



Kommunikáció 2004

Nemzetközi szakmai tudományos konferencia anyaga



-2004-

Zrínyi Miklós Nemzetvédelmi Egyetem
Budapest, 2004. szeptember 15.

Szerkesztették:
Dr. habil. Sándor Miklós ezredes
Dr. Szűcs Gáspár ezredes
Dr. Fekete Károly mk. alezredes

Lektorálta:
Dr. Fekete Károly mk. alezredes

Anyanyelvi lektor:
Fregan Beatrix

Felelős kiadó: Prof. Dr. Szabó Miklós akadémikus, a Zrínyi Miklós Nemzetvédelmi Egyetem rektora
Megjelent a Zrínyi Miklós Nemzetvédelmi Egyetemi Kiadó gondozásában
Igazgató: Veverka László
Készült a Zrínyi Miklós Nemzetvédelmi Egyetem nyomdájában, 200 példányban
Felelős vezető: Kardos István

ISBN 963 86441 5 X

TARTALOMJEGYZÉK

HÁTTÉR INFORMÁCIÓK	10
BEVEZETŐ	11
Dr. ABOS Imre	
AZ EU CSATLAKOZÁS UTÁN VÁRHATÓ VÁLTOZÁSOK A TÁVKÖZLÉSI PIACON	13
ANTÓK Péter	
ÚJ KÁBELHÁLÓZAT LÉTESÍTŐ TECHNOLÓGIÁK	27
BALAJTI László	
TERRORIZMUS ÉS A KOMMUNIKÁCIÓ 2004.	45
Dr. DÁRDAI Árpád	
AZ OFDM ELJÁRÁSOK A VÉDELMI CÉLÚ MOBIL TÁVKÖZLÉSBEN	49
DLASK Róbert	
AZ MH MRR HARCÁSZATI RÁDIÓK ALKALMAZÁSA	59
DOBÁK Imre	
FEJLŐDŐ KOMMUNIKÁCIÓ – NAGYOBB BIZTONSÁG? A TERRORIZMUS HATÁSA A KOMMUNIKÁCIÓRA	71
DOBOS Attila	
BESZÉD ÉS ADATKOMMUNIKÁCIÓ KONVERGENCIA LEHETŐSÉGE A MAGYAR HONVÉDSÉG TÁVKÖZLŐ ÉS INFORMATIKAI RENDSZEREIBEN	81
FEHÉR Judit	
INTEGRÁLT HÁLÓZATBIZTONSÁG A SZOLGÁLTATÓNÁL	85
Károly FEKETE PhD	
NEW POSSIBILITIES IN THE FIELD OF WAN-WLAN MILITARY COMMUNICATIONS	97
FREGAN Beatrix	
ÖSSZHADERŐNEMI STRATÉGIAI SZEMLELET A FRANCIA HADERŐBEN	103
GÁCSER Zoltán	
A DIGITALIZÁLT KATONA KOMMUNIKÁCIÓS ÉS INFORMÁCIÓS IGÉNYE	111
HAMAR Sándor	
ÚJ KIHÍVÁSOK A KATONAI INFORMÁCIÓS RENDSZEREKKEL SZEMBEN	123
HÓKA Miklós	
AZ ELEKTRONIKA FEJLŐDÉSÉNEK HATÁSA A HARCÁSZATI MOBILKOMMUNIKÁCIÓRA	129

Magyarné KUCSERA Erika	
A MAGYAR HONVÉDSÉG ZÁRTCÉLÚ HÁLÓZATA ÉS HÁLÓZATFELÜGYELETE BIZTONSÁGI OLDALÁNAK SZILÁRDÍTÁSA	145
LANTOS Xénia	
BETEKINTÉS SZERBIA ÉS BOSZNIA-HERCEGOVINA TÁVKÖZLÉSI PIACÁNAK PRIVATIZÁCIÓJÁBA.	155
Dr. LINDNER Miklós	
PUSKÁS TIVADAR A NAGY MAGYAR FELTALÁLÓ SZÜLETÉSÉNEK 160. ÉVFORDULÓJÁRA	157
MAGYAR Sándor	
A JELENLEGI SÁVSZÉLESSÉG KIHASZNÁLÁSÁNAK LEHETŐSÉGEI MULTISZOLGÁLTATÁSÚ KAPCSOLÓKKAL A MAGYAR HONVÉDSÉG KATONAI KOMMUNIKÁCIÓS RENDSZERÉBEN	161
MAROS Dóra – Dr. habil Sándor Miklós	
TÁVKÖZLÉSI HÁLÓZATOK EGYÜTTMŰKÖDÉSÉNEK NEMZETKÖZI ÉS NEMZETI SZABÁLYOZÁSI KÉRDÉSEI VESZÉLY- ÉS KATASZTRÓFAHELYZETBEN	167
Gyula MIKÓ - András MAGYAR	
MOBILE ADAPTIVE RADIO DIRECTION FINDING SYSTEM	173
MONSZPART Zsolt	
ERICSSON IN DEFENSE	189
NEMES László	
SZÉLESSÁVÚ INTERAKTÍV CATV HÁLÓZATOK KIÉPÍTÉSE NAGYSEBESSÉGŰ ADATÁTVITELI SZOLGÁLTATÁSOKHOZ WCDMA TECHNIKA FELHASZNÁLÁSÁVAL	209
NÉMETH András – Dr. habil SÁNDOR Miklós	
A KATASZTRÓFAVÉDELMI KOMMUNIKÁCIÓ JOGI SZABÁLYOZÁSA MAGYARORSZÁGON	213
PÁNDI Erik	
A KORMÁNYZATI TÁVKÖZLÉS ELMÚLT 15 ÉVE	229
Patrice ERULIN	
DELIVERING NETWORK ENABLED DEFENSE CAPABILITIES	261
Dr. ZOLTÁN Rajnai	
LES RADIOS DE L’AVENIR POUR LES ARMÉES	269
RÉVÉSZ Gyula – Dr. habil SÁNDOR Miklós	
A HÍRADÓ KIKÉPZÉS AZ ÁTALAKÍTÁS TÜKRÉBEN	273

SZABÓ Zoltán	
A MEGBÍZHATÓ, INTELLIGENS ÉS BIZTONSÁGOS HÁLÓZAT RECEPTJE	283
Dr. SZÉP József	
A NATO ÚJ KEZDEMÉNYEZÉSE A HÁLÓZAT NYÚJTOTTA KÉPESSÉG	289
TESSEDIK Tamás	
A 2,5 G ÉS AZ UMTS 3. GENERÁCIÓS MOBIL SZOLGÁLTATÁS INFORMÁCIÓ BIZTONSÁGI FELADATAI	304
TÚRI Viktória	
A KAPCSOLAT MEGSZAKADT... REPÜLŐTRAGÉDIA EGY PSZICHOLÓGUS SZEMÉVEL	309
Dr. VÁNYA László	
CYBER WARFARE – VALÓBAN KORSZERŰ KIHÍVÁS A HADERŐKKEL SZEMBEN	317

A nemzetközi tudományos konferencia kommunikációs partnere:

Magyar Távközlési Részvénytársaság



A tudományos konferencia támogatói:

	SIEMENS Nemzeti Védelmi és Biztonsági Ágazat
	Kapsch Telecom Kft
	Alcatel Hungary Kft.
	THALES COMMUNICATIONS



Alcatel PCX 4400 tábori kommunikációs rendszer

Katonai alkalmazásra kifejlesztett, hordozható, megerősített kivitelű, integrált rendezővel, menedzsment és DECT mobil rendszerrel.



Alcatel Hungary Kft.

1116 Budapest, [Kondorfa u. 10.](#)

Telefon: (1) 2099500 Telefax: (1) 2099599

www.alcatel.hu

alcatelh@alcatel.hu

HÁTTÉR INFORMÁCIÓK

A konferencia fővédnöke:

- Mikita János mk. vezérőrnagy, a Honvéd Vezérkar Törzsigazgatója

A konferencia védnökei:

- Prof. Dr. Szabó Miklós vezérőrnagy, akadémikus, ZMNE rektor
- Horváth Ferenc dandártábornok, HVK híradó és informatikai csoportfőnök

A konferencia kommunikációs partnere:

- Magyar Távközlési Részvénytársaság

A konferencia támogatói:

- SIEMENS Nemzeti Védelmi és Biztonsági Ágazat
- Kapsch Telecom Kft
- Alcatel Hungary Kft.
- Thales Communications

A konferencia rendezői:

- Zrínyi Miklós Nemzetvédelmi Egyetem Katonai Információs Rendszerszervező Tanszék
- Honvéd Vezérkar Híradó és Informatikai Csoportfőnökség
- Zrínyi Miklós Nemzetvédelmi Egyetem Katonai Műszaki Doktori Iskola
- Hírközlési és Informatikai Tudományos Egyesület ZMNE Egyetemi Csoport

A szervező bizottság elnöke:

- Dr. habil. Sándor Miklós ezredes

A szervező bizottság titkára:

- Dr. Fekete Károly mk. alezredes

A szervező bizottság tagjai:

- Dr. Szűcs Gáspár ezredes
- Dr. Lehel György ezredes
- Szöllősi Sándor okl. mk. őrnagy
- Kis Lajos mk. százados

BEVEZETŐ

A Tisztelt Olvasó a Zrínyi Miklós Nemzetvédelmi Egyetem Információs Rendszerszervező Tanszék, a HVK Híradó és Informatikai Csoportfőnökség, a Zrínyi Miklós Nemzetvédelmi Egyetem Katonai Műszaki Doktori Iskola és a Hírközlési és Informatikai Tudományos Egyesület ZMNE egyetemi csoportja által rendezett nemzetközi szakmai tudományos konferencia szerkesztett anyagát tartja a kezében.

Mivel az ötödik, jubileumi nemzetközi szakmai tudományos konferencia egyben megnyitója volt a „Puskás Tivadar Emléknepok”-nak is, ezért célul tűzte ki maga elé a távközlési és informatikai változások időben nagyobb ívű áttekintését. Kiemelt figyelemmel kísérte az evolúciós versenyt túlélő és a kezdeti alkalmazási fázisban levő kommunikációval kapcsolatos megoldásokat. A konvergencia megjelenési formáit a konferencián kiállított és a résztvevők intézményeinél már hozzáférhető kommunikációs rendszerek és hálózatok példáin 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 többek között egy katonai alkalmazásra kifejlesztett, hordozható, megerősített kivitelű, integrált rendezővel, menedzsment és DECT mobil rendszerrel támogatott tábori kommunikációs rendszer valamint egy harcászati szintű, csapatvezetést-irányítást támogató vezetési-információs rendszer. Első ízben történt kísérlet az interoperabilitási elvárásoknak megfelelő, de eltérő szolgáltatók által üzemeltetett katonai kommunikációs hálózati szegmensek összekapcsolására.

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 EU CSATLAKOZÁS UTÁN VÁRHATÓ VÁLTOZÁSOK A TÁVKÖZLÉSI PIACON

„Kommunikáció 2004” Konferencia
Budapest, 2004. szept. 15.

Az EU csatlakozás után várható változások a távközlési piacon

Dr. Abos Imre, vezető stratégiai tervező
T-LoB Marketingstratégia és Üzletfejlesztés iroda



„Kommunikáció 2004” Konferencia, 2004. szept. 15.



Tartalom

- Az Euro-Atlanti integráció útja
- A távközlés-liberalizáció folyamata
- Az EU csatlakozás hatása
- Európai Unió és magyar célkitűzések
- Magyar Információs Társadalom Stratégia
- Nemzeti szélessávú stratégia
- Szélessávú vezetékes hozzáférés
- Vezetéknélküli hozzáférés
- Digitális televízió
- Összefoglalás



„Kommunikáció 2004” Konferencia, 2004. szept. 15.



Az Euro-Atlanti integráció útja

- 1989 – Az Európa Tanács tagja
- 1991 – Az EU társult tagsági szerződés megkötése
- 1994 – Az EU társult tagság kihirdetése (1994. I. törvény)
- 1996 – OECD tagság
- 1998 – Csatlakozás a WTO Távközlési egyezményhez (GATS)
- 1999 – NATO tagság
- 1998-2003 – EU csatlakozási tárgyalások
- 2003 – Az EU-csatlakozási szerződés aláírása
- 2003-2004 – Ratifikáció
- 2004 – EU-csatlakozás, teljes jogú EU tagság

3



"Kommunikáció 2004" Konferencia, 2004. szept. 15.



A távközlés-liberalizáció folyamata

- 1991 – Koncessziós törvény
 - koncessziós szolgáltatások
 - közcélú távbeszélő szolgáltatás
 - mobil rádiótelefon szolgáltatás
 - személyhívó szolgáltatás
 - műsorszórás
 - minden más szolgáltatás liberalizált
 - végberendezések
 - műholdas szolgáltatások (VSAT)
 - bérelt vonal, adatkommunikáció
- 1992 – Távközlési törvény
- 2001 – Hírközlési törvény (Távközlés, posta, frekv.gazdálkodás)
- 2001-2002 – A távbeszélő-kizárólagosság megszűnése
- 2003 – Elektronikus hírközlési törvény

4

EU csatlakozás → teljes liberalizáció



"Kommunikáció 2004" Konferencia, 2004. szept. 15.



Felkészülés a versenyre

A Matáv fejlődési szakaszai

- 1990 - 1993: Új távközlési infrastruktúra építése
- 1994 - 1997: A távbeszélő-hálózat intenzív fejlesztése
Üzleti szolgáltatások fejlesztése
- 1998 - 2001: Felkészülés a versenyre
- 2002 - 2005: A verseny kiteljesedése a liberalizált piacon

Versenyhelyzet az EU-csatlakozás után

- A távközlési piac teljes liberalizálása
- Magyarország az EU-piac részévé vált
- Az EU-piac alapvető működési elve a VERSENY
- Új szolgáltatók szabadon piacra léphetnek (mi is az EU-ban)
- Új szolgáltatások jelenhetnek meg a piacon
- Árcsökkenés, ügyfelek és forgalom elhódítása

5



"Kommunikáció 2004" Konferencia, 2004. szept. 15.



Európai Unió célkitűzései

Az eEurope2005 akcióterv

- A 2005-ös akcióterv az Internet hatékony és gyors elérésére és használatára összpontosít.

Az eEurope2005 kiemelt célkitűzései:

- Korszerű, nyilvános on-line szolgáltatások (e-kormányzat, e-oktatás, e-egészségügy)
- Az e-kereskedelem dinamikus fejlődését segítő környezet
- Versenyképes áron elérhető szélessávú hozzáférés
 - A szélessávú hálózatok telepítésének elősegítése (jog, úthasználat stb.)
 - A frekvenciaspektrum hatékonyabb kihasználása,
 - Az új szolgáltatásokhoz való hozzáférés különböző technológiai platformokon (pl. ADSL/Ethernet, digitális interaktív TV, WiFi/WiMAX, 3. generációs mobil), a digitális TV-re való átállás felgyorsítása,
 - A szélessávú hozzáférés elősegítése az elmaradottabb régiókban.
- Biztonságos információátvitelt nyújtó infrastruktúra

6



"Kommunikáció 2004" Konferencia, 2004. szept. 15.



Nemzeti Fejlesztési Terv (NFT)

Négy fejlesztési prioritás:

1. A termelőszektor versenyképességének növelése
2. A foglalkoztatás növelése és az emberi erőforrások fejlesztése
3. **Jobb infrastruktúra**, tisztább környezet biztosítása
4. A regionális és helyi potenciál erősítése, illetve a technikai segítségnyújtás

A NFT operatív programjai:

1. **Gazdasági Versenyképesség Operatív Program**
2. Humán Erőforrás Fejlesztés Operatív Program
3. Környezetvédelmi és Infrastruktúra-fejlesztési Operatív Program
4. Agrár- és Vidékfejlesztési Operatív Program
5. **Regionális Fejlesztési Operatív Program**

7



"Kommunikáció 2004" Konferencia, 2004. szept. 15.



A Magyar Információs Társadalom Stratégia (MITS)

A MITS főirányai

- Tartalom és szolgáltatások
- **Infrastruktúra**
 - Szélessávú infrastruktúra – Közháló, NIIF
 - Hozzáférés - eMagyarország-Pont
 - Infrastrukturális szolgáltatások
- Tudás és ismeret
- Jogi és társadalmi környezet
- Horizontális (K+F stb.)

8



"Kommunikáció 2004" Konferencia, 2004. szept. 15.



Várható hatások – fontos területek

EU és magyar prioritások

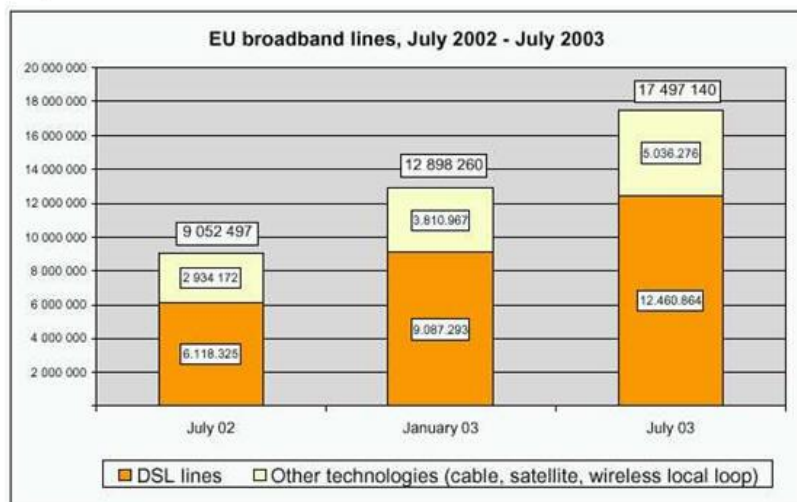
- **Szélessávú vezetékes hozzáférés (ADSL, KTV)**
 - A nagyobb településeken a telefonhálózaton létesített ADSL elérhető lesz az előfizetők 80%-a számára
 - A KTV hálózatok jelentős része visszirányúsított, Internet hozzáférés lehetővé válik rajtuk
- **Vezetéknélküli hozzáférés (WiFi, WiMAX, műhold)**
 - Sok kistelepülésen a vezetéknélküli hozzáférés fogja lehetővé tenni a szélessávú Internet hozzáférést
 - A műholdas vétel kisebb jelentőségű
- **Digitális televízió (földfelszíni, kábeles, műholdas)**
 - a digitális televízióval egy frekvenciasávban 3-4 programot lehet átvinni
 - a háztartások 96%-ában van televízió (analóg)
 - 1,9 millió háztartásban van KTV (analóg)
 - 100 ezer feletti UPC Direct digitális műholdvevő

• • • • •

"Kommunikáció 2004" Konferencia, 2004. szept. 15.



Szélessávú hozzáférés az EU-ban

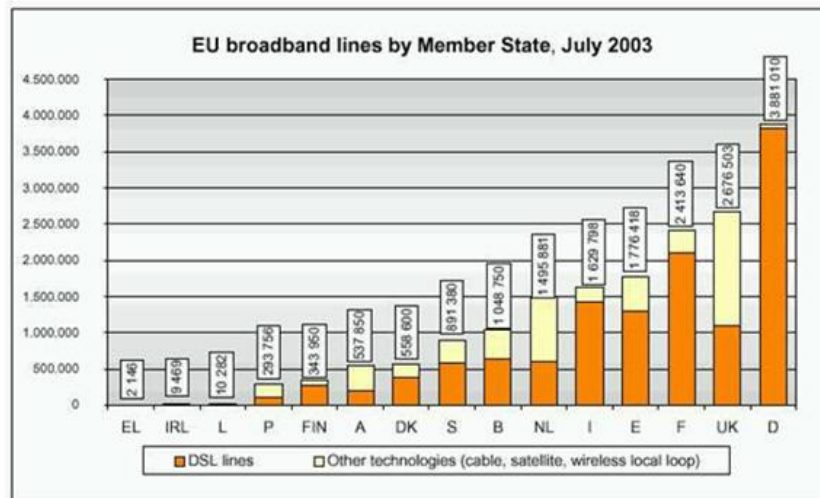


• • • • •

"Kommunikáció 2004" Konferencia, 2004. szept. 15.



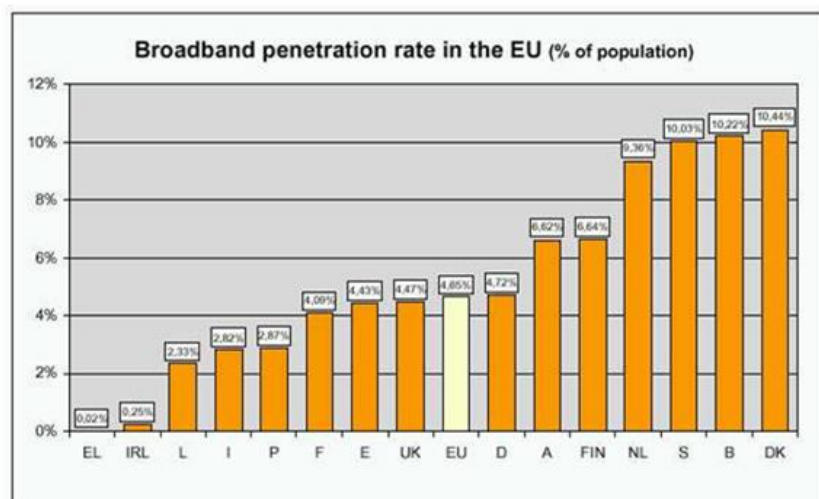
Szélessávú hozzáférés az EU-ban tagállamonként



"Kommunikáció 2004" Konferencia, 2004. szept. 15.



Szélessávú elterjedtség az EU-ban tagállamonként

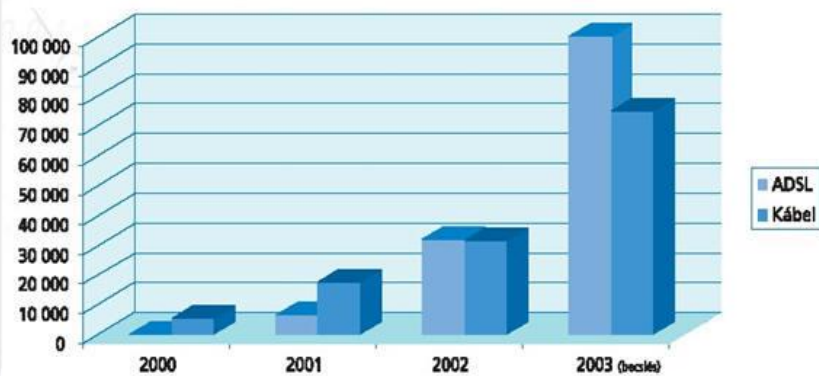


"Kommunikáció 2004" Konferencia, 2004. szept. 15.



Szélessávú hozzáférés Magyarországon

Az ADSL és kábel modem előfizetések számának alakulása, 2000-2003



13

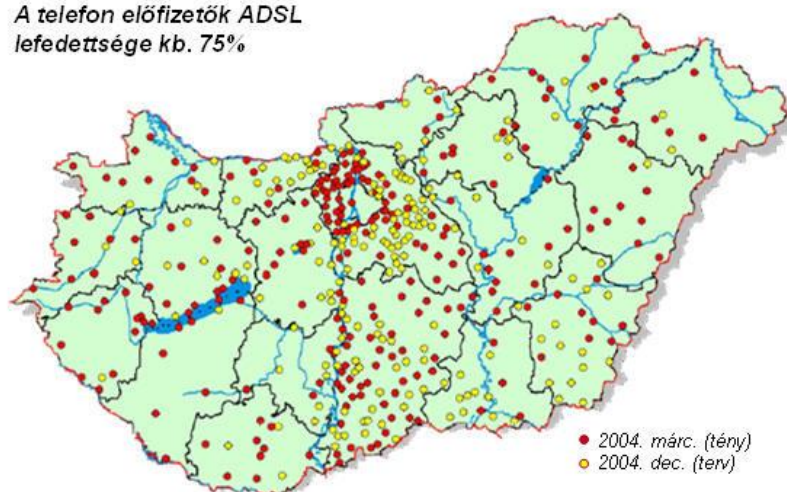
• • • • •

"Kommunikáció 2004" Konferencia, 2004. szept. 15.



ADSL lefedettség

A telefon előfizetők ADSL lefedettsége kb. 75%



14

• • • • •

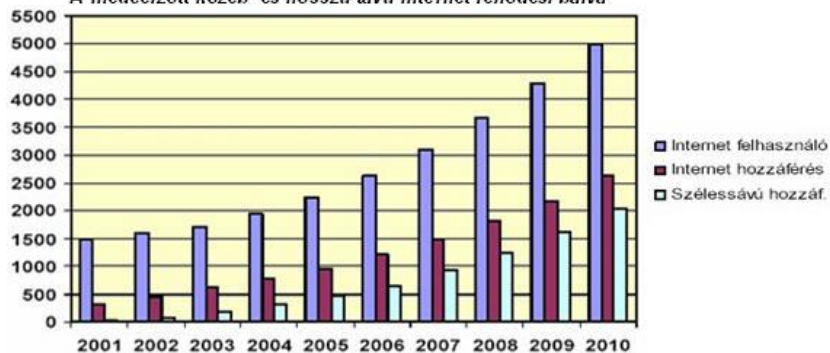
"Kommunikáció 2004" Konferencia, 2004. szept. 15.



Nemzeti szélessávú stratégia (NSzS)

- Lakosság és vállalkozások szélessávú lefedése
- Szélessávú közösségi hozzáférési pont minden településre
- Szélessávú hozzáférés a közszférában

A megacélzott közén- és hosszú távú Internet fejlődési nálva



"Kommunikáció 2004" Konferencia, 2004. szept. 15.



Nemzeti szélessávú stratégia

- Szélessávú szolgáltatás minden településen
- Elmaradott településeken megvalósítás állami szerepvállalással

Településkategóriák és technológiák

Települések lélekszáma	települések száma (db)	lakosság száma (fő)	Technológiák					
			LMDS WiMAX V-SAT DTV	KTV	ADSL	VDSL	FTTx + VDSL	FTTx
1.000.000 fölött	1	1 749 389						
100.001- 1.000.000	8	1 175 041						
50.001-100.000	12	768 375						
25.001-50.000	25	830 314						
20.001-25.000	17	380 645						
15.001-20.000	28	487 459						
10.001-15.000	51	618 273						
7.501-10.000	46	397 763						
5.001- 7.500	90	549 986						
2.501- 5.000	335	1 141 463						
2500 és alatta	2 522	2 088 870						

"Kommunikáció 2004" Konferencia, 2004. szept. 15.



Vezetéknélküli hozzáférés - WiFi, WiMAX, műhold

WiFi (Wireless Fidelity, IEEE 802.11b szabvány)

- Frekvencia: 2,4 GHz, max. sebesség 11 Mbit/s, hatótávolság kb. 100 m
- „Hot-spot”-ok - szállodák, éttermek, konferenciatermek, repülőtér
- Laptopok, PDA-k kapcsolódása az Internethez (belső megoldás)

WiMAX (IEEE 802.16a szabvány)

- Frekvencia: 2-11 GHz (pl. 3,5 GHz), max. sebesség 70 Mbit/s, hatótávolság: 32-56 km
- Alkalmas mikrohullámú gerinchálózat kiépítésére
- Lehetővé teszi városrészek, települések szélessávú ellátását
- Kombinálható a WiFi-vel (épületig WiMAX, épületben WiFi)

Műholdas Internet kapcsolat

- Csak a letöltés lehet nagysebességű
- A visszirányú kapcsolat telefonon, ISDN-en, mobilon valósul meg
- Kiegészítő technológia, kisebb jelentőségű

• • • • •

"Kommunikáció 2004" Konferencia, 2004. szept. 15.



TV a háztartásokban az EU-ban

Table 1: TV households (analogue and digital) in 2003
(in millions and in percentage of national households)

	Total TV HH	Cable TV		Satellite TV		Terrestrial TV - only	
		TV HH	%	TV HH	%	TV HH	%
Austria	3.2	1.32	40.8%	1.6	49.6%	0.31	9.6%
Belgium	4.2	3.9	93.0%	0.1	2.0%	0.21	5.0%
Denmark	2.3	1.1	46.4%	0.6	26.5%	0.61	27.1%
Finland	2.3	1.0	43.9%	0.24	10.5%	1.04	45.6%
France	24.4	2.9	11.9%	5.0	20.5%	16.51	67.6%
Germany	36.6	20.6	56.3%	14.0	38.3%	1.96	5.4%
Greece	3.0	0.00	0.0%	0.25	8.6%	2.72	91.4%
Ireland	1.31	0.47	35.8%	0.38	28.7%	0.47	35.8%
Italy	20.9	0.06	0.3%	3.2	15.5%	17.59	84.2%
Luxembourg	0.2	0.16	81.7%	0.01	5.8%	0.00	2.4%
Netherlands	7.1	6.3	89.0%	0.27	3.8%	0.51	7.2%
Portugal	3.1	0.90	28.7%	0.42	13.2%	1.82	58.1%
Spain	12.6	0.9	7.1%	1.8	14.3%	9.89	78.5%
Sweden	4.5	2.10	47.1%	0.8	17.9%	1.56	35.0%
UK	24.4	3.8	15.6%	7.6	31.3%	12.98	53.2%
TOTAL EU	149.94	45.4	30.3%	36.3	24.2%	68.2	45.5%

• • • • •

"Kommunikáció 2004" Konferencia, 2004. szept. 15.



Digitális TV a háztartásokban az EU-ban

Table 2: Digital TV households in 2003

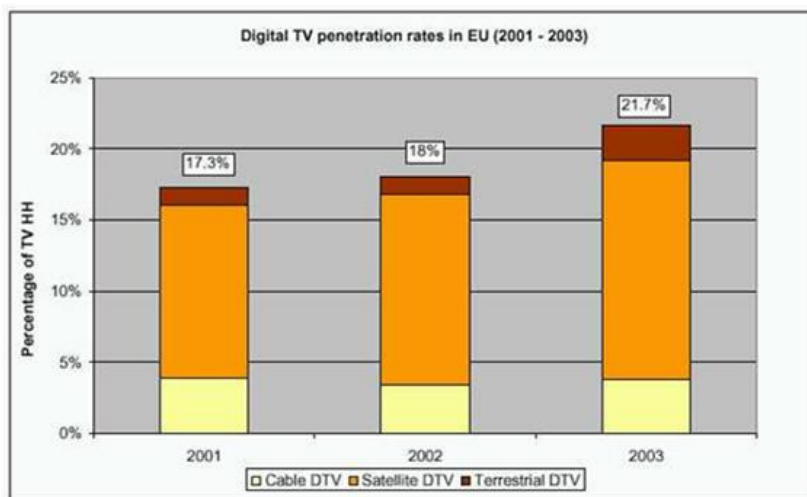
(in millions and in percentage of national households)

	Total TV HH	Total Digital TV HH		Cable DTV		Satellite DTV		Terrestrial DTV	
		TV HH	%	TV HH	%	TV HH	%	TV HH	%
Austria	3.2	0.55	17.1%	0.05	1.6%	0.50	15.5%	0.00	0.0%
Belgium	4.2	0.18	4.3%	0.16	3.8%	0.02	0.5%	0.00	0.0%
Denmark	2.3	0.35	15.5%	0.08	3.5%	0.27	11.9%	0.00	0.0%
Finland	2.3	0.21	9.2%	0.02	0.9%	0.10	4.4%	0.09	3.9%
France	24.4	4.62	18.9%	0.92	3.8%	3.70	15.2%	0.00	0.0%
Germany	36.6	5.16	14.1%	1.63	4.5%	3.15	8.6%	0.38	1.0%
Greece	3.0	0.25	8.4%	0.00	0.0%	0.25	8.4%	0.00	0.0%
Ireland	1.3	0.46	35.1%	0.10	7.6%	0.36	27.4%	0.00	0.0%
Italy	20.9	2.85	13.6%	0.00	0.0%	2.85	13.6%	0.00	0.0%
Luxembourg	0.2	0.01	5.3%	0.00	1.0%	0.01	4.2%	0.00	0.0%
Netherlands	7.1	0.69	9.7%	0.11	1.6%	0.55	7.8%	0.03	0.4%
Portugal	3.1	0.51	16.2%	0.02	0.6%	0.49	15.6%	0.00	0.0%
Spain	12.6	2.38	18.9%	0.15	1.2%	2.06	16.4%	0.17	1.3%
Sweden	4.5	1.25	28.0%	0.17	3.8%	0.88	19.7%	0.20	4.5%
UK	24.4	13.14	53.8%	2.29	9.4%	8.04	32.9%	2.81	11.5%
TOTAL EU	149.94	32.6	21.7%	5.7	3.8%	23.2	15.5%	3.7	2.5%

"Kommunikáció 2004" Konferencia, 2004. szept. 15.



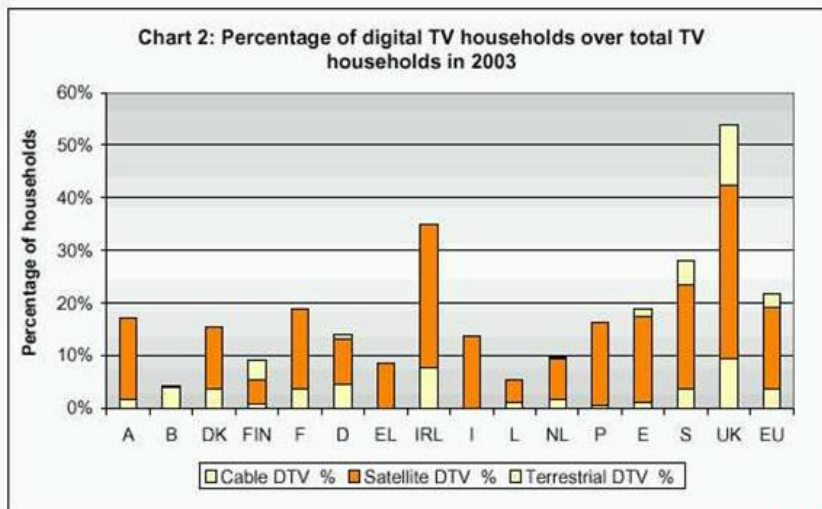
Digitális TV elterjedtség az EU-ban



"Kommunikáció 2004" Konferencia, 2004. szept. 15.



Digitális TV elterjedtség az EU-ban tagállamonként



21

"Kommunikáció 2004" Konferencia, 2004. szept. 15.



A földfelszíni digitális TV Magyarországon

Digitális földfelszíni sugárzású televízió

- Antenna Hungária kísérleti adás Budapesten és Kabhegyen
- UHF 43. cs. (647,25 MHz)
- 64 QAM (Quadratura AM)

Digitális műholdas televízió

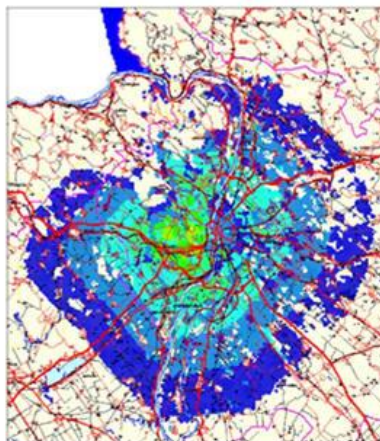
- A UPC Direct 2003. decemberben elérte a 100 ezres előfizetőszámot

Digitális kábeltelevízió

- Kísérletek folynak, rövidesen várható a bevezetés

A kormányzat támogatja a digitális TV elterjesztését, tervezett átállás 2012-ig

Budapest 43. cs. DVB-T kísérleti sugárzás
ND ERP = 1 kW



22

"Kommunikáció 2004" Konferencia, 2004. szept. 15.



Műholdas digitális műsorszórás Magyarországon

UPC Direct

- A UPC Direct 2000. szeptemberében elsőként teremtette meg Magyarországon a legkorszerűbb, digitális műholdas televíziózás lehetőségét.
- A szolgáltatás előfizetői több mint 150 digitális tévé- és rádióadást, köztük több mint tucatnyi magyar nyelvű tévécsatornát nézhetnek.
- A UPC Direct műholdas digitális szolgáltatás előfizetőinek száma 2003. decemberében túllépte a 100 ezret.
- A Digital Media Centre (DMC) saját készítésű műsorain kívül műholdakon, valamint nagysebességű kábelhálózatokon érkező televízió, rádió és adatjeleket továbbít Európa és Amerika több mint ötven országába.
- A UPC Direct műsorait Amszterdamból a UPC feladóállomása továbbítja az Astra műholdra.
- A kész műsorokat három műholdon keresztül juttatják el a kontinens KTV fejállomásaira, illetve a UPC Direct előfizetők otthonaiba is.

23



"Kommunikáció 2004" Konferencia, 2004. szept. 15.



A digitális televíziózás jövője Magyarországon

Kormányzati célkitűzések

- A kormányzat – az EU prioritásoknak megfelelően – jelentős mértékben támogatja a digitális televíziózás elterjedését.
- Várhatóan 2005-től megkezdődik a digitális műsorszórás, majd fokozatosan az összes műsor 2008-ig digitálisan is sugárzásra kerül.
- A digitális TV-re való átállással párhuzamosan a multimédiás és interaktív szolgáltatások fejlesztését is el kell végezni.
- A digitális műsorok multiplexálását, egyetlen csomagban való egyesítését meg kell oldani, a multiplex hálózatot folyamatosan bővíteni kell.
- Nemzetközi frekvencia koordinációra van szükség, a szabad frekvenciák alternatív felhasználásáról gondoskodni kell.
- 2008-2012-ig az analóg szolgáltatás lépcsőzetes megszűnik

24



"Kommunikáció 2004" Konferencia, 2004. szept. 15.



Összefoglalás

- Az EU-csatlakozással vált teljessé a távközlés területén a liberalizáció és a verseny
- A Matáv felkészülten fogadta az EU-csatlakozást mind szolgáltatás-választék, mind műszaki színvonal, mind az ügyfélszolgálat szempontjából
- Az EU-csatlakozással a magyar kormány átvette az EU célkitűzéseit, csatlakozva az eEurope2005 programhoz
 - Nemzeti Fejlesztési Terv és Operatív Programok
 - Magyar Információs Társadalom Stratégia (MITS)
 - Nemzeti Szélessávú Stratégia (NSzS)
- Kiemelt prioritások
 - e-kormányzat - szolgáltatások, alkalmazások
 - Szélessávú vezetékes és vezeték nélküli hozzáférés elterjesztése
 - A digitális televíziózás fejlesztése, műsorsugárzással átállás 1012-ig
 - Biztonságos információátvitelt nyújtó infrastruktúra

25



"Kommunikáció 2004" Konferencia, 2004. szept. 15.



**Köszönöm a
figyelmet!**

26



"Kommunikáció 2004" Konferencia, 2004. szept. 15.



ÚJ KÁBELHÁLÓZAT LÉTESÍTŐ TECHNOLÓGIÁK



Antók Péter:

ÚJ KÁBELHÁLÓZAT LÉTESÍTŐ TECHNOLÓGIÁK

KOMMUNIKÁCIÓ 2004 * ZRINYI MIKLÓS NEMZETVÉDELMI EGYETEM * BUDAPEST, 2004. SZEPTEMBER 15.



Kommunikáció 2003

ÚJ KÁBELHÁLÓZAT LÉTESÍTŐ TECHNOLÓGIÁK

1. Új fényvezető száltípusok
2. Új fényvezető kábelszerkezetek
3. Új hálózat rendszerek,
4. Új építési stílusok, technológiák
5. Új szerelési technológiák
6. Tervezés, nyilvántartás – tartalom és forma

KOMMUNIKÁCIÓ 2004 * ZRINYI MIKLÓS NEMZETVÉDELMI EGYETEM * BUDAPEST, 2004. SZEPTEMBER 15.

A HÍRKÖZLŐ RENDSZER



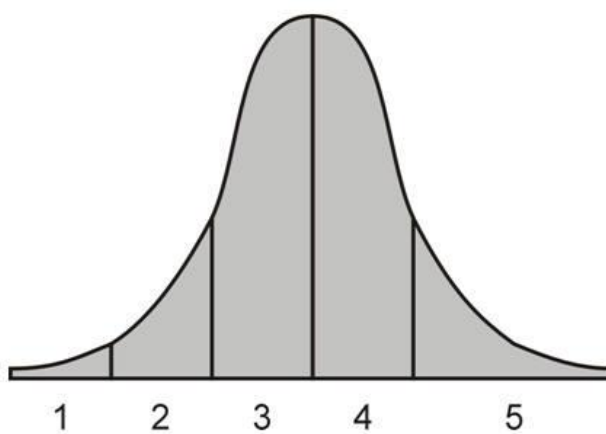
AMORTIZÁCIÓ: 4%



AMORTIZÁCIÓ: 20%

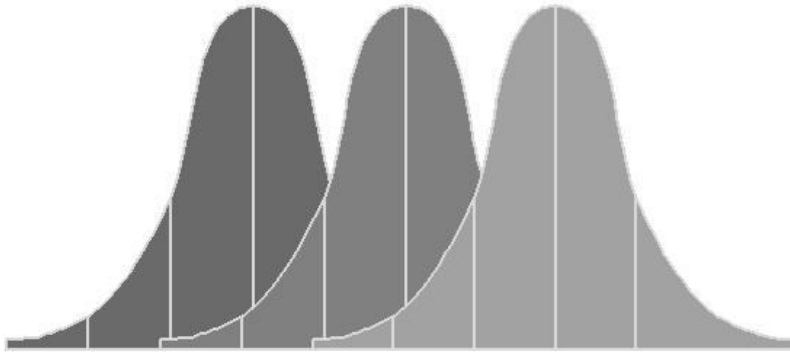
KOMMUNIKÁCIÓ 2004 * ZRINYI MIKLÓS NEMZETVÉDELMI EGYETEM * BUDAPEST, 2004. SZEPTEMBER 15.

AZ ÚJDONSÁG ELFOGADÁSA



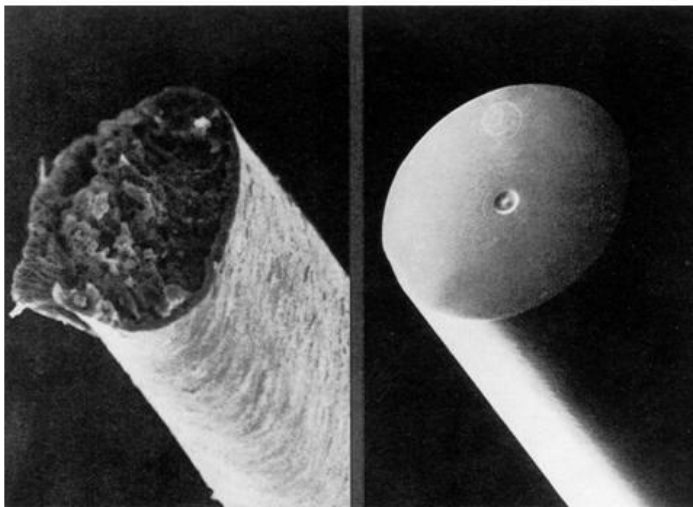
KOMMUNIKÁCIÓ 2004 * ZRINYI MIKLÓS NEMZETVÉDELMI EGYETEM * BUDAPEST, 2004. SZEPTEMBER 15.

AZ ÚJDONSÁG ELFOGADÁSA



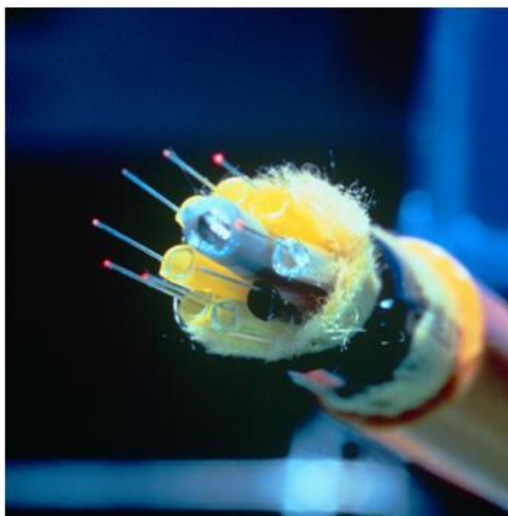
KOMMUNIKÁCIÓ 2004 * ZRINYI MIKLÓS NEMZETVÉDELMI EGYETEM * BUDAPEST, 2004. SZEPTEMBER 15.

A HAJSZÁL ÉS A FÉNYVEZETŐSZÁL



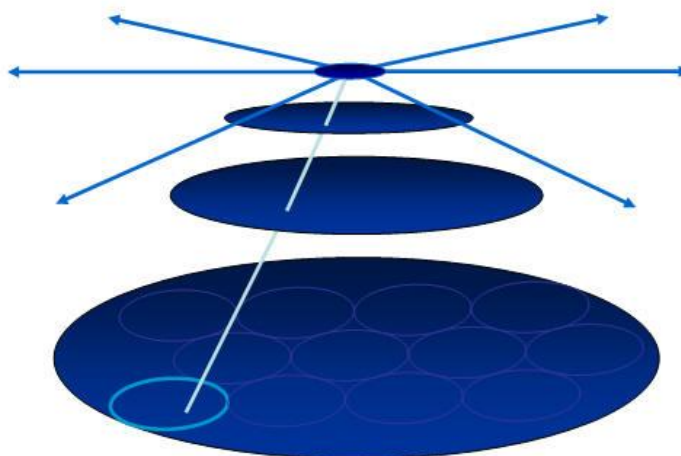
KOMMUNIKÁCIÓ 2004 * ZRINYI MIKLÓS NEMZETVÉDELMI EGYETEM * BUDAPEST, 2004. SZEPTEMBER 15.

FÉNYVEZETŐ KÁBEL



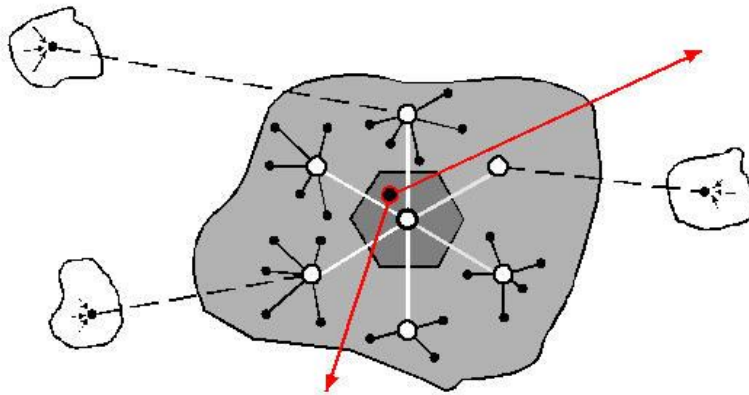
KOMMUNIKÁCIÓ 2004 + ZRINYI MIKLÓS NEMZETVÉDELMI EGYETEM + BUDAPEST, 2004. SZEPTEMBER 15.

HÁLÓZATI SÍKOK



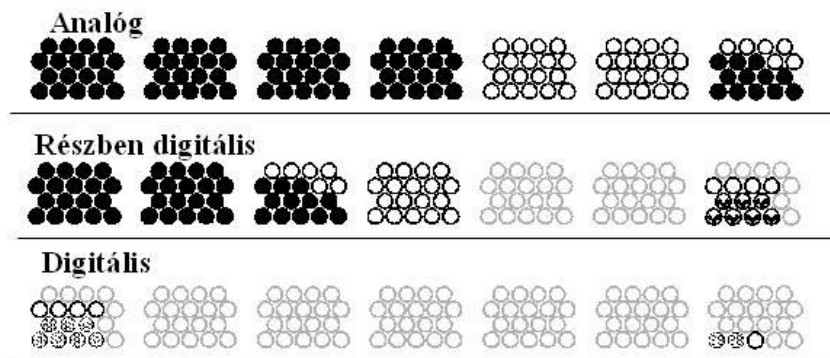
KOMMUNIKÁCIÓ 2004 + ZRINYI MIKLÓS NEMZETVÉDELMI EGYETEM + BUDAPEST, 2004. SZEPTEMBER 15.

HELYI HÁLÓZAT



KOMMUNIKÁCIÓ 2004 * ZRINYI MIKLÓS NEMZETVÉDELMI EGYETEM * BUDAPEST, 2004. SZEPTEMBER 15.

KÁBELHÁLÓZAT HELYÍGÉNYE



KOMMUNIKÁCIÓ 2004 * ZRINYI MIKLÓS NEMZETVÉDELMI EGYETEM * BUDAPEST, 2004. SZEPTEMBER 15.

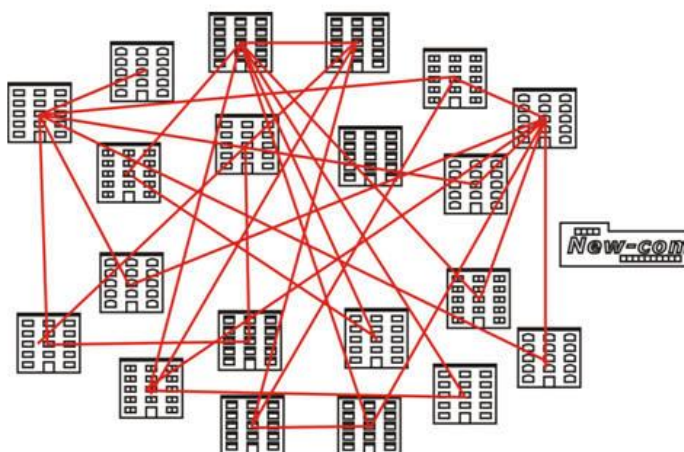
KÁBELHÁLÓZAT HELYE

Távközlő kábelek helye belterületen
az MSZ 7487/2-80 szerint



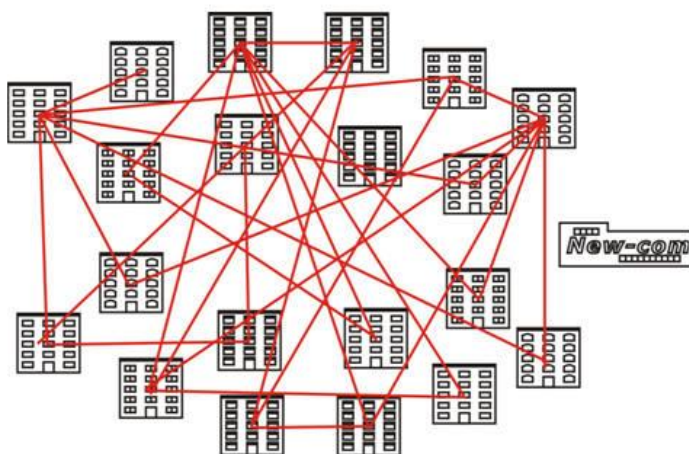
KOMMUNIKÁCIÓ 2004 + ZRINYI MIKLÓS NEMZETVÉDELMI EGYETEM + BUDAPEST, 2004. SZEPTEMBER 15.

ADATHÁLÓZAT



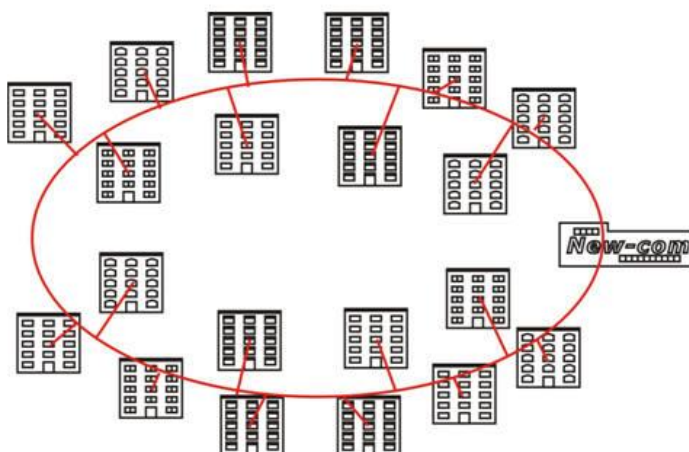
KOMMUNIKÁCIÓ 2004 + ZRINYI MIKLÓS NEMZETVÉDELMI EGYETEM + BUDAPEST, 2004. SZEPTEMBER 15.

ADATHÁLÓZAT



KOMMUNIKÁCIÓ 2004 * ZRINYI MIKLÓS NEMZETVÉDELMI EGYETEM * BUDAPEST, 2004. SZEPTEMBER 15.

ÜZLETI CÉLÚ HÁLÓZAT



KOMMUNIKÁCIÓ 2004 * ZRINYI MIKLÓS NEMZETVÉDELMI EGYETEM * BUDAPEST, 2004. SZEPTEMBER 15.

FÉNYVEZETŐSZÁL HEGESZTŐ



KOMMUNIKÁCIÓ 2004 + ZRINYI MIKLÓS NEMZETVÉDELMI EGYETEM + BUDAPEST, 2004. SZEPTEMBER 15.

FÉNYVEZETŐ KÁBEL KÖTÉS



FOSC 100



FOSC 400



FIST

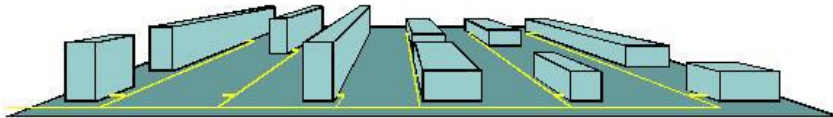
KOMMUNIKÁCIÓ 2004 + ZRINYI MIKLÓS NEMZETVÉDELMI EGYETEM + BUDAPEST, 2004. SZEPTEMBER 15.

UTCAI MIKROKÁBEL RENDSZER



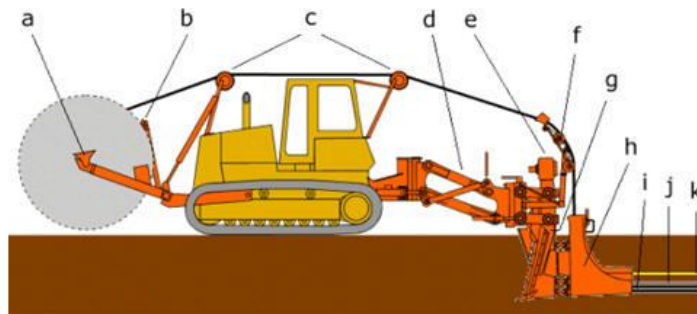
KOMMUNIKÁCIÓ 2004 * ZRINYI MIKLÓS NEMZETVÉDELMI EGYETEM * BUDAPEST, 2004. SZEPTEMBER 15.

UTCAI MIKROKÁBEL RENDSZER



KOMMUNIKÁCIÓ 2004 * ZRINYI MIKLÓS NEMZETVÉDELMI EGYETEM * BUDAPEST, 2004. SZEPTEMBER 15.

ERŐGÉPRE ÉPÍTETT VAKONDEKE



- | | |
|------------------|------------------------|
| a - dobtengely | b - dobfék |
| c - vezető görgő | d - gerendely |
| e - vibrátor | f - hossz mérő |
| g - eke | h - leeresztő kazetta |
| i - kábel | j - villámvédő vezeték |
| k - jelzőszalag | |

KOMMUNIKÁCIÓ 2004 + ZRINYI MIKLÓS NEMZETVÉDELMI EGYETEM + BUDAPEST, 2004. SZEPTEMBER 15.

ERŐGÉPRE ÉPÍTETT VAKONDEKE



KOMMUNIKÁCIÓ 2004 + ZRINYI MIKLÓS NEMZETVÉDELMI EGYETEM + BUDAPEST, 2004. SZEPTEMBER 15.



MARKOLÓRA ÉPÍTETT VAKONDEKE



KOMMUNIKÁCIÓ 2004 * ZRINYI MIKLÓS NEMZETVÉDELMI EGYETEM * BUDAPEST, 2004. SZEPTEMBER 15.



VAGONRA ÉPÍTETT VAKONDEKE



KOMMUNIKÁCIÓ 2004 * ZRINYI MIKLÓS NEMZETVÉDELMI EGYETEM * BUDAPEST, 2004. SZEPTEMBER 15.

CSIGÁS LÉGKÁBEL FÜGGESZTÉS



KOMMUNIKÁCIÓ 2004 + ZRINYI MIKLÓS NEMZETVÉDELMI EGYETEM + BUDAPEST, 2004. SZEPTEMBER 15.

LÉGKÁBEL FESZÍTŐSPIRÁL



KOMMUNIKÁCIÓ 2004 + ZRINYI MIKLÓS NEMZETVÉDELMI EGYETEM + BUDAPEST, 2004. SZEPTEMBER 15.

ZÚZMARA TERHELÉS

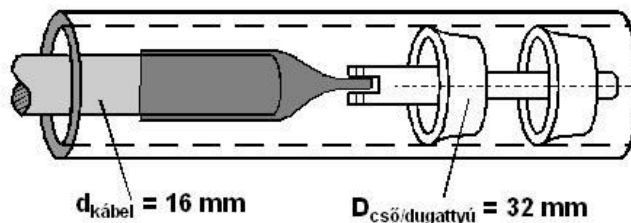


KOMMUNIKÁCIÓ 2004 * ZRINYI MIKLÓS NEMZETVÉDELMI EGYETEM * BUDAPEST, 2004. SZEPTEMBER 15.



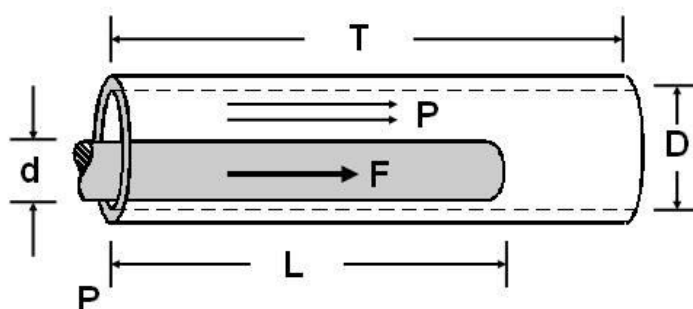
KOMMUNIKÁCIÓ 2004 * ZRINYI MIKLÓS NEMZETVÉDELMI EGYETEM * BUDAPEST, 2004. SZEPTEMBER 15.

DUGATTYÚS KÁBELBEFÚJÁS



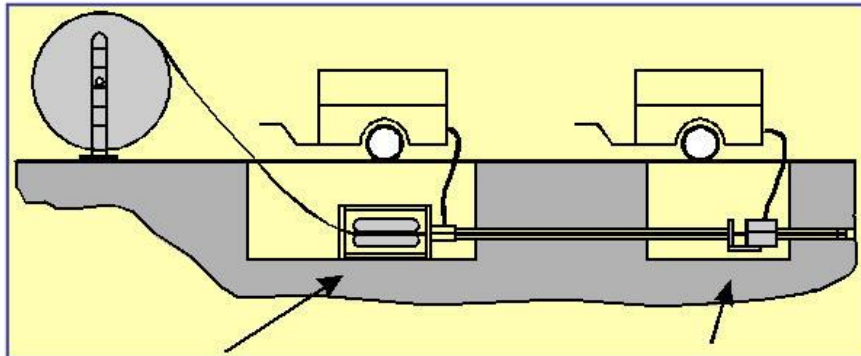
KOMMUNIKÁCIÓ 2004 + ZRINYI MIKLÓS NEMZETVÉDELMI EGYETEM + BUDAPEST, 2004. SZEPTEMBER 15.

KÁBELBEFÚJÁS



KOMMUNIKÁCIÓ 2004 + ZRINYI MIKLÓS NEMZETVÉDELMI EGYETEM + BUDAPEST, 2004. SZEPTEMBER 15.

KÁBELBEFÚJÁS

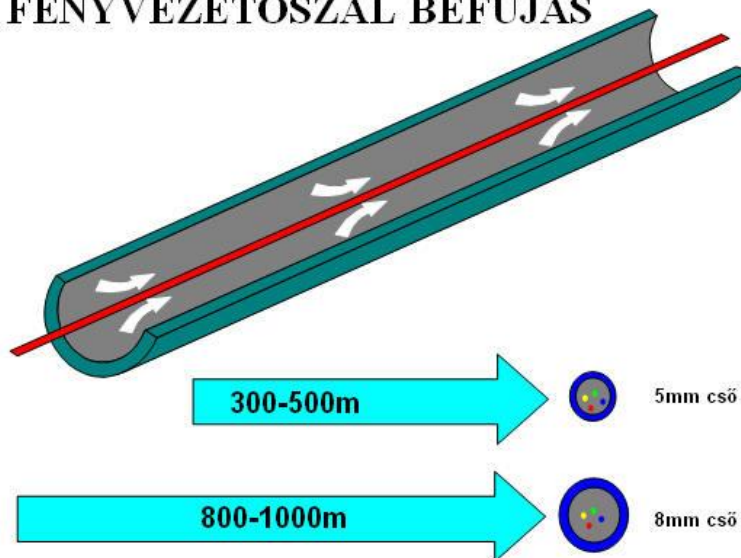


FIBERCAT

Kábel-BOOSTER

KOMMUNIKÁCIÓ 2004 * ZRINYI MIKLÓS NEMZETVÉDELMI EGYETEM * BUDAPEST, 2004. SZEPTEMBER 15.

FÉNYVEZETŐSZÁL BEFÚJÁS



300-500m



5mm cső

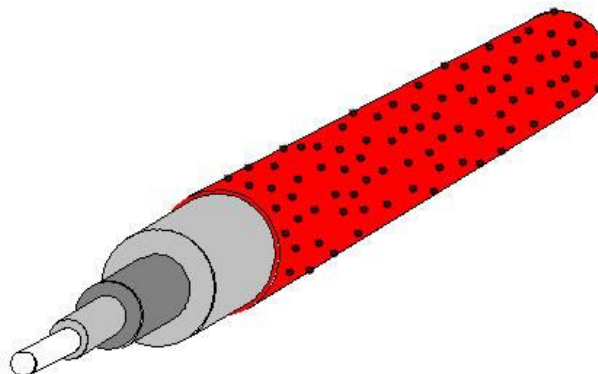
800-1000m



8mm cső

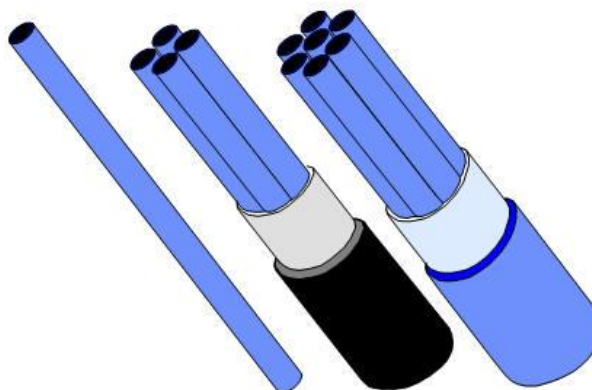
KOMMUNIKÁCIÓ 2004 * ZRINYI MIKLÓS NEMZETVÉDELMI EGYETEM * BUDAPEST, 2004. SZEPTEMBER 15.

BEFÚJHATÓ MIKROKÁBEL

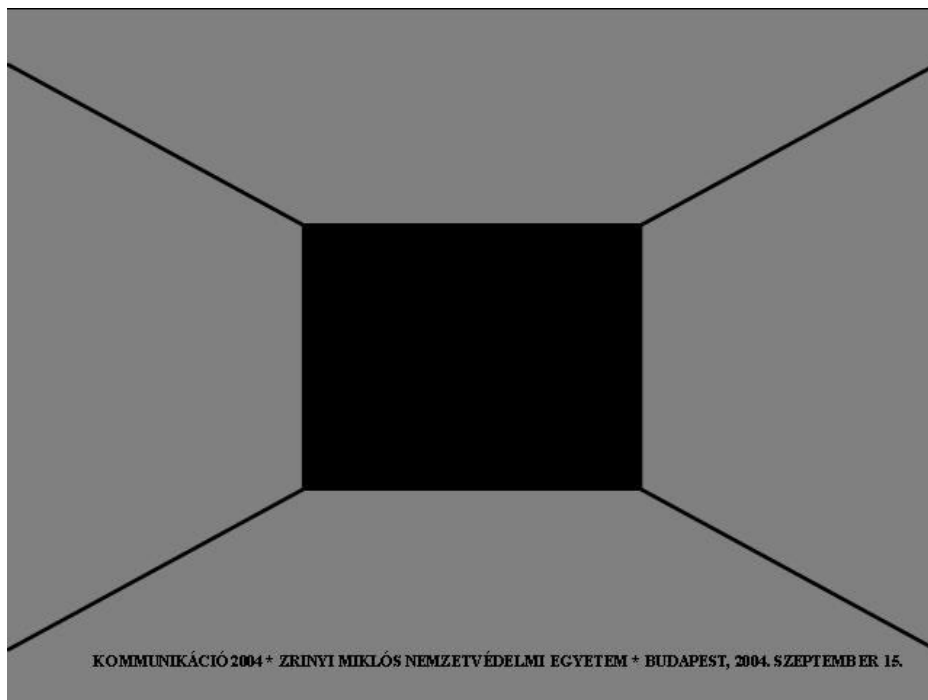


KOMMUNIKÁCIÓ 2004 + ZRINYI MIKLÓS NEMZETVÉDELMI EGYETEM + BUDAPEST, 2004. SZEPTEMBER 15.

BEFÚJÓCSŐ



KOMMUNIKÁCIÓ 2004 + ZRINYI MIKLÓS NEMZETVÉDELMI EGYETEM + BUDAPEST, 2004. SZEPTEMBER 15.



KÖSZÖNÖM A FIGYELMÜKET.

KOMMUNIKÁCIÓ 2004 * ZRINYI MIKLÓS NEMZETVÉDELMI EGYETEM * BUDAPEST, 2004. SZEPTEMBER 15.

TERRORIZMUS ÉS A KOMMUNIKÁCIÓ 2004.

Napjaink egyik fő problémája a terrorizmus.

Előadásomban szeretném egy bizonyos részterületét bemutatni és ismertetni, hogy napjaink terrorszervezetei milyen eszközökkel valósíthatnak meg kommunikációt. Kapcsolat felvételi és kapcsolattartási módszereket, titkosítási eljárásokat fogok ismertetni.

A lehetőségek csak egy kis területének előnyeit és hátrányait fogom bemutatni. Azon területét, amely már felderíthető és lefigyelhető lenne, ha országunkban és Európában működne az összehangolt felderítés és információcsere.

Ismereteim szerint azonban nem működik. Előadásom célja, hogy a lehetőségek tükrében felhívjam a figyelmet a véleményem szerint nem jól összehangolt felderítésre és az információcsere hiányára.

Előadásomban a rádióhullámok útján terjedő információk ellenőrizhetőségével kívánok foglalkozni. Ezen belül a rövidhullámú, az ultrarövidhullámú, mikrohullámú sávtartományokkal, valamint a műholdas telefonokkal.

Rövidhullámon megvalósíthatóak nagy távolságú összeköttetések. Korszerű rádiófelderítő eszközökkel a rádió-kisugárzás felderíthető. Az adóoldal közelében a legkönnyebb felderíteni, ugyanis a nagy távolságú összeköttetésekhez nagy adóteljesítmény szükséges, így a közel térben a forgalmazás egy spektrumanalizátor segítségével könnyen észlelhető. A kisugárzás helye iránymérők alkalmazásával meghatározható. A vételi oldal közelében már nehezebb a felderítés, mert több hasonló adás közül kell kiválasztani azt amit keresünk. Ha a keresett rádióösszeköttetésnek sem az adó körzete, sem a vevő körzete nem ismert, akkor is van lehetőség a felderítésére szinte a Föld bármely pontján, de ez függ az aktuális terjedési viszonyoktól, amit számos természeti jelenség befolyásol (napkitörés, meteorok stb.). Beszéd és adat típusú forgalmazás egyaránt lehetséges. Korszerű adaptív rádiómodemek alkalmazásával és gondos tervezéssel biztonságos, több kbit/s átviteli sebességű adatkapcsolat hozható létre számítógépek között több ezer kilométerre egymástól.

Az URH sávtartományban elég széles a rádióhullámok terjedési tulajdonságainak a skálája. Alsó tartományban rövidhullámú tulajdonságok, felső tartományban mikrohullámú tulajdonságokat figyelhetünk meg. Minél nagyobb a frekvencia, annál kisebb akadályt tud a rádióhullám „megkerülni”, mikrohullám esetén optikai rálátás szükséges az adóra. Vannak mobil és fix telepítésű rádiókészülékek. A mobil lehet járműbe épített nagyobb teljesítményű (15 – 100 W) illetve kézi kis teljesítményű rádió (0,2 – 15 W). Az összeköttetés maximális távolsága függ az alkalmazott rádió adóteljesítményétől, a használt antennától, a használt frekvencia terjedési tulajdonságaitól, terepviszonyoktól. Ez a távolság terjedhet néhány száz métertől több száz kilométerig. A több száz kilométeres összeköttetéshez fixen telepített nagy teljesítményű rádió és magas helyre kitett jó minőségű, az adott frekvenciára hangolt, sok elemből álló, irányított antenna szükséges.

A forgalmazás történhet analóg vagy digitális formában. Típusa lehet beszéd vagy adatátvitel. Az analóg beszéd különböző módszerekkel védhető a behallgatás

ellen, illetve titkosítható. Pl.: alapsávi gyors elhangolás pozitív és negatív irányba, sávfordítás, frekvencia-hopping, analóg VOICE-SCRAMBLER –ek alkalmazása. Ezek közül a frekvencia-hopping –ot alkalmazó rádiót a legnehezebb felderíteni, főleg ha széles sávban (több 10 MHz) történik a frekvenciák változtatása. Irányt mérni is nehéz az ilyen forgalmazásokra, ha azok rövidek vagy több magas épület van a környékén. A folyamatos vivőjű forgalmazások könnyebben felderíthetőek és azonnal felismerhető, hogy a forgalmazás típusa titkosított beszéd. Ezeknek a titkosított főniáknak a visszaállítására léteznek eszközök, de mi ilyenekkel nem rendelkezünk. A digitális beszédátvitelt nehezebb felismerni. Binárisan rejtjelezhető, ezért lehallgatása bonyolult. Többek között a Motorola cég gyárt olyan rejtjelező paneleket mely sokféle kézi adó-vevő készülékbe utólag is beépíthető. A kézi rádiókat a terroristák illetve azokat segítő személyek akciók lebonyolításában tudják használni.

URH sávtartományban könnyen megvalósítható a gyújtószerkezeteknek az indítása. A legegyszerűbb módszer az, ha egy autó távirányítós központi zárját használják fel. A szerkezet úgy működhet, hogy a rádióvevő egység érzékeli a távirányító által kibocsátott impulzus sorozatot, és az elektronikus kapcsoló (amely a zár nyitását, zárását indítja) zárja az áramkört az elektromos gyújtószerkezet és a gyújtófeszültséget biztosító akkumulátor között. Ahhoz, hogy a távirányító hatótávolságát megnöveljük, építeni kell az adott frekvenciára egy erősítőt, vagy venni egy adó-vevő készüléket. Az adóvevő készüléket SSB üzemmódban a távirányító frekvenciájára hangoljuk, ezáltal az impulzussorozatot lekeverjük az alapsávba. A távirányító jelét rögzítjük egy számítógép hangkártyájával vagy egy jó minőségű digitális diktafonnal, majd a kb. 15 W teljesítményű rádióadó, mikrofon-bemenetére vezetjük a hangkártya kimenetét és ugyancsak SSB üzemmódban kisugározzuk a visszajátszott jelet. Így akár több kilométer távolságból beindítható egy gyújtószerkezet. A központi zárok és a riasztók általában a 433.920 MHz frekvencián vagy ennek a környékén üzemelnek, de előfordulhatnak más sávokban is, ahol ilyen kis teljesítményű adók üzemelhetnek (446 MHz, 862 MHz). Az ilyen szerkezet ellen úgy lehet védekezni, hogy az adott frekvenciasávokat nagy teljesítményű adókkal zavarjuk. Számítógépek közötti adatkapcsolat megvalósítására a teljes URH sáv alkalmas. Létezik olyan katonai célra kifejlesztett, de a kereskedelmi forgalomban kapható rádiókészülék, mely a 30 – 70 MHz sávtartományban képes 64 kbit/s sebességű adatkapcsolatot létrehozni számítógépek között, mellyel valósidejű képátvitel is megvalósítható. Az összeköttetés távolsága több 10 km is lehet. Képes működni frekvencia-hopping –os vagy szórt spektrumú üzemmódban, melyek megnehezítik a felderítést. Az adatok valós idejű titkosítása és a kommunikációban résztvevők egymással szembeni hitelesítési eljárása szinte lehetetlenné teszik a passzív lehallgatást, illetve a rendszerbe történő behatolást és onnan az információk kinyerését. Létezik ennél könnyebben beszerezhetőbb és jóval olcsóbb megoldás is. WLAN eszközök alkalmazásával modern kommunikációs hálózat építhető ki, de egyszerű rejtett kommunikáció is megvalósítható. Pl.: 2 WLAN eszközzel felszerelt PDA számítógéppel és a megfelelő szoftverrel IP alapú telefonbeszélgetés is megvalósítható 300-400 méteres körzeten vagy egyenes rálátás esetén akár egy kilométeren belül anélkül, hogy bármilyen szolgáltatóhoz is csatlakoznánk. Ilyenkor a lehallgatást csak az adott eszköz közelében lehet megvalósítani. A WLAN eszközök segítségével már nagyon sok helyen hozzáférhetünk az Internethez. Ez a hozzáférés történhet szolgáltatón keresztül PRE-PAID–es kártyával vagy akár egy olyan nem kellően védett háló-

zatba való bejutással, amely rendelkezik Internet kapcsolattal és meg is osztja azt a hálózatban lévőkkel. Ezzel a módszerrel megszűnnek a távolságok és bármilyen információ könnyen és gyorsan eljuttatható a címzetthez. A WLAN eszközök felderíthetőségét és támadhatóságát jelenleg vizsgáljuk. Jó kommunikációs lehetőséget nyújt a mobiltelefon. Ez pedig az IP alapú kommunikáció. Azokra a telefonkészülékekre, amelyekre lehet JAVA alkalmazásokat feltölteni, létezik olyan szoftver, mely segítségével a telefonbeszélgetés nem a GSM TRAFFIC csatornáján valósul meg, hanem a GPRS kapcsolaton keresztül. Jelentek már meg olyan telefonkészülékek is, melyek rendelkeznek egy úgynevezett PUSH TO TALK funkcióval, amely szintén GPRS-en keresztüli IP alapú kommunikáció. Funkcióját tekintve ez úgy működik, mint egy adó-vevő rádiókészülék. Egyszerre több telefon is részt vehet a kommunikációban. 2005-től kezdve ezt a funkciót minden GSM telefonba be fogják építeni.

A 3 GHz fölötti tartományban a nagy adatforgalmú gerinchálózatok, GSM mikrolánc, telefonközpontok közötti összeköttetések, egymástól távolabb lévő számítógép-hálózatok közötti összeköttetések működtetésére használják. Előadásomban arra kívánom a figyelmet felhívni, hogy ezen a rendszeren továbbított információk védelme mennyire fontos. Képzelnék csak el, hogy a nem kellően védett információk milyen lehetőségeket biztosítanak egyes terrorszervezetek részére.

A műholdas telefonok is jó kommunikációs lehetőséget nyújtanak, azokon a területeken, ahol más hálózat nem elérhető, de ezek többségének a lehallgatására a nagy gyártók (Pl.: Rhode & Schwarz) kínálnak különböző eszközöket. Viszonylag nagy távolságból lehallgathatóak.

AZ OFDM ELJÁRÁSOK A VÉDELMI CÉLÚ MOBIL TÁVKÖZLÉSBEN

Dr. Dárdai Árpád, okleveles híradástechnikai szakmérnök,
a Magyar Hadtudományi Társaság szakértője
dardai.arpad@axelero.hu

Bevezetés

A katonai és a polgári vezetéknélküli távközlésnek az utóbbi években a legdinamikusabban fejlődő ágazata a különféle kód, ill. frekvenciaosztású többszörös hozzáférési eljárásokat felölelő technológiák. Ilyenek az SST-CDMA (Spread Spectrum Technique - Code Division Multiple Access – szórt spektrumú technika – kódosztásos többszörös hozzáférés), és az OFDM (Orthogonal Frequency Division Multiplexing – ortogonális frekvenciaosztásos többszörös hozzáférés) eljárások. Szerepük a polgári és a katonai távközlésben egyre nagyobb.

A katonai vezetéknélküli távközlésben kiemelkedően fontos a titkosság, a megbízhatóság és a hálózat elosztott területi működőképessége. Kombinálva a fenti hozzáférési technikákkal, ezen belül is különösen az OFDM eljárással, egyéb, területileg elosztott hálózati technikával, pl. az alkalmi, vagy más szóval az ad hoc hálózati megoldásokkal, a nemzetvédelmi és a katonai távközlést a vezetés és a csapatok számára igen hatékonyra és megbízhatóvá teszi. E tulajdonságokat, és a hálózat állékonyságát tovább növelheti a csomagkapcsolt Internet Protokoll és szolgáltatásainak alkalmazása. A fejlett távközlő és hálózati technikák között meg kell említeni a LAN és a WLAN rendszereket is, amelyekben a fenti CDMA és OFDM vezetéknélküli hozzáférési technikákat széles körben alkalmazzák.

Az előadás a vezetéknélküli többszörös hozzáférési-, közöttük is, a vezetéknélküli rendszerekben egyre fontosabb OFDM eljárásokat tekinti át. A védelmi, katonai alkalmazási lehetőségek és az ilyen megoldások értéknövelő hatásai között hangsúlyozzuk, hogy a fejlett technológiák, különösen az OFDM eljárások bevezetése a védelmi-biztonsági távközlésben, biztosítja a képességet a rádiótechnikai, a távközlési és az informatikai fölényhez is.

Multiplexelési eljárások vezetéknélküli rendszerekhez

A multiplexelés definíciója és célja

A multiplexelés definíciója. A multiplexelés, vagy csatornamegosztás, vagy többszörös hozzáférés az a folyamat, amely több felhasználó számára lehetővé teszi azt, hogy egy távközlési csatornát megosztva, a csatornához hozzáférjenek. A többszörös hozzáférés tehát egy olyan technika, amelynek segítségével számos felhasználó hozzáférést nyerhet egy közös távközlési csatornához. A többszörös hozzáférés multiplexerrel valósítható meg. A multiplexer olyan készülék, amely számos jelet multiplexel, vagyis nyalábol egy közös távközlési csatornába. A multiplexelés számos módon megoldható, így beszélhetünk frekvenciaosztásos (FDMA), időosztásos (TDMA), kódosztásos (CDMA), ortogonális frekvenciaosztásos (OFDM), vagy egyéb, más elven történő többszörös hozzáférésről.

Az OFDM ortogonális frekvenciaosztásos többszörös hozzáférés

Az OFDM az ortogonális frekvenciaosztásos többszörös hozzáférés rövidítése. Az OFDM egyike a digitális modulációs és távközlési átviteli technikáknak. Az eljárás a távközlési csatornát nagyszámú, egyenlő osztású frekvenciasávokra osztja. Minden egyes sávban egy alvivőfrekvencia továbbítja a teljes felhasználói információk meghatározott részét. Az alvivők egymással kölcsönösen ortogonálisak. Az OFDM átvitt adat alvivők ortogonalitása különbözteti meg a hagyományos FDM eljárásoktól. Egyetlen átvitt adat szimbólum idő alatt ortogonális villamos rezgések százait, ezreit multiplexálja és viszi át a rendszer.

A multiplexelés távközlési alkalmazásai

A többszörös csatorna-hozzáférési eljárások használata szinte valamennyi távközlő-rendszer lényeges sajátja, fontos része. Követelmény, a hálózat olyan legyen, hogy egyes csomópontok meghibásodása, kiesése ne akadályozza a hálózat további működését. Ilyen tulajdonságokkal rendelkeznek a csomagkapcsolt hálózatok (pl. X.25), az Internet és az Internet Protokollt (IP) használó hálózatok, valamint az alkalmi (ad hoc) hálózatok, amelyeket egyre inkább használnak mind a polgári, mind a katonai távközlési rendszerekben.

A távközlő-rendszerek fejlődése során, az egyre újabb rendszer-generációknál a multiplexelés átviteli sebességével és a mobilitással szemben egyre magasabb követelmények léptek fel. A 3G, és különösen a 4G rendszerek, valamint a WLAN megoldások rádióinterfészében fontos szerepet kap a CDMA és az OFDM hozzáférési mód. Az OFDM kiválóan alkalmas szélessávú digitális adatátvitelhez: HDTV (High Definition Television), 4G mobil rendszerek, egyéb távközlési feladatok (pl. ADSL, IEEE802.11a szabványú WLAN) és a korszerű katonai távközlés.

Nemzetközi programok.

A CDMA és az OFDM technikákkal és fejlesztésével, szabványosításával, elterjesztésével, valamint bevezetési kérdéseivel nemzetközi távközlési szervezetek és nemzetközi programok (ETSI – European Telecommunications Standard Institute, COST – Cooperation on Science and Technology, IEEE – Institute for Electrical and Electronics Engineers) foglalkoznak összehangolt munkamegosztással. A COST program, amely számos egyéb projekt között a fejlett hozzáférési technikákkal (CDMA, OFDM) is foglalkozik, jelentősen hozzájárult a 2G, 3G, 4G rendszerek rádiós interfészének kifejlődéséhez. Fontosak még az IETF gondozásában kidolgozott Internet szabványok és ajánlások (RFC Request for Comment) is.

Az OFDM technika kialakulásának főbb állomásai

Az OFDM többszörös hozzáférési eljárást számos tudományos munka, kísérlet és kezdeti kutatás után 1950-es években kezdték javasolni és alkalmazni. Ezekben az években a többszörös vivőjű modulációs technikákat (MCM Multi Carrier Modulation) katonai és polgári célokra egyaránt használták (pl. rövidhullámú katonai MCM rádióösszeköttetések). Az 1960-as évekre lényegében befejeződött az OFDM – amely az MCM átvitel egy olyan speciális változata, amelynél az alvivők ortogonálisak – elméletének kidolgozása. Az 1970-es években már olyan OFDM megvalósításokat is használtak, amelyek diszkrét vagy más szóval gyors Fourier-transzformációt

(DFT Discrete Fourier Transform, FFT Fast Fourier Transform) alkalmaztak. Az 1980-as években nagy sebességű modemekhez és digitális mobil összeköttetésekhez használták. 1987-ben az OFDM átvitelt digitális hang műsorszórásra (DAB) is kezdték használni Európában. Az 1990-es évektől szélessávú mobil összeköttetésekhez, xDSL digitális előfizetői vonalakhoz, és DAB, DVB, ill. HDTV célokra alkalmazták. Ma az OFDM eljárást már a távközlés számos területén használják (xDSL, WLAN, DAB, DVB, HDTV, DMB, UMTS, 4G mobil rendszerek, katonai alkalmazások).

Az OFDM multiplex eljárás tulajdonságai

A szimbólumközi interferencia hatása a hozzáférési technika választására

A rádiócsatorna tulajdonságai (többutas hullámterjedés, frekvencia szelektivitás, Doppler-hatások és a mozgás következtében időbeli szórás), és hatásukkal, pl., a szimbólumközi interferenciával (ISI Inter-Symbol Interference) kapcsolatos megfontolások arra ösztönöztek, hogy a jelenleg rendelkezésre álló csatornamegosztást nyújtó hozzáférési technikák (FDMA, TDMA, CDMA) mellett, ezek tulajdonságai, előnyei, és az újabb igények (mobil multimédia, szélessávú alkalmazások, fokozott biztonság) alapján, más átviteli és többszörös hozzáférési eljárást keressenek. Ebbe az irányba terelte a kutatókat az is, hogy jelentősen nőtt az igény az átvitt információk biztonsága és a fokozott titkosítás iránt is. Ezek az OFDM többszörös hozzáférési eljáráshoz vezettek, amely a mobil 4G rendszerekhez és a korszerű katonai vezeték nélküli távközléshez megfelelő jelöltnek tűnik.

Az OFDM eljárás alapgondolata és alkalmazásai

Az OFDM (Orthogonal Frequency Division Multiplex) frekvenciaosztású átvitel és többszörös hozzáférés alapgondolata, hogy egy nagy adatátviteli sebességű adatfolyam több kisebb adatátviteli sebességű adatfolyamra osztható. Ezek alvivőinek modulációja egyedi, a többitől független, és azokkal egy időben történik. Ezzel a módszerrel a részcatornák, ill. az alvivők adatátviteléhez tartozó szimbólumidő az eredeti szimbólumidő többszöröse lesz, ezáltal a részcatornák átvitele ellenállóbb a csatorna többutas hullámterjedés okozta idősórásával és a zajokkal szemben. A vivőfrekvencia összetevők kölcsönösen ortogonálisak.

Ha nagy adatátviteli sebesség szükséges mobil környezetben (frekvencia-szelektív fadinges, időben szórt rádiócsatornán), és amelyeknél a szimbólum időhöz képest a maximális késleltetés viszonylagosan nagy, megfelelő megoldást ad az OFDM átviteli és hozzáférési mód. OFDM ortogonális frekvenciaosztású multiplex eljárást használnak, pl., a digitális hang- és képműsorszóró rendszerek, az ETSI BRAN, az ETSI HIPERLAN/2 és az IEEE 802.11a szerinti WLAN eszközök, de ez az átviteli mód a 3G, még inkább a 4G mobil távközlő-, és a megfelelő fejlettségű katonai távközlő rendszerekben is egyre fontosabb szerepet kap.

Az OFDM jel sávszélessége és spektruma

Az OFDM tehát olyan átviteli és multiplex eljárás, amely nagyszámú, ortogonális frekvenciát alkalmazva, a frekvencia összetevőkkel kódolva, és a frekvencia összetevőket modulálva viszi át a kívánt információkat a küldőtől a rádiócsatornán a kívánt című célhelyre, miközben jelentősen csökkenti a többutas hullámterjedés okozta interszimbólum interferenciát. Az OFDM az adatszimbólumokat a nagyszámú frek-

vencia-összetevő segítségével párhuzamosan viszi át. Az adatszimbólumok továbbítása így a szélessávú OFDM jelet nagyszámú keskenysávú jelösszetevőre bontva, az egyes különálló frekvencia-összetevők segítségével, keskenysávú átvitelrel történik. Az átvitel után az összetevők adatfolyamát egyesítik és visszaalakítják az eredeti nagy adatátviteli sebességű, nagy sáv szélességű adatfolyamot. A szélessávú jel további feldolgozása és felhasználása a vétel helyén ezt követően történik. A rádiócsatorna átviteli függvénye frekvencia és időfüggő, de a kézi és a mobil állomások mozgása miatt, helyfüggő is.

Az OFDM átvitelnél az alapsávi alvivő-impulzusok időfüggvényének alakja szinusznégyszög. Ha a vivők száma N , akkor az OFDM jel teljes B sáv szélessége a frekvencia-összetevők számától és a közöttük lévő $f_0 = \Delta f = 1/T_r$ távolságtól függ, vagyis $B \approx N / T_r = N \cdot \Delta f$.

A Fourier-transzformáció elmélete szerint a szinusznégyszög impulzus frekvencia-spektruma $\sin x/x$ alakú. Az egyenlő Δf alvivőtávolság paraméterválasztással az alvivők spektruma nem lesz teljesen elválasztva. Az OFDM jel különböző ortogonális összetevőinek spektrumai átlapolódnak, de az összetevők spektrumainak maximumai a többi frekvencia összetevő spektrumának minimumaival esnek egybe, az OFDM jel összetevőinek egymással kölcsönös ortogonalitása következtében. A spektrumok egyéb részei Δf távolságokként, a spektrumok zérus értékeinél kereszteződnek. A teljes OFDM spektrum kialakításánál arra is törekszenek, hogy az alvivők spektrum energiájának döntő része egy adott, meghatározott sáv szélességen belül legyen, és az átlapolódás ellenére is, a szomszédos frekvencia-összetevő sávjába minél kevesebb energia jusson. Az alvivőspektrumok kialakítása következtében, a teljes OFDM jel B sáv szélességű spektrumának alakja gyakorlatilag négyszögletes, ami az OFDM jel nagy spektrumhatékonyágát mutatja.

