lehet.

Ezek a tanfolyamok az előző (főiskolai) képzés óta eltelt időben a szakterületet érintő fontosabb eredmények, változások, történések kerülnek oktatásra olyan igénnyel, hogy képesek legyenek rendfokozatuknak (beosztásuknak) megfelelő végrehajtói, vezetői, irányítói tevékenység végrehajtására.

De ezek a tanfolyamok **nem helyettesíthetik** az iskolarendszerű képzést. Csak kiegészíthetik.

Miért?

Köztudott, hogy a megszerzett tudás 4-6, de a szakterület gyorsan változó ismeretanyaga 2-3 év alatt elavul. Ezért is kell egy átgondolt, személyi és tárgyi feltételekkel ellátott képzési/felkészítési rendszert létrehozni, a működési feltételeit biztosítani.

A képzés tehát:

- szorosan kapcsolódjon az előmeneteli rendszerhez, de az ne legyen gátja;
- mindenkor elégítse ki a szervezet igényeit;
- biztosítsa a különböző, azonos rendfokozathoz kötött beosztások közötti átjárhatóságot. Ez egy izgalmas kérdés, külön tanulmányokat kellene írni róla.

Ismételten meg kellene vizsgálni:

- az egyetemi végzettséghez kötött munkaköröket;
- újra kellene gondolni a képzés követelmény- és feladatrendszerét;
- ismételten át kellene tekinteni és módosítani a tiszti és főtiszti feladatköröket.

Különösen akkor, amikor a tisztek szerepe, feladata, feladatköre, szerepvállalása átalakul, módosuláson megy át.

Köszönöm a figyelmet!

GPRS: ÚT A MOBIL INTERNET FELÉ

A huszadik századot joggal nevezhetjük a kommunikáció évszázadának. Igaz, a legalapvetőbb találmányok még a XIX. században keletkeztek, de ezek tömeges megjelenése csak később kezdődött el. A század első évtizedeiben terjedt el rohamosan a telefon, a húszas években a rádió, míg az ötvenes években a televízió indult hódító útjára. A század utolsó évtizede újabb hatalmas fejlődést hozott a kommunikációban, mely méltán hasonlítható az előbb említettekhez – ez a mobiltávközlés megjelenése, az egész világon történő elterjedése...

A mobil kommunikáció nem új találmány, hiszen mintegy hetven évvel ezelőtt már megszületett az igény az ilyen jellegű kommunikációs kapcsolatok kiépítésére, akkor, amikor 1930-ban, St. Louis városában felállították az első mobil összeköttetés létesítésére alkalmas „hálózatot”. A kísérlet során egy magaslati pontot választottak az adó telepítésére, amelytől néhány kilométeres távolságban egy haladó tehergépjárműbe vevőt helyeztek el. Az összeköttetés megteremtése sikerrel járt, ennek ellenére a további fejlesztések lelassultak, sőt szinte le is álltak.

Azóta eltelt közel hetven év, kidolgozásra került a cellás elv, és a technika robbanásszerű fejlődésen ment keresztül. A kis dombon felállított adó, és a több száz kilós teherplatóra szerelt vevő az egész világot behálózó rendszerré nőtte ki magát. Napjainkra, pedig elértünk arra a szintre, hogy a Kínai piacutatások szerint naponta mintegy 15 millió felhasználóval bővül a felhasználók egyre népesebb tábora.

A technikai fejlesztések hatására a készülékek mérete miniaturizálódott és mindössze pár dekagrammosra zsugorodott. A piacra kerülő egyre kisebb, sokoldalúbb és olcsóbb készülékek iránt megnövekedett a kereslet, ami újabb lökést adott a technológiai fejlődésnek. A lényeg mindazonáltal ugyanaz maradt: a tulajdonos bárkivel, bármikor, bárhol beszélhessen, avagy adatot cserélhessen; országhatároktól függetlenül is!

A mobil kommunikáció fejlődésének eddigi lépcsőfokai az első, második és harmadik generációs mobil rendszerek (1G – 2G – 3G). Az 1G rendszer analóg, míg a 2G rendszer már digitális rádiós technikát alkalmaz. Mindkét rendszer hozzáférési hálózata cellás elven épül fel, és míg az 1G rendszereket (pl.: Magyarországon a Westel 0660) napjainkra már lassan kivonják a forgalomból, addig a 2G rendszerek most éli fénykorukat. A 2G rendszerekben, kezdetben globális szabványok hiányában helyi irányzatok jöttek létre. A két fő irányzat az európai GSM (Global System for Mobile) és az észak-amerikai

CDMA-TDMA (Code/Time Division Multiple Access) rendszer. A 2G rendszer nem kimondottan alkalmas vezeték nélküli adat-szolgáltatás biztosítására a kis adatátviteli sebessége miatt (10-13 kb/s). Ezt a problémát a 2.5G és 3G rendszerekben a HSCSD (High Speed Circuit Switched Data - 57,6 kb/s), a GPRS (General Packet Radio System - 115 kb/s) és az UMTS (Universal Mobile Telecom System - 2 Mb/s) hálózati technológiák, valamint az IP (Internet Protocol) vezeték nélküli kiterjesztése hivatottak leküzdeni. Ezekkel a technológiákkal a fejlesztők reményei szerint megvalósulhat a mobil Internet.

A fejlesztők álma technikai oldalról tekintve már teljesült, hiszen a 3G rendszerek, ha csekély számban is, de működnek. Ezzel ellentétben áll a fogyasztói társadalom igénye és főképp „pénztárcája”. A 2G rendszerek leváltásának ideje még nem jött el, azonban a szolgáltatók már tudnak olyan szolgáltatásokat nyújtani, amelyek ízelítőt adhatnak a jövőbeni lehetőségekről.

A GPRS (General Packet Radio Service) egy egyszerű megoldás, amelylyel a GSM technológiákat alkalmassá tesszük a nagyobb adatátviteli sebességek kezelésére. A GPRS olcsóbbá, gyorsabbá és még inkább felhasználóbaráttá teszi a mobil-adatátvitelt.

Mivel csomagkapcsolt adatátviteli technológia, a hálózatüzemeltetők számára költség hatékony megoldást jelent. A rendelkezésre álló rádióspektrumot nagyon hatékonyan használja, és nagyobb sávzélességet biztosít az előfizetők számára. A GPRS ugyanakkor teljesen új mobilkörnyezeti alkalmazások előtt is megnyitja az utat, és **hídként szolgál a GSM rendszer és az Internet között.**

A GPRS a csomagkapcsolási technológiával és az internet protokollal (IP) bővíti a mobilhálózatokat. A GPRS rendszer lehetővé teszi, hogy a hálózatüzemeltetők mobil internetes és egyéb IP alapú szolgáltatásokat nyújtsanak a jelenlegi, hangátviteli alkalmazásokra optimalizált mobilhálózatokénál tízszer nagyobb sebességen. A GPRS adatátviteli sebessége egészen 115 kbit/s-ig terjed, és bármely típusú átvitelre alkalmazható, különösképpen nagy terjedelmű adatforgalom esetén.

Az előfizetők részére a GPRS a hang- és adatátviteli hívások egyidejű kezelésének lehetőségét kínálja. Az előfizetők a kapcsolati idő helyett az elküldött és fogadott bitek alapján élvezhetik az állandó összeköttetést, a gyors és egyszerű hozzáférést az olyan szolgáltatásokhoz, mint például az e-mailek "expressz" kézbesítése (nagy méretű csatolt fájlokkal, pl. grafikákkal), az Internetböngészés és a vállalati LAN-okhoz vagy intranetekhez való hozzáférés. A GPRS az előfizetőt a szolgáltatások igénybevételére buzdítja, aki nem érzi szükségét, hogy véget vessen az adatátviteli kapcsolatnak (amennyiben a hálózatüzemeltető nem számít fel külön díjat a kapcsolati időre).

A csomagkapcsolt GPRS technológia megjelenése előtt a GSM telefonok egy sokkal rosszabb hatásfokú, vonalkapcsolt megoldást használhattak és használnak jelenleg is. A hagyományos vonalkapcsolt adatátvitel során a telefon állandóan foglalja a beszélgetésre is használt csatornát az adott cellában, akkor is, ha éppen nincs semmilyen adatforgalom. A vonalkapcsolt technológiák között is léteznek olyan megoldások, melyek több csatorna használatával növelik az adatátviteli sebességet, tovább rontva ezt a bizonyos hatásfokot.

A GPRS ezzel ellentétben akkor és csak akkor foglal le egy-egy csatornát, amennyiben adatot küld vagy fogad. Ez azt jelenti, hogy ugyanazt a csatornát akár többen is használhatják időosztásos rendszerben akár a sebesség észrevehető csökkenése nélkül is, hiszen nem mindenki töltőget állományokat folyamatosan, s erre a felhasználási célra a GPRS nem is igazán alkalmas. Ez a csomagkapcsolt megoldás a hálózat terhelésének csökkenéséhez vezethet - hiszen mindenki csak addig foglal erőforrást, amíg feltétlenül szükséges- és sokkal költséghatékonyabb szolgáltatások kifejlesztését teszi lehetővé. Itt valóban igaz lehet a mondás: csak annyit fizetünk, amennyit használjuk.

A GPRS telefonok több csatornán képesek egy időben kommunikálni, ennek köszönhető a megnövekedett adatátviteli sebesség. A telefonok természetesen nem egy kaptafára készülnek: van olyan készülék, mely csak 3 csatornát támogat összesen, de van olyan is, amelyik akár 8 visszairányú és 8 letöltési csatornát is használhat. Van olyan telefon is, mely dinamikusan tudja változtatni a letöltésre és feltöltésre használható csatornák számát a rendelkezésre álló 5-ből. A telefonokat e képességük szerint osztályokba sorolják. Például az Ericsson R600-as telefon Class 8 minőségű, azaz 8-as osztályba sorolt, ami azt jelenti, hogy 4 letöltési és 1 feltöltési csatornát használhat maximálisan.

Ezeket a csatornákat a telefon dinamikusan kezeli, ami azt is jelentheti, hogy a GPRS adatátvitel mellett (akár a megszakítása nélkül) fogadhatunk és indíthatunk hívásokat.

Megkülönböztetünk A-B vagy C típusú telefont: az A típus párhuzamos telefonálást és GPRS adatátvitelt támogat, a B típusú telefon automatikusan vált a két mód között, míg a C típusúnál manuálisan kell kiválasztanunk a megfelelő üzemmódot.

Adatátviteli sebesség

Többfajta kódolási séma létezik. Például a Vodafone hálózata CS-2-es kódolási módszert támogat a legjobb körülmények között is, ezért a csatornánkénti adatátviteli sebesség maximálisan 13,4 kbit/s lehet. Amennyiben a térerő, a jelszint ezt a sebességet nem teszi lehetővé, a hálózat automatikusan visszavált a CS-1-es módszerre, így a csatornák csak 9,05 kbit/s-mal továbbítják az

adatokat. Ennek megfelelően elképzelhető a minimális 13400 bit/s sebességnél kisebb adatátviteli sebesség is.

Kódolási séma	CS-1	CS-2	CS-3	CS-4
Adat arány	$\frac{1}{2}$	$\sim \frac{2}{3}$	$\sim \frac{3}{4}$	$\frac{1}{1}$
Adatátvitel kbit/s	9,05 kbit/s	13,4 kbit/s	15,6 kbit/s	21,4
Maximális sebesség				
8 csatorna használatával kbit/s	171,2 kbit/s	72,4 kbit/s	107,2 kbit/s	124,8

A hálózat

Fontos megjegyezni: bár a GPRS adatok vételére és adására a hagyományos GSM adó-vevő csatornákat használják, maguk az adatok nem a beszélgetésekre és vonalkapcsolt adatátvitelre használt technológián jutnak el a szolgáltató központjába. A jövőbeni fejlesztések során elegendő csupán az adott cella, körzet csatornaszámát növelni, a technológia egyéb eszközei által nyújtott adatátviteli szolgáltatások bőven elegendőek lehetnek a megnövekedett forgalom bonyolítására.

A GSM hálózat alapját képező beszédcélra szánt csatornák (MSC) nem képesek a GPRS csomagkapcsolt hálózat, IP alapú csomagjait továbbítani. A GPRS szolgáltatáshoz telepíteni kell úgynevezett SGSN (Serving GPRS Support Node) hozzáférési pontokat, melyek lényegében csomagkapcsolt MSC-k, ezek az egységek fogadják a mobiltelefonok által küldött csomagokat, s a visszirányú csomagok adásáért is ezek az eszközök felelősek.

A hálózatban szükség van még GGSN (Gateway GPRS Support Node) eszközökre is, melyek a belső IP-hálózat csomagjait továbbítják az Internet felé, más mobilhálózatokba vagy vállalati intranetekbe. A GGSN eszközök kezelik a GPRS hálózatra feljelentkezett felhasználók elérési adatait és a csomagok visszajuttatásához szükséges információkat is.

A dinamikus kezelésnek, nyilvántartásnak köszönhetően akár utazás közben is zavartalanul internetezhetünk, WAP-olhatunk, egy jól beállított rendszer automatikusan követ minket egyik celláról a másikra.

A gyakorlat

A GSM hálózatok bővítésével és új mobil készülékek bevezetésével lehetővé válhatna, hogy a felhasználók 115 kbit/s sebességű adatkapcsolatot hozzassanak létre.

A mobil kommunikáció robbanásszerű terjedésével párhuzamosan nő az Internet használatának növekedése. A mobil felhasználók mozgás közben is igénylik az Internet szolgáltatásait, elektronikus levelezést, WAP vagy Web hozzáférést, de sokan szeretnének bekapcsolódni cégük Intranet hálózatába is. A GPRS lehetővé teszi ennek megvalósítását.

Mivel a GPRS csomagkapcsoláson alapul, ezért a felhasználónak csak a ténylegesen forgalmazott adatmennyiség után kell fizetnie, szemben a ma szokásos idő alapú számlázással. Ennek következtében a felhasználók állandóan kapcsolatban maradhatnak a hálózattal.

A GPRS mérőföldkönek számít a GSM hálózatok fejlődésében, a 3G hálózatok felé vezető úton.

Már használható különböző internetes alkalmazásokhoz, de a mobil internetes piaci szegmens várható, éves 100-150%-os fejlődési ütemét a GPRS sem tudja sokáig kiszolgálni.

A következő lépcső az EDGE nagysebességű modulációs technológia és a GPRS ötvözése lesz, mely akár 384 kbit/s sebességű hozzáférést tesz majd lehetővé - mindezt a ma kialakított hálózati infrastruktúrán.

Összegzés

Amit a GPRS-től várhatunk, és amit nem (pingek, sebességek)

A GPRS egy olyan technika, ami csomagkapcsolt adatátvitelt valósít meg GSM rendszereken.

A csomagkapcsolt működésből adódik, hogy csatornát csak akkor foglal, amikor valamelyik fél adatot kíván küldeni. Hagyományos GSM telefonrendszereknél a GPRS a beszéd által kihasználatlan csatornákat veszi igénybe, de azt tudnunk kell, hogy a beszédforgalomnak prioritása van, azaz a beszédforgalom a GPRS által használt csatornát elveheti.

A GPRS rendszeren az adatok kódolva közlekednek. Négyféle GPRS kódolási séma létezik: CS-1, CS-2, CS-3 és CS-4 (Coding Scheme). Ezek rendre 9.05, 13.4, 15.6 és 21.4 kbit/s sebességet támogatnak egy-egy kapcsolatra. Ez így első hallásra kevésnek tűnhet, azonban a GPRS telefonok nem egy, hanem több kapcsolatot tudnak egyszerre kezelni, így az átviteli sebesség is ezek többszöröse lesz. Az átlagos GPRS telefonok 3 kapcsolatot használnak lefelé, és 1-et felfelé irányba, ezeket szokás "3+1 -es GPRS telefon"-nak is emlegetni.

A komolyabb készülékek 4+1 vagy még több kapcsolatot is kezelhetnek, sőt van olyan is, amelyik dinamikusan határozza meg a lefelé és felfelé irányú kapcsolatok számát.

Az a szolgáltató, amelyik a CS-2 sémát használja(pl.: Vodafone), ennek megfelelően kb. 40.2 kbit/s lefelé és 13.4 kbit/s felfelé irányú sebesség érhető el egy átlagos ("3+1 GPRS") telefonnal.

A csomagkapcsolt működésből adódnak a GPRS adatátvitel további sajátosságai. Amikor adatot akarunk küldeni, akkor először fel kell építenie egy kapcsolatot, le kell foglalnia egy csatornát, aztán mehet az adat.

- szembetűnő, hogy viszonylag hosszúak a pingek GPRS-en keresztül, pl. a Vodafone hálózatán gyakorlati tapasztalat alapján 500ms körüli az alsó határ.
- Egy másik sajátos jelenség a sebesség "felpörgése", azaz amikor egy állomány (weblap) letöltésébe kezdünk úgy, hogy előtte nem volt forgalom, először nagyon lassan indul meg (szintén a csatornafoglalások miatt), de utána - ha van elég szabad csatorna - begyorsul.
- További eltérés a vezetékes adatkapcsolatoktól, hogy a sebesség nem állandó. Ez azt jelenti, hogy az adott GSM cella vonzaskörzetében folyó telefonbeszélgetések és GPRS-t használók számától függően hol több, hol kevesebb szabad csatornát kaphatunk, így a sebesség - főleg egy leterhelt cellában, csúcsidőben - elég erőteljesen ingadozhat.
- Szintén eltérés a vezetékes adatátvitelhez képest, hogy a sebesség általában aszimmetrikus. Ez persze telefontól függ, de a készülékek döntő többsége felfelé irányban kevesebb kapcsolatot támogat. Ez a gyakorlatban nem szokott hátrányt jelenteni (a kábeles és ADSL Internet-hozzáférések is aszimmetrikusak.)

Mire is alkalmazható akkor a GPRS?

Összegezve tehát átlagos felhasználásra, weblapok olvasására, levelezésre, csevegésre, kisebb állományok letöltésére, általánosságban olyan dolgokra, ahol nincs folyamatos, nagy mennyiségű adatforgalom. Ezekre viszont folyamatos kapcsolat mellett alkalmas. Nem alkalmas viszont hálózati akciójátékokra, nagy méretű file-ok (pl. teljes CD-k) letöltésére, illetve olyan alkalmazásokra, amiknek használata közben az adatátviteli sebesség ingadozása problémát jelenthet.

INFOKOMMUNIKÁCIÓS SZOLGÁLTATÁSOK ÉS A BIZTONSÁG

Napjaink egyik legfontosabb kérdése a biztonság. Az előadás kétféle aspektusból vizsgálja ezt a kérdéskört.

- Hogyan segíthetik az infokommunikációs szolgáltatások a biztonsági problémák megoldását, kezelését. Ezen a területen kiemelten fontos a terület-, a vagyon- és gépjárművédelem, az személyazonosítás és beléptető rendszerek. Ma már a hagyományos megoldások mellett speciális, a legmodernebb informatikai megoldásokon alapuló, úgy nevezett infokommunikációs szolgáltatások állnak rendelkezésre.
- Napjaink másik legnagyobb problémája informatikai rendszereink, adataink védelme, a hiteles és elektronikus úton megvalósított kommunikáció és dokumentumcsere

A nyílt hálózati alapú rendszerek, megoldások terjedésével egyre komolyabb problémákkal kell megküzdeni a felhasználóknak. A biztonság olyan alapvető kérdéseire kell választ adni, mint:

- Az azonosíthatóság,
- A titkosság,
- Az integritás megőrzése és
- A letagadhatatlanság kérdése

Az előadásban bemutatjuk a Publikus Kulcsú Infrastruktúrát (PKI), mint a fenti kérdések re adott választ, műszaki megoldást. A PKI-n alapuló Hitelesítési szolgáltatások lehetőséget adnak a digitális aláírás megvalósítására, a nyílt hálózatokon megvalósítható és biztonságos titkosító és aláíró kulcsok kezelésére.

A Hitelesítési szolgáltatáson kívül még szó lesz szerver tanúsítványról és alkalmazási területeiről valamint az „erős autentikáció” vagy másnéven „egyszeri jelszó” alkalmazásáról, mint a felhasználói azonosítás egyik lehetséges és egyszerűen megvalósítható megoldásáról.

**A RENDSZERINTEGRÁCIÓ ÉS A KAPSCH SZEREPE A
KORSZERŰ KOMMUNIKÁCIÓS RENDSZEREK
KIALAKÍTÁSÁBAN**

Kapsch TeleCom Kft.



**A rendszerintegráció és a Kapsch
szerepe a korszerű kommunikációs
rendszerek kialakításában**

Szabó Zoltán

ágazatvezető – adatkommunikációs rendszerek
zoltan.szabo@kapsch.net

KOMMUNIKÁCIÓ 2003 – 2003. október 15.

Kapsch TeleCom Kft.



Tartalom

- > Rendszerintegráció – miért is van erre szükség?
- > Végeztünk egy felmérést...
avagy, példák az informatikusokat, cégvezetőket foglalkoztató problémák megoldásaira.
- > Miért a Kapsch?

Kommunikáció = közlés, információ csere

Szóban	Élő szóban	
Írásban	Postai levelezés	
Gesztusok	Morze	
Egyéb jelek	Telefon	Telekommunikáció
	E-mail	
	Chat (csevegés)	Adatkommunikáció
	Internet	

Emberek vagy számítógépek között

Kommunikáció = közlés, információ csere

Szóban	Élő szóban	
Írásban	Postai levelezés	
Gesztusok	Morze	
Egyéb jelek	Telefon	Egységes, integrált kommunikációs rendszer
	E-mail	
	Chat (csevegés)	
	Internet	

Emberek vagy számítógépek között

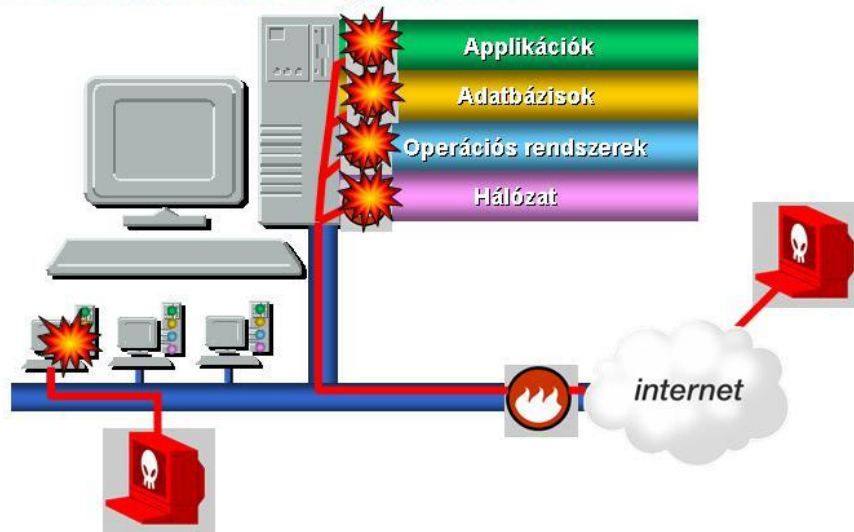
Rendszerintegráció – miért is van erre szükség?