A részcsatornák átviteli függvénye

Az OFDM jelet a $H=H(f,t)$ átviteli függvényű csatorna továbbítja. A H átviteli függvény a frekvencia és az idő függvénye, de a részcsatornák átvitelére nem a szélessávú jelre vonatkozó átviteli függvény érvényes, hanem csak a Δf sáv szélességre eső, ami jó közelítéssel konstans. A keskenysávú részcsatornáknál – megfelelő tervezéssel – az adatszimbólum ideje már lényegesen nagyobb lehet, mint a rádiócsatorna maximális késleltetése, ennek következtében a részcsatornák már nem frekvencia-szelektívek és nincs vagy csak csekély az időbeli szórásuk, vagyis az OFDM átviteli eljárás – legalábbis a részsávokban – az ISI interferenciákat gyakorlatilag kiküszöböli. További előny a frekvencia-szelektív rádiócsatorna esetén az egyfrekvenciás szélessávú rendszerhez képest az, hogy a részcsatornákra bontott szélessávú rendszer részcatornás vevőiben jelentősen csökken a kiegyenlítőik számítási igénye.

Az OFDM jelek előállításának alapelvei

A gyors Fourier-transzformáció származtatása

Az OFDM jel előállítása során a modulált jel, mint időfüggvény feldolgozása, megfelelő kialakítása, átalakítása, felbontása és előállítása a harmonikus függvények elmélete szerint (analízis, szintézis) történik. Ennek matematikai módszere a Fourier-transzformáció. A harmonikus felbontás és a harmonikusok kezelése az OFDM modu-

láció és demoduláció lényege. A harmonikusok módszere előnyös is, mert a szinusz hullámok előállítása, paramétereinek változtatása egyszerű, a vonatkozó matematikai eljárások kidolgozottak, valamint, az átviteli rendszerek szinuszos hullámú gerjesztésre adott válasza (a tranziensek után) szintén szinuszos, amelyeknek frekvenciája a gerjesztőével azonos, csak a kimenőjel amplitúdója és a fázisa térhet el. Ezek a Fourier-módszerek alkalmazását indokolják. Az OFDM esetében különösen fontos a gyors Fourier-transzformáció, amely szintén a Fourier-módszerek családjába tartozik. A gyors Fourier-transzformáció terén Cooley és Tukey munkái (1965 körül) fontosak.

Az OFDM adási alapsávi jel és az OFDM átvitel megvalósítása

Az OFDM eljárást megelőző más sokvívös modulációs eljárások (FDMA, MCM) jellemzője, hogy a részsávok (csatornák) között biztonsági frekvencia-eltávolítást alkalmaztak, annak érdekében, hogy a szűrők a jeleket biztonságosan szétválaszthassák. Az OFDM megoldás rész-frekvenciasávjai ezzel szemben átlapolódnak. Ez azért lehetséges, mert a nagyszámú részvívők egymással kölcsönösen ortogonálisak. Az OFDM jel ortogonális összetevőinek és az átlapolódó spektrumoknak az előállítása az adó és a vevő oldalon digitális jelfeldolgozó eljárásokkal történik. A digitális moduláció a szinuszos jelek három paraméterét modulálhatja: amplitúdó, frekvencia és fázis (ASK, FSK, PSK). Az OFDM átvitelnél a QAM vagy az ASK és a PSK moduláció kombinációja (APSK) szokásos.

Matematikai számításokkal levezethető, hogy az alapsávi jel előállításához N darab alvívő generátor és N darab alvívő modulátor szükséges, vagyis a teljes modulált időfüggvény a külön-külön, de egyidejűleg modulált alvívők időfüggvényeinek összege. Az időfüggvény generálása a nagyszámú modulátorok készítése nélkül, a külön-külön modulált alvívők előállítása és összegzése helyett, a Fourier-transzformáció eljárásaival is megoldható.

Az OFDM jel előállítása és az OFDM átvitel a 0. pontban vázolt matematikai összefüggések alapján megvalósítható.

Hálózati kialakítás az OFDM rendszerrel

A OFDM átviteli rendszer hatásos megoldás a többutas hullámterjedés káros hatásának kivédésére, ellensúlyozására. E tulajdonságánál fogva a OFDM átvitel megfelelően működhet egy egyfrekvenciás (SFN – Single Frequency Network) hálózatban is. Ez azt jelenti, hogy a cellák adói ugyanazon a frekvencián működhetnek, vagyis az A_1 , A_2 , ..., A_n adók valamennyien az f_1 frekvenciát használhatják. Hasonló a tulajdonságot mutatnak a CDMA rendszerek is.

OFDM átviteli és hozzáférési technikák

Kombinációs lehetőségek.

Kezdetben az FDMA, majd a TDMA, majd a CDMA hozzáférési megoldások alakultak ki. Ezeket követte az egyre fontosabb OFDM (ortogonális FDM) frekvenciaosztású multiplex eljárás is, és kialakultak ezek kombinációiként további multiplex és hozzáférési elvek is, amelyek a rádiós rendszerekben is használatosak. Az OFDM megoldás lényegében egy átviteli technika, amelyet az OFDM kezdeti alkalmazásai között, egyebek mellett a digitális hang és videó műsorszóró rendszerekhez használtak, majd távközlési felhasználása is megjelent a LAN (HIPERLAN/2, IEEE802.11a)

rendszerekben. Az OFDM az átviteli alkalmazások mellett többszörös hozzáférési technikaként is használható, ha kombináljuk az FDMA, TDMA, CDMA eljárásokkal: így kapjuk az OFDM-FDMA, az OFDM-TDMA és az OFDM-CDMA hozzáférési eljárásokat.

Hibrid és egyéb OFDM hozzáférési rendszerek

A fenti három fő hozzáférési osztály tovább kombinálható, és különféle hibrid rendszerek alakíthatók ki. Így olyan (3G, 4G) rendszerek valósíthatók meg, amelyek az ellátási feltételek, az összeköttetés jellege (mozgó gépjármű, gyalogos felhasználó, otthoni környezet, ill. a megfelelő védelmi alkalmazások), és a szolgáltatás típusa, a szolgáltatással szembeni követelmények szerint választja meg a hozzáférés módját, típusát. Néhány típus: OFDM-CDMA/FDMA, CP-OFDM (Cyclic Prefix), OFDM-MIMO (MIMO Multiple Input – Multiple Output). Egyéb megoldások is kialakultak: TDS-OFDM (TDS Time Domain Synchronous), és a COFDM (Coded OFDM) eljárás. A kódolás mellett titkosító eljárások is használhatók. A COFDM (Common Frequency FDM/OFDM) a gyakori elnevezése annak a rendszernek is, amelynél az OFDM átviteli mód alapvető tulajdonságának megfelelően, a bázisállomások azonos adási frekvenciát használnak.

Védelmi jelentőség, alkalmazási lehetőségek

Alapkövetelmények

A védelmi és biztonsági távközlés korunk igen fontos igénye. A távközlésnek mindig fontos szerepe volt a különböző korok vezetési, védelmi, biztonsági, katonai és hadviselési tevékenységében, de napjainkban ez fokozottan hangsúlyos. Egyre nagyobbak az igények a távközlési rendszerekkel szemben mind a védelmi, harcászati, taktikai mind a stratégiai alkalmazási területeken. Mindez a távközlés folyamatos fejlődését és az intenzív fejlesztéseket ösztönözte, és a 3G (harmadik generációs), ill., a 4G (negyedik generációs) védelmi-biztonsági távközlő rendszerek tervezéséhez és kifejlesztéséhez, ill., megjelenéséhez vezetett.

A fenti védelmi és biztonsági célokat szolgálják az alábbi távközlési alapkövetelmények: a távközlés és a távközlő rendszer legyen biztonságos, nehezen felderíthető, nehezen zavarható, nehezen megfejthető, hamisan nehezen megismerhető, és megismerhető. Ezekből levezethetők a következő koncepciók, amelyeket a védelmi-harcászati távközlőrendszereknek teljesíteni kell: kis valószínűségű észlelés (LPI – Low Probability of Interception), kis valószínűségű detektálás (LPD – Low Probability of Detection), kis valószínűségű irányazonosítás (LPDF – Low Probability Direction Finding), kis valószínűségű azonosítás kiértékelés (LPIE – Low Probability Identification and Evaluation, ill., kisvalószínűségű érzékelés és kihasználás (LPIE – Low Probability of Interception and Exploitation).

Hálózatos követelmények

A korszerű hadviselés az előző korok hadviselési technikáit, információ továbbítási rendszereit jelentősen megváltoztatta. A hálózatos koncepciók a hadviselésben is kialakultak. A hálózatos hadviselés a védelmi, harci tevékenységben a különböző hierarchia szinteken résztvevő elemeket (vezetés, parancsnokok, fegyvernemek, irányítók,

végrehajtók, katonák, védelmi távközlés, logisztika, egyéb elemek) hálózati rétegeknek és egységeknek tekinti és a közöttük levő kapcsolatokat a hálózat szerkezete, feladata és felépítése szerint határozza meg. A korszerű védelmi-harcászati távközlési elképeléseket ennek megfelelően hálózatos szemlélettel is kibővíti. A védelmi-harcászati távközlést mind a hadviselésben alkalmazott távközlés csomópontjainak és protokolljainak hálózatos jellege és funkcionalitása, mind a topológia és rendszerkialakítás (infrastrukturális, ad-hok és vegyes) hálózatos szerkezete és működése jellemzi. Ezek a koncepciók együttesen: hálózatközpontú hadviselés (NCW – Network Centric Warfare), ill. hálózatos harcvezetés (NCW – Network Control Warfare).

Az OFDM átvitelt és az OFDM alapú többszörös hozzáférési megoldásokat, vagyis az OFDM-FDMA, -TDMA, -CDMA és a hibrid rendszereket, ill., a segítségükkel megvalósított távközlési technikákat a fenti szempontok alapján megvizsgálva megállapítható, hogy az OFDM átvitel és az OFDM hozzáférési változatok közül főleg az OFDM-FDMA és variánsai, ill., az OFDM-FDMA/CDMA kombinációk a felsorolt védelmi és hadviselési követelményekből adódó szempontoknak kiválóan megfelelnek. Az OFDM rádióinterfész segítségével a fenti feladatok végrehajthatók, megfelelően támogathatók. Távlatilag fontos az OFDM/MIMO eljárás is.

Megnövelt védelmi és értéknövelő képesség, korszerű koncepciók

A korszerű vezetési és védelmi, ill., katonai távközlés alapvető követelményeit és az ebből adódó szolgáltatásokat az OFDM alapú távközlés magas szinten képes teljesíteni. A megnövelt védelmi képességek és értéknövelő szolgáltatások az OFDM tulajdonságaiból levezethetők.

A védelmi távközlés hálózati struktúrája

A hálózat centrikus hadviselés (NCW) topológiája és rendszerkialakítása támogatja az alkalmazási feltételek és követelmények szerinti hálózat típusokat. Ez lehet infrastrukturális, ad-hok, vagy vegyes struktúrájú. Ezeket a szerkezeteket és a megfelelő alkalmazásokat az IPv6-os protokollkészlet is támogatja, ezért a korszerű védelmi távközlés célszerűen IPv6 alapú. A fenti elveknek megfelelő, hálózati koncepciójú (NCW), összetett védelmi távközlőhálózat kialakítását az OFDM technológia támogatja. Az ilyen hálózat vezetéknélküli hozzáférési része cellás rendszerű.

A hálózat centrikus hadviselés (NCW) topológikus és rendszertechnikai kialakítása a következő szolgáltatásokat és kialakításokat támogatja: infrastrukturális hálózatok, ad-hok hálózatok, vegyes szerkezetű hálózatok, a hálózat egyes elemeinek kiesése esetén a hálózat működőképes marad. A rendszer támogatja az IPv6 alapú ügyfél-ügynök/terminál és ügynök-kiszolgáló, ill. az ügyfél-ügyfél (terminál-terminál) kapcsolatokat és a mobilügynök funkciókat, a műholdas távközlő és helymeghatározó rendszerekhez való csatlakozást (pl. GPS, FÁK műholdas helymeghatározó rendszer, EU Galileo), az anti EBO (Effect Based Operations – hatásalapú műveletek) felépítést és tulajdonságokat. Az ügyfél ügynök/kiszolgáló, ill., az ügyfél-ügyfél kapcsolat biztosítja azt, hogy az ügyfél a hálózat szolgáltatásaihoz az előírások és a követelmények szerint a megfelelő kiszolgálón, ill. ügynökön keresztül hozzáférhessen és a jogosultságainak és a hálózat topológiájának megfelelően kommunikálhasson.

A mobilügynök funkciók lényege az, hogy meghatározott (vezetési, irányítási) csomópontokból olyan szoftver entitások indíthatók és jutnak el a hálózaton a kívánt

csomópontokba, amelyek ott saját magukat installálva, indítva, meghatározott feladatokkal (ügyfél, ügynök, kiszolgáló, tesztelés, ellenőrzés, átkonfigurálás, feladatok végrehajtása, adatok gyűjtése és továbbítása a kívánt helyre, stb.) rendelkeznek. A mobilügynök a kívánt csomópontokba vagy hálózatrészekbe jutva, feladatát végrehajtja. Ezek közé tartozhat az is, hogy feladat teljesítése után a csomópontot elhagyja, vagy önmagát megsemmisíti.

A korszerű védelmi távközlés legyen anti EBO tulajdonságú és képességű. Az EBO koncepció lényege a következő. A koncepció az ellenséget olyan tárhálós objektumnak tekinti, amely hierarchikus (vízszintes, függőleges, stb.) síkokkal és benne csomópontokkal építhető fel. A koncepció keresi a térháló fontos elemeit a megfelelő síkokban. A koncepció szerint elegendő csak ezeket megsemmisíteni vagy megromlítani, ahhoz, hogy az ellenség fontos objektumai, létfontosságú rendszerei, távközlés, szállítása működésképtelenek legyenek. Fontos követelmény, hogy a védelmi távközlés anti EBO (AEBO – anti EBO) tulajdonságú legyen, vagyis a fontos elemek tartalékoltak, nehezen azonosíthatók és nehezen megsemmisíthetők legyenek.

A védelmi URH rádióhálózatok frekvenciasávjait, cellaszerkezetét, rádiótechnikai paramétereit, az adatátviteli sebességet, hálózati- és rádiós protokolljait, a felhasználás jellege és a követelmények (pl. multimédiás feladatok) szerint lehet meghatározni.

A védelmi távközlőhálózat szolgáltatásai

A hálózat centrikus hadviselés (NCW – Network Centric Warfare) hálózatos jellegének és funkcionalitásának területén a védelmi-harcászati távközlés fogalomkörét az Internet Protokoll 6-os verziójára (IPv6) alapozott katonai távközlés képviseli, amelynek tulajdonságai és szolgáltatásai és kiegészítései nyújtják a megfelelő biztonságos működést. A biztonságos működés néhány főbb területe: titkosság, átvitel védelem, biztonságos átvitel, védelem a behatolásokkal szemben, hierarchikus zárt felhasználói csoportok definiálhatósága, együttműködés más kapcsolódó rendszerekkel, alrendszerrel, ill. robotokkal, a hálózat működésének védelme és működése akkor is, ha a hálózat egyes elemei megszűnnek működni, valamint számos egyéb feladat és funkció támogatása (pl. mobilügynök, anti EBO jelleg).

Követelmény, hogy a védelmi távközlés szolgálja és támogassa a védelmi feladatok magas szintű ellátásához szükséges egyéb szolgáltatásokat, így a fejlett információcserehez szükséges multimédiás alkalmazásokat, és a védelmi tevékenységek távközlési, informatikai, vezetési támogatását.

Az átviteli biztonság védelmi mechanizmusai

A védelmi hálózat átvitelének és rendszerének biztonságát, védelmét több mechanizmus egyidejű működése szolgálja. Az alkalmazott és működő eljárások attól is függenek, hogy az átvitel milyen jellegű, milyen műszaki megoldású. Az OFDM alapú átvitel esetében fontos és hatásos védő mechanizmusok mutatkoznak: saját magából adódó technikai védettség, hatékony csatornakódolás és titkosítás, a WLAN rendszerekre kifejlesztett titkosítás, az Ipv6-os protokollból adódó védelmek, egyéb műszaki, informatikai, kódolási, titkosítási megoldások, és szervezeti, szervezési intézkedések, ill. ezek kombinációja.

Az OFDM adás előnyei és hátrányai, értéknövelő képességek

Az előző fejezetek és pontok alapján egybevetjük az OFDM adás előnyeit és hátrányait. Az előnyök és hátrányok egybevetéséből az előnyök a túlsúlyosak. A hátrányok a korszerű jelfeldolgozási módszerekkel és a modern áramkörtechnikával kiküszöbölhetők.

Az OFDM modulációs módú rádiófrekvenciás átvitel és többszörös hozzáférés az eddigi védelmi távközlő rendszereknél lényegesen előnyösebb, az alábbi szempontok alapján, és az alábbiakra való alkalmasság és képesség következtében: hálózatos szemlélet, átviteli és megbízhatósági tulajdonságok, csatlakoztathatóság és együttműködési képességek (pl.: UAV – Unmanned Aerial Vehicle, és UGV – Unmanned Ground Vehicle objektumokkal), és kedvező frekvenciafelhasználás.

Irodalom

- [1] Pap László Dr.: A hírközlő csatornák fizikai védelme, szórt spektrumú eljárások. Híradástechnika, XLVI/1995.03.
- [2] Pap L., Dr.-Dárdai Á., dr.: SST-CDMA rendszerek tulajdonságai. Cellás rendszerek összehasonlítása. Híradástechnika, XLVI. évf. 1995. április.
- [3] Sklar, Bernard: Digital Communications. Fundamentals and Application. Prentice-Hall, Englew. Cliffs, N.J. 1988.
- [4] Stallings, William: Handbook of Computer Communications Standards. Local Area Network Standards. Volume 1., 2., 3. Second Edition. Howard W Sams and Company Carmel, USA.
- [5] Cooley, J. W.–Tukey, J. W.: An algorithm for the machine calculation of complex Fourier series. Mathematics of Computation. 1965. 19, 90.
- [6] Brigham, E. Oren: The Fast Fourier Transform and its Application. Englewood Cliffs, Nj, Prentice Hall Inc., 1988.
- [7] Casas – Leung: OFDM for Data Communication Over Mobile Radio FM Channels – Part I.: Analysis and Experimental Results. IEEE Transactions on Comm. Vol. 39. May 1991.
- [8] Casas – Leung: OFDM for Data Communication Over Mobile Radio FM Channels – Part II.: Performance Improvement. IEEE Transactions on Comm. Vol. 40. April 1992.

AZ MH MRR HARCÁSZATI RÁDIÓK ALKALMAZÁSA

DLask Róbert hallgató, Zrínyi Miklós Nemzetvédelmi Egyetem
KMKA-2 tanulócsoport

Bevezetés

Az MH eddigi külföldi szerepvállalása leginkább a békefenntartás volt, melyben eddig nem nagy létszámú csapatokkal képviseltette magát hazánk (Ciprus, Sínai-félsziget, Mozambik, Angola – rendfenntartó, őr egységek). A jövőben azonban ez változni fog, melyet bizonyít hazánk részvétele Irak megszállásában. Az MH kijelölt állománya szállítási feladatokat végez, és az itt lévő csapataink létszáma már eléri a zászlóalj szintű erők létszámát. Itt kell megemlítenem a Pristinában szolgálatot teljesítő Őr zászlóaljat, amely már képes harci feladatokat is végrehajtani. Figyelembe véve e tényeket prognosztizálható, hogy a jövőben akár önálló harcra is képes zászlóaljjal kell valahol külföldön képviselnünk hazánkat, ahogy az a NATO által hazánk számára előírt feladatokban is szerepel. Hazánk NATO felajánlásait tekintve elvileg az MH-nak el kell érnie, hogy akár egy egész dandárt fel tudjon ajánlani a NATO haderő számára, valamint rendelkezzen egy dandárral, mely a békefenntartó hadműveletekben való részvételre lesz felkészítve. Valószínűleg e két dandár felépítésében, eszközeiben számottevő különbségek lesznek.

Hazánkban a gépesített lövész zászlóalj meg fog változni, úgy hogy egy új könnyű lövész zászlóalj jön létre, melyet amerikai formára akarnak kialakítani. Ez azt jelenti, hogy elveszti páncélozott harcjárműveit, önjáró tüzéségét és helyükbe gépkocsizó csapatok kerülnek vontatott tüzéséggel meg erősítve. Az új zászlóaljak már a modern rádiókkal lesznek felszerelve előreláthatólag. Az új eszközökkel felszerelt zászlóalj híradó szakaszának felépítése is megváltozik, hiszen új eszközökkel (műholdas készülékek) lesznek felszerelve. A zászlóaljak tehát új eszközökkel fog rendelkezni, amelyekből fel fog épülni a híradó szakasz is. A híradó szakasz áll: HK-2 pc, PK-2 pc, PK-3 pc, híradó raj, mely csatlakozó vezetékes anyagokkal, hordozható rádiókkal és opcionálisan hordozható műholdas berendezések van felszerelve.

1.1. A gl. z-nál rendszeresítésre kerülő eszközök rövid jellemzése:

- **„Zászlóalj szintű digitális központ és rádiórelé állomás (páncélozott jármű) HK-2 pc**, melynek feladata a Vezetési pont hírközpontok bekapcsolása a tábori területi hírendszerbe. Főbb elemei a következők:
 - Digitális kapcsolástechnikai berendezés,
 - két irány egyidejű biztosítására képes 256 vagy 512 kbps-os átvitelű, 225-400 MHz (NATO I. sáv) frekvencia tartományú rádiórelé,
 - 256 vagy 512 kbps-os csoportos titkosító irányonként,
 - csatornarendező,
 - mellékoldali rendező,
 - URH rádió beépített információvédelmi berendezéssel, (mely az MRR rádió lehet),
 - végberendezések a kiépítés függvényében,

-
- csatlakozó kábelek,
 - antenna készlet a szükséges árboccal.
- **Zászlóalj parancsnoki mozgó vezetési pont (MVP) PK-2 pc**, melynek felhasználási területe a katonai szervezetek rádióállomásaként a mozgó vezetési objektumokban, valamint az előretolt repülésirányító pontokban (ERIP) található. Ez a zászlóalj pk-i szintnek megfelelő harcjármű. A MVP fő elemei:
- Beépített információvédelmi berendezéssel, beszéd és adatátviteli lehetőséggel és aktív zavarvédelemmel rendelkező rádióeszközök,
 - belső kommunikációs rendszer,
 - antenna rendszer.
- Fő feladatai:
- RH-URH sávú rádióforgalmi rendszer egyidejű kiszolgálására az előjáró és az alárendeltek viszonylatában,
 - URH, (mely az MRR rádió lehet) sávú - az együttműködő (támogató) szárazföldi szervezetekkel és a rádiófelvevő ponthoz történő csatlakozás érdekében szervezett - rádióforgalmi rendszer kiszolgálására,
 - OPCIONÁLISAN: 1 URH sávú - a repülőeszközökkel való kapcsolattartás érdekében szervezett - rádióforgalmi rendszer kiszolgálására.
- **Század pk-i rádióállomás PK-3 pc**: Ez egy parancsnoki rádióállomás a zászlóaljon belül. Főbb elemei:
- Beépített információvédelmi berendezéssel, beszéd és adatátviteli lehetőséggel és aktív zavarvédelemmel rendelkező rádióeszközök,
 - belső kommunikációs rendszer,
 - antenna rendszer.
- Fő feladatai:
- 1 RH és URH sávú rádióforgalmi rendszer kiszolgálására az előjáró, valamint 1 URH sávú az alárendeltek viszonylatában, (mely az MRR rádió lehet),
 - URH sávú, (mely az MRR rádió lehet) - az együttműködő (támogató) szárazföldi szervezetekkel és a rádiófelvevő ponthoz történő csatlakozás érdekében szervezett - rádióforgalmi rendszer kiszolgálására,
 - OPCIONÁLISAN: 1 URH sávú - a repülőeszközökkel való kapcsolattartás érdekében szervezett - rádióforgalmi rendszer kiszolgálására.”¹

1.2. A gl. z. híradásának sajátosságai külföldön

A külföldön történő alkalmazás, különböző lehet. Meg kell különböztetni a béke és háborús műveleteket, melyek magukkal hozzák a gépesített lövész zászlóalj felépítésének a változatait. A béke műveleteknél a gl. z. nem viszi magával önjáró tűzereszközöket, mert nem kimondottan támadó feladatokat végez, hanem területi biztosító

¹ KKRSZ órai anyag – gl. z. perspektívikus eszközei PowerPoint előadás

feladatokat. A másik probléma a Magyar Honvédségnél, hogy az önjáró tűzér ütegeket ki akarják vonni, mert nem mobilak, ahogy a harckocsik sem (itt a szállítási nehézségre gondolok). A jövő haderejének a legfontosabb tulajdonságának, a mobilitásnak kell lennie, hogy bárhol megjelenhessen a megfelelő időben. Ez általában légi szállítást feltételez. A jövőben valószínű tehát, hogy vontatott ütegek lesznek rendszerezítve amerikai példára. A másik a már említett könnyű zászlóalj felépítése, mely nagyobb harcok megvívására alkalmatlan. Véleményem szerint meg kellene tartani a harckocsikat és a páncélozott harcjárműveket is, mert a jelenlegi tendencia is azt támasztja alá, hogy a könnyű alegységek, egységek nem képesek nagyobb hadműveletek végrehajtására (lásd Irak, ahol a harckocsik nélkül nem tettek egy lépést sem a csapatok). Ez nem azt jelenti, hogy nincs szükség a könnyű csapatokra, csak azt látnám helyesnek, hogy hadjuk meg ezen eszközöket és így szükség esetén bevetethetők lennének.

A híradás az általános híradástól abban lehet eltérő, hogy kiesnek egyes rádióforgalmi rendszerek, hogyha nem alkalmazzák az adott alegységeket, egységeket (például tűzérség). A rádióforgalmi rendszerek nem változtak meg a régi analógokhoz képest, tehát a híradás felépítése sem változott. A változást nem ezen a téren kell megfigyelni, hanem a vezetés oldalán. A híradás a magyar erőknél zászlóalj szinten egyedi felépítésű, ahogyan minden nemzetnél, nem szólnak bele a felépítésébe, de elvárják, hogy képes legyen a feladata elvégzéséhez szükséges híradás biztosítására. A zászlóalj parancsnoknak már rendelkeznie kell, olyan eszközökkel, amik a NATO csapatokkal dandár vagy hadtest szinten is összeköttetést tudnak létesíteni.

Ha a magyar zászlóalj külföldön végzi feladatát, akkor a híradó csapatainak képesnek kell lennie pontos, értékelhető információkat szolgáltatni a csapatok számára úgy, hogy fenntartsák a parancsnok számára az információtovábbítás lehetőségét felfelé és lefelé egyaránt, úgy hogy az rejtve legyen az ellenségtől.

A zászlóaljakban a híradást a törzstámogató század híradó alegységei végzik. A zászlóalj típusú szervezetekben a híradó törzs szakasza biztosítja a vezetés híradó feltételeit a dandártörzs híradó intézkedésének megfelelően, tehát elképzelhetetlen lenne a híradás megszervezése, ha nem lenne megfelelő és kompatibilis híradó eszköze a magyar zászlóaljaknak. Ez az eszköz pedig a Norvég Kongsberg rádiócsalád lesz.

A magyar csapatoknak rendelkezniük kell megfelelő híradó tartalékokkal is. Nagyon fontos szempont, hogy a szövetségeseink más típusú híradó eszközökkel rendelkeznek, melyek nem építhetők be a saját csapataink hírrendszerébe a zászlóalj szinten belül. Mindez maga után vonja, hogy csapataink nagyobb tartalékkal vonuljon fel külföldi szolgálatuk alatt. Elkerülhetetlen, hogy egyes készülékek meghibásodnak és csak saját anyagi technikai eszközeinkre, leszünk utalva, így javasolom külföldi misszióknál nagyobb eszköztartalékkal, kell kitelepülni.

A következőkben bemutatom az új rádiókat, melyek már csapatpróbán vannak a szolnoki felderítő csapatoknál. A rádiók bemutatása után pedig a csapatpróba következtéseivel foglalkozom.

2. MRR harcászati rádiók

Az MRR (Multi Role Radio – többfunkciós rádió) harcászati rádió, mely megnyerte a Honvédelmi Minisztérium által a harcászati rádiókra kiírt tendert. Vannak már hazánkban ilyen rádiók, ahogy ezt már jeleztem, de még az MH nem vette át az

összes rádiót. A rádió alkalmazási területe az MH-ben a zászlóalj parancsnoki szinten jelenik meg először az alárendeltek felé.



1. ábra Az MRR harcászati rádió

Forrás: www.kongsberg.com

Ez egy többfunkciós rádió, mely elsősorban adatátvitelre és beszédátvitelre is kiválóan alkalmas. A digitális URH rádió a 30-88 MHz-es frekvenciasávban üzemel. Funkcionális képességei lehetővé teszik, hogy a rádiót különböző szerepkörökben és különféle felhasználói igények kielégítésére használják. A rádió olyan kiépítésű, hogy akár gépjárműben, akár személyeknél való használatra is kialakítható. Létezik egy gépjárműbe szerelhető (vehicled) változat, mely nagyobb kimenő teljesítményre képes maximálisan 50W, mivel a gépjármű elbírja a teljesítményerősítő egységet is, míg a katonánál lévő változat egy hord táskában (manpack) van elhelyezve és max. kimenő teljesítménye 5W. A harmadik típusa ennek a családnak a kézi rádió, melynek max. kimenő teljesítménye 1W.

A beszédátvitel továbbítása történhet digitális (Electronic Protective Measures, EPM) üzemmódban, vagy analóg FM üzemmódban. A digitális üzemmód rögzített frekvenciát, vagy frekvencia hopping eljárást használhat az adáshoz. Valamennyi digitális kommunikáció titkosított. A rádió azonban titkosítás nélkül képes kommunikálni a hagyományos analóg FM-rádiókkal, és ez teszi lehetővé többek között, hogy kommunikálni tudjunk a szövetségeseink rádióival.

Az adatátvitel az alábbi lehet:

- Korlátozásmentes. (Az adat transzparens módon kerül továbbításra a hálózat egyik rádiójáról a hálózatban lévő összes többi rádióhoz – *all informed*).
- Csomagkapcsolt adat X.25 hozzáférés. (Az adat címzetten a hálózat egyik rádiójának, vagy egy rádiócsoporthoz szól).

A következő berendezések csatlakoztathatóak a rádióhoz:

- Digitális adat végberendezések (X.25 végberendezések, vagy transzparens adatátvitelre szolgáló végberendezések), nyomtató, belső kommunikációs rendszer vagy különálló kihangosító eszközök;
- kimenő teljesítményszabályozó és hálózatkiválasztó egység;
- kézi beszélő, fejhallgató vagy mikrofon.

A következőkben a gépjárműbe szerelt rádió fő elemeit, jellemzőit mutatom be, melyet a hordozható (manpack) rádió elemzése követ, végül a kézi rádió kerül bemutatásra.

2.1. Gépjárműbe szerelhető (vehicled MV300):

A gépjárműbe szerelnél megtalálható a már említett teljesítményerősítő egység, amivel a maximálisan elérhető kimenő teljesítmény 50W. A gépjárműbe szerelt rádió kimenő teljesítménye a menüben választható az alábbiak közül: 0,1W – 0,5W – 5W – 50W



2. ábra A gépjárműbe szerelhető MRR rádió

Forrás: MRR Többfunkciós Rádió Felhasználói kézikönyv, Ericsson 1999

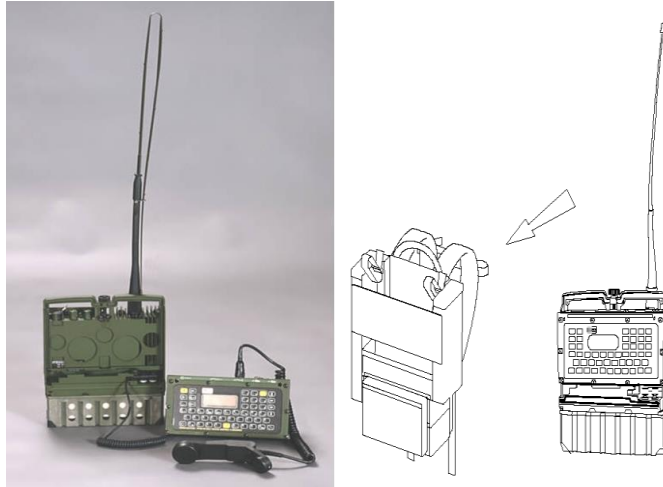
A tápfeszültsége 22-30 VDC (Volt DC – volt egyenáram), ami ~400W teljesítmény felvételt enged meg. Tömege összesen 19,8kg. A rádió egy 3m-es botantennával van ellátva.

2.2. Hordozható (manpack MP300):

Ennél a rádiónál is lehet választani az előző teljesítmények közül, csak a maximálisan választható kimenő teljesítmény értéke 5W. A tápfeszültséget Li elem (18VDC) vagy NiCd akkumulátor (14,4VDC) szolgáltatja. Magyarországon a NiCd akkumulátorral rendszeresítik, melynek 8óra lesz az üzemideje. Megjegyzem a NiCd-os akkumulátornak technikai szempontból sok káros hátulütője, van. A legfontosabb, hogy az időjárás viszontagságaira nagyon rosszul reagál. Legrosszabb esetben télen az üzemidő lecsökkenhet akár 1-2 órára. A maximális tömegük (elemmel vagy akkuval együtt) 7kg. A rádió antennái egyrészes bot, az adó-vevő előlapjához történő csatlakoztatás céljára szolgáló rugalmas, hajlítható (fél merev) "libanyakkal", valamint nagyobb távolságok áthidalására egy több elemből álló hajlékony botantenna.

A hordozható rádió hord táskájának kialakítása kimondottan erpówmikus szempontból lett kialakítva. Magam is kipróbáltam a rádió szállítását a hord táskában

és arra a következtetésre jutottam, hogy némely hátitáskánál is kényelmesebb és nem zavarja a híradó katonát a mozgásban, nem úgy, mint az R-107-es rádió hurcolása. A hord táská levétele nélkül képes a kezelő rádiózni, a kezelőpanel előrevételével, vagy a kézi beszélő készlettel, melyet RS 232-es interfésszel lehet csatlakoztatni a rádióhoz.



3. ábra Hordozható MRR rádió és hord táská

Forrás: MRR Többfunkciós Rádió Felhasználói kézikönyv, Ericsson 1999

2.3. Kézi rádió (hand MH300):

A kézi rádió a rajparancsnokoknál, illetve a mesterlövészek szintjén lesz bevezetve, de külföldi missziók során a lövész pároknál is alkalmazhatják. Ez a rádió a legkisebb teljesítményű. 0,15W és 1W között van a kimenő teljesítménye. LiIon akkumulátorral van felszerelve, mely 18 órás üzemidőt biztosít. A súlya 1kg.



4. ábra MRR kézi rádió

Forrás: Kongsberg Videoton oktató PowerPoint

2.4. MRR alkalmazásai és benne lévő lehetőségek

➤ Harcászati Hálózati Rádió² (Command Net Radio, CNR):

A Harcászati Hálózati Rádió legáltalánosabb alkalmazása autonóm hálózatokban történik, ahol a hálózat tagjai között „Broadcast”³ jellegű forgalmazásra van szükség.

A CNR üzemmód szolgáltatásai:

- Digitális/analóg beszédátvitel,
- transzparens adatátvitel,
- címzett X.25 csomagkapcsolt adatátvitel,
- beépített Üzenetkezelő terminál funkció.

➤ Mobil Végberendezés (Mobil Terminal, MOT):

A rádió egy autonóm hálózatban mobil végberendezésként (mobil telefonként) használatos.

A különböző szolgáltatásokat a menüben lehet elérni és aktivizálni. A szolgáltatások ebben az üzemmódban:

- címzett X.25 csomagkapcsolt adatátvitel,
- beszédkapcsolat a felhasználók között dedikált csatornákon,
- beépített Üzenetkezelő terminál funkció.

A szolgáltatások megosztottsága a CNR és a MOT között:

Paraméter	CNR	Mobil végberendezés
Digitális hailing (kérés)	X	-
FM hailing (kérés)	X	-
Rádiócsend	X**	X**
Automatikus frekvencia kiválasztás	X**	-
Utólagos hálózati belépés	X*	X
Digitális hailing figyelés	X	-
FM hailing figyelés	X	-
Kulcs kiválasztás	X**	X**
Automatikus teljesítményszabályozás	-	X

1. táblázat Speciális szolgáltatások - MRR

Forrás: Többfunkciós Rádió Felhasználói kézikönyv, Ericsson 1999

*FM hálózatra nincs biztosítva

² Továbbiakban harcászati rádióhálónak nevezzük, csak a fordítás sorrendje miatt írtam így

³ Közlemény jellegű híradás. A hálózatban történt adást a hálózat minden tagja veszi.

**Jelen változatra nem alkalmazható

2.4.1. Szolgáltatások:

- „Digitális hailing (kérés): Ez a párbeszéd olyan digitális rádiók felé történő hívások biztosítására szolgál, amelyek nem a hívó (hailing) rádió hálózatában, hanem más hálózatokban tagok. A hívott hálózat(ok)ban legalább egy rádiónál aktívnak kell lenni a Digitális hailing figyelésszolgáltatásnak. A frekvenciatartomány: 30,000 - 87,975 MHz, 25 kHz-es lépésekben. A hailing-kérés az RCT kézi beszélőjén található gomb megnyomásával történik.
- FM hailing (kérés): Ez a szolgáltatás FM-rádiók felé történő hívások kivitelezésének biztosítására szolgál. A szolgáltatás a CNR üzemmód számára férhető hozzá (lásd a 1. táblázatot).
- Rádió csend (radio silence): A szolgáltatás a rádió "elrejtésére" használatos. Amikor e szolgáltatás aktivizálva van, a rádió nem képes információt adni vagy átjatszaní, csak venni. A rádiócsend szolgáltatás aktív állapotát a kijelző jobb felső sarkában egy "R" jelzés mutatja. A szolgáltatás valamennyi üzemmódban használható.
- Automatikus frekvencia kiválasztás (Automatic Frequency Selection, AFS): A szolgáltatást akkor használják, amikor a körülmények a frekvencia hopping adásmód alkalmazását nehezéssé teszik, mint például:
 - kitartó és heves zavarás,
 - frekvencia-torlódás, vagy
 - igen nehezen áttekinthető és elemezhető hálózat.

A szolgáltatás aktiválása esetén a rádióadás/vétel viszonylatban egyaránt kiválasztja az első elfogadható frekvenciát a fix frekvenciás EPM kommunikáció számára. A szolgáltatás a CNR üzemmód számára férhető hozzá.

- Utólagos hálózati belépés (Late Net Entry, LNE): Amennyiben a rádiót még nem használták, vagy nincs szinkronizálva, akkor ez a szolgáltatás teszi lehetővé számára, hogy a digitális hálózathoz (vagy amennyiben a hálózati szinkronitást elvesztette, akkor a saját hálózatához) hozzáférjen. Az időpont beállítása a hálózatban lévő többi rádióéhoz képest ± 1 percen belül legyen. A szolgáltatás az összes üzemmód számára hozzáférhető. A funkciói lehetnek aktív és passzív.
 - Aktív: A rádió jeleket sugároz ki, amely a közelben elhelyezkedő rádiókat szinkronjelek adására készíti. Ez a jel speciális formátumú, mely lehetővé teszi a hívó rádió számára a szinkron felvételét.
 - Passzív: A rádió "csendben" marad, és felhasználja a hálózatba tartozó többi rádió megfigyelt normál forgalmát a szinkronizmus felvételére.

Az, hogy melyik módszert használják az operatív döntés kérdése. Az aktív módszer használata felfedheti a rádió helyét, viszont gyorsabb, mint a passzív módszer. A belépési kísérlet helyzetéről az (Radio Controll Terminal, RCT) kijelző folyamatosan informál. Amennyiben a rádió fel van töltve az összes hálózati paraméterrel és kulccsal, akkor az aktív vagy passzív szinkronizáció kezdeményezése és elindítása minden üzemmódban megvalósítható.

- Digitális hailing figyelés (monitoring): Ez a szolgáltatás a Digitális hailing kérések figyelési funkcióját aktivizálja. A Digitális hailing kérések sikeres "detektálásához" egy vagy több rádió a hailing-frekvencia figyelésére kell állítani. Csak CNR üzemmódban férhető hozzá.
- FM hailing figyelés (monitoring): Ez a szolgáltatás az FM-hailing kérések figyelési funkcióját aktivizálja. Amennyiben egy hailing-kérést észlelnek, egy figyelmeztető hangjelzés (amennyiben a zümmer be van kapcsolva), valamint az RCT kijelzőn egy üzenet kerül kiadásra. Csak CNR üzemmódban férhető hozzá.
- Kulcs kiválasztás: A párbeszéd a hálózatban használandó titkos kulcs kiválasztására szolgál.
- Automatikus teljesítményszabályozás: A szolgáltatást a mobil végberendezés konfigurációkban használják, hogy beszédátvitel esetén lehetővé tegyék a kiemenő teljesítmény automatikus szabályozását.
- 'Nem biztonságos' átvitel jelző figyelmeztetés kikapcsolása (NSW disable): A „Nem-biztonságos” átvitelre vonatkozó figyelmeztetés engedélyezésére/kikapcsolására használatos.”⁴

2.4.2. Rejtjelzés:

Minden forgalom STANAG titkosítóval rejtjelzett, a rádiók NATO titkosítóval vannak felszerelve: Beszéd, tiszta adat, adatcsomag, Harcászati SMS (hazánkban nem került bevezetésre)Több különböző rejtjelkulcs biztosításával történik a rejtjelzés.

- Egy háttér vészhelyzet kulcs mindig rendelkezésre áll, ezzel is törekszenek a biztonságra.
- A rejtjelzés időfüggő TRANSEC és COMSEC.
- Direkt szekvenciális szórt spektrumot használnak.

2.4.3. Telepítési lehetőségek:

A rádió távvezérelhető, a kezelő panel levételével és tábori vezetéssel max 1500m-re történő telepítéssel. Ez lehetőséget nyújt arra, hogy úgy forgalmazzunk rádióinkkal, hogy azt nem deríti fel az ellenség. Ezt azzal érhetjük el, hogy az ő irányukba leárnyékoljuk (hegy mifelénk eső oldalára tesszük, míg mi az ellenség felőli oldalról távvezéreljük a rádiót). Fontos szempont, hogy a titkosító berendezés a kezelő panelben van beépítve, így már rejtjelezett a távvezérlés is.

A rádiók átjátszó állomásként is működnek (CNR alkalmazásnál), minden forgalmat képesek átjátszani, legyen az:

- Beszéd
- Tiszta adat

⁴ MRR Többfunkciós Rádió Felhasználói kézikönyv, Ericsson 1999

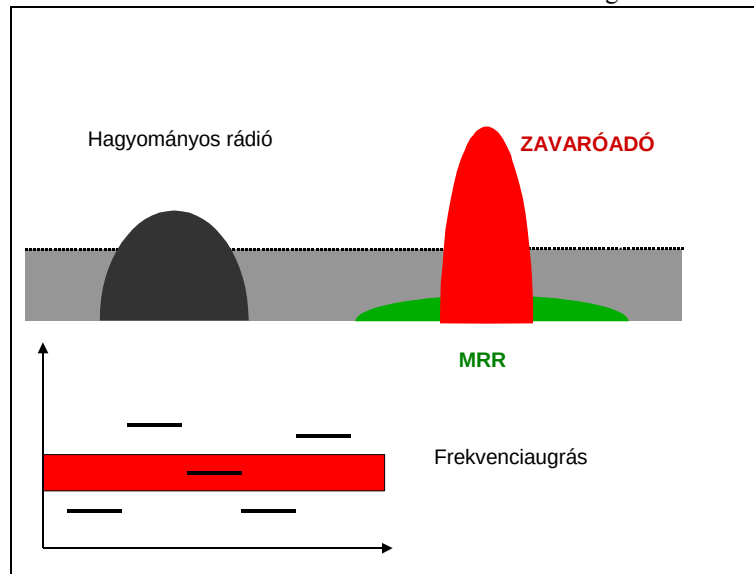
- Adatcsomag

Vezetékes összeköttetés esetén a beszéd átvitelnél a távvezérlés távolsága max. 1500m, míg az adatnál ez max. 3000m is lehet.

2.4.4. Üzem módok:

- Rögzített frekvenciás
 - Rövid szinkronizációs idő
 - Frekvenciaugrás
 - Keskenysávú direkt szekvenciás szórt spektrum (NBDS)
 - Kezeli a változó vételi időt mindegyik frekvencián
 - Többutas terjedés kezelése minden frekvencián
 - Negatív jel-zaj viszony (SNR)
 - Rejtjel vezérelt ugrási minta
- Szabadcsatorna keresés
 - Fix frekvenciás üzem a frekvenciaugrás készletben
- Hagyományos FM
 - STANAG 4204
 - AN/PRC-77

A következő ábra szemlélteti az NBDS és a frekvenciaugrást zavar esetén.



5. ábra MRR üzemmód zavarás esetén
Forrás: Kongsberg Videoton oktató PowerPoint

2.4.5. Hatótávolság és zavarhatóság:

A zavarhatóság szempontjából magas szintű védettséggel rendelkezik az MRR rádiók családja, ugyanis rendelkezik a direkt szekvenciális szórt spektrumú üzemmóddal, az interferencia kioltással és a frekvenciaugratás képességével. Keskenysávú zavarás alkalmazása esetén a zavart rész spektrumánál sokkal szélesebb

spektrumba szórja szét a jelet, úgy hogy még a zavart részen kívüli jelből is visszanyerhető az információ. A zavarást megnehezíti, hogy adat esetében a jel a háttérzaj szintje alatt helyezkedik el, így nagyon nehéz megállapítani az adás tényét.

3. A csapatpróbán jelentkező gondok

A szolnoki csapatpróbán lévő készülékekről megszerzett tapasztalatok a következők:

A rádiók nem rendelkeznek megfelelő szakutasítással, például az akkumulátorokhoz, nem küldtek üzemeltetési szakutasítást, így nem tudjuk, hogy a rádió akkumulátorai feltöltve érkeztek ezen, vagy ki kell őket sütni.

A rádió, titkosító berendezéssel van ellátva, melyet a rádióba szereltek be, ezért azt elzárva kell tartani rejtjelző körletben. A rádió el van látva egy felbontás elleni védő fóliával is, mely arra hivatott, hogy jelezze, ha valaki felbontja a rádiót és hozzáférne a titkosítóhoz. A gond csak az, hogy ezt a fóliát úgy helyezték el, hogy a rádió akkumulátor cseréje közben sérül, így azt mutatja, mintha valaki felnyitotta volna. A rejtjelzés jelenleg úgy valósul meg, hogy a rádiók saját ID azonosító számukat használják a hálózatazonosító mellett. Ez azt jelenti, hogy nem történik meg a NATO STANAG titkosító alkalmazása, nincs felkonfigurálva a rádiókra.

Az üzemmódokat tekintve gyakorlatilag nem képes a szolnoki rádió a frekvencia hoppingra, mivel összesen három frekvencia van biztosítva erre az üzemmódra a szükséges 100-200 helyett. Az előre beharangozottak szerint tudnia kéne az adat és beszédátvitelt egyszerre, melyet a csapatpróbán lévő rádiók nem tudnak.

A kulcsváltás nem tud megvalósulni praktikusán, mert nincsen kulcsváltó berendezés a rádiókhoz, nem beszélve a központi kulcsváltásról (, melyet egy számítógép vezérlésével az összes rádió kulcsváltása megtörténne). A kulcsváltás jelen helyzetben kézzel történik, úgy hogy a rádióknál egyenként végzik a kulcsváltást.

Befejezés

A harcászati rádiók alkalmazása a Magyar Honvédségen belül már-már létkérdés, hiszen az egyre nagyobb mértékű külföldi szerepvállalás és a szövetséges elvárások is ezt igazolják. Az még kérdéses, hogy mekkora erőket visznek ki Magyarországról, de azért is tárgyaltam a zászlóalj keretét, mert ez az eddigi tendencia. A magyar haderő ezzel a rádió családdal biztosítani tudja a századon belüli híradást. Nagy kérdés, hogy az MH a továbbiakban milyen rádiókat szerez be. Híradó és interoperabilitási szempontból az lenne a legmegfelelőbb, ha maradnánk ennél a rádiócsaládnál, így nem lépnének fel kompatibilitási problémák a zászlóalj dandár szintek és a század szintek között. Az MRR rádiók zászlóalj szintig lesznek rendszeresítve (csak URH-t tudnak), mivel a zászlóaljparancsnoknak, olyan rádióval kell rendelkeznie, ami tud RH-t és URH-t is.

A harcászati rádióknak sajnos nem vette meg Magyarország az összes szolgáltatását és a bennük lévő lehetőségek teljes körét, ahogy azt a csapatpróba tanulságai is igazolták. Fontosnak tartom itt megjegyezni a Harcászati SMS-t, ami adat léven nagyobb fokú rejtettséget élvez a hangátvitellel szemben. Az igaz, hogy az MH-ban még eddig nem alakult ki az sms alapú vezetés gyakorlata. Szerintem nem szabad elhatárolódni ettől a megoldástól, hanem inkább meg kéne ismerkedni vele.

A rádió kiépítettsége és kezelőfelülete felhasználóbarát, egyedül az angol nyelvtudás szükséges hozzá vagy megfelelő felkészültség. A rádiók kezelhetősége egyszerű, könnyen saját kezűleg tudja a katona a szükséges beállításokat megtenni. A rádiók mobilak, még a harcjárműbe szerelt is, hiszen bármikor áttelepíthető egy másikba.

Az MRR rádiók digitális működési elvükből adódóan nagyobb távolságok áthidalására képesek az analóg rádiókhoz képest, valamint a NATO frekvenciasávjában dolgoznak és rendelkeznek NATO előírásnak megfelelő titkosítóval is, mely fontos a külföldi alkalmazások esetében. A rádiók távvezérlése egyszerű és jelentős előnyöket hordoz magában a harci alkalmazás során.

Felhasznált Irodalom

- [9] Ábraalbm a „Katonai kommunikációs rendszerek szervezése” című tantárgyhoz, Dr. Rajnai Zoltán mk. őrgy. egyetemi adjunktus Kis Lajos mk. szds. egyetemi tanársegéd, Budapest 2002.
- [10] KKRSZ órák PowerPointos anyagai
- [11] MRR Többfunkciós Rádió Felhasználói kézikönyv, Ericsson 1999
- [12] [www. Kongsberg. com html](http://www.Kongsberg.com/html) oldalai
- [13] Kongsberg Videoton oktató PowerPointok
- [14] Konferenciákon elhangzott előadások anyagai

FEJLŐDŐ KOMMUNIKÁCIÓ – NAGYOBB BIZTONSÁG? A TERRORIZMUS HATÁSA A KOMMUNIKÁCIÓRA

A biztonság és a kommunikáció

A XXI. század információs társadalmának világában egyre gyakrabban kerül szóba a biztonság és a kommunikáció kapcsolata. Jelen tanulmány célja a fejlődő kommunikáció és a biztonság két fogalmából kiindulva, a terrorizmus jelenségének példáját felhasználva, az **elméleti összefüggések bemutatása**.

A biztonság meghatározására számos leírás találni a szakirodalmakban, melyek közös gondolata a veszélymentes állapot. Az egyik ilyen megfogalmazás⁵ szerint a biztonság „egy kíváncsú állapot, amelyben nyugodtak lehetünk afelől, hogy értékeink nincsenek veszélyben, érdekeink sérelme nem valószínű”. Ennek elérése a cél akkor is, amikor kommunikálunk, vagyis információátvitellel kapcsolatos tevékenységet végzünk.

A latin eredetű kommunikáció fogalmának létező meghatározásai közül T. Masano meghatározása miszerint „a kommunikáció információt szállít a tér-idő egységből egy másik tér-idő egységbe” visz közelebb minket a műszaki szemléletű „információtovábbítás”, illetve a távközlés fogalmához, amelyet az Európai Unió Tanácsának állásfoglalása⁶ az alábbi módon definiál:

A távközlés: „Jelek, jelzések, írások, képek, hangok, adatok és ismeretek vezetékes, rádióhullámú, elektromágneses, fényelektromos vagy fényoptikai rendszereken keresztül részben vagy egészben történő bármilyen továbbítása.”

A két fogalom közös kapcsolódási pontja az információ, amelynek valamilyen módon történő

- felhasználása
- birtoklása
- továbbítása
- megszerzése

biztosítható vélt vagy valós biztonságot a felhasználók számára.

Információ birtokában nagyobb biztonságban érezzük magunkat, lehetővé válik a veszélyhelyzetek elkerülése, bekövetkezése esetén a segítségnyújtás megszervezése. Felelősségteljes politikai döntések, gazdasági lépések hozhatók meg naprakész, pontos információk segítségével.

Korunk információs társadalmában, azonban igazi értéket csak a **pontos, időszerrű, mennyiségileg megfelelő, és időben felhasznált információk képviselnek**, mely követelmények a megállíthatatlanul fejlődő modern kommunikációs technológiák és eszközök alkalmazását igénylik. Amellett, hogy az információk áramlását és felhasználását biztosító rendszerek életünk részévé váltak (1.sz. táblázat), és széles körben

⁵ Simon György - *Az információbiztonság aktuális kérdései*, KBH Szakmai Tudományos Közlemények, A biztonság specifikus területei, Információ- és adatvédelem című tudományos konferencia anyaga, Budapest 2003., p7.

⁶ Európai Unió Tanácsának 1995. január 17-i állásfoglalása a távközlés jogszerű lehallgatásáról 97/C329/01 (1996.11.04)

történő alkalmazásuk számtalan felhasználási lehetőséget teremtett számunkra, közvetve fokozták veszélyeztetettségünket is.

Kommunikációs eszközök használatának terjedése a világon / 1.sz.táblázat						
<i>Forrás: ITU - Key Global Telecom Indicators 2001</i>						
	1991	1993	1995	1997	1999	2001
Telefonvonalak száma (millió)	546	604	689	792	905	1053
Mobiltelefon előfizetők száma (millió)	16	34	91	215	490	955
Személyi számítógépek száma (millió)	130	175	235	325	435	555
Internet felhasználó száma (millió)	4,4	10	40	117	277	502

Összegezve, a két fogalom számos ponton összekapcsolódik az egyszerű mindennapjainkat érintő telefonálás, műsorszórás, mobil telekommunikáció, és internet felhasználói tevékenységektől kezdve, egészen a fenti feladatokra szakosodott csoportok, pl. távközlési szolgáltatók, televíziós társaságok, információszerző csoportok (törvényekben meghatározott feladatokat ellátó kormányzati szervek, bűnözői csoportok, stb.) tevékenységéig.

Az életünket a távközlés annyira átszötte, hogy megfelelő kommunikáció (távközlés) megléte nélkül a társadalom közösségeinek működésében zavarok lépnének fel, az egyén pedig az információ, illetve kommunikáció hiányát, személyes biztonságát veszélyeztető tényezőként élné meg.

A terrorizmus, mint biztonságpolitikai veszély hatása a kommunikációra

A kommunikációs technológiák és eszközök robbanásszerű fejlődése részünkre nyújtott előnyei mellett, más, értékeinkkel, érdekeinkkel ellentétes csoportok számára is új lehetőségeket teremtett. A határok nélküli, gyors, személytelen kapcsolattartás lehetőségében rejlő előnyöket, a korábbi rendszerekhez képest nehezebb felfedhetőséget biztosító fejlett eszközök használata tovább növelte. Bűnözői csoportok, terroristák, hírszerző szolgálatok, ellenséges ország haderőinek híradása, ipari „kémek”, pénzmosáshoz felhasznált banki rendszerek vagy egyszerűen csak hackerek információs szükséglete is ezekhez a rendszerekhez kötődik

A nemzetközi terrorista hálózatok, és a hozzájuk köthető egyéb illegális tevékenységek (pl. kábítószer-, ember- és fegyvercsempészet, pénzmosás) szervezési feladatai sem nélkülözik a fejlett kommunikációs technológiák nyújtotta lehetőségeket. Kérdésként merül fel, hogy ezen csoportok kommunikációs tevékenysége, milyen módon veszélyezteti biztonságunkat.

Nem műszaki, hanem biztonságpolitikai szemmel nézve a terrorizmus jelenségének példáját felhasználva a kommunikációhoz kapcsolódó közvetlen veszélyek két gondolati kör köré csoportosíthatók:

- A számunkra ellentétes érdekeket képviselők kommunikációjához köthető veszélyek. Ebbe a csoportba sorolhatóak a terroristák, vagy kapcsolódó csoportok kommunikációi, így a cyberterrorizmus is.
- Nem tudunk kommunikálni a számunkra fontos időben és helyszínen (pl. nem áll rendelkezésünkre a kommunikációs rendszer (pl., túlterheltség), illetve hiányzik a megfelelő kommunikációs rendszer)

Kommunikáció és terrorizmus

A kommunikálásra használt információátviteli formát tekintve, a mobiltelefonokon kívül, korunk talán legjobban terjedő vívmánya az Internet vált az információátvitel egyik leggyakrabban használt formájává a terrorszervezetek körében is. A világ bármely pontján elérhető, gyors, on-line módon történő információtovábbítás lehetősége alkalmas akcióik megtervezésére és koordinálására. Az Internethez számos, a terrorszervezetek által jól használható lehetőség köthető.

- az anonim módon való kommunikáció lehetősége
- a folyamatos jelenlét
- a könnyű hozzáférhetőség, a hálózat decentralizáltsága
- a honlapok létrehozása és fenntartása költségei minimálisak
- a cenzúra nélkülség
- a multimédia által nyújtott lehetőségeket szerepe (video, audió, képek, stb.)

A több száz, terrorszervezetekhez, illetve támogatóikhoz fűződő honlap jelenléte arra utal, hogy majdnem minden aktív szervezet jelen van a világhálón⁷.

*A világháló alkalmas támogatók, önkéntesek toborzására is, amit a terrorizmus ellen folytatott harc során 2004-ben Londonban letartóztatott 13 férfi, köztük Babar Ahmad példája is mutat, aki a vádak szerint az általa üzemeltetett websíto-okon instrukciókat adott pénzek tálib vezetőkhöz, és Csecsenföldön harcoló iszlám gerillákhoz történő eljuttatására*⁸.

Nem hagyható figyelmen kívül a cyberterrorizmus veszélye sem. A nagyméretű információs rendszerekhez köthető terrortámadásokkal okozható károk nagysága felbecsülhetetlen. A fogalom alatt a legegyszerűbb e-mail „hadjáratokon” át (pl. az amerikai vezetés által a Szaddam rezsim ellen folytatott tevékenység az iraki háború kezdeti szakaszában), egészen az informatikai rendszerek és a hozzájuk kapcsolódó irányítórendszerek fizikai támadásáig sok minden érthető. Fő célpontjaik a kommunikációs, a szállítási, az energia ellátási és az alapvető közműellátást biztosító rendszerek.

A cyberháború vagy cyberterrorizmus rémképe igazából a fejlett nyugati társadalmakban, főként az USA-ban fenyeget. A széles körű, átfogó károkat okozó ilyenfajta terrortevékenység kockázata azonban nem tekinthető túl jelentősnek, és napjainkig nagyméretű, terrorista szándékkal okozott támadásnak nem lehettünk tanúi. Az Internetes adatforgalom lelassulására, repterek kommunikációját, erőművek vezérlő rendszereit veszélyeztető támadásokra eddig csak hackerek által okozott vírusok és férgek okán volt példa. Az illetéktelenek által információinkhoz való hozzáférések azonban

⁷ Forrás: Weimann, Gabriel - How modern terrorism uses the Internet – Special report 116 www.usip.org/pubs

⁸ Matthew Taylor – Court told of Internet 'terror' links - Special Report / The Guardian, 2004. Aug. 07. www.guardian.co.uk/alqaida

így is hatalmas károkat okozhatnak, melyek nagyságára csak pontatlan becslések vannak (a hitelkártya adatbázisok feltöréséből származó károk összegét 2003. februárjában pl. 40 millió USD-re becsülték⁹).

Az Internet adta támadási lehetőségek alkalmazása mindkét fél előtt nyitva áll, figyelembe véve, hogy a fejletlenebb, de valamilyen módon terrorizmushoz köthető országok kommunikációs infrastrukturális ellátottsága jóval elmarad a fejlett nyugati társadalmak előtt (2.sz. táblázat). Ezzel szemben az Egyesült Államok pedig már meglévő technikai előnyének birtokában az ezirányú kormányzati stratégia kidolgozásához fogott hozzá és a Bush kormányzat idején lépéseket tettek az információs hálózatok támadási célú felhasználásának előkészítésére.

Kommunikációs eszközök számának megoszlása néhány érintett országban 2.sz.táblázat				
<i>Forrás: ITU Statistics - 2003</i>				
	<i>Internet felhasználók fő / 10 e lakos</i>	<i>Személyi számítógépek db / 100 lakos</i>	<i>cellás mobiltelfon előfizetők száma az adott országban összesen (millió)</i>	<i>cellás mobiltelfon előfizetők fő / 100 lakos</i>
Szíria	129,11	1,94	0,4	2,35
Pakisztán	102,72	0,42	2,624	1,75
Líbia	289,33	2,34	0,1	1,81
USA	5513,77	65,89	158,722	54,3
Magyarország (referencia)	1576,04	10,84	6,862	67,6

Szeptember 11-e az információvédelem területén is fordulópontot hozott az amerikai gondolkodásmódban. Számos, korábban szabadon hozzáférhető információt (pl. katonai bázisok alaprajzai, légi biztonsági adatok) tettek elérhetetlenné honlapjaikon, mondván azok akár az Al-Kaida számára is alkalmasak lehetnek információk gyűjtésére.

Példák igazolják, hogy a terroristák az akcióik előkészítéséhez és tervezéséhez szükséges információk megszerzésére és egymás közötti kapcsolattartásra felhasználják a térségben is egyre szélesebb körben terjedő (3. sz. ábra) fejlett kommunikációs technológiák nyújtotta lehetőségeket. Megemlíthető az Al-Kaidához köthető laptop lefoglalása Afganisztánban, melyen olyan website-ok látogatására utaló információkat találtak, amelyek a szabotázs tevékenységek tanulmányozására vonatkoztak, vagy a

⁹ Gergej Slugin - Nyezaviszímaja Gazeta 2003. április 04.

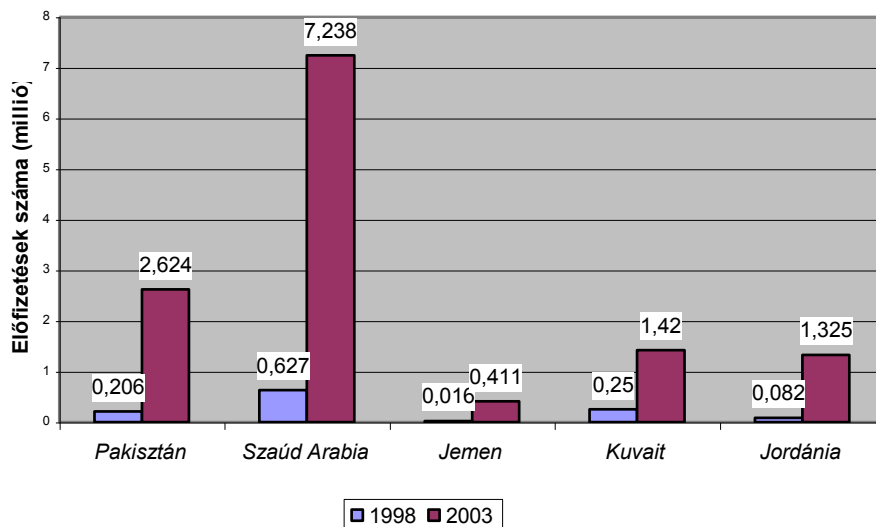
2002-ben Kabulban az amerikai haderő által fellelt számítógép, amelyen folyógiaták katasztrófájának szimulálására alkalmas mérnöki szoftvereket találtak¹⁰.

2004. júliusában Pakisztánban 3 laptopot és 51 számítógép disc-et foglaltak le, melyek átvizsgálása során olyan információkat találtak, melyek az USA öt nagyobb pénzügyi intézménye, továbbá helikopterek és hajók felhasználásával végrehajtandó, New York elleni lehetséges támadásokra vonatkoztak. A disc-eken található fotók helikopter reptereket, és helikopter pilótafülkéket ábrázoltak. A terroristák folyamatosan böngésztek a New York-i helikopteres utazásokat kínáló weboldalakat.¹¹

Cellás mobiltelefon előfizetők számának változása a térségben

1998-2003 között (3.sz.ábra)

Forrás: ITU Statistics - 2004



Az elektronikus médiák szerepének jelentősége külön tanulmányt érdemelne. A társadalom tagjait folyamatosan információkkal ellátó különböző médiák, a műholdas műsorszolgáltatás korában percek alatt befolyásolhatják széles tömegek biztonságát.

A nemzetközi nyilvánosságot biztosító médiák (pl. Al-Dzsazira) nélkül, amelyek a terroristák kezében a pánikkeltés, a félelem és bizonytalanság fenntartásának eszközei, a terroristák többnyire csak elszigetelt, névtelen helyi csoportok lennének. Nagy szerep juthat a médiáknak, azonban a terrorizmus ellenes harc során is. Veszélyhelyzetek, illetve terrorcselekmények bekövetkezése esetén, a lakosság tájékoztatása, azonnali információval történő ellátása csökkentheti a kapcsolódó károk és keletkező káosz nagyságát.

¹⁰ Barton Gellmann, *Washington Post* 2002. jún.27.

¹¹David Teather and Patrick Barkham – *Brown's photo on al-Qaida disks's - Special Report / The Guardian*, 2004. Aug. 09. www.guardian.co.uk/alqaida

A veszélyek csökkentése, nagyobb biztonsági szint elérése érdekében az állam számára így feladatként jelentkezik adataik fokozott védelme, és a bűncselekményekhez kapcsolódó kommunikációk kiszűrése. Az információ átvitelhez kötődő kommunikációs formák ellenőrzéséből adódó előnyökről nem mondhat le egyetlen ország sem, hiszen gyakran a távközlés ellenőrzése révén felmerülő adatokon kívül semmilyen más értékelhető információ nem áll kezdetben a biztonsági szervek rendelkezésére.

A terrorizmus elleni tevékenység során szinte lehetetlen feladatnak tűnik a terroristák előtt is nyitva álló egyre korszerűbb kommunikációs rendszerek nyújtotta előnyök használata során a terrortevékenységre, illetve annak előkészületeire utaló információk kiszűrése is. Az Internethez kapcsolódó elektronikus támadások kiinduló pontjának megállapítása szintén bizonytalan.

Szakértők álltak értetlenül a 2001-es amerikai terrortámadások után az előzetes szervezésre és egyeztetésre utaló kommunikáció nyomait keresve. Peter M. Leitner az amerikai védelmi minisztérium tanácsadója szerint¹²:

„...az igazi tragédia az, hogy a terroristák hogyan voltak képesek megtervezni és koordinálni egy ilyen csapást, anélkül hogy az NSA elfogta volna kommunikációjukat”

Felvetődik a kérdés: milyen kommunikációs eszközökkel rendelkezhetnek a terrorista szervezetek? Évek óta nyomait sem találják a Bin Ladenhez köthető kommunikációnak, habár korábban feltételezték, hogy titkosított cellás és műholdas mobiltelefont használt kapcsolattartásra. A fejlett kommunikációs eszközök, rejtjelző szoftverek ma már a szabadon beszerezhetőek a világban, vagy letölthetők a világhálóról. A terrorizmushoz kapcsolódó egyéb illegális tevékenységekből, pl. kábítószer-kereskedelemből, pénzmosásból befolyó hatalmas összegek pedig lehetővé teszik számukra, hogy a legmodernebb kommunikációs eszközöket vásárolják meg. Ezek forrásai többnyire a nyugati távközlési piacok.

Az előző évtizedben az Egyesült Államok Szíriának modern, katonai célra kifejlesztett kommunikációs eszközök (frekvenciaugratásos rádiók, informatikai és rejtjelző eszközök) adott el, amelyek akár a terroristák kezében is kiköthettek.

Más problémákat vet fel a biztonság kérdésénél, hogy kik azok alanyai. A veszélyben lévő ember kommunikációja, a segítségkérés, a veszélyek (pl. terrortámadás) következményeinek felszámolása során történő kommunikáció a felhasználó számára biztonságát közvetlenül növelő tevékenységként jelenik meg. Bizonyos esetekben, azonban a kommunikációs rendszer nyújtotta információ az egyik fél számára pozitívumként, a másik oldalon pedig jogait sértő eseményként értékelődik. Gondoljunk csak az NSA által létrehozott Echelon elnevezésű, elektronikus üzenetek lehallgatására képes globális rendszer „lelepleződésére” és az EU felháborodására, vagy a terrorizmus elleni küzdelemhez kapcsolódó adatgyűjtés és az adatvédelem között ellentmondásokra. Az állam, mint a társadalom tagjai átfogó biztonsági érdekeinek képviselője és az egyén személyiségi jogainak ellentétes érdekei gyakori vitatéma volt az Egyesült Államokban egészen a terrortámadásokig.

A témakörhöz kapcsolódóan számos olyan írást talál¹³, amelyek az állam biztonsága érdekében végzett kommunikáció-ellenőrzést, és az egyén személyiségi jogai

¹² Paul Sperry – Day of infamy 2001, www.worldnetdaily.com

kapcsolatának problematikáját tárgyalja. Vitathatatlan, hogy mindennapjaink során akaratlanul is számos olyan tevékenység részesei vagyunk, amelyek magánéletünkbe engednek betekintést. Weblapok nézegetésekor, pénzkidő automatak használatakor, bankkártyával történő fizetésekor, beléptető mágneskártyák használatakor számos információ gyűjthető az egyén szokásairól, hollétéről. A cikk példaként említi, hogy a New Yorkban élők vagy dolgozók tevékenységét naponta átlagosan hússzor rögzítik térfigyelő kamerák.

Kommunikációs rendszerek zavarai

Minél szervezesebben válik egy kommunikációs rendszer életünk részévé, minél jobban épülnek rá a társadalom különböző tevékenységei és válnak nélkülözhetetlenné, annál nagyobb károkat okozhat ezek összeomlása. A rendszerek összetettsége azonban megnehezíti a zavarok által okozható problémák jelentőségének, méreteinek, igazi súlyának behatárolását. A banki adatbázisok elérhetetlenné válása rövidtávon, a társadalom széles körét érintő, nemzetközi méretű gazdasági károkat okozhat, míg konfliktushelyzetekben, vagy akár békeidőben a készenléti szervek kommunikációjának hiánya követelhet közvetlenül emberéleteket.

Természetes szükséglet, hogy veszélyhelyzetekben a legrövidebb időn belül információt akarunk kapni az eseményekről, amelyet a rendelkezésünkre álló kommunikációs csatornán próbálunk megszerezni. A katasztrófákat követően megnövekedett kommunikációs igény azonban gyakran a társadalom széles körében alkalmazott távközlési rendszerek (pl. cellás mobiltelefon rendszerek) túlterhelését okozza, amely nagymértékben veszélyezteti a mentést szervező, illetve abban résztvevő szervezetek munkáját.

A hagyományos, vezetékes távközlés sebezhetősége mindenki előtt ismert. A vezetékes távközlési eszközöket természeti katasztrófák tehetik tönkre, a kábeleket esők áztathatják el, a földmunkákat végző markológépek vezetékeket vághatnak el hosszabb időre megbénítva ezzel a kommunikációt, míg a fejlettebb műholdas hálózatok működési biztonsága 99,9 százalék fölötti.

A biztonsághoz közvetlenül kapcsolódó kommunikációs rendszer hiánya hasonló súlyú veszélyeket hordoz magában, hiszen a környezetünkben bekövetkezett szerencsétlenségeket (ipari és természeti katasztrófa, vagy akár terrortámadás) követő mentési feladatok kezelését teszi lehetetlenné.

A New York-i és washingtoni terrortámadásokat követően emberek tömegei próbáltak mobiltelefonon keresztül segítséget kérni, vagy egyszerűen csak információt kapni rokonaik, ismerőseik hollétéről. Az ikertornyokon lévő infrastruktúra megsemmisülése, a mobilszolgáltatók rendszereinek túlterheltsége, a rendőrség és a még analóg rádiókat használó tűzoltóság kommunikációjában fellépő zavarok rámutattak arra, hogy elkerülhetetlen a veszélyhelyzetek kezelését támogató készenléti rendszerek kiépítése.

A kommunikációs rendszerek használatának hirtelen megnövekvő igényét támasztja alá a madridi terrortámadás is, amelynek időszakára a város azonban már rendelkezett készenléti célra telepített rendszerrel. A mentési műveleteinek első napján a spanyol készenléti rendszeren 180 000 hívást bonyolítottak¹⁴.

¹³ pl. Joshua Quittner, *Invasion of Privacy*, Time 1997. aug. 25-i száma

¹⁴ forrás: Motorola Tetra hírlevél 2004./1.

Összefoglalás

Korunk legnagyobb tempóban fejlődő szektora a távközlés, együtt formálódik a társadalommal, a társadalomban megjelenő hatásokkal. Egyre újabb és újabb igények merülnek fel, amelyeket már nem csak kényelmi szempontok, hanem biztonságunk is indokol.

Az elmúlt évtizedben a távközlés globalizálódását meghatározó folyamatok robbanásszerűen mentek végbe és napjainkban is tartanak. Az Internet és a mobiltelefonia tömeges elterjedésével világméretűvé vált az emberek mindennapi életét is meghatározó, jó és rossz célokra egyaránt felhasználható távközlés.

Az előző évszázad második felének „minél több információt, minél rövidebb időn belül, minél nagyobb távolságra eljuttatni” gondolkodását követően korunk hihetetlen mértékű és irányultságú információéhes társadalommá vált. A napjainkra jellemző információdömping korában az adott információ átvitele mellett, azok tömeges feldolgozása, a számunkra szükségesek kiszűrése, illetve a meglévő adataink teljesebb védelme válik egyre meghatározóbbá.

A biztonság, mint szükséglet a háttérben folyamatosan jelen volt a rendszerek fejlődésénél. A második világháború idején a kézi rádiók tömeges elterjedése, a hidegháború okozta katonai versengés során létrehozott katonai kommunikációs rendszerek, a cellás rendszerek térhódítása, a veszélyek elhárítását és felszámolását, rendezvények biztosítását támogató készenléti rádiórendszerek mind-mind olyan fejlesztések eredményei voltak, melyek háttérében a biztonsághoz kapcsolódó érdek, igény, szükséglet állt.

A társadalmunk működését behálózó kommunikáció, azonban veszélyeket is hordoz magában. A terrorizmus példája jól mutatja, hogy a fejlődés eredményeként megjelenő kommunikációs lehetőségek az értékeinkkel, érdekeinkkel ellentétes közösségek előtt is nyitva állnak. A rendszereket érintő zavarok, a hálózatok összeomlása, illetve megbénulása alapjaiban veszélyeztetnék mindennapi életünket. Nem szabad tehát biztonságunkat teljes mértékben kizárólagosan a technikai lehetőségekre építeni, hanem szem előtt kell tartani azok felhasználási területét, az alkalmazás célját és a felhasználással párhuzamosan törekedni kell rendszereink minél teljesebb védelmére.

Az évtizedek óta tartó információs technológia fejlődésének célja egyértelmű: bárki, bármikor, bárhol kapcsolatot tudjon teremteni. Az igazi kérdés az, hogy ennek milyen hatása lesz a társadalom tagjainak egyéni és csoportos biztonságára.

Felhasznált irodalom:

- [1] László Ferenc 2003-ban fokozott veszélyt jelenthet a cyberterrorizmus / www.sg.hu
- [2] Meixner Zoltán Valós veszély – alacsony kockázattal / www.magyarhirlap.hu
- [3] Quittner, Joshua Invasion of Privacy, Time 1997. aug. 25-i száma
- [4] Simon György A biztonság specifikus területei
- [5] Információ- és adatvédelem című tudományos konferencia anyaga
- [6] KBH Szakmai Tudományos Közlemények, Budapest 2003., p7.
- [7] Solomon, Richard – Brown, Sheryl J. Creating a common Communication Culture Interoperability in Crisis Management
- [8] Conference on Crisis Management and Information Technology
- [9] Helsinki, 2003.sept.12.
- [10] Sperry, Paul Day of infamy 2001, The dozen or so Islamic / www.worldnetdaily.com
- [11] Taylor, Matthew
- [12] Court told of Internet 'terror' links - Special Report
- [13] The Guardian, 2004. aug. 07. www.guardian.co.uk/alqaida
- [14] Teather, David and Barkham, Patrick
- [15] Brown's photo on al-Qaida disks's - Special Report
- [16] The Guardian, 2004. aug. 09. / www.guardian.co.uk/alqaida
- [17] Váncsa Julianna Dr. Az elektronikus információbiztonság menedzsmentje
- [18] Információ- és adatvédelem című tudományos konferencia anyaga
- [19] KBH Szakmai Tudományos közlemények, Bp., 2003. május 07., 22. p.
- [20] Weimann, Gabriel
- [21] How modern terrorism uses the Internet – (www.terror.net)
- [22] Special report 116 - www.usip.org/pubs
- [23] www.cnn.com
- [24] Improving communications – 2002.09.06.
- [25] www.cnn.com
- [26] Bin Laden goes low-tech to avoid a trace – 2001.09.14.
- [27] www.cnn.com
- [28] Daniel Sieberg's article
- [29] www.iptvreports.mcmail.com
- [30] Policy issues for the European Parliament
- [31] www.kepesifi.co.yu
- [32] Irak és a cyberterror
- [33] www.msnbc.msn.com
- [34] Homeland Terror Watch: Adequate emergency communication?
- [35] Jesse Ventura looks into citizens' security concerns - 2003. 06.05.
- [36] www.nsa.gov/coremsgs
- [37] Preparing for the future
- [38] www.washingtonpost.com
- [39] Cyber-attacks by Al Qaeda

BESZÉD ÉS ADATKOMMUNIKÁCIÓ KONVERGENCIA LEHETŐSÉGE A MAGYAR HONVÉDSÉG TÁVKÖZLŐ ÉS INFORMATIKAI RENDSZEREIBEN

(összefoglaló)

Bevezetés

A Magyar Honvédség távközlő rendszerének digitalizálása 1998-ban kezdődött. A hosszas döntési eljárást követően a Siemens Telefongyár Kft. került győztesként kihar- detésre. Az eljárás eredményeképpen kiépült a távközlő hálózat alapját képező rend- szer, hálózat-felügyeleti rendszerrel, illetve a kívánt és a törvények által meghatározott alkalmazásokkal.

Az éves költségvetés engedte határokon belül a rendszer tovább épült, ennek kö- szönhetően ma már közel 50 központ, illetve 10.000 végpont üzemel a hálózatban egységes felügyeleti rendszerrel.

Időközben a NATO Core Network kiépítését a Siemens nyerte meg, ennek része- ként egy Siemens központ került Budapesten telepítésre, amely biztosítja a Magyar Honvédség és a NATO távbeszélő rendszereinek együttműködését.

A távbeszélő rendszer lehetőségei

Az ISDN alapú távbeszélő rendszer telepítésekor több olyan kényelmi és biztonsá- gi szolgáltatást tartalmazott, amelyeket a mai napig nem használnak ki teljes körűen. A szabványos ISDN szolgáltatásokon, az LCR (Least Cost Rourting), a hívásadat- feldolgozó rendszer megbízhatóan működnek, azonban a megvásárolt és telepített a PIN kódokkal biztosított szám- és szolgáltatás hordozhatóságot biztosító rendszer, a digitális riasztó-értesítő rendszer, a hálózati szintű hívásrögzítő rendszer, a hálózati tervezést biztosító alkalmazások még kihasználatlanul rejtőznek az alkalmazás- szerverek mélyén. Olyan alkalmazások, amelyek egy zárt célú hálózatot hatékony működtetést biztosítani tudják és a megfelelő biztonságot garantálják.

Gondolkodjunk hálózatban!

Az eltel időben sok tapasztalattal lettünk gazdagabbak. A telepített rendszer meg- bízhatóan üzemel, a karbantartás és üzemeltetés támogatása biztosított, kialakultak a megfelelő szinten együttműködő „csapatok”, akik a tervezéstől az üzemeltetésig bizto- sítják a rendszer képességét alapfeladatainak ellátására.

A haderő átalakításával és a nemzetközi feladatok ellátásából adódó feladatok azonban egyre nagyobb – a Siemens által is látható – terheket ró a csapatra. Az együttműködők az MH részéről egyre inkább „tüzoltó” jelleggel oldják meg a hálózat fejlesztésére vonatkozó feladatokat. Több alkalommal szembesültünk azzal, hogy a probléma lokális megoldását előtérbe helyezve a megrendelőnk nem gondolja át teljes körűen a feladat teljes hálózatot érintő hatásait. Ilyen esetekben amennyiben az idő és a feladat állapota megengedi, megpróbáljuk a figyelmet felhívni, ha már erre nincs lehetőség a jó üzleti partner más módszerrel gondoskodunk a probléma megoldásáról.

Talán meggondolandó, hogy a képzés és továbbképzési rendszerben nagyobb hangsúlyt kellene fordítani a felajánlott támogatások, továbbképzések elfogadására. Az ilyen felajánlott, gyakorlati képzést is tartalmazó rendezvények biztosíthatják a

megfelelő gondolkodásmód kialakulását, a megfelelő szellemi tőkét a rendszer működtetéséhez.

A szövetségi hálózatok tervezői és üzemeltetői szervezeteinél alapkövetelmény a hálózatban gondolkodás.

Az NNC (NATO Network Management Center) szervezetéből évente több rendszermérnök vesz részt kiemelt szintű Siemens tanfolyamokon, az NC3A több közös fejlesztési projektet futtat a Siemens-el közösen, jelentős Siemens kompetencia épült ki a NATO szervezetén belül.

Fejlődési lehetőségek

Az IT szegmens fejlődése félelmetes sebességgel zajlik a világban. Habár kereskedelmi szempontból a szegmens még nem lábalt ki a hullámvölgyből, technológiaiag egyre meredekebb tempóban halad a fejlődés. Ennek eredményeképpen megjelennek technológiák, amelyek a csúcsot képviselik és megtérülő befektetéseket, gazdaságos üzemeltetést ígérnek.

Alapkérdés, hogy kell-e egy megbízhatóan működő, biztonsági követelményeknek megfelelő zárt célú hálózatnak akárcsak megpróbálni rohanni a legfrissebb fejlesztések után?

Nem titok, hogy a legfrissebb fejlesztések bejelentése nem mindig jelenti a teljes funkcionalitással bíró, minden ígért követelményeknek megfelelő és biztonságosan működő termék „megszületését”. A gazdaságos üzemeltetésre vonatkozó adatok a valós működésre vonatkozó tapasztalatok hiányában statisztikai módszerekkel számított értékeken alapul a műszaki támogatást végzők nem rendelkeznek valós tapasztalatokkal.

Ennek a kérdésnek a megoldása a szállító felelőssége.

Mérlegelni kell, hogy az innovációs hírnév, vagy a megbízható partnerség a fontosabb. Néha fel kell vállalni a rosszallást a fejlesztések lassúbb bejelentéért a megbízhatóságért cserébe.

Mit is jelent ez a gyakorlatban a Siemens számára?

A világpiacon hódít az IP alapú telefonía, az integrált beszéd és adatkommunikáció, amelynek bevezetését – sőt egyáltalán bemutatást az MH részére – késleltettük. A hazai piac szereplőitől és néha partnereinktől is megkaptuk a negatív jelzéseket, azonban ezt felvállaltuk, mert a saját követelményeinknek megfelelő – az MH részére is felajánlható megoldás még nem rendelkezett elegendő üzemeltetési tapasztalattal. Tetjük ezt annak ellenére, hogy a NATO már 2001-ben döntött a meglévő Siemens ISDN infrastruktúra IP alapúra történő fejlesztéséről, sőt külön projekt indult – és azóta fejeződött be – mobil, gyorsan, minden körülmények között bevethető Siemens IP központ fejlesztésére.

Tette ezt azért, mert a Siemens megoldásához nem kell beruházásokról és megtérülésről beszélni. Az ISDN – IP fejlesztés a Siemens megoldásai esetében a központok esetében egy nagyobb teljesítményű processzorkártya telepítését, illetve egy bővítő-kártya telepítését jelenti. A felügyeleti rendszerben egy új – lefelé teljesen kompatibilis – alkalmazáscsomag kerül telepítésre, amely képes magába integrálni több gyártótól független felügyeleti rendszert.

Az új felügyeleti rendszer előnyeit kihasználva az NC3A UMBRELLA névvel külön projektet indított, amelynek eredményeképpen a Siemens felügyeleti rendszere fog rátelepülni a meglévő rendszerekre – biztosítva ezzel a teljes integrációt. A rendszer

funkciói önállóan is működőképesek és a biztonság érdekében fizikailag is eltérő helyen és infrastruktúrán kerülnek telepítésre.

Hogyan tovább Magyar Honvédség?

Az elmúlt évben a távbeszélő hálózat mellett megkezdődött az önálló informatikai gerinchálózat kiépítése és egyre erősebb az igény az IP alapú kommunikációra. A hálózat működéséről egyre több on-line információra, statisztikára van szükség. A NATO által finanszírozott 3D radarfejlesztések már teljesen IP kommunikációra épülnek, a hazai más rendszerekhez sem lehet az IP technológia nélkül csatlakozni.

A Siemens által kínált fejlődés beruházásként csak a hálózat felügyeleti alkalmazáscsomag tervezendő, a központok egyedei képességeinek kialakítása nem igényel jelentős beruházást, csupán kártyacseréket.

A meglévő rendszerben semmit nem kell kicserélni, átalakítani, a megszokott alkalmazások, kártyatípusok, interfészek megmaradnak. Megjelennek új IP alapú berendezések, illesztőkártyák, szolgáltatások, alkalmazások, amelyek tovább növelik a hálózat megbízhatóságát, hatékonyságát.

A 2001 óta világszerte megszerzett üzemeltetési tapasztalatok megbízható hátteret biztosítanak az „upgrade” végrehajtásához. Az oktatásokhoz új, web alapú internetes oktatási központ, illetve Budapesten telepített tesztlabor áll rendelkezésre.

Az átállás zökkenőmentesen, üzemkiesés nélkül biztosítható, az átalakított rendszer továbbra is megfelel minden biztonsági követelménynek.

Tény, hogy a világpiaci bevezetéséhez képest 3 évvel később tartjuk bevezethetőnek az IP technológiát a Magyar Honvédség zártcélú hálózatában. De ilyen feltételekkel reméljük megéri a várakozás.

Információs hadviselés – új fenyegetettségek a digitális világból

(összefoglaló)

A korábbi konferenciák hagyományait követve továbbra is a legújabb típusú hadviselési formát vizsgálat az előadás célja.

Rövid áttekintés után a elméleti vizsgálat alá kerül az információs hadviselés maga, módoszatai, feltételei, alkalmazásának indokai és alapjai, illetve e lehetséges védekezési, kockázatsökkentési módok.

Külön elemzésre kerül a napjaink legnagyobb kockázati tényezőjét képviselő hálózatközpontú hadviselés – amely a nem megfelelően szervezett vezetési rendszereket veszi célba.

Az előadás végén bemutatásra kerülnek azok a Siemens megoldások, amelyek több szövetségi hadseregben és magánál a NATO-nál is bizonyították képességeiket, a védelem egyik elemeként vigyázzák a vezetési rendszereket.

INTEGRÁLT HÁLÓZATBIZTONSÁG A SZOLGÁLTATÓNÁL

Bevezetés

Magyarország az elektronizálódás korát éli. Megfigyelhető ez a tendencia a legmagasabbtól a legalacsonyabb szintekig. Kimutatható ez a trend az Európai Unió hazánkkal szemben támasztott elvárásaiban, a kormányzat rövid és hosszú távú stratégiai terveiben.

Az Európai Unió kidolgozott stratégiai elképzelésekkel, tervekkel rendelkezik az informatika és a közigazgatás témakörében is (**eEurope**). Ezzel összhangban kormányzati szinten kialakításra került az **Európa-terv**, illetve annak kisebb időszakokra lebontott ütemei, melyek a kormányzat hosszú távú fejlesztési célkitűzéseit tartalmazzák. Az Európa-terv híd az Európai Unió céljai, illetve támogatásai, és a Magyar Köztársaság kormányának szándékai között. Összehangolja az állam, a gazdaság és a civil társadalom törekvéseit. Egyesíti a központi (állami, önkormányzati) és a gazdasági, pénzügyi forrásokat. Hatékony eszköze a modernizációnak.