Végeztünk egy felmérést...



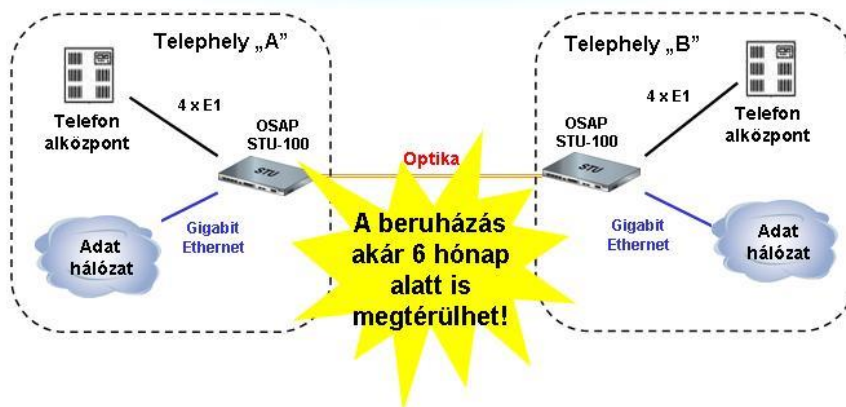
A hálózatsbiztonság kérdése



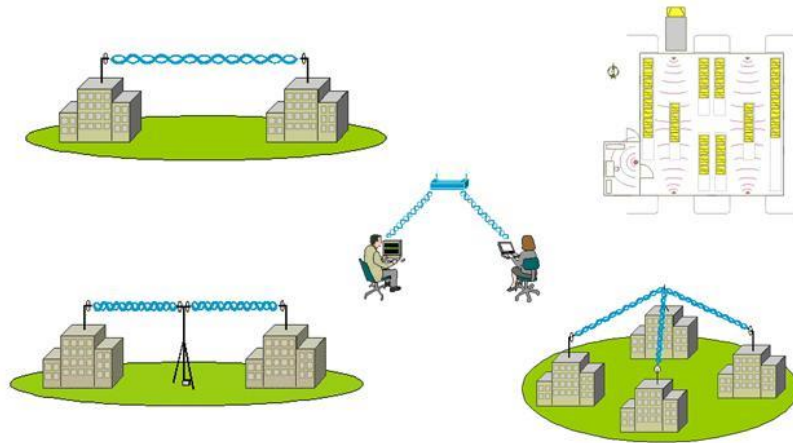
**Mivel lehet még kiváltani
a költséges és lassú bérelt vonalakat?**

Appian – OSAP

Optical Services Activation Platform



Mobilitás – hálózat vezeték nélkül



Tartalom

- > Rendszerintegráció – miért is van erre szükség?
- > Végeztünk egy felmérést...
avagy, példák az informatikusokat, cégvezetőket foglalkoztató problémák megoldásaira.
- > Miért a Kapsch?

Kiemelt partnerkapcsolataink



> Kapsch Bécs – Cisco Silver Partner

- > *VPN/Security specializáció*
- > *Wireless LAN specializáció*
- > *hamarosan routing&switching specializáció*
- > *hamarosan Network Management specializáció*
- > *hamarosan IP Telephony specializáció*

> Kapsch Bp.– hamarosan Cisco Premier Partner

- > *hamarosan Wireless specializáció*

Kiemelt partnerkapcsolataink



> Kapsch Budapest

- > *LAN Gold Solutions Partner*
- > *Corporate WAN Solutions Partner*
- > *IP Telephony Solutions Partner*
- > *PP8600 Gold Product Partner*
- > *PP6000/7000 Product Partner*
- > *PP4000 Product Partner*
- > *Alteon Product Partner*
- > *Optical Solutions Partner*
- > *Carrier Data Products Partner*

Célunk: Ügyfeleink teljes körű kiszolgálása

- > Képzett szakembergárda
- > 0-24 műszaki támogatás
- > Tapasztalat, referenciák
- > Megbízható
partnerkapcsolatok



Milyen előnyöket élvezhetnek ügyfeleink?

- > **Egységes, homogén** megoldások
egy szállítótól - rendszerintegráció
- > Szoros gyártói kapcsolatok
- > Teljes körű szolgáltatások



Köszönöm a figyelmet!

Szabó Zoltán

ágazatvezető – adatkommunikációs rendszerek

zoltan.szabo@kapsch.net

AZ ÚJ TÍPUSÚ HADERŐ ÉS A SÚLYPONT-ÁTRENDEZŐDÉS KÉRDÉSEI A TECHNIKAI STRUKTÚRÁBAN

A Magyar Honvédségben jelenleg zajló folyamatok és a politikai akarat által deklarált hivatásos haderőre történő átállás megköveteli, hogy az új eszközök beszerzése során a „szükséges és elégséges” elv betartása mellett a lehető legjobb, a költséghatékonyság szempontjai mellett a katona hatékonyságát – feladatmegoldó-képességét – legjobban elősegítő eszközök és rendszerek kerüljenek alkalmazásra.

NATO tagságunkból adódóan a kompatibilitás kérdései mellett távolabbi célként figyelembe kell venni az interoperabilitás feltételrendszerének kialakítását is, mely kérdésekkel jelenleg részletesen nem kívánok foglalkozni.

A haderő átalakításának – a katona szemüvegén át – elsősorban a szervezeti és technikai oldala a fontos, mely erősen összefügg a várható feladatok jellegével, nagyságrendjével, helyszínével, a barát vagy a feltételezett ellenség lehetőségeivel, képességeivel. A korábbi elképzelések szerint a Magyar Honvédség csökkenő létszáma mellett elsősorban az ország határainak, területi integritásának, szuverenitásának védelmére kellett felkészülni, bár a hiányzó ellenségkép mellett igen nehezen lehetett a konkrét – és a valósághoz igazodó – feladatrendszert kitalálni. Alapvetően az ország határain belüli feladatokra kellett koncentrálni. Az új elképzelések kimondottan nagy hangsúlyt fektetnek arra, hogy a Magyar Köztársaság védelme az ország határain túl, jelentős földrajzi távolságokra is kiterjed, a szövetségi elvárásoknak is megfelelően¹⁶².

A feladatokban bekövetkező súlyponteltolódás magától adja a kérdést, hogy létérdekünk megvizsgálni azt, hogy milyen szervezetekre és milyen fegyverzettechnikai lehetőségekre, képességekre van szükségünk. A szükséges állománystruktúra kidolgozása és kialakítása folyamatban van. A technikai oldalt tekintve azt kell mondanom, hogy a jelen és jövő háborúinak, harcainak sikeres megvívását a pontos és hiteles valós idejű információ hatékony felhasználása alapvetően fogja meghatározni. Az információs és az informatikai hadviselés eszközzrendszere sok esetben már előre determinálhatja a csapatok sikerességét, vagy az esetleges sikertelenséget. A siker kiemelten fontos részévé válik a minél alacsonyabb személyi veszteség, hiszen a drágán és jól kiképzett, kis létszámú hivatásos hadsereg esetén, különösen külföldön az ember nehezen pótolható. Amennyiben megvizsgáljuk ennek belpolitikai hatásait is, akkor még jobban belátható a fenti elvárás kiemelése, hiszen pártok vagy kor-

162 „A kabinet által elfogadott haderőstruktúra biztosítja, hogy a magyar katona a világ bármely pontján, de mindekelőtt az ország védelmére bevethető, jól felszerelt és képes legyen együttműködni a NATO-tagállamok valamint az Európai Unió haderejének katonáival - mondta a honvédelmi miniszter.” (www.honvedelem.hu/cikk.php?cikk=14241)

mányok buktak bele a világ más országaiban is egy-egy nagyobb veszteségbe – különösen, ha nem volt a harc sikeres.

A továbbiakban vizsgáljuk meg a híradó katona szemszögéből a lehetőségek és követelmények rendszerét. Az információ hatalom volt korábban is, – azok számára, akik élni tudtak vele –, de napjainkban, az információs forradalom napjaiban stratégiai jelentőséggel bír. Ebből az is következik, hogy az információ továbbítására alkalmas eszközrendszer minősége meghatározóvá vált. Az időtényező radikális csökkenése nem engedi meg, hogy az információs csatornak akár technikai problémák, akár ellenséges elektronikai tevékenység, akár saját katonáink kiképzetlensége miatt lassan, vagy akár egyáltalán ne működjenek, hiszen ez katonák, vagy katasztrófavédelem esetén civilek életébe kerülhet.

A jelenlegi analóg technikai struktúra az új feltételeknek képtelen eleget tenni. A mai kor műszaki-technikai lehetőségeinek ismeretében a rendszer hatékonyságáról még beszélni is értelmetlen, akár sugárzó, akár vezetékes rendszerről beszélünk. A ténylegesen rendszeresített eszközparkunk tekintetében csak kényszerpályás megoldások léteznek, mert többek között például valódi zavarálló mobil eszközünk a tábori rendszerek esetén – ahol pedig kiemelten létfontosságú lenne – nincs. Ráadásul igen sok eszközünk „képes” jelentős ön- és kölcsönös zavarást okozni, – analóg rádiók jelentős része ilyen –, mely csak manuális technikai, illetve szervezési módszerekkel csökkenthető. Tudomásul kell venni, hogy az információ átvitelére alkalmazott, a „morzézástól” eltekintve alapvetően analóg beszédátvitelre korlátozott eszközeink döntő többségén túlhaladt az idő, műszakilag, katonailag és erkölcsileg leamortizálódtak, sok esetben csak papíron működőképesek, illetve hadrafoghatóak. Ezt szépen úgy szoktuk fogalmazni, hogy: „elérkeztek teljesítőképességük végső határához”. Az én megítélésem szerint jó néhány évvel már azon is túl vannak, hiszen nem véletlen az, hogy nem ez a régi technikai eszközpark került alkalmazásra a külföldi katonai misszióink esetén. Az sem véletlen, hogy a honvédség közreműködésével zajló katasztrófavédelmi feladatoknál – pld. a tiszai, vagy a dunai árvizek esetén – katonáink a saját mobiltelefonjaikat használták, – persze a lefedettség függvényében –, mint az egyik legmegbízhatóbb eszközt. Sok esetben nem voltunk képesek saját eszközeinkkel az együttműködő katasztrófavédelmi és más erőkkal kapcsolattartásra, csak kölcsön rádiókészülékekkel. A mobiltelefon tömeges alkalmazása katonáink körében rögtön felvet egy logikus gondolatot: olyan eszközökkel kell ellátni őket, hogy bárki, – legyen az honvéd vagy tábornok, tüzér, gépesített lövész, vagy akár híradó szakember –, külön kiképzés nélkül is azonnal képes legyen az új típusú eszközök kezelésére. Ennek egy alapvető feltétele az, hogy közel ugyanolyan jellegű kezelési és szolgáltatási lehetőségek legyenek beleépítve, mint ami a „civil eszközök” esetén megszokott.

A korábbi elképzelések szerint az az elvárás alakult ki, hogy a katona a napi munkakörnyezetéből kiszakadva tábori körülmények között is ugyanolyan lehetőségekkel rendelkezzen, mint korábban. Ez, ha jól végiggondoljuk valóban ideális lenne, de:

- Az „irodai” eszközök alkalmasak-e terepen való szállításra és a katonai szabványok által előírt elvárások biztosítására?
- A szükséges infrastruktúra kiépítésére – pld. az épületen vagy béke-elhelyezési körleten belüli telefonhálózat, számítógépes infrastruktúra tábori kiépítésére van-e lehetőség (anyag, eszköz, idő, szakemberlétszám)?
- Biztos, hogy ragaszkodnunk kell az egyenrangú feltételek megteremtéséhez a megváltozott napi élet és a megváltozott napi feladatok mellett?
- Olcsó ez így?

A válaszom egyértelműen NEM. Véleményem szerint az új technikai megoldások következtében kimutatható egy olyan tendencia, hogy a tábori rendszerekben a sugárzó eszközök – és elsősorban a rádiók, vagy a vezeték nélküli informatikai rendszerek – szerepe ugrásszerűen megnő, míg a hagyományos vezetékes, valamint vivőáramú technikára alapuló csoportképzési eljárások, modemes adatátviteli rendszerek és megoldások háttérbe szorulnak, ezért megfontolás tárgyát kellene képeznie a következő elveknek:

1. **Külön kell választani** az anyaországban és külföldi katonai missziók esetén várható feladatokat.
2. A kétféle, sok ponton jól elkülöníthető feladatoknak megfelelően kell a műszaki-technikai képességeket kialakítani – a „képesség alapú haderő” elve így is igaz.
3. Az emberi tényező esetén nem szabad eltérő kiképzést alkalmazni, tehát megmarad a lehetőség a rotációra.
4. Az **anyaországban** törekedni kell:
 - a. olyan **közös híradó és informatikai struktúra** kiépítésére, mely kis beruházási és fenntartási költséggel jár,
 - b. nem kell feltétlenül **önálló, országos szintű** honvédségi kommunikációs infrastruktúra, hanem támaszkodni kell a biztonsági szempontból (is) minősített civil szolgáltatók hálózataira, hiszen műszaki lehetőségeik messze meghaladják jelenlegi és valószínűleg hosszabb távú igényeinket is,
 - c. elsődlegesnek kell tekinteni a polgári szolgáltatók által a – vonatkozó törvényi előírásokban¹⁶³ is rögzített – csatlakozási feltételek (mind a **műszaki**, mind a **szervezési, együttműködési** oldalát tekintve) kialakítását,

¹⁶³ 2001. évi XL. törvény a hírközlésről; 50/1998. (III. 27.) Kormányrendelet a zártcélú távközlő hálózatokról

-
- d. a külföldi katonai missziókkal történő stabil, műszakilag magas színvonalú **kommunikációs rendszer**¹⁶⁴ kialakítása, mely alapvetően műholdas összeköttetéseken alapul, meghagyva a vezetékes rendszerekkel történő elérési lehetőséget is, bár ennek alkalmazása a földrajzi viszonyok és az információ védeltségének függvénye,
- e. katonai szövetségeseink rendszereihez való kapcsolódásban törekedni kell valamennyi síkon történő együttműködésre a kompatibilitás és interoperabilitás szempontjainak figyelembevételével – pld. szabványos interfész-felületek kialakításában (STANAG),
- f. a sugárzó eszközök esetében törekedni kell olyan eszközök beszerzésére, mellyel alkalmasak vagyunk felcsatlakozni más szervezetek rendszereire, az együttműködés érdekében, katasztrófavédelmi feladatok végrehajtására (mentők, tűzoltók, rendőrség, katasztrófavédelmi szervezetek, polgármesteri hivatalok, részt vevő repülő erők, stb.) – valamennyi érintett féllel együttműködve – pld. itt is közös interfészfelületek kialakítása valamennyi érintett szervezetnél, mely elősegíti a közös platform létrejöttét
- g. az olcsóbb és hatékony kiképzés érdekében valamennyi fegyvernem esetén biztosítani kell a legkorszerűbb szimulációs rendszerek alkalmazását, mely természetesen akár egy törzsvezetési gyakorlat, vagy hadijáték számítógépes modellezése is lehet
- h. nem feltétlenül szükséges a legújabb generációs eszközök beszerzése és rendszeresítése, de:
- műszakilag hátrányos helyzetbe nem szabad kerülni sem a szövetségesek, sem az együttműködő szervezetek, sem a polgári szolgáltatókhoz való felcsatlakozási lehetőségek szempontjából
 - mindenképpen el kell mozdulni az analóg technikától a spektrumkiterjesztéses rendszerek irányába
 - a rádió eszközök legyenek alkalmasak szoftveres feltöltéssel bármelyik sáv használatára, vagy eleve legyenek szélessávúak
 - az eszközök legyenek alkalmasak a külföldön feladatot végrehajtó katonáknál lévő eszközökkel való együttműködésre, **kezelésük** csak minimális mértékben térhet el azokétól
- i. kitelepüléskor legyen meg a képességünk vezetékes rendszerek alkalmazása nélkül azonnal tábori kommunikációs rendszer működtetésére vezetékek nélküli tábori távbeszélő rendszerek és katonai minősítésű WLAN-ok alkalmazásával
- j. mobil rádiófelvevőpontok rendszerével valamint mobil digitális mikrohullámú átjátszóállomásokkal legyünk képesek bármilyen információ azonnali átvitelére viszonylag kisebb távolságokon – többek között a rej-

¹⁶⁴ közös híradó és informatikai rendszer

-
- tettség érdekében – és a polgári szolgáltatók rendszerét felhasználva a jelek továbbítására
- k. szükség esetére néhány védett üzemmódú nagyobb hatótávolságú rádió-eszköz üzemeltetésével legyünk képesek a kieső szolgáltatók vonalait a szükségüzem elvárásainak megfelelően pótolni
 - l. eszközeink legyenek képesek adaptív teljesítmény-szabályzásra
 - m. a minőségi összeköttetések megvalósítása érdekében törekedni kell a tér-informatika, ezen belül a digitális terepmodellezés, a digitális térképi adatbázisok eszközrendszerére alapuló tervezési eljárások preferálására
 - n. valamennyi eszköz és rendszer legyen alkalmas egyéni, illetve csoportos információvédelmi megoldásra
 - o. a felhasználónak teljesen mindegy, hogy informatikai eszközön ill. hálózaton, vagy a hagyományos értelemben vett távközlő hálózaton továbbítja az információt – a nála lévő készülék legyen képes akár beszéd, akár – a szükséges sávszélesség technikai hátterének biztosításával – gyors adatátvitelre
 - p. az adatátvitel során célszerű törekedni a rövid, gyors üzenetküldő rendszerek alkalmazására, mely kellően sávszélesség takarékos és védett az felderítés és zavarás ellen is
 - q. ahol a vezetékes megoldások nem kerülhetők el, ott tábori kivitelű optikai kábelek legyenek rendszeresítve
 - r. a nem kézi sugárzó eszközök esetén valamennyi műszakilag megvalósítható esetben legyen az állomástól az antennarendszer alkalmas 300÷500m távolságra való letelepítésre, – minimális személyzettel –, lehetőleg a nagyfrekvenciás teljesítményfokozat antennalábhöz történő ki-telepítésével
 - s. a mobil eszközök olyan mértékben kerüljenek csak automatizálásra, hogy hiba esetén az automatika kiváltható legyen kézi módszerekkel, de minimális kezelői állomány legyen csak szükséges
 - t. a hordozóeszközöknél nem elsődleges a páncélvédett járművek alkalmazása, ezzel szemben a könnyű, gyors, túlnyomósos, vegyi és biológiai behatásoknak ellenálló terepjáró eszközök rendszeresítése a célszerű
 - u. az ország határain belül is fontos szerepet kell szánni a különböző felderítő, adatgyűjtő és továbbító szondáknak, robotoknak, melyek elsősorban katasztrófavédelmi, terror-elhárítási esetekben kaphatnak kiemelt jelentőséget. Pld. nukleáris-, vagy vegyi baleset, belvíz feltérképezése, eltűnt személyek, vagy esetlegesen diverzáns csoportok, terroristák felkutatása, stb.
5. **Külföldön** feladatot végrehajtó alakulatok esetén:
- a. hasonlóan a hazai rendszerekhez, de a képességek tekintetében azt meghaladó technikai szint biztosítása

-
- a spektrum-kiterjesztéses rendszerek esetén legyenek alkalmasak azok kombinált működtetésére
 - a helyi infrastrukturális viszonyoktól független képességekkel és lehetőségekkel rendelkezzen, természetesen a szövetségi rendszerekhez való kapcsolódások mellett
 - a felderítés kiemelt jelentőségűvé válik a saját és a szövetséges erők megóvása érdekében, ahol a robothadviselés eszközszerkezere döntően befolyásolja a csapatok működőképességét, hatékonyságát
 - a páncélvédett de nagy mozgékonyaságú – pld. gumikerekes – eszközök alkalmazása szükségszerű
 - a rendkívül szélsőséges klimatikus viszonyoknak is ellenálló eszközök iránti igény meg fog nőni, hiszen a korábbi elvárások és a hozzájuk kapcsolódó katonai szabványok korábban nem igényelték azt, hogy akár a sarkkörön, akár a trópusokon, vagy sivatagi viszonyok között, esetleg tengereken, vagy a légiszállítás különleges körülményeinek is megfelelően – az igen bonyolult automatikával ellátott, ezért viszonylag érzékeny – a berendezéseink megőrizték működőképességüket
 - a védettség fokozása érdekében új típusú álcázórendszerek alkalmazása – pld. járművek termikus sugárzásának a rejtése, stb.
 - barát-ellenség felismerő rendszerek és eszközök alkalmazása nem csak a légierő, hanem a harc- és gépjárművek, majd a távolabbi jövőben az egyes katona vonatkozásában is¹⁶⁵, valamint speciális adatok továbbítására alkalmas technikai megoldások az erők és eszközök állapotáról
 - a GPS rendszer felhasználása
 - egyéni segélyhívó, vészjelző automaták, rádiók rendszeresítése
 - a gyors helyzetváltozások és a kapcsolódó helyváltoztatások dinamikáját lekövetni képes kommunikációs rendszer működtetése

Az általam gondolatébresztőnek szánt szempontok megfontolását mindenképpen javaslom a döntési helyzetben lévőknek, hiszen ezen feltételek megvalósításán is múlik az, hogy mennyire hatékony a magyar katona és milyen esélye van különleges körülmények között a túlélésre.