Az Európai Unió a csatlakozó államokkal folytatott közös tervezés támogatására Strukturális és Kohéziós Alapokat hozott létre, melyeknek hazai szintén való forrásként történő felhasználására kialakításra került a **Nemzeti Fejlesztési Terv (NFT)**, ami a különböző célkitűzések megvalósításának támogatására operatív programokat hoz létre folyamatosan.

2002 elején megalakult a Kormányzati Informatika és Társadalmi Kapcsolatok Hivatala (MEH KITKH) a kormányzati informatikai feladatok ellátására. 2002 végén a kormány elfogadta a Magyar Információs Társadalom Stratégia elkészítésének rendjét. Az egyes minisztériumok részstratégiái (köztük az elektronikus kormányzattal foglalkozó szakanyag) az IHM ajánlásai alapján készültek el. A MITS fejlesztése az e-Europe programmal és a Nemzeti Fejlesztési Tervvel (NFT) összhangban történik, ezáltal biztosított Magyarország számára, hogy az Európai Unió támogatási alapjaiból részesülhessen.

Az uniós tagállamként való sikeres működés, az uniós források hatékony kihasználása, illetve a közigazgatási szolgáltatások hatékonyságának és színvonalának javítása azonban komoly kihívások elé állítja minket.

1. AVDH- Anya Vállalat Digitális Hálózata

Az integrált hálózatbiztonság lehetőségének tárházából egy példát mutatok be. Egy kitalált kormányzati szolgáltatón keresztül egy lehetséges alternatívát fogunk látni. Nevezzünk ezen egységünket **Szolgáltatónak**.

A Szolgáltató más 219 egyéb központi közigazgatási intézményi végponttal együtt kapcsolódik a képzeletbeli Elektronikus Gerinchálóra.

A Szolgáltató egy nemzetközi Anya Vállalathoz csatlakozik, és az egységes MPLS (Multiprotocol Label Switching) VPN (Virtual Private Network) alapú hálózatot (AVDH, Anya Vállalat Digitális Hálózata) üzemeltet az Anya Vállalat szervezeti számára. Ezen az egységes hálózaton valósulnak meg a Szolgáltató WAN kapcsolatai is. A Szolgáltató központja Budapesten működik.

A kommunikációs rendszer fő részét a Budapestet a megyei kirendeltségek központjaival összekötő nagysebességű transzporthálózat alkotja, mely a különböző rendszerek (távbeszélő, adatátviteli) forgalmát bonyolítja le. Az átviteli gerinchálózathoz – *megyén belül* – a megyei kirendeltségeken, a kapcsolódó Közigazgatási Hivatalon, illetve az alegységeken létesített csomópontokon keresztül lehet csatlakozni, melyeken keresztül a **körgyűrűbe szerveződő** országos központok (0. Objektum; 1-es objektum; 2-es objektum, 3-as objektum) elérhetőkké válnak.

A transzporthálózatot **elsődlegesen** a Szolgáltató kezelésében levő országos *mikrohullámú rendszer* összeköttetései alkotják, biztosítva a kerülőutak automatikus kialakításának lehetőségét is, másodsorban a közcélu távközlési szolgáltató FLEX-COM átviteli útjai.

A gerinchálózaton az ATM kapcsolási technika került alkalmazásra, ami távlatilag a felhasználók irányába **adat, hang, kép és mozgókép** átvitelét biztosítja.

Az egységes digitális hálózathoz alapvetően (de nem kizárólagossággal) más közigazgatási szervezetek csatlakoznak elkülönült módon, virtuális magánhálózatok (VPN – virtual private network) kialakítása útján.

A látszólagos, logikailag elkülönített rendszerek lehetőséget biztosítanak egy közös adatátviteli közeg felhasználásával (alapvetően: Szolgáltató mikrohullámú rendszer) a független, adatbiztonsági szempontból teljesen védett alrendszerek kialakítására, melyben a menedzsment tevékenységet is saját erőforrások (műszaki-technikai, humán) alkalmazásával lehet biztosítani, függetlenül a többi felhasználótól.

2. Integrált hálózathbiztonság a Szolgáltatónál

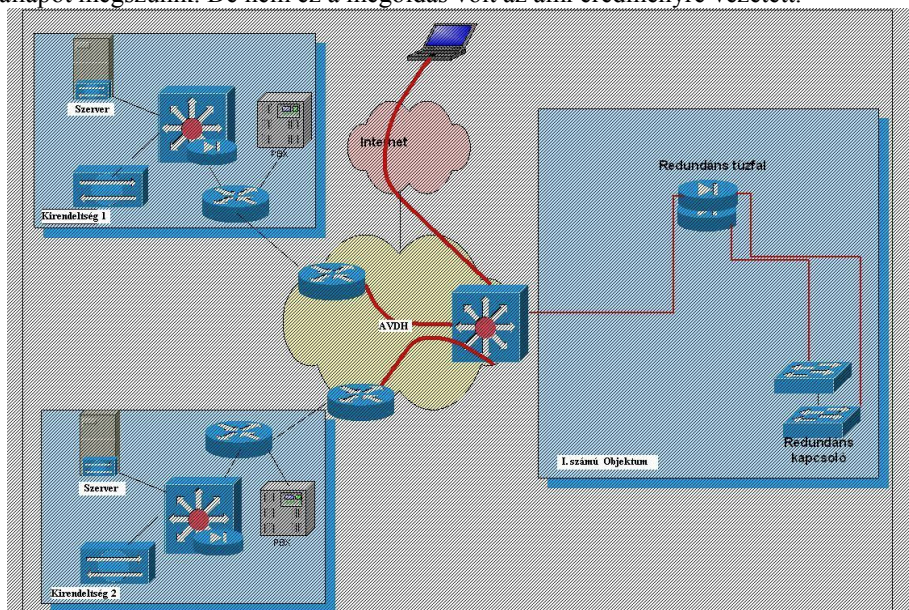
A Szolgáltató az Európai Unió csatlakozására felkészülve megelőző vizsgálatokat folytatott információtechnológiai területein. A vizsgálatok eredményeképpen megállapítást nyert, hogy szükséges a hálózat rekonstrukciója biztonságtechnikai okokból. A felmérések alapján több tervezet is készült egy új egység informatikai hálózat kiépítésére.

A Szolgáltató olyan egységes, biztonságos hálózatot szeretne kiépíteni és költség-hatékonyan üzemeltetni, amelyen egyidőben több hálózati szolgáltatás is meg tud valósulni. Ilyen szolgáltatások egyike az adathálózattal integrált hangátvitel, amelyet a Szolgáltató már jelenleg is több kirendeltségén üzemeltet.

A jelenlegi rendszerünkben a Központi Távközlési Szolgálat üzemeltetésében egy országos gerinchálózat (AVDH- Anya Vállalat Digitális Hálózata) működik ami ugyan MPLS VPN (Multiprotocol Label Switching és Virtual Private Network) hálózat de csak a „külvilág számára” van elkülönítve ez a hálózat, jelen felépítésében a hálózatban szereplő többi szervezet számára (o. Objektum, 1-es objektum, Szolgáltató, stb.) nem. Ezen szolgáltatói hálózat jelenlegi állapotában nem biztosít a Szolgáltató adatai számára teljes körű titkosítást.

Ez tényyszerűen azt jelenti, hogy a Szolgáltató bármely, routolt hálózatba kapcsolt munkaállomása IP-s kapcsolatba kerülhet a AVDH-ba bekapcsolt szervezetek munkaállomásaival. Ezt a kapcsolatot a Szolgáltató szervezetei jelen feltételek mellett nem

tudják kontrollálni, ami az adatbiztonság kérdését felveti. Az adatvédelmi törvény előírja, hogy különböző szervezetek adatállományait nem lehet összekapcsolni. A jelenlegi helyzetben közvetlen hozzáférhetőség kínálkozik adatainkhoz a AVDH-n keresztül. Rövidtávú megoldásként felvetődött, hogy ha logikailag leválasztjuk a jelenleg hálózatainkra kapcsolt Központi Távközlési Szolgáltató routereket, akkor ez az állapot megszűnik. De nem ez a megoldás volt az ami eredményre vezetett.



A Szolgáltató, hálózati topológia szempontjából csillag elrendezés alapján került kialakításra. A középpontban az 1-es objektum a Szolgáltató központja áll, ezzel vannak kapcsolatban a megyei kirendeltségek, majd ezek alatt a városi alegységek találhatók. Ezt a topológiát követik a szolgáltatások, vagyis az NDS címtár parciális replikációra lett beállítva. A levelezési szolgáltatást a Groupwise kiszolgálók biztosítják.

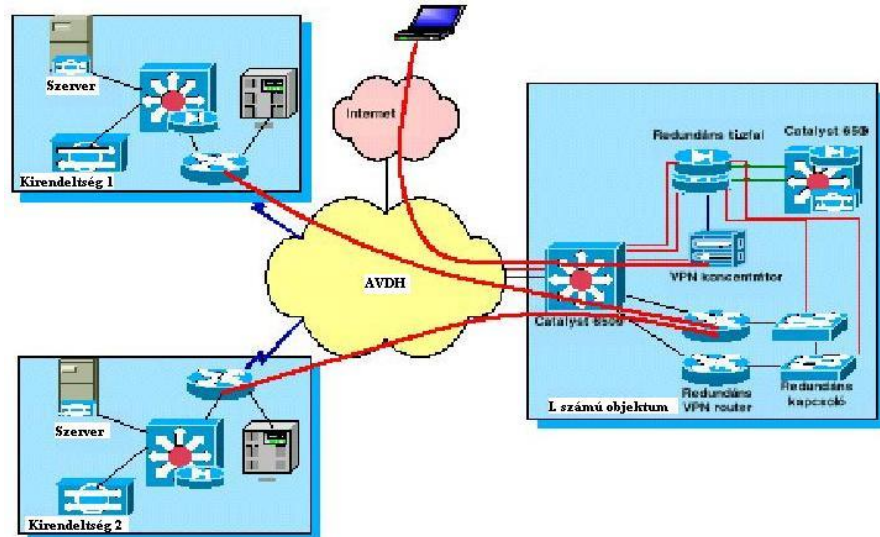
A helyi hálózaton a hang-adat integráción kívül követelmény volt még a magas rendelkezésre állás, illetve a hálózatbiztonság. Ezeket a követelményeket vettük figyelembe a helyi hálózat tervezésénél.

3. Az 1-es objektum helyi hálózatának rekonstrukciója

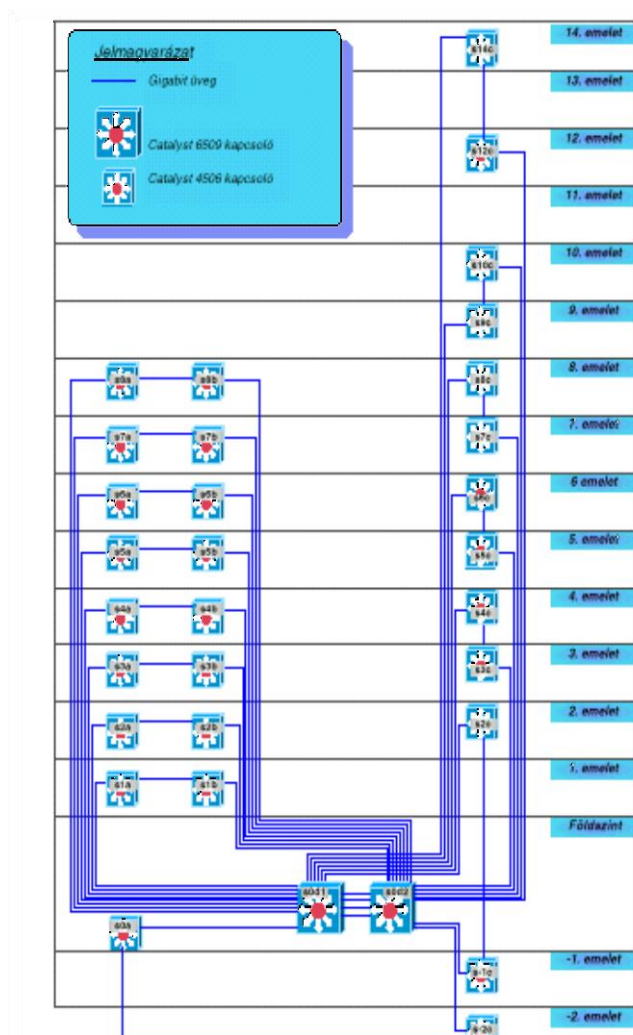
A Szolgáltató 1-es objektuma – jelenleg üzemeltetett LAN hálózata - már nem elégti ki a kor követelményeinek megfelelő biztonsági és a modern hálózati szoftverek által megkövetelt sávszélesség igényt. Az egyre növekvő hálózati igények, az új szolgáltatásokkal szembeni elvárások tették szükségessé az 1-es objektum központ helyi hálózatának rekonstrukcióját.

A megoldás a főrouterek VPN-es kapcsolatai egymással, egyetlen – az 1-es objektumban levő – tűzfal kijáratával az Anya Vállalat társzervei felé. Ezáltal autonóm hálózattá válik a Szolgáltató hálózata, a külső bejutásokat a Szolgáltató szervezetének kezelésében levő tűzfalak engedélyezhetik. (Megszűnik a közvetlen adatkapcsolati lehetőség és a kontrollátlanság) A Központi Távközlési Szolgálat ezáltal tiszta

kommunikációs szolgáltatóvá válik, elhatárolódnak a Szolgáltatói és az Anya Vállalati felhasználások, üzemeltetési hatáskörök.



A változtatás alapja két, nagy megbízhatóságú párként üzemelő Cataliyst 6509 kapcsoló, mely hálózat szintű (OSI layer 3) kapcsolást is végez. A szintenkénti kapcsolást Catalyst 4506 kapcsoló berendezések végzik. Ezek a kapcsolók a Cisco helyi hálózati kacsolói közül a legkorszerűbbek, moduláris szinti illetve gerinckapcsolók. Minden szinti kapcsoló redundánsan kötődik a központi Catalyst 6509 kapcsolókhöz. Az A és B tömbben ugyanaz a szinten lévő kapcsolón keresztül kerül biztosításra a redundáns kapcsolat, míg a C tömbben páros emeltenként (kivétel 11, 13, földszint és az 1. emelet) kerül kialakításra a redundáns konfiguráció. A konfiguráció biztosítja, hogy az esetlegesen előforduló optikai szál szakadása esetén automatikusan, gyorsan át tudjanak állni a kapcsolók a másik tartalék kapcsolatra.



A konfiguráció megvalósítása már elkezdődött. 10 darab Catalyst 4506 kapcsoló került telepítésre, ezek közül 8 darab szinti kapcsolóként 2 darab központi kapcsolóként üzemel most. Minden kapcsolóban a felhasználói portok támogatják az ún. in-line power szolgáltatást, azaz tápellátást tudnak biztosítani akár IP telefon, vagy rádiós hálózatos megoldásnál alkalmazott Access Point számára. Minden Catalyst 4506 szinti kapcsoló 96 darab 10/100 ethernet interfészt szolgáltat. Minden kapcsolóban redundáns tápellátással, illetve a központi kapcsolókba redundáns vezérlő kártyával (Supervisor Module) készült a tervezet. A redundáns vezérlő kártya biztosítja a gyors automatikus átkapcsolást a másodlagos vezérlő kártyára.

A Catalyst 6509 kapcsolók konfigurációjával kapcsolatban megjegyzem, hogy a jelenlegi konfigurációban még nem szereplő, nemrég kifejlesztett WS-X6548V-GE-TX modul szoftver támogatása a Cisco Kft-től már elkészült. Ezzel az új, a kapcsoló nagy teljesítményét kihasználó – ún. fabric-enabled – modul alkalmazásával, akár gigabites sebességű portok is beköthetők tápellátással együtt. A WS-X6516-GE-TX modulokkal kapcsoljuk a szervereket a hálózatra akár rezes gigabites interfészekon keresztül – nem lettek megtervezve a tápellátás portok a szerverek számára –, míg a WS-X6516A-GBIC modulok szolgálnak a szinti kapcsolóktól érkező optikai gigabites csatlakozások fogadására.

A konfiguráció üzemeltetése IEEE 802.1x hozzáférés szabályozással fog történni, azaz mielőtt a felhasználó hozzáférne a hálózathoz azonosítania kell magát, ehhez az Access Control Server funkcionalitásra van szükség.

Az 1-es objektum LAN alapja egy redundáns központi csillag topológia, tartalék linkekkel, melyek a 'csillagok' két-két ágát hurokká egészítik ki.

Az épület kiterjedtsége és belső elrendezése miatt emeletenként 3 rendező (A, B, C) szolgálja ki a végpontokat. A központi rendező (0D) a földszinten helyezkedik el, benne két Catalyst 5500 (s0d1, s0d2) és két 4506 (s0d3, s0d4) switch alkotja a csillag-pontot. Az emeleti rendezőkben többségében 1-1 Catalyst 5000 switch működik, de a tavaszi fejlesztés során már bővített -2c, 0a, 5a, 5b, 6a, 6b, 7c, 8c rendezőkben már 4506-os switchek működnek. Minden egyes emeleti rendezőhöz a két központi switch (s0d3, s0d4) valamelyikéről egyetlen link vezet. Ezen túl a központi négy switch is össze van kötve egy linkkel, s az emeleti rendezők is páronként össze vannak kötve egy-egy linkkel.

4. A továbbfejlesztés

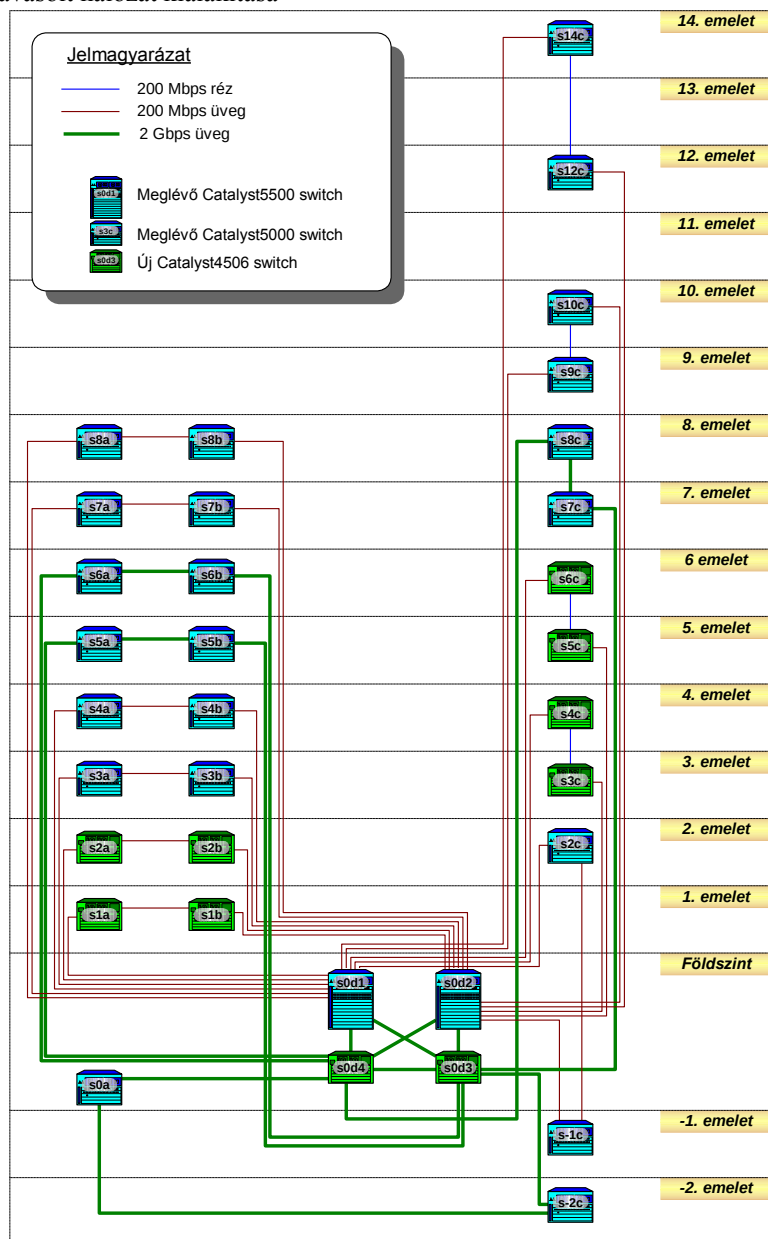
Célunk egy homogén, integrált, biztonságos hálózati infrastruktúra kifejlesztése.

Az eszközökbe csatlakozó felhasználók száma és az általuk használt programok sávszélesség igénye az idők folyamán megnövekedett. Ennek kielégítésére szükség lenne a pillanatnyilag használt kapcsoló modulok korszerűbbre cserélésére. A pillanatnyilag használatban lévő switchek beépített moduljainak legnagyobb része, csak 10Mbps vagy 100Mbps sebességre képes (kivéve ahol az új 4506-os switchek működnek). Ezek a kártyák „groupswitch” technológiát használnak, aminek hátránya, hogy az egy csoportban lévő felhasználók együttesen használják a számukra adható 10 vagy 100Mbps sávszélességet. Ez a megoldás biztonságtechnikai problémákat felvet még, ugyanis az egy csoportban lévő felhasználók hálózati adaptereihez eljut a csoportba küldött összes csomag, ezáltal egy program segítségével hozzá lehet jutni a csoportba küldött információkhoz. Ennek megoldására ezeket a modulokat, „portswitch” modulokra kell cserélni azokon a helyeken, ahol még eddig nem volt switch csere. Ezekre a helyekre is 4506-os switchek javasolunk a hálózat aktív eszközparkjának homogenizálása végett. Ezen az eszközök minden portja támogatja az in-line power szolgáltatást, amellyel tápellátást tudnak biztosítani az IP telefonok, illetve rádiós hálózati megoldásnál alkalmazott Access Point-ok számára.

A biztonság megvalósításának a lehetősége az új eszközökben egyszerűbb, mert támogatják az AAA (Authentication, Authorization és Accounting) funkciók megvalósítását, ami lehetővé teszi, hogy a hálózati erőforrásokat biztonságos módon lehessen

engedélyezni a felhasználóknak, megbízhatóan azonosíthatók legyenek, valamint a hozzáférést egyértelműen lehessen naplózni.

A javasolt hálózat kialakítása



5. A nagytávolságú hálózat kialakítása a megyei kirendeltségek routereinek rekonstrukciójával

A Szolgáltató eddig is nagy üzembiztonsággal használt Cisco 3640 routereket megyei kirendeltségek szintjein. Ezek a routerek kiválóan teljesítették a feladatukat, de a mai kor kihívásai (hardveres AES titkosítás és tömörítés) már egy korszerűbb, nagyobb teljesítményű platformot (pl.: Cisco 3745) igényelnek.

5.1. A tervezet alapján az alábbi változtatásokat vezetnénk be

Ezen tervezet keretében a Cisco 3810 és a Cisco 2522 routereket is upgrade-ljük. Továbbá az őrsi, illetve városi alegységek routereit is bevonjuk az upgrade-elési tervezetbe, mivel csak a végponttól végpontig terjedő tervezés és a szolgáltatások megvalósítása biztosítja a Szolgáltató számára a magas rendelkezésre állást, illetve a szolgáltatások (hang-adat integráció, Quality of Service, QoS) homogenitását. Ilyen átfogó hálózati megoldást a Cisonál találtunk (V3PN Voice and Video enabled VPN), amely rendelkezett a titkosításon alapuló VPN hálózatok és a hangszolgáltatás integrációját tekintve, a QoS szolgáltatásokat igénybe véve.

A megyei kirendeltségek routereinek kiválasztásánál fő szempont volt, hogy biztosítson elég szabad modul helyet a későbbi fejlesztéshez (pl. IDS Network Module), korszerű, időtálló platform legyen, nagy sebességgel szolgáltatson korszerű titkosító megoldásokat, illetve a már meglévő Cisco 3640 routerek moduljait fel tudjuk használni. Ezért került a választás a Cisco 3745 platformra megyei routerként. Ez a router az előbbi szolgáltatásokon túl redundáns tápellátással rendelkezik, és akár tápellátást biztosító ethernet kapcsoló modullal is kiegészíthető. A routerek az AIM slot-ba épített VPN gyorsító kártyával rendelkeznek, melyek nagy sebességű IPsec DES, 3DES, AES titkosítást és tömörítést tesznek lehetővé. Ez a mi szempontunkból rendkívül fontos, mivel a Szolgáltató az IPsec titkosítás módszerét helyezte előtérbe. De erről bővebben, későbbi fejezetben beszélünk.

A jelenlegi Cisco 3640 routerekben az alábbi Network Modulok üzemelnek: NM-HDV-1E1, NM-4T, NM-1CE1, NM-1FE2W, NM-2CE1. Ezek a modulok a Cisco 3745 routerekben felhasználásra kerülnek.

Minden megyei kirendeltség routerébe VPN gyorsító kártyákat helyezünk, mely nagy sebességű titkosítást tesz lehetővé. A megyei kirendeltségek központjainak biztonsága érdekében a helyi hálózatot IDS (Intrusion Detection System, betörésdetektáló) megoldással fogjuk védeni. Véleményem szerint érdemes minden egyes szervert és munkaállomást ezzel a módszerrel védelmezni.

Az IPsec kapcsolat végét az 1-es objektum központi telephelyre tervezzük, ez azt jelenti, hogy minden megyei router IPsec kapcsolata az 1-es objektumon egy redundáns VPN router párban végződik. A központi VPN routerként a redundáns konfigurációban Cisco 7206 VXR routerek lesznek elhelyezve, melyek a VAM-2 service modul segítségével nagy teljesítményű, a már korábban említett titkosítást biztosítja a hardveres tömörítéssel együtt.

A konfigurációban különálló IDS szenzor eszközt terveztünk be, mely sebessége révén akár a helyi hálózatot is képes védeni. A Cisco 3745 routerbe az IDS Network Module kerülne alkalmazásra kisebb forgalom esetén.

A tervezetben szerepel a VPN koncentrátor kiépítése is, mely segítségével távoli internetes elérés esetén egy mobil munkatárs, vagy akár egy mobil hálózat is biztonságosan, IPsec titkosított kapcsolat segítségével tud kommunikálni a Szolgáltató hálózata-

tával. A konfigurációban egy redundáns (High Availability) pár szerepel, mely hardveres AES titkosítási algoritmust is támogat.

Az átfogó hálózatbiztonsági menedzsmentben egységesen lehet konfigurálni, menedzselni az egyes hálózatbiztonsági rendszereket (VPN, tűzfalak és IDS megoldások).

6. IPSec

A Szolgáltató a tervezetben az IPSec titkosítási módszert helyezte előtérbe. Miért döntöttünk ezen technológia mellett:

Az IPSec protokollcsomagot az *IETF* (Internet Engineering Task Force) dolgozta ki, az egyes protokollok definícióit RFC-kben rögzítették. Az IPSec hálózati szinten nyújt lehetőséget arra, hogy a kommunikációban résztvevők *hitelesen* azonosítsák egymást (*authentication*) és kódolják (*encryption*) az egymás közt zajló adatforgalmat.

6.1. Az IPSec előnye

A legáltalánosabb megvalósítása az ilyen jellegű szolgáltatásoknak az IP-n belül. A magasabb szintű szolgáltatások, mint amilyen a *PGP* csak egy konkrét protokollt képesek védeni, míg az alacsonyabb szintűek, csak egy adott fizikai médiumot. Ezzel ellentétben az IPSec bármilyen protokollt képes védeni, amely IP fölött fut, és bármely médiumot, amelyen IP fut. Továbbá képes védeni vegyesen használt alkalmazás protokollokat, vegyesen alkalmazott médiákon, amely az Interneten mindennapos.

Az IPSec képes néhány olyan háttérszolgáltatást nyújtani, amelynek nincs érzékelhető hatása a felhasználókra. Ellentétben például a *PGP*-vel, amelyhez a felhasználónak meghatározott lépéseket kell tenni a használat során.

Annak ellenére, hogy tulajdonképpen az IPSec nem nyújt email titkosítási funkciót, képes titkosítani az email-t. A gyakorlatban ez úgy fest, hogy ha a támadó a publikus hálózatról tekint a forgalomra, nem tudja elolvasni a levelet. Ebben a szituációban az IPSec ugyanúgy megakadályozta az illetéktelen hozzáférést, mintha *PGP*-vel lett volna titkosítva a levél.

Az előny ott jelentkezik, hogy ez nem csak az email-ekre igaz, hanem minden IP felett folyó kommunikációra. IPSec átjárók bárhol kialakíthatóak ahol szükséges:

- Egy szervezet dönthet úgy, hogy a LAN és az Internet között elhelyezkedő tűzfalon létesít ilyen szolgáltatást. Ezzel a megoldással több irodájukat kapcsolhatják össze a külvilágtól védetten.
- Egy másik esetben a vállalat úgy dönthet, hogy a részlegeket összekötő gerinchálózatát védi ezzel a mechanizmussal. Így az üzenetek mindenkitől védettek, csak a küldő és fogadó részleg látja őket.
- Más talán nem az információ titkosításában látja a fő célt, hanem abban, hogy korlátozza a szolgáltatásokhoz és erőforrásokhoz való hozzáférést. Ekkor az IPSec csomag*hitelesítést* (packet authentication) a hozzáférés vezérlési mechanizmus (access control mechanism) részeként lehet alkalmazni, akár titkosítva, vagy anélkül.
- Igény szerint akár minden gépre telepíthető IPSec átjáró, ehhez természetesen minden gépen szükséges megfelelő feldolgozó kapacitás. Így minden gép kommunikációjára igaz, hogy csak a forrás és a cél látja azt.
- A fenti lehetőségek tetszés szerint kombinálhatóak.

6.2. Az IPSec hátrányai, korlátozó tényezők

Az IPSec-et arra tervezték, hogy biztosítsa a kapcsolatokat a gépek között. Ezt a feladatot nagyszerűen megoldja, de fontos, hogy észben tartsuk: ez nem minden. A legfontosabb korlátozó tényezők:

- Az IPSec gépeket hitelesít és nem felhasználókat

Csak bizonyos gépekről legyen elérhető a szolgáltatás és arra, hogy a gépek között a kommunikáció védett legyen, de itt az IPSec feladata véget ér, a további feladatokat más eszközökkel kell biztosítani.

- Az IPSec nem gátolja meg a forgalomelemzést

Az elemzés során sok információ származtatható a forgalomból anélkül, hogy ismernénk a kódolást, vagy értenénk az üzeneteket.

- Az IPSec nem old meg mindent

Ha arra van szükségünk, hogy egy dokumentum egy konkrét személy által legyen *hitelesítve*, azaz aláírva, akkor szükségünk lesz az elektronikus aláírássra és a *nyilvános kulcsára*, hogy ellenőrizzük azt.

- Az IPSec önmagában nem nyújt biztonságot

Ha a biztonsági átjárók nincsenek megfelelően védve a rendszer nem képes megvédeni magát.

- Az IPSec nem végponttól-végpontig terjed

A privát hálózatban elhelyezkedő forrásgéptől a security gateway-ig, illetve a security gateway-től a másik privát hálózatban lévő célgépig alapértelmezésben sem biztosítja az adatok sértetlenségét.

6.3. Alkalmazási területek, módok

- **Hitelesítés titkosítás nélkül**

Ha nem szükséges, az adatokat nem kötelező titkosítani. Ennek a következő okai lehetnek:

- az adatok publikusak, csak afelől akarunk bizonyosak lenni, hogy megfelelő helyről származnak, például egy cég website-ján publikált információk.
- ahol az adatok titkosítását nem ítélik szükségesnek, tipikusan olyan hálózatrészen, ahol azonos jogkörű és biztonsági szintű emberek dolgoznak.
- ahol a titkosítást az IP szint alatt, vagy felett végzi valamilyen más protokoll, vagy eljárás.
- ahol a titkosításra fordított erőforrás (overhead) más irányú felhasználásának igénye nagyobb prioritással bír, mint az adatok titkossága.

Titkosítás alkalmazása hitelesítés nélkül veszélyes

Eredetileg az IPSec titkosítási protokoll az *ESP* nem végzett *integritás* ellenőrzést, csak titkosítást. Steve Bellovin (AT&T Research) sok módot talált arra, hogy megtámadja a *hitelesítést* nem, csak *ESP*-t alkalmazó kommunikációt.

Manapság leggyakrabban a következőképpen alkalmazzák ezeket:

- *ESP* - titkosítás és hitelesítés
- *AH* - csak hitelesítés

Összefoglalva az IPSec biztonsági szolgáltatásai az alábbiak:

- Adatintegritás
- Adatforrás azonosítás
- Adatviisszajátszás megakadályozás

- Bizalmasság

7. Összefoglaló

A Szolgáltató esetében a kommunikáció jelenleg az Anya Vállalat Digitális Hálózatán valósul meg, mely teljes egészében az Anya Vállalat menedzselése alatt áll. A tervezet célja, hogy a szigorúbb szintű adatszűrési technológia bevezetésével az 1-es objektum központi routereinek, a Szolgáltató különböző intézményeinek routerei és a megyei kirendeltségek routerei között biztonságosabb kommunikáció jöjjön létre.

A megoldás a Szolgáltató főruterei között VPN-es kapcsolat létrehozása, egyetlen – az 1-es objektumban levő – tűzfal kijáráttal az Anya Vállalat társszervei felé.

Az autonommá vált hálózatra a külső bejutásokat a Szolgáltató szervezetének kezelésében levő tűzfalak engedélyezhetik. A Központi Távközlési Szolgálat kommunikációs szolgáltatóvá válik, üzemeltetési feladatokat lát el.

Az adatok tartalmának szűrése a tervezet alapján a megyei kirendeltségek routereinek feladata lesz az IPSec-es technológia segítségével. (Mint az Internetes szolgáltatók esetében: a szolgáltató biztosítja a hozzáférést és az igénybe vevő korlátozza saját szervezetén belül a használatát a szolgáltatásnak.)

Ezen tervezetekből jelenleg a gerinchálózatra való csatlakozás valósult meg. Teljes körű kiépítésre került az optikai körgyűrű hálózat Budapest területén, a Szolgáltatónál. Továbbá két új Cisco router került elhelyezésre. Ezen fejlesztések a felhasználó számára láthatatlanok de a biztonság érdekében elengedhetetlenek.

A tervezet további pontjainak megvalósítása a tervezett árkalkulációk szerint:

- A megyei kirendeltségek routereinek ára összesen 362816 \$
- Az 1-es objektum konfigurációjának ára összesen 439319\$
- Összesen 894073\$
- Menedzsment modulok összesen:66693\$
- Az 1-es objektum helyi hálózatának ára összesen: 1090170\$

A fejlesztés költségességét tekintve a későbbi fejlesztések kezdetének időpontja a pénzügyi források meglététől fog függeni.

Irodalomjegyzék

- [1] CISCO Systems hálózat fejlesztési konfiguráció ajánlata 2003.
- [2] Bogár Tamás r. alezredes ORFK GF ITFO Főosztályvezető
- [3] Tanka László r. őrnagy ORFK GF ITFO munkatársa
- [4] Zsidkovszky Sándor r. fhdgy. ORFK GF ITFO munkatársa
- [5] Az Egységes E-közigazgatási Politika előkészítésére készített II. tanulmány a Megyei Jogú Városok Szövetsége és az Informatikai és Hírközlési Minisztérium együttműködésében 2002.
- [6] Pándi Erik őrnagy: ORFK Híradástechnikai Szolgálat; kiemelt főelőadó ;
- [7] Fekete Károly: A Magyar Honvédség állandó telepítésű kommunikációs rendszere továbbfejlesztésének technikai lehetőségei, doktori (PhD) értekezés 2003., Zrínyi Miklós Nemzetvédelmi Egyetem.

**NEW POSSIBILITIES IN THE FIELD OF WAN-WLAN
MILITARY COMMUNICATIONS**

Zrínyi Miklós National Defense University
Department of Information System Management
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 a short description of the recent broadband wireless access WiMAX with regard to improving the infrastructure of the military communications networks (MCN). The candidate solution within the MCN is constructed from a variety of wireless local area network (WLAN) technologies. This paper describes those new and relevant technologies which will have to address interoperability, technological compatibility, flexibility of use, legacy bandwidth, data transport in NATO Network Enabled Capability (NNEC) environment. Few years ago the most popular modulation methods in hungarian MCN were TDM and even analogue procedure but we may pay attention to more powerfull solutions as the CDMA and OFDM defined by IEEE 802.11b-g or 802.16-20 standards.

Introduction

For the past few years, the Department of Information System Management of Zrínyi Miklós National Defense University has been focused on advantages of the powerful wireless access technologies as implementation of OFDM waveform. The main aim was set to found the new solutions of new military communication infrastructure in areas of tactical and operational communications networks. The legacy technologies as analogue and time-division multiplexing modulation methods are assimilated into the MCN but such a new applications as the fast and massive mobile data and video transmission with special regard to NATO Network Enabled Capability (NNEC) environment from network centric warfare¹⁵ (NCW) are compose the bandwidth bottlenecks. During the interim period, military network operators will need to provide solutions that will improve by offering increased mobility, bandwidth and more solid COMSEC and COMPUSEC level.

The MCN and mobile and secure bandwidth hungry military communications applications are suppose:

- flexible 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;

¹⁵ 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 –77.)

- real-time surveillance, for immediate assessment and response to actual events even in rapid changing situation.

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

Aim of the WiMAX

The IEEE 802.16a standard, amended in January 2004 by the IEEE to cover frequency bands in the most popular and wide used range between 2 GHz and 11 GHz, specifies a bigger than local area network (LAN) protocol.

This wireless metropolitan size LAN (MAN) may enable a high speed wireless technologies alternatives for traditional cable, TDM microwave or E1 level military communications services. The main power of the IEEE 802.16 based solution we can find as in backhaul for personal LAN – body LAN (PLAN – BLAN) wireless applications namely Bluetooth and 802.11 protocol and as for last kilometers broadband access (Fig. 1).

Global Wireless Standards

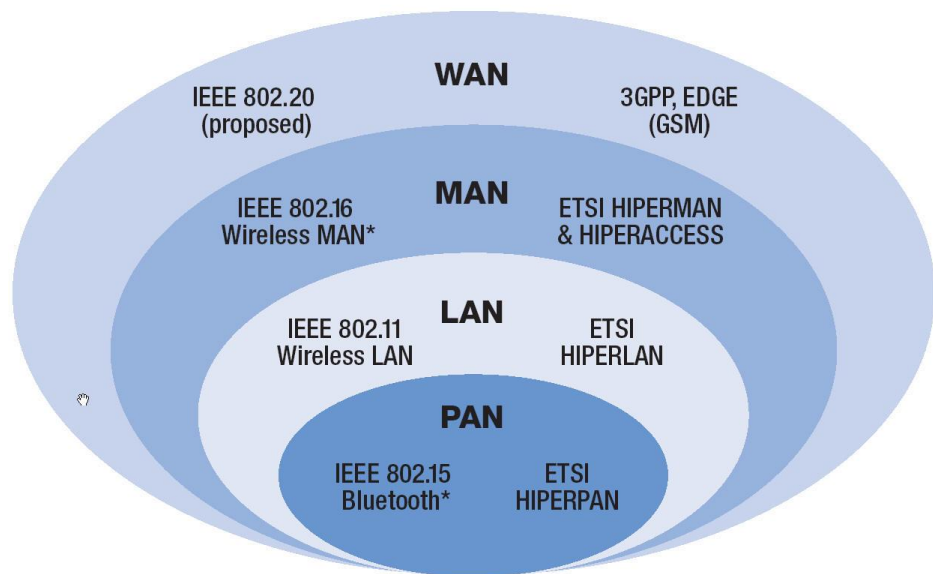


Fig. 1 The wireless standards by own sizes

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. 25-30 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 evolution¹⁶ 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 forces.

The IEEE 802.16 standard based on the orthogonal frequency division multiplexing (OFDM) method. The OFDM we may apply in the 4G wireless military Internet or Intranet solutions. The WiMAX is a higher performing version of WiFi and simpler and much more cost effective alternate to competing wireless technologies such as wideband CDMA. As we know the evolution process was the AMPS – 1G, GSM – 2G, CDMA and EDGE – 2.5 G, UMTS – 3G and now the OFDM based WiMAX – 4G. WiMAX is the abbreviation of the Worldwide Interoperability for Microwave Access and is the next step on the road to a wireless military communications, extending broadband wireless access to the new locations and to the rapid deploying Military headquarters and forces and over longer distances.

WiMAX promises a wireless access range of up to 50 kilometers, compared with IEEE 802.11b-g 100 meters max. and Bluetooth 10 meters. While WiMAX is the new shorthand term for IEEE Standard 802.16, also known as Air Interface for Fixed Broadband Wireless Access Systems. The 802.16a extension does not require line-of-sight transmission and it boasts a 70 Mbit/s data transfer rates. Consequently the WiMAX can support hundreds and even thousands of military subscribers and the 802.16 standards are cover:

- 802.16b – Quality of services (QoS);
- 802.16c – Interoperability;
- 802.16e – Support for mobile as well as fixed broadband.

Beyond these advantages of the 802.16 protocols the Weimax we can apply as a backbone of base stations of hungarian strategic military communications networks connected to the tactical or mobile military networks or to the public wired or wireless networks.

Each WiMAX base station can supports hundreds of fixed military subscriber stations which can be WiFi hot-spots in HQ and firewalled military datacommunication networks.

The IEEE 802.16 protocol based base stations we can use as the Media Access Control (MAC) ISO-OSI layer as a common interface. This MAC layer can easy makes the military communications networks interoperable. The MAC layer may allocate uplink and downlink bandwidth to military users according to their needs even on an essentially real-time basis.

The benefits of the WiMAX MAC layer protocol are:

- support for adaptive modulation, which is enables highest data rates;
- security and encryption (Triple DES – 3DES), which is protects military user privacy;
- Scalable 1 to hundreds of military users, allows cost effective deployments;

¹⁶ 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.

- TDM/TDMA Scheduled uplink and downlink frames for purpose of efficient bandwidth usage;
- Low latency for delay sensitive military communications services (TDM, Voice, VoIP) with QoS.

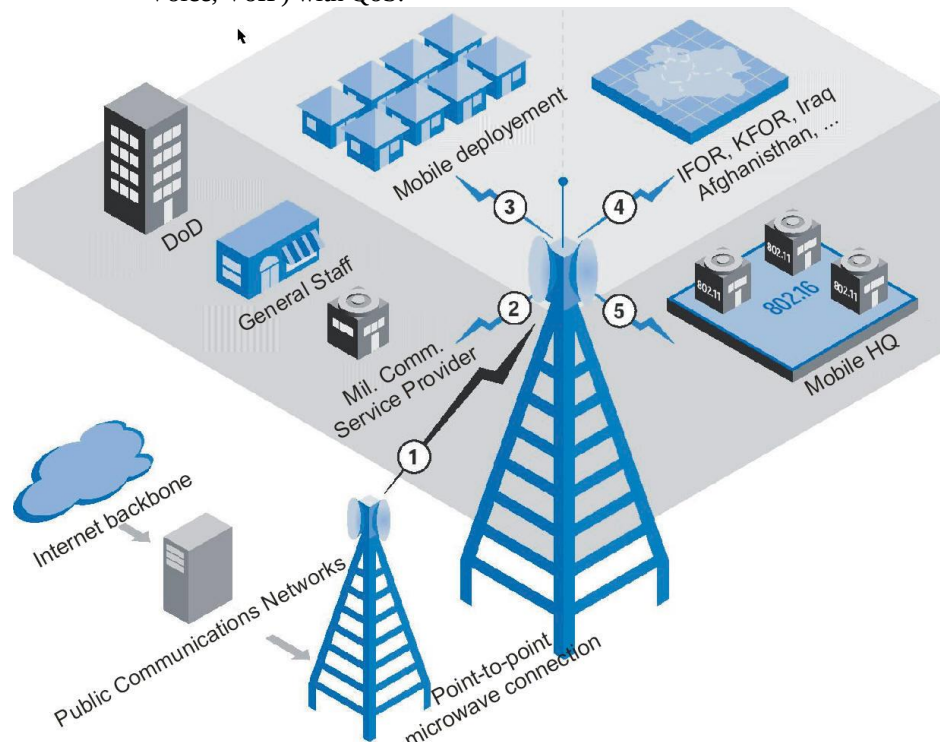


Fig. 2. The alternatives of WiMAX in global military communications

The positive sides of the physical layer of the IEEE 802.16a protocol are:

- flexible Channel sizes (e.g. 2 MHz, 5 MHz, 10 MHz, etc.), provides the flexibility necessary to operate in many different frequency bands and channel requirements;
- TDD and FDD duplexing support;
- Adaptive Modulation and variable error correction, ensures a robust RF link while maximizing the data transmission speed for each military users;
- 256 point FFT OFDM waveform for addressing in outdoor military Line-of-Sight (LOS) environments.

Conclusions

WiMAX protocol offers the most efficient characteristics with special regard to military applications. They are cellular backhaul, broadband on demand, QoS, security, interoperability, throughput and scalability. Consequently the high-speed wireless broadband technology based on the IEEE 802.16a-e promises to opportunity for military communications service-providers. The precisely defined modern characteristics will help fill the high-speed broadband coverage gaps between possibilities of the nowadays hungarian MCN.

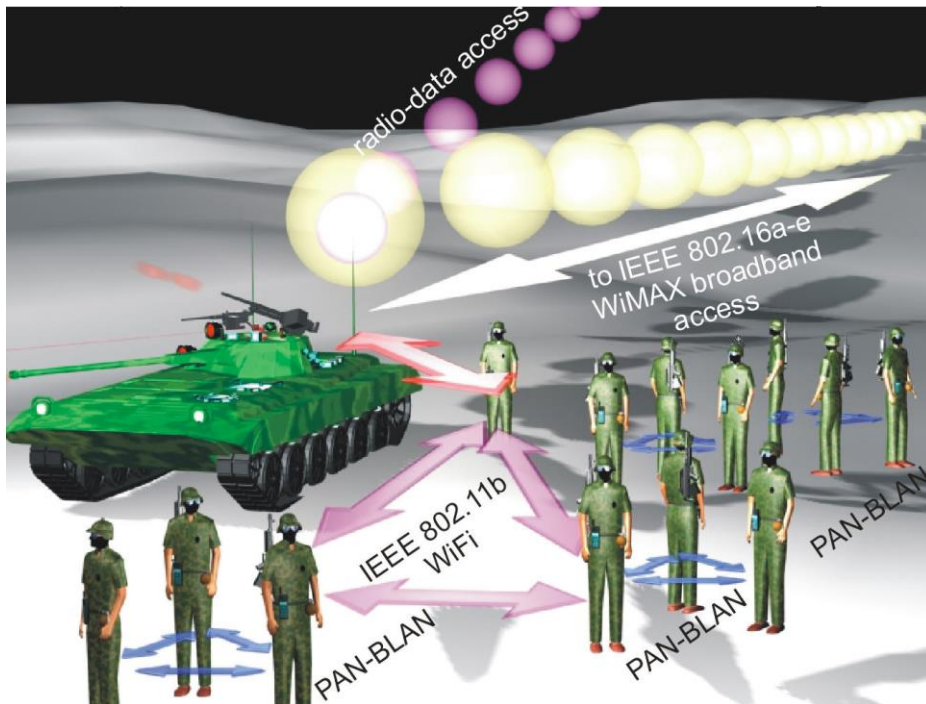


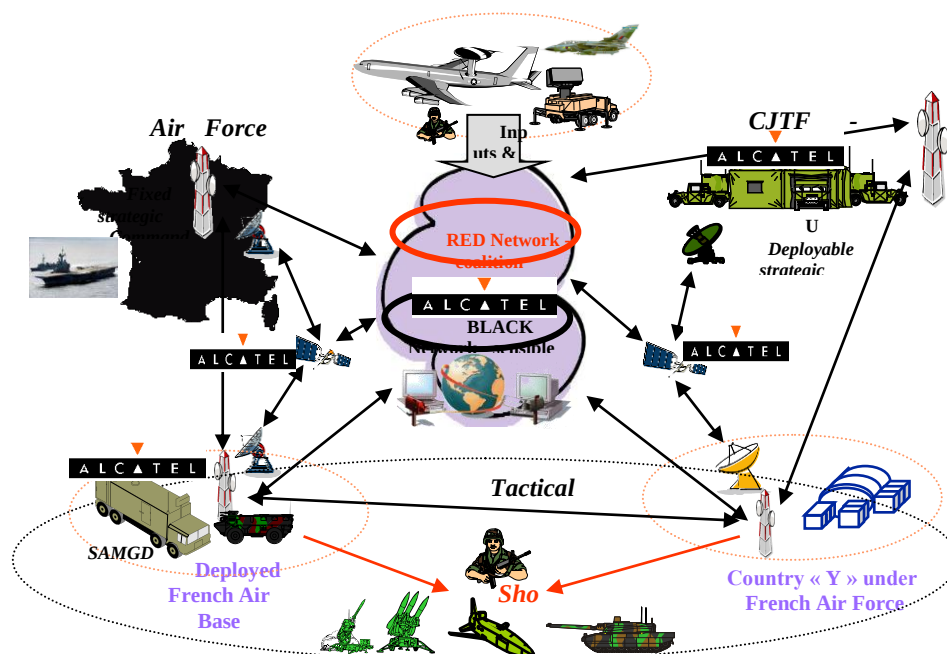
Fig. 3. PLAN-BLAN, WiFi and WiMAX in military communications network

References

- [15] IEEE 802.16* and WiMAX, Broadband access for everyone, White Paper Broadband Wireless Access, Intel Corporation, 2003.
- [16] www.wimaxforum.org
- [17] www.ieee802.org/16
- [18] IEEE 802.16 Broadband Wireless Access Group: Channel Models for Fixed Wireless Applications, July 2001.
- [19] D. G. Michelson, V. Erceg and L. J. Greenstein: Modeling Diversity Reception Over Narrowband Fixed Wireless Channels, in MTT-S Symp. on Tech. for Wireless Applic., 1999, pp. 95-100.
- [20] Shyamal Ramachandran, Charles W. Bostian, Scott F. Midkiff: Performance Evaluation of IEEE 802.16 for Broadband Wireless Access, Center for Wireless Telecommunications, Virginia Tech, Blacksburg, Virginia.
- [21] IEEE 802.16-2001, „IEEE Standard for Local and Metropolitan Area Networks – Part 16: Air Interface for Fixed Broadband Wireless Access Systems”, April 2002.
- [22] T. J. Eshler: Adaptive Protocols to improve TCP/IP Performance in an LMDS Network Using a Broadband Channel Sounder, M.S. Thesis, Virginia Polytechnic Institute and State University, April 2002.
- [23] Antony Klinkert: IEEE 802.16e requirements from an operator’s perspective, IEEE 802.16 presentation Submission Template (Rev. 8.3), WorldCom 6828 Collonade Drive, Plano, Texas 75024, Info@Klinkert.net, March 2003.



Az Alcatel jelenléte a JWID 2004 programban



Alcatel Hungary Kft.

1116 Budapest, [Kondorfa u. 10.](http://www.kondorfa.u.10)
Telefon: (1) 2099500 Telefax: (1) 2099599
www.alcatel.hu
alcatelh@alcatel.hu

ÖSSZHADERŐNEMI STRATÉGIAI SZEMLÉLET A FRANCIA HADERŐBEN

Napjaink törzstisztjeinek tevékenysége jelentősen befolyásolja az alegységek, csapatok tevékenységét és annak sikerét. A jól képzett törzstisztek jó helyzetmegítélő képességgel, széleskörű összefegyvernemi, beosztástól függően összhaderőnemi ismeretekkel rendelkeznek, képesek az ellenség és a saját csapatok helyzetének, a terep, az időjárás és a környezet (társadalmi, politikai, stb.) gyors értékelésére, valamint a parancsnok elhatározásának, döntéseinek megalapozására, adatokkal és cselekvési változatokkal történő alátámasztására. Ismereteinek megszerzése egyéni tanulásokon, parancsnoki- és törzsfoglalkozásokon, valamint iskolarendszerű képzés keretében valósul meg.

A Magyar Honvédség alakulatainál, törzseinél a végrehajtandó feladatok semmiben nem különböznek a nyugat-európai hadseregekben végrehajtandóktól, hiszen törzsei NATO-elvek alapján szervezettek, a parancsnoki és törzsmunka terén kompatibilitási képességeinket elértük, melyet a multinacionális környezetben végrehajtott gyakorlatok – magyar alegységek részvételével – és a nemzetközi keretekben szolgáló alegységekkel jól bizonyítottak.

Az Összhaderőnemi Védelmi Kollégium

Az összhaderőnemi szemlélet azonban, mint globális hadművészeti tendencia a nyugat-európai tisztképzésben és a gyakorlati életben már erőteljesen jelentkezik. Napjainkra a fegyveres konfliktusok jellege megváltozott. A tömeghadseregek széles arcvonalon, nagy mélységben végrehajtott bonyolult hadműveleteinek ideje lejárt. A fegyveres erők tevékenysége az alacsony intenzitású konfliktusok irányába mozdult el. Ugyanakkor a fegyveres konfliktusban résztvevő erők nagysága csökkent megnövekedett technológiai fejlettségű fegyverekkel, fegyverrendszerekkel. Folyamatosan csökkent a kizárólag egy haderőnem által végrehajtott hadműveletek jellege, napjaink katonai műveleti összhaderőnemivé váltak, amiben több haderőnem együttesen vesz részt. Ez vezetett el az összhaderőnemi szemlélet megerősödéséhez.

Az összhaderőnemi szemlélet kialakulásának folyamata

Az első világháborúban az összhaderőnemi műveleteket állami, katonapolitikai szinten hangolták össze, míg a második világháborúban az összhaderőnemi hadműveletek egy szinttel lejjebb, a védelmi minisztériumok, egyesített vezérkarok szintjére kerültek. Az ilyen hadműveletek megtervezésére a szövetségesek közös tervezőcsoportot, majd ennek bázisán a végrehajtás irányítására közös parancsnokságot állítottak fel. Ezen parancsnokságok alárendeltségébe rendszerint több szárazföldi hadsereg és légiflotta tartozott.

A második világháborút követő időszakban a haderőnemek együttműködése számos példát szolgáltatott a közös hadműveleti-harcászati szintű tervezésre és végrehajtásra (lásd: arab-izraeli háborúk, vietnami háború, Öböl-háborúk).

Napjainkra az összhaderőnemi tervezés és végrehajtás - a konfliktusba bevont fegyveres erők nagyságának csökkenése, technológiai fejlettségük, illetve a leküzdeni kívánt távolságok miatt - tartósan gyökeret vert harcászati szinten is.

Mindez óhatatlanul megnövelte a parancsnokságoknak és törzseknek az összhaderőnemi hadműveletekben jártas tisztek iránti igényét, amely értelemszerűen maga után vonta az összhaderőnemi tisztképzés fellendülését a nyugati országok katonai felsőoktatásában. Ennek egyik kiemelkedő példáját szeretném bemutatni tanulmányomban, konkrétan a francia összhaderőnemi képzést. Ennek fő oka, hogy három hónap időtartamban ennek az intézménynek a hallgatója voltam, ahol lehetőségem nyílt megismerni többek között a legfelső szintű tisztképzés logikáját, valamint a hadászati szintű döntéshozatali rendszer NATO-hoz adaptált metódusát is.

Ez az iskola, a CID¹⁷, egyike azon európai országoknak, ahol elsőként valósították meg az összhaderőnemi képzési formát. Ugyanakkor el kell ismerni azt is, hogy - bár a NATO katonai szervezetétől való sajátos elhatárolódás a fegyveres erők képzésében a legutóbbi időkig is érvényesült - a közös szövetségi műveletekben (NATO, EU, EBESZ, stb.) mint résztvevő ország, minden szinten igazodik a NATO struktúrákhoz, metódusokhoz.

A francia összhaderőnemi képzés fellelőjére a Párizsban található Összhaderőnemi Védelmi Kollégium (CID), mely 1993. januárjában kezdte meg működését, magába olvasztva minden olyan törzstiszti iskolát, amely a haderőnemek főtisztjeinek haderőnemi képzését végezte. Innen ered az iskola azon sajátossága is, hogy az összhaderőnemi képzés erős volta mellett a haderőnemi ismeretek további elmélyítését is az összhaderőnemi tanintézet keretein belül folytatják tovább.

A képzési forma főbb tartalmi súlypontját az összhaderőnemi hadművelati képzés (az oktatott tananyag 50%-a) alkotja, majd fajsúlyát tekintve a menedzsment és tevékenységi technikák (20%), a geopolitikai és hadászati képzés (20%) adják a legnagyobb részét az oktatott tananyagnak. A tanév során ezen felül még a haderőnemi ismeretek (5%), és az egyéni tudományos kutatómunka (5%) is szerepel az iskola képzési kínálatában.

Az összhaderőnemi hadművelati képzés a haderőnemek és a jelentősebb külföldi hadseregek megismerésén, a különféle hadszínterek és konkrét hadművelati helyzetek - nemzeti, szövetséges, illetve nemzetközi - gyakorlatok kereteiben történő tanulmányozásán keresztül valósul meg. A képzés alapvető formája az összevont előadás, melyek a központi amfiteátrumban folynak, majd ezeket követik a csoportos foglalkozások. A menedzsment és tevékenységi módszerek a legáltalánosabban használt csoportmunka-metódusokon, az analízis és a szintézis technikáinak megismerésén, továbbá a francia haderők által a stratégiai, hadászati-hadművelati szinten használt döntéshozatali rendszer, a MARS rendszer¹⁸ elsajátításán alapulnak.

A képzés kiemelt részét alkotja a kommunikációs problémák megoldása és a médiával való együttműködés elsajátítása is.

A geopolitikai és hadászati képzés kiemelt célja, hogy olyan geopolitikai és stratégiai ismereteket nyújtson a hallgatók részére, amelyek biztosítják a védelmi szféra környezetének és a katonai műveletek hatásának minél teljesebb körű elemzését. A tananyagrészt oktatásának másik kiemelt célja, hogy széles körű globális ismereteket nyújtson az államközi kapcsolatok, a világgazdaság és a nemzetközi együttműködés kérdéskörében is. A tananyagrészt fontosságát jelzi, hogy a hallgatók számára az isko-

¹⁷ CID = Collège Interarmées de Défense: Összhaderőnemi Védelmi Kollégium

¹⁸ Méthode interarmées d'Appréciation et de Raisonnement sur une Situation Militaire = katonai helyzetmegítélés és döntéshozatal összhaderőnemi módszere

laév során kötelezően elkészítendő szakdolgozaton kívül két fő „mérési pont”-ként szerepel egy-egy tanulmány elkészítése (az egyik geopolitikából, a másik pedig hadászatból). A képzés során törekednek a hallgatók önálló gondolkodásmódjának, véleményalkotásának elmélyítésére, így a már említett két tanulmány is ennek keretében készül. A hallgatók 6-8 témakört kapnak a foglalkozás kezdetén, és a rendelkezésükre álló három óra alatt kell elektronikus formában prezentálni egy választott témakörből egyéni véleményalkotásukat.

A képzés módja tehát előadásokon és egyéni kutatótevékenységen alapul, melyhez az év végén végrehajtott tanulmányút szervesen kapcsolódik.

Az összhaderőnemi képzés francia példája főként francia nyelvterületen (elsősorban Európában és kisebb mértékben Észak-Afrikában) terjedt el, ugyanakkor számos elemét hasznosították a brit összhaderőnemi képzés beindításához is.

Franciaország, de különösen a hadsereg nagyon hagyománytisztelő, a változásokra nehezen hajló. Ugyanakkor a szükség és a kényszer gyakran arra ösztökéli a döntéshozókat, hogy szakítsanak a hagyományokkal és a kor kihívásainak megfelelő, rugalmas képzési rendszert alakítsanak ki a katonatisztek felkészítésében; az egyéni érdekeket erősítve a hadsereg érdekeivel megteremtsék a helyzetekhez gyorsan és rugalmasan alkalmazkodó, modern összhaderőnemi gondolkodású tiszti modellt. Az iskola a párizsi Katonai Akadémia, vagy ahogy ott mindenki ismeri, az Ecole Militaire a város egyik legfrekvenciáltabb helyén, az Eiffel-torony lábánál elhelyezkedő Mars mezőn található. Az épületegyüttes már megjelenésében is tekintélyt és hagyományt sugall; épületeit XV. Lajos uralkodása alatt építették, falai közt tanult majd dolgozott többek között Bonaparte Napóleon is, melyre a francia katonák különösen büszkék.

A gyakorlati élet - legkirívóbban az Öböl-háború tapasztalatai - követelményeket szabott a tisztek törzsbeli alkalmazásával szemben. Nyilvánvalóvá vált a katonai felsővezetés számára, hogy az addig önállóan létező fegyvernemi illetve haderőnemi képzéseket integrálni kell, megteremtve az összefegyvernemi, összhaderőnemi jellegű is megőrző új felsőfokú képzési formákat.

A Felsőfokú Törzstiszti Tanfolyam

A Felsőfokú Törzstiszti Tanfolyam a szárazföldi haderő tisztjeinek legmagasabb szintű összefegyvernemi képzést nyújtó 5 hónapos iskolája. Feladata egyrészt az összefegyvernemi vezetés (mint megrendelő) hadművelési igényeinek való megfelelés, másrészt előkészíteni a tiszteket a felsőfokú katonai képzés következő szintjének való megfelelésre az Összhaderőnemi Védelmi Kollégium (CID) keretében. A tanfolyam legfontosabb célkitűzése, hogy a magas fegyvernemi ismeretszinttel rendelkező tisztek képesek legyenek többek között más haderőnem tisztjeivel együtt a hadműveletek vezetéséhez szükséges döntések megalapozása mellett doktrína-kidolgozási eljárások alkalmazására is. A cél tehát nem kisebb, mint hogy a törzstisztek képesek legyenek más haderőnemmel történő együttműködés megvalósítására, tevékenységek vezetésére és irányítására.

Rugalmas és hatékony pedagógia – a metódus

A képzés során meghatározott feladatok teljesítése során az egyéni érdekek és tevékenységek meghatározóak, ezért az oktatási módszerek is ennek megfelelően adaptáltak. A hallgatók aktív részvétele a katonai gondolkodásmód fejlesztése, a szakmai kompetenciák megerősítése előtérbe kerül. Természetesen nem hanyagolható el a katonai intelligencia tökéletesítése, melyet korunk háborús kihívásainak kiértékelésé-

vel, a nemzetközi környezet elemzésével igyekeznek minél magasabb szintre emelni. Tapasztalataim azt mutatják, hogy a fiatalabb katonatisztek is részletesen ismerik az európai országok politikai-gazdasági helyzetét, az európai és más kontinenseken folyó helyi válságok kialakulásának körülményeit, bátran ismertetik véleményüket nagy nyilvánosság előtt is, magabiztosan nyilatkoznak társadalmi-politikai kérdésekben. Ez persze nem nélkülözheti a széleskörű, többségében háborús tapasztalatokkal rendelkező tanári állományt éppúgy, mint a legkorszerűbb oktatástechnikai eszközöket.

A képzés hatékonyságát elsősorban nem az írott tananyag kiadásával fokozzák, hanem magas színvonalú informatikai háttér biztosításával juttatják el a hallgatókhoz a tananyagot, a felhasználható irodalmat hordozható személyi számítógépek útján. Minden hallgató az iskolára érkezve megkapja a tanfolyam alatt használható Notebook-ját, hálózati hozzáféréshez szükséges kódját, jelszavát. A tantermek már első pillanatra sem az „iskolai” jelleget sugározzák, hanem az „U” alakban elhelyezett asztalok mögött ülő hallgatókat önálló gondolkodás után egyéni véleményalkotásra ösztönzik; a hangsúlyt nem a „katonás jelentésekre” helyezik, hanem a minél megalapozottabb, érvekkel alátámasztott vitákat helyezik előtérbe. Első bepillantásra feltűnő az informatikai hálózat „pókháló” jellege. A Notebook-ok mellé minden hallgató megfelelő hosszúságú hálózati kábelt kap, melyet a tanterem közepén a földre letett Hub¹⁹-ba, számítógép hálózati elosztóba csatlakoztat. Az informatikai háttér az oktatáshoz szükséges dokumentációs anyagok, jegyzetek, előadás-vázlatok eljuttatását, egyéni felhasználáshoz azok lementését biztosítja és lehetővé teszi az igények szerinti szelektált információáramlást.

Elmélet és gyakorlat

Az informatikai hálózat korszerű lehetőségeit nagymértékben felhasználják a számítógéppel támogatott feladatok, gyakorlatok során mind az előkészítés, mind a végrehajtás és értékelés fázisaiban, a parancskidolgozás, a hadművelleti üzenetküldő rendszer és a térképészeti adatok továbbításánál éppúgy, mint a Kutatási és Doktrínális Központ szakértőivel folytatott konferenciabeszélgetéseknél.

A szimulációs eszközök és rendszerek szintén fontos elemei a hadművelleti tanulmányok gyakorlatban történő elsajátításának, amelyet külön e célra kialakított néhány fős központ segít. A Szárazföldi Hadművelleti és Szimulációs Kutatóközpont által kifejlesztett döntés-előkészítő informatikai segédeszközök lehetővé teszik a hallgatók számára a pontos tervezőmunkát, a cselekvési változatok szimulálását, a hadművelleti feladat, vagy egyes aspektusainak elmélyült elemzését. Az ugyancsak térinformatikai alapú döntés-előkészítési és parancstovábbítási rendszer – a SICF²⁰ – a Nemzetvédelmi Egyetemen is már több alkalommal bemutatásra került a Katonai Kommunikációs Rendszerszervező Tanszék szervezésében. Ugyanakkor már a tanfolyam keretében nagy hangsúlyt fordítanak a NATO-ban elfogadott és meghonosított „Formázott katonai üzenetkezelő rendszer” működtetésére. E rendszeren keresztül történik minden információáramlás az alárendelt törzsek és az előljáró szervek, valamint az együttműködésre rendelt csapatok törzsei között.

Megállapítható tehát, hogy az oktatás hagyományos előadásokon alapuló jellegét háttérbe szorították, az alapvető ismereteket összevont előadások formájában megtart-

¹⁹ Számítógépes hálózatok elosztó egységei

²⁰ Système d'information et de commandement des forces

ják ugyan, de a gyakorlati alkalmazásokat, szemináriumokat kiscsoportos foglalkozások keretében hajtják végre. Ez alapvetően nem is tér el az egyetemen folyó képzéstől. A különbség a hallgatók egyéni érdekeltségében és az egyéni elgondolás, vélemény kinyilvánításában van. A kiscsoportos foglalkozásokon a megválaszolandó kérdéseket a hallgatók E-mailben kapják meg, amire másfél-két óra időtartamban, írásban kell válaszolni, gondolataikat kifejezni. A kifejtett nézeteiket szintén E-mailben küldik vissza az oktatónak, aki értékeli azokat, összeveti, és a sarkalatos pontokat vélemény-ütköztetésre a csoport elé viszi. Mindenki véleményt alkot a kérdésről, de nem azért, mert „kötelező” felszólalni, hanem mert a hallgatóknak megalapozott véleményük kell, hogy legyen. Nem szégyen rosszat mondani, ha az egyén azt képes alátámasztottan megvédeni! A gyakorlatok végrehajtásánál sincsenek kidolgozott tervek, az operátorok a hallgatók utasításainak megfelelően dolgoznak, a „hadművelet” lefolyásának nincs előre kidolgozott változata. Amennyiben a hallgatók képesek megvédeni a kialakított elgondolást, a tanárok hagyják szabadon dolgozni őket. A térkép alapú munka is már csak úgy jelentkezik, hogy törzsenként egy-egy térképet használnak a csoportok, de alapvetően nem a kialakult helyzet és a hadművelet lefolyásának ábrázolására, hanem a szükséges adatok „levételére”, áttekintő térképként történő alkalmazásra használják.

Az elméleti órákon megalapozott ismeretek feldolgozása, alkalmazása az említett informatikai rendszerek által támogatott gyakorlatokon realizálódik. De ezzel a gyakorlati képzés nem fejeződik be! A csapatoknál tett látogatások nagy hangsúlyt kapnak, ahol a hallgatók elsődlegesen nem az adott kötelék gondjairól, problémáiról hallhatnak tájékoztatót, hanem a tanfolyamon hallottakat és a gyakorlat során tapasztaltakat kérdezhetik meg a tapasztalt parancsnokoktól, akik képesek nagyon precíz, kielégítő válaszokat kapni, hiszen ők is a látogatás előtt felkészülnek a hallgatók fogadására. Egy-egy ilyen látogatás az alakulatok részére nem megterhelést, hanem megbecsülést jelent, a parancsnokok is ez alapján készülnek fel a hallgatók fogadására. Ezek a látogatások elősegítik a reflexiót, a személyes eszmecserét, valamint a doktrínakomponensek csapatoknál történő szembesítését. Így tehát a kialakított képzésben a gyakorlati foglalkozások túlsúlya sokkal konzekvensebb egyéni teoretikus munkát igényel hallgatói részről, melyet minden esetben meg kell előznie a gyakorlati látogatásokat, hiszen ez által kívánják elérni a maximális hatékonyságot.

Tanulmányi struktúra

A Felsőfokú Törzstiszti Tanfolyam tanulmányi struktúráját is a képzés előre meghatározott végcéljai teljesítésének megfelelően alakították ki. A rendszer három alappilléren áll.

1.) Parancsnoki rendszerek

A képzés e részének célja, hogy a hallgatók megismerjék a hadműveleti törzsek felépítését, funkcionális összetételét és a nagyon pontosan behatárolt feladat-rendszerét. Az első fázis végére nem lehet olyan hallgató, aki nem ismeri a funkcionális működést, és ne lenne képes egy adott törzsön belül bármilyen törzstiszti feladat ellátására. Az első fázisban megismerik továbbá a parancsnokságok szervezeti struktúráját, a törzsek hadműveleti helyzetben történő széttelepülésének rendjét, a vezetési pontok szervezetét, összetételét, és különösen az információtovábbítást és a döntési mechanizmust. A törzslátogatások, csapatszintű gyakorlatokon való részvétel egészíti ki a doktrínális képzést, kialakítva ezzel

egyfajta kritikai szemléletet a hallgatókban a doktrínális kérdések és a gyakorlati megvalósítás között. Ez a metódus nagyon fontos eleme a parancsnoki szemlélet további fejlesztésének.

2.) Az összefegyvernemi hadműveleti eljárások

Az iskola kiemelt figyelmet fordít a csapatok hadműveleti alkalmazásának lehetséges módozataira, vagyis a hely és szerep meghatározására a had(harc)rendben. Nem csak a „megszokott” elveket ismerik itt meg a hallgatók, hanem gyakorlati példákon keresztül megismerhetik a kombinált és koherens alkalmazásokat, elsajátítják azok főbb jellemzőit, előnyeit és hátrányait, melyek későbbiekben az összefegyvernemi alakulatok számára biztosíthatják a sikeres feladat-végrehajtást. A hagyományos harcászati és hadműveleti szintű feladatok mellett igyekeznek a képzésbe integrálni a modern kor kihívásait is a hallgatók gondolkodásmódjába, ezért az egyes hadműveleti terület minden aspektusát megismerik a terepértékeléstől a csapatok irányításával kapcsolatos összes nemzeti, multinacionális, CIMIC, politikai, jogi, pszichológiai és médiavonatkozású szempontokig.

3.) A szövetséges hadműveleti parancsnoki munka

A tanfolyamot elvégzett tisztnek feladataik ellátására nem csak saját hadseregükben kell készen lenniük, hanem a szövetséges erők multinacionális környezetében is. Ennek természetesen feltétele, hogy a hallgatók ismerjék meg a szövetséges erők parancsnoki-vezetési rendszerének sajátosságait, a többnemzetiségű összetett és speciális erők jellemzőit. Mindezek során az elsődleges cél az interoperabilitás elősegítése. Ennek erősítése érdekében a gyakorlatok egy részét „hazai környezetben”, de angol nyelven folytatják le. Nem kell persze azt hinn, hogy az iskolán minden francia tiszt felsőfokú angol nyelvismerettel rendelkezik, mert ez nem így van. Gyakran hibásan, de gazdag szókincsel, kommunikációképes nyelvtudással képesek a gyakorlatokat végrehajtani.

Az oktatásnak ebbe a fázisába több összekötő tiszt is bekapcsolódik, akik NATO-törzsekben dolgoznak, vagy dolgoztak, és képesek a szövetség vezetési-irányítási rendszerében eligazodni, ismereteket átadni.

Végezetül a tanfolyam során számos tanulmányutat szerveznek a hallgatóknak szövetséges vezetési pontokra, multinacionális erők parancsnokságaira, valamint megismertetik a hallgatókkal gyakorlatban is Európa több országának politikai, gazdasági, társadalmi rendszerét, valamint más országok katonai iskoláinak képzési rendszerét és metodikáját.

Mindezek az ismeretek nagyban segítik a törzstiszteket abban, hogy eligazodjanak a különböző szintű fegyveres és nem fegyveres küzdelmek politikai, gazdasági, társadalmi problémáiban; képesek legyenek megfelelni az összefegyvernemi és részeiben az összhaderőnemi követelményeknek. Alapvetően természetesen a követelmények egy nagy hadseregben lehetnek mások, mint a Magyar Honvédségben, azonban egyet figyelembe kell venni: Nyugat-Európában nem a szaktisztek képzésére helyeződik a hangsúly, hanem az összefegyvernemi és összhaderőnemi vezetési modell elmélyítése, a vezetési ismeretek elsajátítása és alkalmazása multinacionális, szövetségi és természetesen honi környezetben a cél.

Felhasznált irodalom:

- [1] Dossier d'enseignement (az Összhaderőnemi Védelmi Kollégium tematikai programja) Kiadvány, Collège Interarmées de Défense, Paris, 2003.
- [2] Dossier d'enseignement (a Felsőfokú Törzstiszti Tanfolyam tematikai programja) Kiadvány, Paris, 2002.

A DIGITALIZÁLT KATONA KOMMUNIKÁCIÓS ÉS INFORMÁCIÓS IGÉNYE

Bevezetés

Az afganisztáni és az iraki konfliktusok tapasztalatai rávilágítottak arra, hogy a sikeres katonai műveletek elengedhetetlen feltétele a legkorszerűbb technikai eszközök alkalmazása, és a valós idejű információ támogatás megléte.

Alkalmazkodva az új kihívásokhoz, a fejlett hadseregek modernizációs programjaiban fontos szerepet kap a hálózatközpontú hadviselés, amelynek kulcsfontosságú elemei a fejlett info-kommunikációs és informatikai eszközök. A hálózatközpontú hadviselés egyik meghatározó szegmense az önállóan feladatot végrehajtó digitalizált katona.

A fejlettebb hadseregek különböző projekteket hoztak létre, amelyek célja a katona digitalizálása²¹ és hálózatosítása²².

Néhány program ezek közül[2]:

- az angol „Future Integrated Soldier Technology²³ (FIST)”;
- a német „Infanterist der Zukunft²⁴ (IDZ)”;
- a kanadai „Soldier Information Requirements Technology Demonstration²⁵ (Sireq TD)”;
- az amerikai „Land Warrior ²⁶(LW) és az Objective Force Warrior⁴ (OFW)”.

A fejlesztések célja az, hogy a katonákat olyan eszközökkel lássák el, amelyek nagymértékben megnövelik a feladat végrehajtó és túlélési képességeiket. Ez csak úgy érhető el, ha a katona rendelkezik a legmodernebb, közvetlenül a tevékenységét támogató eszközökkel, és be van kapcsolva egy a tevékenységét közvetetten támogató, magasabb szintű rendszerbe (információs hálózatba).

A hálózatba kapcsolt digitalizált katona csak akkor tudja a feladatát sikeresen végrehajtani, ha képes valós idejű információkat gyűjteni, továbbítani és kapni, vagyis kommunikálni. Ebből is kitűnik, hogy **fejlett kommunikációs eszközök nélkül nem beszélhetünk digitalizált katonáról**.

Mindezeket figyelembe véve e cikkben a digitalizált katona kommunikációs és információs igénye, szükséglete kerül bemutatásra eszközrendszere tükrében.

²¹ A katona digitalizálásának folyamata nem más, mint a katona modern digitális eszközökkel való ellátása.

²² Ezen a kifejezésen a katona viselhető és hálózatba kötött mikro-számítógéppel történő felszerelését kell érteni.

²³ Future Integrated Soldier Technology = a jövő katonájának integrált technológiája

²⁴ Infanterist der Zukunft = a jövő gyalogos katonája

²⁵ Soldier Information Requirements Technology Demonstration = a katona információs technológiájának követelményei

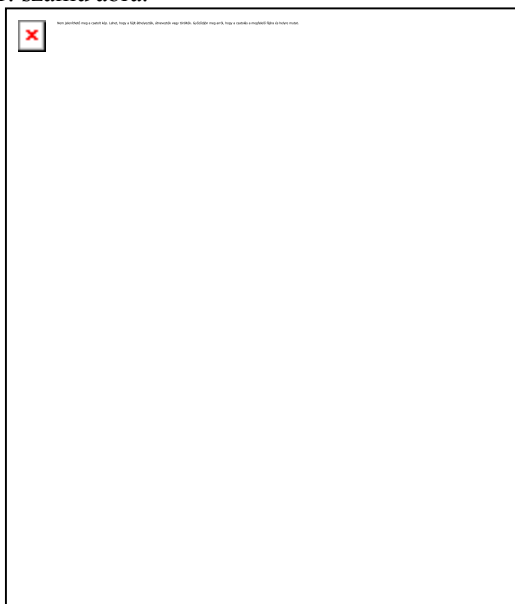
²⁶ Land Warrior = földi harcos, Objective Force Warrior = a célhaderő harcosa

A digitalizált katona kommunikációs rendszere

Mint ahogy az már a bevezetőben is említésre került, a digitalizált katonának szüksége van egy adatátviteli (kommunikációs) rendszerre, ami biztosítja számára a nélkülözhetetlen információkat. Ennek a rendszernek azonban nem csak a katona információs igényeit kell kielégítenie, hanem képesnek kell lennie a katonától érkező információk továbbítására is. Tehát a rendszernek mindenféleképpen kétirányú kommunikációs szükségletet kell kiszolgáltatnia²⁷. Igaz ez akkor is, amikor a katona:

- közvetlenül (pl.: rádión keresztül) a parancsnokával vagy a társaival tart fenn kapcsolatot;
- saját pilóta nélküli repülő eszközét vagy szárazföldi robotját irányítja, és ezzel párhuzamosan valós idejű információkat kap ezektől;
- a harctéri információs hálózathoz kapcsolódva információkat továbbít és kérdez le.

Fontos megemlíteni, hogy a digitalizált katona kommunikációs rendszere nem elszigetelt hálózat, hanem szerves részét képezi a hadszíntéri számítógépes hálózatnak. Ezt szemlélteti az 1. számú ábra.



1. ábra

A digitalizált katona helye a harctéri kommunikációs rendszerben[1]

A katona része a harctéri kommunikációs rendszernek, így biztosítják számára, hogy adatokat kapjon a hálózattól, vagy éppen szolgáltatson a hálózat részére.

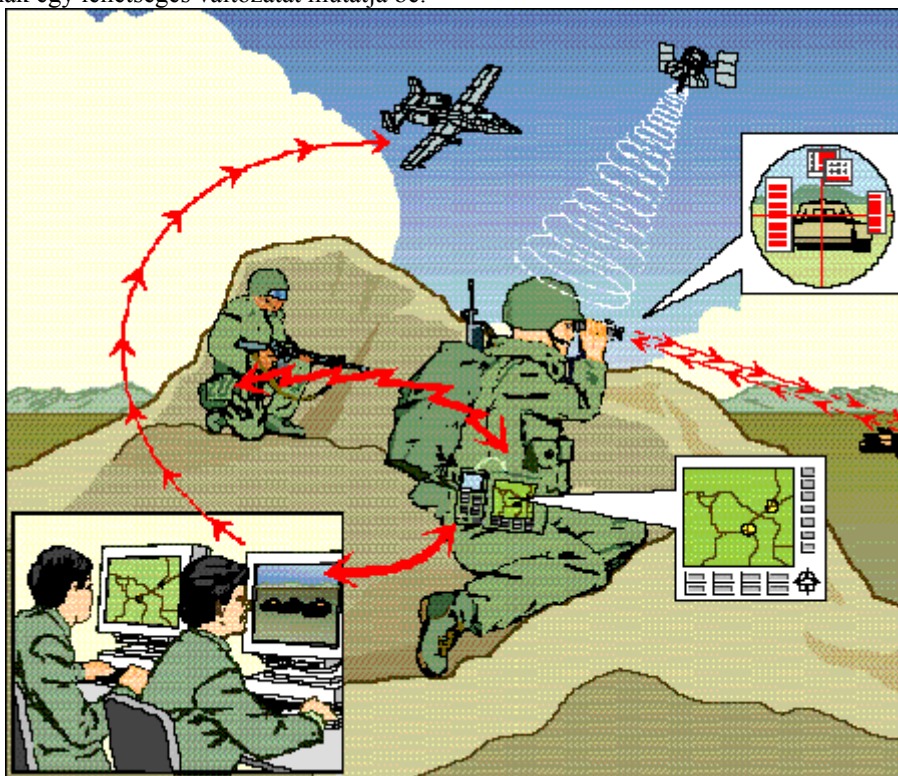
²⁷ Van olyan eszköze a katonának, amely vonatkozásában nem szükséges a kétirányú információáramlás megvalósítása. Példa erre a biológiai szenzor

Meg kell különböztetni két hálózati szintet a katona kommunikációjának vizsgálatakor. Az első szint a helyi hálózat szintje, amely a viselhető és hordozható digitalizált eszközök, érzékelők alrendszereinek hálózatát jelenti.

A másik szint a helyi hálózat bekapcsolódása a hadszíntéri számítógép hálózatba, hiszen így valósul meg a külső rendszerekkel²⁸ való kapcsolattartás.

Mindkét szinten kulcsfontosságú szerepet tölt be a katona egyéni számítógépe. Az első esetben a vezérlés, az információ feldolgozás és az eszközök működésének összehangolása, a második esetben a külső rendszerektől érkező és oda továbbított adatok (információk) kezelése kapja a fő szerepet.

A számítógép segítségével képessé válik a katona az általa szerzett felderítési adatokat a megfelelő helyekre továbbítani. A 2. ábra ennek az információs folyamatnak egy lehetséges változatát mutatja be.



2. ábra

A digitalizált katona felderítési adatainak továbbítása[2]

Amint az a fenti ábrán is jól látható: a felderítési adat különböző helyeken más-más formában jelenik meg. Hiszen csak így válhat értékelhető információvá. Ennek megfelelően más-más kommunikációs igényeik lesznek az egyes elemeknek. Például a katona kijelző panelén nem a harcjármű képe, hanem egy ezt szimuláló ikon jelenik

²⁸ Külső rendszerek lehetnek például: más katonák helyi hálózatai, vezetési pontok, műhol-dak.

meg. A csapásmérésre kijelölt repülőgépnél viszont csak a megsemmisítendő eszközök pontos koordinátáira van szüksége.

A digitalizált katonák bevethetőek szakasz vagy raj kötelékben, de képesek önálló feladat végrehajtásra is. Ezt azért fontos hangsúlyozni, mert mindhárom esetben különböző kommunikációs igények jelennek meg.

Önálló feladat végrehajtás esetén, a katona kommunikációs igénye a helyi hálózaton belüli eszközök közötti adatátvitelen kívül kiterjedhet a harcvezetési központtal és a harctéri információs rendszerrel történő kapcsolattartásra is.

A raj vagy szakasz kötelékben történő alkalmazás során a katona kommunikációs csatornáinak ki kell bővülnie a társakkal és a raj-, illetve szakaszparancsnokkal történő kétirányú kapcsolattartásra is. Ebben az esetben a katonának közvetlenül nem szükséges bekapcsolódnia a harctéri információs hálózatba, hiszen a parancsnokától megkapja a szükséges adatokat. Az általa küldött adatok eljuthatnak a parancsnok kommunikációs rendszerén keresztül a központi hálózatba, amennyiben erre szükség van.

Látni kell azt is, hogy a digitalizált katona egyes eszközeivel szemben eltérőek az adatátviteli igények. Ennek megfelelően tekintsük át a digitalizált katona eszközszerét.

A digitalizált katona eszközszerkezete

Az elektronizált felszerelések azokat az eszközcsoportokat tartalmazzák, amelyek nélkül a katona nem képes a kor színvonalának megfelelő, sikeres katonai műveletet végrehajtani.

A digitális katonának rendelkeznie kell az alábbi eszközökkel:

- speciális ruházat;
- nagy felbontású digitális térképadatbázissal ellátott GPS²⁹ vevő egység;
- helyzetjelentő egység;
- idegen-barát felismerő rendszer;
- nagy felbontású kép és megjelenítő egység;
- beszélő készlet;
- fényerősítő eszköz;
- nappali- és hő kamera;
- nagy teljesítményű, viselhető számítógép;
- nagy zavarvédetségű személyi rádió;
- védett kommunikációs csatorna;
- folyamatos kapcsolat a hálózattal (harctéri információs rendszerrel);
- egészségügyi állapotjelentő szenzorok³⁰;
- folyamatos áramellátást biztosító tápegység;
- hordozható szárazföldi és légi robot
- elektrooptikai eszközökkel ellátott speciális fegyver.

A digitalizált eszközszerkezet többek között alkalmassá teszi a katonát:

- valós (közel valós) idejű audiovizuális felderítési adatok megszerzésére a nap bármely szakaszában;

²⁹ GPS: Global Positioning System = globális helymeghatározó rendszer

³⁰ A szenzorok csoportjába sorolható minden érzékelő.

- ellenséges területek, objektumok felderítésére biztonságos távolságból;
- meghatározni a saját és társai, illetve az ellenséges erők vagy eszközök pillanatnyi helyzetét;
- audiovizuális információkat eljuttatni társainak és parancsnokának;
- audiovizuális információkat fogadni társaitól, parancsnokától vagy a hálózatra kapcsolt bármely más felderítési adatforrástól;
- kiemelt fontosságú célpontok megjelölésre, távkövetésre, célkoordinátáinak megadására;
- a pillanatnyi fizikai és egészségügyi állapotának folyamatos ellenőrzésére;
- sérülés (veszélyhelyzetbe kerülés) esetén automatikus segélykérés leadására;
- az általa nem beszélt nyelvek megértésére;
- vegyi és sugárszenyezettség detektálására.

A felszerelés-csomag –kommunikációs rendszere segítségével– hozzájuttatja a katonát a feladat sikeres végrehajtása szempontjából nélkülözhetetlen valós idejű információkhoz, és kibővíti érzékszerveinek korlátait. Mindezek mellett bekapcsolja őt egy, a tevékenységét közvetett módon támogató hálózatokon alapuló hálózatba. A katona így szerves részét tudja képezni a digitális hadszíntérnek, és a rajta folyó hálózatközpontú hadviselésnek.

A digitalizált katona eszközeivel szemben támasztott kommunikációs igények

A **speciális ruházatnak** biztosítani kell a katona számára vizuális és infravörös felderítéssel szembeni védelmet; a megváltozott külső körülmények függvényében hőmérsékletszabályozást, mintázat és színváltozást; biológiai, vegyi hatások elleni védelmet; a fontosabb szerveinek lövedék elleni védelmét. Részeit képezi többek között az integrált sisak, a lövedékálló málhamellény, az elhajlás érzékelőkkel ellátott kesztyű, az energiaellátó bakancs.



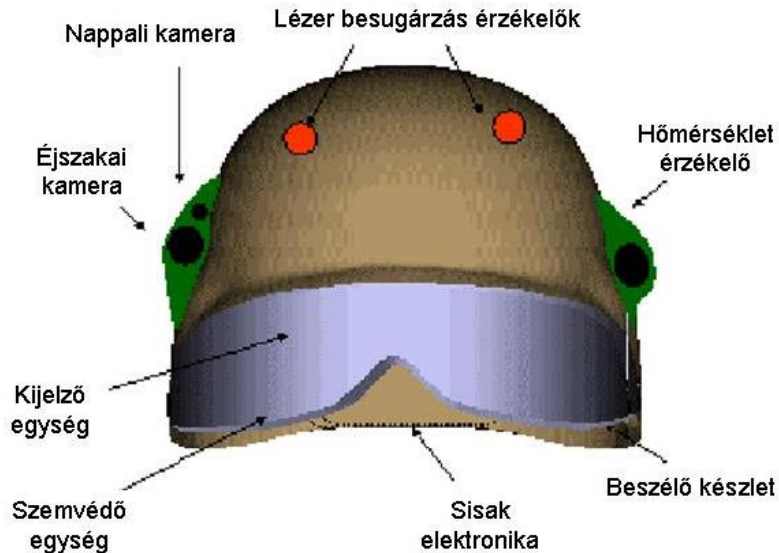
3. ábra

Mindezekon túl olyan kialakításúnak kell lennie, hogy elhelyezhetőek legyenek rajta és a katona testfelületén a helyi kommunikációs hálózat eszközei, továbbá az ezeket összekötő kábelek.

A helyi hálózat eszközei közötti adatátviteli kapcsolat alapján véve megoldható vezetékeken keresztül.

A digitalizált katona viselhető kommunikációs hálózatának egy változata[3]

A ruházat egyik fontos eleme az **integrált sisak**. Ez nemcsak a katona fejét védi, hanem „hordozó” szerepet is betölt, hiszen felszerelhető rá például a fényerősítő szenzor, a hő kamera, a kijelző panel, a lézer besugárzás érzékelő, a szemvédelmet biztosító egység és a beszélő készlet is. A 4. számú ábrán egy integrált sisak modellje látható.



4. ábra

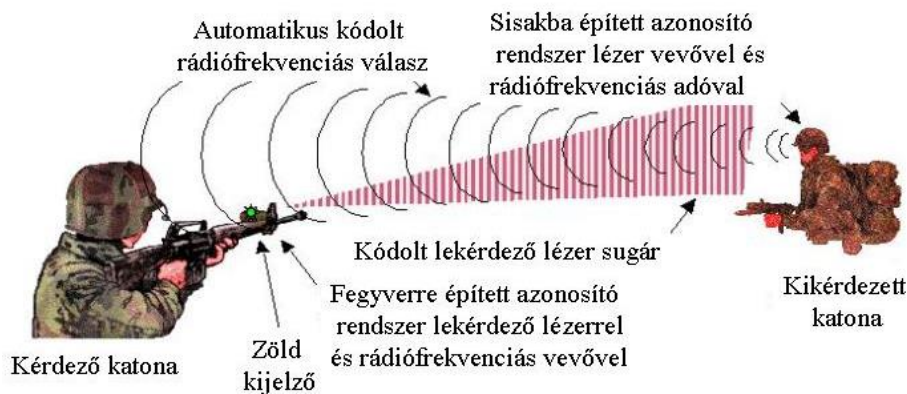
Az integrált sisak

A sisak elektronikai egységében helyezhető el például az elektromos iránytű, az elemek és a vezeték nélküli adatátvitelt biztosító adóvevő egység.

A sisakra integrált eszközök vonatkozásában már megjelenik a hang és a képi adatátvitelének igénye is.

A **helyzetjelentő** egység –a GPS vevő segítségével– megadja a katona mindenkori pontos pozícióját önmaga és a hálózat részére. Így szükség esetén társai és parancsnoka nyomon tudják követni a katona mozgását. Ennek megfelelően adatátviteli igény jelenik meg a GPS vevő, a számítógép, a kijelző panel és a központi hálózat között.

Az **idegen-barát felismerő rendszer** feladata megakadályozni a saját élő erő és technikai eszköz pusztítását. Fontos követelmény, hogy a katona által használt berendezés együtt tudjon működni minden, a harcmezőn megjelenő, nem ellenséges katona és technikai eszköz felismerő rendszerével. A két katona közötti idegen-barát azonosítási folyamat elvi vázlatát az 5. ábra mutatja be.



5. ábra[5]

Az egyes harcost azonosító rendszer működési elve

A **nagy felbontású kép megjelenítő eszközök** olyan szemüvegbe vagy sisakra rögzített kijelzők, amelyek a harctevékenységekhez szükséges információkat közvetlenül a katonák szeme elé juttatják.

Megjeleníthető a kijelzőn például:

- a katona pontos tartózkodási helye;
- a közelben lévő saját, illetve ellenséges katonák és eszközök tartózkodási helye;
- egy másik katona, vagy felderítő szenzor által rögzített hang és videokép;
- a harctevékenységek körzetében lévő épületek, létesítmények tervrajzai,
- egyéb más, a katona számítógépéről, vagy a harcászati hálózatról lekérdezett adatok is.

Ennek megfelelően mindezeket biztosító adatátviteli igény jelenik meg a kijelző panel és a számítógép között.

A **beszélő készlet** mikrofonokból és fülhallgatóból áll. Feladata a katona audio kommunikációjának biztosítása.

A katona sisakján (szem elé lehajtható kivitelben) elhelyezett **fényerősítő eszközök** a csekély meglévő fény felerősítésével a katona vizuális felderítését segítik.

A **nappali kamera** alapvető feladata a katona által látott kép továbbítása a társak vagy a parancsnok felé. Ebben az esetben a kamera képét először a katona viselhető számítógépéhez kell eljuttatni.

A **hő érzékelő kamera** az infra tartományú felderítésben játszik fontos szerepet. A passzív hő érzékelő segítségével a hőt kibocsátó ellenséges katonák, technikai eszközök már nagy távolságból felderíthetők, nemcsak nappal, hanem éjszaka vagy rossz látási viszonyok között is. A feladat függvényében ilyen kamera elhelyezhető a katona sisakján, fegyverén vagy az általa alkalmazott robotok hasznos terheként is. A kamera által érzékelt kép először a számítógépbe érkezik be, majd innen továbbítani kell a katona kijelzőjére. A sisakon vagy fegyveren elhelyezett kamera esetében megoldható a vezeték nélküli adattovábbítás. A robotokra szerelt kamerák esetében vezeték nélküli kommunikációs igény jelenik meg.

A **nagy teljesítményű, viselhető számítógép** összehangolja a digitalizált eszközrendszer működését. Rendszerezi a különböző szenzoroktól, eszközöktől jövő jeleket és továbbítja a megfelelő egységnek. A katona a harctevékenység végrehajtása során a számítógép vezérlését és a szükséges adatok bevitelét különböző módon valósíthatja meg. A számítógépnek védettnek kell lenni a külső hatásokkal szemben, ezért (a jelenlegi megoldásoknál) szilikon gélbe ágyazzák. A komputer működtetésének egyik módja lehet a rövid parancsokkal történő hangvezérlés. „A másik megoldás, egy olyan speciális elhajlás érzékelővel ellátott kesztyű, amely a hagyományos klaviatúrát és az egeret is helyettesítheti.”[6]

A **nagy zavarvédelemmel rendelkező személyi rádió**nak ki kell szolgálnia a katona kommunikációs igényét, képesnek kell lennie valós idejű adatátvitel teljesítésére. Ez az eszköz biztosítja az összeköttetést a társakkal, a kiküldő parancsnokkal és a harctéri információs hálózattal is.

Az **egészségügyi állapotjelző szenzorok** feladata a katona folyamatos fizikai és egészségügyi állapotának ellenőrzése. A harctéri öltözet belső felületén, vagy a testfelületen elhelyezett érzékelők jeleit a számítógép dolgozza fel, és továbbítja a (rádióon keresztül) harcvezetési központba. Ennek a kommunikációs kapcsolatnak kétirányúnak kell lennie. Fontos, hogy a parancsnoknak le tudja kérdezni a katona pillanatnyi állapotát. Így valós idejű információt kaphat a katonák sérüléseiről vagy a harcból való kiesésükről.

A **hordozható szárazföldi és légi robot** egyre nagyobb szerepet kap a katonai műveletekben. Megfelelő hasznos terhekkel ellátva különböző (felderítési, csapásmérési, kutató-mentő) feladatokat tud megoldani a katona helyett. Ezeket az eszközöket a katona magával tudja vinni a bevetésekre, mert elférnek a hátizsákjában.

A pilóta nélküli repülőgépekre és a szárazföldi robotokra különböző hasznos terheket lehet szerelni. Jelenleg a legelterjedtebb alkalmazási területük az elektrooptikai felderítés. A robotokon elhelyezett eszközök által látott képeket a katona kijelzőjére sugározva valós idejű felderítési adat nyerhető. A 6. ábra egy szétszerelhető pilóta nélküli repülőgépet és a repülőgép fedélzeti kamerája által lesugárzott (a katona kijelzőjére vetített) képet mutatja be.



6. ábra

A Dragon Eye pilóta nélküli repülőgép és a katona által látható kép[14]
A következő képen egy hordozható szárazföldi robotot látható.



7. ábra

A Packbot szárazföldi robot[15]

Szárazföldi vagy légi robot alkalmazása során nemcsak a hasznos teherként elhelyezett szenzorok adatait kell lejuttatnia a kommunikációs rendszernek, hanem biztosítani kell az eszközök irányítását is.

Az **áramellátást biztosító tápegység** kulcsszerepet tölt be a feladat végrehajtó képesség fenntartásában, hiszen ez felel a katona eszközszerének folyamatos

energiaellátásáért. Ez megvalósítható nagy kapacitású, hosszú élettartamú elemekkel vagy akkumulátorokkal. Az akkumulátorok folyamatos töltése többek között biztosítható az áramellátó bakancsal, amelynek talpa olyan különleges műanyagból készült, amely képes a mechanikus energiát elektromos energiává átalakítani.



8. ábra

Elektromos energiaellátó bakancs [7]

A **speciális fegyver** jellemzője kell, hogy legyen a pontos lézervezérlésű célzás, a nagy tűzerő és tűzgyorsaság. Kritérium a fegyverrel szemben az is, hogy rászerezhető legyen egy korszerű, a személyi számítógéppel összekapcsolható elektrooptikai irányzék, amely biztosítja a katona részére a pontos célzást éjszaka és nappal egyaránt. Igényként jelenik meg a kommunikációs rendszerrel szemben, hogy jelezze a katona számára a rendelkezésre álló lőszer mennyiségét, a cél távolságát és jellegét (típusát) is.

Összegzés

A digitalizált katonának kommunikációs eszközökre van szüksége, hogy kapcsolatot tudjon tartani a parancsnokával, a társaival, vagy a központi hálózattal. Ugyancsak kommunikációs eszközökre van szüksége a harcosnak, hogy a kiküldött érzékelői (pl.: pilóta nélküli repülőeszköz, szárazföldi robot) által gyűjtött adatok eljuthassanak hozzá, és értékelhető információkká válhassanak a számára.

Igényként jelenik meg a digitalizált katonát kiszolgáló kommunikációs rendszerrel szemben a kiváló minőségű hang és képátviteli (nem csak álló-, hanem inkább mozgókép), információ titkosítási, és a nehezen lehallgatható adatátvitel biztosítása. Ez kiegészül továbbá a valós idejű, több résztvevős video és audio konferenciák biztosításának lehetőségével.

Mindezek alapján megállapítható, hogy a digitalizált katona elképzelhetetlen a (testfelületen vagy harctéri ruházaton) viselhető kommunikációs rendszer nélkül.

Felhasznált irodalom

- [1] A world leading supplier of defence electronics and military information networks, <http://www.ericsson.com/microwave/products.shtml>
- [2] Ellison C. Urban: The Information Warrior <http://www.spectrum.ieee.org/publicaccess/1195inf1.html>
- [3] Next generation wearable network <http://islab.oregonstate.edu/koc/ece399/notes/ry031.pdf>

-
- [4] Fekete Károly: Az egyes harcos katona jövőbeni személyi kommunikációja, ÚJ Honvédségi Szemle, Budapest, 2002/12
- [5] Szalai Tibor: A harctéri azonosító rendszerek értékelése, közvetlen és közvetett eljárások alkalmazásának sajátosságai, Diplomamunka, ZMNE, Budapest, 2001.
- [6] Fekete Károly: Toward the Within of Military CIS Convergence (IPV4 and IPV6), A katonai kommunikációs rendszerek fejlődési irányai–kihívások és trendek a XXI. században c. konferencia kiadvány, ZMNE, Budapest, 2001.
- [7] Paul Eng: These Boots Are Made for Power, abc news, October 18, 2001. <http://abcnews.go.com/sections/scitech/CuttingEdge/cuttingedge011012.html>
- [8] Fekete Károly: Personal Military Communications System, Kommunikáció 2002 c. konferencia kiadvány, ZMNE, Budapest, 2002.
- [9] Hóka Miklós: A harctéri kommunikáció egyik lehetséges jövőképe: a harcászati internet, Kommunikáció 2003 c. konferencia kiadvány, ZMNE, Budapest, 2003.
- [10] Hóka Miklós: A városharc kommunikációs jellemzői a 21. században, Kommunikáció 2003 c. konferencia kiadvány, ZMNE, Budapest, 2003.
- [11] T J Gander, E H Biass, J Kegler: Tomorrow's infantry warrior, Armada International, 5/2003.
- [12] Alexander Stilwell: Technology aims to assist tomorrow's infantryman without adding to his burden, Jane's Defence Weekly, 10 December 2001.
- [13] StuartMcGhie: Digital soldier in command, Jane's Defence Weekly, 10 October 2001.
- [14] Eyes in the Sky http://www.sciencentral.com/articles/view.php3?article_id=218391898&language=english
- [15] David Buchbinder: In Afghanistan, a new robosoldier goes to war <http://www.csmonitor.com/2002/0731/p01s03-usmi.html>

ÚJ KIHÍVÁSOK A KATONAI INFORMÁCIÓS RENDSZEREKKEL SZEMBEN

Hamar Sándor ezredes
A HM HVK Híradó és Informatikai Csoportfőnökség csoportfőnök-helyettese
(híradó)

Tábornok és Tiszt Urak! Hölgyeim és Uraim!

Tisztelt Tudományos Konferencia!

Az USA védelmi minisztériuma a 90-es évek derekán - jelentősrészt az öböl-háború tapasztalataira támaszkodva - olyan elképzelést dolgozott ki, amely a katonai műveletek vezetési hatékonyságának jelentős javítására irányul az információtechnológia totális alkalmazása révén. A koncepció a **Network Centric Warfare**, tehát a Hálózatközpontú Hadviselés nevet kapta, amely alapvetően hivatott a katonai műveletek vezetési módszereit megváltoztatni az információhoz való hozzájutás lehetőségének radikális kiterjesztésével. A Hálózatközpontú Hadviselés jelenlegi állapotában egy vízió, amelynek megvalósulását 2020-ra tervezi az USA hadereje. A program a képességek megfogalmazásának szakaszában tart, a részletes követelményeknek és a megvalósítás módjának kidolgozása csak most kezdődik.

A koncepció lényegét - a prágai csúcstalálkozón megfogalmazott újfajta stratégia nyomán - a NATO is magáévá tette, és a **NATO Network Enabled Capabilities** (NNEC) terminológiát alkalmazza rá, amely **NATO Hálózat Nyújtotta Képességnek** fordítható. A megvalósíthatóság elemzése céljából a NATO C3 testület munkacsoportot állított fel, amelynek a megvalósíthatóságról jelentést kell készítenie.

Mit jelent a NATO számára az NNEC?

1. **Technológiát**, amely a kommunikációt, az információfeldolgozást célozza meg, mint alapvető funkciót? A NATO és a nemzeti rendszerek közötti interoperabilitási problémákra keres megoldást? Ne felejtjük el, hogy beruházások nem hoznak igazi értéket a vezetés-irányítási rendszerekben szükséges - az új technológia által megkövetelt - szervezeti változtatások nélkül.
2. Milyen **következményei** lesznek a műveletekre, hogyan hat a döntéshozatali folyamatra a jövőben? Hogyan érinti a műveleti eljárásokat, a vezetés-irányítást és a képzést?
3. Milyen **hatással** lesz a szervezeti **struktúrára**, feladat és felelősségi rendszerre? Jelenleg az információs hadviselésre gyakorolt hatása felmérhetetlen. A kibernetikus térben a fizikai határok elvesztik jelentőségüket.
4. Milyen **hatással** lesz **az információfeldolgozásra**? Hogyan oszthatjuk meg az információkat és őrizhetjük meg az információs fölényt?
5. Milyen **hatással** lesz **a biztonságra**? Milyen biztonsági intézkedéseket kell hozni a katonai információs rendszerek védelmében? A megnövekedett felhasználói végpont és kapcsolók száma milyen hatással lesznek a biztonságra?

-
6. Mekkora az **erőforrás igény**? A hálózati technológiák költségigénye magas, mint ismeretes. Hogyan osztható ez meg a tagállamok között? Milyen legyen a nemzetek befektetési mechanizmusa.

Számtalan megválaszolatlan kérdés merül fel a NNEC kapcsán. Hogyan lehet mégis a NNEC elgondolást összefoglalni?

A **konceptió egyszerűen összegezhető**: a katonai műveletekben részt vevő valamennyi szervezet és személy valós időben képes legyen hozzájutni a feladata végrehajtásához szükséges összes információhoz a megfelelő helyen, időben, tartalomban, bontásban és formában. Ehhez olyan információs (kommunikációs) hálózat kialakítására van szükség, amely képes a hálózat különböző pontjain egy időben vagy közel egy időben megjelenő, egymástól akár jelentős mértékben eltérő igényeket továbbítani, feldolgozni, és a választ a követelményeknek megfelelően rendelkezésre bocsátani.

A konceptió magában foglalja annak lehetőségét, hogy a hálózatban nagyszámban kerülnek továbbításra valósidejű, nem összegzett és feldolgozott ún. elsődleges információk akár jelentősen eltérő vezetési szintek, parancsnokságok, illetve különböző feladatot végrehajtó műveleti egységek között. A katonai tevékenységekhez szükséges információk a rendszer adatbázisaiban folyamatosan rendelkezésre állnak, a kialakult helyzetnek megfelelően folyamatosan aktualizálásra kerülnek, onnan bármikor kinyerhetők, és felhasználhatók. Az adatokhoz való hozzáférés szabályozása rugalmas, a jogosultságok a feladathoz és a végrehajtás körülményeihez egyszerűen, gyorsan hozzáigazíthatók.

A kommunikáció új rendszerének kialakítása nem hagyja változatlanul a vezetési folyamat elemeit. A különböző feldolgozottsági fokú információk - gyakorlatilag vezetési szinttől független - rendelkezésre bocsátása lehetővé teszi a döntések helyének megváltoztatását a szervezeti hierarchiában, amelyek egyrészt felfelé, másrészt a hierarchia alsóbb szintjei felé tolódnak el. A magasabb parancsnokságok bizonyos esetekben képessé válnak akár zászlóalj vagy század szintű szervezetek vezetésére, ha azt úgy ítélik meg, illetve az alegységek a feladat végrehajtásához szükséges valamennyi információ birtokában objektívebben értékelhetik a kialakult helyzetet és cselekvési változatokat, nem feltétlenül várva előljárói jóváhagyásra vagy részletes feladatszabásra az idő szorításában.

A konceptió több olyan követelményt tartalmaz, amelyet a jelenleg alkalmazott katonai kommunikációs és információs rendszerek egyike sem képes teljes körűen biztosítani:

1. A hálózat szolgáltatásainak a legmagasabb vezetési szinttől a feladatot végrehajtó egyes katonáig mindenki számára elérhetőnek kell lennie. Az információs kapcsolat kialakítása automatikusan, emberi közbeavatkozás nélkül kell hogy történjék. Az információáramlás útja nem alkalmazkodik a szervezeti hierarchiához, az információk lehívása, illetve küldése közvetlenül, vezetési szintek és előljáró parancsnokságok megkerülésével történhet. A kommunikációs rendszerben elvileg bármely végpont bármelyikkel kapcsolatot teremthet akkor, ha az a számára szükséges infor-

máció megszerzéséhez feltétlenül szükséges, és ezt az esetek jelentős részében tábori körülmények között, és mozgásban is meg kell tudni valósítani.

2. Gyakorlatilag minden információt az információs (kommunikációs) rendszerből kell kinyerni, ezért a tevékenységek során keletkezett adatok csaknem mind-egyikét oda valamilyen módon be kell juttatni. E célból a hálózat szinte valamennyi csatlakozási pontjának alkalmasnak kell lennie különböző típusú végberendezések szabványos csatlakoztatására annak érdekében, hogy az egymástól eltérő jelek egységes digitális jelsorozattá alakítva oda automatikusan bejussanak. A hálózat szolgáltatásainak igénybevétele ún. „Plug and Play” elven történik, amely a hozzáférési pontokhoz történő egyszerű, gyors és szabványos csatlakozás révén valósul meg.

3. A hálózatnak biztosítania kell a garantált szolgáltatási minőséget a rendszer nagyfokú leterheltsége, egyes rendszerelemeinek kiesése, vagy a felcsatlakozási pont változása esetén is. Ehhez a rendszer automatikus, forgalomtól és felhasználótól függő gyors adaptációjára, a topológia rugalmas, egyszerű és gyors módosíthatóságára van szükség. A rendszernek a főbb átviteli irányokban nagy sávszélességgel kell rendelkeznie ahhoz, hogy lehetőséget adjon jó minőségű mozgókép és hang párhuzamos átvitelére az egyéb adatforgalom mellett.

4. A hálózatban alkalmazott rendszerszoftvereknek el kell fedniük a felhasználók elől az általuk kért információk fizikai tárolásának helyét, módját, kódolását, struktúráját, valamint a kommunikáció belső eljárásrendszerét, amelyhez integrált adatkezelés és szabványos, strukturált kommunikációs felületek kialakítása szükséges.

5. A rendszernek komplex informatikai szolgáltatást kell nyújtania. Ez vonatkozik az irodaautomatizálási, üzenetkezelő és csoportmunka rendszerekre, a kimon-dottan katonai célú informatikai alkalmazások párhuzamos, távoli munkahelyeket és adatbázisokat összekapcsoló igénybevitelére, valamint a különböző forrásból származó és különböző formájú valósídejű információk egyazon végponton történő igény szerinti szemléletes megjelenítésére.

6. A NATO tagállamok rendszerei egyszerűen, szabványos felületeken keresztül összekapcsolhatók kell hogy legyenek, és az egymás adatbázisaiban tárolt adatokat – megfelelő jogosultság birtokában – hatékonyan el kell tudniuk érni. Ebből a célból egységes elvek szerint építkező hálózati architektúra és interoperabilitási elvek kerültek, kerülnek kidolgozásra és elfogadásra. Az adattípusok közös struktúrájának és értelmezésének kialakítására jelentős erőfeszítések történtek a NATO C3 Testület ezért felelős munkacsoportjában. A szárazföldi műveletek adatainak egységes kódolása és értelmezése céljából a NATO tagállamok jelentős része a MIP program keretében évek óta közösen fejleszti az egységes adatrendszert.

7. A hálózatnak alkalmasnak kell lennie olyan jelzésrendszer működtetésére, amelynek révén prioritás érvényesíthető az üzenetek továbbításának, feldolgozásának és megjelenítésének sorrendjére vonatkozóan. Bizonyos típusú üzenetek elsőbbséget kell hogy élvezzenek másokkal szemben, amelynek alkalmazására felhasználói cso-

portok is kialakíthatók. Ily módon a kommunikációs hálózat a felderítő, a navigációs és a fegyverirányítási rendszerek által szolgáltatott jelek értelmezését, feldolgozását és továbbítását is azonos platformon, egységes rendben, a követelményeknek megfelelően képes végrehajtani.

8. A hálózat működésképtelensége az egész feladat kudarcát vonhatja maga után, ezért annak működését folyamatosan figyelemmel kell kísérni, a rendellenességeket távfelügyelet útján rövid időn belül el kell tudni hárítani. E célból ki kell alakítani a megfelelő monitoring rendszert, amely magában foglalja a felügyeleti szoftvereket, az eljárási rendszabályokat, valamint a megfelelő szervezeteket és személyeket. Az ún. aszimmetrikus hadviselés körülményei között a hálózat bénítása, zavarása elsődleges cél, amelyet mindenképpen meg kell megakadályozni. A digitális technika csaknem kizárólagos alkalmazása új típusú veszélyt hordoz magában, a hálózat működésének szoftveres úton történő megbontása, a szoftverek révén megvalósított illetéktelen adatnyerés jelentős kihívásként jelentkezik, ezért a távfelügyeletnek a behatolások detektálásának is hatékony eszközévé kell válnia.

A NATO Hálózat Nyújtotta Képességek elérése hosszú folyamat, amelynek eredményei legkorábban a következő évtizedben jelentkezhetnek. A rendszer megvalósíthatóságának, erőforrásainak és tulajdonságainak elemzését, a fejlesztési tervek megfogalmazását és szakaszokra bontását viszont már ma meg kell kezdeni.

A tervek kidolgozása és maga a fejlesztés több területen párhuzamosan is megvalósítható. A felcsatlakozás szabványos felületeinek kialakítása, az adatátviteli rendszer architektúrájának és átviteli csatornáinak megtervezése, a rendszer alapszolgáltatásainak és alkalmazási körének meghatározása, az adatrendszer és az adatbázisok struktúrájának kialakítása egymással párhuzamosan, de nem egymástól függetlenül folyhat. Fontos kérdés, hogy a jelenleg fejlesztés alatt álló híradó és informatikai infrastruktúra megfelelő alapot nyújt-e egy hasonló rendszer kialakítására, illetve a korábban hosszú távra megfogalmazott elgondolásainkat szükséges-e módosítani.

A korábbi rendszerfejlesztési elgondolásokkal szemben a NATO Hálózat Nyújtotta Képességek koncepció önállóan is megállja a helyét, azaz a C2 képességek megfogalmazását követően a vezetési rendszer részletes ismerete nélkül is kialakítható az a híradó és informatikai infrastruktúra, amely moduláris felépítéséből és rugalmas alakíthatóságából adódóan, paraméterezhető szoftvermegoldásokra támaszkodva gyakorlatilag minden vezetői információs igényt ki tud elégíteni, egyszerűen adaptálható a vezetés rendjéhez, az alkalmazási körülményekhez és a végrehajtandó feladatokhoz. A hálózatközpontú koncepció legfontosabb elve, hogy az információk igény és szükség szerint legyenek biztosíthatók és az információs (kommunikációs) rendszer képességei azt a lehető legkisebb mértékben korlátozzák.

Ehhez természetesen megfelelő műszaki humán erőforrásokra van szükség, amely nem nélkülözheti a költséghatékonysági elemzéseket. A koncepció jelenlegi stádiumában azonban erre nem kerül sor, egyelőre az a kérdés, hogy technikailag megvalósítható-e egy ilyen hálózat, ki valósítsa meg, milyen rendszerteknikai és

szervezési megoldásokat kell ehhez alkalmazni, és milyen mértékben nőhet általa a katonai vezetés hatékonysága. Ugyancsak fontos kérdés, hogy milyen szakaszokra, projektekre bontható a teljes folyamat, és azok időben hogyan követik egymást.

Ebbe a munkába a magyar katonai és megfelelő minősítéssel rendelkező civil szakemberek is bekapcsolódhatnak. A műszaki tudományos fórumok elsődleges témaköre lehet, sőt lennie kell a jövőben. Figyelemmel kísérhetik a NATO katonai kommunikációs és információs rendszerei fejlesztésének fő irányait, a hálózatközpontú koncepció megvalósulását, abban meghatározhatják a Magyar Honvédség szerepét, lehetőségeit és a fejlesztés sajátos hazai módszereit.

Köszönöm a figyelmet!

AZ ELEKTRONIKA FEJLŐDÉSÉNEK HATÁSA A HARCÁSZATI MOBILKOMMUNIKÁCIÓRA

(Katonai rádióeszközök fejlődése a hadviselés tükrében)

A XXI. század elején a számítógép, a mobiltelefon mindennapjaink munkaeszköze, szinte az élet minden területén érezzük hatásait. A modern technológiák használatának korában sokak számára talán feleslegesnek tűnik a rádiózás történetének néhány emlékezetes pillanatát feleleveníteni, hiszen az ember, főleg a fiatalabb generáció, teljesen természetesnek veszi a csúcstechnológia napi megnyilvánulását. Úgy vélem azonban, hogy a rádiózásról alkotott kép nem lehet teljes anélkül, hogy ne tiszteljük azon kiemelkedő személyiségek népes tömege előtt, akik munkásságukkal, kitartásukkal hozzájárultak a huszadik század egyik korszakalkotó felfedezéséhez és elterjedésének lehetőségéhez. A téma aktualitását az is növeli, hogy 2004.-ben ünnepeljük Puskás Tivadar születésének 160. évfordulóját, és jelen sorok szorosan kapcsolódnak a megemlékezéshez.

A rádió kialakulása

Egyértelmű választ adni arra a kérdésre, hogy ki volt a rádió feltalálója, nehéz feladat. Híres tudósok, kutatók és névtelen kísérletezők versenghetnének ezért a címért.



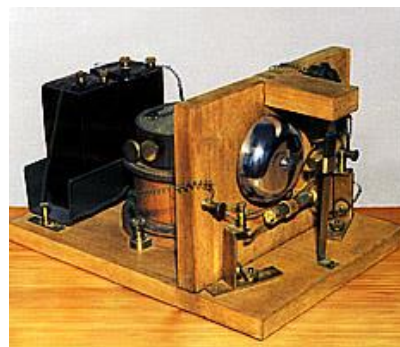
Guglielmo Marconi

Vajon eljutott volna Hertz 1888-ban, az elektromágneses hullámok felfedezéséig, ha nincs az olasz Galvani, aki híres, békacombos kísérleteivel vonult be a tudomány világába, vagy ha Benjamin Franklin nem eresztí fel papírsárkányát, amelynek nedvessé vált zsinégéből a légköri elektromosság hatására szikrák pattantak ki, így alkotva meg a villámhárítót? Bevészhette volna nevét a halhatatlan tudósok márványtáblájára az olasz Marconi, az orosz Popov, a német Arco, ha nem születik meg Jedlik Ányos, a dinamó megalkotója, vagy Edison, találmányainak hosszú sorával? A válasz, valószínűleg akkor is: igen, – legfeljebb a történelem más neveket jegyez fel –, hiszen a felfedezés, megismerés belső kényszere egyidős az emberiség kialakulásával.

Az elektromágneses hullámok felfedezője maga sem gondolta, hogy milyen nagy horderejű dologban alkotott maradandót, sőt ki is jelentette, hogy az elektromágneses hullámok nem alkalmasak nagyobb távolságok áthidalására.

Szerencsére bőven akadtak kételkedők, akik rácăfoltak e kijelentésre, és bebizonyították a távolság leküzdését a vezeték nélküli technikában.

Ki tudná leírni azt a pillanatot, amikor a kutató, a kísérletező elme erőfeszítéseit siker koronázza? Mint a francia Ferrié kapitány, aki 1903-ban az Eiffel tornyot használta antennaként vezeték nélküli távírókísérleteihez, vagy az olasz származású Marconi, aki már 1897-ben vezeték nélküli távíró összeköttetést létesített az angliai Bristol csatornán, a Lawernock-Point és a Flatheolm sziget közötti öt kilométeren.



Popov rádiója 1905



Fleming „lámpája”

A boldog békeidők kedveztek a különböző polgári kutatások fellendülésének, így a múlt század elején, Fleming feltalálja, majd Marconi szabadalmaztathatta az elektroncsövet, amely forradalmasította a rádiózást (detektoros rádió). A Nobel-díj felemlítése sem maradhat ki a történelmi visszatekintésből, hiszen Marconi és Braun professzorok 1909-ben éppen a rádióval kapcsolatos találmányaikért kapták meg a tudományos világ legnagyobb elismerését.

Kezdetben az első rádióösszeköttetések után a rádiót drótnélküli távírónak hívták. Ezt a nevet használta Marconi is, amikor 1901-ben az első összeköttetést létesítette Nagy Britannia és Amerika között. Ugyancsak ekkor tapasztalta, hogy a légkörben van valamilyen visszaverő réteg, amely mint egy tükör, megtöri a rádióhullámokat. A jelenség magyarázatára mintegy húsz évet kellett várni, az amerikai Kennellynek és az angol Heaviside-nak 1921-ben sikerült kísérleti tényekkel is bebizonyítani a légkör egy rétegének rádióhullám-visszaverő képességét.

Az új technika természetesen nem kerülhette ki a hadi alkalmazást sem. Egyre nagyobb távolságú rádióösszeköttetések válnak lehetővé: 1904-ben már katonai rádió-távíró kísérletek folynak Budapest és Bécs között.

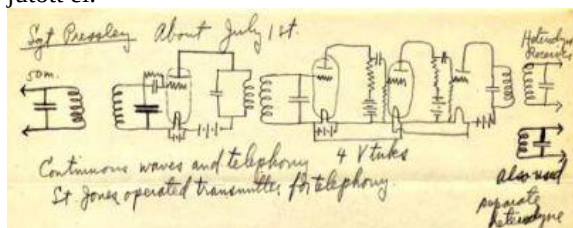
Korai katonai alkalmazások

Hadviselési célokra először az orosz-japán háborúban (1904-1905), és a német fennhatóságú Délnyugat Afrikában alkalmazták az adó és vevőberendezéseket, mintegy 200 km-es távolságokon. A fél világ megkerülésére kényszerült orosz hajóhad útban a Csúzimai szoros – és végzete felé, a német gyarmatként nyilvántartott Kamerun partjainál vett fel ivóvizet és szenet a gőzhajóira, amikor az első – német gyártmányú – készülékeket is elhelyezték a hadihajók fedélzetén. Természetesen nem az összeköttetés hiánya okozta később az orosz flotta vereségét...

Az I. Világháború kezdetének idejére Edwin H. Armstrong megalkotja az első visszacsatolt kapcsolást (1914), nem sokkal később (1916-ban) megépült az első elektroncsöves rádió távbeszélő célokra, és az rögtön alkalmazást is nyert a tábori híradócsapatoknál. Az orosz hadsereg volt az első haderő, ahol a rádióhíradás szerepet játszott egy katonai műveletben, a Tannenburg-i csatában (1914. augusztus. 26 - 30.) a harcparancsok eljuttatására használták a csapatok felé. Ugyancsak itt történt az első rádiólehallgatás is a német csapatok részéről: majdnem olyan gyorsan nyilvánossá váltak ezek a harcparancsok, ahogy az oroszok előállították őket.

A kezdetleges készülékek nem igazán váltották be a várakozásokat, a morzekódos, később hangátvitelű rádiók zömében csak kis távolságon voltak használhatósak, a nagyteljesítményű adó-vevők ritkaságszámba mentek (elsősorban a tápellátási problémák miatt).

Számos esetben az alkalmazások csak tervek maradtak, például az amerikai csapatoknál 1917-18-ban a rádiók repülőgépeken való használata csak a tervezési fázisig jutott el.



Armstrong „superheterodin” vevőjének rajza

Rádiók a II. Világháborúban

Az elmúlt évszázad első tömegmértű rádiógyártása a Harmadik Birodalomhoz fűződik. Az 1929-33-as gazdasági válságból kivezető utat Németország vezetői a fegyverkezésben látták, így a rádiógyártás vonatkozásában a Telefunken cég került vezető pozícióba. Egy másik német cég, a Lorenz, amely az amerikai ITT konszern alvállalata volt, - együtt a Telefunkenkel és a Siemenssel - 1935-ben megkezdte a német harcászati rádiók gyártását, speciálisan fejlesztett, kisméretű csövekkel [1].

Meghatározó volt a kevés típusváltozatú vákuumcsövek alkalmazása: a legtöbb rádiókészülékben ugyanazokat az elektroncsöveket használták. Ennek előnye egyértelműen az esetleges javításoknál jelentkezett. A csöveket kifejezetten katonai alkalmazásra fejlesztették ki, a speciális foglalatú miniatűr csövek azokban az időkben nagyon strapabíró eszközök voltak, és szabványként szolgáltak a civil rádiókészülékek gyártásánál is.



Lövészárok rádió az I. Világháborúból

A rádiózás igazi áttörése az I. világháborút követő években következett be. Armstrong 1918-ban egy 8 vákuumcsöves rádiót tervez, melyet szuperheterodin vevőnek nevez el, és ezzel kezdetét veszi a rádiózás elterjedése a civil szférában is. Ezt az elvet követi a mai rádiók és TV-k 98%-a.



**Feld Fu
hátirádió**

A szabványosítást olyan megfontolásból is végezték, hogy a kellően begyakorolt mozdulatok alapján sötétben is lehetett akkumulátort cserélni a készülékekben, a tetejükön kialakított fémkampók letapogatása alapján, de Braille írással is feltüntették a készülékek kezelőszervein a beállítási értékeket, hogy akár vakok is tudják kezelni, hangolni a rádiókat.

A rádiók belső kialakításánál a modulrendszer volt az alap, egyszerűen és könnyen kapcsolták össze az egyes paneleket, funkciójuknak megfelelően. A modulok kialakításánál külön szempont volt, hogy mind mechanikailag, mind elektronikai szempontból önálló egységet képezzenek. *(Hasonlítsuk össze ezt a gyártási szemléletet napjaink elvárásaival a modern rádióeszközök kialakításában!)*

Az alkalmazott rádióhálózatok tiszta képet adtak a német parancsnokoknak a harcmezőről, gyors és precíz manővereket téve lehetővé a vezetett páncélosoknál. *(Ez az elvárás ugyancsak napjainkban jelenik meg ismét, a harcászati helyzetismeret formájában, igaz, már zömmel informatikai eszközökkel).*

A nagy tömegben gyártott rádiókészülékek használatával vált lehetővé Lengyelország gyors lerohanása, majd később a Franciaországi villámhadjárat.

A németek javára billentette a mérleget a kiképzettségük, és az, hogy rendelkezésükre álltak azok a minőségi rádiók, amelyek megfeleltek a páncélos csapatok harci követelményeinek. A kiképzéshez tartozott például: ha egy német páncélos harcjármű lerobbant és fennállt a veszélye, hogy a felszerelés az ellenség kezére jut, a rádiókezelőnek kötelessége volt a rádióeszközöket elrejtteni vagy megsemmisíteni.

A II. Világháborúban használt német rádiókészülékek több szakíró véleménye szerint is világszínvonalat képviseltek az 1930-as évektől kezdve. A modulegységek elektronikai csatlakozásai sokérintkezős, „tűs” csatlakozókkal történtek, a különösen erős konstrukciójú rádiókészülékek ennek is köszönhetően hibamentes működésüket, de az egyszerű szervizelési lehetőségeiket is.

A rádiók üzemképességéről csak annyit, hogy még 60 évvel a II. Világháború után is jelentős hányaduk működőképes (már az a néhány száz darab, ami elkerülte a szétszerelést³¹).



**Telefunken rádió moduláris
elemekből összeállítva (1938)**

³¹ A német hadsereg által a II. Világháborúban használt híradó berendezések nagyon kevés ismertek napjainkban. Ennek a fő oka az, hogy 1945 végétől 1946-ig, a Szövetségesek összegyűjtötték a német hadifelszerelést, és nagy részüket megsemmisítették. A rádiók esetében egyszerűen szétszereltették azokat, és az alkatrészeket, főleg a csöveket a polgári rádiókészülékekben használták fel.



SCR-511 „pogo stick”

Az amerikai kontinensen kevés rádiós fejlesztés történt, egészen 1939-ig. Ekkor fejlesztették ki az első kézi rádiót, a "walkie-talkie"-t, mely mindjárt három típusban jelent meg: SCR-193, SCR-194 és SCR-195.

Az első „walkie-talkie” széria nem volt sikeres, nem lehetett hosszú távon hordozni őket, a méretük és a súlyuk miatt. 1942-ben jelent meg az SCR-536 „kézibeszélő” (handy-talkie) és az SCR-511 „zászlórúd” (pogo-stick), melyek rendszeresítésre is kerültek az amerikai hadseregben.

Az SCR-511 kézirádiót eredetileg arra tervezték, hogy lovaglás közben is lehessen rádiózni. Érdekes mérnöki bravúr volt úgy kialakítani a rádiót, hogy egy kézzel lehessen használni, miközben a másik kézzel a lovat irányította a kezelő. [2]

Ennek ellenére az első valódi kézirádiónak az SCR-536-os tekinthető, amely a gyalog közlekedő felhasználóknak nyújtott összeköttetési lehetőséget.

A két kézirádiót - fő felhasználási területként - a rendőrségnél alkalmazták először (lovas- és gyalogosrendőrök), viszont az 1940-es évek elején hadbalépő amerikai csapatok is ilyen eszközökkel lettek felszerelve, a hadműveletek növekedésével egyre nagyobb számban³². Az olaszországi műveletekben például már a legtöbb lövész szakaszparancsnok rendelkezett kézirádióval (SCR-536), amelyet magával hordott a művelet folyamatos vezetésének biztosítására, de csak az előljáró századparancsnok felé rendelkezett a rádiókommunikációval.

A szakaszon belüli híradás továbbra is a kézjelekre és élőszóbeli utasításokra korlátozódott (pl.: hírlánc).

A II. Világháborúban jelent meg az első igazi amerikai hátirádió, az SCR-300, amely a katonai megítélés szerint egy nagyon sikeres eszköz volt. Századparancsnoki, és a fölötti szinteken használták, ez biztosította a „nagyávolságú” rádióhíradást.

Sikerét mi sem bizonyítja jobban, mint az, hogy több országban is rendszeresítésre



SCR-536 „handie talkie”



SCR-300 hátirádió

³² Mindkét rádiókészülék a Galvin Manufacturing Co.-nál készült, amely céget ma Motorola-ként ismeri a kommunikációs világ.

került a háború után. Az angol haderőben a Wireless Set 31. típusszámot kapta, míg a franciáknál az eredeti gyári BC1000 néven szerepelt a hadrendben.

Mind az európai, mind a Csendes-óceáni hadszíntér szárazföldi csatáiban jelentős szerepet kaptak ezek az eszközök, melyeknek hordozható és járműbe épített változatai a manőverek főszereplőivé léptek elő. Az orosz frontokon kezdetben a segélyszállítmányokból származó szövetséges, illetve zsákmányolt német rádióeszközöket is használtak, később már saját fejlesztésű rádió adó-vevőekkel látták el nagyobb számban a szovjet csapatokat.



A magyar harcászati rádiózás kialakulása szorosan kapcsolódott a nemzetközi (főleg német illetve olasz) fejlesztésekhez. A trianoni hadsereg-fejlesztési megszorítások végétől (1927) a magyar hadiiparhoz kapcsolódó elektronikai cégek nagyon jó rádiókészülékek gyártására voltak képesek: a Magyarországon gyártott rádióadócsövek hosszú ideig világszínvonalú készülékek gyártását tették lehetővé mind a civil, mind a katonai szférában.

A kis, közepes és nagyteljesítményű rádiókészülékek megbízhatóan funkcionáltak, kielégítve a kor katonai-vezetési követelményeit. A magyar katonai rádiókészülékek típusválasztéka az 1920 és 1940 közötti évek elméleti harcászati-hadműveleti irányelveinek szem előtt tartásával alakult ki, melyek azonban az első világháború tapasztalatain alapultak. A II. Világháború új hadműveleti-harcászati elgondolásai (villámháború, nagy mélységben történő lerohanás páncélos ékekkel, óriási méretű bekerítő hadműveletek, katlanacsaták) végrehajtására a magyar hadsereg sem a felszerelés, sem a kiképzettség tekintetében nem volt képes.

A nagy távolság jelentett kihívást az üzemeltetők számára, a Don partján kiépített (mélység nélküli) „pókhálóvédelem” harcoló alakulatai és parancsnokságai között 1943 januárjában, amikor a feltételezett távolság többszörösére történő rádióírhíradást kellett megvalósítani [3].

A II. Világháború egyik legfőbb tanulsága az volt a rádiózás területén, hogy bebizonyosodott, milyen egyszerű az ellenség adásait lehallgatni. A bizonyos fokig védett harcászati rádióadások biztosítása került középpontba a nagy viláégés után, de a technológia megkövetelte egyéb szolgáltatások, mint például a zavar és lehallgatás-védett rádiócsatornák, vagy akár a tranzisztor, még nem álltak rendelkezésre. A gyakorlatban ez azt jelentette, hogy – némi túlzással – mindenki hallhatott mindenkit.

A lehallgathatóság is közrejátszott abban, hogy a negyvenes évek közepén új rádióadás módszerek után kezdtek kutatni, és hamarosan megalkották a közvetlen szekvenciás³³, más néven szórtspektrumú rádiózást. A szórtspektrumú adás újszerűsége abban rejlett, hogy a kisugárzott adóteljesítmény egy széles frekvenciaspektrumban, mintegy szétnyomva jelentkezik, és ez által csökken a jelkisugárzás felderíthetősége. Ha ehhez még hozzáadjuk a frekvenciaugratás³⁴ lehetőségét, máris egy korszerű, kato-

³³ Direct Sequence (DS) vagy Spread Spectrum (SSP)

³⁴ Frequency Hopping (FH), amikor nem egy állandó frekvencián sugárunk, hanem egy álvéletlen generátor meghatározása szerint a kisugárzott jel másodpercenként több frekvenciát is

nai harcászati rádió birtokosai vagyunk. Ennek a precíz megvalósítása viszont csak később, a félvezetőkön alapuló technológiák elterjedése után vált lehetővé. Addig is az elektroncsövek paramétereinek fejlesztése maradt a konstruktőrök egyik legfontosabb feladata.

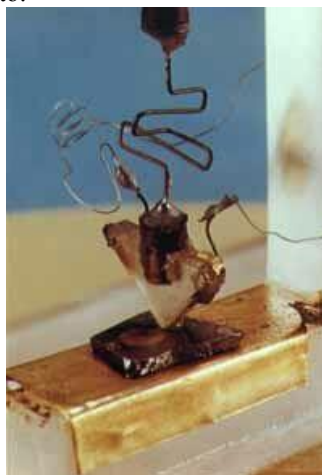


PRC-6 rádió

Félvezető eszközök megjelenése

Az elektroncsöves polgári és katonai rádiókészülékek sikerei ellenére a korai vákuumcsövek „hatalmas étvággal” rendelkeztek: az anód nagyfeszültségű táplálása mellett a katód fűtési igényét is meg kellett oldani, ami jelentős problémákat okozott a még gyerekcipőben járó áramellátási területen, a hordozható, szárazakumulátorok kialakításának vonatkozásában. A háború után sikeres kísérletek folytak az elektroncsövek áramigényének csökkentésére, ugyanakkor a csövek, és ezzel együtt a készülékek méreteinek a csökkentésére is.

A Koreai háborúban (1950-53) szerepet kapott amerikai rádiók, a PRC-8 (páncélos), a PRC-9 (tüzérségi), és a PRC-10 (lövész) típusok, amelyekben szubminiatur (golyóstoll átmérőjű), új fejlesztésű vákuumcsövek kerültek aktív erősítőelemként felhasználásra, a korábbiaknál jóval szélesebb frekvenciasávbeli üzemelést tettek lehetővé. Ugyancsak a Koreai háború „terméke” a PRC-6 szakasz szintű kézirádió, amely egyben az SCR-536 továbbfejlesztésének is tekinthető.



Az első tranzisztor 1948

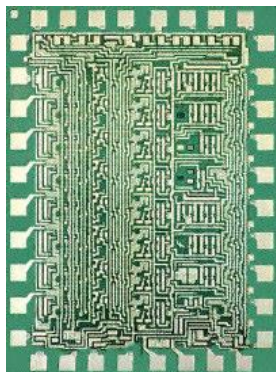
felhasználni. A frekvenciaugratásos szórt spektrumú rádiók első harci alkalmazása az 1982-es, ötödik arab-izraeli háborúban történt, izraeli részről, és teljes sikerrel.



Az első IC 1958

Nevezetes az 1958-as év is: ekkor jelennek meg először az integrált félvezető áramkörök (Integrated Circuits), új lendületet adva az áramköri korszerűsítésnek és a miniaturizálás lehetőségének.

Az integrált áramkör megjelenése ugyanakkor jelentős hatást gyakorolt az áramköri elemek szerelésére is, ekkortól kezdték alkalmazni a nyomtatott áramköri lap kialakítást a készülékekben.



**CMOS logikai IC
1967**

Lényeges pont volt a fejlődésben a logikai integrált áramkörök feltalálása, ez adta meg a lehetőséget, hogy az eddig analóg elven működő, elektroncsöves, tranzisztoros berendezések helyett új, digitális elven működő készülékek kerüljenek kifejlesztésre. A 70-es években egy lassú fejlődési trend következtében apránként mind szélesebb körű szolgáltatások jelentek meg a harcászati rádiók újabb és újabb modelljeiben: a digitális hang (delta enkóder felhasználásával), később a rejtjelzett hang, majd az adatátvitel biztosítása. Az integrált áramkörök fejlesztési eredményei a kétpólusú világ katonai szembenállása miatt stratégiai szerepet kaptak az elektronikai készülékek gyártásában, így a tranzisztorral kezdődő miniaturizálás, áramfelvétel csökkenés, kisebb készüléksúly kialakításának előnyei csak nagy késéssel jelentek meg a VSZ és így hazánk hadseregének híradóeszközeiben.

A nagy integráltságú integrált áramkörök (VLSI) megalkotása nem csak a logikai IC-k fejlődésének mérföldkövét jelentette, hanem a számítástechnikai processzorok fejlődésének is az alapja.

Digitális rádiókészülékek megjelenése

A nyugati haderőkben a mikroprocesszor és az ASIC³⁵ technológia alkalmazása voltak az első lépések a rádiókészülékek digitalizációja felé, ami aztán a COMSEC³⁶ funkció integrálásával hamarosan valósággá vált. A fő szempont ebben az időben az *elektronikai hadviselés* általi zavarok elleni védelem volt, a megalkotott szabványok csak a háttér kompatibilitást biztosították az előző generációs készülékekkel.

³⁵ Application Specific Integrated Circuits, nagy bonyolultságú integrált áramkörökkel felépített, alkalmazás specifikus, moduláris egységek

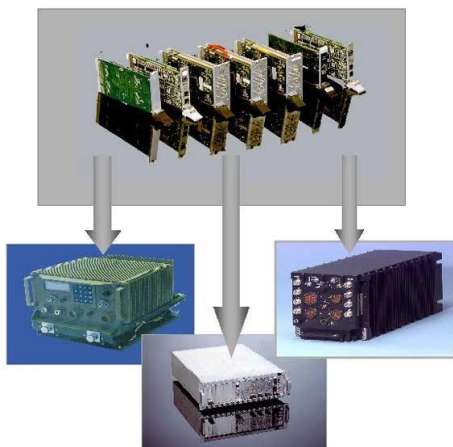
³⁶ Híradó biztonság (COMmunications SECurity). A távközlést érintő biztonsági rendszabályok alkalmazásának összessége, mely egyfelől biztosítja az illetéktelen személyek kizárását a távközlési hálózat értéket tartalmazó információihoz történő hozzáféréseinek és azok feldolgozásának lehetőségéből, másfelől pedig a jogosultak számára garantálja a hozzájuk eljuttatott információk hitelességét. Ezen intézkedések alapvetően a rejtjelzéssel és az információk továbbításának és kisugárzásának védelmével kapcsolatos rendszabályokat tartalmazzák. (AAP-31)

A digitális rádiók megalkotása a mikroelektronika gyors fejlődésével vált lehetővé, amely alatt jelen esetben a digitális jelfeldolgozó processzorok (DSP), az analóg-digitális és digitális-analóg átalakítók (ADC, DAC), a dedikált alkalmazásokhoz kifejlesztett integrált áramkörök (ASIC), és a könnyen (akár „terepen” is) programozható kapusor áramkörök (FPGA³⁷) nagyarányú előretörését értjük. Az utóbbi időben pedig egyre gyakrabban alkalmazzák az általánosan felhasználható digitális jelfeldolgozó processzorokat (GPP³⁸).



ADC IC (90-es évek)

Szoftverrádiók



JTRS modulok minden hullámformára
(Raytheon)

A *szoftver vezérlésű rádió*³⁹ vagy röviden szoftverrádió technológiája lehetővé teszi, hogy a különböző nemzeti haderők egységei akadály nélkül kihasználhassák a csúcstechnológiában rejlő szolgáltatásokat. A szoftvervezérlésű rádió átfogalmazhatja a katonai rádiózás szabályait, megvalósítva a *multimédia alapú információfolytató*, a hang, a kép, a szöveg és egyéb adatok átjátszását a felhasználók igényei szerint.

A sikeres kísérletek nyomán és a katonai műveleti doktrínák új meghatározásai alapján kialakult az *Összhaderőnemi Harcászati Rádiórendszer* (Joint Tactical Radio System, JTRS).

A rádiócsalád, amely a 2 MHz-2 GHz közötti sávban szolgáltat videó és adatátvitelt az összhaderőnemi műveletekben, az alábbi kihívásoknak kell megfeleljen:

- Moduláris felépítés, rugalmas fejlesztetőség;
- Méretezhetőség - további sávszélesség és csatornabővítés lehetősége, nagyobb teljesítmény;
- Új technológiák beilleszthetősége: új processzorok, új hullámformák;
- Gerinchálózat kompatibilitás, illeszkedés a nagysebességű hálózatokhoz;

³⁷ Field Programmable Gate Array

³⁸ General Purpose Processor

³⁹ Az eredeti Software-Defined Radio (SDR) kifejezés *szoftver vezérlésű rádió*nak való fordítása úgy vélem helyesebb, mint a szó szerinti, szoftver meghatározású rádió, mivel alapvetően a rádió működtetése, azaz a hardver vezérlése történik az alkalmazott szoftverekkel.

- Rádiócsalád, amely a légierő, a haditengerészet, a szárazföldi csapatok kommunikációs támogatásán túl fix állomásként is képes üzemelni;
- Interoperabilitás, intra-operabilitás, vagyis nemcsak a szövetséges rendszerek közötti szolgáltatásnyújtás és fogadás, de a haderőnemek közötti egységes felhasználás;
- Hálózati szolgáltatások, IP kompatibilitás, adatforgalom irányítás.

Rádióháló szervezés

Heinz Guderian (1888 – 1954), egy akkor még ismeretlen német törzstiszt, az I. Világháború kezdete előtt egy rádiós kurzuson vett részt, és ez a későbbiekben nagy hatással volt a rádiózás katonai elterjedésére. A harckocsik alkalmazásának elemzésével, már 1917-ben felismerte az összeköttetés fontosságát a manőverezésben, és szorgalmazta, hogy minden tankon legyen rádió [4].

A katonai rádiókészülékek tömeges előállítása a 30-as években kezdődött, különösen az újabb háborúra készülő német haderőben volt jellemző a csapatok nagyobb arányú ellátása rádióeszközökkel, - nem utolsósorban az ekkor már páncélos tábornokká előlépett Guderian szorgalmazására.



Guderian tábornok

A rádióeszközök koordinációs alkalmazására az egyik legszemléletesebb történelmi példa, a német páncélos csapatok gyors előretörése a Somme folyó torkolatáig 1940-ben, amikor stratégiai előnyt szereztek a szövetséges angol – francia csapatok megosztásával. A gyors manőverezés, különösen az Ardenneknben, nem sikerülhetett volna a *precízen megszervezett* rádióhíradás nélkül. Guderian tankjai és motorizált gyalogsága olyan gyorsan tört előre, hogy ellenfeleinek nem maradt ideje a hidak és egyes útszakaszok megrongálására, a támadás késleltetésére. A harckocsizók megvalósították a tábornok jelmondatát, amely így szólt: *vezess, rádiózz, tüzelj*. A műveletekben repülőgépek is részt vettek, amelyek elsődlegesen a veszélyjelzéseket és az előretörés lehetőségének információit adták meg rádión a felsőbbszintű vezetési pontokra [5].

A rádióeszközök egyre intenzívebb elterjedésével igény jelentkezett összefüggő rendszer kialakítására, amelynek egyik előfeltétele a családely, vagyis az azonos alaprádiók alkalmazása. Az első katonai rádiórendszer, amely megfelelt a családelynek, a brit haderőben került rendszeresítésre, LARKSPUR néven 1962-ben.



LARKSPUR A-412 hátrádió

Az angol haderőben a II. Világháború alatt szinte kizárólag KH és RH rádiók voltak rendszerben, Wireless Set megnevezéssel, amely számozás 1948-ra elérte a 88-as számot. Ezután amerikai és kanadai rádiók licence alapján megjelentek az URH sávban üzemelő eszközök is, és a 60-as évekre ezen típusokból került kialakításra a már említett LARKSPUR rendszer, ahol a hátán hordozható (manpack), a járműbe (vehicle), repülőkhöz épített eszközök mellett komplett rádióállomások is megjelentek.

A 60-as évek NATO hadseregeiben, a földfelszíni rádiózásban előtérbe kerültek a szervezési kérdések, kialakították a *trónkölt rádiórendszereket*; a többszörös hozzáférés lehetősége egy rádiócsatornához, a csoportos rádióvezérlések kialakítása ebben az időben kezdett határozott körvonalakat ölteni. Némely esetben a sajátos földrajzi környezet kényszerítette a konstruktőröket új, addig ismeretlen elvek megalkotására a rádiózásban (pl.: a Hawaii szigetek tagoltsága miatt az ALOHA rendszer), máskor a nagy földrajzi távolságok közötti adatsere biztosításának kényszere (pl.: az ARPANET hálózat⁴⁰). A két terület integrálásával alakult ki a 70-es évek elején a csomagkapcsolt rádiózás (packet radio), amelynél az információt meghatározott egységekre, csomagokra bontva továbbítják a címzett felé.

A hálózati rendszerszervezésre az egyik legjobb példa az ARPANET kialakítása. Az 1969-es kezdeti négy munkaállomás összekapcsolása hamarosan kinőtte kereteit, és ennek eredményeként 18 évvel később már meghálózatként megszületett egy új média, az Internet. Napjainkra pedig az egyik meghatározó médiává alakult, annak ellenére, hogy senki sem felügyeli teljes egészében.

Katonai rádiórendszerek

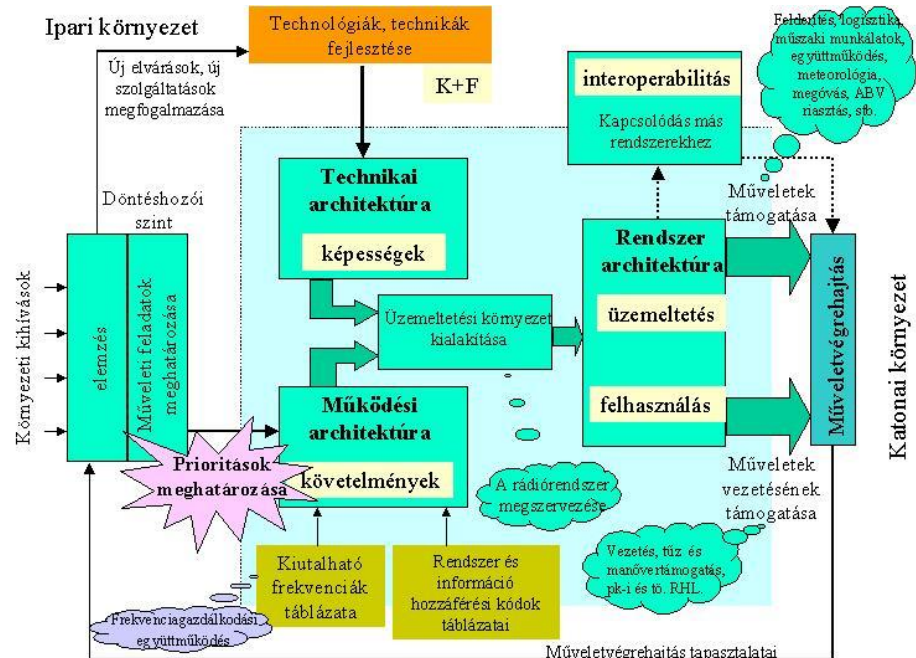
A katonai rádiórendszer tartalmában lényegesen több mint a harcászati rádióhálózat. A technikai rendszerkialakításból adódóan ide kell értenünk az egycsatornás RH, URH és szélessávú rádiókkal kialakított harcászati rádióhálókat, az egycsatornás műholdas híradás eszközrendszerét, és a különböző adatterminálokat is. A rádióeszközök ezen túl, átviteli utakat biztosíthatnak a hozzájuk közvetlenül csatlakoztatott számítógép, fax és távbeszélő végkészülékek számára, a hálózathoz csatlakoztatott más, illesztett végkészülékekkel való hang- és adatkommunikáció megvalósítására. Ennek alapján megállapítható, hogy a rádiórendszer összetevői a következők:

- A rádióeszközök a technikai paramétereikkel, a szolgáltatásaikkal;
- Az üzemeléshez szükséges frekvenciaspektrum;
- A különböző frekvenciátáblázatok, adatlapok és beszélgetési táblázatok;
- Az előbbieket segítségével létrehozott rádióhálókat és irányokat;
- A hálózati kapcsolóelemek, amelyek a rádióeszközöket illesztik a kommunikációs hálózathoz;
- A hálózati szoftverek, amelyekkel a rendszer menedzselhető, felügyelhető;

⁴⁰Az ARPANET természetesen nem rádiós technológián alapult, de a fejlődés szempontjából meg kell említeni, mint a rádiózásra ható újdonságot.

- A hálózatot kialakító és üzemeltető kezelőszemélyzet, (amennyiben erre szükség van).

Az optimális rádiós architektúra kialakítása a gyakorlatban úgy jelenik meg, mint a rádiórendszerek alkalmazása a katonai műveletekben. Egy művelet-végrehajtáshoz rendelt katonai kommunikációs rendszervezés csak folyamatában értékelhető, kezdve a környezeti kihívások értékelésétől a művelet-végrehajtás elemzéséig, illetve az új elvárások (szolgáltatások) megfogalmazásáig, így ezeket mind figyelembe kell venni a rádióhíradás szervezésénél is.



A harcászati rádiórendszer optimalizált kialakítása

Forrás: saját

Lényeges pont a feladat-meghatározás sorában a *prioritások megadása*. Ezekben jelenik meg egy fontos vezetői elvárás a tényleges rendszer üzemeltetésére során. Az elsőbbségek meghatározása, a csatornakapacitások tartalékolása, az elsődleges információk körének felvázolása a művelet harcparancsában kell, hogy testet öltson, *ennek hiánya esetén a rendszer üzemeltetési környezete sem fogja célját betölteni*.

Katonai rádiórendszerrel lévén szó a rendszerarchitektúra kialakítása kétsíkú. Egyrészt a *műveletek vezetésének támogatásában* jelenik meg, de számolni kell a *műveletek támogatásával* is, hiszen önálló felderítő, logisztikai, műszaki munkálatok támogatására szervezett rádióháló is szerelnek ebben. (A parancsnok elgondolása szerint).

A napjaink gyakorlatában megjelenő harcászati rádiók előnyös tulajdonságait csak egy stabilan működő üzemelési környezetben képesek maximálisan felkínálni a felhasználóknak. A szolgáltatások hatékony kihasználásához, a kommunikációs képességek fejlődéséhez az alábbi jellemzőket kell kialakítani:

Digitális harcmező. Lényeges, hogy a kommunikáció mind függőlegesen (vezetés), mind vízszintesen (együttműködés) megvalósuljon, valamint a reagálási idő az el-lenség döntési ciklusán belül legyen.

A műveletek maximális információval való ellátása. Hang, adat és lehetőleg videó szolgáltatás a harc, a művelet minden fázisában, előreprogramozott, zavarásmentes üzemmódokban.

A kommunikációs eszközök gyors hordozóeszközökbe építve. Gyors előrevonás után rövid idejű telepítés, és gyors kommunikációs csatorna átadás (a felhasználónak) lehetséges.

Önkonfigurációra képes rádiórendszerek. Olyan eljárások kidolgozása, amelyek a bekapcsolás után automatikusan felépítik a szinkronizációt, azonosítják a felhasználói készülékeket, és stabilan üzemeltetik magát a rádiórendszert.

Maximális interoperabilitás. A kölcsönös szolgáltatások biztosítása a stabil vagy gerinchálózati rendszerekkel, mindez szövetségi keretekben is (NATO közös műveletek).

Integrált hálózatmenedzsment. A hálózat tervezés, konfigurálás, felügyelet fejlett szoftverekkel történik, rugalmas és gyors beavatkozási lehetőséget adva a kritikus helyeken.

Az amerikai elvek már konkretizálják, hogy a szoftverrádió szervesen beépül a C4I infrastruktúrába: az alkalmazott szoftverektől függően a híradó és elektronikai felderítés, a navigációs és azonosítási rendszerek, az elektronikai hadviselés, az információs hadviselés, az elektronikai ellentevékenységek területén, valamint a rakéta-irányzásban, vezérlésben kaphat kiemelt szerepet. A szoftverrádiók költséghatékonysága megmutatkozik ezen túl az új katonai, műveletorientált szervezeti változásokban is, mivel az ebből eredő felhasználói igények változásai, a szolgáltatási paraméterek, sokkal rugalmasabban és egyszerűbben köthetők a megváltozott szervezeti beosztásokhoz [6].

Összefoglalás

Ahogy az a rádiózás történeti áttekintéséből is kitűnik, a tudományos felfedezések (pl.: az elektroncső, a félvezető dióda, a tranzistor vagy az integrált áramkör) viszonylag rövid idő alatt alkalmazásra kerülnek a készülékek sorozatgyártásaiban (elsősorban a nyugati haderőknél), és ez a trend napjainkban fokozottan jelentkezik. Olyan korban élünk, amikor nemcsak új termékek, szabványok jelennek meg, de az elavultnak kikiáltott *analóg technológiák helyét digitális eljárások veszik át.* Ez a folyamat várhatóan még 5 – 7 évig eltart: az előrejelzések 2010-re teszik a digitális fényképezőgépek, TV-k, rádiók, kommunikációs eszközök teljes körű elterjedését a világon. A katonai kommunikáció, és ezen belül a rádióhíradás technológiai fejlődése sem mentes ezektől az előrejelzésektől, gondoljunk csak a szoftverrádiós kutatásokra.

Ugyancsak szembetűnő, hogy a hidegháborús veszélyek csökkenésével (a 80-as évek közepétől) a technológiák – technikák egyre inkább kívül esnek a valamikori katonai „elsődlegességen”, és a civil szférában, profitorientált vállalatoknál, üzleti megfontolások alapján történik a kutatások, fejlesztések nagy többsége. Nem hagyható figyelmen kívül az a tény sem, hogy a gazdasági, üzletpolitikai megfontolások átbil-lentek a széles, - civil - fogyasztói rétegek igényeinek kielégítésére, és a katonai szükségletek, a katonai technológia minőségi fejlesztése már nem a közvetlen háborús veszélyeztetettségéből fakad.

A történeti áttekintés összegzéseként jelenik meg a következő táblázat, amely alapján generációs elkülönítést végezhetünk a katonai rádiókészülékek között. (Némely készülékgyártónál más alapokon határozzák meg a rádiókészülékek generációit, pl: a Rohde and Schwarz cégnek az 5. generációs rádiója a M3TR szoftverrádió, vagy a francia PR4G rádiórendszer is már 4. generációs a Thales cégnél.)

Megnevezés		Jellemzők	Példák
Korai rádióeszközök	Elektromechanikus (rádió) eszközök	• kezdetben nincs erősítőelem • bonyolult hangolás • alacsony hatásfok • adatátvitel nincs vagy nagyon kezdetleges	I VH. előtti rádiók
	Vákuumsöves rádióeszközök		I. és II. VH rádiói; koreai háb. rádiói
1. generációs rádiók	Analóg rádióeszközök (fejlett vákuumsöves és tranzistoros)	• analóg AM v. FM moduláció • FSK adatátvitel és ez is nagyon lassú • egyszerű lehallgathatóság és zavarhatóság	Angol LARKSPUR rádiórendszer; amerikai, francia, orosz rádiók
2. generációs rádiók	Digitális rádióeszközök	• deltamodulációs hangátvitel • alacsony adatátviteli sebesség (<9,6 kbps RH és 64 kbps URH) • FH mint ECCM eljárás • csomagkapcsolt adatátvitel támogatása	CLANSMAN; PR4G; SINCGARS; HARRIS; Utóbbiak Harcászati Internetekben is
3. generációs rádiók	Többsávos, többfunkciós digitális rádióeszközök	• számos hullámforma támogatása (5 – 20) • fejlett csomagkapcsolt adatátvitel (kép és hang együtt is) • együttműködés civil és kényszerítési rendszerekkel (pl.TETRA)	R&S M3TR; HARRIS FALCON II; fejlett Harcászati Internet
4. generációs rádiók	A JTRS koncepció alapján szoftverrádiók	• széleskörű COTS eszköz ellátás • szoftver-vezérlésű funkciók • magas adatátviteli sebesség (> 256 kbps) → videóátvitel is • összhaderőnemi szintű műveletek támogatása	fejlesztés alatt

1. táblázat: A katonai rádióeszközök fejlődésének összefoglaló táblázata

Forrás: saját

A 60-as évek óta fejlődő integrált áramkörök a 90-es évek nagybonyolultságú, ugyanakkor széleskörű felhasználhatóságú alkatrészé váltak. Az ASIC chipek ma már

egy kétutas (adó-vevő) rádiót képesek integrálni egyetlen lapkán, amely jelentős méretbeli és áramfelvétel csökkenési jellemzőkkel bír, míg az FPGA mikroáramkörök igény szerint programozható, nagyszámú logikai kapcsolóelemmel rendelkeznek. Ezen utóbbi sokoldalú felhasználása alacsonyabb szintű ugyan, mint az ASIC-é, de az áramkör a teljes élettartama alatt szabadon programozható, így az esetleges szabványváltozások okozta nehézségek egyszerűen áthidalhatók, továbbfejlesztésük pedig a felhasználás függvényében rugalmas. Mindkét technológia meghatározó a mai digitális rádiókészülékek tervezésénél, sőt a szoftverrádiók kialakításánál is.

Kiemelt figyelmet fordítva a digitális technológián alapuló hardver és szoftver elemek összehangolt fejlesztésére, a jelfeldolgozó processzorok alkalmazásával, és ez által jelentős számítástechnikai kapacitás biztosításával lehetővé válik egy összefüggő hálózati rendszerkialakítás, amely már képes a magas szintű szolgáltatások nyújtására / fogadására az összhaderőnemi vagy többenemzetiségű katonai műveletekben, azaz az interoperabilitás megvalósítására. Ugyanakkor a civil technológiák alkalmazása nem nélkülözheti a speciális katonai elvárások figyelembevételét: az ilyen elemekből felépített készülékek, de komplett rendszerek vizsgálata is az elektronikai harc változatainak alkalmazása mellett mindenképpen szükséges.

Gordon Sullivan, az Egyesült Államok haderejének Vezérkari Főnöke 1993-ban így fogalmazott a jövő hadviselésével kapcsolatban: „*Míg a XX. század szárazföldi hadviselésének meghatározója a harckocsi volt, a XXI. századé a számítógép lesz.*” [7]

Ez a kijelentés meghatározza azt az irányvonalat, amely egyfelől a hadviselés fejlődési / átalakulási sajátossága, (ha úgy tetszik: az erőn alapuló hadviselés helyett a tudás alapú hadviselés korszaka fog beköszönten), de egyben utal az elektronika fejlődésének a felgyorsulására is. A kijelentésből kitűnik egy új szemléletmód elsajátításának szükségessége, amelyet ugyancsak Gordon Sullivan fogalmazott meg, mely szerint: „*Az információ a győzelem záloga a harcmezőn*”[8].

Hivatkozások:

- [1] www.armyradio.com/Articles/William_Howard_German/General_Information.htm
- [2] <http://www.gordon.army.mil/ocos/Museum>
- [3] A magyar katonai rádiózás hőskora. Budapest, 1995, szám nélkül
- [4] International military and defence encyclopedia, 606. oldal, Brassey's (US) Inc. ISBN 0-02-881065-1 (vol2)
- [5] John McDonald: A II. világháború nagy csatái, 9. oldal, GABO Kft., 1995, ISBN 963 8009 071
- [6] Army Science and Technology Master Plan 1998. Annex E. Global Technology Capabilities and Trends B.6. Command, Control, and Communications. (Internetes letöltés: <http://www.fas.org/man/dod-101/army/docs/astmp98/index.html>)
- [7] Field Manual No106, Information Operations. Department of the Army, Washington, DC. Aug 1999. (Internet: <http://www.adtdl.army.mil/cgi-bin/atdl.dll/query/download/FM+100-6>)
- [8] U.o. mint az előző

A MAGYAR HONVÉDSÉG ZÁRTCÉLÚ HÁLÓZATA ÉS HÁLÓZATFELÜGYELETE BIZTONSÁGI OLDALÁNAK SZILÁRDÍTÁSA

A Magyar Honvédség jelenlegi zártcélú távközlő és informatikai hálózatai a régi technológia lépcsőzetes, szakaszos kiváltásának, valamint a jelenleg már működő eszközök fejlesztésekre történő beintegrálásának elveit szem előtt tartva jöttek létre. A költségvetési előirányzat szűkössége következtében komoly előzetes elemző és tervező munkát követel meg annak felmérése és eldöntése, hogy a távközlés és informatika robbanásszerű fejlődési folyamatából mely technológiákat vagy rendszereket szerezzük be, illetve helyezzük rendszerbe. Köztudott, hogy naprakészen, lemaradás nélkül követni a telekommunikációs eszközök, struktúrák, szemléletek változását oly mértékű anyagi terheket ró a rendszerüzemeltetőkre, mely csak néhány speciális feladatkörű szervezetnél áll arányban a kommunikációs hálózat „globális értékével”. Az általunk üzemeltetett hálózatok jelenleg még képesek kielégíteni a felhasználók igényeit, azonban már rövidtávon is robbanásszerű követelménynövekedésre kell számítani. A technológia és a rajta forgalomként megjelenő bármely jellegű információ olyan védendő érték, melynek oltalmazására a kockázatelemzés alapján kialakított biztonsági rendszer költsége mindenképpen megtérül az általa elhárított esetleges veszteségek figyelembevételével. A Magyar Honvédség szakirányú anyagi ráfordításainak elhanyagolható részét képezik jelenleg a távközlő és informatikai hálózatok biztonságát szavatoló eszközök, alkalmazások beszerzése, pedig ezen terület kiemelt figyelmet érdemel. Napjainkra az összefonódó távközlési és informatikai alkalmazásoknál a hálózatokat és ezzel együtt a hálózatfelügyeleti tevékenységüket ellátó szervezeteket érő támadások oly széles skálája vált jellegzetessé, napi szinten előfordulóvá, hogy ez az infokommunikációs kihívások első számú tényezőjévé vált.

Fenyegetettségek

A hálózati szolgáltatások (mind hang- és adatkommunikáció) területén a minőségi kritériumok mellett a megbízhatóság és védetség is ugyanolyan fontos szempont a védelmi szférában, így a hálózatokon forgalmazott bármely információ illetéktelen kézbe jutása, megmásítása, megrongálódása nem megengedhető. Ugyanakkor a hang- adat forgalom, az ezeket biztosító hálózatok folyamatos, üzemkiesés nélküli működését biztosító Hálózatfelügyeleti Központ tevékenységi köre jelenleg nem terjed ki a hálózatbiztonság globális kezelésére. A globalizáció jelensége soha nem látott utat nyitott a világviszonylatú jó- és rosszindulatú információszerzés és az ezzel történő visszaélések területén. A menedzsment feladatkörének az eddig felölelt üzemfelügyelet, fenntartás, hálózati forgalomelemzés területei mellett már a hálózatbiztonság komplex feladatrendszerét is szükséges tartalmaznia, hiszen ezen oldal gyengeségei a teljes hálózati struktúrát valamint a rajtuk folyó információkat és ebből kifolyólag a felhasználók tevékenységét is veszélyeztetik.

Míg világviszonylatban a támadást, az illetéktelen hozzáférést végrehajtó személyek korábban általában tehetséges fiatalok voltak, akik indítéka többnyire önmegvalósítás, politika és eszméktől mentes figyelemfelkeltés volt, addig napjainkra

már a tudatos, eszmei, anyagi vagy egyéb határozott célú profi, erre specializálódott kiemelkedő tudású emberek által végrehajtott betörések a jellemzőbbek. Általánossá vált, hogy ezen támadók megrendelés alapján is tevékenykednek, így látszólagos okkal - bizonyos adat megszerzésére, vagy esetleg módosítására - a végrehajtó személy nem is rendelkezik, mely jelenség a betörés indítékainak megfejtését jelentősen megnehezíti.

Reális veszélyként jelentkezik a védelmi szférában többek között az ipari kémkedés, az egyéb kémtevékenység, a nem tudatos és tudatos betörés, rongálás veszélye. Az ipari kémkedés mindig is jelen volt a világ gazdaság szinte minden területén, így a hadiiparnál is. Az információs társadalom térnyerésének felfokozódásával a különböző lokálistól a világhálózatokat is felölelő hálózattípusok térnyerésével könnyebbé vált az illegális hozzáférést folytatók helyzete. A központi adatbázis kezelés biztonsági rései hihetetlen értékű, összetételű és mennyiségű adatbázishoz juttatja az illetéktelen behatolót. A Magyar Honvédség zártcélú hálózatán a hangátvitelen kívül a legkülönbözőbb szakterületek (pénzügyi, ügyviteli, logisztikai, személyügyi, légtérfigyelési, meteorológiai, belső levelezés stb.) adatbázisainak forgalma zajlik, melyek titkosítása ugyan általánosan nem indokolt, azonban illetéktelen kézbe kerülését kívánatos akadályozni. Szükséges ezért egy kockázatelemzés készítése, mely mérlegeli a különböző adatátviteli hálózatokon forgalmazott információk „értékét”, felállítja a szervezeti elemek kommunikációs igényeinek biztonsági szemléletű kielégítési rangsorát, valamint felméri a kommunikációs hálózatok védettségét és biztonsági hiányosságait. Az ez alapján kialakított biztonsági koncepció bevezetése és betartatása és a kijelölt szerven keresztül folyamatos ellenőrzés magas szinten védetté tenné a Magyar Honvédség zártcélú hálózatát az illetéktelen behatolásokkal szemben.

Korunk kihívásai és ezzel együtt Magyarország biztonságpolitikai helyzete az utóbbi évtizedben jelentősen átalakult, ezzel együtt a Magyar Honvédség feladatköre a vele szemben támasztott követelmények alapjaiban megváltoztak. A missziós híradás előtérbe kerülése, a terrorizmus általi fenyegetettség időszerezése a távközlési-informatikai követelményeket is teljes mértékben megváltoztatta. A mobilitás mellett a biztonság kiemelt tényezővé vált a beszéd és adatcélú forgalmazás területei egyaránt a Magyar Honvédség zártcélú hálózatában. A kommunikáció és informatika robbanásszerű fejlődése és mind nagyobb mértékű használata a védelmi szférában teret nyit az informatikai bűnözés, kémtevékenységek valamint vallási, eszmei szélsőségeket képviselő csoportok illetéktelen információhoz történő hozzáférésehez.

A betörők felderítését a tudatos rejtőzést biztosító alkalmazásokon kívül a mind több helyen biztosított, mindenki által hozzáférhető nyilvános területen lévő Internet hozzáférési pontok (Internet-kávézók, egyetemek internetszobái stb.) is bonyolítják, hiszen itt a betörés termináljának lekövetésével sem lehet megfogni és felelősségre vonni az elkövetőt, mivel a személy rövid ideig, anonim módon tevékenykedik csak adott helyszínen.

A betöréseket végrehajtók céljai, indíttatásai és az általuk okozott kár eltérő. Azon kategória, melynek tagjai többnyire tehetséges fiatalok, akik kihívásokat, kalandot keresnek, általában a legkisebb kárt (anyagi, szakmai, jogi) okozzák a hálózatok üzemeltetőinek, mivel nekik nincs speciális információ megszerzésre való indíttatásuk. Ők többnyire az Interneten keresztül támadnak, így ellenük az általános biztonsági fellépések hatékonyak.

Másik kategóriában jelentkezik és mindig jelen van a szervezet belsejéből, az állomány valamely tagjától eredő illetéktelenség, mely általánosságban az intranet hálózaton jelentkezik. Az okok itt nagyon sokszínűek, a bosszútól az anyagi haszon reméléséig terjedhetnek. Az intranet hálózatok hozzáférési korlátozásai kijátszásának módjai és keresett információk begyűjtésének lehetőségei sajnos az Interneten is hozzáférhetők. Ebbe a kategóriába sorolandók a „nem szándékos” bűntársak, akik a biztonsági szabályok be nem tartásával utat nyithatnak hozzáféréseknek nem várt és esetleg nem védett pontokon.

A saját üzemeltetésű intranet- és Internet- hozzáférési hálózat térnyerése a Magyar Honvédség zártcélú hálózatában is általános, mely rengeteg előnye mellett a veszélyeztetettség szintjét bizony emeli.

Újabb kategóriába sorolandók azok a kiemelkedően magas szintű tudással rendelkező személyek, akik tudatos tevékenységgel általában észrevétlenségre törekedve, de néha javító szándékkal utólagosan betörésüket felfedve tevékenykednek. Szándékaik lehetnek rombolók, vagy csak információszerzők, módosítók. Dolgoznak megbízásra, de saját egyénüket érintő érdekből úgyszintén. A profi hackereknek például olyan kapcsolatrendszerük van, melyen keresztül egy- egy hálózat biztonsági gyengeségeiről szerzett tapasztalataikat megoszthatják egymással. Ide sorolandók a hackerek, crackerek és az ügynöki információszerzés is.

Ezen kategóriák természetesen csak egy általános felosztását mutatják az informatikai bűnözésnek, de minden említett terület valós fenyegetettséggé jelenik meg hálózataink és azok menedzsmentje irányában. Az említetteken kívül természetesen jelen vannak egyéb elektronikus támadási fenyegetések (pl. zavarás, irányított energianyalábú eszközök alkalmazása stb.) , melyek elleni védekezés csak tudatos felkészüléssel valósítható meg.

Valószínűsíthető, hogy már több észrevétlen betörés történt rendszerünkbe a hasonló civil szférában működő ellenőrzött hálózatok tapasztalati statisztikáira támaszkodva. Reálisan fel kell készülni információszerzést, módosítást, blokkolást, a vezetés folyamatosságának megbénítását célzó támadások bekövetkezésére, melyek elleni védekezésre tudatosan készülni szükséges. Ezen illetéktelen hozzáférések száma világviszonylatban is folyamatosan növekszik, ezért szükséges megfelelő biztonsági menedzsment kialakítása.

A Magyar Honvédség információs szolgáltatási rendjében nem vagy csak nehezen választhatók szét az úgynevezett hagyományos adatszolgáltatási és beszédcélú szolgáltatások hordozófelületei, ezért az összehangolt távközlő hálózatnak is az informatikai igények mind magasabb elvárásainak szükséges megfelelnie. A hang- adatszolgáltatások platformjainak összekapcsolódása célszerűvé teszi hálózatfelügyeleteik magasabb szintű egy kézbe fogott koordinálását, hiszen ezek egységes egészének együttkezelésével valósítható meg, üzemeltethető legoptimálisabban a Magyar Honvédség zártcélú hálózata. Ugyanakkor ezen központi menedzsment a hálózatbiztonság különböző használatban lévő technológiákból eredő sokszínű, de mégis összefonódó problémáit magas hatékonysággal lenne képes együtt kezelni.

A védelmi felülvizsgálattal összhangban a távközlő hálózat kiépítettségének és a vele szemben támasztott követelményeknek az elvei is jelentősen változtak. A kiterjedt, nagy „mozdíthatatlan” stacioner távközlő hálózatok elméletének háttérbe szorítása, a gyorsan áthelyezhető, esetlegesen mozgatható eszközök, átviteli utak elvének

hangsúlyossá válása a jellemző. Az állandó távközlő hálózat digitális központjai viszonylag könnyen áttelepíthetők másik alakulathoz, mely tulajdonság a haderőcsökkentésből adódó változásokhoz, feladatokhoz itt jól alkalmazkodik.

Mind nagyobb hangsúlyt képviselő feladatot jelent a missziós-, békefenntartó tevékenységek híradását is biztosító távoli hírhálózat elemek biztonságos bekapcsolása a távközlő hálózatba. Az új feladatrendszerhez igazodó igények emelkedésével már jól bevált felcsatlakozási koncepció újragondolása szükséges. A nemzeti területen kívül tevékenykedő alegységeink híradásának jelentős része műholdas bérelt összeköttetésen keresztül valósul meg, a stacioner zártcélú hálózatra történő felcsatlakozásnak védelme csak fizikailag megoldott. A zártcélú hálózat intranet és Internet hálózatai bizonyos missziók állománya számára elérhetők, ezzel a szolgáltatások biztosítása, mint pozitív, munkát segítő tényező mellett sajnos ez újabb kockázati elemeket hoz magával.

A tábori híradást szolgáló központok és hálózati felkapcsolódási struktúra elavultsága indokoltá tette a tábori híradás eszközeit modernizáló tender kiírását. Fontos szempontként jelent meg már az a követelmény, hogy ne csak a stacioner hálózatban jelenleg használt ISDN alapú hálózathoz⁴¹, hanem az IP alapú hálózathoz⁴² is képes legyen kapcsolódni, ezeket kezelni, szolgáltatni. Amellett a tábori híradás menedzsmentjének is kompatibilisnek kell lennie a jelenlegi stacioner hálózatával, hiszen gyors hibafelismerést, hibaelhárítást, beavatkozást csak ez tesz lehetővé. A legfontosabb követelményként az jelentkezik, hogy lehetőség legyen a tábori és stacioner hírhálózat együttes kezelői síkon történő felügyeletére.

Ezek a -közeljövőben rendszerbe kerülő esetlegesen eddig még a Magyar Honvédségben nem rendszeresített- eszközök és berendezések előrevetíthetik azt, hogy a technológia fejlődésével a Magyar Honvédség egyre fejlettebb alkalmazásokat használ és utat nyit a jobb, dinamikusabb sávzélesség kihasználású lehetőségeknek, ezzel elválaszthatatlanul korábban ismeretlen biztonsági problémákkal kerül majd szembe, amelyekre a hatékony védelmi és elhárítási felkészülés elengedhetetlen.

Hálózatzbiztonság

A Magyar Honvédség zártcélú hálózata jelenleg is felvonultatja az eszközök és alkalmazások legszélesebb skáláját, ezzel bonyolítja a hálózati biztonság egyenletes szinten tartásának megvalósításához vezető egységes rendszabályok, valamint globális technológiák bevezetését. A hálózatzbiztonság kritériumai részterületenként változhatnak, ezért a költséghatékonyabb védelmi szisztéma kialakítása érdekében átfogó jellegű kockázatelemzés végrehajtása szükséges. Elengedhetetlenül fontos a biztonsági rendszer méretezése szempontjából felmérni a támadók lehetséges okait, identitását annak érdekében, hogy a védelmi stratégia megfontolt és arányosan méretezett legyen.

A biztonsági kritériumok szigorítása leginkább az átviteli utak, aktív eszközök, hálózat összekapcsolási pontok és a menedzsment területén szükséges. A hálózat központjainak alacsony szintű védelme a jelenlegi távfelügyeleten keresztül megvalósul, de a kockázatelemzés eredményei szerinti fejlesztés véghezvitele elengedhetetlen.

⁴¹ ISDN (Integrated Service Digital Network) Integrált Szolgáltatású Digitális Hálózat

⁴² IP (Internet Protocol) Internet Protokoll

A végberendezések védelme pedig néhány speciális területtől eltekintve a Magyar Honvédség zártcélú hálózatában jelenleg nem indokolt, hiszen a kinyerhető információk értéke nem áll arányban a ráfordítandó védelmi költségekkel.

Általánosságban a Magyar Honvédség átviteli útjai biztonsági szempontok szerint túlnyomó részben gyengén védettek. A mikrohullámú átviteli utak biztonsági paraméterei rangsorolva a leggyengébbek, de a hagyományos kábelek területén sem sokkal jobb a helyzet. Alapvető paraméterei alapján az optikai kábeles megoldás adja a legjobb védetségű szintet, de magas bekerülési költsége miatt sajnos igen kis számú saját optikai kábellel rendelkezik a Magyar Honvédség, inkább a bérlemények a jellemzők. Mivel látható, hogy általánosságban az átviteli utak nem rendelkeznek magas védelmi paraméterekkel (lehallgatás, zavarás ellen), így szükséges lenne az átviteli utak egy részén csoportos titkosítás alkalmazása. A csoportos titkosítók használata a kiemelt fontosságú adatátviteli rendszerek, valamint a kiemelt prioritású hang és adatszolgáltatások hordozófelületének átviteli útjain indokolt, mely megvalósulásoknál a ráfordított költségek aránya megfelelő a védeni kívánt információk értékhez viszonyítva. Az igen magas számú átviteli utak mindegyikének csoportos titkosítása azonban gazdaságilag nagyon magas ráfordítást igényelne és nem is indokolt. Hálózatrányítással a védeni kívánt információk az adott trónk forgalmát terhelve továbbíthatódnak, melyet figyelembe véve csak ezen kijelölt átviteli utak titkosítása kerülhetne végrehajtásra.