¹⁶⁵ Károly Fekete: Personal military communications system, Kommunikáció 2002 Nemzetközi szakmai tudományos konferencia, ZMNE, ISBN 963 86229 2 X

Dr SZÜCS Gáspár

**A MAGYAR HONVÉDSÉG INFORMATIKAI HELYZETE,
FEJLESZTÉSI TERVEI, PROBLÉMÁI**

**A Magyar Honvédség
informatikai helyzete,
fejlesztési tervei, problémái**

Dr. Szűcs Gáspár mk. ezredes
HM HVK HÍRCSFH

Fejlesztési időszakok

- **1999-2003: a NATO tagsághoz szükséges minimum, az informatikai infrastruktúra és rendszerek felső- és középső vezetési szinten történő kialakítása,**
- **2004-2005: az állandó informatikai rendszer kiterjesztése a csapattagozat irányába**
- **2004: a tábori informatikai rendszer kialakításának megkezdése**
- **2006 után: a rendszerépítés befejezése, fenntartás, továbbfejlesztés**

Hálózaton, vagy lokálisan működő informatikai rendszerek

- **Felderítő alrendszer**
- **HKSZ rendszer**
- **Irodaautomatizálási rendszer**
- **Állománytábla karbantartó rendszer**
- **Erőforrás megjelenítő rendszer (HKSZ-hez kapcsolódik)**
- **CFE, CSBM megjelenítő (Felderítő alrendszerhez kapcsolódik)**
- **Dokumentum-kezelő**
- **Katonai meteorológiai rendszer**
- **Vegyisugár helyzet értékelő információs rendszer**

Hálózaton, vagy lokálisan működő informatikai rendszerek

- Közlekedési Információs rendszer
- Légierő Informatikai Vezetési Rendszere
- Légierő Repüléstervező és Nyilvántartó Rendszere
- MH Egészségvédelmi Intézet rendszere
- Drog Prevenációs rendszer
- Költségvetési és Gazdálkodási Informatikai Rendszer (KGIR)
- Logisztikai jelentő rendszer
- NATO rendszerek
- Tábori rendszerek

A NATO rendszerekkel való együttműködés biztosítása érdekében elvégzendő legfontosabb feladatok:

- A NATO Irodáautomatizálási Rendszer (NIAR) további fejlesztése és a rendszer üzemeltetése
- Számítógép alapú adatszolgáltatás kialakítása a NATO központi hadrend-hadrafoghatósági adatbázisba (ORBAT)
- Csatlakozás a NATO légierő vezetési és légi helyzet nyilvántartási informatikai rendszerhez, a meglévő légierő rendszerek továbbfejlesztése (ICC)
- A Nemzeti Befogadó Támogatás informatikai rendszer kiépítésének szakmai felügyelete, csatlakozás a NATO haderő felvonulási informatikai adatbázishoz (ADAMS), a hazai adatbázis létrehozása.
- NATO felderítő rendszer üzemeltetése (BISEC)

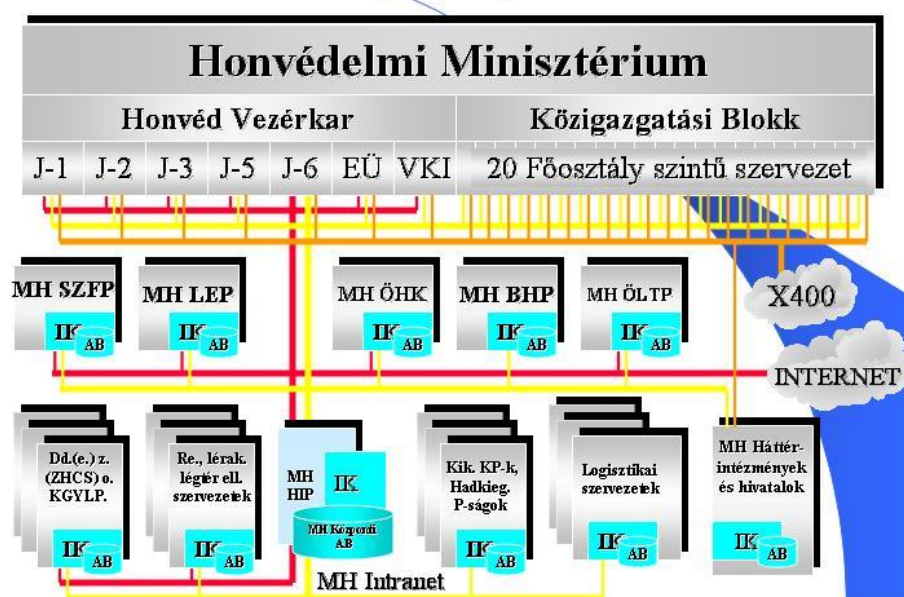
Tábori informatikai rendszerek

- A Magyar Honvédség nem rendelkezik tábori kivitelű, szélsőséges körülményeket tűrő informatikai eszközökkel, számítógépekkel.
- A katonai törzsek az általuk stacionáris körülmények között is használt asztali vagy laptop kivitelű számítógépeiket használják tábori környezetben, amely igen sok meghibásodásra ad(hat) alkalmat.
- A számítógépek nagy távolságot áthidaló összekapcsolása (több mint 1000 méter) nem megoldott, a rendszeresített híradó eszközök túlnyomó része erre nem alkalmas. Az összeköttetést kísérleti jelleggel mikrohullámú átjátszók segítségével egyes gyakorlatokon már létrehozták.

- A Magyar Honvédség rendelkezik jóváhagyott informatikai stratégiával.
- Részletes helyzetfelmérést és elemzést követően az HÍRICSF-ség kidolgozta és a HM Kollégium számára felterjesztette a Magyar Honvédség hosszú távú informatikai fejlesztési elgondolását, amelyet a kollégium elfogadott.
- A fejlesztési tervek évenként pontosításra kerülnek.

A Híradó és Informatikai Csoportfőnökség kiemelt feladatának tekinti a Magyar Honvédség átfogó, egységes informatikai rendszerének megteremtését, amelynek technikai alapját az MH nagytávolságú adatátviteli gerinchálózata (transzport hálózat) fogja képezni.

Az MH vezetési-irányítási rendszere technikai hátterének logikai kapcsolati vázlata



A HÍRICSF-ség legfontosabb feladatai a Magyar Honvédség informatikai rendszere kiépítésének vonatkozásában

1. Az MH zártcélú szolgálati használatú Intranet hálózatának kiépítése, a hálózati operációs rendszer és a közös használatú szoftverek alkalmazásba vételének előkészítése
2. Az MH zártcélú, titkos minősítésű Intranet és NATO hálózatának kiépítése, a hálózati operációs rendszer és a közös használatú szoftverek alkalmazásba vételének előkészítése
3. Az MH szervezeteinek csatlakoztatása a nyilvános Internet hálózathoz az MH Internet alhálózatán keresztül
4. Az MH videokonferencia rendszerének kiépítése
5. A nagytávolságú honvédségi adatátviteli gerinchálózat (transzport hálózat) aktív elemeinek rendszerbeállítása

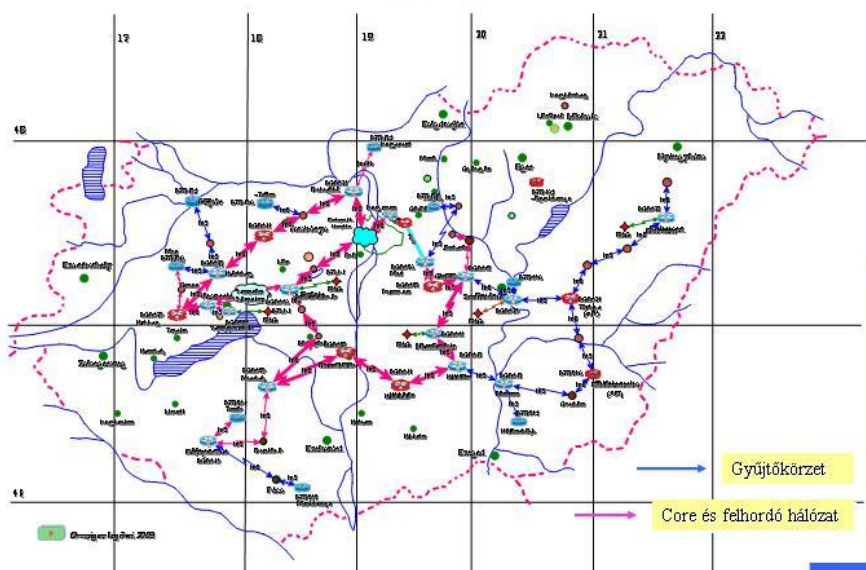
Az Intranet hálózat kiépítésének legfontosabb feladatai

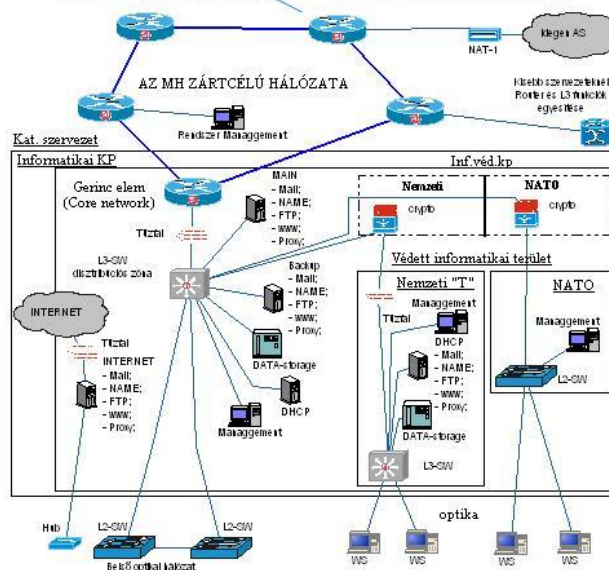
1. A hálózatvezérlő és felügyeleti rendszer kiépítése
2. Egységes felhasználói kezelői felület megteremtése
3. Az elektronikus aláírás (PKI) bevezetés feltételrendszerének megteremtése
4. Elektronikus levelező, valamint dokumentum- és üzenetkezelő rendszer üzembeállítása, a katonai szervezetek WEB, levelező és fájlszervereinek telepítése és alkalmazásba vétele
5. Az MH különálló informatikai rendszereiben tárolt adatok tartalmának, struktúrájának és kódolásának egységesítése, a NATO adatmodellel harmonizáló egységes MH adatmodell kidolgozása
6. Katonai célú informatikai alkalmazások fejlesztése

Jelenleg folyó feladataink

- Az MH szolgálati célú Intranet hálózat hardver és szoftver elemeinek üzembe helyezése, az alkalmazásba vétel megszervezése.
- Az alakulatoknál a strukturált helyi számítógép-hálózatok kiépítésének folytatása (jelenleg kiépítve 15 helyszínen, 2004 végéig újabb 17 helyszínen, majd a fennmaradó összes objektumban)
- A nyilvános Internet hálózathoz való csatlakozás kapcsolódási pontjainak bővítése, a sávszélesség növelése.
- A HM objektumok informatikai üzemeltetési szervezeteinek létrehozása
- Az MH Országos Rendszer Felügyeleti Központ informatikai felügyeleti feladatokkal és beosztásokkal történő bővítése
- További katonai szervezetek bekapcsolása az MH nagytávolságú informatikai (transzport) gerinchálózatába

AZ MH ADATÁTVITELI (TRANSPORT) HÁLÓZATA





Problémák: (1)

Az informatikai rendszerek üzemeltetésére a katonai szervezetek jelentős részénél nincs rendszerezített szakállomány

A nagytávolságú gerinchálózat és a rá épülő Intranet hálózat üzemeltetésére, valamint a rendszerfelügyeleti feladatok ellátására irányuló képzés lassan halad

A digitális (IP alapú) titkosító eszközök hazai akkreditációjának elmaradása lehetetlenné teszi minősített adatok továbbítását számítógépek között

Az egyes csoportfőnökségek, alakulatok, háttérintézmények egymástól függetlenül fejlesztik informatikai alkalmazásait, amely jelentős mértékben akadályozza a rendszerek együttműködését és az egységes honvédségi szintű informatikai hálózatba való integrálásukat.