Csoportos titkosítók helyenkénti alkalmazásával megoldható a kijelölt átviteli utak biztonságossá tétele, így kielégítve azt a kritériumot, mely szerint a kommunikációs csatorna és adatforgalom kellően biztonságossá válik, az adatok módosíthatóságának esélye csekély, az információfolyam nehezen lehallgathatóvá válik és az illetéktelen hozzáférés észlelése időben megtörténik.

Kiemelten fontos szempont, hogy ezen védett és titkosított trónkón belül folyhasson a távközlési-, adatkarbantartó-, biztonsági menedzsment tevékenység is, ezzel kivéve a felügyeleti tevékenységnek álcázott támadásokat, vagy az ezen területen keresztüli illetéktelen hozzáféréseket.

Jelenleg a hálózati adatállományok mind a digitális hálózat, mind az adatátviteli rendszerek egy részének tekintetében ezeken a nyílt távközlő átviteli utakon forgalmazódnak, így veszélyeztetettek mindennemű támadással szemben. A Magyar Honvédség digitális kapcsolóközpontokat összekötő átviteltechnikája jelenleg ISDN technológiára épül, bár a fejlesztési koncepciók hosszú távon az IP irányába mutatnak. A Magyar Honvédség országos adatátviteli transzporthálózatának létrehozásánál azt a végcélú tűzték ki, hogy a szervezetek között a digitális kapcsolástechnikát elkerülő független 2 Mbps-os csomagkapcsolt összeköttetéseket hozzanak létre, melynél már nagyobb hangsúlyt fektettek a biztonsági oldalt figyelembe vevő tervezésre is, mivel az összeköttetéseket védő biztonsági eljárások meghatározásra kerültek.

Mivel a többi területen ez az elv még nem érvényesül, ezért szükséges a hang és adatszolgáltatások hordozófelületét alkotó átviteli utak biztonsági megfeleléségi szintjének általános emelése.

Menedzsmentbiztonság

A távfelügyelet, menedzsment lényege, hogy a szakállomány közvetlenül az általa felügyelt rendszerrel kerül kapcsolatba, így ezen közvetlen összeköttetésen keresztül időszerű információkhoz jut a rendszer állapotáról és képes beavatkozni a fo-

lyamatokba. A hibaelhárítás lehetősége az ilyen kapcsolatban a lehető leggyorsabb, mivel legtöbbször így megtakarításra kerül a helyszíni kiszállás és munkavégzés anyagi ráfordítása, hiszen így az intézkedés, beavatkozás az esetek túlnyomó részében távoli pontról végrehajtható. Különösen a kiterjesztett hálózatfelügyelet növeli a megbízhatóságot, ráadásul humán erőforrások hatékonyabb kihasználását teszi lehetővé, így a hálózatgazda üzemeltetési ráfordításai jelentősen csökkennek. Másik nagy előnye, hogy a prevenció lehetőségével az üzemeltetési és karbantartási folyamat alacsonyabb költségekkel előre tervezhetővé válik.

A hálózat üzemeltetésének, fenntartásának, védelmének alapja a megfelelő menedzsment kialakítása. Ehhez a hálózatnak a menedzsment rendszerével együtt a szakirodalom általános kategorizálása szerint az integritás (hitelesség, sértetlenség, pontosság), a hozzáférési kontroll és titkosság, az elérhetőség és a megbízhatóság általános kritériumainak kell megfelelnie.

Mivel a hálózat- és menedzsmentbiztonság az egyik legfontosabb kritérium a távközlő hálózat tekintetében, így még nagyobb hiányossággént jelentkezik az a tény, hogy a tényleges biztonság és védetség tesztelése kiképzett szakállomány, vagy megbízott civil cég által jelenleg nem kerül végrehajtásra.

Jelenleg a digitális központok menedzselése ugyanazokon az átviteli utakon történik, melyeken a tényleges kommunikációs forgalom is zajlik. Ezen átviteli utakon keresztül kerülnek továbbításra többek között a felhasználónevek és jelszavak valamint ezeken történik az esetleges szerverek adatgyűjtési folyamata, adatlekérdezés, módosítás és egyéb felügyeleti és menedzsmenttevékenység is. Ezen átviteli utak nyíltak, illetéktelen hozzáféréssel szemben védtelenek.

A távfelügyelet biztonságának hatékonyságát egyfelől növelte az a kiépített lehetőség, mely szerint a digitális központok általában a PSTN⁴³-en keresztül másodlagos eléréssel is hozzáférhetővé váltak, hiszen így a zártcélú hálózattól történő esetleges elszigetelődés esetén is képes a menedzsmentállomány a távfelügyeletet, távkonfigurációt végrehajtani. Azonban ezzel ismét megnyílt egy nehezen nyomon követhető kapu az illetéktelen behatolók előtt. Bár jelszavas azonosítás szükséges a belépéshez, de amennyiben valaki által jogosan használható jelszóhoz egy jogosulatlan felhasználó hozzájut, akkor jelenleg észrevétlenül felléphet vele a kiválasztott központba. A hozzáférés biztonságosságának növelése érdekében javasolt a „dial-back” klasszikus biztonsági megoldás alkalmazása, azaz a felhasználó visszahívása. Ekkor a felhasználó bejelentkezik, majd bont a kapcsolat és a hívott eszköz, vagy a jelzést megkapó kezelő visszahívja (esetleg egy másik vonalon) a bejelentkezni kívánó felhasználót. Ezzel a felhasználó telefonszámának azonosítása megoldódik, így egy biztonsági lépéső kerül be a folyamatba. Ez a megvalósítás különösebb költségvonzattal nem jár.

A biztonság növelése céljából jól alkalmazhatók a nagy helyrajzi terjedelemben elhelyezkedő más eszközrendszerek távfelügyeleti lehetőségei kiegészítő távfelügyeleti- riasztási céllal. A Magyar Honvédség igen nagy kiterjedésű mikrohullámú hálózatának felügyeleti rendszere képes lekezelni egyes szigetszerűen kihegyezett eszközök távfelügyeletét, mely megoldás a biztonságosság fokát nagyban megemeli minimális költségfordításért cserében. Az ilyen lehetőségek széleskörű

⁴³ Public Switched Telecommunication Network Közcélú Nyilvános Távközlő Hálózat

kihasználása mindenképpen javasolt, hiszen a menedzsmentbe történő bevonás által kontrolálhatóvá válik ezen eszközök használata a tényleges forgalmazással egy időben és így lehetőség adódna a távfelügyeleti állományának a be nem azonosított, vagy illetéktelen hozzáféréseknél a kapcsolat megszakítására, kizárásra. A távközlési és informatikai terület bármely részén fenntartási szerződés keretében tevékenykedő külső, civil cégekkel való együttműködésnél kiemelten fontos feladat egy írásbeli szabályzás, melynek értelmében a civil szolgáltató szakembere bármely tevékenység megkezdése előtt köteles bejelentkezni a hálózatfelügyeletre az esetleges jelszavas azonosítástól függetlenül. Ennek szükségességének egyik indoka, hogy a cégek által alkalmazott és kijelölt szakemberek általában nem használnak külön személyes azonosítókat, csak egy globális, valamennyiük által ismert felhasználónevet és jelszót. Ezen jelszó esetleges szándékos, vagy véletlen kitudódásánál és illetéktelen felhasználásánál a hálózatfelügyeleti állomány csak ezen szabályzás esetén képes hatékonyan fellépni a támadással szemben.

Nagyobb gondot okozhat viszont az az illetéktelen felhasználó, aki egy tényleges jelszavat megszerezve a felügyeleti LAN-on keresztül éri el a célállomást, hiszen ez a hozzáférés észrevétlen marad, mivel minden mozzanat teljesen szabályosnak tűnik. Ezen illetéktelen felhasználó valós idejű elfogására jelenleg nincs mód, ezért is fontos nagy figyelmet fordítani a támadások megelőzésére mind a technikai oldalon és a humán oldalon is.

Menedzsment biztonsági kritériumai

A menedzsment biztonságát vizsgálva több oldalról közelíthetjük meg a problémát. E megközelítések az alábbiak:

- szükséges a menedzsmenttevékenység szigorú írásos szabályzása.
- védeni kell a hálózatot és menedzsmentet azon jelenség ellen, hogy a menedzsment tevékenység rejtése alatt esetlegesen illetéktelen hozzáféréssel szabadon belépve átjussanak a betolakodók a hálózat biztonsági védelmi lépéseiben.
- védeni szükséges a menedzsment által használt hozzáférési pontokat és lehetőségeket.
- védeni szükséges a menedzsment központi szervereit, annak duplikációit.
- szükséges a duplikált szerver élő adatbázissal ellátása.
- védeni szükséges a jelszóállományt illetéktelen kézre kerüléstől.
- kiemelten fontos a napló fájl védelme az illetéktelen behatoló nyomainak eltüntetésének megakadályozása céljából.

A Magyar Honvédség távközlő hálózata tehát igen sokrétű mind a szolgáltatásai mind az alapjait alkotó elemek, berendezések tekintetében. A hálózat részenkénti kezelése nem adhatja meg a teljes hálózat forgalmi és biztonsági optimalitását. Amennyiben az egyes részterületek esetleges rejtett hibáiról nem értesülnek időben más részterületek szakemberei, ez a látszólagosan jelentéktelen esemény a hálózat egészét tekintve végzetes probléma, hiba generálódásához vezethet.

Amennyiben lehetőség adódik, egy központosított hálózati, forgalmi, hibaelhárító és biztonsági menedzsment központ létrehozására, akkor a hálózat minden területén az optimálisabb és költséghatékonyabb megvalósulás alkalmazása válna lehetővé a már jelenleg meglévő infrastruktúrákra épülve.

Központosított telekommunikációs és biztonsági menedzsment

A már említett telekommunikációs eszközök, átviteli utak fenntartási menedzsmentje már működik, azonban az összefonódó távközlési és informatikai eszközök, szolgáltatások, a hálózati veszélyeztetettségek ugrásszerű növekedése indokoltá tesz egy olyan központosított menedzsmentet, mely a Magyar Honvédség zártcélú távközlő hálózatának magas szintű üzemi működtetését és védelmét is szolgálja.

A illetéktelen hozzáféréseű tevékenységek a hálózat működőképességét akár teljesen, de részlegesen mindenképpen megbéníthatják, valamint oly mértékű szakmai, anyagi és egyéb járulékos károkat okozhatnak, melyek nagyságrendi értékben sokszorosra a ráfordítandó biztonsági költségeknek. Napjainkban a betolakodók (pl. hackerek, crackerek) a hálózat sebezhető pontjait és a gyengeségeit könnyű szerrel feltérképezik és ezek után ezeket a réseket kihasználják. Ez a veszély már a zártcélú hálózatoknál is nagyon időszerű, hiszen a belső- és világhálók bizonyos esetekben akár csak gondatlan felhasználókon keresztül is érintkeznek. A támadások leginkább az adatcélú forgalmazásnál jellemzőbbek, de ezen forgalmazásba a mindent átölelő és kézben tartó menedzsmenttevékenység is beletartozik.

Mivel a felfokozott ütemben fejlődő hálózatot támadó oldal az illetéktelen hozzáférések lehetőségeinek újabb és újabb megoldását fejleszti ki és használja, ezért ezek elleni védekezésül időszerűvé válik, hogy a távközlő és informatikai hálózatok központosított menedzsmentállományába beintegrálásra kerüljön olyan elem, mely feladatai közé tartozna többek között:

- a felhasználónevek, jelszavak rendszer ellenőrzése;
- váratlan időpontú, területű belépések ellenőrzése (pl. hétvégén, munkaidőn kívül; felhasználó szabadságolási időszakában);
- bejárások alkalmával az eszközök, átviteltechnika biztonsági szempontok szerinti vizsgálata;
- esetleges illetéktelen felhasználás nyomon követése, jelentése;
- a naplózó fájl folyamatos elemzése biztonsági szempontok szerint is;
- behatolás detektálás;
- biztonságossági vizsgálatok végzése, betörési tesztek végzése szigorúan ellenőrzött keretek között.

A kiterjesztett feladatkörű hálózatfelügyelet tevékenységi körébe nem célszerű belevenni a fizikai őrzés- védelmi funkciókat, hiszen ezek helyi szolgálatok, biztonsági cégek által kerültek megoldásra, valamint nagy részben az országos szinten központosított regisztrált beléptető rendszerrel valósulnak meg. Bizonyos kiemelten védendő berendezéseknél viszont szükségesnek találom lehetőség szerint a fizikai belépési távriasztások bekötését a központosított menedzsmentközpontba is, vagy ahol nincs erre mód, ott a kapcsolattartási rend meghatározását a helyi őrzés- védelmi szervvel. Ezzel megeremtődne annak a lehetősége, hogy az egyébként észrevétlenül a fizikailag helyszínen megjelenő illetéktelen célzatú hozzáférést megkísérlő személyt (akár a tudatosan rosszszádekú, akár bejelentetlen például karbantartást, cserét végző szolgáltatói alkalmazott) a helyszínen beazonosítsák és irányába a megfelelő ellenlépéseket végrehajtsák.

A kiterjesztett menedzsment személyi megvalósulásának minimális akadályai lennének csak, hiszen az ezen funkciókat ellátó szervezeti elemnél a hagyományos telekommunikációs – és adatátviteli rendszerek forgalom- és hibafelügyeletére

rendszeresített beosztások jelenleg is szerepelnek, így minimális átszervezéssel a hálózatbiztonsági felügyeleti funkciókat is képes lenne ellátni megfelelő szakirányú képzést követően.

Összegzés

A nemzetközi és ezzel együtt a nemzeti biztonságpolitikai helyzet változása, a telekommunikációs, informatikai lehetőségek nagymértékű kiszélesedése új típusú veszélyeket hoz magával. A Magyar Honvédség zártcélú hálózatának vonatkozásában időszerűvé vált minden részterületre kiterjedő kockázatelemzés készítése, mely mérlegeli védendő különböző formátumú (hang, adat, stb.) információk, összeköttetések „értékét”, valamint alapul szolgál egy átgondolt, megalapozott stratégiára épülő biztonsági koncepció bevezetésének. Ezen koncepció bevezetése és betartatása és a kijelölt szerven keresztül folyamatos biztonsági ellenőrzések végzése magas szinten védetté tehetné a Magyar Honvédség zártcélú hálózatát az illetéktelen behatolásokkal szemben.

A műben említett javaslatok megfontolása esetlegesen lehetővé tenné egy oly forgalmilag hatékony, mindennemű biztonsági paraméternek megfelelő, általánosan védett hálózat megteremtését, mely megfelelő felügyeleti, biztonsági, fenntarási funkciókat ellátó központosított menedzsment mellett a kor mindennemű igényeinek képes megfelelni és általánosságban minden irányú támadás ellen védetté válik.

Irodalomjegyzék

- [1] Viasztó Tamás: Titkosítás és adatrejtés. Biztonságos kommunikáció és algoritmus védelem NetAcademia Kft. 2004.
- [2] Othmar Kvas: Számítógépes hálózatok biztonsága Kossuth 2000.
- [3] Dictionary of Information Technology Peter Collin Publishig 2002
- [4] Czirkóczy András: Távközlési hálózatok fejlődési iránya a következő 5- 10 évben Híradástechnika 2003 október pp. 9-15
- [5] Dr Kovács János, Rortmbacher Tibor, Horváth Gergely: Távközlési Hálózatok Közeli jövőképe PKI Tudományos napok 2003. november 20-21. (MATÁV Budapest 2003.) 862862003 ÜDI pp. 119-130.
- [6] Tannenbaum-Andrew S.: Számítógép hálózatok (Budapest, Novotrade 1992.)
- [7] Kassai Károly- Magyar Sándor: Zártcélú hálózat felügyeletének biztonsági kérdései. Új Honvédségi Szemle 2002/11.szám, 88-95.oldal, HU ISSN 1585-4167
- [8] Kassai Károly- Magyar Sándor: Híradó és informatikai rendszerek csomópontjainak védelmi kérdései. Felderítő szemle.

BETEKINTÉS SZERBIA ÉS BOSZNIA-HERCEGOVINA TÁVKÖZLÉSI PIACÁNAK PRIVATIZÁCIÓJÁBA.

A MATÁV-hoz hasonlóan számos külföldi társaság tekinget a Balkán távközlési hálózatainak privatizációja felé. Jelen esetben az általam megemlített két példában az osztrák „Mobilkom” kerül kiemelésre.

Az ausztriai „Mobilkom” vállalat a bolgár piacra való betörés mellett a szerb „Mobtel” meghódításán is gondolkodik. Itt azonban először a tulajdoni viszonyokat lenne szükséges rendezni, hogy elkerüljék a későbbiekben az esetleges vitákat.

A „Mobtel” értéke osztrák szakértők szerint 5-600 millió euró. A vállalat jövedelmének nagy részét partner-megállapodásokon keresztül történő szolgáltatásokkal valóítja meg. A „Mobtel” eladásával a potenciális tulajdonos a vállalattal együtt ezeket a megállapodásokat is megvásárolja, amik a pár százmillió eurós hitel, hitel korlátozások és jelzálog mellett jelentősen csökkentik a vállalat értékét. Fennáll annak a veszélye, hogy a „Mobtel” ezen szolgáltatásainak lebonyolítását magába foglaló szerződéseket nem, vagy csak nagyon kedvezőtlen feltételekkel lehet felbontani.

A „Mobtel” új tulajdonosa jobb szolgáltatásokat fog magával hozni, az előfizetők több, kedvezményes csomag közül választhatnak majd, alacsonyabb árak mellett, mert a „Mobilna telefonija Srbije” (Szerb Mobiltelefon Társaság) egyre nagyobb konkurenciát jelent a „Mobtel” hálózatnak.

Technológiailag a „Mobtel” ugyan elérte határait, de várhatóan az új tulajdonos agresszíven fog harcolni, hogy minél több előfizetőt nyerjen meg.

A liszensz ára 50-70 millió eurót tenne ki, ami nem nagy összeg, ezzel azonban mindkét mobiloperátor értéke lecsökkenne.

Egy jó megoldás lehetne, ha az állam felajánlaná a 3. generációs mobiltelefon liszenszének kiválását. Magáért a liszenszért az állam nem kapna semmit, de hosszú időre tervezve az adók beszedésével már sokat nyerhetne. Vagyis az állam világosan definiált és szigorú feltételekkel biztosítja ennek a hálónak a fejlődését, ezért cserébe pedig jövedelmet kap. Ez a telekommunikáció fejlődésének és a költségvetési bevételek új modellje.

Az osztrák „Mobilkom” Bosznia-Hercegovinában is ajánlatot tett, ott az „Eronet” részvényeinek megvásárlására, 24 millió euró értékben. A „Mobilkom” mellett a német „Deutsche Telekom” is ringbe száll az „Eronet” részvényeiért. A vállalat részvényeinek 50,5%-t a „Hercegovacka banka” birtokolja a „Hercegovina osiguranje” (Biztosítótársaság) közreműködésével, valamint az „Alpina komerc” vállalat és Grude település. A maradék 49% tulajdoni részt a „HT Zagreb” (Horvát Telekommunikáció, Zágráb) birtokolja, amely a „HT Mostar” részvényese is.

Az osztrákok további kedvezményeket is felajánlottak, mint például egy 200 000 millió eurós értékű infrastruktúra befektetés Grudében. Ezzel egyidőben a „Hercegovina osiguranje” megkapná az „Eronet” biztosítási-, míg valószínűleg az „Alpina komerc” kapná az új mobiltelefon bázisállomások felállításának üzletét. Ugyanakkor ez „Eronet” többségi tulajdonosai tisztában vannak azzal, hogy elővásárlási joga van a részvényekre a „HT Zagreb”-nak, amely mögött viszont a „Deutsche Telekom” áll.

A liszenszet végül július közepén a „Hrvatski telekom Zagreb”-nak ítélték oda (ahogy az várható is volt, mivel a maga 49%-val az „Eronet” legnagyobb egyéni tulajdonosa), mire válaszként a „Hercegovina” Biztosítótársaság és Grude település panaszt nyújtottak be arra hivatkozva, hogy a „HT Mostar” nem képes biztosítani a mobiltelefon szolgáltatásokat. Neheztelnek továbbá a zágrábi partnerre is, amely szakértők véleménye szerint nyíltan feláldozta az „Eronet” érdekeit, hogy többségi részvénytulajdonos lehessen a „HT Mostar”-ban. A „HT Zagreb” felajánlotta a Bosznia-Hercegovinai Föderáció kormányának 49%-os „Eronet” részvénytulajdonát, cserébe pedig részesedést kért a „HT Mostarba”-n, aminek a Bosznia-Hercegovinai Föderáció kormánya a többségi tulajdonosa.

A privatizáló fél részéről várható egy olyan stratégia bemutatása, amelynek a célja minél több előfizető megnyerése, ami természetesen magában foglalja a szolgáltatások árának csökkentését is. Ezen kívül tervezik egy minőségibb és szélesebb körű mobil szolgáltatás elindítását, amelyet jelenleg egyetlen GSM hálózat sem tud nyújtani ezen országokban.

Irodalomjegyzék

- [1] „Drzava vecinski vlasnik Mobtela” In: www.novosti.co.yu/ekonomija, 2004. Június 24.
- [2] I. KRASNIC: „Branislav Andelic: Mobtel vredi do 600 miliona evra” In: www.glas-javnosti.co.yu/ekonomija, 2004. Július 25.
- [3] „Mobilkom kupuje 063?” In: www.glas-javnosti.co.yu/ekonomija, 2004. Július. 17.
- [4] „Austrijski Mobilkom i Deutsche Telekom natjecu se za treceg GSM operatera u BiH” In: www.vjesnik.hr/gospodarstvo, 2004. Június 24.
- [5] M. CUBRO: „Hrvatska zeli da spoji Eronet i HT Mostar” In: www.nezavisne.com/dogadjaji, 2004. Július 18.
- [6] www.vecernji.list.hr/vijesti/bih, 2004. Június 23.
- [7] A. OMERAGIC: „Suvlasnici Eroneta nezadovoljni zbog dodjele GSM licence” In: www.oslobodjenje.co.ba, 2004. Július 14.
- [8] A. OMERAGIC: „Regulatorna agencija za komunikacije odlucila” In: www.oslobodjenje.com.ba, 2004. Július 13.
- [9] www.vecernji-list.hr/vijesti/bih, 2004. Július 14.
- [10] M. CUBRO: „Treci GSM operater bice zajedno HT Mostar i Eronet” In: www.nezavisne.com/ekonomija, 2004. Július 09.
- [11] Z. KRESIC: „HT Mostar i Eronet zajedno ce dobiti trecu GSM licencu” In: www.vecernji-list.hr/vijesti/bih, 2004. Június 25.
- [12] www.mobtel.co.yu
- [13] www.telekomunikacije.co.yu
- [14] www.063.co.yu

Dr. LINDNER Miklós

PUSKÁS TIVADAR A NAGY MAGYAR FELTALÁLÓ SZÜLETÉSÉNEK 160. ÉVFORDULÓJÁRA

Dr. Lindner Miklós nyá. vezérőrnagy
a Puskás Tivadar Híradó Bajtársi Egyesület elnöke

A ZMNE Katonai Kommunikációs és rendszerszervező tanszéke által gondozott immár hagyományossá vált technikai konferencia időpontja ez évben egybeesik a nagy magyar feltaláló és hazafi Puskás Tivadar születésének 160. évfordulójával. E jelentős dátum - a Honvéd Vezérkar Híradó és Informatikai Csoportfőnöksége és a Puskás Tivadar Távközlési Technikum összehangolt előkészítő munkája eredményeként - az egyetemes kommunikáció kiemelt eseményévé vált, amelynek egyik kiemelkedő szegmense jelen konferencia is.

Az évforduló kiemelt jellege indokolja, hogy e konferencián ismételten áttekintsük Puskás Tivadar életét, munkásságát és tisztelegjünk a nagy magyar hazafi immár teljes fényében ragyogó emléke előtt.

E konferencia résztvevőinek rangos összetétele, a konferencián elhangzó előremutató referátumok, a jövőt kereső és a jövőt álló megoldások azt bizonyítják, hogy az egyetemes kommunikációban tevékenykedő magyar szakemberek méltó örökösei a „puskási” gondolatoknak a kommunikáció - benne a katonai kommunikáció - erőinek, eszközeinek, rendszereinek racionális továbbfejlesztése területén. Jelen konferencián - az előző konferenciákhoz hasonlóan - jeles szakemberek előadásaiban, javaslataiban összegeződnek azok az erőfeszítések, amelyek fókuszában az információs társadalom által a kommunikáció iránt támasztott követelmények mindenoldalú biztosítása áll.

Kérem, hogy engedjék meg, hogy mint a Puskás Tivadar Híradó Bajtársi Egyesület elnöke e jeles évforduló alakalmából méltassam a hosszú időn át méltatlanul mellőzött, agyonhallgatott nagy magyar feltaláló és hazafi munkáját és emlékét.

Régi adósságot törlesztett 5 évvel ezelőtt a Vk. Híradó Csoportfőnökség, amikor a Puskás Tivadar Távközlési Technikum vezetésével karöltve a "Puskás Tivadar Tudományos Emlékhét" keretében - a médiák tevékeny közreműködésével először állította reflektorfénybe a nagy magyar feltalálót.

Puskás Tivadar azok közé a magyar hazafiak közé tartozik, akit a reformkor szellemét követő deáki kiegyezéssel járó elodázhatatlan gazdasági fejlődés igénye állított a közérdeklődés középpontjába. A kor, melyben élt és dolgozott a nemzet függetlenségéért, a polgári átalakulásért, az önálló gazdasági felemelkedésért vívott állandó harc időszakára volt.

Széchenyi István álmainak fokozatos megvalósulását jelentették azok az események, melyek a XIX. század II. felének Magyarországot jellemezték, melyek nagy hatást gyakoroltak a fiatal Puskásra, aki nem csak a műszaki fejlesztés elkötelezett híve, hanem jó érzékkel megáldott üzletember is.

Miközben a nemzeti ipar létesítményei kialakulnak Puskás érdeklődési köre túllép Az Osztrák- Magyar Monarchia országhatárain. Érdeklődésének középpontjában Anglia áll, amely ez időben Európa legjelentősebb ipari országa köszönhető a gőzgép feltalálásának, kiterjedt gyarmatbirodalmának.

Az osztrák Teresianumban megszerzett diplomát követően Angliában tanul, majd Erdélyben egy angol vasútépítő cég alkalmazottjaként vasútépítéssel foglalkozik.

Magyarországon az 1867. évi kiegyezést követően felgyorsult a külföldi tőke beáramlása, gomba módra alakulnak bankok, hitelintézetek, szövetkezetek. Gyárak, gyártelepek, malmok épülnek, fejlődik a kereskedelem. Ez parancsolólag követeli a közlekedési infrastruktúra mielőbbi gyors kiépítését.

A nemzetközi munkamegosztás megvalósulásának reménye új távlatokat ígér. Ennek szép példája az 1873. évi bécsi világkiállítás, ahol a kor másik nagy magyar műszaki zsenije Jedlik Ányos mutatta be az általa szerkesztett dinamót, melynek elvét 6 évvel a német Siemens előtt álmodta meg.

Puskás nagy érdeklődést mutatott az új világ, az Amerikai Egyesült Államok és annak ipara iránt. Nagyra értékeli a Függetlenségi Nyilatkozatot. Ez időben Amerika ténylegesen a korlátlan lehetőségek hazája, a különféle bevándorolt népek tömegeinek olvasztótégelye. Puskás 30 éves korában Amerikába utazik. Első időkből - a korabeli romantika jegyében - aranyásással is foglalkozik, majd a világ nagy műszaki zsenije Edison közeli munkatársa lesz, akitől sokat tanul. Egymás iránti kölcsönös érdeklődésük tartós barátsággá és üzleti kapcsolattá fejlődik. A tőke koncentrációja már zömében létrehozta az infrastruktúrát Amerikában, az ipar termel, a közlekedés fejlődik, de ezt csak nagyon rossz hatásokkal tudják irányítani.

Már van ugyan távírógép, de összefüggő, továbbkapcsolható, szelektív hálózat hiányában határfoka gyenge, áteresztőképessége minimális, esetenként katasztrofális, szinte gátja a gazdaság további fejlődésének. E közben Bell 1876-ban feltalálja a telefont, ami világszenzáció, azonban csak pont-pont között használható. Ez viszont nem felel meg az egyre jobban prosperáló gazdaság sokrétű igényeinek. Puskás jó érzékkel ismeri fel a gazdaság vezetésének problémáját, és ennek megoldása foglalkoztatja.

Ötlete, hogy olyan berendezést kell létrehozni, mely segítségével a telefonok tettesz szerint célirányosan egymással összekapcsolhatók. Az ötletet valóra váltja, ami fényesen igazolja a hozzáfűzött reményeket. Amerikában 1877-78-ban létrejönnek az első Puskás elvén működő telefonközpontok. Mint Edison barátja és európai képviselője 1879-ben elkészül első európai telefonközpontjával Párizsban. A központ építését nem kíséri a jogosan elvárható társadalmi támogatás. Már 1878-ban felmerül benne egy hazai telefonközpont megépítésének gondolata. E gondolatot öccse Ferenc is magáévá teszi és támogatja a gondolat megvalósítását.

A magyar arisztokrácia feudális beidegződése, a kivárássra játszó óvatossága az égető gyakorlati igény ellenére meggátolja a szükséges hitelek felvételében. Puskás így saját finanszírozásában hozta létre 1881-ben az első 200 vonalas telefonközpontot Budapesten, mely a XIX. századi Magyarország egyik kiemelkedő műszaki létesítménye, ami a közelmúltban két városrészből egyesített fővárost Európa egyik legjelentősebb fővárosává emelte.

1884-85-ben jelentős hálózat építésre és a nyilvános állomások telepítésére került sor. Puskás a hálózatot saját pénzén fejlesztette. Miután hitelfelvételi forrásai nem voltak, saját anyagi lehetőségei kimerültek, a fejlesztés megtorpant.

1888-ban Baross Gábor hazánk kiemelkedő gazdaságpolitikusa, közmunka és közlekedési minisztere, a "vasminiszter" felismerte, hogy a beindult gazdasági növekedés érdekében - a vasút mellett - a távközlési infrastruktúra gyorsabb fejlesztése szükséges

ezért a hálózatot állami kezelésbe vette. Így a fejlesztést az állam finanszírozta, de szakértelmével Puskás részt vett a munkában.

Baross 1888-ban törvényjavaslatot nyújtott be, mely elfogadását a követően 1888. évi távbeszélő törvényként látott napvilágot.

E törvény kimondja: „A berendezések létesítésére és üzemeltetésére vonatkozó műszaki és eljárási szabályokat a közmunka és közlekedési miniszter állapítja meg”, továbbá „a ház és földtulajdonosok kártérítés nélkül eltérni tartoznak, hogy a közhasználatú távbeszélők és villamos jelzők huzalai épületeik és földjeik felett elvezetessenek (illetve azok) az épületekre vagy azok tetőzetére való felerősítését és bekapcsolását eltérni kötelesek”. Talán van valami hasonlóság a hatályos távközlési törvényünkben (1992. évi LXXII. törvény) és 1999. évi júniusi módosításában (1999. évi LXVI. törvény).

E törvény lényeges előrelépést jelentett:

- a fejlesztési tervek megvalósítása
- a kettős vezetékre való áttérés
- a helyközi kapcsolatok fokozott kiépítése terén

1893-ban - röviddel halála előtt - megalkotta a telefonhírmondót, mellyel a telefónia és az újság ötvözetéből egy világgraszoló kommunikációs lehetőséget varázsol a századvég elképedt közvéleménye elé. Ezt tartjuk a közszolgálati rádióhír szórás őseinek.

A később megalakult Magyar Rádió kezdetben Magyar Telefonhírmondó és Rádió Rt. néven működött. Ennek tárgyi emlékei megtalálhatóak a ma még több helyen - többek között a Gellért fürdő előcsarnokában - működő egykori villamos órák számlapjának feliratán.

Mit köszönhet az egyetemes magyar hírközlés - benne a Magyar Honvédség híradó szolgálata - Puskás Tivadarnak. Elsősorban azt, hogy találmányaival erősítette Magyarország nemzetközi tekintélyét.

Tevékenységevel bebizonyította, hogy egy európai kis nép fiai a világ élenjáró tudósai között - a népesség számából származtatható többszörösen meghaladó számban - foglalhatnak helyet. Gondoljunk csak a műszakiak közül Jedlik Ányosra, Bláthy Ottóra, Zippervosky Károlyra, Ganz Ábrahámra, Bánki Donátra és a többiekre, továbbá legújabb kori történelmünk Nobel díjasaira. Köszönhetjük Puskásnak az is azt, hogy a XX. század elején Magyarországon jelentős híradástechnikai ipar jött létre (Standard, Siemens, Orion) és ezek több generáción át kitűnő szakember gárdát neveltek, amelyek hatását még ma is érzékeljük.

Ha Puskás Tivadar találmányainak katonai vonatkozásait vizsgáljuk, úgy a fejlődés a haderő híradó szervezeteinél is megindult.

A XIX. század végén szörványosan, az első világháborúban már nagyobb számban jelentek meg a katonai híradás esetenként kezdetleges eszközei melyek a katonai vezetés nélkülözhetetlen elemeit képezték.

Az 1930-as évek Magyar Királyi Honvédségének voltak Puskás elven épített 10-es, 30-as, központkapcsolói, 2-4 Néper erősítési tényezővel rendelkező tábori vonalerősítői, tábori könnyű és nehézvezetékes alegységei. Távirógépek, közepes és nagyteljesítményű rádiói melyek az 1950-es évekig a Néphadsereget is kiszolgálták. (R-3, R-7 stb.) Az 1940-es években kerültek rendszerbe a Hell aritmikus és a Siemens ritmikus távirógépek.

Az I. és II. világháború valamint az ötvenes évek katonai híradóeszközei megtalálhatók a Bolyai János Katonai Műszaki Főiskola igényesen és szakszerűen rendezett és állandóan bővülő Híradó Múzeumában, amelyet a híradó tanszék gondoz, őszinte köszönet érte Dr. Koczka Ferenc ezredes úr híradó és telematikai tanszékvezető vezetete tanszéki kollektívának. A kiemelkedő eredményességgel működő híradástechnikai ipar katonai produktumai minden területen megfeleltek a velük szemben támasztott követelményeknek.

Kiemelkedően magas színvonalon állt a katonai vevőberendezések tervezése és gyártása. Némely típusért a tervezők Állami díjban részesültek. Panorámavevőket, központkapcsolókat 10, 20, 40, 80, 160 kapacitással a hazai ipar gyártotta.

A vezetékes eszközök között találjuk a tábori könnyű és az egységes nehézvezeték melyen géppel építve hazai gyártású vivőfrekvenciás berendezésekkel - az adott vezetékes szinttől függően -12-24-36-48 csatornás összeköttetések létesíthetők.

Talán nem tűnik szerénytelenségnek, de a hadsereg híradó szolgálata rendelkezett az országban először GHz-es sávban működő digitális mikrohullámú rendszerrel, melynek létrehozásában a magyar ipar, az Orion, míg üzemeltetésében az akkori Magyar Posta Rádióműszaki Igazgatósága, jelenleg az Antenna Hungária Rt. nyújt sokoldalú segítséget,

Hazánkban a NATO-ba történő felvétele kapcsán természetesen új eszközök, új szervezési elvek, és új módszerek kerülnek a híradó szolgálat birtokába. Ezek az új eszközök és módszerek egy tekintetben változatlanok, magukon viselik Puskás Tivadar zseniális felfedezését, amelyek az állomások tetszésszerű összekapcsolásának elvében, valamint a rádió hírszórásnak, ha úgy tetszik a rádióhíradásnak a telefonhírmondóból történő származtatásában jut kifejezésre.

A VK. Híradó és Informatikai Csoportfőnökségnek távlati fejlesztési tervében a stacioner és tábori hírendszer teljes digitalizálása szerepel, ami előreláthatólag 2013-ig valósul meg. E témában a tanszék két fiatal oktatója Dr. Rajnai Zoltán és Dr. Fekete Károly értekezései tartalmaznak értékes gondolatokat.

Puskás Tivadar viszonylag rövid élete bizonyítja, hogy a célok világos megfogalmazása, az emberi akarat és leleményesség produktuma évszázadokon és kontinenseken átnyúló megbecsülést vált ki a hálás utókorból.

Ma a hálás utókor meghajtja az elismerés és az emlékezés zászlaját a nagy hazafi előtt. A Puskás Tivadar Híradó Bajtársi Egyesület, amelynek célja az alapszabály szerint - az aktuálpolitikától fényévnnyi távolságot tartva- a híradással foglalkozó szakemberek összefogása, az együvé tartozás érzésének kialakítása, az egyetemes magyar híradó szolgálat becses értékeinek és hagyományainak megőrzése, sokat tehet e nemes célok megvalósításáért. Egyesületünk várja a hivatásos és nyugállományú katonákat, polgári szakembereket, a szolgálattal kapcsolatban álló szervezetek dolgozóit, munkatársait.

Mindannyiunk közös és megtisztelő kötelessége a jövő híradó szolgálatának kialakítása Puskás Tivadar alkotó szellemének megőrzése és ápolása, az információs társadalom felépítésében való aktív részvétel.

E nemes feladathoz kívánok valamennyi jelenlévőnek jó erőt-egészséget.

Köszönöm megtisztelő figyelmüket.

**A JELENLEGI SÁVSZÉLESSÉG KIHASZNÁLÁSÁNAK
LEHETŐSÉGEI MULTISZOLGÁLTATÁSÚ KAPCSOLÓKKAL
A MAGYAR HONVÉDSÉG KATONAI KOMMUNIKÁCIÓS
RENDSZERÉBEN**

A távközlési és informatikai rendszerek fejlődésével egyre jobban előtérbe kerülnek a nagyobb sebességet igénylő alkalmazások, amelyeknél a rendelkezésre álló átviteli sebesség, illetve a jelenlegi csatornák kihasználása nem megfelelő. A mindennapi életben a multimédiás alkalmazások terjedése már megszokott, egyre jobban teret nyer az Internet, a papír alapú nyilvántartások helyét a digitális adatbázisok veszik át, az átvitelre kerülő adatállományok mérete növekszik. A több telephellyel rendelkező vállalatok esetében a telephelyek közötti kommunikációban a meglévő sávszélességek kihasználása egyre inkább nagyobb szerepet kap.

A kommunikációs hálózatok fejlesztése többnyire magas anyagi ráfordítású beruházásokkal valósítható meg. A jövő kommunikációjának hatékonysága érdekében azonban ennek kiemelten fontos szerepet kell kapnia. Ez az a terület, amelynél a takarékoság visszavetheti a fejlődést, illetve megfontolt költségfordítással látványos eredmények érhetőek el. A civil életben a vállalatok sikerességének egyik mércéje a kommunikációs hálózatuk fejlettségi szintje. A gyorsabb, jobb minőségi paraméterekkel rendelkező rendszerekkel nagyobb hatékonyság érhető el.

A kommunikációs hálózatok egyik meghatározó alkotóelemei a kapcsolóközpontok és az ezeket összekötő távközlési vonalak. A központokat többféle módon lehet összekötni: hálózat kiépítésével, illetve kommunikációs vonalak bérlésével. Mindkettő magában hordozza az előnyöket és a hátrányokat. Abban az esetben, amikor mi építetjük ki a hálózatot igen magas egyszeri beruházási költség lép fel, viszont annak a fenntartása lényegesen költséghatékonyabb. Meg kell venni a végberendezéseket, a csatornáképző eszközöket. Amennyiben saját telephelyeinken kívül kell valamilyen berendezést telepíteni akkor az eszközök elhelyezéséért, áramfelhasználásáért, őrzés-védelméért stb. fizetni kell. A kommunikációs vonalak bérlése esetén az egyszeri beruházás mértéke alacsony és bár a belépési díjak költsége a vonalak bérlési idejétől függően elenyésző lehet, azonban ebben az esetben a csatorna sebességétől, földrajzi helyétől függően minden hónapban vonalbérleti díjat kell fizetni.

Az új csatornák kiépítése mellett fontos cél, hogy a meglévő távközlési csatornákkal jól tudjunk gazdálkodni, kihasználásuk optimális legyen. A hálózatfelügyelet egyik fontos feladata a forgalom-felügyelet, amelynek nagy jelentősége van a csatornák telítettségének feltérképezésében, a szabad kapacitások kihasználásában. A nem megfelelően irányított hálózatban sok esetben előfordulhat túlcsoordulás, amikor az adott csatorna nem képes a további igények kiszolgálására. Ezért a hálózat irányítását a kerülő irányokat minden esetben tervezni kell. Az útvonal irányítás mellett új eszközök beiktatásával is lehet a csatornák kapacitásait növelni.

Jelen előadásban a Magyar Honvédség kommunikációs rendszerének az objektumok közötti meglévő sávszélességek hatékonyabb kihasználására helyezem a hangsúlyt.

Jelenlegi helyzet

A teljesség igény nélkül a Magyar Honvédség kommunikációs hálózatán belül a kapcsolóközpontok és az átviteli utat szolgáltató átviteli berendezéseket vázolnám fel.

Az állandó telepítésű kapcsolóközpontok közötti átviteli utak állhatnak egyrészt a szolgáltatóktól bérelt vonalszakaszokból, másrészt saját tulajdonú összeköttetésekben. A saját tulajdonú összeköttetések nagy része mikrohullámú átviteli berendezések segítségével valósul meg, kisebb része különféle típusú kábeles összeköttetés.

A mikrohullámú berendezéseket Totáltel Kft. telepítette kapacitásukat tekintve 2x2; 4x2, 8x2, Mbps-os sebességűek. Biztosítják a kapcsolóközpontoknak, az informatikai és más rendszereknek szükséges sávsebességet. Az nx2 Mbps-os csatornák PDH⁴⁴ szervezésűek.

A Magyar Honvédség nagy részében már Siemens Hicom ISDN⁴⁵ központ került telepítésre. Az analóg központokra jelen előadásban nem térek ki, mivel ezek tovább nem fejleszthetőek, a digitális összeköttetések szempontjából nem hasznosíthatók (EPF-512, EPF-128, EPF-32, EPK-128/Z, ARM- 503, ARF102/A, RA-15, CA-42V, QA-96, RX-30). A digitális kapcsolóközpontok tekintetében cél egy homogén, egységes, minden részében felügyelhető hálózat kiépítése.

A Hicom központok a kor színvonalának megfelelő ISDN központok. Jellemzőjük, hogy moduláris felépítésűek a központ méretétől függően tetszés szerint bővíthetőek. Típusai: Hicom 310 H, 330 H, 350 H, ahol a „H” betű a szoftververziót jelenti, a szám pedig a központ nagyságára (portszámára) utal. A korábbi típusokat „E” betűvel jelölték. Mindegyik típusban ugyanazok a perifériakártyák használhatóak. A perifériakártyák lehetnek fővonaliak illetve mellékoldaliak. A mellékoldali kártyákat is tovább bonthatjuk analógra, illetve digitálisra. A fővonal kártyák közül kiemelném a 2 Mbps-os kártyát, melyen létesíthetünk másik központtal társközponti (hálózati) kapcsolatot, vagy végződtehetünk például MATÁV (vagy más közcélú szolgáltató) által biztosított primer ISDN (ISDN30) csatlakozást. Az ISDN alapcsatlakozás (ISDN2) számára alkalmas kártya segítségével ugyancsak létesíthetünk központok közötti társközponti kapcsolatot, de ezen keresztül csak két beszédcsatorna áll rendelkezésre, továbbá végződtehetjük a MATÁV (vagy más közcélú szolgáltató) által biztosított ISDN alapcsatlakozást.

Mind a 2 Mbps-os, illetve az ISDN alapcsatlakozás végződtesére alkalmas kártyával a hálózati kapcsolat létesítése esetén a központok közötti hálózati szolgáltatások érvényesíthetőek (visszahívás kérés, hívószám kijelzés, stb).

Az ISDN központokra jellemző, hogy gyors kapcsolat-felvételű, széleskörű szolgáltatásokat biztosító központok. Az ISDN beszédcsatornák 64 kbps-os sebességűek, így a primer ISDN 30 darab beszédcsatornát és egy 64 kbps sebességű adatcsatornát tartalmaz, az ISDN alapcsatlakozás pedig 2 beszédcsatornát és egy 16 kbps sebességű adatcsatornát. A 64 kbps-os beszédcsatornák nagyon jó minőségűek, de a sávsebesség kihasználása szempontjából nem optimálisak. Bizonyos szempontból ez a sebesség lehetne ideális, például ha ezeket a csatornákat 64 kbps-os adatátvitelre akarjuk használni, de ez ritkán fordul elő. A multimédiás eszközök számára (például: vide-

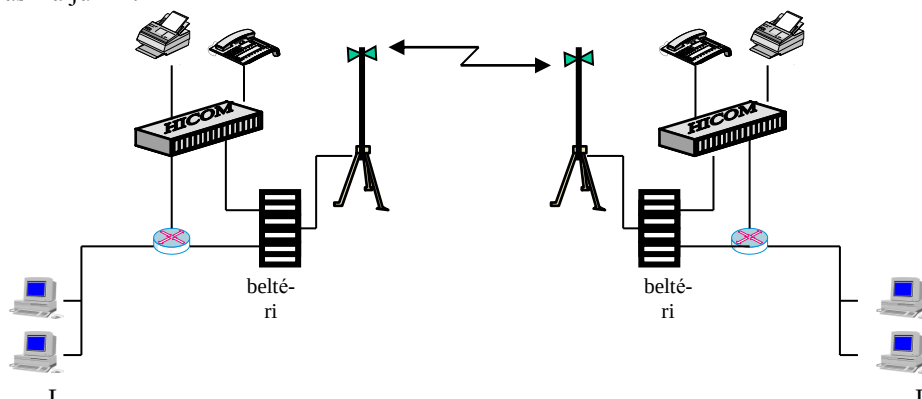
⁴⁴ PDH (Plesiochronous Digital Hierarchy) Pleziokrón Digitális Hierarchia

⁴⁵ ISDN (Integrated Services Digital Network) Integrált Szolgáltatású Digitális Hálózat

otefon) ez a sebesség nem ad elég komfortérzetet a beszélgetés során, a kép szaggat, a beszéd késhet, ezért nagyobb sebesség szükséges. A Hicom központokban a beszédcsatornák összefoghatóak H csatornába (nx64 kbps) de ez a megoldás nehézkes. Beszédcélra a 64 kbps-os sebesség csökkenthető olyan módon, hogy az érthetőség nem változik. Két Hicom központ közötti kommunikáció során használható hangtömörítés, melyet egy külön kártya végez. A tömörítés segítségével 15 nem tömörített beszédcsatornából 4 tömörített, míg 7 nem tömörített beszéd-csatornából 2 tömörített csatornát képes képezni attól függően, hogy milyen kártyára csatlakozik.

A 1. számú ábrán kiragadtam egy megoldást a Magyar Honvédség távközlési és informatikai hálózatának megoldásából. A rajz pusztán elveket és lehetséges kapcsolatokat tartalmaz olyan felépítésben, amelynek továbbfejlesztése lehetséges az átviteli sebesség növelése nélkül.

A kommunikációs csatornát a rajz szerint mikrohullámú berendezés biztosítja, de jelen esetben akár szolgáltató által biztosított 2 Mbps-os bérelt vonal is lehet. A mikrohullámú hálózat és átvitelt pontjai jelen esetben nem lényegesek. A Hicom központok a mikrohullámú berendezés beltéri egységére csatlakoznak 2 Mbps sebességgel, vagyis 30 darab beszédcsatorna áll egy időben rendelkezésre. Ez a 30 csatorna a központ által kiszolgált szervezet(ek) tekintetében lehet sok, kevés, vagy ideális esetben elég. Ha kevésnek bizonyul, abban az esetben a hálózaton túlcsoordulás léphet fel, vagyis nem tudunk a másik objektumba újabb hívásokat (beszéd, fax, adat) kezdeményezni. Amennyiben sok a szabad csatorna akkor pedig a kapacitásunkat nem használjuk ki.



1.számú ábra A Magyar Honvédség jelenlegi távközlési és informatikai hálózatának egy lehetséges egyszerűsített változata

Az informatikai hálózat a rajz szerint külön szeparált hálózatként csatlakozhat a mikrohullámú beltéri egységére, ebben az esetben a Hicom központtól függetlenül rendelkezik valamely Hicom-tól független 2 Mbps-os sávszélességű összeköttetéssel, vagy a Hicom központra csatlakozik de itt csak nx64 kbps-os átviteli sebesség realizálható a Hicom közötti csatornák felhasználásával. A mennyiben a Hicom központokhoz csatlakozik, akkor célszerű a két eszköz közötti csatornák számát maximálni, mivel egy esetleg rosszul beállított informatikai eszköz a két telefonközpont közötti összes csatornát lefoglalhatja.

A sávszélesség hatékonyabb kihasználása

Jelen előadásban két eltérő megoldásra teszek javaslatot a távbeszélő csatornák számának megfelelően, hiszen előfordulhatnak olyan szervezetek, amelyben az informatikai alkalmazások kerülnek előtérbe és a külső és belső távbeszélő igény elenyésző (például 1-6 mellék), továbbá ahol a távbeszélő összeköttetés ugyanakkora prioritással bír.

Dinamikus csatornakihasználás multiszolgáltatású kapcsolókkal

A rendelkezésre álló sávszélesség optimális kihasználása érdekében a jelenlegi rendszer kiegészíthető multiszolgáltatású kapcsolókkal. A multiszolgáltatású kapcsoló felfogható egy sávszélesség menedzselő eszközként. A csatornát nem nx64 kbps-os csatornaként kezeli, hanem IP⁴⁶ alapon, Frame-Relay eszközként, kielégítve a QoS⁴⁷ követelményeit. A beszédcsatornákat tömörítve (8-16 kbps) képesek átvinni, ezzel jelentős sávszélességet megtakarítva. A különböző beszéd, adat, faxforgalom egy csatornába történő beintegrálásával IP csomagokként továbbítva további jelentős sávszélesség szabadítható fel. A rendszerben csak akkor keletkezik terhelés, amikor adatforgalom bonyolódik, így az egyes alkalmazások számára a csatorna teljes sávszélességében rendelkezésre áll. Szemben az ISDN nx64 kbps-os beszédcsatornáival, ebben a rendszerben a tömörített beszéd is csak akkor kerül átvitelre a csendelnyomásnak köszönhetően, amikor éppen beszéd folyik. A rendszer fontos követelménye az előzőekben leírt szolgálatok prioritásának megfelelő beállítása. Vannak olyan átviteli rendszerek, ahol a késleltetés nem okoz különösebb problémát, de a beszédben ez zavaró lehet.

A multiszolgáltatású eszközök kiegészíthetőek (például a WAN⁴⁸ és levelező rendszerek esetében rejtjelző berendezéssel), amellyel teljesen zárt hálózatokat tudunk létrehozni.

A következő két lehetséges megoldás esetében pont-pont összeköttetések láthatóak de ilyen rendszerekkel hálózatok is kiépíthetőek.

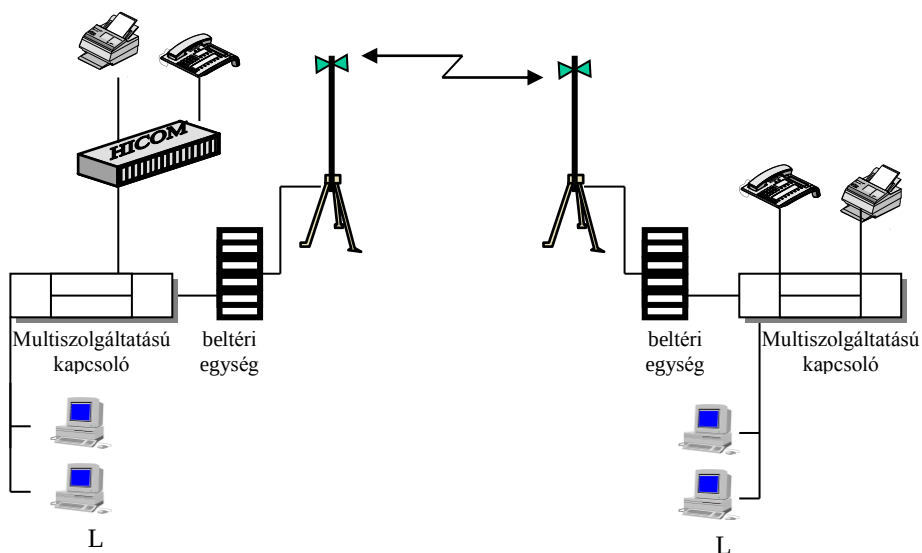
Alacsony számú távbeszélő összeköttetés esetén

Olyan esetekben, ahol az adott végpontokon a távbeszélő mellékek száma igen alacsony, multiszolgáltatású kapcsoló használatával nem szükséges távbeszélő központot telepíteni, illetve a központ kiváltható és olyan helyre telepíthető, ahol arra nagyobb szükség van. A multiszolgáltatású kapcsolók képesek távbeszélő összeköttetéseket létesíteni. Mint a 2. számú ábrán látható az egyik oldalon a multiszolgáltatású kapcsoló csatlakozik a Hicom központhoz. A Hicom központtal összekötve a másik oldalon képes szolgáltatni – igaz analóg módon – a központ távbeszélő mellékeit. A Hicom rendszerben az irányítás beállítása után a mellékállomások belső mellékként jelentkeznek. Ezek az analóg távbeszélő csatornák jelentéktelen sávszélességet foglalnak el. A sávszélesség így közvetlenül az adatátviteli rendszerek részére felhasználható.

⁴⁶ IP (Internet Protocol) Internet protokoll

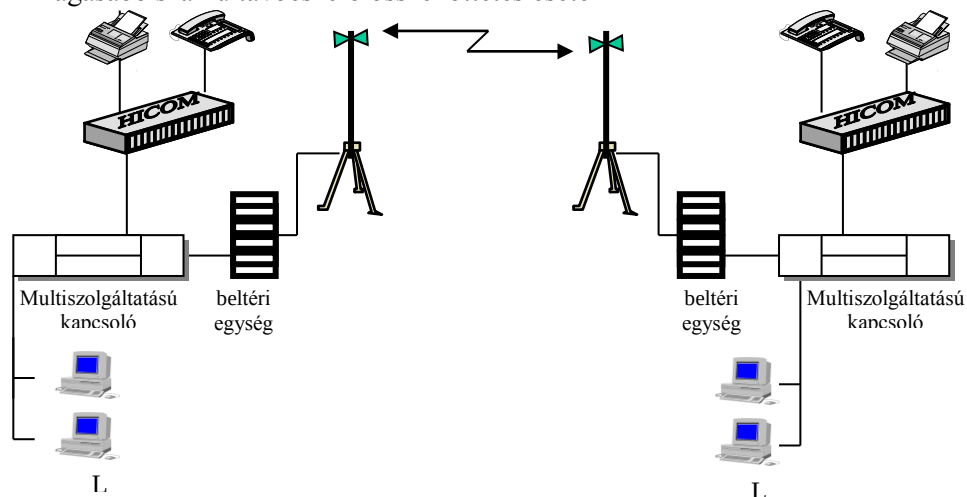
⁴⁷ QoS (Quality of Service) Szolgáltatás minősége

⁴⁸ WAN (Wide Area Network) Nagy kiterjedésű hálózat



2. számú ábra Összeköttetés kis távbeszélő forgalmat bonyolító nagyobb adatátviteli igényű telephellyel

Magasabb számú távbeszélő összeköttetés esetén



Abban az esetben, amikor az adat jellegű összeköttetések mellett a távbeszélő összeköttetéseknek is nagy szerepe van, akkor a két távbeszélő központ számára a multiszolgáltatású kapcsolók képesek a hálózati kapcsolathoz szükséges csatornák átvitelére (3 számú ábra).

3. számú ábra Összeköttetés magasabb távbeszélő forgalmat bonyolító nagyobb adatátviteli igényű telephellyel

Ebben az esetben az adatcsatorna tömörítetlenül kerül átvitelre a beszédcsatornák pedig tömörítve. A távbeszélő hálózatban minden szolgáltatás ugyanúgy él, mint a két központ közvetlen összekötésével.

A összeköttetés tervezése során fel kell mérni az adott objektum irányába szükséges távbeszélő csatornák számát és a két oldalon csatlakozó Hicom központok esetében ezt a csatornaszámot kell beállítani. A megfelelő csatornaszám beállításával egyrészt sávszélesség takarítható meg, másrészt olyan esetekben, amikor nincs szükség például a 2 Mbps-os összeköttetésből mind a 30 csatornára csak 10-re, akkor a két központ oldalon 20-20 fővonalai szoftver megtakarítható, ez a beruházások szempontjából további költségesökkentést eredményez.

Összegzés

Az előadásban a Magyar Honvédség egyes összeköttetésein található sávszélességek hatékonyabb kihasználására adtam javaslatot.

Belátható, hogy a dinamikus csatorna-kihasználású multiszolgáltatású kapcsolók a kor színvonalának megfelelnek és jövőbemutató rendszerek kiépítését teszik lehetővé. Kiváló sávszélesség menedzselő képességüknek köszönhetően, jelentősen növelhetik az átvitt beszédcsatornák számát, illetve az átvitt adatok mennyiségét.

Felhasznált irodalom

- [1] Fekete Károly: A Magyar Honvédség állandó telepítésű kommunikációs rendszere továbbfejlesztésének technikai lehetőségei, doktori (PhD) értekezés ZMNE, 2003.
- [2] Fekete Károly: A Magyar Honvédség állandó hírendszere továbbfejlesztésének lehetőségei, ZMNE: A kommunikáció (híradás) helye és szerepe a vezetés rendszerében, 2000.
- [3] Kapsch Telecom Kft. A NortelNetworks Passport 4400 multiszolgáltatású kapcsolója (oktatási anyag) 1999.
- [4] Kucsera Anita: Garantált minőségű átviteli rendszerek (QoS) felhasználhatósága a Magyar Honvédség távközlési rendszerében különös tekintettel a dinamikus csatorna – kihasználású rendszerekre, diplomamunka ZMNE 2003.
- [5] Magyarné Kucsera Erika: A hálózatfelügyelet és lehetőségei a Magyar Honvédség híradó szolgálatánál ZMNE TDK 2001
- [6] Rajnai Zoltán: A tábori alaphírhálózat vizsgálata és digitalizálásának lehetőségei egyes NATO országok kommunikációs rendszereinek tükrében, doktori (PhD) értekezés ZMNE, 2001.
- [7] SIEMENS Rt.: HICOM 300 E Alkalmazások (oktatási anyag), 1998.
- [8] SIEMENS Rt.: HICOM 300 E Rendszerleírás (oktatási anyag), 1998.
- [9] Tannenbaum-Andrew S.: Számítógép hálózatok BP.-Novotrade kiadó Kft.-1992..
- [10] Tóth Gábor: AZ ISDN alapjai – MATÁV Oktatási Igazgatóság, 1998.

TÁVKÖZLÉSI HÁLÓZATOK EGYÜTTMŰKÖDÉSÉNEK NEMZETKÖZI ÉS NEMZETI SZABÁLYOZÁSI KÉRDÉSEI VESZÉLY- ÉS KATASZTRÓFAHELYZETBEN

Maros Dóra, PhD hallgató

A XXI. század első éveit jelentősen növekedett a különböző típusú veszély- és katasztrófahelyzetek (természeti katasztrófák, terrorista támadások, stb.) bekövetkezésének valószínűsége, és e tendencia jelenleg sem változik kedvező irányban. A távközlési rendszerek katasztrófális sérülése megbénítja az országok közötti és országon belüli kommunikáció normális működését, ezért gyors helyreállításuk és együttműködésük megszervezése, valamint ennek szabályozása létfontosságú feladat. Egy másik aspektus, hogy a távközlési erőforrások üzemképes működése elengedhetetlen a veszély- és katasztrófa helyzet előrejelzése, segélykérés, vagy a mentési feladatok megszervezése során, különös tekintettel a különböző típusú szervezetek együttműködésére, mint például rendőrség, polgári védelem, mentők, tűzoltóság, katonaság, kormányzati szervek, stb.

E feladatok teljesítéséhez szükséges a releváns hazai távközlési szolgáltatók bevonása, eszközeik és szolgáltatásaik igénybevétele. Ugyancsak fontos kérdés, hogy a magyar szabályozási környezetben olyan előírások, jogszabályok jelenjenek meg, amelyek előírják a hazai távközlési infrastruktúra megbízható működésének feltételeit, és veszély- és katasztrófa helyzetekben azok helyreállításának, együttműködésének megszervezését, a munkában résztvevők döntési és felelősségi körét.

Az Egységes Digitális Rádiótávközlő rendszer (EDR) magyarországi tervezett bevezetése is jelentős eszköze lehet a Magyarországon belüli és nemzetközi segítségnyújtásnak és fogadásnak. Szükséges az állami tartalékgazdálkodás racionálisabbá tétele abban az értelemben, hogy a tartalék eszközök a távközlési szolgáltatóknál napi használatban legyenek, biztosítva ezzel a folyamatos működőképességüket.

Hazai veszélyhelyzet esetén, vagy más országok megsegítésekor egyedi döntés alapján lehet és kell a szükséges és lehetséges feladatokat meghatározni. Az Állami Felek közötti kapcsolat alapja a kölcsönös egyeztetés és megegyezés. Fenti feladatokat sok esetben csak kölcsönös nemzetközi segítségnyújtás útján lehet a megfelelő időn belül biztosítani.

A távközlési erőforrások együttes működésére vonatkozó szabályozások létrehozására számos nemzeti és nemzetközi testület együttműködése szükséges. A testületek olyan egységes szabályozási környezet megteremtésére törekcsenek, amelyek veszély- és katasztrófa helyzet esetén meghatározzák a szükséges intézkedések adminisztratív és műszaki követelményeit, a gyors mentési és helyreállítási tevékenységek érdekében használt korlátozott távközlési erőforrások használatának irányelveit.

A katasztrófa következtében bekövetkezett károk esetén a hálózatok működését meghatározó korlátozott műszaki és szolgáltatási erőforrások igénybevételét az ITU Y-roec (új nevén Y.1271) ajánlásának [1] előterjesztésben határozta meg. Az ajánlás tervezetben foglalt következő lista, azokat a speciális - a korlátozott hozzáférés és működési nehézségek következtében csökkent forgalmi kapacitás miatt fellépő - funkciókat tartalmazza, amelyek szükségesek a károk helyreállítása érdekében tett intézke-

dések megkezdéséhez, a mentési feladatokban résztvevő civil, állami és katonai szervezetek együttműködésének biztosításához:

- Jogosult felhasználók hitelesítésének gyors végrehajtása. (A mentésben, helyreállításban résztvevők azonosítása előre megadott jogosultsági szintek szerint.)
- A kommunikáció biztonságának védelme. (Például. speciális titkosítás alkalmazásával.)
- A távközlési erőforrások preferencia szerinti elérésének gyors biztosítása. (Csak a jogosult személyek használhatják a hálózatot).
- A kommunikáció preferencia szerinti létrehozása. (Csak arra jogosult személyek között épül ki a kapcsolat.)
- A kapcsolat preferált útvonalak szerinti felépítése. (Például katasztrófa elhárításban résztvevő szervezetek között)
- Egyéb működési erőforrások preferált használata a forgalom biztosítására. (Például adatátviteli lehetőségek biztosítása)
- Preferált kapcsolat biztosítása a hívást fogadó számára. (A hívott fél csak előre meghatározott számokról fogadhat hívásokat.)
- Opcionális előjogok biztosítása a nem veszélyhelyzeti távközlési erőforrások igénybevételére. (Például a mentésben résztvevők családtagjainak értesítése.)
- A szolgáltatásminőség minimális követelményeinek fenntartása a távközlési infrastruktúra erőforrásainak kiesése esetén (Milyen szolgáltatásokat és milyen „minőségben” szükséges mindenképpen biztosítani.)
- Kritikus helyzetekben alkalmazott távközlési szolgáltatások kezeléséhez szükséges információk cseréje. (Például a. távközlési szolgáltatók, hatóságok, stb. között.)

Természetesen a gyakorlatban a fent felsorolt követelmények közül néhány nem minden esetben biztosítható azonnal és teljes körűen. Minél több funkció együttes biztosítása, valamint alkalmazása növeli a vészhelyzeti feladatok egyre hatékonyabb és gyorsabb végrehajtását.

Nemzetközi szabályozások

A Tamperei Egyezmény

A veszélyhelyzeti időszakokra vonatkozó nemzetközi távközlési együttműködés elveinek kidolgozása az ENSZ keretében működő Nemzetközi Távközlési Unió (ITU) keretében, 1991-ben rendezett konferencián kezdődött. A nemzetközi távközlési együttműködés elvei a több lépcsőben egyeztetett, illetve kidolgozott, *“Tamperei Egyezmény a Távközlési Erőforrások Biztosításáról Katasztrófa Elhárítás és Mentés Céljaira”* [2] nemzetközi egyezmény tervezetben öltöttek formát. Az Egyezmény az Egyesült Nemzetek Szervezetének tagállamai és a Nemzetközi Távközlési Unió tagállamai által, a Tampereben, 1998. június 18. napján megtartott *Intergovernmental Conference on Emergency Telecommunications* című rendezvényen, vagy ezt követően az ENSZ székhelyén (New York) 1998. június 22. napja és 2003. június 21. napja között került aláírásra, amelyhez hazánk is csatlakozott. Az ország távközlési infrastruktúrájának veszélyhelyzetben vagy katasztrófa esetén is megbízható és minőségi működtetése szempontjából a Tamperei Egyezmény aláírása összhangban van Magyarország érdekeivel, földrajzi helyzetével és lehetőségeivel, katasztrófa veszélyeztetési szintjével és elkötelezettségeivel. Az Egyezmény kötelező elismerése jól szolgálhatja részvételét a jövőbeli európai közösségi feladatok végrehajtásában is. A

NATO Polgári Veszélyhelyzet Tervező Bizottsága (CCPC) is szorgalmazta, hogy az Egyezmény aláírása a NATO tagországok részéről is megtörténjen.

A Tamperei Egyezmény segítségnyújtási alapelve, hogy a katasztrófa következményeinek felszámolásához az államok a távközléshez szükséges személyzetet, felszerelést, anyagot, információt, oktatást, átviteli hálózatot, illetve kapacitást, továbbá a távközléshez szükséges minden egyéb forrást biztosítanak. Tehát azokkal az alapelvekkel és eljárási rendekkel foglalkozik, amelyek elősegítik a veszélyhelyzeti feladatokra való nemzetközi és nemzeti felkészülést, illetve szükség esetén a gyors, rendezett végrehajtást. A Tamperei Egyezmény megfelelő kereteket biztosít ahhoz, hogy a résztvevő államok veszélyhelyzet vagy katasztrófa elhárítása esetén – segítséget igénylőként, vagy segítséget nyújtóként – minden gyakorlati lépést megtegyenek a rendelkezésre álló távközlő eszközök, szolgáltatások szervezett, hatékony felhasználása érdekében.

Nemzetközi szabályozási szervezetek

A Nemzetközi Távközlési Unió (ITU) számos munkacsoportja foglalkozik a veszélyhelyzeti telekommunikáció szabályozási kérdéseivel, és a szükséges szabályozási rendszer létrehozásával. Ebben a munkában nagy szerepet vállalt az Európai Távközlési Szabvány Intézet (ETSI), EMTEL (EMergency TELecommunication) nevű szakértői csoportja is. A csoport feladata, hogy szorgalmazza, támogassa, és tevékenyen segítse a területre vonatkozó szabályozások (szabványok, direktívák, együttműködési megállapodások) kidolgozását, valamint figyelemmel kíséri a témához kapcsolódó, de nem ETSI hatáskörön belül történt eseményeket, szabályozásokat (pl. USA, Japán, Ausztrália, stb.). A szabályozások nemzetközi szintjén arra kell törekedni, hogy a távközlési szolgáltatások biztosítását érintő minden fontos műszaki, informatikai és adminisztratív erőforrás az adott veszélyhelyzetben, ha korlátozottan is de rendelkezésre álljon. A szabályozások kidolgozásához a nagy nemzetközi szabványügyi szervezetek aktív részvételén kívül szükség van a nagykiterjedési nyilvános elektronikus hírközlési (távközlési, műsorszóró, Internet-szolgáltató, stb.) hálózatokat üzemeltető szolgáltatók, valamint a hírközlési végberendezéseket és rendszereket gyártó vállalatok együttműködésére is. A területen folyó projektek célja, olyan szabályozási rendszer létrehozása, amely megteremti a hálózatok közötti egységes jelzés és protokollrendszer kialakításához szükséges műszaki feltételeket és szabványokat. Az alábbi ábra a szabályozási munkában résztvevő szabványszervezeteket, munkacsoportokat, valamint az általuk szabályozott területeket foglalja össze.

ITU-T az ITU távközlési szabványosítási szektora, amelyben munkacsoportok (Study Group: SG) végzik az egyes műszaki területek szabványosítási munkáit. Például az SG4 csoport a távközlési hálózatok működtetésének és felügyeletének (Telecommunication Network Management, TMN) kérdéseit tanulmányozza. A csoport egyik eredménye, hogy kidolgozott egy szabványtervezetet (Draft Recommendation M.ets) [3], amely a nemzetközi vészhelyzeti távközlési szolgáltatás (szolgálat) céljaira meghatározza hálózatok és a szolgáltatások információcseréjének követelményeit a TMN-X interfészen keresztül. Az IETF (Internet Engineering Task Force) az Internet hálózattal kapcsolatos szabványosítási kérdéseket kezeli. Az ETSI-ben két szakértői munkacsoport foglalkozik szabványosítási kérdésekkel. A TIPHON (Telecommunication and Internet Protocol Harmonization over Networks) azokkal a műszaki kérdésekkel foglalkozik, amelyek a Közcélú Kapcsolt Távbeszélő Hálózat

(PSTN) és az IP alapú csomagkapcsolt infrastruktúra konvergenciájához szükséges együttműködési paramétereket írja le. A 3GPP (Third Generation Project Partnership) nevű projekt a harmadik generációs mobil rendszerek fenti vonatkozású szabványainak kidolgozását végzi. Az USA több szabványosítási szervezete foglalkozik a nemzetközi szabványok nemzeti kompatibilitásának kidolgozásával, amelyben részt vesznek a nagy távközlési vállalatok is. A TMForum (TeleManagement Forum) egy nagy ipari konzorcium, amelyben 30 ország, hozzávetőleg 250 szervezete törekszik arra, hogy összehangolja a hálózatok működtetés támogatási rendszereinek (Operation Support System) egységes implementálását, és azok együttműködését.

Nemzetközi szabályozási szervezetek és a szabályozások területei



Hazai szabályozások

A 2003. évi C. törvény az elektronikus hírközlésről 92.§-a rendelkezik a távközlési szolgáltatók feladatairól minősített időszakban. A (3) bekezdés alapján „...a szolgáltató köteles a szolgáltatáshoz a (2) bekezdésben meghatározott igényeknek megfelelő műszaki rendszert – így különösen alapkiépítésű monitoring alrendszert – létesíteni és ennek elérhetőségét hálózatában a kilépési pontig biztosítani a Nemzetbiztonsági Szakszolgálat részére...” A törvény előírja, hogy külön jogszabályokban kell rendelkezni az alábbi kérdésekről:

- Az elektronikus hírközlési szolgáltatónak meghatározott esetekben együtt kell működniük a zártcélú hálózatok üzemeltetőivel.
- Műszaki, forgalmi, katasztrófa vagy egyéb veszély miatt keletkező üzemzavar elhárításához a szolgáltató köteles meghatározott tartalmú, folyamatosan felülvizsgált és karbantartott felkészülési, zavar-elhárítási és katasztrófa-elhárítási tervekkel rendelkeznie. Ugyancsak rendelkeznie kell a felkészülésre vonatkozó feladatok ellátásához szükséges mértékű és összetételű tartalékokkal.

c.) Minősített időszak esetében alkalmazandó intézkedési terv kidolgozása és végrehajtása érdekében az elektronikus hírközlési szolgáltatóknak meghatározott módon együtt kell működniük egymással, illetve az illetékes szervezetekkel.

Az említett feladatok pontos szabályozásra ebben az évben született meg az *elektronikus hírközlés veszélyhelyzeti és minősített időszaki felkészítésének rendszeréről, az államigazgatási szervek feladatairól, működésük feltételeinek biztosításáról* szóló 100/2004. (IV. 27.) Kormányrendelet [4]. A Kormányrendelethez kapcsolódóan, a cikk megírása idején két kapcsolódó IHM rendelet tervezet véleményezése volt folyamatban, melyek a következők:

- Az informatikai és hírközlési miniszter...../2004. (TERVEZET) IHM rendelete a védelmi feladatokban résztvevő elektronikus hírközlési, illetve postai szolgáltatók kijelöléséről, és felkészülési feladataik meghatározásáról [5]
- Az informatikai és hírközlési miniszter..../2004. (TERVEZET) IHM rendelete az informatikai és hírközlési, továbbá a postai ágazat ügyeleti rendszerének létrehozásáról, működtetéséről, hatásköréről, valamint a szolgáltatók bejelentési és kapcsolattartási kötelezettségeiről (2004, január) [6]

Összegzés

A veszélyhelyzeti távközlés (Emergency Telecommunication) kérdései a Szeptember 11.-i terrortámadás óta még relevánsabbá váltak a folyamatosan növekvő terrorista támadások miatt, amelyek már nem csak egyes személyeket, vagy kisebb csoportokat, hanem akár egész városrészeket is fenyegetnek. Az utóbbi években, a Föld szélsőséges időjárása számos nagy természeti katasztrófahelyzetet okozott (nagy kiterjedésű árvizek, földrengések, tűzvészek). A bekövetezett katasztrófahelyzetben a távközlési hálózatok sérülése miatt – ha időszakosan is – de megszakad az emberek közötti kapcsolat, a telefonálás és így a segélykérés, vagy a mentőmunka megkönnyítését szolgáló információk közlése is lehetetlenné válik.

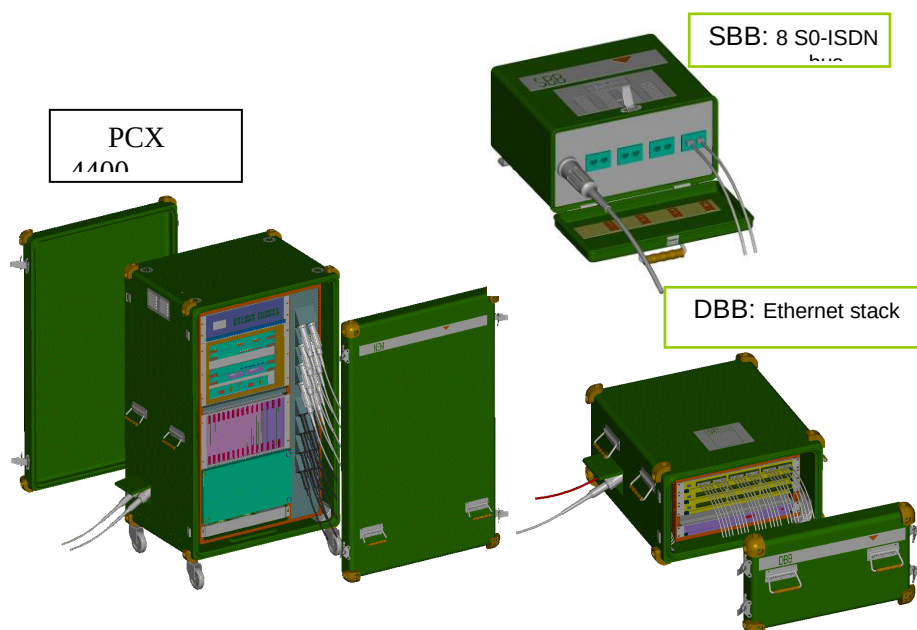
A nemzetközi szabványügyi, kormányzati, polgári és szakmai testületek összefogásával jelenleg olyan nemzetközi szabályozási környezet kidolgozása folyik, amely várhatóan lehetőséget ad a távközlési erőforrások hatékony működésének és együttműködésének biztosítására veszély- és katasztrófahelyzetekben. Sok még a feladat, és a munka még csak kezdeti stádiumban van. A magyar szabályozások, ha lassan is, de követik a nemzetközi elvárásokat. Ennek első jeleit a Tamperei Egyezmény aláírása és a 2004-re tervezett rendeletek megjelenése is alátámasztja.

Irodalomjegyzék

- [1] Draft new Recommendation Y.roec Framework(s) on Network Requirements and Capabilities To Support Emergency Communications Over Evolving Circuit Switched and Packet Switched Networks
- [2] Tampere Convention on the Provision of Telecommunication Resources for Disaster Mitigation and Relief Operations (Conference on Emergency Telecommunications, ICET-98, 1998, Genf)
- [3] Draft Recommendation M.ets, Network and Service Management Requirements for Information Interchange Across the TMN X-interface for the International Emergency Telecommunications Service (ETS)
- [4] COMPLEX CD jogtár, 2004 . június.
- [5] [6] Informatikai és Hírközlési Minisztérium honlapja, (www.ihm.hu)



Az Alcatel PCX 4400 tábori kommunikációs rendszer elemei



Alcatel Hungary Kft.

1116 Budapest, [Kondorfa u. 10.](#)
Telefon: (1) 2099500 Telefax: (1) 2099599
www.alcatel.hu
alcatelh@alcatel.hu

MOBILE ADAPTIVE RADIO DIRECTION FINDING SYSTEM

Gyula Mikó, PHD student of BUTE

e-mail: miko@mht.bme.hu

András Magyar, PHD student of BUTE

e-mail: oma@primposta.hu

Head of the project: Dr. Rudolf Seller

Budapest University of Technology and Economics

Department of Broadband Infocommunications and Electromagnetic Theory

2004.

Abstract: *Growing importance of adaptive arrays motivated us to develop an experimental measuring system, what can be used to inspect the practical behavior of different adaptive algorithms which are well described in theory.*

Introduction

Significance of adaptive arrays in mobile telecommunication is growing nowadays. Base stations use adaptive array techniques to track mobiles and reduce interference to other users by only transmitting the radio energy where it is required. As a result significant RF energy decrease can be achieved. Interference among different mobile terminals can be significantly reduced if base stations use smart antennas. As a result significant capacity increase can be achieved because of the co-channel reuse distance is reduced. This is called Space Division Multiple Access (SDMA) and it is used in the CDMA telecommunication systems.

The incoming signals in mobile systems show faded nature. Usually fading is reduced by multiple sampling of the EM field.

Other spreading area of adaptive arrays may be the military applications. In this case the goal is seeking of a given target in presence of jamming sources. It can be achieved by adaptive beamforming, namely null places of the radiation pattern of the array must be placed on the directions of jamming sources.

Major steps

Theoretical investigation, design and construction of an experimental linear antenna array for reception

1. Theoretical investigation

- general study of the methods of adaptive antennas
- finding the optimal array arrangement for our application
- finding the optimal algorithm for our application (direction finding, side lobe cancelling, diversity algorithms)
- subsystem design

2. Construction of an experimental linear antenna array for reception, where the suggested number of antenna elements is 4.

- design and implementation of the processing network of individual antenna elements
- consideration of the influence of mutual impedance between antenna elements
- design and implementation of a fast digital interface capable of handling even a bigger array

- consideration of a combined transmit-receive antenna element signal processing network and the high speed digital interface for proper handling of bigger arrays
 - design and implementation of the processing software
 - calculation of the receiver antenna pattern
 - measurement of receiver antenna pattern
 - calibration of antenna array
 - design and implementation of direction finding, side lobe cancelling and diversity algorithms
3. Development of IQ receivers for downconverting RF to complex baseband
- to find out the operating frequency range and other RF parameters
 - to select a good circuit design matching to the specification with particular attention to minimize the difference between receiver channels caused by the reproduction process and electronic component parameter variance (the realized IQ receiver block diagram can be seen on Figure 1.)
 - minimal parameter variation between receiver channels with as low thermal and frequency dependency as possible
 - digital output to computer therefore design an analogue to digital conversion unit with multiple input
 - to achieve good RF, thermal and mechanical design

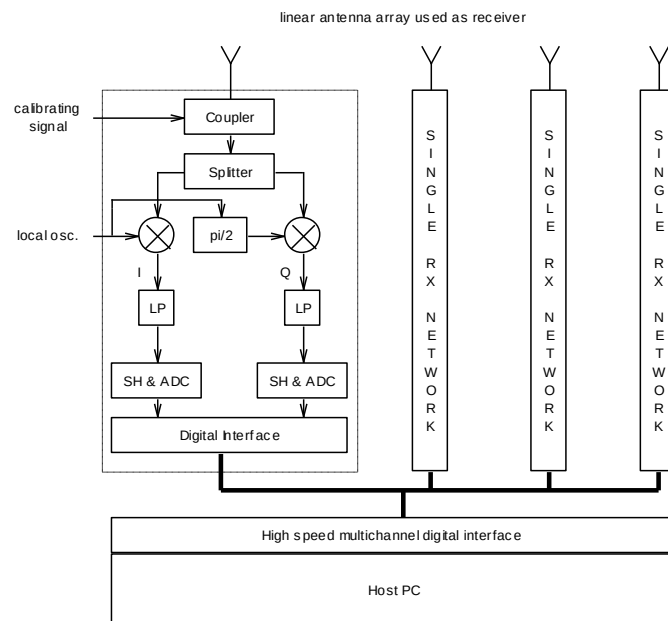


Figure 1. The receiver blocks [3]

System interpretation, theory

This project was started about four years ago, in a course of a diploma work in Budapest University of Technology and Economics.

The complete system includes both a hardware and a software part. The block diagram can be seen in Figure 2.

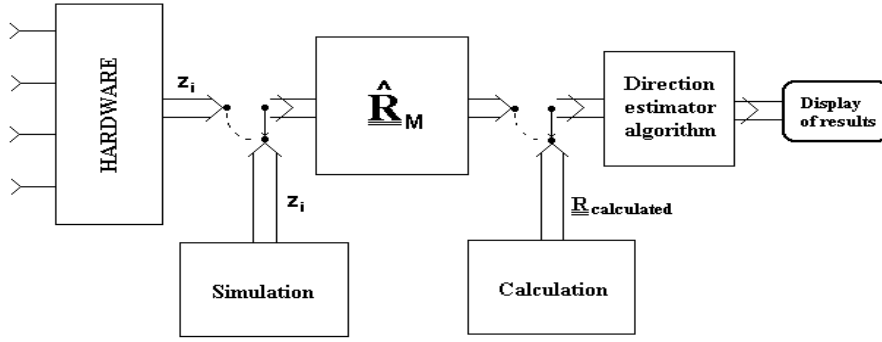


Figure 2. The system blocks [3]

Foremost we accomplish the software part which has dual exertion. In addition to it's capable for simulate the direction finding applying different algorithms, it's able to accept data from an external unit through serial port, and make the calculation with these “real” measured values. Each of the applied direction estimator algorithms set out from the autocorrelation (R) matrix.

$$R = E\{zz^H\} = \lim_{k \rightarrow \infty} \frac{1}{k} \sum_{i=1}^k z(t_i)z(t_i)^H$$

Definition of R matrix is the

following:

Determination of R matrix can be achieved in two different ways. “Calculation” block means that the matrix is determined by simply calculations. In this case occurrence of effects in real situations are ignored. Inconsistently in case of simulation we try to cause real situations, accordingly we have to take some real effects into account, for example phase difference of dividable sources at the antenna elements, and additive noise. Distribution of phase difference is uniform in a specific interval, whereas additive noise is modeled by Gaussian-distribution. In this case the R matrix is determined as an average. The averaging is done by the “ RM ” block.

$$\hat{R}_M = \frac{1}{M} \sum_{i=1}^M z_{ti} z_{ti}^H$$

R_M means an average calculated from M bit of sampled vector (z_{ti}). Elements of z are the signals at the output of the receiver antennas.

As it in Figure 2. can be seen “Calculation” and “Simulation” is optional. Input of the direction estimator algorithms is the R matrix which can be determined by the before mentioned two method. Output is the required spatial spectrum.

In the early version of the software there were three different algorithms to create and visualize the spatial spectrum. (Since then many upgrades were made on the software; easier handling, faster serial port reading, more algorithms and so on.)

These are:

- Classical (Fourier) method
- Capon (Minimum Variance) method
- MEM (Maximum Entropy Method)

Capon and MEM are adaptive methods. For this reason their resolution and dynamic range are better than Fourier method, but they are more sensitive to additive noise and correlation between sources. Increase of the bandwidth also abates the efficiency of the adaptive algorithms. It's important to mention that in case of highly correlated sources the additive noise increases the efficiency, because noises have correlation breaking affection.

In Figure 3. a calculated spectrum by the three algorithms in case of three sources can be seen.

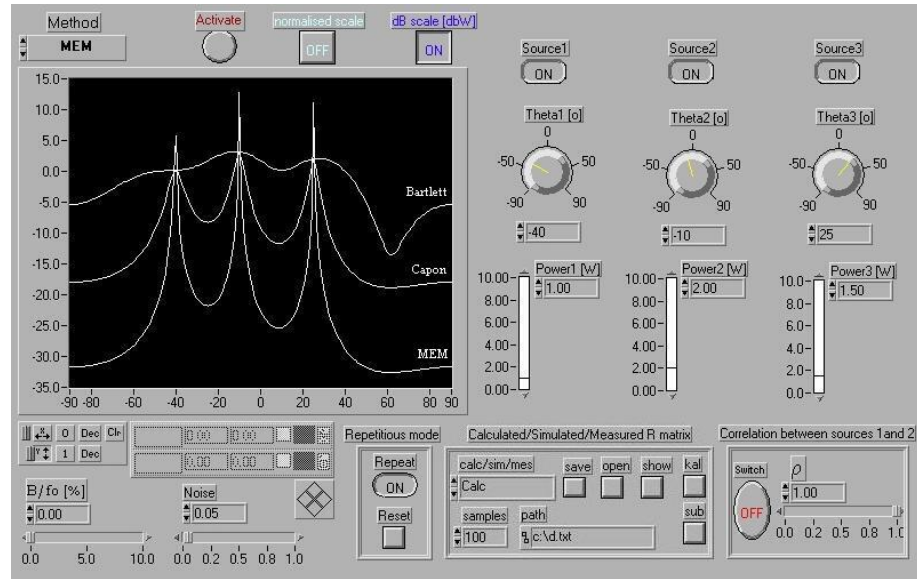


Figure 3. The software control panel [3]

As it seems the classical method gives a very indistinct estimation. Capon's estimation is better, the three direction is well separated as well as in case of MEM. MEM seems the better algorithm both in dynamic range and resolution, but also this is the most sensitive to disturbing elements which attend almost always in real situations.

The structure of the hardware

Pass by the derivation, an N element antenna system can bear N-1 direction. In our system N=4, consequently the maximal number of direction can be measured is 3. The build up of the hardware can be seen in Figure 4.

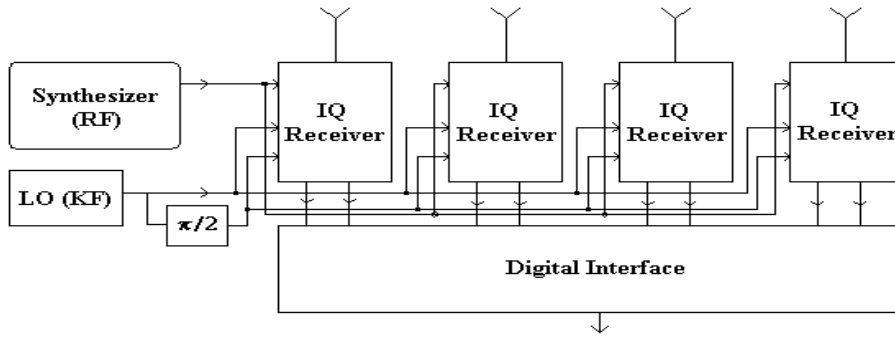


Figure 4. The actual receiver unit in blocks [3]

Each of the antennas connects to an I-Q receiver unit. The I-Q receivers need oscillator signals for mixing down. After the I-Q receivers we apply a digital interface to digitalize and send the data to the computer where the software calculate the spectrum applying one of the direction estimator algorithms.