Problémák: (2)

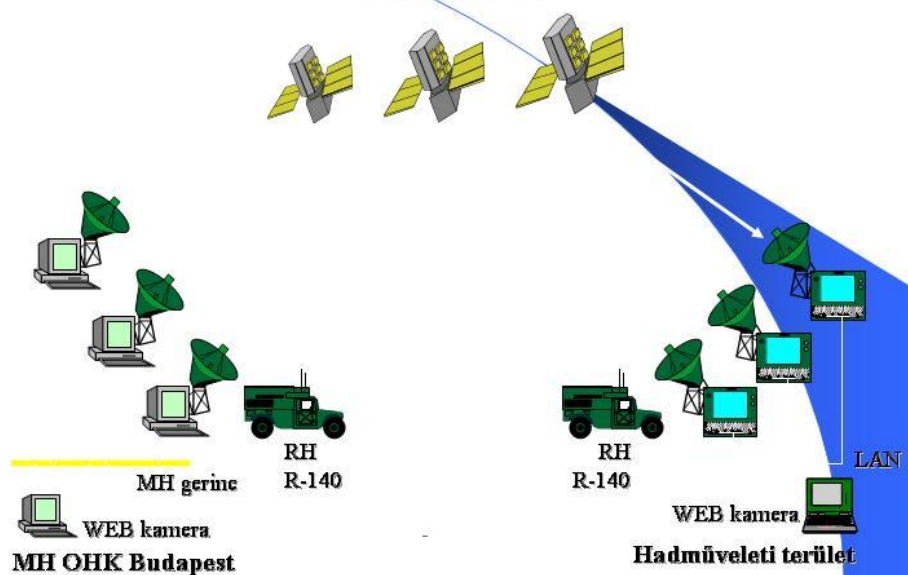
Az informatikai szakirányítás nem érvényesül hatékonyan:

Az alakulatok, katonai szervezetek a beszerzéseknél, gyakran az előírások és szolgálati út megkerülésével szereznek be informatikai eszközöket, szoftvereket, az önállóan fejlesztéseiknél sok esetben nem egyeztetnek a felsőbb szakmai szervezetekkel

Az informatikai beosztások feltöltését, az informatikai állomány mozgatását számos esetben a kamarai jogkört gyakorló megkerülésével, annak tudta nélkül hajtják végre.

Eltérő jogi értelmezés miatt a HM Informatikai és Hírközlési Főosztállyal rendszeresen a hatásköri viták, amely negatív hatást gyakorol a szakmai munkára.

Példa egy AD-HOC informatikai-híradó támogatásra



INFORMÁCIÓ SZOLGÁLTATÁS ÉS VÉDELEM A MINDENNAPI MUNKÁBAN

Bevezetés

A távbeszélő szolgáltatók elsősorban piaci szereplők, akiknek feladataik homlokterében előfizetőik számára nyújtott zavartalan szolgáltatásbiztosítás, és a megbízható számlázási fegyelem áll. Minden szolgáltató számára a legfontosabb üzleti tényező a saját ügyfelének elégedettsége áll.

A távbeszélő szolgáltatások működését és feladatrendszerét a koncessziós szerződésük határozza meg, amely magába foglalja a adatvédelmi, adatszolgáltatási és titkos információ gyűjtéssel összefüggő feladatokat is.

A távbeszélő szolgáltatók helyét és szerepét az alábbi tényezők határozzák meg:

- Objektum védelem,
- Adatvédelem,
- Ügyfél elégedettség folyamatos biztosítása és a szolgáltató iránti bizalom fenntartása,
- A távbeszélő szolgáltatók minden olyan titkai (üzleti titkok), amelyek pozíciójának fenntartása érdekében csak azokkal oszt meg, akiket arra érdemesnek ítél.

Összességében, tehát a szolgáltatók információ biztonsági és védelmi feladatainak rendszere komplex stratégiai tervezést és operatív végrehajtási modellezést igényelnek. Ez utóbbi feladatokat konzekvens magatartással és kellő szakmai felkészültséggel lehet megvalósítani.

- A távbeszélő szolgáltató, mint adatkezelő ügyfeleinek adataival rendelkezik, annak törvény szerinti rögzítéséről, tárolásáról, megőrzéséről, archiválásról, illetve rendszereiből történő végleges törléséről gondoskodni köteles, illetve az eljárások végrehajtásának menetéért felelőséggel tartozik.
- Hasonló képen szigorú rendelkezések írják elő az ügyfelek adataiból történő szolgáltatások rendjét is. Az ügyfél - szerződés kötésének pillanatától – személyes adataitól a hívás rekordjain keresztül számos adatát bízza szolgáltatójára. Ezt, tehát hasonló képen az üzleti életben szokásos bizalmi elv is átszövi, miközben természetesen a törvények is igyekeznek szigorú eljárási elveken keresztül biztosítani az állampolgár jogait. Nem hagyható figyelmen kívül, hogy az arra jogosult szervezet a rendelkező törvények értelmében az előfizető közleményeiről is tudomást szerezhet. Ezekben a feladatokban a szolgáltató csak mint hozzáférést biztosító köz-

reműködik. Ez tehát azt jelenti, hogy a szolgáltatónak közvetlen részvétele a jogosult nem tart igényt.

- Az ügyfél kiszolgálása minél nagyobb megbízhatósággal és tartalom változatossággal. Ezt a tevékenységet nevezhetjük a piaci szereplő front tevékenységének.
- A távbeszélő szolgáltatók minden olyan titkai (üzleti titkok), amelyek akár üzleti sikereit, akár pozíciójának fenntartása érdekében csak azokkal oszt meg, akit abban érdekeltnek ítél.

Összességében, tehát a szolgáltatók információ biztonsági és védelmi feladatainak rendszere komplex stratégiai tervezést és operatív végrehajtási modellezést igényel. Ez utóbbi feladatokat konzekvens magatartással és kellő szakmai felkészültséggel lehet megvalósítani.

A feladat bonyolultságát az alábbi három fő téma kör szerint lehet csoportosítani:

- front feladatok, fő tevékenység és üzleti feladatrendszerek,
- back feladatok, az adat és információ védelme és az abból történő szolgáltatások rendszere,
- az objektum, amelynek védelme fokozottan kiemelt fontosságú feladat, illetve a szolgáltató működési folyamatai során keletkező belső információi.

Az alábbiakban részletezésre kerülő témakörök taglalásakor a végrehajtást megvalósító szervezeti rendszer szervezésének is fő kérdéseire ki kell térni.

Publikációmban eddigi kutatásaimból szeretnék néhány gondolatot rendszerezni. Céлом összefoglalni az utóbbi években lejátszódott robbanás szerű penetráció hatásának biztonsági és védelmi aspektusára is rámutatni. Legvégre, ha csak érintőlegesen is, de foglalkozni szeretnék a szolgáltatók jövőben várható biztonsági feladatainak rendszeréről is.

I.

A távbeszélő szolgáltatók biztonsági feladatainak összefoglalása

A távbeszélő szolgáltatóknak úgy kell biztonsági feladataikat ellátni, hogy az semmilyen körülmények között ne zavarja a szolgáltató alaptevékenységét, de ugyanakkor a koncesszióban vállalt kötelezettségeinek is eleget tudjon tenni az elvárt pontosságnak, megbízhatóságnak és a műveleti feladatoknak is gyorsasággal.

A szolgáltatóknak a biztonsági munkáik során az alábbi feladatokat minden körülmények között el kell látnia:

- Adatszolgáltatás hatósági megkeresésre;
- Előfizetői adatok és információk gyűjtése a különböző adattároló és nyilvántartó rendszerekből,

-
- Műszaki szaktechnikai feladatok biztosítása, ill. távközlő rendszerek hozzáférési pontjainak a biztosítása,
Az adatszolgáltatás változatai az alábbiakat tartalmazzák:
 - az ügyfélszerződési dokumentációk,
 - a forgalmazás során keletkező hívásrekordok információ halmaza,
 - egy másik szolgáltató ügyfelét hívók adatállománya,
 - roaming adatállomány,
 - a forgalmazás helyének meghatározása,
 - készülék és SIM kártya váltás története (Ebben a műveleti munkában le lehet követni, hogy a vizsgált készülék, vagy SIM kártya mikor hol volt található)
 - korlátozottan, de megoldható a vizsgált GSM szám mozgásának figyelése és egy adott környéket ellátó átjátszók sugárzási iránya. (Ez utóbbiakat azért nevezzük korlátozottaknak, mivel a szerzett információ forrása függ az időjárástól és a földrajzi-domborzati viszonyoktól is.)
 - Műszaki szakértői tevékenységek. Ebbe a körbe tartoznak az alábbiak:
 - adatállomány értelmezési konzultáció,
 - a biztonsági feladatokat támogató fejlesztések koordinálása, mind azokon a területeken, amiket a szolgáltatók számára a 75/98 évi korm. rendelet előír-
 - kiszolgáló rendszerek fejlesztése, ami támogatja a gyorsabb és hatékonyabb szolgáltatásokat.
 - A Nemzetvédelem, nemzetbiztonság és rendvédelmi feladatokat ellátó szervekkel történő folyamatos kapcsolattartás, azok tovább fejlesztése, valamint a szakmai együttműködések folyamatos koordinálása.
 - Az állam és szolgálati titkok kezelésének rendje, amihez az alábbiak tartoznak:
 - a biztonsági feladatokban résztvevő személyek kiválasztásának és ellenőrzésének és foglalkoztatásának műveleti feladatai, valamint a foglalkoztatott személyi állományba beállt változások folyamatos kezelése.
 - az informatikai és hírközlő rendszerek technikai és rezsim szabályainak, valamint azon objektumok védelmének kidolgozása, működtetése, ellenőrzése.
 - A nyílt biztonsági iratkezelés és a TÜK rend felügyelete.
 - Folyamatos továbbképzések és jogszabályi ismeretek elsajátításának biztosítása.
 - Nemzetvédelmi feladatok koordinálása, a polgári meghagyás kezelése.
A vonatkozó rendelkezések alapján.

-
- Iparbiztonsági feladatok,
A szolgáltatók az utóbbi időben egyre inkább fordulnak az iparbiztonsági projektek irányába. Ezt az alábbi két tényező indukálja:
 - egyrészt a megszerzett szakmai tapasztalatok piacra ajánlása, másodlagos (secondary) profit szerzési céllal,
 - másrészt pedig az EU-hoz való csatlakozás kapcsán a szolgáltatók számára új, bővített piaci lehetőségre nyílt lehetőség.
 - biztonsági objektumok kialakítása.
Ebbe a körbe tartoznak mind azok az objektumok, melyeket a szolgáltatók a biztonsági feladatok érdekében a műveleti feladatok ellátása érdekében rendszerbe állítanak.
- A feladatok komplexitását a fenti felsorolás koránt sem tudja teljes egészében lefedni, ahhoz minden egyes bekezdésnél további részletezésekre volna szükség, ami meghaladja ennek a munkának a terjedelmét.

II.