I-Q receivers

$$I = A \cos(\phi)$$

$$Q = A \cos(\phi + \pi/2) = A \sin(\phi)$$

This is the major part of the system. The theoretically build-up can be seen in figure 5. Assume that the RF input signal ($f_1(t)$) is a simple sine tone. The signal coming from the receiver antenna come through the band-pass filter and splitted in two ways. The local oscillator (LO) frequencies are equal to the frequency of the input signal, but there is a $\pi/2$ phase difference between them. The output signals are:

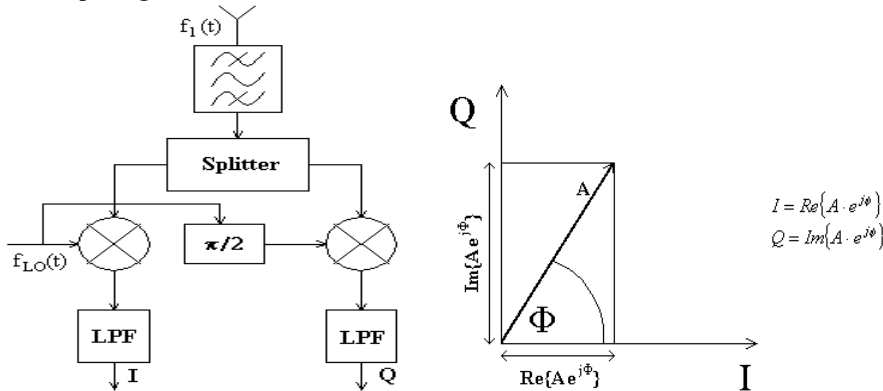


Figure 5. The I-Q components illustration [3]

The photo below shows the completed measuring system except the PC.

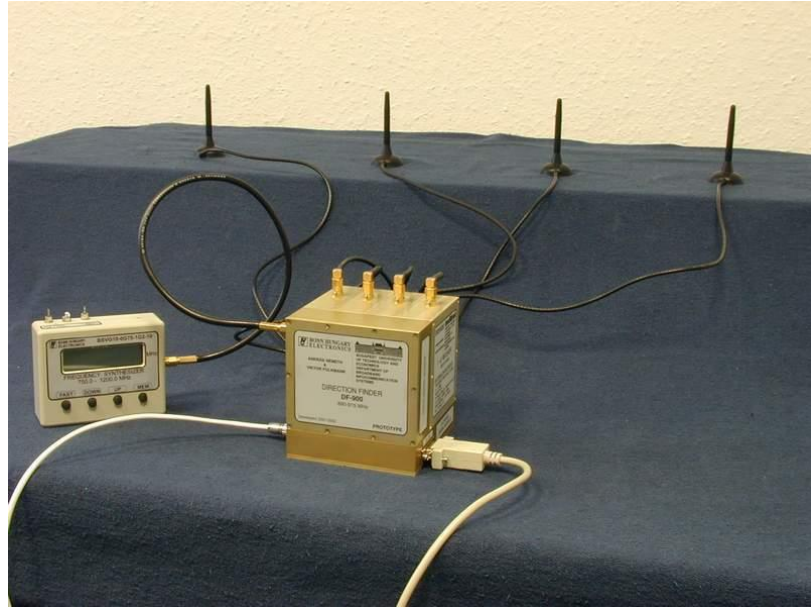


Photo 1. Receiver unit.

Measurement results

Briefly we will show how important adaptive antenna theory is by the following example, where we can see a measurement, where we could observe 2 way propagation, as well as it could have been two sources separated, and get the result that the conventional Fourier method cannot separate the sources from each other.

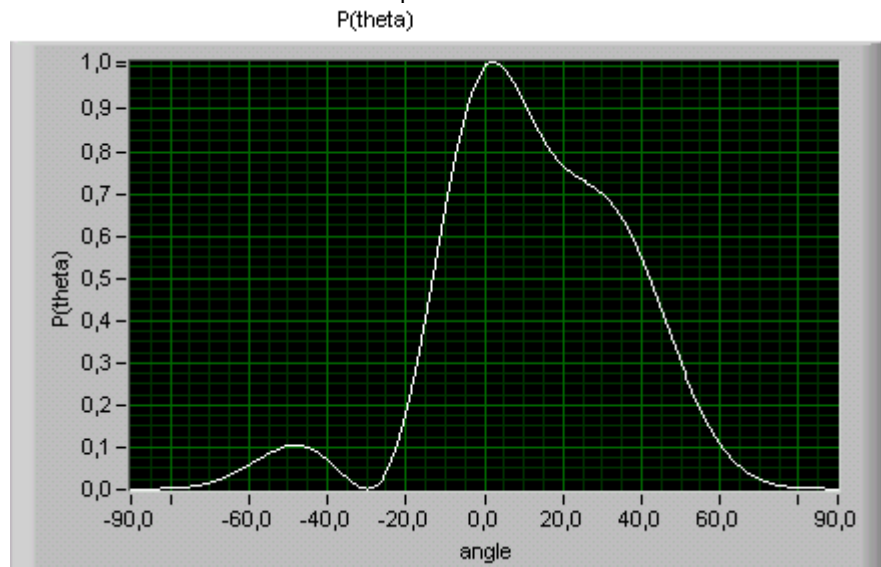


Figure 6. Fourier method

Here we can see the results of the same measurement, calculated with the adaptive Capon and MEM method.

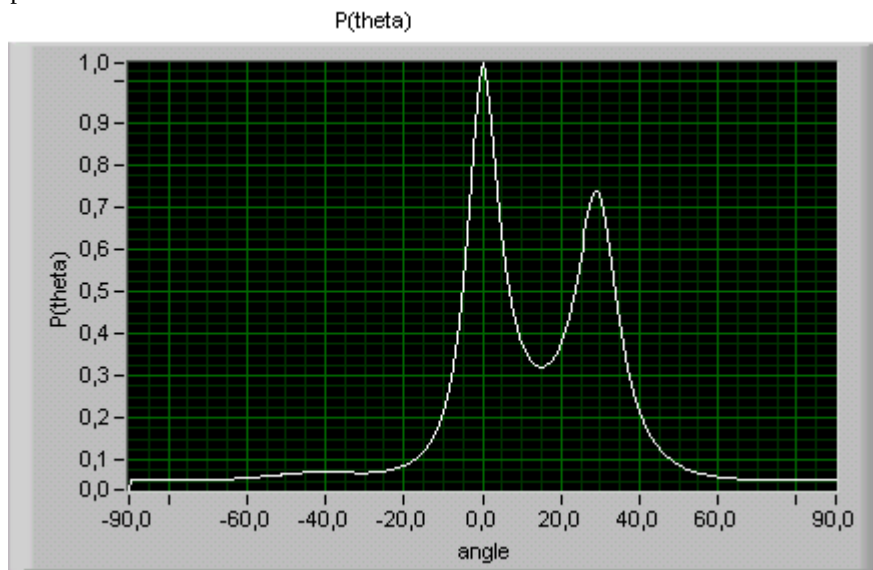


Figure 7. Capon method

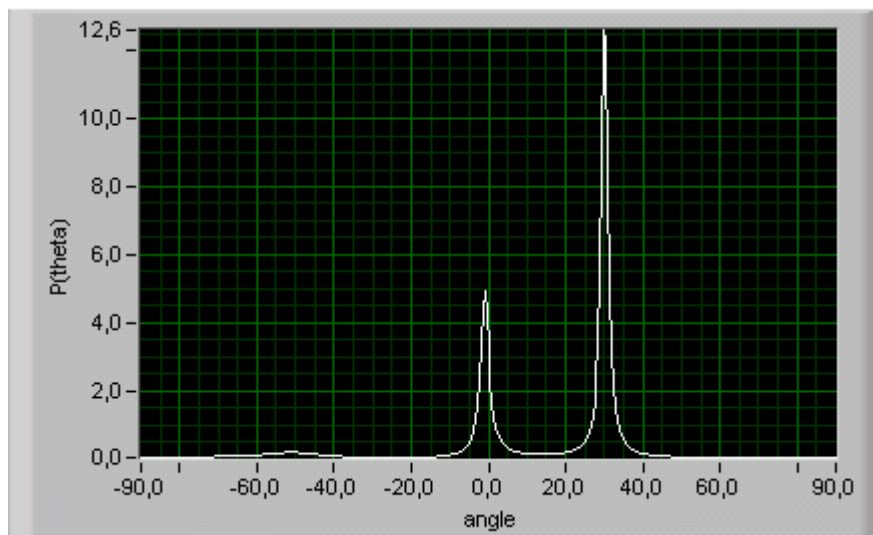


Figure 8. MEM method

As seen the MEM method is one of the most powerful methods, however its magnitude results can be different from the real magnitude relations.

We also conducted measurements with rare element antenna arrays. It means that we use the antenna elements so that they will not be at the same distance from each other, but at larger distances. Their advantage is that we increase the antenna aperture

size, so the main lobe will be narrower, however, hence the energy of the antenna system received remains the same the sidelobe level will rise and it makes the dynamic range worse.

Some of these structures are called MRA (minimum redundancy arrangement arrays).

2 dimensional adaptive radio direction measurement

1. Dimension-independent direction measurements

Dimension-independent direction measurement means that we measure the direction-varying power distribution of the incident EM wave independently, without correlation, in each dimension.

Let U be the power distribution in dimension x , and let V be the power distribution in dimension y . The virtual 2 dimensional power distribution is: $P=U*V$. The original aim was to detect one single dominating EM source in the far field of the antenna arrays. With this method false peaks are generated, which disturb the measurement (in the case of k angularly separated sources k^2 peaks), but the dominating source can be selected.

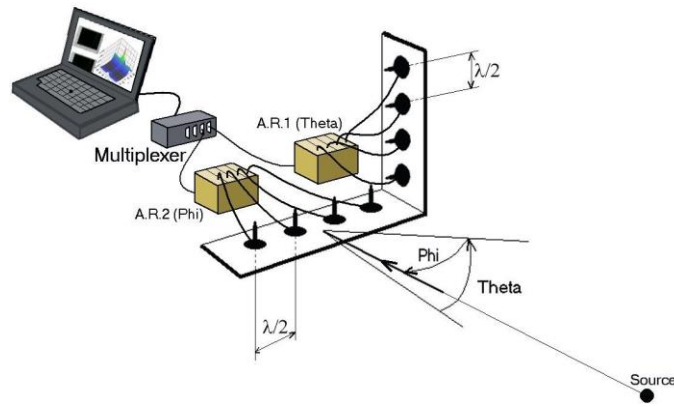


Figure 9. The sketch of the measurement

The vertical array gives directly the elevation angle (Θ) in spherical coordinate system, the azimuth angle (Φ) can be calculated from the angle that is measured by the horizontal array and the elevation angle, with:

$$\Phi = \arcsin\left(\frac{\sin(\Theta)}{\cos(\Theta)}\right),$$

where Θ is the angle measured by the horizontal array.

We used monopole antennae as receivers and 45° inclined monopole antenna as source (at 10m average distance).

Its exact location was measured with the appropriate angle-measuring stand previously.

The two dimensional power distributions of a source placed at 20° elev., -20° azim. angle:

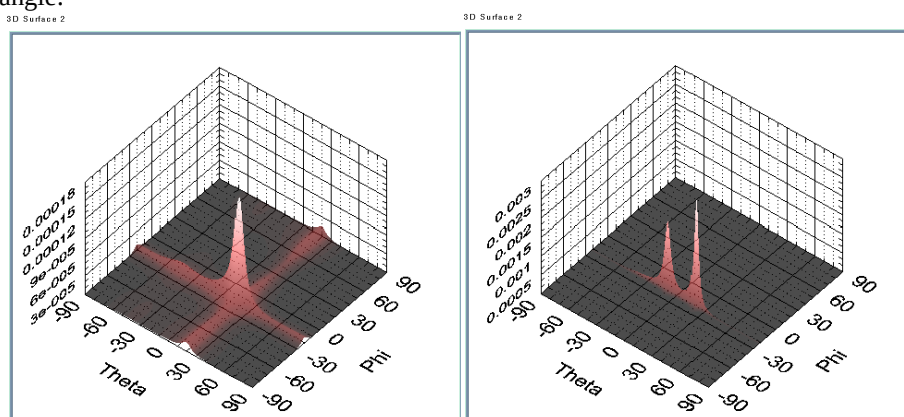


Figure 10. Measurement results in 3D

The first figure calculated with the Capon-method measured $\text{Theta}=19,6^\circ$; $\text{Phi}=-20,5^\circ$; the second with the MEM method measured $\text{Theta}=22,3^\circ$; $\text{Phi}=-21,6^\circ$ and detected a 2-way propagation component. The calculated angular resolution was $0,5^\circ$.

Conclusion: the same basic principles apply to this measurement type as to simple 1D measurements (less accuracy at extreme angles, higher accuracy perpendicular to the plane of the array structure). The false peaks generated have to be taken into account.

Photos about the 2 dimensional measurement system



Photo 2. The antenna arrays in operation.



Photo 3. Measurement (radio source in the foreground on a stand)

2. Coherent 2D direction measurements (theory, simulation)

With 3 basic antenna elements theoretically 3 dimensional measurement is possible, however, in practice these elements must be placed far from each other to be able to detect 3D info. Large element spacing limits the usable frequency band from upwards, considering Shannon's sampling theorem. Therefore, only 2D measurements are possible locally. To measure 2D radiation power distribution, we have to obtain the correlation information between the dimensions. This requires a common reference signal for all elements or the **coherence** of the reference signals.

1D measurements: we specify an **n**-element linear structure, we measure the **nxn** correlation matrix **R** of the structure. Then, we calculate the directions by a function with scanning vector **S** and **R** depending on the method. The elements of **S** depend on the angle of incidence and the geometrical structure of the antenna array.

The estimated correlation matrix: $\hat{R} = \frac{1}{M} \sum_{i=1}^M Z_i * Z_i^H$, where **Z** contains the measured complex field strength values of the antenna elements, **M** times measured.

$\mathbf{S} = [1 \ e^{j\Delta\Phi} \ e^{j2\Delta\Phi} \ \dots \ e^{j(n-1)\Delta\Phi}]$, where **n** is the number of antenna elements. The geometry factor is $\Delta\Phi = \beta d \sin(\Theta)$, where **d** is the distance between elements, $\beta = 2\pi/\lambda$, and Θ is the angle of the incidence.

2D measurements: we specify an **n**-element nonlinear structure, measure the 2 dimensional **R** correlation matrix the same way as in 1D. As previously, the elements of **R** contain the correlation between each two elements. Example: in case of a 4x4 equidistant antenna array, the correlation matrix has 16 rows and columns.

The basic structure of **R** does not depend on the geometry of the antenna system, since it is generated of general complex numbers, just as in the case of 1D calcula-

tions. Therefore, we can apply all known adaptive algorithms directly to this 2D correlation matrix.

What determines how we “read” matrix R, that is, how the antenna structure looks like, is the scanning vector. The geometry factor contains the information on the structure in the scanning vector as phases. All simulations assume isotropic and constant phase characteristics antenna elements with common reference signal.

2D planar antenna array structures

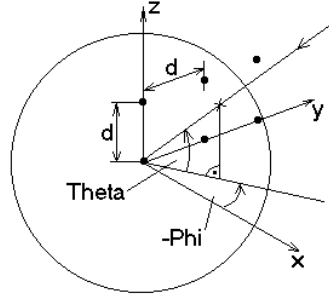


Figure 11. The antenna array

Here we can see a typical 2D array with the angles specified. An antenna element is described by its row (l) and column (m) number, both running from 0.

In my simulations: $d=\lambda/2$, the geometry factor will be:

$$\Delta\Phi=\pi(m*\cos(\text{Theta})\sin(-\text{Phi})+l*\sin(\text{Theta}))$$

For example, the scanning vector of a 2x2 array will be:

$$S=[1 \quad e^{j\pi\cos(\text{Theta})\sin(-\text{Phi})} \quad e^{j\pi\sin(\text{Theta})} \quad e^{j\pi[\cos(\text{Theta})\sin(-\text{Phi})+\sin(\text{Theta})]}]$$

Simulation results with sources at -20° elev., 30° azim. and at 10° elev., -40° azim. for 4x4 array, calculated with the Capon-method and 8x2 (horizontally wide) array, calculated with the Bartlett-method:

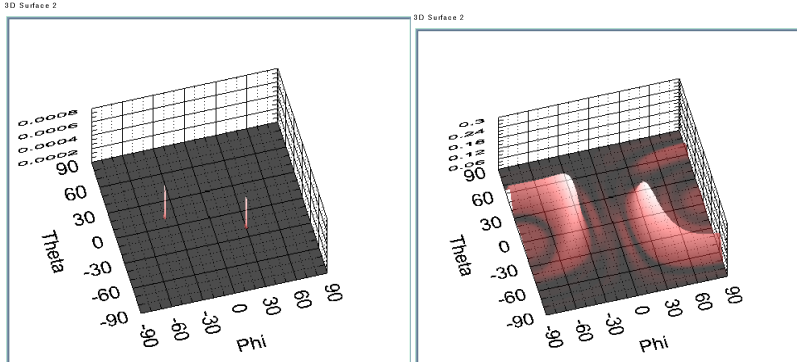


Figure 12. The 2D antenna array simulation results in 3D

We can see how measured resolution changes with the proportions of the antenna structure.

The wider the structure is the sharper the result will be.

Spherically distributed antenna structures

Elevation angle is measured from axis z. The geometry factor will be:

$$\Delta\Phi = \beta r (\sin\gamma \sin\alpha \sin(\Theta) \sin(\Phi) + \sin\gamma \cos\alpha \sin(\Theta) \cos(\Phi) + \cos\gamma \cos(\Theta)),$$

where γ is the elevation and α is the azimuth angle of the antenna element, placed on the surface of a sphere with radius r . Simulations shown (Fig. 5.) with an 8 element antenna system, elements separated by 30° in elevation and 90° in azimuth ($r=\lambda$). With one source at high SNR

($\Theta = -30^\circ$, $\Phi = -20^\circ$) and two sources at low SNR ($\Theta_1 = 0^\circ$, $\Theta_2 = -40^\circ$, $\Phi_2 = 30^\circ$):

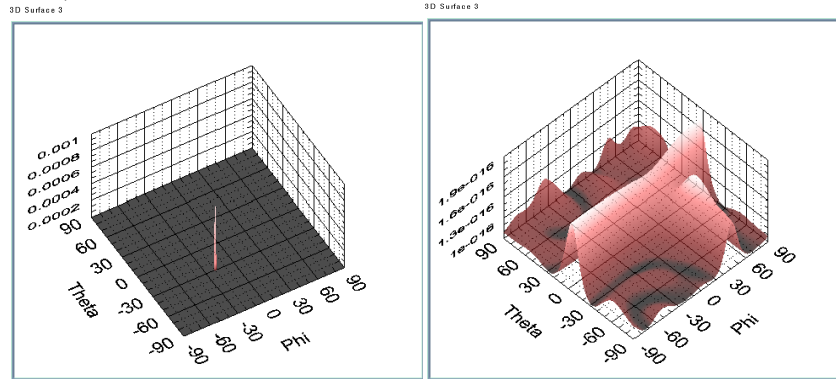


Figure 13. The simulation results of the spherically distributed antenna system

We can see in the right figure that the top point ($\Theta = 0^\circ$), shown on a plane becomes a line with Φ . (Both figures were calculated with the Capon-method.)

Measurement results for a 2x2 antenna arra

Measurement results with a 2x2 array with a 45° progressive phase shifting power divider

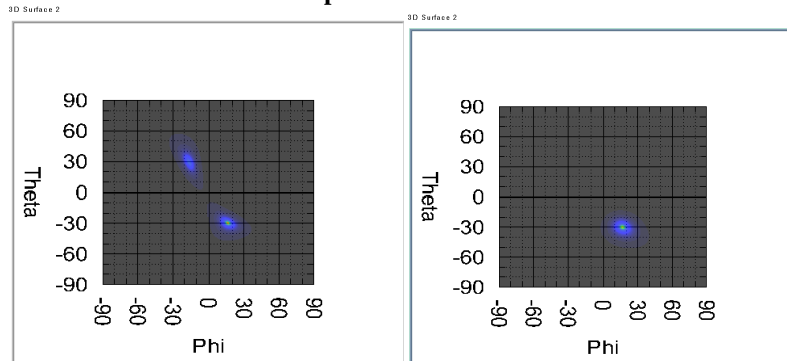


Figure 14. Measured with Capon, left. Simulated the same right. (coupling between divider outputs seen left)

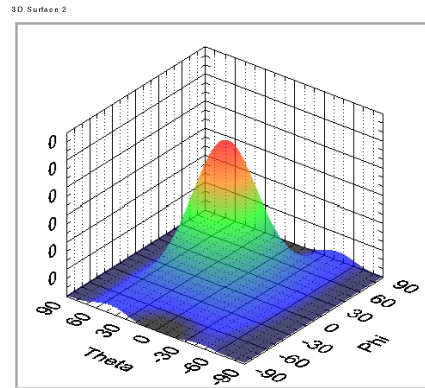


Figure 15. measured with a 0° output phase difference divider (Bartlett method)

Rare element arrays The sharpness of the lobes we measure depends on the antenna aperture size. To increase this parameter we need to increase the aperture size. If we have limited channels we use rare element arrays. The increased aperture size with some elements left out compared to the increased aperture size with all elements has greater sidelobe levels. The energy of the main lobe transfers into the sidelobes. Some of these arrays are also called MRA (Minimum Redundancy Arrangement) Arrays. 2

dimensional rare element structures

Simulation results are shown in the next figure of a source at 0° elevation and azimuth with a 4x4 frame 16 element structure on the left, with a 8x8 frame 64 element equidistant structure on the right. Both calculated with the Bartlett-

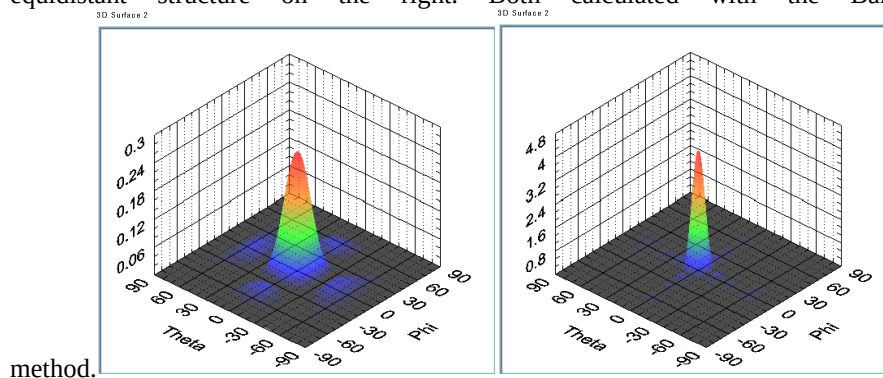


Fig. 16. The resolution increases.

In the next figure we can see a 8x8 frame 16 element structure and the simulation results with the same parameters. Where the switch is up the antenna element is present, where down, it is not present.

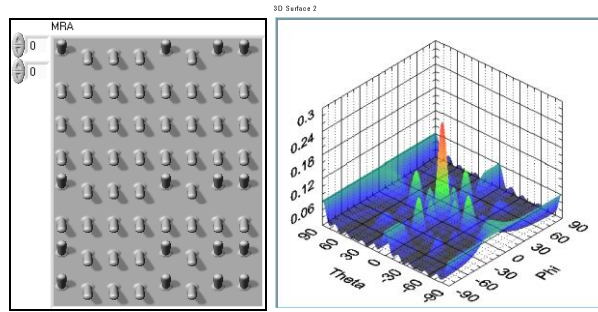


Fig. 17.

We can see, that the main lobe is approximately as narrow as in the case of the full 64 element array, however, the sidelobe level rises significantly.

The effect of element omitting to results with adaptive methods

Simulation results were calculated on the next two structures. Results are shown accordingly.

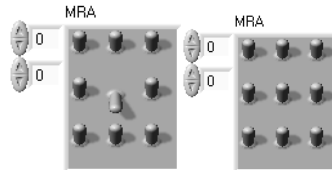


Fig. 18.

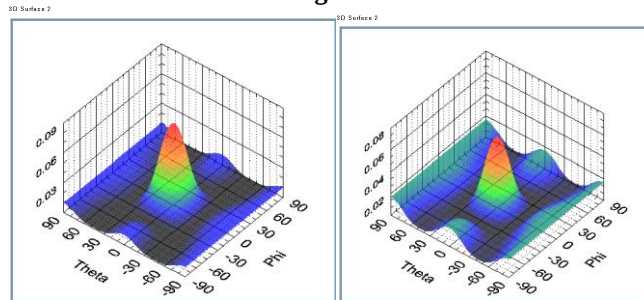


Fig. 19.

Calculated with the non-adaptive Bartlett-method. Shown for comparison. The dynamic range decreases significantly.

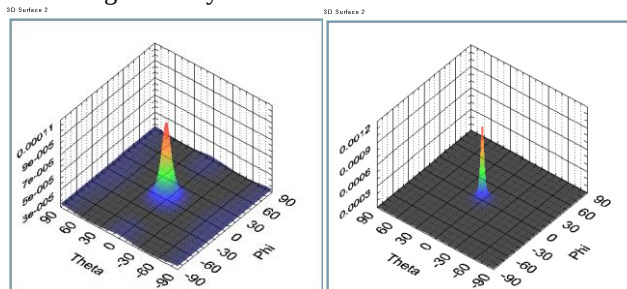


Fig. 20.

Calculated with the Capon-method. The dynamic range does not decrease dramatically, however, the main lobe's sharpness decreases, therefore, the resolution decreases.

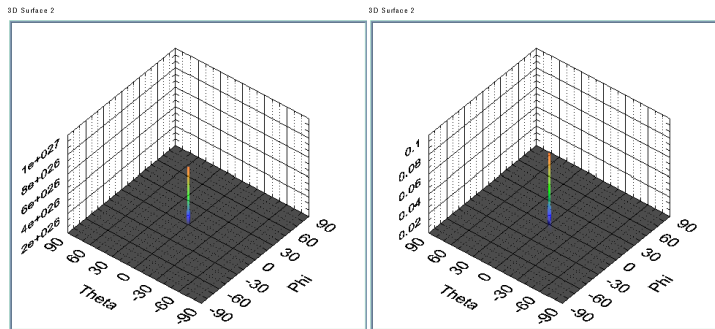


Fig. 21.

Calculated with the MEM method. Omitting one element decreases the performance of this method the least.

Conclusion

We are now in the 4th year of our project. We have realized a 900MHz 4 channel GSM band adaptive antenna receiver system. As the last step we have extended our project from 1 dimensional to 2 dimensional direction finding. We are about to realize a 16 channel 4,5GHz antenna system for military purposes, which is going to serve as an adaptive radar receiver.

Acknowledgements

Our project has been pre-financed by Bonn Hungary Ltd. Hereby, we would like to thank them for supporting us with their great generosity. We would like to thank the useful work and ideas to Mr. Viktor Folkmann and Mr. András Németh lieutenant engineer who started this project.

References:

- [1] Alfonso Farina: Antenna-Based Signal Processing Techniques for Radar Systems, Artech House, Norwood 1992.
- [2] A. Papoulis: Signal Analysis, McGRAW HILL, 1984.
- [3] Viktor Folkmann, András Németh: Direction Finding Based On Adaptive Antennas. Radioelektronika conference 2002., Bratislava
- [4] Gyula Mikó, Csaba Kalmár: GSM Band Direction Finding SystemApplying Adaptive Antenna Principle, Radioelektronika conference, 2003., Brno.

ERICSSON IN DEFENSE



ERICSSON 

Lars Magnus Ericsson, the Swedish Telecom's Pioneer

- Lars Magnus Ericsson (1846-1926)
- Company founded in 1876
- First export orders in 1881
- Trademark registered in 1894
- Manufacturing abroad in 1897



The great idea



>128 years of experience
Communication for hundreds of millions of people
Only company with all major standards for mobile communications

- Communications is a basic human need
- Telecommunications is for everyone
- Standardization and open systems

© 2004 Ericsson. All rights reserved. 2004-09-15

Ericsson in Defence

Ericsson - 128 years of leadership

- 1878 From telegraph to telephone
- 1923 From manual to automatic
- 1968 From electro-mechanics to computer control
- 1981 From fixed to mobile
- 1991 From 1G analog to 2G digital mobile technology
- 1998 Convergence of telecom and data in fixed/mobile networks
- 1999 Evolution towards 3G and Mobile Internet
First 3G WCDMA call on public network (Vodafone)
- 2002 First 3G Call in Hungary
- 2002 World premiere launch of MMS service (Westel - Hungary)
- 2003 EDGE in commercial use in Hungary

© 2004 Ericsson. All rights reserved. 2004-09-15

Ericsson in Defence

ERICSSON MICROWAVE SYSTEMS AB



Products & Solutions for
Information Superiority



Zrínyi Miklós Egyetem 2004-09-15

Ericsson in Defence

Experience

- 60 years of *radar* development
- A world leader providing advanced radar and *electronic defence systems*
- Competence center for Microwave and *Antenna* Technologies
- Commercial network technologies for military and *total defence networks*

Ericsson in Defence 2004-09-15

Ericsson in Defence

Fact and Figures

- Sales for 2003 of approx. €360 million
- 60% export sales
- 2000 employees
- 55% of employees with a university degree

Ericsson in Defence 2004-09-15

Ericsson in Defence



Zrinyi Miklós: Bgyetem 2004-09-15

Ericsson in Defence



Zrinyi Miklós: Bgyetem 2004-09-15

Ericsson in Defence

A world-class company present globally

- More than 3000 radars delivered worldwide
- Operational in more than 30 countries
- All products operated by NATO-countries
- International co-operation world wide
- Ericsson systems and radars supplied also through International system houses
- Strong connection to civilian Information Technology

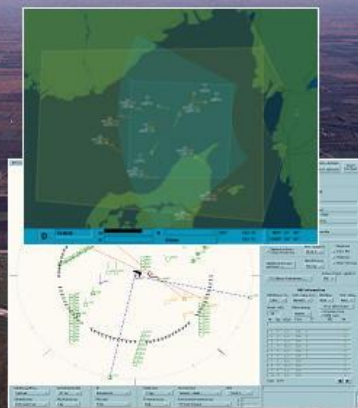
Ericsson in Defence 2004-09-15

Ericsson in Defence

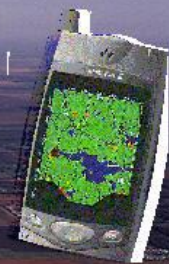
Situational awareness on the network



Before:
Available at the radar



Now: Available in
the stovepipe



Future:
Available
to all
authorized
users

Ericsson in Defence 2004-09-15

Ericsson in Defence

NETWORKS of NETWORKS of NETWORKS of NETWORKS ...



Zrínyi Miklós Egyetem 2004-09-15

Ericsson in Defence

Always best connected



Zrínyi Miklós Egyetem 2004-09-15

Ericsson in Defence



Çiğdem M. B. Eryılmaz 2004-09-15

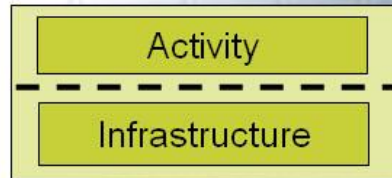
Ericsson in Defence



Çiğdem M. B. Eryılmaz 2004-09-15

Ericsson in Defence

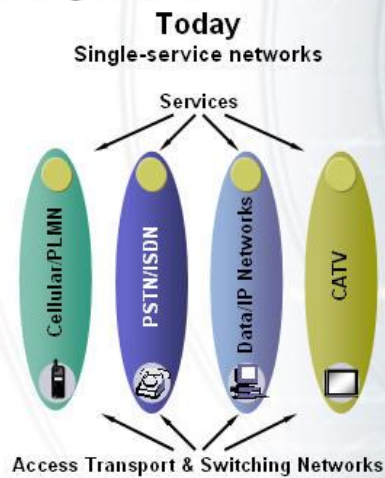
Architecture



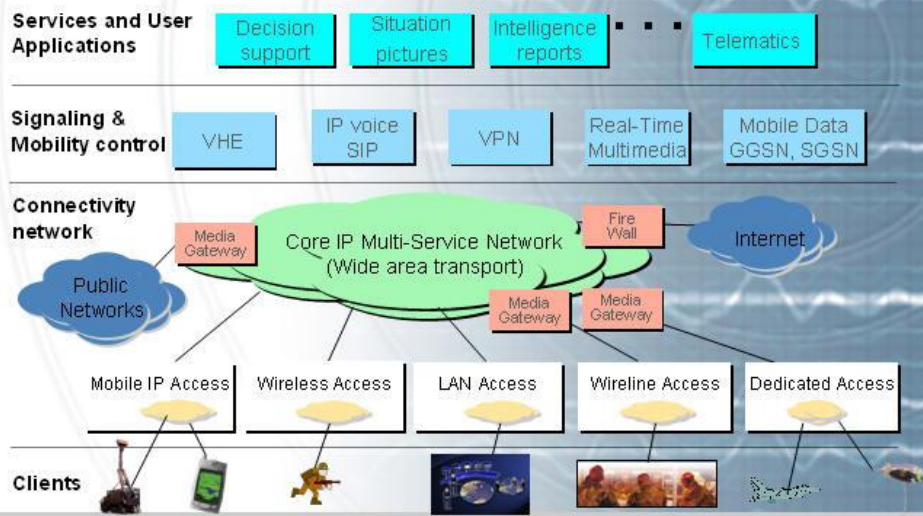
The work is divided into two domains:

- Activities (Business Logic)
- Infrastructure

New-generation commercial network structure



Communications Architecture for NCW



Ericsson in Defence 2004-09-15

Ericsson in Defence

Products & Solutions



Ericsson in Defence 2004-09-15

Ericsson in Defence

Information Superiority in Network Based Defence & National Security Network

- Functions as services
- Services driven by roles in the network
- Information and appliance services can be integrated
- Ericsson offers end-to-end network solutions



Zrinyi Miklos Egyetem 2004-09-15

Ericsson in Defence

Communication solutions in military networks

- Infrastructure built within hours
- Complete transportable mobile infrastructure for 2G or 3G, with reach-back via satellite
- 3G technologies in tactical networks, the perfect complement to today's combat network radio systems
- Military unique ECCM protected transmission and routing



Zrinyi Miklos Egyetem 2004-09-15

Ericsson in Defence

EriTac - Tactical area network

- Secure network with very strong ECCM performance
- Adaptive frequency hopping and advanced routing
- High mobility installed in small cross-country vehicles
- Voice and data communication
- Easy to build user-adapted networks



Örlogsmäktens Bjsystem 2004-09-15

Ericsson in Defence

Command, Control and Communication Systems

- C³ systems for
 - Air Defence
 - Mine Warfare
 - Airborne Early Warning & Control
 - Border Surveillance systems
- NATO Data links (Link 11, 16)
- Simulators and training systems



Örlogsmäktens Bjsystem 2004-09-15

Ericsson in Defence

PS-05/A - Advanced multi-mode fighter radar

- Integrated part of the first operational fourth-generation fighter
- Air-to-air and air-to-ground modes
- Full support for BVR missiles
- NATO interoperable & inventory
- In full scale serial production
- International customers



Zrínyi Művek Egység 2004-09-15

Ericsson in Defence

ERIEYE - Airborne Early Warning & Control System

- Airborne Early Warning
- Sea Surveillance
- Airspace management
- NATO interoperable & inventory
- Modern fixed active phased array pulse Doppler radar
- Commuter-type aircraft
- Low cost of ownership
- In full scale serial production
- Four customers worldwide



Zrínyi Művek Egység 2004-09-15

Ericsson in Defence

Carabas - wide area surveillance in real time

- Meter wave radar system for ground target detection
- Penetrate foliage, discover any concealed items
- Records all topographical changes since last surveillance
- Coverage rate of 100 sq. km a minute



Экспертная Система 2004-09-15

Ericsson in Defence

ARTHUR – The Most Modern Weapon Locating System

- Locates all types of artillery simultaneously (guns, rockets, mortars)
- High multi-target capacity
- NATO interoperable & inventory
- Single vehicle configuration
- High mobility, C-130 transportable
- Short deployment and re-deployment times
- In full scale serial production
- Ten customers worldwide



Экспертная Система 2004-09-15

Ericsson in Defence

GIRAFFE AMB - 3D Air Defence Search Radar

- SHORAD and VSHORAD AA-Systems
- Gap filler
- Integrated C³ system
- NATO interoperable & inventory
- Single vehicle configuration
- High mobility, C-130 transportable
- Short deployment and re-deployment times
- In full scale serial production
- More than 20 customers worldwide



Zrínyi Miklós Egyetem 2004-09-15

Ericsson in Defence

Sea Giraffe AMB - Naval 3D multi-role surveillance radar with stealth capabilities

- Single surveillance radar on small to medium size ships
- Air defence surveillance radar on medium to large ships
- Simultaneous Air and Surface surveillance and high-resolution splash spotting
- NATO interoperable & inventory
- In full scale serial production
- More than 10 customers worldwide



Zrínyi Miklós Egyetem 2004-09-15

Ericsson in Defence

HARD - Highly mobile, lightweight 3D search & acquisition radar

- Easy to integrate with new or existing short range air defence system
- Successfully used with LeFlaSys, ASRAD-R and RBS-90
- Active Phased array radar
- Low Probability of Intercept (LPI)
- NATO interoperable
- In full scale serial production
- International customers



Ericsson in Defence 2004-09-15

Ericsson in Defence

Transportable Mobile Network



Ericsson in Defence 2004-09-15

Ericsson in Defence

Mobile RBS/Satellite unit

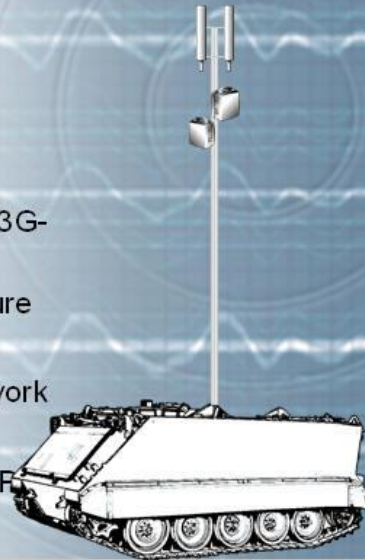


Zrinyi Munka Egyetem 2004-09-15

Ericsson in Defence

Mobile access

- Area coverage : cellular access
 - Autonomous, transportable 3G-network
- Area coverage without infrastructure
 - Manheld MANET
 - Ground sensor Ad Hoc network
- Dedicated access:
 - Sensor communication via IP



Zrinyi Munka Egyetem 2004-09-15

Ericsson in Defence

Local access - short-range communications

- Multiservice access 1 meter - 100 metres
 - Command post LAN, HiperLAN2/IEEE802.11a
 - Soldier personal network, Bluetooth
 - Vehicle onboard network,
 - Bluetooth,
 - Local Information point, Bluetooth



Ericsson in Defence 2004-09-15

Ericsson in Defence

Service and Support Operations

- Ericsson offers a full range of Service and Support solutions to ensure high system capability in all phases
- Ericsson allows the user/operator organization to focus on its core task and obligation



Ericsson in Defence 2004-09-15

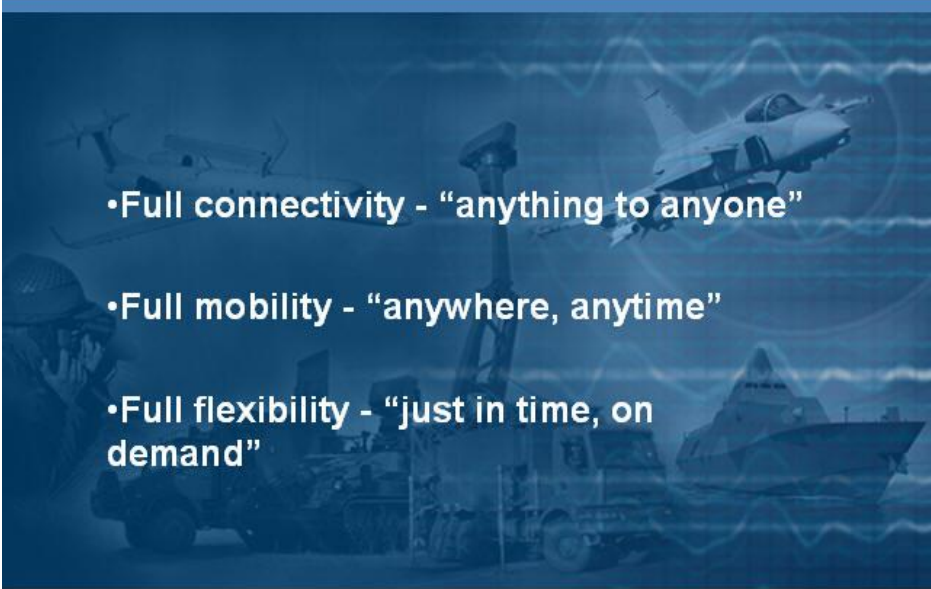
Ericsson in Defence

Services

- **Consultancy** – providing expert advice wherever and whenever needed
- **Training and education** – enabling greater competence
- **Support** – Comprehensive services for key functional areas
- **Spare parts** – addressing logistical needs
- **Maintenance and repairs** – providing high availability
- **Roadmap management** – Phased benchmarking against industry best practice
- **Through life management** – Control of all needs during the product lifecycle
- **Help Desk-FIRST** – centralized support on call
- **Testing and verification services** – ensuring proper analysis

Zrínyi Miklós Egyetem 2004-09-15

Ericsson in Defence

- 
- **Full connectivity** - “anything to anyone”
 - **Full mobility** - “anywhere, anytime”
 - **Full flexibility** - “just in time, on demand”

Zrínyi Miklós Egyetem 2004-09-15

Ericsson in Defence

SZÉLESSÁVÚ INTERAKTÍV CATV HÁLÓZATOK KIÉPÍTÉSE NAGYSEBESSÉGŰ ADATÁTVITELI SZOLGÁLTATÁSOKHOZ WCDMA TECHNIKA FELHASZNÁLÁSÁVAL

Egy-egy nagyterjedésű szélessávú interaktív CATV hálózat kiépítésével, a professzionális nagy távközlő hálózatok berendezés parkjainak felhasználásával, rendkívül sokféle, újszerű információ átviteli szolgáltatás valósítható meg. Ezek között is a 100-250 Mbit/s sebességű nagyszámítógépek közötti – real-time – valós idejű átviteli szolgáltatások, az A4-es formátumú távlevezetések, a nagymennyiségű, és gyorsan változó adathalmazok rövid időn belüli cseréi.

Napjainkig már számos szélessávú interaktív CATV hálózat épült ki a professzionális nagy távközlő hálózatok SDH-ATM technológiájú berendezés parkjának felhasználásával. A szélessávú interaktív CATV hálózat architektúrájában azok rendszertехnikai kiépítéseikben nagyterjedésű, nagy átviteli sebességű gyűrű/busz struktúrát alakítottak ki. A gyűrű/busz kiépítésekben a hublink optikai fénykábel vonalba, több különböző információt hordozó jelfolyamatokat gyűjtő fejállomások, hubok vannak beépítve. Az egyes szakaszokon beépített hubokon különböző routerek és gatewayeken keresztül folyik az információ áramoltatás. A gyűrű busz vonalak terjedelmére jellemző a nagy területet átfogó 15-30 km átmérő.

A fejállomásokhoz, hubokhoz számtalan starlink-HFC (hibrid optikai fénykábel – koax – kábel) busz vonal kapcsolódik. A starlink-busz vonalak gyakorlatban egyenként akár egy-egy üzemelő kisebb kiépítésű interaktív CATV hálózat is lehet. Egy-egy ilyen starlink-busz vonal – HFC kiépítéssel – egyrészt 5-750/850 MHz frekvenciasáv átvitelű AM optikai fénykábel vonalszakaszból, a különböző fa struktúrájú szétosztó koaxkábel-elosztó hálózati szakaszból áll. A közvetlen felhasználói szakaszok pedig már csillagpontos struktúrával kapcsolódnak a felhasználói berendezésekhez. A koaxkábel-elosztó szakaszokhoz nagyszámú, akár 100,000 – 500,000 előfizető is kapcsolódhat.

A starlink-busz optikai fénykábel vonal szakaszai egyrészt autentikusan lehetnek a hagyományos kiépítésű interaktív CATV hálózatok trónk kábel szakaszai. Ezek a trónk kábel szakaszok kiválthatók könnyen 750/850 MHz – 1 GHz átvitelű szélessávú pont-pont összeköttetésű vonalakra, a professzionális optikai fénytávközlésben elterjedt – AM – optikai-fénykábel vonalak eszköz-parkjaik felhasználásával. Ezek a trónk kábel vonalak hordozhatják, a mintegy 50-60 analóg szórakoztatató TV műsor csatorna AM-VSB RF jeleit, mind pedig mindkét irányban az overlay hozzáférő hálózatokon keresztül forgalmazott kis- és közepes sebességű, digitális jelfolyamokat. Ugyancsak ezeken a trónk vonalakon forgalmazhatók, nyalábolt formában a 100-200 Mbit/s nagysebességű, számítógépek közötti kétirányú kommunikációk is.

A starlink-busz vonalak ugyancsak autentikusak lehetnek a hagyományos kiépítésű interaktív CATV hálózatok feeder elosztó kábel szakaszaival is, kiegészítve azokat az optikai FDDI szétosztó eszközökkel. A starlink-busz trónk és feeder vonalakba kedve-

zően építhetők be az SDH - ATM technika 155 Mbit/s – 2.5 Gbit/s hierarchia szintű multiplexer berendezései, különböző multiplexer kapcsolási funkciókkal. Hiszen ezen multiplexer berendezések között a leágazó ADM, HUB, MUX valamint DXC kapcsolási funkciók kínálnak kedvező lehetőséget a nagysebességű interaktív CATV hálózatok funkcionális szolgáltatásainak kibővítéséhez a nagysebességű, címzett kétirányú kommunikációk folytatásához.

Annak ellenére, hogy a nagysebességű digitális multiplexerek és egyéb eszközök tisztán digitális üzeműek, a starlink-busz vonalak kevés kiegészítéssel kedvezően használhatók fel a vegyes analóg RF és digitális jelfogalmak átvitelére, hiszen éppen a több optikai szálú AM fénykábelek alkalmasak a vegyesen mind az analóg, mind a digitális jelforgalmazásokhoz. Természetesnek véve azt, hogy mind a trónk mind a feeder vonali kiépítések olyan kétirányú kommunikációs kapcsolatok lehetőségét valósítják meg, ahol perspektivikusan mind a fejállomásoktól az előfizetők-felhasználók felé irányuló jelfolyamok, mind pedig, az előfizetőktől a fejállomások felé irányuló jelfolyamok közel azonos arányban kerülhetnek átvitelre.

A korszerű SDH és ATM átviteli technológiák hálózati elemeinek felhasználásával kiépítendő sokszolgáltatású, interaktív CATV hálózatok rendszertechnikájában fontos kérdés, a különböző épületek lépcsőházi elosztópontjaiban üzemeltetendő technikai berendezések területe. Ugyanis ezekben az elosztó pontokban már a nagyszámú felhasználói – előfizetői – csoportok közvetlen kiszolgálására alkalmas berendezések kell, hogy beépüljenek. Alapjában, hogy milyenek is legyenek azon csomópontok berendezésparkjai, amelyeken keresztül közvetlenül kell, hogy eljussanak a kétirányú sokrétű szolgáltatások jelfolyamai a felhasználókhoz, több elgondolás is napvilágot látott. Miután ezeken a csomópontokon nagyobb számú a mintegy 30 - 50 előfizetői pont között már a korszerű nagysebességű számítógépek belső órajelével meghatározott 100-150 Mbit/s sebességű kétirányú kommunikációt is ki kell építeni, ehhez szükségszerűen merül fel a csomópontokban egy-két közepes kapacitású szerver számítógép az üzembeállítása. A szerver számítógépekkel való összekapcsolással az előfizetők számítógépei például egy lépcsőházon belül akár már Ethernet, vagy Token hálózati struktúrán keresztüli kiépítéssel is kommunikálhatnak egymással. Ugyanitt felmerül még egy másik nagyobb sebességű szerver számítógép igénye is a lépcsőházak közötti számítógépes kommunikációhoz, illetve a további nagyhálózati külső kapcsolatok létrehozásához. Ilyen berendezés parkkal napjainkban az előfizetők számítógépei között már folynak kommunikációs kapcsolatok.

A fenti technikai csomóponti rendszer kiépítése mellett, kézzelfogható, egy másik megoldás is. Egy másik kiépítésben, a lépcsőházi csomópontban üzembe állítható a mintegy 30 – 50 csatlakozási pontú és kapacitású hub funkciójú multiplexer berendezés csoport. Az SDH hub multiplexer berendezések üzemelhetnek oly módon is, hogy azokkal egy átlagos sebességű és kapacitású számítógép vezérlésével az előfizetők számítógépei csillaghálózaton keresztül kommunikálhatnak egymással. A hub funkciójú multiplexer berendezéscsoport akár STM-4-es kapacitású is lehet, amely ezáltal alkalmas a 100-150 Mbit/s sebességű jelek forgalmazására is. Ez utóbbi technikai megoldásnál kedvezően kihasználható olyan további előny is, hogy a hub funkciójú multiplexerek tributális pontjai képesek fogadni $n \times 64$, vagy $n \times 2048$ Kbit/s sebességű jelfolyamokat is. Más szóval a virtuális konténerek (VC) megtölthetők nagyszámú,

kisebbségi PDH jelfolyamokkal, akár vegyesen is együtt a nagysebességű jelfolyamokkal. Ez a megoldás még azt a lehetőséget is előreveti, hogy könnyen megvalósítható az alulról való sebesség növelési igényű építkezés a csomóponti berendezések a nagyobb hierarchia sebességek irányába, a fokozatosan magasabb szintű multiplexer berendezések üzembeállításával.

A fentiekből kitűnik, hogy pl. a lépcsőházi elosztópontokba a különböző hierarchia szintű modul rendszerű multiplexer berendezések multiplikált beépítésével, és a szerver vezérlésű kapcsolatokkal olyan interaktív szolgáltatási lehetőségek valósíthatók meg mint az ISDN által biztosított $n \times 64$ kbit/s duplex mód, az ADSL duplex üzemmód vagy az $n \times 2048$ kbit/s, vagy már a közvetlen nagysebességű 100 – 150 Mbit/s jelforgalmazás nyálábolt duplex üzemmóddal.

A jövőbeni szélessávú interaktív CATV hálózatokon forgalmazandó széleskörű szolgáltatásoknál természetesen merülnek fel az egy időbeni, több – párhuzamos kétirányú kisebb-nagyobb átviteli sebességű jelek forgalmazása. Ilyenek lehetnek többek között:

- multimédia kép és, hang és más kiegészítő tájékoztató információk jelfolyamainak egyidejű kétirányú forgalmazásával működő szolgáltatások (időtartam, poénok megválasztása, stb.)
- elektronikus távjátékok (pl. NINTENDO vagy JAVA alapú) szolgáltatásánál, ahol egy időben több párhuzamos csatornás kétirányú parancsok forgalmazására van szükség.
- Megbízható elektronikus kereskedelmi, banki tranzakciók bonyolítása.

Ez utóbbiaknál felhasználva a kriptográfia kutatás eredményeit, amikor is egy időben a tranzakciós jelekkel már csak 2-3 aktív kulcsos real-time jelfolyamokkal, állandó kriptográfiai kapcsolatok visszairányú regisztrálásával lehet biztosítani a tranzakciók sértetlenségét. Mindezek annál inkább is fontosak miután a számítógépekből származó egyes fájlok nem tartalmazzak ilyen irányú címzéseket.

A szélessávú interaktív CATV hálózatokon a szigorúan címzett egy időbeni többcsatornás kétirányú információ egzakt áramoltatására a WCDMA technika felhasználása ad lehetőséget. A WCDMA alapját a szórt spektrumú modulációs technika adja, ahol az információk továbbításánál egy-egy vivőjel többszörösen véletlen változással generált impulzus jelfolyammal az egy időben több egymástól eltérő ortogonális kóddal is modulálható. Ilyen kapcsolódó modulációk lehetnek

- a scrambling kód, amely alkalmas az különböző identifikációs kódok hordozására
- csatorna kód, amely a különböző információt hordozó csatornák megkülönböztető kódja lehet
- szórás kód, amely az összetartozó csatornák szétválaszthatóságot biztosítja.

Összességében a felvázolt perspektívikus szolgáltatások bevezetése bár még csak a jövőt vetik előre, mégis különös fontossággal bírhat a nagyszámú címzett párhuzamos

csatornák egyidejű működtetésénél. Tudomásul kell venni, hogy minden előfizetőnél a többszörös multiplexeléssel forgalmazott jelfolyamatokból folyamatos szelektálással kell biztosítani az érkezett információkat.

Felhasználva a fenti hálózati kiépítéseket a csillaghálózati csatlakozási pontokhoz kapcsolódó előfizetők a lakásaikban, irodai helységeiben már igen széles skálán elhelyezkedő adatátviteli kommunikációs berendezések működtethetők. Napjainkban az előfizetőknél a sokrétű információszolgáltatás fogadására az interfészek óriási bázisa áll rendelkezésre. Az előfizetőknél rendelkezésre áll a hibrid, analóg-digitális egyirányú és a duplex összeköttetésű információ jelátvitel forgalmazásához minden szükséges eszköz, amelyek igen széles már néhány kbit/s-tól a néhány száz Mbit/s bitsebesség tartományban üzemelhetnek. Ideértve az olyan sokrétű információt reprodukáló interfészeket, a helyi-központi vezérlő terminálokat, mint az előfizetői vezérlő választó berendezés, amit ma az angolból átvett módon SET TOP boxoknak nevezünk. Ezekkel a set top készülékekkel valósítható meg egy-egy információ fajta kiválasztása, hívás kezdeményezése és az átláthatóság kiépítése a különböző információforrás központokkal. De ezekben a készülékben indul el a címzés, a titkosítás és a tarifális funkciók regisztrálási és kezdeményezési folyamata is. Ugyancsak ebben az egységben vannak beépítve különböző multiplexerek, kombinátorok és modemek, majd egyéb hálózat elérési részek is, amelyek a távvezérlési funkciók részei. Természetesen tudomásul kell venni, hogy nem minden interfész eszköz rendelkezik nagybonyolultságú, nagyintelligenciájú kiépítéssel, így pl. a fogyasztási célú eszközök sem. Mindebből adódóan, a set top boxok ma még a legkülönbözőbb intelligenciájú kiépítéssel vannak forgalomban. Különösen, ha meggondoljuk, hogy a multimédia legújabb szolgáltatásait vezérlők még hiányoznak, hiszen azok csak az utóbbi időkben láttak napvilágot.

* * *

A KATASZTRÓFAVÉDELMI KOMMUNIKÁCIÓ JOGI SZABÁLYOZÁSA MAGYARORSZÁGON

A természet elemi erőinek, az időjárásnak és Föld mélyén rejlő energiáknak szélessége jelenti napjainkban az egyik legjelentősebb veszélyforrást az emberi környezetre, hiszen ezek képviselik azon kevés tényezők egyikét, melyet mesterséges úton nem vagyunk képesek elvárásainknak megfelelően, irányított módon befolyásolni. Földrengések, árvizek, tornádók orkánok, hurrikánok, szökőárak, lavinák ezrei bizonyítják évről-évre, hogy milyen sebezhetőek és védtelenek is vagyunk valójában. Azonban nem csak elemi csapások veszélyeztetik civilizációnkat, hanem olyan, ipari balesetek, terrortámadások, vagy egyéb emberi tevékenység következményeként kialakuló katasztrófák, melyeket felelőtlenség, gondatlanság, téves ideológiák táplálta gyűlölet eredményez.

Beszéljünk akár természeti, akár civilizációs katasztrófákról, az ellenük való védekezés, a károk enyhítése, felszámolása, az emberáldozatok csökkentése, egyszóval a katasztrófavédelem komplex és bonyolult feladat, széleskörű összefogást követel a társadalom minden szereplőjétől. Ezen a jelenségek gyakran határokon is átnyúlva fejtik ki káros hatásukat, így az ellenük való védekezésben szükség van átfogó kooperatív és gyakorlati nemzetközi együttműködésre.

A XXI. századra a fegyveres erők feladatainak prioritási szintjei a nemzetközi biztonsági környezet gyökeres megváltozásának hatására jelentősen eltolódtak, így a területvédelem mellett a hangsúly a terrorizmus elleni küzdelemre, az etnikai konfliktusok megelőzésére, béketeremtésre, békefenntartásra, katasztrófák megelőzésére, illetve káros következményeinek felszámolására helyeződött. Bár ez utóbbi terület nem a Magyar Honvédség irányítása alá tartozik, szerepe mégsem kérdőjelezhető meg, hiszen vannak olyan speciális képességek, technikai eszközök, járművek, emberi erőforrások, amelyekkel Magyarországon egyetlen más szervezet sem rendelkezik. Ide tartozik például a szervezeti szinten egyedülálló logisztikai támogatás, amellyel a hadsereg elhúzódnó védekezési műveletek esetén is képes biztosítani egységei számára az utánpótlást (pl.: nagy kiterjedésű erdőtűzek, tiszai árvizek, hó okozta rendkívüli helyzetek stb.).

A katasztrófavédelemben, mint komplex rendszerben, melynek elemi többek között a politikai és szakmai irányító szervek, a Honvédség, Katasztrófavédelem, Polgári védelem, Tűzoltóság, Rendőrség, Határőrség, Mentőszolgálat, valamint számos más helyi és országos hatáskörű szervezet, kiemelt szerepe van az információk cseréjének, a kommunikációnak. A legfontosabb feladatok egyike, hogy a mentésben, illetve védekezésben résztvevők állandó összeköttetésben legyenek egymással, a technikai eszközök kezelőivel, a munkálatokat irányító helyi és központi parancsnokságokkal.

Az ilyen hírközlési rendszerek esetében, alapvető követelmény az állandó, megbízható rendelkezésre állás, valamint a biztonságos együttműködési képesség (kompatibilitás).

Vizsgálni, elemezni szükséges tehát, hogy katasztrófahelyzetben milyen távközlési rendszerek és állnak rendelkezésre a védekezés vezetési feladatainak technikai biztosí-

tására, továbbá miként lehet az ország különböző távközlő hálózatait igénybe venni ilyen feladatok ellátására.

Jelenlegi állapotok szerint a forgalom jelentős hányada a különböző szervezetek zártcélú hálózatai mellett a vezetékes és mobil szolgáltatók hálózatain bonyolódik, így foglalkozni szükséges a különböző kormányzati és országos hatásközü szervek, valamint a piaci alapokon működő távközlési szolgáltatók együttműködését, hálózataik minősített időszakokban történő összekapcsolását érintő jogi szabályozással.

A vonatkozó jogszabályok tanulmányozása előtt mindenképpen fontos az alapvető, kapcsolódó szakkifejezések definiálása.

A **minősített időszak** a Magyar Köztársaság Alkotmányáról szóló 1949. évi XX. törvény 19. § (3) bekezdésének h) és i) pontjában meghatározott *rendkívüli állapot* és *szükségállapot*, valamint a 35. § (1) bekezdésének i) pontja, és a polgári védelemről szóló 1996. évi XXXVII. törvény 2. § (2) bekezdése szerinti *veszélyhelyzet* összefoglaló megnevezése. Ezek értelmében a **rendkívüli állapot**, hadiállapot, vagy idegen hatalom fegyveres támadásának közvetlen veszélye (háborús veszély) esetén kihirdetett állapot, aminek kihirdetésére az országgyűlés, annak akadályoztatása esetén a köztársaság elnök jogosult.

A **szükségállapot**, az alkotmányos rend megdöntésére, vagy a hatalom kizárólagos megszerzésére irányuló fegyveres cselekmények, továbbá az *állampolgárok élet- és vagyonbiztonságát tömeges mértékben veszélyeztető*, fegyveresen vagy felfegyverkezve elkövetett súlyos erőszakos cselekmények, *elemi csapás vagy ipari szerencsétlenség* (együtt: szükséghelyzet) esetén kihirdetett állapot, melynek kihirdetésére az Országgyűlés, annak akadályoztatása esetén a köztársasági elnök jogosult.

A **veszélyhelyzet**, a szükséghelyzetet el nem érő mértékű, az *állampolgárok élet- és vagyonbiztonságát vagy a környezetet veszélyeztető természeti csapás, illetőleg ipari baleset okozta állapot*, melynek kihirdetésére a Kormány jogosult.

Az Alkotmány, valamint a Polgári védelmi törvény alapján, a katasztrófák elleni védekezés irányításáról, szervezetéről és a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről szóló 1999. évi LXXIV. törvény 3. § f) pontja - figyelemmel a d), e) és k) pontokra a **katasztrófahelyzetet** a következőképpen definiálta: olyan mértékű *katasztrófaveszély*, illetőleg bekövetkezett *katasztrófa*, amikor az arra felhatalmazott állami szerv vezetője a *katasztrófa* veszélyének, bekövetkezésének tényét megállapította, és a szükséges intézkedéseket elrendelte. A d), e) és k) pontok tartalma a következő:

d) **Nemzetközi segítségnyújtás**: külföldi államoknak az ENSZ-hez, a NATO-hoz, illetőleg nemzetközi szerződés alapján a Kormányhoz közvetlenül továbbított, illetve a regionális határmenti egyezmények segítségnyújtási igénye alapján *katasztrófák* következményeinek felszámolásához nyújtott anyagok és információk átadása, illetve a mentéshez és a *katasztrófa* következményeinek a felszámolásához kiküldött eszközök és személyi állomány biztosítása.

e) **Katasztrófa**: a *szükséghelyzet* vagy a *veszélyhelyzet* kihirdetésére alkalmas, illetőleg a *minősített helyzetek* kihirdetését el nem érő mértékű olyan állapot vagy helyzet (pl. természeti, biológiai eredetű, tűz okozta), amely emberek életét, egészségét, anyagi értékeit, a lakosság alapvető ellátását, a természeti környezetet, a természeti értékeket olyan módon, vagy mértékben veszélyezteti, károsítja, hogy a kár megelőzése, elhárítása vagy a következmények felszámolása meghaladja az erre rendelt szerveze-

tek előírt együttműködési rendben történő védekezési lehetőségeit és különleges intézkedések bevezetését, valamint az önkormányzatok és az állami szervek folyamatos és szigorúan összehangolt együttműködését, illetve *nemzetközi segítség* igénybevételét igényli.

k) **Katasztrófaveszély:** olyan folyamat vagy állapot (pl. természeti, biológiai eredetű, tűz okozta), amely közvetlenül és súlyosan veszélyezteti az emberi egészséget, környezetet, az élet- és vagyonbiztonságot, ha okszerűen lehet számolni a katasztrófa bekövetkezésének valószínűségével.

Ugyanezen paragrafus j) pontja a **katasztrófavédelem** fogalmát így határozta meg: a különböző *katasztrófák* elleni védekezésben azon tervezési, szervezési, összehangolási, végrehajtási, irányítási, létesítési, működtetési, tájékoztatási, riasztási, adatközlési és ellenőrzési tevékenységek összessége, amelyek a *katasztrófa* kialakulásának megelőzését, közvetlen veszélyek elhárítását, az előidéző okok megszüntetését, a károsító hatások csökkentését, a lakosság élet- és anyagi javainak védelmét, a katasztrófa sújtotta területen az alapvető életfeltételek biztosítását, valamint a mentés végrehajtását, továbbá a helyreállítás feltételeinek megteremtését szolgálják.

A definíciók fenti rendszere segítséget nyújthat a következőkben tárgyalt jogszabályok alkalmazási körülményeinek értelmezéséhez.

A katasztrófák elleni védekezés irányításáról, szervezetéről és a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről szóló 1999. évi LXXIV. törvény határozza meg a védekezésben résztvevő kormányzati és belügyi szervek, felelős személyek feladatait, az egyéb szervezetekkel való együttműködés, valamint a nemzetközi segítség igénybevételének kereteit.

A jogszabály 26. §-a alapján a katasztrófavédelem központi szerve a Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság, amely elsősorban tervezési, szervezési, felkészítési, irányítási, felügyeleti, szakértői és szakhatósági feladatokat lát el a védekezés, illetve a védekezésre való felkészülés folyamán.

A 2. § (1) bekezdése rendelkezik a katasztrófavédelemben résztvevők együttműködési kötelezettségéről: A védekezést és a következmények felszámolását az erre a célra létrehozott szervek és a különböző védekezési rendszerek működésének összehangolásával, valamint a polgári védelemről szóló 1996. évi XXXVII. törvény alapján létrehozott polgári védelmi szervezetek, a hivatásos katasztrófavédelmi szervek, a hivatásos önkormányzati tűzoltóság, a gazdálkodó szervezetek, a *Magyar Honvédség*, a Hátőrőrség, a rendvédelmi szervek és az állampolgárok, továbbá az Országos Meteorológiai Szolgálat, az Országos Mentőszolgálat, az Állami Népegészségügyi és Tisztiorvosi Szolgálat, az önkéntesen részt vevő társadalmi szervezetek, valamint a civil és az erre a célra létrehozott köztestületek, továbbá a nem természeti katasztrófák esetén annak okozója és előidézője, az állami szervek és az önkormányzatok bevonásával, illetve közreműködésével kell biztosítani.

A 8. § b) és c) pontja szerint a kormány intézkedhet a *Magyar Honvédség*, a Hátőrőrség, illetve a rendvédelmi szervek bevonásáról, valamint ha a védekezéshez vagy a következmények felszámolásához a *Magyar Honvédség* békeállományának erői, eszközei nem elegendőek, dönt a Honvédelmi törvény 124. § (5) bekezdése szerint a tartalékos hadkötelesek igénybevételéről, illetve a leszerelő hadkötelesek tartalékos katonai szolgálatra történő visszatartásáról és a szolgálatteljesítés időtartamáról és

rendjéről. (Ezen pontok módosítása a sorozások felfüggesztése, vagy a kötelező sorkatonai szolgálat eltörlése esetén szükségessé válik.)

A 10. § c) pontja kimondja, hogy a Kormányzati Koordinációs Bizottság hangolja össze a *Magyar Honvédség*, a Határőrség és a rendvédelmi szervek védekezési tevékenységét.

A *Magyar Honvédség* katasztrófavédelem rendszerében betöltött szerepének kereteit a honvédelemről szóló 1993. évi CX. törvény rögzíti, egységes szerkezetben a végrehajtásáról szóló 178/1993. (XII. 27.) kormányrendelettel. A 2002-ben indított védelmi felülvizsgálat eredményeként meghatározott feladatok között, a polgári hatóságok támogatása címszó alatt a katasztrófavédelem is helyet kapott, mint az új biztonsági kihívások egyik legfontosabb eleme.

A katasztrófavédelemben résztvevő szervezetek hatékony együttműködésének alapja a megfelelő kommunikációs csatornák biztosítása, ami messze túlmutat a különböző zártcélú hálózatok összekapcsolásán.

A rendszerváltás előtt az 1964/II. Posta törvény deklarálta, hogy a postai és távközlési feladatok állami tevékenységi körbe tartoznak, azaz 1989-ig az állami tulajdonú Magyar Posta monopóliuma volt minden távközlési és postai szolgáltatás, beleértve a rádió és televízió műsorszórást, valamint a frekvenciagazdálkodást. Ebben az időszakban az országvédelmi érdekek érvényesítését nem befolyásolják a privatizált távközlő szolgáltatók profitorientált törekvései.

Amikor 1989-ben a Közlekedési, Hírközlési és Építésügyi Minisztérium átvette a szabályozási funkciókat, kettéválasztották a fenti felügyeleti jogkört, két hatóságot hozva létre: a Posta és Távközlési Főfelügyeletet és a Frekvenciagazdálkodási Intézetet. A postai, távközlési és műsorszóró szolgáltatásokat 1990-ben választották szét, aminek eredményeként létrejött az állami tulajdonú Magyar Távközlési Vállalat, a Magyar Műsorszóró Vállalat, valamint a Magyar Posta Vállalat. A távközlés valódi reformjának kezdetét, a Koncessziós törvény által megteremtett alapokon (privatizáció lehetősége), az új távközlési törvény elfogadása, illetve hatályba lépése jelentette.

A *távközlésről szóló 1992. évi LXXII. törvény* meghatározta a távközlési szolgáltatások nyújtásának módját és feltételeit, a távközlési szolgáltatásban résztvevők (szolgáltatók, üzemeltetők, tulajdonosok, igénybe vevők, előfizetők) jogait és kötelezettségeit, a távközlő hálózat tervezésének, létesítésének, üzemben tartásának, védelmének, és a távközlő hálózatok együttműködésének lehetőségeit, azzal a kitételrel, hogy a zártcélú távközlő hálózatokra vonatkozó szabályokat kormányhatározat állapítja meg. [1]

Ebben a jogszabályban került megfogalmazásra a *közcélú távbeszélő hálózat*, *különcélú távközlő hálózat*, *sajátcélú hálózat*, *a zártcélú hálózat*, valamint a *rendkívüli összeköttetés* definíciója, továbbá a különböző rendeltetésű hálózatok összekapcsolásának alapelve.

Ezek alapján:

A **közcélú távbeszélő hálózat** olyan távközlő hálózat, mely az állandó helyű szolgáltatás-hozzáférési pontok között lehetővé teszi 0,3–3,4 kHz közötti hangfrekvenciás jelek átvitelét többek között távbeszélő beszéd-összeköttetések felépítése és fenntartása, vagy legalább 2400 bit/s sebességű modemes adatátvitel útján. A hívott előfizető elérése a nemzeti, illetőleg nemzetközi számozási tervben rögzített választási eljárás útján lehetséges.

A **különcélú távközlő hálózat** zárt felhasználói csoportot alkotó igénybevevők által használt távközlő hálózat, melyen elsődlegesen azok belső távközlési forgalma bonyolódik.

A **saját célú hálózat** olyan távközlő hálózat, melyet egy adott vállalkozás vagy személy kizárólag saját távközlési igényeinek kielégítésére használ.

A **zártcélú hálózat** kormányzati, nemzetbiztonsági, igazságszolgáltatási, közbiztonsági és védelmi érdekeket szolgáló – rendeltetésük szerint elkülönült – távközlő hálózatok és berendezések együttese, melyek kizárólagosan a speciális igények kielégítését, az e célra létrehozott szervezet és technika működését szolgálják.

A közcélú távközlő hálózatok egymással, illetőleg más távközlő hálózatokkal történő összekapcsolásának, továbbá a különféle távközlő hálózatok összekapcsolásának feltételeit értelmezve a távközlő hálózatok együttműködése terén szóba jöhet:

- közcélú távközlő hálózat összekapcsolása más távközlő hálózattal
- külön célú távközlő hálózat összekapcsolása közcélú távközlő hálózattal
- külön célú távközlő hálózat összekapcsolása külön célú távközlő hálózattal
- rendkívüli összekötés

A különféle távközlő hálózatokat olyan szabványos műszaki feltételek szerint kell felépíteni és működtetni, hogy a jogszabályban meghatározott esetekben szükséges kapcsolat létesítéséhez, a megfelelő egységek (hálózati elemek, berendezések, eszközök stb.) beiktatásával működőképes, egységes rendszert alkothassanak. A távközlési szolgáltatók ezért az ország közcélú távközlő hálózatának egysége érdekében a hálózatok létesítése, működtetése, módosítása és megszüntetése során együttműködni kötelesek, ami kiterjed a kölcsönös tájékoztatásra és adatszolgáltatásra, a működtetéshez kapcsolódó mérésekre, a karbantartási rendszerek összehangolására, a szolgáltatási zavarok elhárítására.

A **rendkívüli összekötés** meghatározása a következő: *rendkívüli állapot, szükségállapot, ipari katasztrófa*, továbbá az állampolgárok élet- és vagyonbiztonságát veszélyeztető elemi csapás, illetőleg ezek következményeinek elhárítása céljából *különcélú távközlő hálózat közcélú távbeszélő hálózattal* összeköthető. A rendkívüli összekötés nem minősül összekapcsolásnak.

A rendkívüli összekötésre tekintettel a hálózati szolgáltatóknak és az üzemeltetőknek egyeztetéseket kell végezniük, figyelembe véve, hogy a rendkívüli összekötés ne veszélyeztesse a külön célú hálózat rendeltetésszerű működésének fenntartását. [1]

(A távközlési törvényt az 1997. évi LXV. törvény módosította, az időközben elfogadott hazai és európai jogszabályokhoz való harmonizáció megteremtése érdekében.)

A **hírközlésről szóló 2001. évi XL. törvényben** ismét egyesítették a távközlési és postaszolgáltatásokra vonatkozó jogi szabályozást. A 13. §-a kimondja, hogy a hírközlési szolgáltatók közérdekű kötelezettsége, hogy közreműködjenek a más törvényekben meghatározott, közbiztonságot, nemzetbiztonságot érintő, illetőleg *védelmi feladatok* ellátásában. A szolgáltatóknak együtt kell működniük a zártcélú hálózatok üzemeltetőivel, továbbá *rendkívüli állapot* és *katasztrófa* esetén felmerülő sajátos távközlési feladatok ellátása érdekében együtt kell működniük mind egymással, mind pedig az arra illetékes szervezetekkel. A szolgáltató az e körben végrehajtott intézkedései és nyújtott szolgáltatásai után azok tényleges költségeinek megtérítésére jogosult. A szolgáltatás és az együttműködés biztonsága, megbízhatósága és zavartalansága megköveteli, hogy a szolgáltató felkészüljön a műszaki eredetű és a külső veszélyeztető

körülmények által okozott üzemzavarok elhárítására, továbbá a *rendkívüli állapot és katasztrófa* esetében reá háruló sajátos feladatokra. E helyzetek kezelésére adott esetben a szolgáltatónak megfelelő tervekkel és eszköz-tartalékokkal kell rendelkeznie, ezért folyamatos feladat ezek készítése, készletezése, illetőleg felülvizsgálata, karbantartása. A 107. § felhatalmazást ad a Kormány részére, hogy megalkossa a korlátozott erőforrás-gazdálkodással, a hírközlés veszélyhelyzeti és minősített időszaki felkészítési rendjével, a hatóság szervezetével és működésével, a szolgáltatások nyújtásával kapcsolatos szabályait. (Ezen felhatalmazást az elektronikus hírközlésről szóló törvény szövegébe is átemelték.)

A hírközlésről szóló 2001. évi XL. törvény alapvető célkitűzései közé tartozott, hogy

- biztosítsa a hírközlési szolgáltatások - mint közérdekű szolgáltatások – elérhetőségét és a nemzetközi szerződéseinkkel összhangban lévő szabad forgalmát,
- megteremtse az információs társadalom hírközlési infrastruktúrájának fejlődését elősegítő, kiszámítható, átlátható, a használt technológiától független és versenysemleges szabályozás kereteit,
- elősegítse a hírközlési verseny fejlődését és új szereplők piacra lépését a jelentős piaci erővel rendelkezők befolyásának - a hatékony versenypiac kialakulásához és fenntartásához szükséges mértékű - differenciált ellensúlyozásával,
- szükség esetén iparági keresztfinanszírozással tegye lehetővé, hogy az alapvető szolgáltatások egy meghatározott köre az országban bárhol, előírt minőségben és elérhető áron, bárki számára hozzáférhető legyen,
- biztosítsa a fogyasztók védelmét és a hírközléssel összefüggő adatvédelmet,
- biztosítsa az összeegyeztethetőséget az Európai Közösség hírközlés szabályozásával és elősegítse a magyar hírközlési piacnak a közösség piacába való integrálódását.

A jogszabály azonban nem váltotta be teljes egészében a hozzá fűzött reményeket, és habár a MATÁV és a többi koncessziós társaság kizárólagos szolgáltatási joga megszűnt, nem alakult ki igazi piaci verseny. Az Európai Unió az 1998-as liberalizáció sikeres végrehajtását követően átfogó reformba kezdett a távközlés területén azzal a céllal, hogy a piac szegmensein az ágazati szabályozás alkalmazott mértéke dinamikusan a hatékony verseny kialakulása és fenntartása által igényelt szinthez legyen igazítható. Az új közösségi szabályozás ezért felhatalmazta a nemzeti szabályozó hatóságokat arra, hogy kellő gyakorisággal végrehajtandó piacelemzés eredményétől függően a hatékony verseny kialakulásához, illetve fenntartásához szükségesnek ítélt piacélénkítő intézkedéseket vezessenek be, tartsanak fenn, illetve szüntessenek meg egy meghatározott eszköztárból. Az egységes belső piacon az egységes jogalkalmazás megteremtése céljából az új közösségi szabályozás a nemzeti szabályozó hatóságok szoros együttműködését rendeli el, továbbá tevékenységük felett az Európai Bizottságnak erős felügyeleti jogkört biztosít. Magyarország nem kért átmeneti mentességet az új szabályozás hazai bevezetése alól, így csatlakozásunkig nemcsak az elmaradt, illetve hibásan bevezetett EU-s jogintézményeket kellett pótolni, korrigálni, hanem el kellett végezni az új szabályrendszer jogharmonizációját is.

A piaci anomáliák, továbbá a jogharmonizációs kényszer a hírközlés hazai szabályozásának átfogó felülvizsgálatát tette szükségessé. Ennek eredményeként a hírközlési törvényt olyan nagymértékben kellett volna módosítani - a legtöbb fogalom meghatározásának tartalmi pontosítására is kiterjedően - hogy a félreérthetőség elkerülése és a kezelhetőség érdekében új törvény megalkotása vált szükségessé. (A felülvizsgálat eredményeként ismét szétválasztásra került a távközlési és postai tevékenységek szabályozása.) Ennek folyományaként 2004. január 1.-étől hatályba lépett a **2003. évi C. törvény az elektronikus hírközlésről**, mely számos ponton eltér elődjétől.

Az egyik legjelentősebb változás, hogy a szabályozó hatóság vonatkozásában új szervezeti modellt hoztak létre, megalakult a Nemzeti Hírközlési Hatóság (korábban: Hírközlési Főfelügyelet), melynek irányítását a kormány, felügyeletét az ágazati miniszter, vezetését a Tanács látja el. A hatóság feladata az elektronikus hírközlési piac zavartalan, eredményes működésének és fejlődésének, az elektronikus hírközlési tevékenységet végzők és a felhasználók érdekei védelmének, továbbá a tisztességes, hatékony verseny kialakulásának, illetve fenntartásának elősegítése az elektronikus hírközlési ágazatban, valamint az elektronikus hírközlési tevékenységet végző szervezetek és személyek jogszabályoknak megfelelő magatartásának felügyelete.

A *Magyar Honvédség* távközlő hálózatainak működését jogilag megalapozva, a zártcélú hálózatokkal kapcsolatban a törvény a következőképpen rendelkezik:

A törvényt kizárólag kormányzati, nemzetbiztonsági, igazságszolgáltatási, rendvédelmi, illetőleg védelmi igények kielégítését szolgáló - rendeltetésük szerint elkülönült - hírközlő hálózatok (zártcélú hálózatok) tekintetében, a rájuk vonatkozó külön törvényekben és más jogszabályokban foglalt eltérésekkel kell alkalmazni. (50/1998. kormányrendelet)

A Nemzeti Hírközlési Hatóság a zártcélú hálózatok létesítése, összekapcsolása, fejlesztése, korszerűsítése során a zártcélú hálózatokról szóló jogszabály szerint egyeztet a hálózatgazdákkal.

Az elektronikus hírközlési szolgáltatónak - jogszabályban meghatározott esetekben - együtt kell működnie a zártcélú hálózatok üzemeltetőivel.

A Kormány felhatalmazást kap, hogy rendelettel állapítsa meg az elektronikus hírközlés vonatkozásában a zártcélú hálózatokra vonatkozó, e törvénytől eltérő szabályokat. [a jelenleg is hatályos zártcélú távközlő hálózatokról szóló 50/1998. (III.27.) kormányrendelet utolsó módosítása az 5/2004 (I.9.) kormányrendelettel történt]

A *katasztrófavédelmi kommunikációt* érintő kérdések tekintetében az Elektronikus hírközlési törvény a következőket tartalmazza:

A törvény egyik céljaként szerepel az elektronikus hírközlés állami feladatai ellátásával kapcsolatos alapvető szabályok meghatározása, különös tekintettel az elektronikus hírközlés biztonságára, veszélyeztetettségére, a *rendkívüli állapot*, *szükségállapot* vagy *veszélyhelyzet* idejére irányuló felkészítés rendjére.

A Kormány feladatául szabja, hogy meghatározza az elektronikus hírközlés biztonságának alapelveit, *minősített időszaki* felkészítésének rendszerét, biztosítja az államigazgatásra háruló feladatok ellátásának feltételeit.

Az informatikai és hírközlési miniszter részt vesz az elektronikus hírközlés nemzetbiztonsági és védelmi jellegű feladatainak végrehajtásában, kijelöli a honvédelmi és a *katasztrófavédelmi* feladatok ellátásában részt vevő elektronikus hírközlési szolgáltatókat, meghatározza a minősített időszaki helyzetekre történő felkészüléssel kapcsolata-

tos feladatokat, koordinálja az elektronikus hírközléssel kapcsolatos polgári, kormányzati, nemzetbiztonsági, igazságszolgáltatási, rendvédelmi és védelmi tevékenységet.

Minősített időszak esetén, illetőleg következményei elhárítása érdekében - a Honvédelmi Tanács, a köztársasági elnök, illetve a Kormány döntése alapján – az ágazati miniszter határozattal állapítja meg az elektronikus hírközlési tevékenység átmeneti korlátozását vagy szünetelését.

Az elektronikus hírközlési szolgáltatók a nyilvános elektronikus hírközlő hálózatok üzemeltetésével, valamint a hálózatok összekapcsolásával, illetve azokhoz való hozzáféréssel megvalósuló együttműködéssel összefüggésben kötelesek minősített időszakban külön jogszabályban meghatározott módon együttműködni más szolgáltatókkal.

A 92. § (5) (6) (7) pontjai alapján fogalmazhatók meg általánosságban az elektronikus hírközlési szolgáltatók kötelezettségei:

(5) Az elektronikus hírközlési szolgáltatónak - jogszabályban meghatározott esetekben -

együtt kell működnie a zártcélú hálózatok üzemeltetőivel.

(6) Műszaki, forgalmi, *katasztrófa* vagy egyéb veszély miatt keletkező üzemzavar elhárításához a szolgáltató köteles külön jogszabályban meghatározott tartalmú, folyamatosan felülvizsgált és karbantartott felkészülési, zavarelhárítási és katasztrófaelhárítási tervekkel és a felkészülésre vonatkozó jogszabályokból következő

feladatok ellátásához szükséges mértékű és összetételű tartalékokkal rendelkezni.

(7) Minősített időszak esetében alkalmazandó intézkedési terv kidolgozása és végrehajtása

érdekében az elektronikus hírközlési szolgáltatóknak külön jogszabályban meghatározott módon együtt kell működniük egymással, illetve az illetékes szervezetekkel.

(Ugyanezen paragrafus (8) bekezdése rendelkezik a nyújtott szolgáltatások ellentételezéséről.)

Az elektronikus hírközlésről szóló 2003. évi C. törvény 182. §-a három, védelemmel kapcsolatos jogszabály kidolgozására ad felhatalmazást:

- az elektronikus hírközlés veszélyhelyzeti és minősített időszaki felkészítésének rendszeréről, az államigazgatási szervek feladatairól, működésük feltételeinek biztosításáról szóló kormányrendeletre (hatályba lépett, 100/2004)
- a zártcélú távközlő hálózatokról szóló kormányrendeletre (előkészítés alatt),
- a védelmi feladatokban résztvevő elektronikus hírközlési szolgáltatók kijelöléséről és felkészülési feladataikról szóló IHM rendeletre (előkészítés alatt).

A fenti pontokhoz kapcsolódó több tucat jogszabály közül a rendeletek megalkotásakor ötnek kiemelt szerep jutott:

- 50/1998. (III. 27.) kormányrendelet a zártcélú távközlési hálózatokról (Alapvetően ezen rendelet „távközlés honvédelmi felkészítésével” foglalkozó részeire épülnek a 100/2004 megfelelő paragrafusai, továbbá a kizárólag a zártcélú hálózatokkal foglalkozó szakaszainak felhasználásával folyik az új, zártcélú hálózatokról szóló kormányrendelet tervezet kidolgozása.)
- a honvédelemről szóló 1993. évi CX. törvény (Ez az ország védelmi felkészítésének alapvető dokumentuma.)

- 133/1994. (X. 21.) kormányrendelet váratlan légitámadás esetén az ország légiriasztásáról (A lakosság légiriasztásával és tájékoztatásával kapcsolatos feladatok általánosságban bekerültek 100/2004 kormányrendeletbe, illetve az érintett szolgáltatók kijelölésével foglalkozó miniszteri rendelet tervezetébe.)
- a katasztrófák elleni védekezés irányításáról, szervezetéről és a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről szóló 1999. évi LXXIV. törvény (veszélyhelyzetek kategorizálása)
- 131/2003 (VIII. 22.) kormányrendelet a nemzetgazdaság védelmi felkészítése és mozgósítása feladatai végrehajtásának szabályozásáról (A nemzetgazdaság egészére megfogalmazott gazdaságmorgósítási elvek egy része szolgált alapul az elektronikus hírközlés - mint a nemzetgazdaság egyik ága – felkészítésének szabályozására.)

Az elektronikus hírközlésről szóló törvény felhatalmazásai alapján tehát egyetlen jogszabály lépett hatályba, a **100/2004 (IV. 27.) kormányrendelet az elektronikus hírközlés veszélyhelyzeti és minősített időszak felkészítésének rendszeréről, az államigazgatási szervek feladatairól, működésük feltételeinek biztosításáról**, amely részletesen meghatározza a védelmi felkészítés céljait és elveit, illetőleg a zártcélú távközlő hálózatokról szóló 50/1998. (III. 27.) kormányrendelet korábban e tárgyban megfogalmazott egyes rendelkezéseit megújítja, érvényre juttatva az azóta életbelépett új szabályokat, szervezeti, hatásköri módosulásokat, a megváltozott szemléletet mind a hírközlési, mind a védelmi politika terén.

Az elektronikus hírközlés védelmi felkészítési rendszerének önálló jogszabályban történő szabályozása többek között azért fontos, mert a nemzetgazdaság ezen ágánál a veszélyhelyzetek kialakulása – a biztonságpolitikai elveknek megfelelően – elsődlegesen regionális méretekben, meghatározott térségekre korlátozódva, az új típusú és hagyományos kihívások egyidejű megjelenésével történhet. A hálózatok kapcsolódása, a forgalmi, kommunikációs sajátosságok, a távközlés és az informatika összefonódása következtében az elektronikus hírközlésben jelentkező hatásuk ennél kiterjedtebb, akár országos szintű is lehet. Alátámasztja a téma fontosságát, hogy a távközlési erőforrások biztosításáról katasztrófa-elhárítás és mentés céljára tárgyú Tamperei Egyezmény nemzetközi sikra is kiterjeszti az elektronikus hírközlésben adódó veszély- és katasztrófa-helyzetek kezelésében történő együttműködést.

Mindezeket figyelembe véve a rendelet – a hatályos jogszabályi elemekre alapozva és azok továbbfejlesztésével – határozza meg:

- az elektronikus hírközlés felkészítési rendszerének általános értelmezését;
- a felkészítés célját;
- a felkészítés rendszerének összetevőit, amelyek magukba foglalják az állami feladatokat, a hatásköröket, a tervezést és a naprakészen tartást, a feladatok végrehajtásának rendjét (együttműködés, irányítás stb.), a végrehajtás (megvalósítás, üzemeltetés, fenntartás) finanszírozását, a szervezeti feltételeket, a veszélyhelyzet bekövetkezésének kezelését, valamint az események alatti és utáni (visszaállítási) tevékenységeket;
- a felkészítési rendszer összetevőinek ellenőrzését, gyakorlását.

A rendszer elemeinek felsorolásából következik, hogy az állami feladatok többsége csak a szolgáltatókkal történő együttműködés során valósítható meg. Az állam és a

szolgáltatók együttesen oldják meg az elektronikus hírközlés felkészítési rendszerébe tartozó feladatokat, a rendelet azonban megosztja a feladatköröket.

A rendelet, a *védelmi felkészítés elveinél* aktualizált formában átvette a zártcélú távközlő hálózatokról szóló 50/1998. (III. 27.) kormányrendelet 3. sz. mellékletéből az állami és szolgáltatói feladatkörök általános elhatárolását, valamint a honvédelmi rendeltetésű összeköttetési igények kielégítésének sorrendjét.

Ugyanakkor az elektronikus hírközlési törvény szabályozási elvei alapvetően módosították az állam beavatkozási lehetőségét a hírközlés piaci viszonyaiba. Míg az eredeti melléklet a távközlés felkészítésének általános elveiből adódó feladatokat „állami feladatként” határozza meg, amelyen belül a kötelező előírások alkalmazása képezi a szolgáltatók kötelezettségét, addig az új rendelet az elektronikus hírközlés védelmi felkészítéséből adódó feladatokat „egységes és közös tevékenységként” fogja fel, amelyen belül mindkét oldalnak adottak a feladatai, a meghatározott felelősségi körök szerint.

A jogszabály tartalmazza továbbá az államigazgatás azon személyeinek és szerveinek feladatait, amelyek meghatározóak az elektronikus hírközlés felkészítésében. A hatályos jogszabályokhoz viszonyított bővülés, a Nemzeti Hírközlési Hatóság védelmi felkészítéssel kapcsolatos feladatainak megfogalmazása. A hatóság kötelezettsége olyan védelmi célú adatszolgáltatási és információs rendszer létrehozása, amely kötelező szolgáltatói adatszolgáltatáson alapul.

A rendelet, a felkészítés rendje keretében - a zártcélú távközlő hálózatokról szóló 50/1998.(III. 27.) kormányrendeletet követve – megfogalmazza az elektronikus hírközlés védelmi felkészítése alá tartozó területeket, a felkészítés tárgyát (a hírközlő hálózat, a hálózati irányítás, a tartalékolás, az információs rendszer, a feladatok gyakorlaltatása), kitér a sajátos feladatot ellátó műsorszórásra, a rendszer átállítására, leírja a felkészítési tevékenység folyamatát, a követelmények meghatározásától a finanszírozáson át a helyreállításig.

A felkészítési rendszer kritikus pontja a veszélyhelyzet tényleges bekövetkezése (elrendelése), amikor át kell állni a normál állapottól eltérő működésre. Veszélyhelyzetben (minősített időszakban) a hírközlési ágazatnak rendelkeznie kell olyan irányító szervezettel, amely képes összefogni a különböző szolgáltatókat, szolgáltatásokat, intézni az igények, feladatok prioritás szerinti végrehajtását, mozgósítani a lehetséges erőket, eszközöket. A szükséges feladatok végrehajtásához a kellő gyakorlattal már normál állapotban is rendelkezni kell, mert veszélyhelyzetben a felkészítésre nincs idő. A feltételeknek az új törvényi szabályozás szerinti Nemzeti Hírközlési Hatóság, illetve az általa működtetett ügyeleti szolgálat felel meg, melynek részletes szabályozása a törvényi felhatalmazás szerinti miniszteri (IHM) rendeletben történik.

Az informatikai és hírközlési miniszter **„az informatikai és elektronikus hírközlési, továbbá a postai ágazat ügyeleti rendszerének létrehozásáról, működtetéséről, hatásköréről, valamint a kijelölt szolgáltatók bejelentési és kapcsolattartási kötelezettségeiről”** szóló rendeletének kidolgozására az elektronikus hírközlésről szóló 2003. évi C. törvény 182. §-a (4) bekezdésének p) pontja, továbbá a postáról szóló 2003. évi CI. törvény 53. §-a (2) bekezdésének g) pontja ad felhatalmazás. (Jelenleg tervezet formájában létezik.)

A rendelettervezet szabályozott kereteket kíván biztosítani a napjainkban is működő, de a jogszabályi alapokat nélkülöző ügyeleti rendszernek. A megfelelően szabá-

lyozott keretek között működő ügyeleti rendszer lehetővé teszi, hogy az elektronikus hírközlésről szóló 2003. évi C. törvényben, valamint a postáról szóló 2003. évi CI. törvényben meghatározott feladatok, valamint a katasztrófavédelmi, polgári védelmi, nemzetbiztonsági, honvédelmi és nemzetközi kötelezettségek ellátásához az Informatikai és Hírközlési Minisztérium és a Nemzeti Hírközlési Hatóság – a hálózatok és a szolgáltatások állapotát illetően is – a szükséges tájékoztatással rendelkezzen a szolgáltatások biztosítását jelentősen befolyásoló bekövetkezett vagy várható rendkívüli eseményekről. Rögzíti az ügyeleti rendszer célját és szervezeti kereteit, valamint a rendszerrel szembeni elvárásokat, követelményeket. Meghatározza az ügyeleti rendszer működtetésében érintettek, azaz az Informatikai és Hírközlési Minisztérium, a Nemzeti Hírközlési Hatóság, továbbá az ügyeleti rendszerbe bevont szolgáltatók feladatait, valamint a működés, a tájékoztatás, valamint az együttműködés rendjét. Az ágazat ügyeleti rendszerének középpontjában a Nemzeti Hírközlési Hatóság szervezeti egységeként működtetett Országos Informatikai és Hírközlési Főügyelet áll, mely gyűjti a hálózatok, szolgáltatások állapotára jellemző információkat, figyelemmel kíséri a tevékenységet befolyásoló rendkívüli eseményeket. Fogadja a szolgáltatók által bejelentett, valamint az együttműködő szolgáltatóktól kapott tájékoztatások alapján ismertté vált rendkívüli eseményekről szóló információkat, majd továbbítja azt a Minisztérium részére. Információkat nyújt a szolgáltatók számára, felkészülésük elősegítése érdekében. A szolgáltatók az általuk működtetett hálózatok, szolgáltatások felügyeletét szakszerűen ellátó ügyeleti szolgálatokat működtetnek és együttműködnek a Főügyelettel. A rendelettervezet megfogalmazza azon rendkívüli események tárgykörét, amelyek jelentősen befolyásolják (befolyásolhatják) a hálózatok, szolgáltatások működését és bejelentésük az ügyeleti rendszerben indokolt mind a megelőzés, mind a súlyosabb következmények elhárítása érdekében.

Az ágazat ügyeleti rendszerébe bevont szolgáltatókat „a védelmi feladatokban részt vevő elektronikus hírközlési és postai szolgáltatók kijelöléséről, és felkészülési feladataik meghatározásáról” szóló IHM rendelet – amelynek előkészítése jelen rendelet tervezettel párhuzamosan folyamatban van – jelöli ki. A rendelet magalkotásához szükséges felhatalmazást az elektronikus hírközlésről szóló 2003. évi C. törvény 182. §-a (4) bekezdésének l) pontja, valamint a postáról szóló 2003. évi CI. törvény 53. §-a (2) bekezdésének f) pontja tartalmazza. Tekintettel arra, hogy a védelmi felkészülés feladataiban résztvevő szolgáltatók köre szélesebb, mint az informatikai, hírközlési és postai ágazat ügyeleti rendszerébe bevontak köre, ezért a rendelet tervezett mellékletében mátrix-szerűen kerültek meghatározásra az egyes szolgáltatók kötelezettségei. A tervezet alapvető célja, hogy

- jogszabályi alapon tudatosítsa az elektronikus hírközlési és postai szolgáltatókban az ország védelmi felkészülési tevékenységében való részvételre történő kijelölésük, illetve bevonásuk szükségességét és jelentőségét;
- meghatározza a szolgáltatók által a védelmi felkészülés és a konkrét végrehajtás során ellátandó alapeladatokat;
- biztosítsa a védelmi felkészülési és végrehajtási tevékenység ellátásához szükséges feltételek megteremtésének – közvetlen és közvetett együttműködéssel történő – lehetőségét.

A kijelölés nem normatív feladatokra, hanem azoknak a komplex védelmi felkészülési követelményeknek a meghatározására irányul, amelyek alapot biztosítanak a

minősített időszak során bekövetkező bármilyen jellegű rendkívüli esemény kezeléséhez szükséges feltételek biztosításához. A kijelölés szempontjai között kiemelkedő jelentőséggel bírt az egyetemes szolgáltatók (mind az elektronikus hírközlés, mind a postai szolgáltatás területén) kijelölése, tekintettel arra, hogy a minősített időszakban várható összetett igények hiánytalan és gyors kielégítésének követelménye mellett, alapelveként szerepel a minősített időszakokban a lakosság hírközlési igényeinek folyamatos biztosítása. *A mobilszolgáltató társaságok védelmi feladatokra történő kijelölése is elkerülhetetlen, tekintettel a magyar hírközlési piac sajátosságaira, a mobil szolgáltatás jelentős arányú elterjedtségére, és a rendkívüli körülmények közötti alkalmazásának lehetőségeire.* A tervezet a védelmi felkészülés alapfeladatainak meghatározásáról, tartalmáról, végrehajtási módjáról is rendelkezik, továbbá összefoglalja a szolgáltatók többsége által az eddigi gyakorlatban is alkalmazott – a jelen rendelettel intézményesített – rendszert, amely jogszabályi alapokra helyezi a feladat meghatározási jogosultságokat és végrehajtási kötelezettségeket. Tekintettel a hírközlési és postai tevékenység mindenkor védelmi, társadalmi, valamint állam- és gazdaságirányítási és működtetési, továbbá nemzetközi szükségességére, a rendelet a szolgáltatók védelmi felkészülési alapfeladatait olyan szakmai területekre vonatkoztatva összevontan állapítja meg, amelyek meghatározó jelentőségűek a minősített időszak bármely esete során várható feladatok végrehajtásánál. A szolgáltatók a felsorolt feladatkörökből határozzák meg és adaptálják a tevékenységi körükbe tartozókat, és azokból kiindulva készülnek fel a végrehajtásukhoz szükséges feltételek biztosítására. A rendelet értelmében a védelmi felkészülés, illetve a végrehajtás során a szolgáltatókat érintő egyedi feladatokat (azok jellegére, minősítésére, végrehajtási módjára tekintettel) az irányító szervek az érintettek számára külön határozzák meg. Az így meghatározott feladatok közlése történhet írásban, a tárca vezetői által kiadott levélben, illetve az Országos Informatikai és Hírközlési Ügyeleten keresztül operatív közleményben. A rendelet megerősíti azt az eddig is követett gyakorlatot, amely szerint a szolgáltató részére védelmi feladatot határozhatnak meg a területileg illetékes védelmi igazgatási szervek (védelmi bizottságok, hadkiegészítő szervek) is, a külön jogszabályokban meghatározott eljárás szerint.

Az elektronikus hírközlésről szóló törvény alapján még egy szorosan a katasztrófa-védelmi kommunikáció témaköréhez kapcsolódó kormányrendelet van előkészítés alatt, amely kiválthatja a jelenleg is hatályos, zártcélú hálózatokról szóló jogszabályt. Az elektronikus hírközlésről szóló 2003. évi C. törvény 182. §-a (2) bekezdésének k) pontjában kapott felhatalmazás alapján lehetőség nyílt az időközben hatálybalépett, és a jelenleg is előkészítés alatt álló jogszabályok figyelembevételével az uniós kapcsolódó joganyaggal harmonizálva, a korábbi változat foltozgatása helyett egy új letisztult, a „zártcélú hálózatokról” szóló kormányrendelet megalkotására. Ebben definiálásra kerülnek a kapcsolódó fogalmak, meghatározásra a zártcélú hálózattal rendelkező szervezetek köre (pl.: Magyar Honvédség), a hálózatgazdák feladatai, a Nemzeti Hírközlési Hatóság szerepe, valamint a sajátos rendeltetésű zártcélú hálózatokkal kapcsolatos paragrafusok (Elektronikus Kormányzati Gerinchálózat –EKG, Egységes Digitális Rádiótávközlő rendszer –EDR). A zártcélú hálózatok minősített időszakra történő felkészítésére vonatkozó utalásokat az 5. és a 22. §-ok tartalmazzák.

A védelmi feladatokban résztvevő elektronikus hírközlési, illetve postai szolgáltatók kijelöléséről és felkészülési feladataik meghatározásáról szóló IHM rendelet tervezetében kijelölt szolgáltatókat a következő táblázat tartalmazza:

A szolgáltató megnevezése	Védelmi feladatok ellátására kijelölt	Az ágazat ügyeleti rendszerébe bevont
AM-IT Informatikai Szolgáltató és Kereskedelmi Rt.	X	-
AnteCom Távközléstechnikai Fejlesztő, Gyártó és Szolgáltató Rt.	X	-
Antenna Hungária Magyar Műsorszóró és Rádióhírközlési Rt.	X	X
Antenna Multimédia Technológia és Tartalomszolgáltató Rt.	X	-
Antenna Távközlési Szolgáltató Rt.	X	-
Antenna Torony Építő és Szolgáltató Rt.	X	-
BankNet Adatátvitel és Műszaki Fejlesztő Kft.	X	X
EMITEL Távközlési Rt.	X	X
GTS Data Net Távközlési Kft.	X	X
Hungarotel Távközlési Rt.	X	X
INVITEL Távközlési Szolgáltató Rt.	X	X
Magyar Posta Rt.	X	X
Magyar Távközlési Rt.	X	X
Magyar Villamosművek Rt.	X	-
Monor Telefon Társaság Rt.	X	X
PANNON GSM Távközlési Rt.	X	X
PanTel Távközlési és Kommunikációs Rt.	X	X
T-MOBILE Magyarország Távközlési Rt.	X	X
Vodafone Magyarország Rt.	X	X

Össességében elmondható, hogy rendkívül átfogó, a nemzetközi ajánlásokkal harmonizáló szabályozási folyamatban jelenleg is tart a katasztrófavédelmi kommuni-

káció jogi kereteinek kialakítása, ami egy ilyen komplex rendszer esetén alapvető feltétele a különböző állami szervek és szolgáltatók együttműködésének egy bonyolult, de rugalmas vezetési rendszer kialakításában, valamint szükség esetén üzemeltetésében. A rendszer hatékony működtetése a piacgazdaság keretei között, maximális toleranciát, valamint a 100/2004. kormányrendelet mellékletében megfogalmazott elvek maradéktalan betartását kívánja az együttműködő felektől. Az elektronikus hírközlés rendkívüli, vagy szükségállapot idején történő alkalmazásának és irányításának elvei tehát a következők:

- Gazdaságmozgósítás, továbbá rendkívüli-, vagy szükségállapot elrendelése esetén az elektronikus hírközlés egy részét vagy egészét alapvetően a honvédelem, az ország vezetésének szolgálatába kell állítani, a védelem igényeit soron kívül kell kielégíteni.
- A hírközlő hálózatban bekövetkező rombolások, üzemkiesések esetén elsősorban a fegyveres erők, az államvezetés, a rendvédelem összeköttetéseit, illetve a lakosság légiriasztását, tájékoztatását, egészségügyi ellátását szolgáló eszközöket, összeköttetéseket kell helyreállítani, illetve pótolni.
- Kiemelten kell kezelni a Honvédelmi törvény által a honvédelemben való részvételre kijelölt szervek, valamint a külkapcsolatok, különösen a NATO és az EU vezető szervei, összeköttetési lehetőségeinek megőrzését, illetve biztosítását.
- Ameddig lehetséges, változatlanul vagy korlátozott mértékben biztosítani kell az egyéb nemzetgazdasági szervezetek és a lakosság köznapi kommunikációs lehetőségét mind a vezetékes, mind a mobil rádiótelefon hálózaton, valamint a közszolgálati rádió és televízió műsorszórásban.
- A védelmi igények kielégítése érdekében, illetve nemzetbiztonsági érdekből az elektronikus hírközlésben rendkívüli intézkedésként kihirdetett jogszabály alapján differenciált korlátozások rendelkezhetnek el.
- A hatályos jogszabályok alapján üzemelő zártcélú távközlő hálózatok működését változatlanul vagy módosított formában fenn kell, vagy lehet tartani.
- A fegyveres erők helyőrségeiket elhagyó csapataik vezetését alapvetően saját haditechnikai eszközeikkel oldják meg, de kiegészítésként – különösen a fegyveres konfliktussal érintett térségben – külön jogszabály alapján felhasználhatják az ország hírközlő hálózatainak lehetőségeit, elsődlegesen a jelen jogszabályban foglaltak alapján felkészített szolgáltatás hozzáférési pontokon keresztül, valamint a **mobil rádiótelefon szolgáltatás** igénybevételével.
- Az elektronikus hírközlési szolgáltatók – a hatóság jogszabályban rögzített koordinálásával – kötelesek megtenni a szükséges és lehetséges intézkedéseket a fegyveres erők és a kormányzat nem tervezett igényeinek kielégítésére, az esetleg igényelt csatlakozási pontok rövid idő alatti kialakítására, belföldi vagy nemzetközi kapcsolatok gyors létesítésére.
- Az elektronikus hírközlés irányítási rendszere tegye lehetővé az átállítással összefüggő feladatok megoldását és a folyamatos áttérést a minősített időszakirányításra, amelynek főbb elvei a következők:
 - a) az elektronikus hírközlés védelmi és országmozgósítási célú felhasználását a Honvédelmi Tanács felügyelete alatt e célra létrehozott

-
- csoport irányítja, együttműködve a katonai, belügyi és nemzetbiztonsági felső vezetés meghatározott szerveivel;
- b) az a) pontban meghatározott csoport irányítja a megyei és fővárosi védelmi bizottságoknál létrehozott hasonló csoportokat, valamint a Honvédelmi törvény értelmében, a honvédelemben való részvételre kijelölt elektronikus hírközlési szolgáltatókat;
 - c) az elektronikus hírközlés országos koordinálását, irányítását az ágazati miniszter az NHH útján látja el, a külön jogszabály által kijelölt elektronikus hírközlési szolgáltatók saját szakterületük minősített időszaki vezetésére, irányítására megfelelő szervezetet alakítanak meg az erre alkalmas hírközlési csomópontokban;
 - d) a fegyveres erők és rendvédelmi szervek azon irányító pontjait, amelyek a c) pont szerinti szervekkel együttműködnek, a honvédelmi és a belügyminiszter jelöli ki, és gondoskodik működtetésükről;
 - e) a hírközlő hálózaton bekövetkező rombolások, üzemkiesések helyreállításával összefüggő döntéseket jellegüktől és méretüktől függően vagy az érintett szolgáltató, vagy a szaktárca hozza meg, a munkák végzését a miniszter utasítása szerint az Nemzeti Hírközlési Hatóság vezeti és koordinálja;
 - f) az elektronikus hírközlő hálózaton végrehajtandó minden jelentősebb változtatás, így különösen nem tervezett igények kielégítése, átcsoportosítások, kerülő útvonalak igénybevétele, nemzetközi kapcsolatokat érintő tevékenységek, események, új szolgáltató bevonása az igények kielégítésébe, kizárólag az a) pont szerinti csoporttal való egyeztetés alapján történhet.

Cikkemben megpróbáltam feltárni és összefogni a katasztrófavédelmi kommunikáció hazai szabályozásának jelenlegi és kialakulóban lévő rendszerét, a jogszabályok közti kapcsolódási pontokat. „Az informatikai és elektronikus hírközlési, továbbá a postai ágazat ügyeleti rendszerének létrehozásáról, működtetéséről, hatásköréről, valamint a kijelölt szolgáltatók bejelentési és kapcsolattartási kötelezettségeiről” szóló IHM rendelet tervezetben konkrét utalás található a mobilszolgáltató társaságok védelmi feladatokra történő kijelölésére is. Ez mutatja, hogy kiemelt szerepet kell számukra biztosítani a katasztrófavédelmi kommunikáció területén, tekintettel a magyar hírközlési piac sajátosságaira, a mobil szolgáltatás jelentős arányú elterjedtségére, és rendkívüli körülmények közötti alkalmazásának lehetőségeire. Noha tapasztalható a jogalkotó részéről egy Egységes Digitális Rádiótávközlő rendszer kialakítására való törekvés, ami nagy valószínűséggel a legjobb megoldást jelenthetné a védekezésben közreműködő szervezetek hatékony és egységes vezetésének biztosítására, ennek megvalósulása – elsősorban anyagi okok miatt – korábban többször megghiúsult. Ettől függetlenül a későbbiekben, az új rendszer esetleges felállása esetén is, azt kiegészítve szükség lehet a mobiltelefon szolgáltatók hálózatainak védelmi célú igénybevételére, ami indokolja az ilyen irányú kutatások folytatását.

Felhasznált irodalom:

- [1] FEKETE Károly: A Magyar Köztársaság kommunikációs infrastruktúrája (Egyetemi jegyzet) – Budapest 2004
- [2] DÉRFOLDI László, Pintér István (Szerk.): A Honvédelmi felkészülésre, Nemzetbiztonságra, Polgári Védelemre, Katasztrófavédelemre, Titokvédelemre vonatkozó és a NATO tagságból adódó fontosabb Jogszabályok - Hírközlési Felügyelet, Budapest, 2003
- [3] 1949. évi XX. törvény, A Magyar Köztársaság Alkotmánya
- [4] 1992. évi LXXII. törvény a távközlésről
- [5] 1993. évi CX. törvény a honvédelemről
- [6] 1996. évi XXXVII. törvény a polgári védelemről
- [7] 1997. évi LXV. törvény a távközlésről szóló 1992. évi LXXII. törvény módosításáról
- [8] 1999. évi LXXIV. törvény a katasztrófák elleni védekezés irányításáról, szervezetéről és a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről
- [9] 2001. évi XL. törvény a hírközlésről
- [10] 2003. évi C. törvény az elektronikus hírközlésről
- [11] 2003. évi CI. Törvény a postáról
- [12] 50/1998. (III.27.) kormányrendelet a zártcélú távközlő hálózatokról
- [13] 133/1994. (X. 21.) kormányrendelet váratlan légitámadás esetén az ország légiriasztásáról
- [14] 131/2003 (VIII. 22.) kormányrendelet a nemzetgazdaság védelmi felkészítése és mozgósítása feladatai végrehajtásának szabályozásáról
- [15] 100/2004 (IV. 27.) kormányrendelet az elektronikus hírközlés veszélyhelyzeti és minősített időszaki felkészítésének rendszeréről, az államigazgatási szervek feladatairól, működésük feltételeinek biztosításáról
- [16] 9/2004 (III. 10.) országgyűlési határozat a "Távközlési Erőforrások Biztosításáról Katasztrófa Elhárítás és Mentés Céljaira" tárgyú Tamperei Egyezmény aláírásáról
- [17] Tamperei Egyezmény a Távközlési Erőforrások Biztosításáról Katasztrófa Elhárítás és Mentés Céljaira
- [18] IHM rendelet-tervezet a védelmi feladatokban résztvevő elektronikus hírközlési, illetve postai szolgáltatók kijelöléséről és felkészülési feladataik meghatározásáról
- [19] IHM rendelet-tervezet az informatikai és elektronikus hírközlési, továbbá a postai ágazat ügyeleti rendszerének létrehozásáról, működtetéséről, hatásköréről, valamint a kijelölt szolgáltatók bejelentési és kapcsolattartási kötelezettségeiről
- [20] Kormányrendelet-tervezet a zártcélú hálózatokról
- [21] www.ihm.hu

A KORMÁNYZATI TÁVKÖZLÉS ELMÚLT 15 ÉVE

A nyolcvanas évek közepétől megindult társadalmi-politikai változások az 1989-1991 években csúcsozodtak ki, mely időszakban lejátszódott események összessége⁴⁹ fordulópontot jelentett a közép-kelet-európai régió több országának, így hazánknek is. Az országban komplex folyamatok kezdődtek jelentős hatást gyakorolva a gazdasági élet szereplőire, melyet Paul Kennedy⁵⁰ így jellemzett: *„Kelet- és Közép-Európa társadalmainak anélkül is épp elég gondjuk van, hogy a technológia, a környezeti irányzatok és a demográfiai változás által serkentett világméretű változások miatt aggódniának. [...] Mivel ezen országokban nincsen tőzsde és az ipar szerkezetváltásra szorul, jelenleg kevés lehetőségük van arra, hogy élvezzék a határidős ügyletekkel folytatott napi huszonnégy órás üzletelés vagy a teljesen automatizált gyárak áldásait. Kelet- és Közép-Európa nemzetei azonban rendelkeznek néhány fontos erőforrással: sok tehetséges és becsvágyó polgárunk van; alapvetően egészséges az oktatási infrastruktúrájuk; [...] a matematikában és a tudományban (Magyarország) elért kiváló eredmények nagy hagyománya...”* [1]. A gazdaság szerkezetátalakítása⁵¹ a hírközlési szektort is mélyen érintette, melynek első állomása volt a Magyar Posta szervezetének 1990. január 1-jei hatállyal történt átalakítása. A továbbiakban a postai, a műsorszórási és a távközlési tevékenységek végzését az újonnan alakult vállalatok vették át. A gazdaságot érintő döntések mellett a hírközlési ágazatnak szembe kellett nézni a globalizáció⁵² és a konvergencia technikai rendszereket és szolgáltatásokat érintő hatásaival is, melyek pontos megismerése a COCOM-bizottság addigi működése miatt nem vált lehetőséggé.

⁴⁹ gondolok itt többek között a két német állam egyesülésére, a Magyar Köztársaság kikiáltására, a romániai forradalmi eseményekre, a dél-szláv válságra és polgárháború kirobbanására, a Csehszlovákiában meginduló politikai eróziós folyamatra, mely nemsokkal később Csehország és Szlovákia egymástól való elszakadásához vezet, a Független Államok Közösségének megalakulására, valamint a VSz és a KGST megszűnésére

⁵⁰ Dr. Paul Kennedy: „A nagyhatalmak tündöklése és bukása” című műve megjelenését követően a legtöbbet olvasott amerikai történész

⁵¹ a gazdasági szerkezet átalakításával célként jelentkezett egyrészt az állam gazdaságban betöltött szerepe túlsúlyának mérséklése, másrészt a magántőke bevonásával az infrastrukturális elmaradottság (úthálózat, távközlő rendszer, mezőgazdasági rendszerek, stb.) csökkentése, illetve megszüntetése. A tervgazdaságról a piacgazdaságra való áttérés szimbólumaként az Országgyűlés 1990-ben megszüntette az Országos Tervhivatalt és annak néhány megmaradó makroökonomiai feladatát a Pénzügyminisztériumhoz csoportosította át. Szintén ez évben alakult meg a gazdasági átalakulás kulcsintézménye az Állami Vagyongyűnökség, mely 1990. júliusától a Kormány felügyelete alatt működik

⁵² globalizáció: azoknak a bonyolult folyamatoknak az összessége, amelyek a gazdaság, a technika, a politika és a kultúra területén az egész Földre kiterjedő, új rendszereket hoznak létre. E területeken a XX. század közepéig független, földrajzilag körülhatárolható, lokális rendszerek éltek egymástól elszigetelten vagy egymásra kölcsönösen hatva ugyan, de identitásukat mindvégig megőrizve. A század második felében a nemzetállamok közötti egyre intenzívebben és egyre sűrűsödő kölcsönhatások ma már az egész világra kiterjednek, és gazdasági, technikai és kulturális téren olyan bonyolultan fonódnak össze, hogy a keletkező hatások követhetlenné és kiszámíthatatlanná válnak. A világ gazdaságának új összefüggésrendszere és új működési elvei a globalizáció folyamatában jönnek létre úgy, hogy egyúttal felbontják és megváltoztatják a régi nemzeti rendszerek működését is

A Magyar Posta átalakításával egyidejűleg a kormányzati távközlés megvalósulásában résztvevő államigazgatási szervek struktúrája is átalakításra került. Az 1989/90-es év fordulóján radikálisan megváltozott a Kormány és az erőszakszervezetek viszonya. A katonai vezetést végző szervek kiváltak a Honvédelmi Minisztériumból, a Magyar Honvédség⁵³ parancsnoka lett a hadsereg személyi állományának előljárója. Ebben az időszakban a rendőrség irányításában a Minisztertanács,⁵⁴ illetve a belügyminiszter meghatározó szerepe érvényesült. Az 1990. márciusában elfogadott törvénymódosítás⁵⁵ az Országos Rendőr-főkapitányságot leválasztotta a Belügyminisztérium szervezetről, megszüntette a miniszter operatív beavatkozási jogát. Az új szabályozás értelmében a belügyi tárca csupán normatív eszközökkel irányíthatta a rendőrséget, az utasítás és parancsadás joga az országos rendőr-főkapitányt illette meg. Szintén 1990 tavaszán, a Kormány az állambiztonsági szolgálatok egész rendszerét és irányítási rendjét gyökeresen átalakította. Megszüntetésre⁵⁶ került a Belügyminisztérium keretében működő III. Főcsoportfőnökség és az újonnan alakult polgári nemzetbiztonsági szolgálatok a miniszterelnök felügyelete alá kerültek, mint önálló, országos hatáskörű szervek. A közigazgatást érintően a politikai és közigazgatási kar is gyors ütemben szétválasztásra került. A két szféra elkülönítése egyben sajátos szolgálati utat is intézményesített a minisztériumokban, vagyis a miniszter és politikai államtitkár, illetőleg a hivatali apparátus kizárólag a közigazgatási államtitkár⁵⁷ közvetítésével jöhetett létre kapcsolat. A szélesebb minisztériumi ügycsoportokat helyettes államtitkárok fogják össze. Ez időszakban alakult át a Minisztertanács Hivatala⁵⁸ Miniszterelnöki Hivatallá, így az adminisztratív és jogi-technikai előkészítő apparátusból végérvényesen a kormányzati hatalom legbefolyásosabb centruma fejlődött ki [2]. Elmondható tehát, hogy a kormányzati távközlés gyakorlati megvalósulásának külső feltételrendszere 1989 és 1991 között teljesen megváltozott. Az új helyzet kialakulását az államigazgatás struktúrájának módosulása, a világban megfigyelhető technológiai konvergencia hatásai, – *a gazdasági rendszer átalakításával összefüggésben* – a hírközléssel kapcsolatos új jogszabályi környezet kialakítása, valamint az e kettő eredőjeként az informatikai és távközlési szektorban lebonyolított technikai fejlesztések befolyásolták.

E fejezetben áttekintem az **1990-2004** közötti időszakot felölelően a teljes hírközlési ágazat hazai jogszabályi hátterének átalakulását és e területen végbement változások rendészeti-, katonai-, közigazgatási- és a polgári szektor kommunikációs rendszerei fejlődési irányait befolyásoló hatásait, illetve azokat a döntéseket és lépéseket amelyek egy kormányzati kommunikációs rendszer kialakításához vezethetnek.

2.1. A hazai szabályozási háttér

⁵³ a Magyar Honvédség elnevezés használatát a honvédelemről szóló 1976. évi I. törvény módosításáról szóló 1990. évi XXI. törvény rendelte el

⁵⁴ az 1990-es választásokat követően: Kormány

⁵⁵ az 1990. évi XXII. törvény 22. §-ával kiegészített 1974. évi 17. törvényerejű rendelet 11/A. §

⁵⁶ a különleges titkosszolgálati eszközök és módszerek engedélyezésének átmeneti szabályozásáról szóló 1990. évi X. törvény 7. §-ával módosított és kiegészített 1974. évi 17. törvényerejű rendelet 11. § (1) és (5) bekezdés

⁵⁷ közigazgatási államtitkár: egy minisztérium hivatali apparátusának elsőszámú vezetője. Szemben a politikai államtitkárral megbízatását határozatlan időre kapja, így elviekben munkája során szakértelme révén mindig az éppen hatalmon levő kormány tevékenységéhez igazodik

⁵⁸ a Minisztertanács (MT) Hivatala 1988 tavaszán jött létre az MT Titkárságának és a Tájékoztatási Hivatal összevonásával

Bármilyen kommunikációs rendszer létesítésének, működtetésének, fejlesztésének és megszüntetésének egyik feltétele olyan szabályozott környezet kialakítása, amelyben a rendszer az alapfunkciójának és egyéb rendeltetésének megfelelő szerepét hatékonyan betöltheti. Az államnak, mint a közösség felett főhatalmat gyakoroló szervezetnek tehát – *különböző egyéb szempontokat*⁵⁹ is mérlegelve – kötelessége az állami irányítás jogi eszközeivel⁶⁰ elősegítenie a legkedvezőbb feltételrendszerek kialakulását, illetve megteremtését. Az 1990-es évek elején, a piacgazdaságra való áttérés megkövetelte, hogy az addig a tervutasítás normatívái szerint működtetett hírközlési szektorban az alkalmazott szabályozási szisztéma is koncepcionális felülvizsgálatra kerüljön, mely célta a távközlésről szóló 1992. évi LXXII. törvény preambuluma⁶¹ is jól kifejez: „Az Országgyűlés a távközléssel kapcsolatos igények kielégítése, a korszerű távközlési szolgáltatások hatékony és gazdaságos fejlesztése, a vállalkozások és a verseny elősegítése céljából – a nemzetközi szabályokkal összhangban – a következő törvényt alkotja:...” [3]. A felülvizsgálat hatására hazánkban a hírközléssel kapcsolatos szabályozási környezet reformja fokozatosan, az ágazat fejlődésével egyidejűleg ment végbe, mely során a szabályozási- és a szolgáltatási funkciók is megosztásra, szétválasztásra kerültek [4]. A jogi háttér változásai nem hagyták érintetlenül az állami vagyont és tulajdonrészeket sem, így Magyarország kommunikációs infrastruktúrájának⁶² jelentős része került magántulajdonba. A fennmaradó kommunikációs rendszereket a különböző államigazgatási szervek vagyionkezelésébe utalták, mely új helyzet elé állította a kormányzati távközlés egész addigi működési szisztémáját. A 2004-re kialakult helyzethez vezető folyamatokat elsősorban a kormányzati célú kommunikáció és a technológiai konvergencia megvalósulásának aspektusából – a mértékadó jogszabályok⁶³ áttekintése útján – vizsgálom.

2.1.1. A piaci feltételek kialakítása

A távközlési szektor hazai piaci feltételei megteremtésének nemzetközi vonatkozásaival kapcsolatosan Dr. Török Gábor⁶⁴ a következőket állapítja meg: „...a távközlés területén az utóbbi évtizedekben jelentős szemléletváltozásra került sor. A folyamat az Amerikai Egyesült Államokban kezdődött, ezt némi késéssel, de átvette az Európai Unió szabályozása is. A korábbi felfogás magától értetődőnek tartotta, hogy egy országban a távközlési szolgáltatást végző cég egyrészt állami tulajdonban van, másrészt pedig monopolhelyzetben. A szemléletváltás első jelét az a gondolat jelentette, hogy katonai és belbiztonsági érdekek az állami tulajdonjog fenntartása nélkül is biztosíthatóak, amelyből egyenesen következett, hogy ezen a területen is lehetségessé vált a privatizáció.” [5].

A korábbi felfogásnak megfelelő helyzet volt megfigyelhető Magyarországon is, hiszen a postáról és a távközlésről szóló 1964. évi II. törvény és végrehajtási utasítása alapján 1988-ig a Magyar Posta szabályozta és nyújtotta a hírközlési szolgáltatásokat. A frekvenciagazdálkodás, az elektromágneses zavarok vizsgálata, valamint a távközlő hálózatokkal kapcsolatos engedélyek és panaszok elsőfokú hatóságként való rendezése szintén jogkörébe volt utalva. Az infra-

⁵⁹ ilyen szempontok lehetnek például: társadalmi-, gazdasági-, politikai- és szociális célkitűzések

⁶⁰ jogszabály (jogi norma) útján, ami nem más, mint az állam által alkotott és állami kényszerrel is biztosított magatartási szabály, amelynek megvalósulását vagy megsértését pozitív vagy negatív előjelű jogkövetkezmény kíséri

⁶¹ preambulum: valamely alapvető jelentőségű, általában nagyobb terjedelmű jogszabály vagy nemzetközi szerződés bevezető része, amely elkülönül a jogszabály rendelkező (normatív) részétől

⁶² Magyarország kommunikációs infrastruktúrája alatt értem a hazánkban működő kommunikációs rendszerek összességét, függetlenül tulajdonkezelésük formájától

⁶³ jogszabályok alatt értem itt az állami irányítás egyéb jogi eszközeit is (elsősorban: kormányhatározat)

⁶⁴ Dr. Török Gábor az idézett publikáció megjelenésének időpontjában a Budapesti Közgazdaságtudományi és Államigazgatási Egyetem tanszékvezető egyetemi tanára volt

struktúra korszerűsítéséhez szükséges nemzetközi hitelszerződések⁶⁵ alapfeltétele volt a hírközlési ágazaton belüli keresztfinanszírozás megszüntetése, így 1989-ben kerültek szétválasztásra a szabályozási és működési funkciók, mely szerint a Közlekedési, Hírközlési és Építéstudományi Minisztérium vett át szabályozási feladatokat a Magyar Postától. A hatósági feladatokat a továbbiakban a Postai és Távközlési Főfelügyelet és a Frekvenciagazdálkodási Intézet, míg 1990-től a működési funkciókat a Magyar Távközlési Vállalat⁶⁶, a Magyar Műsorszóró Vállalat⁶⁷, és a Magyar Posta Vállalat⁶⁸ látta el. A megosztott működési funkciók a koncesszióról⁶⁹ szóló **1991. évi XVI. törvény** alapján kerültek ki az állam hatásköréből. A jogszabály az állami tulajdon hatékony működtetése érdekében került megalkotásra és intézményesítette a koncessziós szerződés szerinti tevékenység gyakorlását. Ennek értelmében az állam – *díj ellenében, meghatározott időre* – törvényben meghatározott tevékenységének végzéséről, vagy vagyontárgyai használatáról vállalkozások javára lemondhat. A távközlés területén az állam a következő szolgáltatások nyújtásának⁷⁰ jogát adta át: távbeszélő szolgáltatás; mobil rádiótelefon szolgáltatás; országos személyhívó szolgáltatás; rádió- és televízió műsorok országos és regionális szétszórása és sugárzása. A folyamat következő lépcsőfoka a távközlésről szóló **1992. évi LXXII. törvény** megalkotása⁷¹ volt, mely meghatározza és szabályozza a távközlési szolgáltatások nyújtásának módját és feltételeit, a távközlési szolgáltatásban résztvevők jogait és kötelezettségeit, a távközlő hálózat tervezésének, létesítésének, üzemben tartásának, a távközlő eszközök és berendezések használatának feltételeit, a távközlés védelmére vonatkozó rendelkezéseket, valamint a távközléssel kapcsolatos állami feladatokat.

A jogforrás rögzíti, hogy a koncesszióba adott szolgáltatásokon kívül egyéb távközlési szolgáltatást – *hatósági engedély alapján* – bárki nyújthat, mely a technológiai konvergencia hatására később megjelenő új kommunikációs szolgáltatások elterjedését segítette elő. A konvergenciát támogatva a törvény lehetőséget ad a hálózatok előírt feltételek melletti összekapcsolására, illetve részleges vagy teljes használatának szolgáltatás céljára történő ideiglenes átengedésére abban az esetben, amennyiben az igénybevevő által továbbítani kívánt jel, jelzés, írás, kép vagy hang olyan tevékenység terméke, amelyre vonatkozóan jogosultsággal rendelkezik. Az ország távközlési infrastruktúrája egységességének biztosítása érdekében a törvény szabályozza a hálózatok együttműködési kötelezettségeit, valamint a távközléssel összefüggő állami feladatokat, mely többek között előírja: a nemzeti távközlési politika kialakítását és a megvalósításhoz szükséges feltételek megteremtését; a távközlési piac felügyeletének megvalósítását; a távközléssel kapcsolatos hatósági feladatok teljesítését; a piacra lépők egyenlő feltételeinek biztosítását; a domináns szolgáltatók tevékenységének szabályozását; az országos távközlő hálózatok műszaki- és forgalmi egységét biztosító gazdasági, műszaki és jogi szabályozást.

E törvénnyel kerültek bevezetésre a **közcélú**⁷², **különcélú**⁷³ **zártcélú**⁷⁴ és **saját célú**⁷⁵ fogalmak, mivel a hazai kommunikációs infrastruktúra irányítása és fenntartása

⁶⁵ a Világbankkal és az Európai Fejlesztési Bankkal kötött szerződések

⁶⁶ 2003-ban: Magyar Távközlési Részvénytársaság, mely 100%-os magántulajdonban van

⁶⁷ 2003-ban: Antenna Hungária Részvénytársaság, mely többségi állami tulajdonban van

⁶⁸ 2003-ban: Magyar Posta Részvénytársaság, mely többségi állami tulajdonban van

⁶⁹ koncesszió: kizárólagos engedély

⁷⁰ ezek csak a civil szektort érintették, vagyis mai fogalmainkkal élve ezek közcélú szolgáltatások

⁷¹ csak 1993. július 1-jén lépett hatályba

⁷² például a díjfizetés ellenében történő kiszolgálás céljából létesülő hálózatok minőségét jelzi

⁷³ például a zárt felhasználói csoport igényeinek kielégítésére szolgáló hálózatok minőségét jelzi

⁷⁴ például a kormányzati, nemzetbiztonsági, igazságszolgáltatási, közbiztonsági és védelmi érdekeket kiszolgáló hálózatok minőségét jelzi

egységes állami monopóliumának megszűntekor a Magyar Posta utódszervei kezében levő hálózatokon túlmenően az államigazgatás, valamint egyes nagyvállalatok⁷⁶ korábban létesült kommunikációs rendszereik használatáról – *elsősorban állami feladatokból, illetve működési kényszerükből adódóan* – nem mondtak le.⁷⁷ A normatívában ezért a hálózatok funkcionális határok mentén, logikailag megosztásra kerültek, így szentesítve egyfajta elkülönülést, melyet azonban az együttműködési kényszer előírásával igyekeztek ellensúlyozni. A hírközlési ágazattal összefüggésben korlátozott erőforrásként került meghatározásra a frekvenciavagyon, mellyel való gazdálkodás⁷⁸ az állam feladatkörében maradt. Ezzel kapcsolatos jogszabály a frekvenciagazdálkodásról szóló **1993. évi LXII. törvény**,⁷⁹ amely az állam fő feladatként szabja meg a következőket: a frekvenciahasználat műszaki, gazdasági és jogi feltételeinek meghatározását; az alapvető műszaki tervek, előírások, a szolgáltatások minőségi, műszaki és technológiai feltételeinek szabályozását; a frekvenciahasználatból eredő állami tulajdonosi jogok gyakorlását, az elektromágneses spektrum igénybevételének összehangolását, elosztását, az ezzel kapcsolatos adatok nyilvánosságra bocsátását; a rádiótávközlő berendezések és hálózatok műszaki adatainak nemzetközi koordinációját. A teljes képhez hozzátartozik, hogy az ágazat fennmaradó területeinek törvényi szabályozása a postáról szóló **1992. évi XLV. törvény**,⁸⁰ valamint a rádiózásról és televíziózásról szóló **1996. évi I. törvény** kihirdetésével vált teljessé. A távközlés és frekvenciagazdálkodás területét a törvényekkel összefüggésben kiadott végrehajtási- és egyéb kormány-, illetve miniszteri rendeletek és kormányhatározatok is szabályozzák.

Elmondható, hogy 1998-ra a hírközlési szektor fő ágazatainak tevékenysége újraszabályozásra került. Az állam feladatainak egy része koncessziós szerződések alapján a magánszektorhoz került kihelyezésre, melynek felügyeletére hatóságok jöttek létre. Egységesítésük⁸¹ viszonylag hamar lezajlott, mely hatósági modell még csak néhány országban volt akkoriban alkalmazott szisztéma. A műszaki, gazdasági és jogi keretek megállapítása révén megindulhatott a civil szektor hírközlési infrastruktúrájának fejlesztése, mely során többek között a közcélú távbeszélő hálózat primer körzetei⁸² váltak koncessziós területté, illetve megjelentek a mobil rádiótelefon-szolgáltatók.⁸³ Amint látható a jogszabályok egy része a kihirdetésüket követő viszonylag rövid időn

⁷⁵ például adott vállalkozás vagy személy kizárólag saját távközlési igényeinek kielégítésére szolgáló hálózatok minőségét jelzi

⁷⁶ gondolok itt a Magyar Olaj és Gázipari Részvénytárság, a Magyar Államvasutak Részvénytársaság, vagy a vízügyi szervezetek jogelődjeire

⁷⁷ hiszen a távbeszélő szolgáltatás-hozzáférési pontok mennyiségi növelésének programja csak 1994 után, a koncessziós szerződések hatálybalépésekor gyorsultak fel. Addig viszont a nyolcvanas évekre jellemző mennyiségi hiány nem mérséklődött

⁷⁸ ami többek közt az elektromágneses spektrum felosztásában, felügyeletében és a felhasználás ellenőrzésében nyilvánul meg, mely érinti mind a polgári-, mind a kormányzati frekvenciákat

⁷⁹ a távközlési törvénnyel egyidőben vált hatályossá

⁸⁰ mely törvény szintén a távközlési törvénnyel egyidőben vált hatályossá

⁸¹ a Hírközlési Főfelügyelet 1994-ben jött létre a Postai és Távközlési Felügyelet és a Frekvenciagazdálkodási Intézet összevonása révén

⁸² primer körzet: a közcélú távbeszélő hálózat azon részegysége, amelyen belül két szolgáltatás-hozzáférési pont közötti kapcsolat létesítése érdekében az előfizetői szerződés keretében nyújtott szolgáltatáshoz nem szükséges a gerinchálózat igénybevétele. Ez 1994-ben 25 körzetet érintett. A gerinchálózat a MATÁV Rt. kezelésében maradt

⁸³ elsőként a Westel 450 Rádiótelefon Kft., majd 1995-től a Westel 900 Mobil Távközlési Rt., illetve a Pannon GSM Távközlési Rt.

belül módosításra kerültek. Ennek oka hazánk Európai Közösséghez való társulásából, illetve az Európai Unióhoz való csatlakozásából eredő jogharmonizációs⁸⁴ vállalások teljesítésére vezethetők vissza.

A piaci háttér kialakításában a fordulópontot 1998 jelentette, mivel ebben az évben került kihirdetésre a jelenleg is érvényes szakmapolitikai követelményeket rögzítő 1071/1998. (V.22.) Korm. határozat.⁸⁵ Megítélésem szerint a határozat egyértelműen lezárja a hírközlési szektor kilencvenes évekbeli fejlődésének addigi szakaszát és az ágazattal kapcsolatosan az 1998-2005 közötti évekre vonatkozóan új elvárásokat, valamint feladatokat fogalmaz meg. A technológiai konvergenciát és a globalizációs folyamatokat is figyelembe véve a határozat szerkesztői kiemelik, hogy a: „...hírközlés és ezen belül különösen a távközlés területén végbemenő és prognosztizálható fejlődés, a szolgáltatások és technológiák integrációja, az informatika, a távközlés egyre szorosabb összekapcsolása egyértelművé teszi, hogy a hírközlési infrastruktúra nemzetgazdasági és társadalmi jelentősége egyre meghatározóbb lesz a jövőben. [...] Az ezredforduló utáni társadalmi fejlődés már elsősorban a hírközlésre és a vele szorosan kapcsolatban lévő informatikára épül. Az oktatás, a kereskedelem, az ipar, az államigazgatás és a háztartások működésének nélkülözhetetlen része lesz a kommunikáció és az annak bázisán megvalósuló integrált információs infrastruktúra. [...] A magyar információs társadalom megteremtése csak a már kialakulóban levő globális információs társadalom részeként képzelhető el. [...] Az előttünk álló gazdaságfejlesztési feladatok, felzárkózásunk a fejlett országokhoz, valamint csatlakozásunk a NATO-hoz és az Európai Unióhoz azt követelik meg, hogy [...] a hírközlés fejlődését mintegy 8 évre szóló szakmapolitika alapozza meg.” [6].

Az új piaci háttér liberalizálttá válik, melynek fő jellemzője, hogy a beszédcélú és nem beszédcélú, valamint a keskeny- és szélessávú szolgáltatások aránya eltolódik, vagyis a nem kizárólag beszédcélú szolgáltatások részaránya növekedik nagyobb ütemben, ezért hangsúlyosabban fognak jelentkezni az adatátviteli igények is. A liberalizációs folyamattal egyidejűleg – a piaci verseny fenntartása – megköveteli a párhuzamos távközlési infrastruktúrák kialakítását elsősorban az alternatív szolgáltatók⁸⁶ megjelenésének elősegítése útján. A vegyes távközlési infrastruktúra és az arra épülő szolgáltatási piac lehetővé teszi a civil szektor mellett a kormányzati és államigazgatási szervezetek is, hogy gyakorolják a felhasználói igények szerinti szabad választás lehetőségét mind a szolgáltatókat, mind a szolgáltatásokat tekintve. Az infrastruktúra fejlesztésének és bővítésének azonban előfeltételét képi az állami irányítás 1990-98 közötti szerepének további módosítása is, mivel a korábbi jogi normatívák 1998-ra gátat szabtak az új technikai lehetőségek elterjedésének, illetve az információforrások tetszés szerinti elérésének.

Elmondható, hogy a hírközléspolitikai megszabja többek között a távközlési szolgáltatások technológiájának, infrastruktúrájának, integrációjának, tulajdonosi és piaci szerkezetének, intézményi hátterének, valamint szabályozási környezetének fejleszté-

⁸⁴ jogharmonizáció: különböző országok jogának egymáshoz való közelítésére irányuló tevékenység. Megvalósítása során az érintett országok teljes jogrendszerében vagy annak egyes részeiben a hatályos jogi szabályozás kisebb-nagyobb mértékű módosításával az idegen jogi szabályozással vagy szabályozásokkal harmonizáló, azokhoz hasonló megoldásokat alakítanak ki

⁸⁵ a nemzeti hírközléspolitikai elkészítésére a távközlési törvény hatalmazta fel a Kormányt

⁸⁶ alternatív szolgáltatók: mindazon szolgáltató szervezetek, melyek a koncessziós törvényben nem rögzített távközlési (hírközlési) szolgáltatások nyújtására engedéllyel rendelkeznek

sével kapcsolatos állami feladatokat annak érdekében, hogy a társadalom – *várhatóan egyre szélesedő körű* – kommunikációs igényeinek kielégítésének alapjai biztosítottak legyenek. Az információs (tudásalapú) társadalom koncepciója támogatása érdekében előirányozza, hogy a lakosság minden rétege számára 2004-ig elérhetővé kell tenni a minimum 64 kbit/s sebességű adatátviteli kapcsolatú Internet-szolgáltatást az egyetemes szolgáltatási kötelezettség keretében [7].

Ennek teljesülése igen nagy minőségi ugrást – *és egyúttal kihívást* – jelenthet a távközlési szektor 1990-es évi várakozói listákkal jellemzett helyzetéhez képest. A kitűzött célok megvalósításának alapját a hírközlésről szóló – *a kormányhatározat megjelenését követően három évvel később kihirdetett* – **2001. évi XL. törvény** képi, mely egyértelműen leszögezi, hogy „...az információs társadalom hírközlési infrastruktúrájának továbbfejlesztése, valamint a fogyasztók biztonságos, megfelelő minőségű és áru hírközlési szolgáltatásokkal való ellátása érdekében, a hírközlési piac fejlődése, védelme, a verseny biztosítása, továbbá a hírközlési hálózatok hatékony együttműködésének biztosítása céljából...” került megalkotásra [8]. A jogszabály megjelenésével egyidejűleg veszítette hatályát a postáról szóló törvény,⁸⁷ valamint a távközlési törvény⁸⁸ is, melyek majd egy évtizeden keresztül szolgáltak alapvető jogforrásként.

A törvény célja tehát a hírközlési piac liberalizálása, a versenyfeltételek megteremtése, így a jogszabály – *és végrehajtási rendeletei* – lényeges változásokat és újdonságokat tartalmaztak. Egy évvel a törvény hatálybalépését követően (2002), a hírközlési piac helyzetével kapcsolatosan a Hírközlési Felügyelet elnöke megállapítja, hogy a jogszabály kihirdetésével hazánkban jogilag is megvalósult a piac liberalizációja, melynek kiinduló helyzete azonban teljesen eltér az Európai Unió távközlési piacának 1998-as megnyitásakor fennállt állapotától. A piacnyitással összefüggő várakozások hazánkban nagyobbak voltak és ez a folyamat akkor következett be, amikor a telekommunikáció súlypontja a mobil távközlési- és az Internet-szolgáltatások irányába tolódott el. Ennek ellenére az új szabályozás kedvezőbb feltételeket teremtett a távközlésben, és gyakorlatilag megszüntette az adminisztratív piacra lépési korlátokat. Év végén 470 regisztrált szolgáltató⁸⁹ közel 650 szolgáltatást kínált fel, melyek minőségi mutatói fokozatosan emelkedtek [9]. A hírközlési törvény alapján Hírközlési Felügyelet néven átalakul a hírközlési hatóság, melyet a Kormány irányítása, és az ágazati szakminiszter felügyelete alá helyeznek. A Hírközlési Felügyelet⁹⁰ központi közigazgatási és önállóan gazdálkodó központi költségvetési szerv, mely a feladatai ellátásával összefüggő kiadásokat saját bevételeiből fedezi. A működés finanszírozásának

⁸⁷ 2001. évi XL. törvény 103. § (8) c) pontja alapján, 2001. december 23-ai hatállyal

⁸⁸ 2001. évi XL. törvény 103. § (8) e) pontja alapján, 2001. december 23-ai hatállyal

⁸⁹ a legtöbb szolgáltató adathálózati szolgáltatást nyújtott

⁹⁰ a Hírközlési Felügyelet szervei: Hírközlési Főfelügyelet, Hírközlési Területi Hivatal (a kettő együtt: hatóság) és a Hírközlési Döntőbizottság. A hatóság ellátja a hírközlési szolgáltatások bejelentésével kapcsolatos, a polgári célú frekvenciagazdálkodási, az azonosító gazdálkodási, az egyedi engedélyezési, a zavarelhárítási, a piacfelügyeleti és egyéb hírközlési hatósági ügyeket. A Döntőbizottság kérelemre, illetve az e törvényben meghatározott esetekben hivatalból ellátja a jelentős piaci erővel rendelkező szolgáltatók kijelölésével, a referencia hálózati szerződési ajánlatok jóváhagyásával, az együttműködési kötelezettségek teljesítésének elősegítésével, az egyetemes szolgáltatás alóli mentesítéssel, a hálózati szolgáltatások árával, és az egyetemes szolgáltatás finanszírozásával kapcsolatos jogviták rendezésével összefüggésben e törvényben meghatározott feladatait, valamint teljes ülésben dönthet a hírközléssel kapcsolatos elvi jelentőségű ügyekben

módja, újszerű szervezeti felépítése, illetve vezetőjének a kormányciklusoktól eltérő, hosszabb kinevezési időtartama garantálja a szabályozó szervektől való szakmai semlegességét.

Az információs társadalom jogszabályrendszerében a hírközlési törvénnyel egyidőben került megalkotásra az elektronikus aláírásról⁹¹ szóló **2001. évi XXXV. törvény**: „...az elektronikus kereskedelem fejlődése és ez által a gazdasági fejlődés előmozdítása, valamint az információs társadalommal összefüggő szolgáltatások révén a magyar gazdaság nemzetközi versenyképességének javítása, továbbá az elektronikus kereskedelmi kapcsolatokban a fogyasztók jogainak védelme érdekében...” [10]. Az informatikai ágazat rohamos fejlődése követelte meg az elektronikus aláírás mielőbbi szabályozását, hiszen a levelezés (ügyiratforgalom), mint a kommunikáció egyik fő fajtájának egy része már digitális úton terjed. A törvény célja, hogy megteremtse a hiteles elektronikus nyilatkozattétel és adattovábbítás jogszabályi feltételeit az üzleti életben, az államigazgatásban és az információs társadalom által érintett egyéb területen is, így a jogszabály csak általánosan határozza meg az elektronikus aláírás szabályait függetlenül attól, hogy a társadalom mely területei⁹² használják fel azt. Az elektronikus aláírással kapcsolatos hatósági feladatokat⁹³ – *hasonlóan a távközlés területéhez* – a hírközlési hatóság látja el. Mivel az egyes szolgáltatói formák feltételeit a jogszabály eltérően állapítja meg,⁹⁴ így a felügyeleti tevékenységgel a szabályozás kellő alapossággal foglalkozik.⁹⁵ A piac kibontakozása 2002-ben folytatódott, de nagymértékű felfutás nem következett be. 2002. év végéig hazánkban öt fokozott biztonságú elektronikus aláírással kapcsolatos szolgáltatót és két tanúsító szervezetet⁹⁶ vett a hírközlési hatóság nyilvántartásba [11].

Avizsgált időszakot tekintve a piaci feltételek kialakításának utolsó állomásaként tekinthető az elektronikus hírközlésről szóló **2003. évi C. törvény**⁹⁷ megalkotása, mely egyúttal hatályon kívül helyezte a hírközlési törvényt. Némileg szokatlanul tűnik, hogy az iparág működését alapjaiban befolyásoló törvény életképessége mindösszesen két esztendő volt, mely helyzetet fokoz azon tény is, hogy az Európai Unió távközlési

⁹¹ elektronikus aláírás: elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt és azaz elválaszthatatlanul összekapcsolt elektronikus adat, illetőleg dokumentum

⁹² lehetnek államigazgatás-államigazgatás, gazdasági szereplők-államigazgatás, illetve egyéb viszonylatok is

⁹³ a 2001. évi XXXV. törvény, valamint a végrehajtással kapcsolatos 151/2001. (IX.1.) Korm. rendelet alapján

⁹⁴ szigorúbb az eljárási szabály a fokozott biztonságú szolgáltatások esetében, mint az alapeljárás követelményrendszerével. Például fokozott biztonságú szolgáltató működésének megkezdése bejelentési kötelezettséggel bír, melynél az előírt technológiai követelményeket is teljesíteni kell

⁹⁵ a hatóságnak feladata a nyilvántartásba vételi, illetve minősítési tevékenység folytatása is, mely keretében a szolgáltatókról nyilvántartást vezet. Jogosult a hitelesítés-szolgáltatókat ellenőrizni és az előírásoknak megfelelő működést kikényszeríteni. Felhívhatja a szolgáltatókat az előírások betartására, megtilthatja technológiai alkalmazását, eljárások lefolytatását. Ideiglenes intézkedést rendelhet el, felfüggesztheti az új tanúsítványok kiadását, elrendelheti a régiek visszavonását, bírságot szabhat ki, a szolgáltatót törölheti a minősített hitelesítés-szolgáltatók nyilvántartásából

⁹⁶ 15/2001. (VIII.28.) MeHVM rendelet alapján. Tanúsító szervezet csak független, hatósági jogosítványokkal nem rendelkező, Magyarországon székhellyel vagy lakóhellyel rendelkező, kijelölt szervezet lehet, mely írásban igazolhatja, hogy az elektronikus aláírási termék megfelel a mértékadó előírásokban meghatározott követelményeknek

⁹⁷ 2003. november 27-én került kihirdetésre

piacára⁹⁸ vonatkozó közösségi szabályozási keretrendszer⁹⁹ 2002-ben teljesen átalakult. A tagországoknak 2003. július 25-éig kellett belső jogrendszerüket az új szabályozási elvekhez igazítaniuk.

A hírközlési törvény és végrehajtási rendeleteinek elsődleges célja volt a hírközlési piac liberalizációja a közösségi jogszabályokkal nagyrészt harmonizáló szabályozás útján, azonban a HÍF elnöke korábban tett megállapításai ellenére a szabályok nem váltották be a hozzájuk fűzött, a verseny kialakulásával, elmélyülésével kapcsolatos reményeket, illetve nem segítették elő új piacra lépők megjelenését, nem eredményezték az összekapcsolási, és rajtuk keresztül a végfelhasználói díjak csökkenését. Ennek fontosságát erősíti meg Dr. Martin B. H. Weiss¹⁰⁰ 1990-es évek második felében kialakított véleménye is, amely szerint: „*A szabályozás olyan helyzetekben rendkívül fontos, ahol nincs életképes konkurencia. Ennek célja egy szolgáltató monopolisztikus árszabásának megakadályozása. [...] A szabályokat megalkotó testület legyen független a szolgáltatótól, és felügyelje, hogy ne legyen félrevezető áralakítás, biztosítsa a szolgáltató életképességét és teremtsen stabil jogi és gazdasági keretet a távközlés számára, hogy a szolgáltatók hosszú távú tervezését lehetővé tegyék.*” [12]. A tényleges piaci verseny elmaradásának egyik legfontosabb oka volt, hogy a hírközlési törvény intézményi és eljárási szabályai nem biztosítottak a Hírközlési Felügyelet számára megfelelő eszközöket ahhoz, hogy képes legyen megakadályozni egyes piaci szereplők piaci erejükkel való folyamatos visszaélését. Az Európai Unióhoz történő csatlakozás érdekében hazánk – *többek közt* – jogharmonizációs kötelezettséget¹⁰¹ is vállalt, így kijelenthető, hogy a 2001. decemberében hatályba lépett törvényi szabályozás eleve nem vette figyelembe az unió távközlési piacát teljes mértékben átalakító, előrehaladott közösségi törekvéseket sem. Úgy ítélem meg, hogy a hírközlési törvény a szabályozott és versenyen alapuló piaci viszonyok kialakításának egyik katalizátora volt csupán, hiszen sem a hazai, sem a nemzetközi (közösségi) szakítóp próbát nem állta ki. A régi jogszabályt felváltó törvény kidolgozásakor a kormányzat célul tűzte ki az információkhoz való széleskörű és gyors hozzáférés biztosítását megfizethető áron és javuló minőségben, mely alapelv világosan megjelenik az elektronikus hírközlési törvény preambulumban is: „...*az információs társadalom elektronikus hírközlési infrastruktúrájának továbbfejlesztése, a fogyasztók megbízható, biztonságos, megfelelő minőségű és lehető legalacsonyabb díjú elektronikus hírközlési szolgáltatásokkal való*

⁹⁸ EU terminológia szerint: elektronikus kommunikációs szolgáltatások és hálózatok piaca

⁹⁹ fő irányelvek: az Európai Parlament és a Tanács 2002/19/EK irányelve az elektronikus hírközlő hálózatokhoz és kapcsolódó berendezésekhez való hozzáféréstől és azok összekapcsolásáról (hozzáférési irányelv); a 2002/20/EK irányelv az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások engedélyezéséről (engedélyezési irányelv); a 2002/21/EK irányelv az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások közös keretszabályozásáról (keretirányelv); a 2002/22/EK irányelv az egyetemes szolgáltatásról és az elektronikus hírközlő hálózatokhoz és elektronikus hírközlési szolgáltatásokhoz kapcsolódó felhasználói jogokról (egyetemes szolgáltatási irányelv); a 2002/58/EK irányelv a személyes adatoknak az elektronikus hírközlési ágazatban történő feldolgozásáról és magánjellegének védelméről (az adatvédelemről és az elektronikus hírközlésről szóló irányelv)

¹⁰⁰ a megállapítás publikálásakor Dr. Weiss az egyesült államokbeli Pittsburgh Egyetem tudományos munkatársaként és a Távközlési Program társigazgatójaként dolgozott

¹⁰¹ a társulással kapcsolatosan aláírt Európai Megállapodás 67-68. cikkeiben meghatározottak alapján. A megállapodás a Magyar Köztársaság és az Európai Közösségek és azok tagállamai között társulás létesítéséről szóló, Brüsszelben, 1991. december 16-án aláírt Európai Megállapodás kihirdetéséről szóló 1994. évi I. törvénnyel került kihirdetésre

ellátása érdekében, az elektronikus hírközlési piacon a hatékony, az alkalmazott technológiától független verseny biztosítása, valamint az Európai Közösség jogszabályainak való megfelelés...” érdekében kerül újraszabályozásra az ágazat [13]. Az elektronikus hírközlési törvénnyel ismételtlen megszűnt a postai és a távközlési ágazat egységes kezelése, így mindkét terület működése – *a korábbihoz hasonló módon* – külön jogszabály útján kerül szabályozásra.¹⁰² Az időszakot röviden összegezve elmondható, hogy a hazánk kommunikációs infrastruktúrájának logikai felosztása 1992-ben, törvényi szinten valósult meg. A közcélú távközlési szektor teljes állami monopóliumának lebontására két lépcsőben került sor. Az első szakasz 1990-98 között zajlott, mikor a koncesszió révén lehetőség nyílt az állam számára, hogy feladatai végzésének egy részéről lemondjon, így teremtve lehetőséget a magánszervezetek útján történő – *halaszthatatlan* – infrastrukturális fejlesztések megindításához. Az új koncessziós szolgáltatók a szerződésekben meghatározott beruházási kötelezettségeiket ellensúlyozta, hogy az újonnan megalkotott jogszabályok védeltséget biztosítottak a piacra újonnan belépőkkel szemben, mely mind a felhasználók, mind a szolgáltatók közötti együttműködési eljárások során kedvezőtlen, verseny nélküli helyzetekhez vezetett, mely lehetőséget biztosított az erőfölény következmények nélküli gyakorlására.

A koncesszió alá nem eső távközlési szolgáltatások terén a verseny már gyakorlatilag a kilencvenes évek elején megkezdődött, melyet az új kommunikációs eljárások megjelenése és általános használata, az Internet térhódítása, valamint az információs társadalommal kapcsolatos koncepciók világméretű elfogadása is elősegített. E tendencia hatására a Magyar Posta szervezetének 1990-ben történt szétválasztását követő tizenhárom év alatt több száz regisztrált szolgáltató jelent meg a hírközlési piacon. A vizsgált időszakban kerültek teljeskörűen szétválasztásra a szabályozási-, hatósági- és szolgáltatási funkciók is, mellyel összefüggésben kell megemlíteni, hogy a hatósági tevékenységek végzése során a szakmai függetlenség nem minden esetben valósult meg, amihez párosultak a jogrendszer azon korlátai is, melyek nem tették lehetővé egyes szabályozási előírások, illetve hatósági döntések kikényszerítését.

A hírközléspolitikai 1998-ban történt kihirdetése nyitotta meg az átalakulás második szakaszát, mely még napjainkban sem zárult le. A koncessziós szolgáltatások területe piaci viszonyoknak megfelelő megnyitása, azaz a teljes piac liberalizációja 2001 végén, a koncessziós szerződések lejártával és az új hírközlési törvény életbe lépésével kezdődött meg. A törvény a neki szánt szerepet – *a gyengén megfogalmazott szankcionálási lehetőségek, illetve a változó közösségi szabályozás miatt* – gyakorlatilag nem tudta betölteni, de katalizátora volt az elektronikus hírközlési törvény megalkotásának. A második szakaszban lényeges változásként értékelhető, hogy a jogszabályok különböző balanszírozó lehetőséget biztosítanak a piac aszimmetriájának csökkentésére, így többek között a hatóság által megállapított, úgynevezett jelentős piaci erővel rendelkező szolgáltatókkal szemben – *a tényleges piaci verseny biztosításának érdekében* – kedvezőtlenebb működési feltételek alkalmazása is kikényszeríthető. A változó jogszabályi környezetben a hírközlési hatóság szakmai függetlensége is fokozatosan szilárdul, illetve feladatköre bővül, hiszen az információs társadalom pillérének számító informatikai infrastruktúra gyakorlati használatához kötődő hitelességi problémák kezelésére megalkotott jogszabályban rögzített feladatok és tevékenységek felügyeletét, valamint ellenőrzését szintén a Nemzeti Hírközlési Hatóság feladatkörébe utalták.

¹⁰² a postai tevékenység kereteit a postáról szóló 2003. évi CI. törvény szabályozza

Összességében véve, a tényleges versenyalapú piac csak hazánk Európai Unióhoz való csatlakozásával¹⁰³ valósult meg, hiszen az elektronikus hírközlési törvényben foglaltak teljes hatályosulása ekkor történt meg oly módon, hogy az alacsonyabb szintű szabályozások¹⁰⁴ egy jelentős része e határidőig nem készült el. A tényleges versenypiaci helyzet kialakulásával kapcsolatos megállapítást a nemzeti szabályozó hatóságok tevékenységének módosulása kapcsán 2003-ban tartott előadásában indirekt úton erősíti Dr. Somogyi András¹⁰⁵ is, aki kijelentette, hogy: „Konzultálva több tagállami társhatóság szakembereivel, általában két évre prognosztizálják a teljes piacanálízis módszertani kidolgozásának és lebonyolításának időigényét.” [14], vagyis az elektronikus hírközlési törvény céljainak teljes eléréséhez még szükség lesz türelmi időre. Kijelenthető azonban, hogy 2004-re elérhetővé vált, hogy a civil távközlési szektor sokszereplős szolgáltatói körrel, önállóan funkcionáló hatósággal és szabályozó kormánysszervvel,¹⁰⁶ a tényleges piaci feltételeknek megfelelően, három pilléren nyugodva működjek tovább.

2.1.2. A zártcélú kommunikációs rendszerek jogi alapjai

Hazánk kommunikációs infrastruktúrájában a zártcélú rendszerek – új minőségként – 1992-ben jelentek meg. A hírközléspolitikai kidolgozása a zártcélú kommunikációs rendszerek tekintetében is fordulópontot¹⁰⁷ jelent, mivel új stratégiai célokat fogalmaz a fejlesztéssel és együttműködéssel kapcsolatosan. 1998-ban, a 1071/1998. (V.22.) Korm. határozat kiadásakor több hálózat is funkcionált, melyek egy része az 1990 előtti kommunikációs rendszerekből, más része pedig újonnan, a jogi környezet módosulása révén szerveződött.

2.1.2.1. Átalakuló rendszerek

A katonai- és rendészeti kommunikációs rendszerek 1989-ben a kor színvonalához, valamint a hazai ágazati infrastrukturális körülményekhez mérten fejlettek voltak könnyen belátható, hogy a kilencvenes évek elején nem állt fenn olyan sürgető távközlés-szakmai körülmény, mely markánsan megfogalmazta, illetve indokolta volna e rendszerek önállóságának megszüntetését. Az állam tehát kezdetben nem mondott le arról a lehetőségéről, hogy az erőszakos szervezetek feladatainak ellátásához szükséges kommunikációs támogatást saját hatáskörben és erőforrásainak¹⁰⁸ alkalmazása útján valósítsa meg. A szándék mellett kezdetben nem voltak tisztázottak a szervezeti keretek, hiszen 1990-től az államigazgatás szervezeti- és funkcionális struktúrájában változások kezdődtek, mely folyamatok az államközpontúság megszüntetésére irányult elsősorban. A változások a rendészeti kommunikációs rendszerek oldaláról tekintve bizonyultak jelentősebbnek, hiszen a kilencvenes évek elején a Belügyminisztérium

¹⁰³ mely a Belga Királyság, a Dán Királyság, a Németországi Szövetségi Köztársaság, a Görög Köztársaság, a Spanyol Királyság, a Francia Köztársaság, Írország, az Olasz Köztársaság, a Luxemburgi Nagyhercegség, a Holland Királyság, az Osztrák Köztársaság, a Portugál Köztársaság, a Finn Köztársaság, a Svéd Királyság, Nagy-Britannia és Észak-Írország Egyesült Királysága (az Európai Unió tagállamai) és a Cseh Köztársaság, az Észt Köztársaság, a Ciprusi Köztársaság, a Lett Köztársaság, a Litván Köztársaság, a Magyar Köztársaság, a Máltai Köztársaság, a Lengyel Köztársaság, a Szlovén Köztársaság és a Szlovák Köztársaság között, a Cseh Köztársaságnak, az Észt Köztársaságnak, a Ciprusi Köztársaságnak, a Lett Köztársaságnak, a Litván Köztársaságnak, a Magyar Köztársaságnak, a Máltai Köztársaságnak, a Lengyel Köztársaságnak, a Szlovén Köztársaságnak és a Szlovák Köztársaságnak az Európai Unióhoz történő csatlakozásáról szóló szerződés kihirdetéséről szóló 2004. évi XXX. törvény szerint valósult meg 2004. május 1-jén

¹⁰⁴ elsősorban kormányrendeletek, illetve miniszteri rendeletek

¹⁰⁵ Dr. Somogyi András a publikáció megjelenésekor a Hírközlési Felügyelet döntőbiztosa volt

¹⁰⁶ kormánysszerv: ezen a szakminisztériumot kell érteni. 1989-1990: Közlekedési, Hírközlési és Építési Minisztérium, 1990: Közlekedési és Hírközlési Minisztérium, 1990-2000: Közlekedési, Hírközlési és Vízügyi Minisztérium, 2000-2002: Miniszterelnöki Hivatal (Informatikai Kormánybiztosság), 2002-től: Informatikai és Hírközlési Minisztérium

¹⁰⁷ melyet megelőzően kerül kiadásra a zártcélú távközlő hálózatokról szóló kormányrendelet

¹⁰⁸ erőforrások lehetnek: humán-, pénzügyi-, illetve technikai

szervezetéből kiválva jelentek meg a különböző nemzetbiztonsági szolgálatok¹⁰⁹ és önálló belügyi rendészeti szervek.¹¹⁰ A kommunikációs támogatással kapcsolatos kiforrott álláspontot, valamint az államigazgatás szervezeti struktúrájának módosulását is tükrözi a távközlésről szóló 1992. évi LXXII. törvény, mely megalkotta a zártcélú hálózatok¹¹¹ fogalmát, ezzel teremtve meg az elsőszámú jogi alapot e kommunikációs rendszerek fennmaradásához és további fejlődéséhez. Az 1990 előtti szabályozáshoz képest újdonságnak tekinthető, hogy önállóan is megjelenik a **kormányzati hálózat**, mint a zártcélú hálózatok egyik fajtája.

A törvény a fogalom bevezetésén túl a zártcélú hálózatokra vonatkozó szabályokkal egyáltalán nem foglalkozik, a szabályozás gyakorlati kidolgozását a Kormány hatáskörébe utalta, azonban a konkrét jogszabály megalkotására – *jóval később* – mintegy öt évvel később kerül csak sor. A zártcélú távközlő hálózatokról szóló **50/1998. (III.27.) Korm. rendelet** kihirdetésekor a kormányzati távközlést korábban kiszolgáló rendszerek struktúrájában már több változás is bekövetkezett, melyek alakulását egyrészt kormányzati, másrészt a távközlési szektor szereplőinek¹¹² egyéni szakmai szempontjai befolyásolták. Az előző fejezetben tett megállapítás alapján a kormányzati távközlés megvalósulásában a katonai- és rendészeti kommunikációs rendszerek, a kormányhíradó rendszerek, valamint a Magyar Posta által fenntartott rendszerek játszottak szerepet a kilencvenes évek előtti időszakot tekintve. A honvédelmi ágazat hálózatában, a kormányzati távközlés biztosítása szempontjából lényegi változás nem következett be, mivel a katonai kommunikációs rendszer topográfiáját¹¹³ csak az 1990-1998 között lefolytatott haderőreformok keretén belül lebonyolított szervezeti diszlokáció változása módosította [15].

A minősített időszakokat tekintve az állami és katonai felsővezetés közötti kommunikáció döntően e hálózat útján valósulna meg továbbra is, mivel a rendszer elemei megtalálhatók a „K” vezetési rendszer védett objektumaiban. A távközléssel kapcsolatos szakirányítási, központosított fejlesztési és beruházási tevékenységek végzése továbbra is a vezérkar feladatköre maradt. A rendészeti kommunikációs és a kormányhíradó rendszerek esetében igen jelentős módosulások történtek az állambiztonsági szolgálat megszüntetésével. A *kormányhíradás* körébe tartozó rendszerek¹¹⁴ továbbra is a Belügyminisztérium felügyeletében maradtak [16]. Üzemvitelüket és fenntartásukat 1990-ben a BM Híradástechnikai Szolgálat vette át,¹¹⁵ mely háttérintézmény miniszteri döntés alapján¹¹⁶ 1993-tól az Országos Rendőr-főkapitányság egyik területi

¹⁰⁹ a BM állambiztonsági szolgálatból alakult szervek (a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. évi törvény megnevezései alapján): Nemzetbiztonsági Hivatal, Információs Hivatal, Nemzetbiztonsági Szakszolgálat és a Katonai Biztonsági Hivatal

¹¹⁰ rendőrség, tűzoltóság, polgári védelem, de kettős jogállása miatt ide sorolható a határőrség is

¹¹¹ 1992. évi LXXII. törvény mellékletének 32. pontja alapján: a kormányzati, nemzetbiztonsági, igazságszolgáltatási, közbiztonsági és védelmi érdekeket szolgáló – rendeltetésük szerint elkülönült – távközlő hálózatok és berendezések együttese, amelyek kizárólagosan a speciális igények kielégítését, az e célokra létrehozott szervezet és technika működését szolgálják

¹¹² itt gondolok egyrészt az államigazgatási szervekre, illetve a piaci szereplőkre is

¹¹³ a rendszerelemek konkrét földrajzi elhelyezkedése

¹¹⁴ kormányzati védett távbeszélő hálózat, kormányzati titkosított távbeszélő hálózat, és kormány-összeköttetési géptávíró hálózat

¹¹⁵ az egykori BM I/2. Osztály, vagy ismertebb nevén BM Híradástechnikai Osztály

¹¹⁶ az 1993. április 14-én kelt 16-47/1993. BM számú átirat szerint

szerveként, mint rendőri szervezet¹¹⁷ folytatta tevékenységét. Az ORFK Híradástechnikai Szolgálat továbbra is ellátta a jogelőd szervezet üzemviteli és fenntartási feladatkörét,¹¹⁸ így ettől az évtől kezdődően gyakorlatilag a Belügyminisztérium hatásköréből kikerült az ágazati kommunikációs rendszerek közvetlen irányításának lehetősége. Az ágazati távközlés kilencvenes évek előtt funkcionált szakirányítási módozata a BM Híradástechnikai Szolgálat megszűnésével alakult át véglegesen, mely összhangban volt azzal a kíváncsisággal is, mely szerint a miniszter csak normatív eszközökkel vehet részt az ágazati rendészeti szervek¹¹⁹ irányításában [17]. A kommunikációs tevékenységek szakirányítását így 1993-tól a minisztérium egy hivatali egysége vette át, és ettől az időponttól beszélhetünk egységes ágazati irányítási rendszerről.¹²⁰ A belügyi szervezeti struktúrák átalakulása mellett a közigazgatási ("K") távbeszélő-hálózat és az "ALTÁJ" mobil rádiótelefon hálózat megszüntetéséről szóló **1003/1998. (I.12.) Korm. határozat** előírta az „ALTÁJ” országos mobil rádiótelefon-hálózat felszámolását, majd a **3027/1999. Korm. határozat**¹²¹ alapján került rendszerből való kivonásra a kormányzati védett távbeszélő hálózat (KV), a kormányzati titkosított távbeszélő hálózat (KT), és kormány-összeköttetési géptávíró hálózat is, tehát az egykori kormányhíradó rendszer közel három évtizednyi működést követően végleg megszűnt.

A kormányhíradó rendszer felszámolásának gondolata az évtized első felében fogalmazódott meg, mivel a külföldi viszonylatokban alkalmazott összeköttetések fennmaradása tárgyában több nemzetközi megkeresés¹²² is érkezett a kormányzathoz. A helyzet ellentmondásosságát fokozta a témakörrel összefüggésben 1994 végén összeállított kormányelőterjesztés is, mely kifejti, hogy a kormány-összeköttetési géptávíró kapcsolat egyszerűbb műszaki megoldással, jobban védett információtovábbítást tesz lehetővé az érintett országok kormány szervei felé, mint KT távbeszélő kapcsolat, ugyanakkor rögzíti, hogy a távbeszélő rendszeren a kezelők évi több mint 6.000 beszélgetést kapcsolnak nemzetközi relációban, míg a géptávíró hálózaton többnyire csak szolgálati közlemények továbbítására került sor. A nyilvánvaló ellentmondástól függetlenül a rendszer megszüntetése iránti igény elsősorban biztonsági és politikai megfontolásokra vezethető vissza, mivel az előterjesztésben foglaltak szerint az e témakörrel foglalkozó tárcaközi bizottság a rendszert műszakilag korszerűtlennek, az információhoz való hozzáférés szempontjából¹²³ nem eléggé védettnek, gazdaságilag nem kifizetődőnek, politikailag – *régi kapcsolat-*

¹¹⁷ megnevezését tekintve ORFK Híradástechnikai Szolgálat

¹¹⁸ e körbe tartozik az „ALTÁJ” országos mobil rádiótelefon-hálózat, a BM MRKB mobil rádiótelefon-hálózat, valamint a BM távhívó-távbeszélő hálózat és a BM országos géptávíró hálózat és a „K” vezetési pontokat kiszolgáló kommunikációs hálózatok hatáskörébe rendelt technikai rendszerelemek

¹¹⁹ ágazati rendészeti szervek: rendőrség, határőrség, tűzoltóság, polgári védelem

¹²⁰ az egységes ágazati szakirányítási rendszerben a rendészeti szervek országos parancsnokságain funkcionáló, a rendészeti szerv specifikuma szerinti kommunikációs igényeket szervező és tervező központi szervezeteket fogta össze a minisztérium hivatali egysége. A szakirányítás hatékonyságának egyetlen komoly gyenge pontja a belügyi ágazatnál alkalmazott dekoncentrált támogatási rendszerben rejlik

¹²¹ 1999. december 31-ei hatállyal

¹²² az együttműködéssel kapcsolatos szerződést első ízben Németország mondta fel egyoldalúan, mivel a német jogértelmezés szerinti határidőn belül (3 hónap) nem kapott a magyar fél részéről értesítést megkeresésével kapcsolatosan. 1994-ben a cseh és román kormány részéről érkezett igény a szerződések újratárgyalásával kapcsolatos kérdéskörben

¹²³ az információvédelmi eszközök kriptográfiai működéséhez szükséges kódkulcsokat – a kommunikációs rendszer teljes felszámolásáig – a Федеральное Агентство Правительственной Связи и Информации при Президенте Российской Федерации (ФАПСИ – az Oroszországi Föderáció elnökének alárendeltségében működő Kormányzati Távközlési és Információs Szövetségi Ügynökség) elnevezésű orosz titkosszolgálati szerv készítette. A szervezet 1991. december 24-én, az Oroszországi Föderáció elnökének 313/1991. számú rendelete alapján jött létre az egykori KGB átszervezése kapcsán. A rejtjelző eszközök rendszervál-

rendszer szerinti kiépítettsége miatt – egyes államok részéről félreérthetőnek, ezért összességében véve értelmetlennek tartja a távbeszélő rendszer további fenntartását [18]. A rendszer megszüntetésével kapcsolatos végleges politikai-szakmai döntés mintegy öt évvel később született csak meg.

A kilencvenes évek elején a kormányzati távközléssel összefüggő egyik fontos kritérium továbbra is változatlan maradt, vagyis a kormányzati szervek kommunikációját kiszolgáló rendszer fő minőségi mutatója az információvédelmi képesség szintjével is arányos volt. Ezt a megállapítást támasztja alá, hogy a **3443/1993. (XI.25.) Korm. határozat** előírta a Kormányzati Távközlési Iroda¹²⁴ Nemzetbiztonsági Hivatal szervezetében történő megalakítását. A „K” távbeszélő hálózat¹²⁵ – *hasonlóan a katonai- és rendészeti kommunikációs rendszerekhez* – korszerűnek volt tekinthető az infrastruktúra többi eleméhez képest, így megszüntetése távközlés-szakmailag szintén nem volt indokolt a '90-es évek elején. A hálózat működtetését és fenntartását a Magyar Távközlési Vállalat, mint tulajdonos vette át, mely társaság a koncessziós és távközlési törvény hatására a piac egyik meghatározó szolgáltatójává vált. A MATÁV új szolgáltatói szerepköre tehát megkövetelte a rendszer használatának jogi és finansziális rendezését is, mely a közigazgatási („K”) távbeszélő hálózat használatáról szóló **1010/1991. (II.26.) Korm. határozat** megalkotásával teljesült.

Az egységes kezelésben levő országos hálózat egyes rendszerlemei az évtized közepén, a koncessziós pályázatok útján került más-más szolgáltató tulajdonába és kezelésébe. A rendszer további, azonos elgondolások szerinti fejlesztése és üzemeltetése a piacra lépő szolgáltatók számára nem jelentett gazdasági hasznot, hiszen a koncessziós szerződésekben kötelezően vállalt technikai fejlesztések folyamatos realizálódása révén a „K” rendszer lényege¹²⁶ szűnt meg, melyhez párosultak a sokszereplőssé vált piac érdekellentétei. E feltételek közepette a „K” távbeszélő hálózat az évtized második felére mind technikailag, mind erkölcsileg amortizálódott. Teljes felszámolására a 1003/1998. (I.12.) Korm. határozat alapján került sor. A minősített időszakok állami vezetésével szemben támasztott egyik legfontosabb követelmény a kilencvenes évek elején sem változott. A „K” vezetési rendszernek¹²⁷ tehát továbbra is garantálnia kell a társadalommal való állandó kommunikációs képességen keresztül az állam szervezett életének, az államigazgatás rendszerének, a gazdaság működésének, a lakosság ellátásának, védelmének és mentésének, valamint a fegyveres erők és rendészeti szervek tevékenységének irányítását. A „K” vezetési rendszer kommunikációs igényeinek többségét biztosító K-600-as hírendszerrel kapcsolatos fenntartási és üzemeltetési feladatokat 1990-ben a Magyar Távközlési Vállalat vette át. A társaság a rendszer működtetését normál gazdasági tevékenységének részeként, piaci alapon vállalta, mely a kilencvenes évek elején súlyos finanszírozási problémát vetett fel. A problémát to-

tást követő használatával kapcsolatosan a magyar kormány 1991-ben kötött megállapodást a szovjet kormánnyal, mely tény a 3324/1991. számú Korm. határozattal került kihirdetésre

¹²⁴ a Kormányzati Távközlési Iroda működteti a különböző állami szervek felsővezetői körében rendszerezett információvédelmi végberendezéseket, melyeket a távbeszélő szolgáltatások igénybevétele során, pont-pont viszonylatban lehet használni bármely szabványos analóg távbeszélő szolgáltatás-hozzáférési ponton. 2004-ben kezdődött meg az addig alkalmazott, amerikai gyártmányú eszköz (ARAMIT) hazai fejlesztésű és gyártású eszközzel való (ARGON) kiváltása. A szervezet jelenleg a Nemzetbiztonsági Szakszolgálat szerveként működik annak megalakulása óta, vagyis továbbra is a titkosszolgálatok keretében végzi feladatát.

¹²⁵ itt e hálózat részeként értelmezem az „MK” rendszert is

¹²⁶ vagyis a korábbi elmaradottabb infrastruktúrával szemben nyújtott szolgáltatásbeli minőségkülönbség

¹²⁷ a „K” vezetési rendszer kormányzati jellegének felszámolása a 3015/2004. (III.31.) Korm. határozat kiadásával kezdődik meg

vább fokozta, hogy a részvénytársasággá alakult szolgáltató és az állam közötti tulajdonmegosztás¹²⁸ kérdése is függőben volt.

A megoldás érdekében a Kormány a **3557/1992. (XI.24.) Korm. határozat**ában előírta a MATÁV Rt. igényeinek¹²⁹ költségvetés keretében történő rendezését, mellyel egyidejűleg a hírendszer rendeltetésszerű működésének határáig a követelmények mérsékelhetőek voltak. A helyzet konszolidálásának ellenére a K-600-as hírendszer összeköttetései mennyisége folyamatosan csökkent. A „K” vezetési rendszer új alapokra helyezett kommunikációs rendszerével szembeni elvárásokat¹³⁰ a **3030/1995. (IV.6.) Korm. határozat** és a **3031/1995. (IV.6.) Korm. határozat** fogalmazza meg, melyek napjainkban is alapját képezik rendszerrel szemben támasztott főbb követelményeknek. A minősített időszaki távközlés biztosításával összefüggésben az egykori Magyar Posta hálózatában a belügyi tárca részére fenntartott K-400-as rendszer a kilencvenes évek elején – *a minisztérium funkciójának és jellegének gyökeres átalakulásával, valamint hazánk védelme koncepciójának módosulásával*¹³¹ – teljes felszámolásra került. Az 1990-től megkezdődő védelmi felülvizsgálatok kapcsán, fennmaradó katonai szervezeteinek arányában a honvédelmi szektor is redukálta a K-300 és K-500 hírendszerei útján kialakított jelszavas és számjeles áramkörei¹³² számát.