Adatszolgáltatás alakulása

Az adatszolgáltatási igény a közleményszolgáltatás mellett megjelenő kísérő adat informatikai tárolásával és hozzáférhetőségével vált a biztonsági feladatok izgalmas kérdésévé.

A kezdeti időszakban a sikeres alkalmazhatóságot korlátozta:

- a jogszabályi ismeret alkalmazás szintű hiánya,
- a biztonsági feladatokban résztvevők felkészítésének nem megfelelő szintje,
- a folyamat szervezés alacsony színvonala.

A technikai eszközök rohamos fejlődésével, és a penetráció robbanásszerű növekedésével a közlemények mellett megjelenő kísérő információk halmaza minden más eszközt megelőzve a legfontosabb informáló technikává nőtte ki magát a biztonsági és rendvédelmi szervek munkájában. (A továbbiakban a szolgáltatók összessége kerül összevetítésre a felderítendő feladatok mennyiségével.)

Az adatszolgáltatási megkeresések száma a 90-es évek vizsgált időszakában jelentős változást nem mutatott. Az információ kérések száma össz. szolgáltatói szinten, átlagosan nem haladta meg 12.000 db dokumentációt és a 20.000 db előfizetői információk mértékét. Összevetve az előfizetők számának alakulását, a jogszabályi ismeretek betanulását, valamint az igénylő szervek eszköz ismeretét, 2000-től egy merőben új helyzet állt elő, melyet egyszerűen az adatigénylés penetrációjának lehet nevezni.

Az adatkérés növekedésének okai:

- a GSM használók számának exponenciális növekedése,
- a felderítő hatóságok operatív eszközei között a legpreferáltabb technikájává vált,

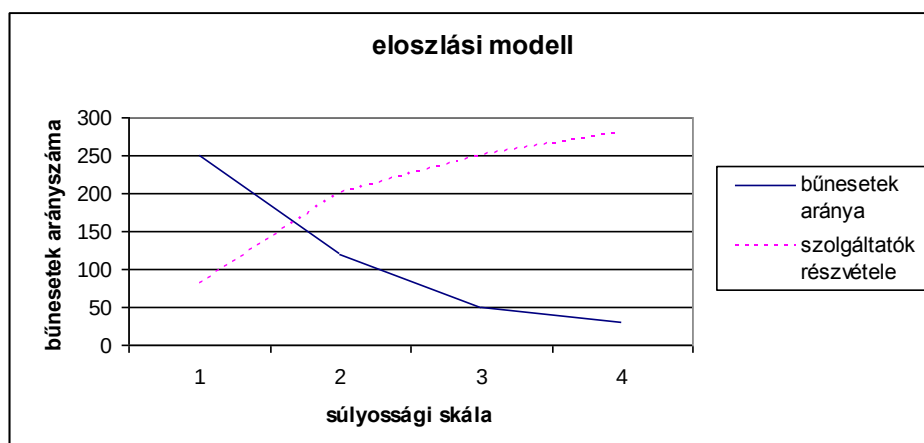
- az elkövetői körben rendkívül meg növekedett a mobil forgalmazás aránya,
- valamint az elkövetői magatartás brutalitásának növekedése.

A GSM adatszolgáltatás aránya 2000 és 2002 közötti időszakban az adatigény évente 75%-kal növekedett, amit viszont sem a szolgáltató, sem a törvényi eszköztár nem követett kellő módon.

Napjainkban a megkeresések számának emelkedése nem csökkent, de a növekedés mértéke 22%-ra mérséklődött. Hazánkban az ismertté vált bűnesetek száma 480 – 500 ezer körül mozgott évente. A mobil távbeszélő szolgáltatók minden kiemelt bűnesetek felderítő munkájában részt vettek.

A bűnesetek társadalomra való veszélyességének és a szolgáltatóknak a felderítő munkában való részvételének eloszlását az alábbi táblázat és ábra reprezentálja.

bűnesetek aránya	250	120	50	30
szolgáltatók részvétele	80	200	250	280



A szolgáltatók kb. 240-250 ezer GSM számhoz kapcsolódó előfizető adatait, hívás listáját, stb. dolgozzák fel. Az ismertté vált hazai bűnesetek számához viszonyítva (kb. 430-450 ezer) ez azt jelenti, hogy az összes kiemelt bűnesetek valamint a társadalomra fokozottan veszélyes bűncselekmények felderítésében veszik igénybe a szolgáltatók adatfeldolgozási munkáját. A hagyományos előfizetői adatok, híváslisták és szerződés másolatok mellett jelentős szerepet kapott a trace típusú műszaki figyelés, az IMEI-IMSI-GSM history adatbázis-kezelő rendszer, és az egy adott környéket lefedő átjátszó állomások szerinti adatállomány időtartam szerinti kigyűjtése.

Az 2. sz. táblázat mutatja az elmúlt három év adatszolgáltatási igényeinek alakulását.

	Év	nyílt	TÜK	össz.
	2000	87 ezer	33 ezer	120 ezer
	2001	141 ezer	40ezer	181 ezer
	2002	175 ezer	45 ezer	220 ezer
Változás	2001-2002	60,99%	22,73%	50,60%
	2002-2003	24,44%	8,29%	20,87%

A 2003 évi várható éves adatfeldolgozási mennyiség kb. 230.500 db., ami azt jelenti, hogy ebben az évben még várható növekedés, de ez már nem jelentős mértékű. Előzetes becslés szerint a jövő évben beáll az adatszolgáltatás iránti kérelem egy átlagos üzemviteli mennyiségre, melyben jelentős eltérés az azt követő időszakokban nem várható.

Jelentős változás várható a feldolgozói kapacitások és a feldolgozói sebesség növekedésével.

Összefoglalva, a szolgáltatók adatfeldolgozási munkái eredményesen támogatja az igénybe vevő hatóságok munkáját.

III.

Műszaki szaktechnikai feladatok biztosítása, ill. távközlő rendszerek hozzáférési pontjainak a biztosítása

A Nemzetbiztonsági tv. és a 75/1998 évi kormányrendelet értelmében a szolgáltatók együttműködési megállapodások keretében rögzítik a műszaki és szaktechnikai eszközök szükségleteit. Ennek megfelelően a fentiekben részletezett adatszolgáltatáson kívül a szolgáltatók hozzáférési pont nyújtásával biztosítják a monitoring funkciók működtetését. A szolgáltatóknak e feladatkörben nincs műveleti funkciója, tevékenysége kizárólag technikai egyeztetésig terjed.

Műszaki szakértői tevékenységek

Az titkos szolgálatok különböző szervei, akik technikai fejlesztéseket is végre hajtanak, rendszeres konzultációt kérnek munkatársainktól. A konzultációk a GSM rendszer különböző alkalmazásaira, a GPRS technika monitorozására, stb. terjedt ki.

IV.

A Nemzetvédelem, nemzetbiztonság és közbiztonsági feladatokat ellátó hatóságokkal történő folyamatos kapcsolattartás és a kapcsolatok fejlesztése

A szolgáltatók megismerték és megértették a hatóságok szakmai igényeit, és az évek során sikerült is a probléma mentes kapcsolati rendszert kialakítani.

Ez azért is volt rendkívül fontos a hatóságok számára, mivel a piacgazdasággal megjelenő konkurens piaci szereplők maguk váltak a technikai eszközök, adatok és információ hordozójává. A kapcsolati rendszer helyes működését az alábbi tényezők biztosíthatják:

- a feladatok pontos meghatározása,
- a szolgáltatók üzleti funkciójának tiszteletbe tartása, (Ez az igénybevevő részéről nagy fokú türelmet, és empátiát vár el. Tudomásul kell venni, hogy a szolgáltató törvényi kötelezettségeinek eleget kíván tenni, de nem a konkurens szolgáltatók előnyére. Ezért van, hogy minden új biztonsági feladat bevezetésénél elvárt követelmény, hogy a szolgáltatók egy időben és azonos módon nyújtsanak támogatást.)
- személyes kontaktus,
- biztonsági vezetők szakmai rátermettsége, (A biztonsági vezető az a személy, akinek minden esetben mérlegelnie kell tudni az adott feladat végrehajtható-e vagy sem, mivel végrehajtása sértheti és visszahathat a szolgáltató piaci érdekeire.
- A szolgáltatók biztonsági funkcióinak folyamatos korszerűsítése, (A technika és adatbirtokos szolgáltatók az igénylő szempontjából decentralizált jellegűek, eltérő technikai és szervezeti rendszerűek)

Összességében, tehát mind két fél valós érdeke a probléma mentes együttműködés. Mára már sikerült a szolgáltatóknak olyan biztonsági vezetőket foglalkoztatniuk, akik jól ismerik a hatósági feladatok rendszerét, a jogszabályi rendelkezéseket, rendelkeznek technikai ismeretekkel, valamint képesek ellátni az adat- és titokvédelem felügyeleti funkcióit is.

Befejezés

A szolgáltatók biztonsági területei az elmúlt években robbanásszerű változásokon mentek keresztül, melynek legfőbb oka az előfizetők hasonló méretű növekedése, valamint az elkövetői körben történt mobil használatok elterjedése. A biztonsági szolgáltatások általában kis létszámmal működnek, viszont hatásköre országos méretű, munkájukat ennek a felelőségnek a tudatában végzik.



TANÁCSADÓ, SZAKÉRTŐ, SZOLGÁLTATÓ KFT

Antók Ingenieurbüro GmbH, Antók's Engineering Office LTD.

vezetője: **ANTÓK PÉTER**

Okleveles távközlési üzemtechnikus

MMK 01/1842 W-H2-V Hírközlési vezető szakértő

HIF FMV-TV / 026 / 2007 Felelős műszaki vezető

IM 006744 Igazságügyi távközlési szakértő

**TANÁCSADÁS, TÁVKÖZLÉSI-MŰSZAKI SZAKÉRTÉS,
RENDSZERTECHNIKA ÉS RENDSZERSZERVEZÉS,
HÁLÓZATÉPÍTÉSI- ÉS SZERELÉSI TECHNOLÓGIÁK
HÁLÓZAT MINŐSÉGI JELLEMZŐK ELLENŐRZÉSE
HÁLÓZATOK MŰSZAKI-GAZDASÁGI ÉRTÉKELÉSE**

MŰSZAKI DOKUMENTÁCIÓ

- egyedi hálózati rendszerek
- tervezési irányelvek
- hálózatepítési előírások
- hálózatszerelési technológiák
- kábel mérések
- üzemvitel, fenntartás
- kezelési leírások



LANCIER

CABLE GMBH KÉPVISELET

kábelbehúzó-, kábelfektető eszközök,
kábeldob szállítók, kábelbehúzó csőrlők

HÁLÓZATI TECHNOLÓGIÁK

- honosítás
- magyar nyelvű dokumentálás
- oktatási anyag szerkesztés
- szakember képzés, - továbbképzés
- kivitelezés műszaki vezetés

HÁLÓZAT BIZTONSÁG - MSZ 17128

ZÁRHATÓ BELSŐ AKNAFEDLAP

Vezetékes - nyomvonal jellegű
hírközlő hálózatok fizikai védelme.
Kiemelt védettségű, különösen nehéz
hozzáférésű, "figyelt" hálózatok
tervezése, létesítése, üzemeltetése

KÉPZÉS, -TOVÁBBKÉPZÉS

Oktatási anyag fejlesztése, szerkesztése
oktatás szervezés, képzés, továbbképzés.

Antók Mérnöki Iroda Kft.

1035 Budapest. Szél utca 17. V. 29.

Telefon: (1) 439-1353

Fax: (1) 439-1354

e-mail: peter.antok@axelero.hu

www.antoknet.hu

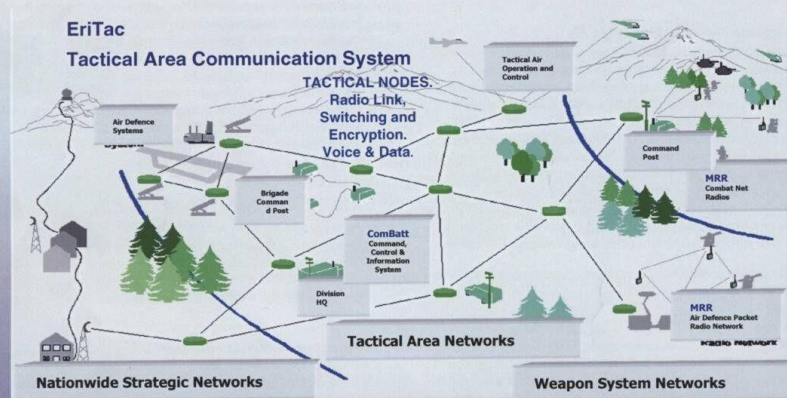
Kongsberg Védelmi Kommunikációs Kft.

Az Ön teljeskörű védelmi kommunikációs rendszer és berendezés szállítója

A Kongsberg Védelmi Kommunikációs Kft. (Kongsberg Defence Communications AS) a katonai felhasználású mobil távközlési rendszerek kulcsfontosságú szereplője. Az EriTac harcászati kommunikációs rendszer, illetve az új MRR többfunkciós rádió rendszer nagysebességű adat, illetve beszédátvitelt biztosítja harcászati körülmények között.

Az EriTac illetve az MRR biztosítja a harcászati vezetés és ellenőrzés alapját a Harcászati híradó Rendszerünkben, a ComBatt-ban. A kommunikációs, és rejtjelezési termékeinket a világ különböző hadseregeinek, valamint a légvédelemének szállítjuk, beleértve számos NATO tagállamot is.

Vállalatunk több évtizedes tapasztalattal rendelkezik a harcászati kommunikációs rendszerek tervezése, gyártása, illetve telepítése területén. Vállalatunk az AQAP-110, AQAP-150, valamint az ISO-9001 minősítésekkel rendelkezik.



A KONGSBERG Norvégia, és a NATO fegyveres erőinek, valamint további nemzetközi vásárlóknak a szállítója.

- Védelmi kommunikáció,
- Hajó elhárító cirkáló rakéták,
- NATO rejtjelező rendszerek (GSM és IP)
- C3I valamint fegyverzet irányító rendszerek,
- Légvédelmi fegyverzet irányító rendszerek.
- Tengerészeti védelmi rendszerek,
- Kiképzési, és szimulációs rendszerek,
- Tengeralattjáró elhárító fegyverzeti rendszerek,
- Tengeri akna ellenintézkedés rendszerek,
- Járműre telepített fegyverek.

Kongsberg Defence Communications AS
P.O. Box 87, N-1375 Billingstad, Norway
Tel.: + 47 66 84 24 00. Fax: + 47 66 84 82 30
E-mail: sales@kongsberg.com
www.kdefence.com
www.kongsberg.com





KONGSBERG

MRR

Többfunkciós rádió rendszerek a digitális harctér számára

•Egyedülálló kommunikációs védelmi jellemzőkkel felszerelt Harcászati URH rádió

•Negatív jel/zaj viszony mellett is üzemel,

•Megszünteti a többutas hullámterjedés vétel problémáit,

•Jelentős mértékű elektronikus hadviselés elleni teljesítmény mutatók (ECCM, EPM)

•Jelentős mértékű bit-hiba arány (BER) csökkenés az adatátvitelben.

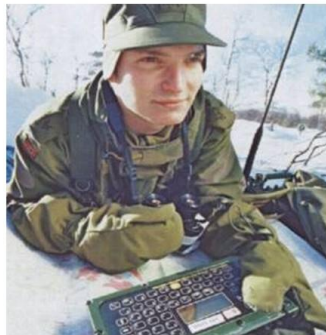
Független, nemzetközi teszt nyilatkozatok:

"AZ MRR EGYIK LEGEGYEDÜLLŐBB JELLEMZŐ TULAJDONSÁGA AZ ÁLTALA HASZNÁLT FREKVENCIA UGRATÁSOS / KÖZVETLEN SORRENDŰ (FH/DS) JELALAK, VALAMINT AZ M-ARRAY KÓDOLÁS: EZEK A TULAJDONSÁGOK SZÁMOS TELJESÍTMÉNY MUTATÓ JAVULÁSÁT BIZTOSÍTJÁK.

A TISZTA EREDMÉNY A HARCÁSZATI KÖRÜLMÉNYEK KÖZÖTTI HATÓSUGÁR, A BESZÉD, ILLETVE ADAT FORGALOM MEGBÍZHATÓSÁGA TERÜLETÉN ELÉRT DINAMIKUS JAVULÁS."



Az MRR a digitális hertéren hatalmas
jelentőséggel bír, egyedülálló
szolgáltatások
széles körét vezette be. Ime néhány példa ezekre:



Kombinálás:

Üzenet terminállal integrált **X.25 packet rádió** protokoll

Ez a kombináció hatékonyan terjeszti ki a
készülék hatósugarát, és az adatesomagok
átirányításával, vagy pedig az MRR
rádióhálózaton belüli több ugrás beiktatásával
megtöbbszörözt zavarás elleni immunitást biztosít.

Beépített adaptív

interferencia kioltási üzemmód, mely FF, vagy az FH üzemmód valamennyi ugrásában is működik.

Keskenysávú interferencia források jobb, mint
25dB-es bizonyítható elnyomása.

Ilyen interferencia eredhet hagyományos FF és
FH rendszerű FM rádióktól, – vagy zavaró
állomásoktól. Ez gyakorlatilag azt jelenti, hogy
az MRR (látszólag észleletlenül, és így zavarástól
mentesen!) képes dolgozni az ellenség
frekvenciáin, és elkerülni az ellenséges zavarást.

Új elven működő hailing, a

digitális hailing üzemmód.

Bekapcsolt digitális hailing esetén az MRR-t nem
zavarhatják a megszakított, vagy a hibás hailing
jelek, vagy a hailing frekvencián kisugárzott
egyéb jelek.

A STANAG 4292 szerinti analóg hailing is
támogatott.

A lehetséges konfigurációk a következők:

MH300, kézi MRR rádió

teljes MRR kompatibilitás úgy FF mint FH EPM üzemmódokban.
Beépített üzenet terminálja van, beépített rejtjelezés, és
verziófrissítés lesz kapható a 64 kbps adatátviteli sebességre.



MP300, PRC hordozható MRR rádió



MV300, VRC jármű fedélzeti MRR rádió



MV300 kettős szerelésű MRR rádió



Az adatkezelő eszközök magukban foglalják a GPS-t, térkép megjelenítő rendszert, katonai üzenettovábbító és képtovábbító szolgáltatásoktól várják el a harcmezőn történő teljesítménymutatók javulását. Az előretolt zónában a megnövelt mozgékonyság és magas sebesség az egyes katonák és fegyverzeti terminálok szintjére lebontott rádió kommunikációs lehetőséget igényelnek.

A felhasználók szemszögéből a beszéd, valós idejű adat és üzenet forgalmazás elérhető kell legyen, egy egyetlen rádió készüléken keresztül, vagy közvetlenül magába a rádiókészülékbe funkcionálisan integráltan, a rádió készülék szabványos illesztő felületeken keresztül.



Az MRR a 30 – 88 MHz-es frekvencia tartományban működő valóban moduláris rádiókészülék. Ugyanazok a modulok alkotják az MP300 hordozható PRC, a MV300 jármű fedélzeti egyes és kettős szerelésű VRC, 10mW - 5W közötti, vagy 50W teljesítményű konfigurációit. A kis kézi hordozható egység 10 mW vagy 1W teljesítményű.

Rádió vezérlő terminál - RCT



Adóvevő -TRX



Hordozható rádió keret - PRB



Szerelő-rögzítő, és akkumulátor töltő egység – MBU



Co-site szűrő egység - CSFU



Rádiófrekvenciás teljesítmény erősítő – PA



**Mobil telekommunikációhoz és katonai felhasználáshoz tervezett
gyorstelepítésű mobil antenna (karbon)**

Utánfutóra, terepjáróra vagy
furgonra szerelhető
tűzihorganyzott tartó szerkezetű.
A torony test, árboc, kitámasztók
karbon erősítésű epoxi csős
szerkezetek.
Az árboc szintenként
pneumatikusan kitolható,
telepítése antennák számától
függetlenül 1-2 óra



**Mobil telekommunikációhoz és katonai felhasználáshoz tervezett
gyorstelepítésű mobil antenna (acél)**

Az egész konstrukció tűzihorganyzott (120-
150 μ) acél szerkezetű, amely nagyfokú
korrózióvédelmet biztosít.



Fő partnereink:

- Westel Mobil Telekommunikációs Rt.
- NOKIA Hungary Kft.
- V.R.A.M Telekommunikációs Kft.
- Kongsber Defence Communications As
- Honvédelmi Minisztérium
- Ázsiai Országok
- Fisher Rosemount Kft.
- Orion Electronics Kft
- PHILIPS Components LLC.



Elérhetőségeink:

VT-Rendszertechnika Kft.
H-8002 Székesfehérvár
Berényi út 72-100
Pf.:284
Telefon: 22/533-790
Fax: 22/533-799

E-mail: vtsys@rendszertech.videoton.hu
Home page: www.vtsys.videoton.hu

VIDEOTON
SYSTEMTECHNICS LTD.

TELEKOMMUNIKÁCIÓS

TERMÉKEK

- Mobil telefon bázisállomás megvalósítása az alapoktól egészen a rádiós szerelésig
- Telekommunikációs konténerek gyártása és előszerelése



VÉDELMI ELEKTRONIKA

TERMÉKEK:

- Védelmi elektronikai rendszerek
- Kommunikációs rendszerek
- Automata felderítő, iránymérő és zavaró rendszerek tervezése és gyártása
- RH és URH adóvevők
- Tápegységek
- Teszt berendezések és tartozékok
- Acél és alumínium konténerek



**KONTÉNEREK MOBIL TELEKOMMUNIKÁCIÓS
BÁZISÁLLOMÁSOKHOZ**



Kifejlesztett NATO kompatibilis konténer



KS-20 típusú konténer



**Mobil telekommunikációhoz és katonai felhasználáshoz tervezett
gyorstelepítésű mobil antenna (karbon)**

Utánfutóra, terepjáróra vagy
furgonra szerelhető
tűzihorganyzott tartó szerkezetű.
A torony test, árboc, kitámasztók
karbon erősítésű epoxi csős
szerkezetek.
Az árboc szintenként
pneumatikusan kitolható,
telepítése antennák számától
függetlenül 1-2 óra



**Mobil telekommunikációhoz és katonai felhasználáshoz tervezett
gyorstelepítésű mobil antenna (acél)**

Az egész konstrukció tűzihorganyzott (120-
150 μ) acél szerkezetű, amely nagyfokú
korrózióvédelmet biztosít.