2.1.2.2. Új rendszerek kialakítása

A zártcélú rendszerek bővítési igénye és szükségessége a közigazgatási struktúra 1990-től történő átalakításának¹³³ megindításával jelent meg, mellyel kapcsolatosan Dr. Torma András¹³⁴ a következőket állapítja meg: *„A társadalom szervezetrendszerei közül a közigazgatás a legnagyobb, ennél fogva – objektíve – a legnehezebben mozgítható és mozduló struktúra. [...] A napjainkban zajló információs és kommunikációs forradalom azonban kikényszeríti a változást a közigazgatásban. A számítógép, a számítástechnika, a modern információs és kommunikációs technológiák behatolása a közigazgatásba már Magyarországon is napjaink realitása, ami új feladatokat, új kihívásokat állít a közigazgatás elé.”* [19]. A bővítéssel kapcsolatos munkálatok a **3296/1991. (VII.5.) Korm. határozat**¹³⁵ megjelenésével, a szervezeti keretek kialakításával indulnak meg. Az általános elképzelésekben az információs rendszerek moder-

¹²⁸ a problematika egyaránt érintette mind a katonai, mind a rendészeti kommunikációs rendszereket üzemeltető szerveket is, mivel 1990 előtt sok esetben a tulajdon pontos megosztására az állami szervezetek nem mindig fordítottak különös gondot

¹²⁹ a fennmaradt dokumentumok alapján 1991-ben 130,6 millió forint, 1992-ben 337 millió forint volt

¹³⁰ legfőbb követelményként jelentkezik, hogy a távközlési és informatikai szolgáltatások integrált rendszerben kerüljenek biztosításra, de egyúttal tegye lehetővé a K-600-as hírendszer fennmaradt elemeinek, az zártcélú és közcélú hálózatok lehetőség szerinti felhasználását is. E mellett a rendszert úgy kell kialakítani, hogy annak minél több eleme működjön békeállapotban, tehát üzemeltetést és fenntartását költségkímélő módon kell szervezni

¹³¹ a megváltozott védelmi koncepciót először a Magyar Köztársaság biztonságpolitikájának alapelveiről szóló 11/1993. (III.12.) OGY határozat és a Magyar Köztársaság honvédelmének alapelveiről szóló 27/1993. (IV.23.) OGY határozat foglalja össze

¹³² mai közzismertebb nevei: JUHARFA, LAVINA, V-500 rendszerek

¹³³ a reformok mind a mai napig nem zárultak le. Ezt bizonyítja, hogy a vizsgált időszakban e témakörben egy sor kormányhatározat jelent meg, melyek közül a legfontosabb a területi államigazgatási szervek fő irányairól szóló 1105/1995. (XI.1.) Korm. határozat, valamint a közigazgatási rendszer korszerűsítésével kapcsolatos feladatokról szóló 2198/2003. (IX.1.) Korm. határozat

¹³⁴ Dr. Torma András az idézett publikáció megjelenésének időpontjában a Miskolci Egyetem Alkotmányjogi Tanszékének tanszékvezető egyetemi docense volt

¹³⁵ a határozat alapján jön létre az Informatikai Tárcaközi Bizottság és a Miniszterelnöki Hivatal Informatikai Koordinációs Irodája. Hatálytalannítja a 1066/1999. (VI.11.) Korm. határozat 11. pontja

nizációja kap prioritást, vagyis a korszerűsítés elsősorban – *a távközléshez képest elmaradottabb* – informatika területét célozza meg.

1992-ben a közigazgatás korszerűsítéséről szóló **1026/1992. (V.12.) Korm. határozat**¹³⁶ előírja, hogy fel kell tární a közigazgatás információs rendszereiben meglevő párhuzamosságokat és javaslatot kell tenni a Kormány információs rendszerének kialakítására, mely feladat továbbfejlesztése révén a következő évben jelenik meg a **1039/1993. (V.21.) Korm. határozat** a központi államigazgatási szervek informatikai fejlesztésének koordinálásáról. A határozat a kormányzati távközlés megújítása szempontjából jelentős okmány, mivel előírja, hogy ki kell dolgozni a kormányzat integrált adatátviteli és távközlő hálózatának fejlesztési tervét, valamint meg kell határozni a hálózat működtetésének szervezeti, személyi és tárgyi feltételeit.¹³⁷ Az 1994-es jelentések alapján az Egységes Kormányzati Zártcélú Hálózat (EKZH) megvalósíthatósági tanulmányának kidolgozása az Amerikai Egyesült Államok kormányának segítségével taladott, de az, az előírt határidőre¹³⁸ mégsem készült el [20]. Az EKZH koncepcionális elvei csak 1995-ben kerültek hivatalosan is megfogalmazásra a 3030/1995. (IV.6.) Korm. határozat, valamint a 3031/1995. (IV.6.) Korm. határozat¹³⁹ által. A határozatok kiadásával egyidejűleg a Kormány hozzájárult a tervezési és előkészítési munkák megkezdéséhez a Miniszterelnöki Hivatal és a Közlekedési, Hírközlési és Vízügyi Minisztérium közötti megosztott koordinációs felelősséggel. A Miniszterelnöki Hivatal koordinálásában összeállított koncepció alapján az EKZH igen széles felhasználói kört¹⁴⁰ célzott meg, a tervek csak Budapesten mintegy 25-30 ezer fő felhasználót¹⁴¹ regisztráltak [21]. Más zártcélú távközlő hálózatokhoz való csatlakozás szempontjából a Honvédelmi Minisztérium (HM), a Belügyminisztérium (BM) által fenntartott rendszerek és az X.400 kormányzati levelezőrendszer¹⁴² jött szóba elsősorban. A budapesti HM és BM objektumok¹⁴³ esetében az EKZH keretében telepítésre kerülő eszközök által, míg a vidéki helyőrségekben az EKZH megyei központja¹⁴⁴ és az adott katonai szervezet hírközpontjának összekapcsolása útján jön létre a kommunikáció. A BM területi és helyi szervei¹⁴⁵ szintén az EKZH megyei központjaival kerülnek összekötte-

¹³⁶ hatálytalanítja a 112/1994. (VIII.6.) Korm. rendelet 4. § (1) bek.

¹³⁷ a kidolgozás koordinálásáért a Miniszterelnöki Hivatal volt a felelős

¹³⁸ a határidőt a 1038/1994 (V.19.) Korm. határozat 1994. október 31-re módosította

¹³⁹ a kormányhatározatok a minősített időszak tevékenységgel kapcsolatos, államtitkot képző információkat is tartalmaztak. Az EKZH kialakításával összefüggő kormányzati koordináció során a tárcák részéről kritikák érkeztek a minősítési eljárással kapcsolatosan, hiszen a biztonsági intézkedések miatt a végrehajtásba bevonható kört is szűkíteni kellett. Megoldásként merült fel a béke- és minősített időszak követelmények kettéválasztása

¹⁴⁰ a felhasználói kör kiterjedtségét az értekezés 1. számú melléklete tartalmazza

¹⁴¹ ez természetesen a helyhez kötött szolgáltatás-hozzáférési pontokat fedi le. Az EKZH rádiós alrendszerében 30-50 ezer tagállomással számolt a terv

¹⁴² az X.400 levelező rendszer ekkor 16 budapesti kormányhivatalra terjedően működött

¹⁴³ honvédelmi tárca: HM-I. és HM-II. objektum, belügyi tárca: BM központi épület, illetve BM Mogyoródi út

¹⁴⁴ az EKZH megyei kommunikációs központjai az adott megye Közgyűlésének működési helyén teleptek volna. A megyeszékhelyeken az EKZH csak a megyei közgyűlés, illetve a vele egy létesítményben elhelyezett szervek számára biztosított volna teljes ellátást. Az egyéb, bevonásra tervezett szervezetek esetében csak az adott vezető beosztású személyek, illetve a központi szervekkel való kapcsolattartás szempontjából meghatározó szervezeti elemek számára került volna EKZH szolgáltatás-hozzáférési pont kiépítésre

¹⁴⁵ ez vonatkozik mind a rendőri, mind a határőrizeti szervekre egyaránt

tésbe. Az átviteli kapcsolatokat¹⁴⁶ elsősorban a szolgáltatóktól való bérlemény alkotja. A „K” távbeszélő hálózat funkcióját az EKZH teljes körűen átveszi, míg a „KT” és „KV” rendszerek tekintetében ekkor még nem született konkrét döntés. Architektúra szempontjából az EKZH két távbeszélő tranzitközpont mellett a BM hálózathoz igazodó két- vagy háromsíkú gerinchálózati topológia szerint épül fel. Az adatátviteli megoldás alapjául az ISDN – Frame Relay¹⁴⁷ kombináció szolgál, a különböző LAN¹⁴⁸-okat összekötő új adatátviteli hálózat közege a száloptikára alapozott SDH,¹⁴⁹ melyhez csatlakozott az „ALTÁJ” mobil rádiótelefon-rendszerre alapozott mobil hálózat. Alapvető célkitűzés volt a kivitelezés kezdetétől számított 5 éven belüli 80 %-os kiépítettség elérése.

A koordinációért felelős kormányzati szervek 1996 végére újabb, államtitkot nem képző előterjesztést állítottak össze az egységes kormányzati célokat szolgáló kommunikációs rendszer megvalósítása feladatainak konkrét meghatározása érdekében. Az előterjesztés kihangsúlyozza, hogy: „...az új politikai intézményrendszer szinte azonnal megteremtette, az informatika térnyerése pedig meggyorsította a további párhuzamos kormányzati távközlési rendszerek kiépítését. Most azonban már ágazaton, sőt egyes minisztériumokon belül is jellemző a többszörös párhuzamosság és a teljes káosz.” [22]. Rögzíti továbbá, hogy a költségvetés a távközlési és informatikai igények teljes kielégítésére évente mintegy 50 milliárd forintot biztosít, azonban a források a különböző tárcáknál erősen széttagolva jelennek meg, amelyhez hozzátartozik, hogy e szakterületen foglalkoztatottak száma meghaladja a 2.000 főt. A KTR kialakításával kapcsolatosan előterjesztett határozattervezet nem került elfogadásra, helyette a MeH és a KHVM által kidolgozott **3021/1997. (V.8.) Korm. határozat** jelent meg, mely többek között tartalmazza az ismertetett elgondolásokat is.

A kiépítésre tett kormányzati erőfeszítések ellenére sem az EKZH, sem a KTR projekt nem mutatott fel kézzel fogható eredményeket. Az eredménytelenség okainak konkrét megállapítása a forrásdokumentumok hiányában nehézkes, azonban a korábbi alfejezetekben eddig bemutatott környezet ismerete alapján az okokat a következőkben látom:

- mind az EKZH, mind a KTR olyan zártcélú kommunikációs infrastruktúrára alapozott, melyekben túlsúlyos volt a hagyományos (analóg) távbeszélő, rádiótávközlési, és adatátviteli technológia aránya. Ezek a műszaki adottságok a kezdetekben nem jelentettek hátrányt, hiszen a nem kormányzati szektor minőségi mutatói nem voltak kedvezőbbek;
- a kormányzati szinten elhúzódó koordinációs, tervezési és döntési folyamatok eredményeképpen a megvalósításba bevonni tervezett zártcélú hálózatok csak késve alkalmazkodnak a megváltozó technológiai és szolgáltatásnyújtási környezethez, így az alpinfrastruktúra gazdasági jellegű megítélése kedvezőtlenül változott meg. Természetesen ez visszavezethető az 1990-es évek elején

¹⁴⁶ 1995-ben önálló, országos átviteli hálózattal csak a honvédelmi tárca rendelkezett, azonban a katonai, rendészeti és közigazgatási szervek eltérő diszlokációja nem tette lehetővé a rendszer felhasználását

¹⁴⁷ Frame Relay: az X.25 csomagkapcsolt adatátviteli szabvány továbbfejlesztett változata

¹⁴⁸ LAN: Local Area Network – Helyi Hálózat

¹⁴⁹ SDH: Synchronous Digital Hierarchy – Szinkron Digitális Hierarchia. SDH – Synchron Digital Hierarchy (Szinkron Digitális Hierarchia). Olyan átviteli rendszer, amely alkalmas arra, hogy tetszőleges szintű PCM jelsorozatok hierarchikus multiplexálás és demultiplexálás nélkül, külön-külön behelyezhetők, illetve abból kivethetők legyenek

bekövetkezett és elhúzódó, az államigazgatás működését jelentősen befolyásoló recesszióra is;

- a konvergencia hatásaként egyre szélesebb körben elterjedő multimédia alkalmazások használatának igénye a fontosságot a hagyományos távközlési szektorról egyre inkább az informatikai szektor irányába mozdítja el, mely egyértelműen megfigyelhető kormányzati szinten is. Ez a folyamat nem kedvez a hagyományos távközlési alapokkal (technológia, humán erőforrás) rendelkező szervezeteknek az elkerülhetetlen szervezeti integráció során;
- igen fontos körülmény, hogy a távközlési törvény lehetővé tette a zártcélú hálózatok elkülönült módon való további fenntartását, mely helyzetet megerősített az egy évvel később kihirdetett, a zártcélú hálózatok működését rögzítő 50/1998. (III.27.) Korm. rendelet. E két szabályozási aktussal az 1990-es évek előtti állapothoz képest a hálózatgazdák száma jelentősen nőtt, mely helyzet – *véleményem szerint* – végső soron lehetőséget teremtett arra, hogy a kormányzati szinten elhúzódó koordinációs, tervezési és döntési folyamatok miatt önálló utas fejlesztések induljanak meg;
- miután a liberalizált, versenyen alapuló távközlési piac kialakítására tett kísérletek csak az évtized elején kezdődtek meg, így a közigazgatás gyakorlatilag minden szegmensén megjelenő, jelentős felhasználói kört magába foglaló, saját kommunikációs szolgáltatásokat nyújtani kész szervezet megjelenése egyértelműen veszteséget okozott volna a monopolisztikusan működő távközlési szolgáltatások piacán, mellyel várhatóan – *a szolgáltatók részéről* – gazdasági érdekek is sérültek volna.

A zártcélú kommunikációs rendszerek további jogszabályi környezetének vizsgálata szempontjából az 1998-as esztendő mérföldkőnek tekinthető. Ez évben jelent meg a Kormány 1998-2005 évekre vonatkozó hírközléspolitikája, illetve a távközlési törvény felhatalmazása alapján a zártcélú hálózatokra vonatkozó szabályozás. A két joganyag majdnem egyidejű megjelenése¹⁵⁰ némileg ellentmondásos helyzetet teremtett, melynek feloldására (mérséklésére) első ízben 2001-ben került sor. A hírközléspolitikai függeléké leszögezi, hogy: „*Létre kell hozni - elsősorban a szolgáltatók versenyeztetése útján és a kormányzati szervezetek és állami többségi tulajdonú gazdálkodó szervezetek meglévő távközlési erőforrásait is felhasználva - a közigazgatási, valamint a rendvédelmi szervezetek igényeit kielégítő, többszintű, szintenként differenciáltan védett, költségtakarékos, integrált távközlő rendszert. A közcélú és különhálózatok optimális kombinációjaként megvalósítandó rendszer egységes irányítását kormányzati (ágazati) felügyelet alá kell vonni. Egyidejűleg meg kell szüntetni az indokolatlan párhuzamosságokat a zártcélú kormányzati távközlő hálózatok létesítése és működtetése terén. Az egységes, európai színvonalú rendszernek béke idején és a minősített időszakban is folyamatosan biztosítania kell az országirányítás távközlési feltételeit. Mindenkor és mindenhol szükségesek a megfelelő szintű és minőségű távközlési kapcsolatok az Európai Unió és a NATO kormányzati és védelmi szerveivel.*” [23]. Tehát a kormányzat – *korábbi elképzeléseit továbbra is fenntartva* – egyértelmű célként fogalmazza meg az egységes kormányzati felügyelet alatt levő, integrált, költségtaka-

¹⁵⁰ a zártcélú távközlő hálózatokról szóló kormányrendelet hozzávetőleg két hónappal korábban kerül közzétételre

rékos kommunikációs rendszer kialakítását oly módon, hogy a meglevő zártcélú hálózatok működése által kialakult párhuzamosságok¹⁵¹ teljes mértékben megszűnjenek. E kívánnalommal némileg ellentétes, hogy az 50/1998. (III.27.) Korm. rendelet kihirdetésekor¹⁵² hét különböző hálózatgazdát nevesít, amely 2003-ra összesen nyolcra¹⁵³ emelkedik [24]. A rendelet meghatározza, hogy a hálózatgazda köteles a működtetés és fejlesztés forrásairól ön maga gondoskodni,¹⁵⁴ melyből egyértelműen következik, hogy a megjelenő ágazati igények kormányzati igényekkel való összehangolása gyengült, főleg azon szervek esetében, melyek jelentős önálló hálózattal rendelkeznek. A koordináció gyengülése, az önállósult fejlesztések felerősödése természetesen nem segíti elő a költségtakarékossággal összefüggésben megfogalmazott követelményeket sem.

További szakmai előrelépésként értékelhető, hogy a hírközléspolitikában megfogalmazódik: „Elkerülhetetlen a készenléti szolgálatok részére biztosított 380-400 MHz-es sávban, valamint egyéb kormányzati célokra a 410-430 MHz-es sávban működő (PAMR)¹⁵⁵ digitális trónkölt diszpécser jellegű rádiótelefon-szolgáltatás bevezetése 1999-ben.” [25]. A digitális trónkölt rádiórendszerek¹⁵⁶ hazai bevezetésének gondolata az EKZH, illetve KTR koncepciókban jelenik meg első ízben, mely egyúttal nóvumként is értékelhető, hiszen az Európai Rádiótávközlési Bizottság csak 1995 februárjában állította össze az Európai Bizottságnak szóló jelentését a készenléti szolgálatok európai együttműködésére alkalmas trónkölt rádiókommunikációs technológia működtetését elősegítő frekvenciaspektrum¹⁵⁷ tényleges kijelölésének lehetőségéről.

A hírközléspolitikai egyértelművé teszi, hogy az ország hosszútávon elkötelezi magát az európai szabvány alkalmazása mellett,¹⁵⁸ igaz a vizsgált időszakban nem szüle-

¹⁵¹ a párhuzamosságok alatt itt egyértelműen az azonos helyeken, azonos típusú, de különböző kommunikációs infrastruktúra igénybevételével történő szolgáltatásnyújtásról van szó

¹⁵² a rendeletet 2004-ig összesen hét alkalommal kerül módosításra a következő jogszabályokkal: 131/2001. (VII.13.) Korm. rendelet, 227/2001. (XI.30.) Korm. rendelet, 205/2002. (IX.26.) Korm. rendelet, 107/2003. (VII.18.) Korm. rendelet, 212/2003. (XII.10.) Korm. rendelet, 5/2004. (I.9.) Korm. rendelet, 100/2004. (IV.27.) Korm. rendelet

¹⁵³ megállapította az esélyegyenlőségi tárca nélküli miniszter feladat- és hatásköréről szóló 107/2003. (VII.18.) Korm. rendelet 11. § (2) bek.-e. Ekkor került az Egységes Digitális Rádiótávközlő Rendszer hálózatgazdájaként nevesítve az IHM miniszter

¹⁵⁴ ezt a kitételezt a zártcélú távközlő hálózatokról szóló 50/1998. (III.27.) Korm. rendelet módosításáról szóló 131/2001. (VII.18.) Korm. rendelet 1. § (1) bek. módosította oly módon, hogy megállapodás alapján az üzemeltetést végző szervezet is gondoskodhat a pénzügyi fedezetéről

¹⁵⁵ vagy PMR (Professional Mobile Radio). Gyakorlatilag a nem kormányzati szervek rádiókommunikációs igényei kielégítésére szolgáló rendszer

¹⁵⁶ trónkölt rádiórendszer: 1988-ban az ETSI STC (European Telecommunications Standardization Institute, Standard Telecommunications Committee) 6. számú határozatában megfogalmazta, hogy a jövő rádiótávközlésében a spektrumhatékonyság növelése érdekében digitális adást kell alkalmazni és azt trónkölt rendszerként szervezni

¹⁵⁷ a 380-400 MHz-es sáv, mely 1996 előtt NATO katonai sávként került felhasználásra. A CEPT (Conference of European Post and Telecommunications Administration) a NATO szerveivel történt egyeztetést követően 1993-ban alkotta meg a használatlalt kapcsolatos CEPT T/R 02-02 számú ajánlását. A spektrum 1996-ban az Európai Rádiótávközlési Bizottság (European Radiocommunications Committee) ERC/DEC (96) 01 határozata alapján került az EU készenléti szervek kizárólagos használati körébe. Magyarországon erre a Frekvenciasávok Nemzeti Felosztási Táblázatának megállapításáról szóló 204/1997. (XI.19.) Korm. rendeletben foglaltak alapján kerül sor. 1999. április 23-án az ETSI legfelsőbb döntéshozó fórumán a küldöttek egyedülként a TETRA szabványt ismerték el

¹⁵⁸ a trónkölt rádiórendszer hazai bevezetésének egyik szükségességét indokolja (mind a mai napig) a Benelux államok, NSZK és Franciaország között 1985. június 14-én létrejött egyezmény (schengeni egyez-

tik egyértelmű döntés sem az ezt megvalósító technológiát,¹⁵⁹ sem a szállító szolgáltatókat illető kérdésekben. A hazai bevezetéssel kapcsolatos nemzetközi egyeztetések 1996-ban kezdődtek meg, majd 1998 novemberében Budapesten került összeállításra és beüzemelésre az európai kontinens legnagyobb TETRA kísérleti mintarendszere¹⁶⁰ [26]. A 1071/1998. (V.22.) Korm. határozat megjelenését követő években az egységes kormányzati kommunikációs rendszer kialakítására irányuló törekvések folytatódtak, hiszen a hírközlést érintően már létezett hírközlési stratégiai terv, illetve a korábbi, meghatározó jelentőségű kormányhatározatok továbbra is érvényben maradtak, azaz megfelelő jogszabályi alap állt rendelkezésre.

E téren tovább erősödött a központi kormányzat¹⁶¹ vezető szerepe, melyet az államigazgatási informatika koordinációjának továbbfejlesztéséről szóló **1066/1999. (VI.11.) Korm. határozat**¹⁶² is megerősít. A rendszerek továbbfejlesztését illetően elsőként 1999-ben, a Miniszterelnöki Hivatal összeállításában jelent meg újabb előterjesztés¹⁶³ az egységes kormányzati adatátviteli optikai (KODNET) hálózat kialakításáról, és az egységes kormányzati adatátviteli optikai (KODNET) hálózat kialakításáról [27]. Az előterjesztés igyekszik hasznosítani az EKZH, valamint a KTR tervezése során született eredményeket, azonban nem tűzi ki célul a hagyományos beszédátviteli szolgáltatások kormányzati szintű bevezetését, elsősorban a trónkölt rádiórendszer kialakítására, valamint az adatátviteli képességek növelésére tesz javaslatot. A rendszerek kialakítására való törekvések illeszthetők voltak a korábbi, még érvényben levő kormányhatározatokhoz,¹⁶⁴ azonban az előterjesztő érzékelteti, hogy kormányzati körökben a KTR koncepció továbbfejlesztése esetleg már nem mutatkozik kívánatosnak.

Elsőrendű követelményként fogalmazódik meg, hogy centralizált – *a Miniszterelnöki Hivatal vezető miniszter által történő* – irányítást és felügyeletet kell gyakorolni

mény) alapján kidolgozott és az egyezményhez csatlakozott további államok által 1990. június 19-én jóváhagyott végrehajtási megállapodásban rögzített azon kötelezettség, amely szerint a tagállamok kialakítják a közrend és közbiztonság, valamint az állambiztonság fenntartását támogató Schengeni Információs Rendszert. A rendszer egyik elemét képi a tagállamok mindegyikében (a harmonizált frekvenciasávban) működtetett digitális trónkölt rádiórendszer is

¹⁵⁹ a digitális trónkölt rádiórendszerek tekintetében két jeltovábbítási technológia létezik: időosztásos (TDMA – Time Division Multiple Access), illetve frekvenciaosztásos (FDMA – Frequency Division Multiple Access). Ezen belül hazánk számára – gazdasági és politikai megfontolásokból – alapvetően a TETRA (időosztásos), illetve a TETRAPOL (frekvenciaosztásos) rendszer használata járható

¹⁶⁰ a kísérlet műszaki hátterét az ORFK Híradástechnikai Szolgálat bázisán a Motorola biztosította. A szolgáltatások tesztelését alapvetően a BRFK XIV. kerületi Rendőrkapitányság állománya, szolgálati feladataik ellátása során, tehát munkakörülmények között végezte. A teszt sorozat közel másfél évig zajlott, mely időszakban a TETRA rendszerek különböző gyártók által készített gyártmányainak együttműködési tesztjére, illetve TETRAPOL rendszer próbájára is sor került

¹⁶¹ a központi kormányzat vezető szerepének erősödését jelzi, hogy – *német minta alapján* – a Miniszterelnöki Hivatal átalakításával összefüggő egyes jogszabályok és kormányhatározatok módosításáról szóló 168/1998. (X.6.) Korm. rendelet kihirdetését követően a hivatal vezetését miniszteri rangú köztisztviselő veszi át az addigi közigazgatási államtitkártól

¹⁶² a határozat mellékletében meghatározásra kerül a miniszter feladata, mely gyakorlatilag megszabja teljes felelősségét a kormányzati informatikai tevékenységek (stratégiai tervezés, fejlesztés, szabványosítás, ajánlás-kibocsátás, oktatás, képviselet) gyakorlása tekintetében

¹⁶³ az előterjesztés a korábbi anyagokhoz képest általánosabb kidolgozottságú, kevesebb konkrét követelményt határoz meg. Az előterjesztés évében már kivonásra került az ALTAJ, KT, KV és kormány-összeköttetési géptáviró rendszer

¹⁶⁴ alapvetően: a 3031/1995. (IV.6) Korm. határozat, 3021/1997. (V.8.) Korm. határozat és 1071/1998. (V.22.) Korm. határozat

a belügyminiszter és a honvédelmi miniszter békeidejű feladatainak, valamint az „M” időszak feladatainak érintetlenül hagyása mellett, úgy, hogy az érdekelt kormányzati szerveknek az eddig megszerzett tapasztalataik felhasználásával közre kell működniük. Másodsorban – *a hírközléspolitikában megfogalmazottaknak megfelelően* – megjelenik, hogy célszerű mind a két beruházással és üzemeltetéssel kapcsolatos tevékenységet a hírközlési piac többségi állami tulajdonban levő szolgáltató szervezetein keresztül – *szolgáltatási alapon* – igénybe venni [28]. A szolgáltató szervezet kiválasztása tekintetében az előterjesztés egyértelműen olyan társaságot¹⁶⁵ jelöl meg, amely akkori infrastruktúrája révén képes mindkét rendszer kialakításával és üzemeltetésével kapcsolatos követelményt teljesíteni. Műszaki szempontból a KODNET hálózat kialakítását úgy kell tervezni, hogy az mindenfajta multimédia alkalmazásra egységesen előkészített legyen. Biztosítani kell az IP és SDH együttműködéseket, a WDM¹⁶⁶ optikai rendszerekhez való átjárókat, valamint a meg kell oldania a beszéd adatként való kezelését.¹⁶⁷ Mindkét beruházás teljes finanszírozása egyértelműen a szolgáltató szervezetet terhelő az állam halasztott konstrukcióban történő visszafizetési kötelezettsége mellett, melyen az üzemeltetés (szolgáltatási díj) költségeibe épül be.¹⁶⁸ Az előterjesztés kapcsán végzett kormányzati koordinációs tevékenység nem járt gyakorlati eredménnyel, így – *több korábbi anyaghoz hasonlóan* – tervezet maradt, azaz nem kerül véglegesen elfogadásra és megjelentetésre.

A kormányzati kommunikációs rendszer kialakítására tett 1999. évi elvi erőfeszítéseket követően egyértelműen megfigyelhető, hogy a kormányzati gondolkodásmódban teljes mértékben kettévált – *az addig összességében véve egységesen kezelt* – rádió-kommunikáció, valamint a hagyományosnak tekinthető vezetékes kommunikáció.¹⁶⁹ Ennek indokait elsősorban abban látom, hogy a 1066/1999. (VI.11.) Korm. határozat alapján legfelsőbb kormányzati szinten, a szolgáltató típusú állam és közigazgatás koncepciójának¹⁷⁰ megjelenésével került ismételt megerősítésre az informatika szerepének elsődlegessége,¹⁷¹ mely háttérbe sorolta a – *nem rádiókommunikációval foglalkozó* – távközlési szakterületet, azonosítva az informatikai igények támogatói szerepével. A szolgáltató állam és közigazgatás megteremtése érdekében történő informatizálás jelentősége az alábbiak szerint fogalmazódik meg [29]: az állam, mint a társadalom aktív szereplője – *végrehajtva és biztosítva közigazgatási funkcióit* – saját hatékonysága érdekében alkalmazza az informatikát; az állam, mint a demokrácia és az alkotmányos állampolgári jogok fenntartója igyekszik létrehozni az állampolgári és

¹⁶⁵ 1999-ben: állami többségi tulajdonban levő Antenna Hungária Rt.

¹⁶⁶ WDM: Wavelength Division Multiplex – hullámhosszosztásos multiplexálás

¹⁶⁷ az előterjesztés az optikai rendszer alkalmazásának elsődlegességét egyértelműen csak a mikrohullámú hálózattal szemben fennálló biztonsági kritériumok miatt indokolja hozzátéve, hogy a TETRA rendszerrel szemben támasztott magas szintű igények miatt szükséges a rádiós rendszer optikai támogatottsága is

¹⁶⁸ a TETRA rendszer kialakításának költségét 15-20 milliárd forintba, a végberendezések költségét (50 ezer fő felhasználóra vetítve) további 5-10 milliárd forintba becsüli az előterjesztő. A KODNET beruházás költségét 10 milliárd forintban kerül meghatározásra

¹⁶⁹ vezetékes kommunikáción értem itt a távbeszélő szolgáltatást, valamint minden olyan adatátviteli szolgáltatást, amelyek az informatikai rendszereket szolgálják ki

¹⁷⁰ mely koncepció a Miniszterelnöki Hivatal által 1999-ben kiadott *Magyar válasz az Információs Társadalom kihívásaira* c. tanulmányban jelenik meg. A tanulmány az állam információs társadalom megvalósításával kapcsolatos teendőinek kimunkálása céljából került elkészítésre

¹⁷¹ melyet megerősít azon tény, hogy a kormányzati koordináció felelőssévé a kormányfő helyettese, azaz a Miniszterelnöki Hivatal vezető miniszter került kijelölésre

regionális esélyegyenlőséget; az állam, mint a jövőt meghatározó információk birtokosa, és mint aki a stratégiai elemzésekre képes intézményrendszerrel rendelkezik irányítólag befolyásolja az információs társadalom kialakulásának feltételeit.

Ahhoz, hogy a közigazgatás elősegítse a jobb társadalmi integrációt, szolgáltatásaival, illetve az általa gyűjtött és prezentált adatokkal egyenlő esélyeket biztosítson az állampolgárok számára magának is változónak kell lennie, melyhez többek között: hatékonyan kell működnie, azaz szervezetében és eljárásaiban áttekinthetőnek kell lennie, gyorsabban és olcsóbban kell megbízható adatokat és szolgáltatásokat nyújtania; tevékenységét úgy kell végeznie, hogy nyilvános szolgáltatásai széles körben és univerzálisan hozzáférhetők legyenek, miközben biztosítja a megfelelő jogi biztonságot és garanciákat.

Fenti gondolatokból kiindulva a kormányzat stratégiai célként tűzte ki a papír nélküli, vagyis elektronikus közigazgatás megteremtését, mely kapcsán elérendő célként fogalmazódik meg a kormányzat és a közigazgatás információs munkájának digitális alapon történő megszervezése. Ennek keretében a közigazgatás szervei, valamint azok adatbázisai – *elsődlegesen az alapadatbázisok* – összekapcsolásra kerülnek. Az így kialakított integrált adatbázisokkal megoldhatóvá válik a kormányzati és a közigazgatási információk egymáshoz kötése. Az alapadatbázisok felhasználásával az állampolgár és a közigazgatási szervek közötti kapcsolat interaktívvá tehető, így oldva meg a modern, elektronikus ügyintézésrel kapcsolatos elvárásokat. Az elektronikus közigazgatás gyakorlati lehetőségének és továbbfejlesztésének megteremtése az Európai Unióhoz történő integráció egyik kulcskérdése is volt, mely kapcsán a kormányzat a XXI. század elején – *az e témakörben korábban megszerzett, valamint hazánk integrációs tapasztalatainak birtokában* – újabb stratégiai tervet dolgozott ki, melyet egyúttal alapul szánt a magyar információs társadalom – *általános, a fejlett államok stratégiai elképzeléseinek is megfelelő* – kialakítására.¹⁷² A Magyar Információs Társadalom Stratégia¹⁷³ megfogalmazza, hogy: „...[a MITS] a gazdaság és a társadalom európai fejlődéséhez történő felzárkózásának stratégiája. Céljaiban és megoldásaiban az európai értékrendet és cselekvési utakat követi, a magyar adottságok és lehetőségek figyelembe vételével. A MITS az ország felzárkózása kulcsának az információs és kommunikációs technológiák alkalmazásának kiterjesztését tekinti. E technológiák széleskörű alkalmazása, termelőerővé válása biztosíthatja a gazdaság modernizálását, a hatékonyság és versenyképesség növelését, és ezen keresztül egy új fejlettségi szint, az **információs társadalom** célkitűzéseinek megvalósítását. Információs társadalomról akkor beszélhetünk, amikor az információs ágazat társadalmi, gazdasági súlya dominánssá válik, az információ beépül az egyének, szervezetek és intézmények mindennapjaiba, és a társadalmi kommunikáció nagy része a digitális csatornákon zajlik. [...] Az elektronikus kormányzat radikálisan újszerű, sokkal hatékonyabb, felelősségteljesebb hatalomgyakorlási, illetve államigazgatási forma, amelynek középpontjában a „**szolgáltató állam**” koncepciója áll.” [30]. A MITS az e-kormányzat stratégia megvalósításának programjai során többek közt előíranyozza a kormányzati szervek csatlakozta-

¹⁷² a munka a Magyar Információs Társadalom Stratégia készítéséről, a további feladatok ütemezéséről és tárcaközi bizottság létrehozásáról szóló 1214/2002. (XII.28.) Korm. határozat alapján kezdődött meg

¹⁷³ rövidítve: MITS. Az anyag az IHM koordinációjában, a szaktárcák együttműködésével készült el. Közzététele a Magyar Információs Stratégia és annak végrehajtásáról szóló 1126/2003. (XII.12.) Korm. határozat alapján történt

tását az Elektronikus Kormányzati Gerinchez (EKG), a kormányzati elektronikus aláírás rendszer (PKI), valamint az egységes kormányzati címtár és levelező rendszer kialakítását. A rádiókommunikációs és a vezetékes kommunikáció kétutas további fejlődésének meghatározó állomása egyértelműen a **2001.** év volt, mivel ebben az évben jelentek meg az EKG, valamint az Egységes Digitális Rádiótávközlő Rendszer (EDR) kialakításával kapcsolatos kormányhatározatok.¹⁷⁴ Mindkét joganyag előterjesztését a 2000-ben újonnan alakult MeH Informatikai Kormánybiztosság¹⁷⁵ állította össze.

Az EKG kialakításával összefüggésben a **1122/2001. (XI.22.) Korm. határozat** intézkedik. A határozat kiadása egyértelművé tette, hogy a kormányzat szakított az EKZH, a KTR, és a KODNET koncepciók kidolgozása során addig alkalmazott, eredményességét tekintve sikertelen koordinációs eljárásokkal, vagyis erős központi akarat és finansziális erőforrások felhasználása útján rendelkezett egy országos nagysebességű hálózattal megvalósítására. A rendszer elsődleges feladatául a kormányzati és közigazgatási adatbázisok és informatikai rendszerek összekapcsolása került meghatározásra, mellyel elősegíthető az elektronikus kormányzat kialakítása. A hálózat annak a kritériumnak is megfelel, hogy legyen meghatározó infrastrukturális eleme a kormányzati informatikának. Az EKG kiépítésével cél volt mind a budapesti, mind a vidéki közigazgatási szervek közötti nagysebességű kapcsolatok megvalósítása. A hírközléspolitikában rögzítettek szellemében, a szolgáltatók versenyeztetése útján került mind a fővárosi, mind az országos optikai gerinchálózat kialakításra bérelt viszonylatok felhasználása¹⁷⁶ révén. A központi üzemeltetési szervezet szintén nem közigazgatási szerv. A teljes kialakítása 2001-2002-ben volt esedékes. A kormányhatározatban megfogalmazottaknak megfelelően a 227/2001. (XI.30.) Korm. rendelet 1. §-a módosította az 50/1998. (III.27.) Korm. rendeletet és előírta, hogy a BM, HM, KVM,¹⁷⁷ OM¹⁷⁸ és a MeH¹⁷⁹ által működtetett zártcélú hálózatokon kívül a központi

¹⁷⁴ az egységes digitális rádió-távközlő rendszer (EDR) kialakításáról szóló 1074/2001. (VII.13.) Korm. határozat, ennek módosításáról szóló 1100/2001. (VIII.27.) Korm. határozat, valamint az Elektronikus Kormányzati Gerinchálózat kialakításáról szóló 1122/2001. (XI.22.) Korm. határozat

¹⁷⁵ az Informatikai Kormánybiztosság (IKB) lényegében Katona Kálmán közlekedési, hírközlési és vízügyi miniszter 57/2000. (V.24.) KE határozat alapján megvalósított felmentését követően, az egyes miniszterek feladat- és hatáskörének változásával összefüggésben szükséges törvény-módosításokról szóló 2000. évi LXXXIX. törvény, valamint az információs társadalom megvalósításával összefüggő feladatokról, az informatikai kormánybiztos feladat- és hatásköréről szóló 100/2000. (VI.23.) Korm. rendeletben fogalmazottak szerint szerveződött meg. Az IKB fő céljaként fogalmazta meg az információs társadalom hazai kialakulásának elősegítését, valamint ezzel összhangban az elektronikus kormányzat és az elektronikus közigazgatás létrejöttéhez szükséges feltételek megteremtését. Az IKB kialakításával egyidőben a KHVM-et Közlekedési és Vízügyi Minisztériummá szervezték át úgy, hogy a hírközléssel kapcsolatos feladatok a Miniszterelnöki Hivatal (IKB) hatáskörébe kerültek. Az informatikai kormánybiztos kinevezéséről szóló 1045/2003. (V.31.) Korm. határozat alapján Sík Zoltán lett kormánybiztos, aki beosztását az informatikai kormánybiztos felmentéséről szóló 1097/2002. (VI.10.) Korm. határozat alapján, menesztéséig (2002. május 31.) töltött be. Ezt követően az IKB felszámolásra került

¹⁷⁶ az EKG-val kapcsolatos előterjesztés alapján a kialakítás költségei 2001-ben 765 millió forint és 2002-ben 695 millió forint, melyet követően az éves fenntartási költség 750 millió forintban került meghatározásra

¹⁷⁷ a Közlekedési és Vízügyi Minisztérium által működtetett EDR

¹⁷⁸ a Nemzeti Információs Infrastruktúra Fejlesztéséről (NIIF) szóló 95/1999. (VI. 23.) Korm. rendelet alapján az Oktatási Minisztérium részéről felügyelt NIIF által üzemeltetett SULINET program. Ezt a szervezési elvet módosította a 212/2003. (XII.10.) Korm. rendelet, mely alapján a felügyelet az IHM hatáskörébe került

közigazgatás budapesti és területi szervei kötelesek csatlakozni az EKG-hoz úgy, hogy az egyes minisztériumok által működtetett zártcélú távközlő hálózatoknak az EKG-val kiváltható gerincszakaszai és csomópontjai megszűnnek és az összekapcsolást követően ezek a zártcélú hálózatok egymással együttműködnek. Az újonnan kialakítandó hálózatok esetében a gerinchálózati összeköttetések csak az EKG-n keresztül valósulnak meg. A zártcélú hálózatokról szóló kormányrendelet módosításával némileg feloldásra került a hírközléspolitikai és a rendelet között az önálló rendszerek fejlesztése és fenntartása terén kialakított mesterséges ellentmondás, hiszen határozottan megfogalmazódik az EKG-hoz való csatlakozási, illetve az egymással való együttműködési kötelezettség. A probléma ettől függetlenül továbbra is fennáll, hiszen a legnagyobb kiterjedésű és ennél fogva a legköltségesebb hálózatok csatlakozási és szorosabb együttműködési kényszere továbbra sem előírás, melyhez csatlakozik az újonnan kialakításra tervezett, országos kiterjedésű EDR is. 2001-et követően az EKG-val kapcsolatosan az értekezés által vizsgált időpontig összesen két jogi norma jelent meg. Az Elektronikus Kormányzati Gerinchálózatról és az Informatikai Közhálóról szóló **1188/2002. (XI.7.) Korm. határozat** hatályon kívül helyezte a 1122/2001. (XI.22.) Korm. határozatot. A határozat megfogalmazta, hogy az EKG-ba be nem vont, a kormányzati informatikába nem tartozó helyi közigazgatási szervek, közintézmények, közfeladatot ellátó egyéb szervek, civil szervezetek informatikai ellátásának biztosítása érdekében ki kell alakítani az Informatikai Közhálót (Közháló), melynek felügyeleti szerveként az IHM került nevesítésre.

Miután a korábbi kormányhatározatban rögzített határidőre az EKG tervezett kialakítása (és működési szabályzatának kidolgozása) nem fejeződött be, így a normatíva új határidőt rögzít¹⁷⁹ és meghatározza, hogy a csatlakozó szervek kötelesek költségmegosztást alkalmazni. Ez érvényes mind az EKG, mind a Közháló használata tekintetében. Az EKG használati szabályzatának kiadása az **5/2004. (I.9.) Korm. rendelet** kihirdetésével valósul meg. Az új kormányhatározat megoldást talált az üzemeltető szervezettel kapcsolatosan felvetett problematikákra is, mely egyrésztől gazdasági, másrésztől biztonsági jellegűek voltak.¹⁸¹

A kormányzati kommunikációval kapcsolatos kétutas fejlődés másik ágát a trónkölt rádiórendszer hazai kialakításával kapcsolatos törekvések jelentik. A rendszer bevezetésével kapcsolatos szakmai felmérések és viták, illetve az ennek alapján meghozott politikai döntések összességében hosszabb időt vettek igénybe,¹⁸² mint az EKZH, KTR, KODNET koncepciók eredményeképpen megszülető konszenzus, mely az EKG kialakulásához vezethetett. Függetlenül attól, hogy az EDR kialakításával kapcsolatos szabályozási környezet 2004-ben már rendelkezésre állt, csak az értekezés által vizsgált időszak végére született meg a Gazdasági Kabinet¹⁸³ tényleges megvaló-

¹⁷⁹ az IKB hatáskörébe került K-600-as rendszer

¹⁸⁰ a teljes működésre 2003. június 30.

¹⁸¹ a társasággal korábban megkötött üzemeltetői szerződés 2002 végén járt volna le, így a további működtetés vált egyértelműen kérdésessé. A biztonsági kockázatok csökkentése érdekében a társaság állami tulajdonba vételére tett javaslatok kerültek elfogadásra, mely a részvények visszavásárlásán és tőkeemelésen keresztül vezetett út. Az EU támogatási szabályai szerint akkor lehet egy céget állami tulajdonúnak tekinteni, amennyiben az állam tulajdonosi részaránya meghaladja a 90 %-ot

¹⁸² hiszen az EKZH koncepció megszületésével egyidőben jelenik meg

¹⁸³ Gazdasági Kabinet: a Kormány kabinetjéről szóló 1107/2002. (VI.18.) Korm. határozat 2. pontja rögzíti, hogy A Kormány a gazdaságot érintő koncepcionális kérdések véleményezésére, illetőleg gazdaság-

sulást konkrétan elősegítő pénzügyi döntése. A rendszer kiépítésével kapcsolatosan első ízben az egységes digitális rádiótávközlő rendszer (EDR) kialakításáról szóló **1074/2001. (VII.13.) Korm. határozat** jelenik meg, melyet igen rövid időn belül módosít a **1100/2001. (VIII.27.) Korm. határozat**.¹⁸⁴ A vizsgált időszakban hatályos az egységes digitális rádiótávközlő rendszer (EDR) kialakításáról szóló **1158/2002. (IX.26.) Korm. határozat**, valamint az ugyancsak a digitális rádiótávközlő hálózat (EDR) kialakításáról szóló **1031/2003. (IV.9.) Korm. határozat**. A 2001-ben megalkotott kormányhatározatok alapján döntés született arról, hogy az országos rendszer kiépítése szolgáltató szervezetek bevonásával, szolgáltatásvásárlás útján fog megvalósulni. A kiépítéssel kapcsolatos kormányzati és szakértői koordinációt a MeH IKB vezette, szolgáltatóként a 2001 végén újonnan a Magyar Posta Rt.¹⁸⁵ szervezetében létrehozott TETRA Távközlési Szolgáltató Rt. került kijelölésre. Az EDR kialakítása kapcsán döntés született a rendészeti és közigazgatási szervek igényeit kiszolgáló analóg rádiórendszerek fejlesztési és bővítési tilalmáról¹⁸⁶ is, melyet megelőzően¹⁸⁷ a Kormányzati Frekvenciagazdálkodási Hivatal a 380-400 MHz frekvenciatartományban korábban meglevő, minden más felhasználást megszüntetett.

A rendszer kialakítása körül elhúzódó döntések, illetve a megváltozó kormányzati struktúra és elgondolás vezetett oda, hogy 2002-ben újabb szakértői konzultációk indultak meg a MeH Kormányzati Informatikai és Társadalmi Kapcsolatok Hivatal koordinációjában, egyúttal számolva fel a TETRA Távközlési Szolgáltató Rt.-t 2002 végén. A 2003-ban megjelent kormányhatározat ismételten deklarálta a megvalósítás szolgáltatásvásárlással történő végrehajtását, egyúttal a koordinációs és szakfeladatok ellátása miniszteri biztosi felügyelet mellett az IHM feladatkörébe került. A trónkölt rádiórendszer kapcsán 2004-re kialakult kormányzati döntések áttekintését követően megállapítható, hogy az EDR várható működtetési szisztémája nagy hasonlóságot mutat az EKG jelenlegi gyakorlatával. Mindkét esetben a rendszer technikai kivitelezésébe nagy gyakorlattal rendelkező távközlési és informatikai szolgáltatók kerülnek bevonásra, melyet követően az állami tulajdonban levő üzemeltető szervezet átveszi az üzemviteli feladatokat szerződést kötve a szolgáltatást igénybevevő kormányzati és közigazgatási szervekkel. A rendszer felügyeletét a hálózatgazdák látják el.

Összességében véve, a vizsgált időszakban a jogszabályi környezet módosulása a kormányzati, katonai, rendészeti és közigazgatási, valamint a hírközlési ágazat nem kormányzati szervezeti struktúráit jelentősen átalakította. A lezajló folyamatokkal párhuzamosan megindult a

politikai döntéseinek elkészítésére Gazdasági Kabinetet létesít. Ennek vezetője a pénzügyminiszter, tagjai az egészségügyi, szociális és családügyi miniszter, az európai integrációs ügyek koordinációjáért felelős tárca nélküli miniszter, a foglalkoztatáspolitikai és munkaügyi miniszter, a földművelésügyi és vidékfejlesztési miniszter, a gazdasági és közlekedési miniszter, az informatikai és hírközlési miniszter, a környezetvédelmi és vízügyi miniszter. Állandó meghívott a Magyar Nemzeti Bank elnöke, a miniszterelnök kabinetfőnöke, a Külügyminisztérium Integrációs és Külgazdasági Államtitkársága külgazdasági kérdésekért felelős helyettes vezetője

¹⁸⁴ a módosított 1074/2001. (VII.13.) Korm. határozatot az egységes digitális rádiótávközlő rendszer (EDR) kialakításáról szóló 1158/2002. (IX.26.) Korm. határozat 8. pontja helyezi hatályon kívül, míg az 1100/2001. (VIII.27.) Korm. határozat az egyes kormányhatározatok hatályon kívül helyezéséről szóló 1015/2004. (III.3.) Korm. határozat melléklete alapján kerül hatálytalanításra

¹⁸⁵ a Magyar Posta Rt. a mai napig az állam kizárólagos tulajdonában van. Felügyeletét a KHVM át-szervezését a KVM látta el, ezért hálózatgazdaként is a minisztérium került kijelölésre, mely tény rögzítésre a 227/2001. (XI.30.) Korm. rendelet 1. § útján rögzítésre került az 50/1998. (III.27.) Korm. rendeletben is

¹⁸⁶ mely intézkedés az értekezés által vizsgált időszak végén még fennállt

¹⁸⁷ 1998. január 1-jei hatállyal

kommunikációs rendszereket üzemeltető szervezetek átszerveződése és a szolgáltatási igények bővülését követő technológiai modernizáció. A zártcélú kommunikációs rendszerek jogszabályi alapjai gyakorlatilag 1998-ra megalkotásra kerültek, mellyel párhuzamosan törekvések történtek az egységes kormányzati kommunikációs rendszerek gyakorlati kialakítására is. Ez időszakban az egységes kormányzati kommunikációs rendszerekkel kapcsolatosan többfajta koncepció került kialakításra. Nézőpontom szerint az elképzelések folyamatos módosulása alapvetően három fő okra vezethető vissza: a konvergencia jelenségéből adódó technológiai fejlesztési kényszer, a zártcélú hálózatokkal kapcsolatos jogszabályok és kormányzati koncepciók között rejlő ellentmondások, az ország szövetségi rendszerekhez való csatlakozásából eredő jogszabályi, szervezési és gazdasági jellegű változtatási kényszer. Elmondható azonban, hogy 2004-re hazánkban kialakult egy olyan gazdasági, jogszabályi és szakmai környezet, mely megfelelő alapját képezheti a kormányzati távközlést kiszolgáló önálló kommunikációs rendszer tényleges kialakításának.

2.2. Összegzés, következtetések

Kétségtelen tény, hogy az elmúlt 15 esztendő folyamán a kormányzati távközlés szempontjából is igen jelentős változások mentek végbe hazánkban. A kommunikációs technológia tekintetében lezajló fejlődés, valamint a jogszabályi környezet átalakítása igen széles, változatos lehetőséget nyitott meg és kínál mind a mai napig az önálló kormányzati kommunikációs rendszer kialakítására. Magyarország gazdasági szerkezetátalakítása megszüntette az állami tulajdon túlsúlyát, a kialakuló piacgazdaság¹⁸⁸ egyértelműen elősegítette a korszerű távközlési és informatikai technológia hazai elterjedését, mellyel kapcsolatos információk addigi megismerésére a COCOM-bizottság működése miatt nem volt lehetőség. A technikai eszközök és rendszerek fejlődésével a kommunikációs szolgáltatásfajták palettája is szélesebbé vált, így az addig legfőbb távbeszélő szolgáltatás elvesztette kizárólagos vezető szerepét.¹⁸⁹ A gazdasági és politikai viszonyok átalakulása erőteljesen kihatott mind a gazdálkodás, mind a közigazgatás szervezeti felépítésére és működési rendjére, így a kormányzati távközlés technikai megvalósulásában korábban részt vevő szervek összetétele és állami felügyeleti viszonyai is jelentősen megváltoztak. A technikai, gazdasági és szervezeti struktúrák folyamatos módosulásának természetes katalizátora a jogszabályi környezet, mely a vizsgált időszakban szintén permanensen változik.

A **konvergencia** hatása a kormányzati távközlést és annak megvalósítási formáját is érinti, hiszen olyan intelligens (és globális) kommunikációs rendszerek szerveződnek környezetünkben, amelyek magukba foglalják az informatikára és a távközlésre épülő **adatkommunikáció** mindazon termékeit és szolgáltatásait, amelyek elsősorban a személyek és szervezetek közötti kapcsolattartás és együttműködés, valamint az információkhoz való távoli és gyors hozzáférés lehetőségét teremtik meg. A kommunikációs (multimédia) szolgáltatások ilyen mértékű, hazánkban is jelentkező megváltozása és elterjedése a kormányzatot már a kilencvenes évek elején arra ösztönözte, hogy a szolgáltató típusú közigazgatási modell, illetve hosszútávon az elektronikus kormányzás kialakítása érdekében jogszabályi úton segítse elő ezen újfajta lehetőségek a munkafolyamatokba való beépülését. Ehhez természetesen hozzátartozik, hogy egyes szolgáltatások felhasználási kultúrájának közigazgatásban történő meghonoso-

¹⁸⁸ a Magyar Köztársaság Alkotmányáról szóló 1949. évi XX. törvény 9. § (1) bek. alapján került deklarálásra, hogy Magyarország gazdasága piacgazdaság. Ezt a bekezdést a Magyar Köztársaság Alkotmányának módosításáról szóló 1990. évi XL. törvény 4. § állapította meg

¹⁸⁹ amely azt jelenti, hogy a beszéd célú távbeszélő felhasználás 2004-ben is a legtöbbször igényelt szolgáltatás

dását a gazdasági élet szereplői indirekt úton kényszerítették ki a mindennapi együttműködés fenntarthatósága¹⁹⁰ érdekében. A távközlő és informatikai rendszerek hordozó és távszolgálati funkcióinak összemosódása a rendszerek közötti további együttműködést fogja erősíteni, mely azonban az eddig elkülönülő szervezetek egyre magasabb fokú integrációjához fog vezetni. A tárolókapacitások növekedésével várhatóan újabb multimédia alkalmazások megjelenésére is számítani kell, aminek következménye, hogy a gyakorlati felhasználáshoz elengedhetetlen az átviteli lehetőségek további kvalitatív és kvantitatív bővítése. Fentiek alapján rögzíthető, hogy a kormányzati távközlésben – *technológiai szempontból* – a jövőben egyre inkább fajsúlyossá válik a multimédia típusú szolgáltatások nyújtására való képesség, mely azonban feltételezi a további átviteli kapacitásbővítéseket. A megvalósulás szervezeti háttere tekintetében várhatóan egyre magasabb fokú integrációval kell számolni.

A kormányzati távközlés megvalósítása releváns szereplőinek köre és viszonyrendszere a **jogszabályi környezet** módosulásával jelentősen átalakult. Magyarország kommunikációs infrastruktúrájának meghatározó része került magántulajdonba a gazdasági és hírközlési ágazattal kapcsolatosan megalkotott törvények és egyéb jogszabályok útján, hiszen átalakult az a szemlélet is mely korábban a katonai és belbiztonsági érdekek miatt nem engedte az állami tulajdon jog meghatározó szerepét e területen megváltoztatni. A piaci viszonyok megteremtése mellett azonban az állam kezelésében továbbra is fennmaradtak különböző kommunikációs rendszerek alapvetően azért, mert a kilencvenes évek elején ezek magas műszaki színvonalat képviseltek, jó alapot képezve a további fejlesztésekhez, melyet a nem kellőképpen szabályozott piaci viszonyok miatt kialakult kedvezőtlen működtetési feltételek megváltoztatása is generált. A rendszerek fennmaradásukat gyakorlatilag minden, a hírközléssel kapcsolatos jogi szabályozás megerősített, azonban a technológiai fejlődés hatására egyes rendszerek megszűntek, mások továbbfejlődtek, illetve újak létesültek.

A kormányzati távközlést érintő fejlesztési törekvések gyakorlatilag már a '90-es évek elején, de az informatikai szakterülettel még párhuzamos szálon indultak meg. A koncepciók és a jogszabályban rögzítettek elemzése alapján egyértelműen kijelenthető, hogy 1998-ig a fejlesztések kiindulópontját a Belügyminisztérium és Honvédelmi Minisztérium távközlési infrastruktúrája¹⁹¹ és szolgáltatásnyújtási képessége jelentette, így mind az EKZH, mind a KTR koncepciók a meglévő távbeszélő hálózatra alapozva fogalmazták meg elképzeléseiket. E megállapításhoz szorosan hozzátartozik, hogy a fenntartás és üzemeltetés ellenőrzése és végrehajtása – *hasonlóan az előző időszak koncepcionális elképzeléseire* – az állam gazdasági és humán erőforrásaira támaszkodott történet volna meg. 1998-tól kezdődően teljes mértékű szemléletváltás figyelhető meg, melyet alapvetően befolyásolt a korábbi sikertelenség, a konvergencia technológiára és kommunikációs szolgáltatásokra való hatása, az üzemeltetéssel összefüggő biztonsági koncepciók megváltozása, valamint a szolgáltató állammal és elektronikus kormányzással kapcsolatos elképzelések folyamatos erősödése. A vizsgált időszak végére határozott központi akarral az informatikai rendszerek alkalmazása elősegíté-

¹⁹⁰ ennek igazolására a legszembevetőbb példa, hogy a közcélú távbeszélő technika és kapcsolódó átviteltechnikai rendszerek digitalizálása a zárteélú távközlő hálózatokkal rendelkező szervezetek is rákényszerítette a modernizálásra, hiszen a közcélú szolgáltatások igénybevétele a rendszerek együttműködési képességének hiányában hosszútávon bizonyosan ellehetetlenül volna

¹⁹¹ a honvédelmi és belügyi tárca korábbi rendszerei, illetve a kormányhíradó rendszerek

se szemszögéből kiindulva kialakításra került az Egységes Kormányzati Gerinchálózat, mely rendszerrel összefüggésben elmondható, hogy 2004-re a kormányzati kommunikáció egyik meghatározó szegmenseként jeleníthető meg. Igaz, hogy fő szolgáltatásai elsősorban az adatkommunikáció megvalósulását segítik elő, azonban a szakterületek közti határ elmosódásával megindult a rendszer beszédcélú kommunikációs szolgáltatásokra való felkészítése. Kijelenthető, hogy a kormányzati távközlés gyakorlati megvalósulásában résztvevők a rendszert továbbra is sokszereplőssé teszik, némileg ez a kör bővebbnek mutatkozik, mint az 1967-1989 közötti időszakban, melynek egyik indoka, hogy a jogalkotási folyamat során a megállapított stratégia és a gyakorlati megvalósítás között ellentétek alakultak ki, nevezetesen a zártcélú hálózatgazdák körének meghatározásakor. Ennek ellensúlyozására lépések történtek, azonban az ábrát áttekintve a következő megállapítások tehetők: létrejött a Miniszterelnöki Hivatal felügyeletében működő EKG, mely a közigazgatás központi és meghatározott körű területi szerveinek **adatkommunikációs** igényeit szolgálja ki; a Honvédelmi Minisztérium (HM) felügyeletében létezik, a HM és a Magyar Honvédelem szervei által fenntartott katonai kommunikációs rendszer, amely elsősorban a honvédelmi ágazat **beszéd- és adatkommunikációs** igényeit elégíti ki. A rendszer gyakorlatilag továbbra is csak a távbeszélő célokat szolgáló kapcsolóközpontok szintjén csatlakozik az egyéb – *elsősorban* – rendészeti kommunikációs rendszerekkel; a Belügyminisztérium (BM) felügyeletében funkcionál a BM szervei által működtetett rendészeti kommunikációs rendszer. Lényegében véve a katonai kommunikációs rendszerrel kapcsolatosan tett megállapítások e rendszerre ugyanúgy érvényesek; az ágazati miniszterek, illetve a Legfőbb Ügyész felügyeletében az irányított szervek üzemeltetési körében kommunikációs rendszerek működnek, elsősorban az adott államigazgatási szerv **adatkommunikációs** igényeit elégítve ki; az Informatikai és Hírközlési Minisztérium (IHM) felügyeletében kialakítás alatt áll a kormányzati célokat szolgáló EDR rádiókommunikációs rendszer. Ugyancsak létesítési fázisban van az Informatikai Közháló, mely a közigazgatás és az önkormányzatok alsófokú szervezetei **adatkommunikációs** lehetőségét kívánja megteremteni; az IHM felügyeletében és a Magyar Távközlési Rt. üzemeltetési körében működik a K-600-as hálózat, mely a minősített időszakos kommunikációs igények kielégítésében vállal szerepet. A „K” vezetési rendszer jelentőségéből folyamatosan vesztett a vizsgált időszak során. Látható, hogy a résztvevők köre jelentősen bővült, azonban az is, hogy a konvergencia hatására a beszédcélú igények kiszolgálása helyett az adatforgalom irányába terelődött a hangsúly. A további bővülés elkerülése érdekében került meghatározásra, hogy a kormányzati kommunikációban a 4. pontban meghatározottak köre csak az EDR-t felhasználva, azzal együttműködve vehet részt. Az ábrán nem került feltüntetésre, de mindenképpen meg kell említeni, hogy a közcélú távközlési és informatikai szolgáltatók jelentős mértékben járulnak hozzá a kormányzat és a közigazgatás szervezeti egységei kommunikációjához az általuk nyújtott szolgáltatások útján.¹⁹²

A fejezetben leírtakat mérlegelve azt a következtetést vonom le, hogy a kormányzati távközlés elkülönülő rendszerek útján történő biztosításának igénye az 1990-2004 közötti időszakban továbbra is fennmaradt. A gazdaság szerkezetátalakítása folytán hazánk kommunikációs infrastruktúrájának jelentős része magánosításra került, mely

¹⁹² itt elsősorban a helyhez kötött és mobil távbeszélő, valamint az Internet hozzáférést célzó szolgáltatásokra gondolok, melyhez kapcsolódik az infrastruktúra bérlete is

azt eredményezte, hogy a kormányzati távközléssel összefüggő érdekek érvényesítése a kialakuló piaci viszonyok miatt háttérbe szorult, melyet nem kompenzált az állami kézben maradt infrastruktúra jogszabályok útján garantált függetlensége sem. Az újonnan kialakított jogszabályi alapok lehetőséget teremtettek az önálló, ágazati érdekeket figyelembe vevő fejlesztések megindítására, melyek elsősorban a kedvezőtlen piaci viszonyok kompenzálására irányultak, azonban a kormányzat kezdetben gyenge koordinációs tevékenységet folytatott a központi érdekek érvényesítése terén. 2004-re a kormányzati távközlés megvalósításában részt vevő rendszerek technológiai alapjai megváltoztak, illetve jelentősen módosultak, a működtetést végző szervezetek átalakultak. Ennek ellenére a sokszereplős megoldás nem változott, de törekvések történtek az érintett kör szűkítésére. A kormányzati távközlésben résztvevők törvényességi szempontból történő felügyeletét a hírközlési ágazat hatósági szervei látják el, azonban a kormányzati törekvések koncepcionális megjelenítését a Miniszterelnöki Hivatal látja el. Az ágazati érdekek alapján történő fejlesztések letörése és a centralizáció irányába történő elmozdulás 2001-ben, a Miniszterelnöki Hivatal által kialakított EKG bevezetésével indult meg, mely folyamat a vizsgált időszak végéig nem fejeződött be.

Mindezek alapján kimondható, hogy hazánkban 1990-2004 között a kormányzati távközlést továbbra sem szolgálta ki önálló kommunikációs rendszer. Az igényeket különböző államigazgatási, illetve állami szervezetek kommunikációs rendszerei, valamint a liberalizálódó hírközlési piac szereplői elégítik ki, az állam felügyeleti és koordinációs tevékenysége mellett.

Hivatkozások

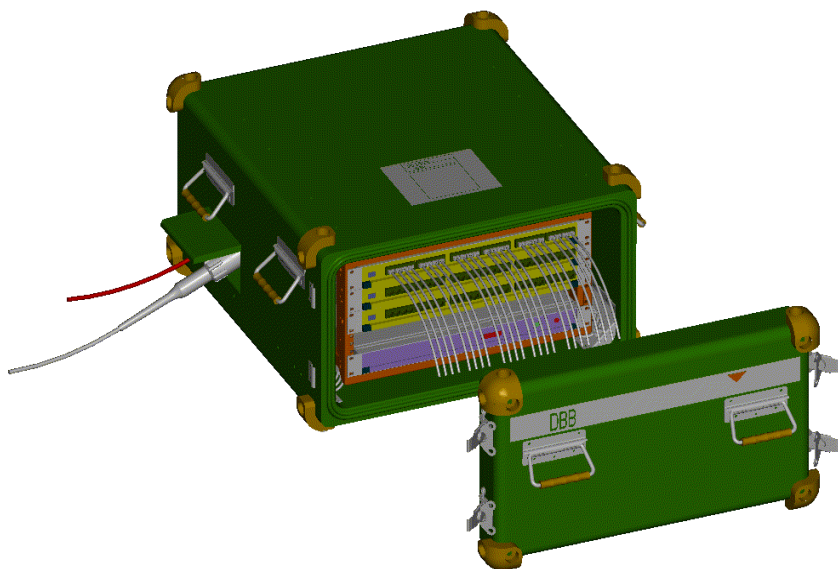
- [1] Kennedy, Paul: A huszonegyedik század küszöbén, Napvilág Kiadó, Budapest, ISBN 963 9082 09 0, 238. oldal, 1997.
- [2] Wiener György: Hatalmi viszonyok és kormányzati struktúra a rendszerváltás időszakában és a '90-es évek első felében (1988-1994), Politikatudományi füzetek XVIII., MTA Politikatudományok Intézete, Budapest, ISSN 1417-3514, 6-13. oldal, 1997.
- [3] Magyar Közlöny
- [4] A hírközlés szabályozása és felügyelete Magyarországon – kék könyv, Hírközlési Főfelügyelet Nemzetközi Igazgatóság (nyilvános anyag), 7. oldal, 1999., <http://www.hif.hu>
- [5] Dr. Török Gábor: Az új hírközlési törvény néhány polgárjogi problémája, Az információs társadalom és a jog átalakulása – Magyarország az ezredfordulón, Stratégiai kutatások a Magyar Tudományos Akadémián, Műhelytanulmányok, Magyar Tudományos Akadémia, Budapest, ISBN 963 508 377 7, 210. oldal, 2002.
- [6] Magyar Közlöny
- [7] Dr. Sallai Gyula – Vácziné Dr. Takács Zita – Aranyosné Dr. Börcs Janka (szerk.): A távközlés és információtechnológia jogi szabályozása – kiegészítő kötet, Hírközlési Főfelügyelet, Budapest, ISBN 963 00 4343 2, 121. oldal, 2000.
- [8] Magyar Közlöny
- [9] Hírközlési Felügyelet elnöke, Beszámoló a Kormány részére a Hírközlési Felügyelet 2002. évi tevékenységéről, gazdálkodásáról és a hírközlési piac helyzetéről, BM Távközlési Szolgálat irattár, Budapest, Iktatási szám: LN-2291/2003., 3. oldal, 2003. április 02.
- [10] Magyar Közlöny
- [11] Hírközlési Felügyelet elnöke, Beszámoló a Kormány részére a Hírközlési Felügyelet 2002. évi tevékenységéről, gazdálkodásáról és a hírközlési piac helyzetéről, BM Távközlési Szolgálat irattár, Budapest, Iktatási szám: LN-2291/2003., 15. oldal, 2003. április 02.

-
- [12] Dr. Martin B. H. Weiss: Távközlési technológiák, UNESCO Információs világlejentes 1997-1998, Magyar UNESCO Bizottság, Országos Rádió és Televízió Testület, HÉA Stratégiakutató Intézet, Budapest, ISBN 963 8493 27 5, 186. oldal, 1998.
- [13] Magyar Közlöny
- [14] Dr. Somogyi András: Az aszimmetrikus szabályozás módosulása, „Az Európai Unió távközlés-szabályozásának reformja – feladataink és lehetőségeink” konferencia és vita-fórum, Hírközlési és Informatikai Tudományos Egyesület, Budapest, 82. oldal, 2003.
- [15] Végh Ferenc: A Magyar Honvédség a felkészüléstől a teljes interoperabilitásig, A NATO-tag Magyarország, Külügyminisztérium, Budapest, ISBN 963 7038 11 6, 40-41. oldal, 1999.
- [16] 3557/1992. (XI.24.) Korm. határozat, BM Irattár, Budapest, Iktatási szám: 00758, 1992.
- [17] Dr. Pintér Sándor: A magyar rendőrség átvilágításának fő tapasztalatai, azok hasznosításának lehetőségei a rendőrség korszerűsítésében, A magyar rendőrség és a határőrség a közvéleményben és a valóságban, A Belügyminisztérium és a Hanns-Seidel Alapítvány konferenciája, Hanns-Seidel Alapítvány – Batthyány Lajos Alapítvány – HM – BM, Budapest, ISBN 963 7703 80 2, 16. oldal, 1993. február 23.
- [18] Belügyminiszter, Előterjesztés a Kormány részére a nemzetközi titkosított kormányzati távbeszélő és távgépíró összeköttetések helyzetéről, a további működtetés lehetőségeiről, BM irattár, Budapest, Iktatási szám: 6-1/29/1994., 1994. november 30.
- [19] Dr. Torma András: A területi államigazgatás informatikai helyzete, Magyar Közigazgatás XLVIII. évf. 12. szám, Budapest, ISSN 0865 736 X, 724. oldal, 1998.
- [20] ORFK GIF Híradástechnikai Szolgálat igazgatója, Jelentés a „KT”, „KV” rendszer megszüntetéséről, BM Távközlési Szolgálat irattár, Budapest, Iktatási szám: 48-00186/1994., 1994. december 12.
- [21] Miniszterelnöki Hivatal, Felhívás EKZH megvalósításhoz, BM Távközlési Szolgálat irattár, Budapest, Iktatási szám: 2212-5/1995. ált., 1995.
- [22] BM Híradástechnikai és Frekvenciagazdálkodási Osztály, MeH államtitkár – KHVM miniszter, A kormányzati távközlési hálózat (KTH) megvalósításának feladatairól szóló kormány előterjesztés-tervezet véleményezésére való felkérés, BM Távközlési Szolgálat irattár, Budapest, Iktatási szám: 90-131/1/1996., illetve 2284-2/1996. ált., 3. oldal, 1996. november 14.,
- [23] Magyar Közlöny
- [24] Magyar Közlöny
- [25] Magyar Közlöny
- [26] Nagy, Lajos – Pándi, Erik: Hungary samples TETRA communications system, Fire International, DMG, Eastbourne, England, ISSN 0015-2609, pp 21., No. 171., 1999.
- [27] Pándi Erik – Szűcs Péter: Az államigazgatási igényeket kiszolgáló távközlő hálózatok fejlesztési iránya, Bolyai Szemle, Bolyai Szemle, IX. évf. 2. szám, Budapest, ISSN 1416-1443, 131-135. oldal, 2000.
- [28] MeH miniszter, Az egységes TETRA rádióforgalmi és az egységes kormányzati adatátviteli optikai hálózat (KODNET) kialakításáról szóló kormány előterjesztés, BM Távközlési Szolgálat irattár, Budapest, Iktatási szám: 9003-8/1999. ált. 1999. szeptember 22.
- [29] Magyar Válasz az Információs Társadalom kihívásaira (nyilvános anyag), Miniszterelnöki Hivatal, 5. fejezet: Szolgáltató Állam-, és Közigazgatás (Polgár-barát ügyintézés), 1999., http://www.iif.hu/~lengyel/valasz/valasz_3-5.htm
- [30] Magyar Információs Társadalom Stratégia, Informatikai és Hírközlési Minisztérium, 2003., [http://www.ihm.hu/MITSmagyarPDF\[1\].pdf](http://www.ihm.hu/MITSmagyarPDF[1].pdf)



A jövőbeni rendszerek növekvő mobilitási igényét kiszolgáló hálózati megoldás a DNARS (Dynamic Network Addressing Resolution Scheme). A

DNARS teszi lehetővé, hogy bármely felhasználó, bármelyik (LAN vagy WAN) csatlakozási ponthoz kapcsolódva az automatikus konfigurálással időt és ráfordításokat takaríthat meg.



Alcatel Hungary Kft.

1116 Budapest, [Kondorfa u. 10.](#)

Telefon: (1) 2099500 Telefax: (1) 2099599

www.alcatel.hu
alcatelh@alcatel.hu

DELIVERING NETWORK ENABLED DEFENSE CAPABILITIES



Defense must address the challenge of the new Information technologies

> In place of the giant NCW* US DoD objective, each MoD needs a realistic defense **Transformation program** that:

- Optimize available budget resources
- Maintain coalition capabilities by selection of relevant standards and architectures
- Deliver greater networking and more advanced services (cooperative tools, ...)
- Addresses the new Security issues (OS, multilevel, ...)
- Emphasize knowledge management

* Network Centric Warfare

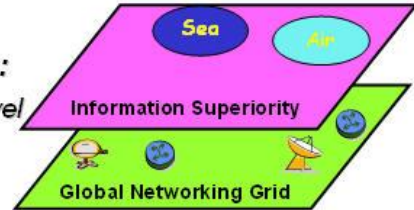
Alcatel approach for Defense Communications

> **Global Networking Grid is the foundation layer:**

- *Ubiquity of access and multiservices/multiprotocol for global connectivity*
- *Maximised Broadband & Flexibility & Resilience by leveraging space*
- *Interoperability with combat communications via IP and gateways for extension to strategic areas*

> **Information Superiority with:**

- *Enterprise services at agency level*
- *Knowledge management tools*
- *Interoperability of functional IS*



— 3

All rights reserved © 2004, Alcatel

ALCATEL

Alcatel Contribution

- > Broad Network competency (world-leader in optical and Multi Protocol/Multi Service switches, N°3 in GSM/UMTS, ...)
- > World leader in broadband and carrier-grade products (non-stop routing)
- > Voice/Data (converged) over IP and NGN solutions catering dynamic addressing (mobility) and assured services
- > Full turnkey solutions with proven defense experience for complex projects integrating technologies, services, middleware, ... (prime for 1 billion € Syracuse III program, ...)
- > Unique mix of space and telecom expertise (N°1 European in space)



— 4

All rights reserved © 2004, Alcatel

ALCATEL

Current defense projects engaged by Alcatel

- > **Hi-speed backbone** (optical, SDH micro-waves)
 - Increase reliability and bandwidth, cut operation/maintenance charges
 - Trends: greater use of private transmission (versus carrier LL)
- > **Outsourcing services** (PPP, PFI, ...)
 - Is one solution to solve the « project complexity-budget constraint-human resource » dilemma. Comes with a risk to lose strategic control
 - Trend: creation of a joint defense agency managing outsourcing projects
- > **Deployable communications based on COTS** (Commercial Off The Shelf)
 - Enhance at low cost speed of deployment, bandwidth and flexibility
 - Trends: leveraging SATCOM, WIP, VoIP, ...
- > **Enterprise solutions for user networks** (open architecture)
- > **IP in Combat systems** (tactical C2, computing power, ...)
- > **Space systems** (MILSATCOM, sensors, ...)



— 5

All rights reserved © 2004, Alcatel

Innovative Integration for the Global Networking Grid

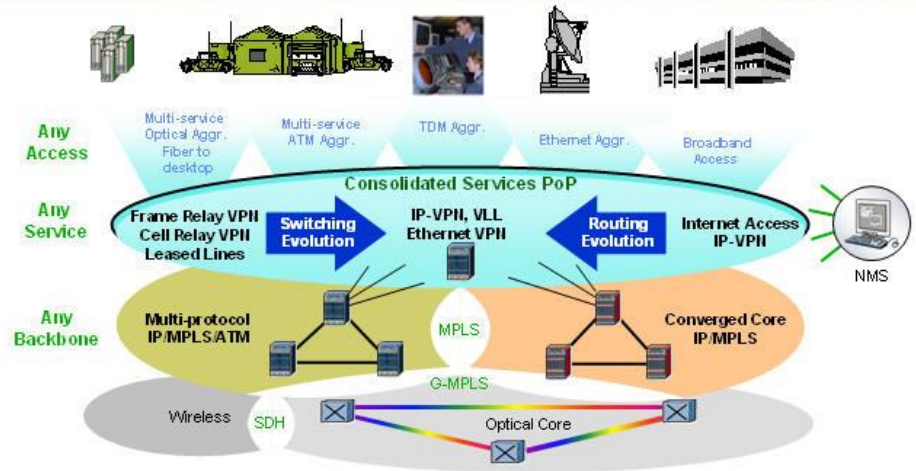
- > Understanding of telecom technologies & trends
 - Technological complexity increases need to master Innovation
 - Innovation is a key differentiator
- > Capacity to manage complexity and risk on behalf of the customer
 - Project size and execution difficulty increase need to master Project management
 - Network operation and maintenance know-how
 - Ability to understand end-customer issues
- > Solutions fitted for Multi-vendor environment
- > Solutions fitted for any project environment (fixed, mobile, broadband, defense, ...)
- > Ability to select best products available from the market
- > Global reach
 - Servicing NATO in Afghanistan and Balkans
 - Delivering networks to US forces in US, Irak, South Korea, Germany



All rights reserved © 2004, Alcatel



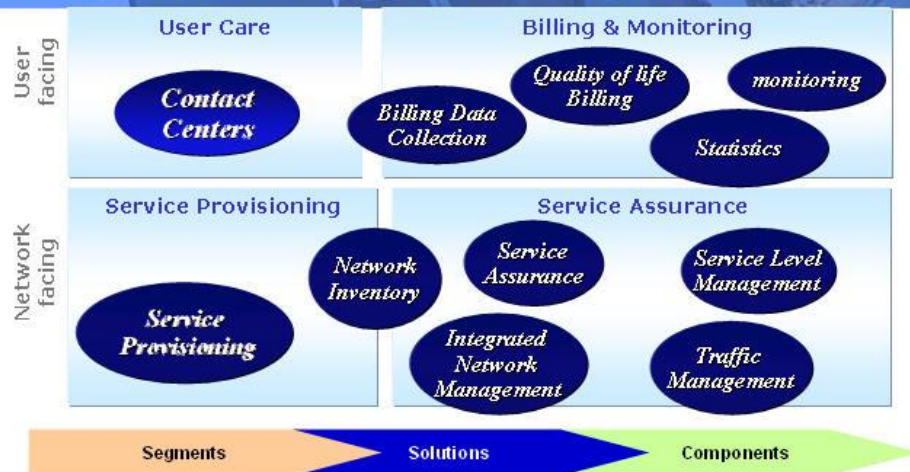
The service aware multi-access network to enable the Global Networking Grid



All rights reserved © 2004, Alcatel

ALCATEL

A Network supervision system operates the Global Networking Grid and delivers reconfigurable end to end services in line with the tempo of action



All rights reserved © 2004, Alcatel

ALCATEL

**Will be presented at NATO RCMCIS conference
(October 2004 – supporting NATO NEC with next generation CIS)**

- > Use of Session Border Controller (SBC) technology to improve interworking of collaborative planning tools across Coalition boundaries.
- > Use of Multi-Protocol Label Switching (MPLS) Explicit Routes (ER) to monitor/control packet flow of sensitive traffic.
- > Use of advanced Network Search Engines (NSE) and Content Inspection Engines (CEI) for improved information sharing across national domain boundaries.
- > SAPIPsec for security of wireless IP multicast

— 11

All rights reserved © 2004, Alcatel

ALCATEL



Thanks for your attention



BIOGRAPHICAL INFORMATION



Patrice Erulin
Director Defense Strategy
ALCATEL

Patrice Erulin is currently the Director of the Defense business development for Alcatel. Convinced that Alcatel, thanks to its unique positioning both in telecom and space systems, can play a major role in driving NCW oriented architectures, he focuses on the smart integration of telecom, IP, e-business and space technologies into all components of a military. He is in contact with defense IT executives from multiple countries, and currently under his direction, Alcatel has been awarded by NATO and prestigious European defense organizations a bunch of innovative communication projects.

Patrice served in the French Navy during 16 years as a naval officer and a jet fighter pilot in a variety of embarked assignments. He circled the world twice on-board warships. During the period 1994-1996, he participated as a jet squadron Executive Officer to the French and NATO air operations over Bosnia. In addition during that period he was assigned Project Leader for the implementation on-board the aircraft carrier of new Information Systems supporting the Naval Force air operations over the land.

Patrice holds an Advanced Degree in Engineering from the French Naval Academy, an MBA from the University of HEC at Paris, and post-graduate studies at the Hong Kong University of Science and Technology.

LES RADIOS DE L'AVENIR POUR LES ARMÉES¹⁹³

Les postes radio de quatrième génération ont été mis en service en 1995, au début de l'essor d'internet et du téléphone portable dans la société civile. En dix ans, ces deux moyens de communication ont changé notre vie quotidienne et la prochaine génération de radios militaires va introduire des évolutions comparables dans les télécommunications militaires tactiques, en empruntant largement les technologies développées pour internet. Cette prochaine génération doit relever un certain nombre de défis techniques :

- l'insertion des radios dans l'intranet militaire ;
- l'agrégation des radios en un réseau unique permettant de relayer les informations au-delà de la simple portée des ondes radios ;
- l'augmentation des débits d'un facteur 100 à 1 000 par rapport au poste radio de quatrième génération ;
- l'avènement de la technologie de radio logicielle, qui permettra de paramétrer la radio avec la forme d'onde la mieux adaptée à l'environnement radio du moment.

Depuis son développement au début du XXe siècle, les militaires ont largement utilisé la radio pour leurs communications tactiques, car ce moyen permet d'échanger des informations sans avoir besoin de déployer d'infrastructure. Les radios tactiques actuellement en service ont été développées dans les années quatre-vingt. Le poste emblématique de cette génération est le poste radio de quatrième génération développé et mis en service en 1995 dans les forces armées françaises et vendu à plus de 100 000 exemplaires à travers le monde.

La prochaine génération, dont la mise en service est prévue à l'horizon 2010. Cet article présente les principales caractéristiques attendues et les risques techniques, calendaires et financiers.

Cette interconnexion des réseaux militaires, analogue à celle qui a abouti à la constitution d'internet dans le monde civil à la fin des années quatre-vingt-dix, est rendue possible par l'utilisation du protocole IP (Internet Protocol). Elle permet d'échanger des informations de façon transparente entre tous les acteurs de l'espace de bataille et non plus seulement entre un chef et ses subordonnés.

L'intranet militaire permet par exemple à l'ensemble des acteurs d'avoir en temps réel les positions amies et ennemies, et donc d'accélérer le "tempo de la manœuvre". L'autre évolution majeure est l'augmentation de la taille des réseaux formés de radios identiques, ce qui permet de faciliter et d'augmenter la portée des échanges d'information à l'intérieur du réseau. Les radios tactiques actuelles (par exemple le PR4G pour l'armée française), conçues dans les années quatre-vingt, étaient au départ destinées à garantir des échanges phoniques ou de messages formatés entre un chef et ses subordonnés en portée radio (distance inférieure à 30 km). Avec le développement des systèmes de commandement comme le SIR à la fin des années quatre-vingtdix, des protocoles ont été développés pour augmenter la portée des échanges d'information en utilisant comme relais d'autres postes de radio. Mais les réseaux radio en mode SAP

^{D'}après une conférence du Collège Interarmées de Défense à Paris

sont limités à quelques dizaines de radios. Pour la prochaine génération il faut développer des réseaux qui pourront contenir jusqu'à plusieurs milliers de radios mobiles, afin de permettre une couverture radio homogène dans tout l'espace de bataille. Ce type de réseaux formés de centaines de radios autonomes n'existent pas pour l'instant dans le monde civil. Ils pourraient voir le jour dans les années à venir et font l'objet de nombreuses études, en particulier à l'IETF (organisme de normalisation du monde internet) où ils sont connus sous le nom de réseaux MANET (Mobile Ad hoc Network).

La troisième avancée concerne l'augmentation des débits : les radios de quatrième génération permettent des débits de quelques kbits/s, mais des débits 100 à 1 000 fois supérieurs sont envisagés pour la prochaine génération.

Cette augmentation des débits correspond à un changement dans les besoins: le poste radio de quatrième génération était conçu à l'origine pour transmettre en priorité de la voix (donc des débits de quelques kbits/s). Il s'agit maintenant de transmettre également les volumes importants générés par les systèmes d'information et d'échanger des données multimédias.

Cette évolution suit celle du monde civil, en particulier celle d'internet où les modems téléphoniques à 56 kbits/s sont progressivement remplacés par des modems ADSL avec des débits de plusieurs Mbits/s. Enfin, la dernière révolution est liée aux progrès de l'électronique numérique: alors que dans les années quatre-vingt-dix les radios comportaient principalement des composants analogiques (filtres, modems), ces fonctions sont maintenant réalisées par des processeurs numériques de traitement du signal tels que les microprocesseurs, Digital Signal Processors (DSP).

L'utilisation de processeurs numériques génériques et programmables permet de reprogrammer les radios en cours de mission avec la forme d'onde adaptée aux conditions du moment (brouillage, interopérabilité avec les autres réseaux...). Ce concept est appelé radio logicielle car comme un ordinateur de bureau, la radio devient configurable en fonction du besoin (débit, résistance à la guerre électronique...). Ces technologies ont été étudiées dès le milieu des années quatre-vingt dix, mais récemment le département de la défense américain a développé un standard d'architecture logicielle, le SCA (Software Communication Architecture), qui définit des interfaces claires entre les composants matériels, la couche middleware développée sur la technologie du monde civil CORBA et la couche des logiciels télécoms. Cette séparation, analogue à la séparation dans le monde informatique entre matériel, OS (Operating System/systèmes d'exploitation) et logiciels permettra de mieux réutiliser les développements logiciels lors des mises à niveau des matériels et de raccourcir les cycles de développement et de mise à niveau des futures radios.

Pour s'intégrer dans le futur intranet militaire formé de réseaux hétérogènes et soutenir la connectivité globale du système de communication de l'espace de bataille, les radios de la prochaine génération auront des interfaces IP. Le paramétrage de ces interfaces est défini par les résultats de l'étude ATTILA (architecture transit de théâtre interconnectant les Local Area Network des armées). À partir de l'architecture visée pour l'intranet militaire en termes de sécurité, management, etc., l'étude ATTILA a établi un certain nombre de recommandations qui s'appliquent aux réseaux militaires en général et aux futurs réseaux radio en particulier. Pour la prochaine génération, comment appliquer les protocoles issus du monde civil (comme ceux définis par le

projet MANET cité précédemment) au défi que constituent l'envoi, le relais et la réception des informations au sein d'un réseau formé de milliers de radios mobiles les unes par rapport aux autres.

Les études précédentes se prêtent bien à des simulations. Cependant, pour vérifier que les radios atteindront la portée et les débits visés, la simulation ne suffit plus. La réalisation de démonstrateurs permet de lever les risques techniques (puissance suffisante des processeurs, dissipations thermiques, maîtrise des pertes électromagnétiques, environnement radioélectrique réel). Ainsi, le démonstrateur radio haut débit (DRHD) confirmera que les performances nécessaires pour répondre aux besoins de l'armée de Terre et de la Marine nationale française (des débits de l'ordre du Mbit/s entre des radios distantes de 20 à 30 km) sont techniquement atteignables. Il se distinguera des radios existantes par son haut débit dans des applications de mobilité en topologie multipoint. Des expérimentations contradictoires seront réalisées au deuxième semestre 2004 :

- deux bandes de fréquences : la bande UHF (225-400 MHz) et la bande SHF (4,4-5 GHz) ;

- deux formes d'onde : une forme d'onde COFDM (Coded Orthogonal Frequency Division Multiplex, technique utilisée dans la norme civile Wireless Fidelity – WiFi) et une forme d'onde à étalement de spectre à séquence directe (technique utilisée par l'Universal Mobile Telecommunications System – UMTS); deux sources industrielles différentes.

Ces expérimentations seront confrontées afin de déterminer la meilleure adéquation au besoin. Les expérimentations sur le terrain dans un environnement de guerre électronique pour des topologies point à multipoint mettant en œuvre 4 plates-formes permettront de vérifier la tenue des exigences. Depuis une dizaine d'années, le SPOTI étudie le concept de radio logicielle car il offre des services supplémentaires à l'utilisateur (possibilité de configurer sa radio...) et permet de développer plus rapidement les formes d'ondes radio (ingénierie logicielle mieux maîtrisée). Deux démonstrateurs correspondant à deux générations successives ont été réalisés. Le premier démonstrateur, le MMR (Multimode Multirole Radio) est réalisé en coopération avec l'Allemagne depuis la fin de l'année 1999. Il est reconfigurable avec 7 formes d'onde différentes, dont le PR4G et le SEM93 (équivalent pour les forces allemandes) avec leurs cryptographies associées. Cette capacité de reconfiguration autorise l'installation et la désinstallation des formes d'onde à la demande. Elle nécessite un effort particulier porté aux méthodes d'ingénierie logicielle, d'autant plus que le développement est réalisé avec plusieurs partenaires industriels. Les progrès de l'électronique numérique ont également permis d'améliorer les performances du MMR par rapport à la génération actuelle, puisqu'il autorise un fonctionnement bivoie (2 voies de communications simultanées) et multigamme (capacité à communiquer dans plusieurs gammes de fréquence, de 1,5 MHz à 600 MHz dans le cas présent). Des expérimentations démontrant ces caractéristiques et des tests d'interopérabilité avec des radios PR4G et SEM93 de génération actuelle seront menées au cours de l'été 2004.

Au vu du premier retour d'expérience du développement du MMR, il a été nécessaire de porter un effort supplémentaire sur les techniques d'ingénierie logicielle : en 2002, le démonstrateur Architecture logicielle a été lancé avec trois objectifs

principaux. Le premier est d'évaluer les technologies et méthodologies logicielles émergentes qui permettent d'abstraire le logiciel (forme d'onde) des ressources matérielles de l'équipement. Il s'agit en particulier d'évaluer le standard américain SCA issu du programme JTRS (Joint Tactical Radio System) qui révolutionne le paysage des radiocommunications outre-Atlantique. Une attention particulière est également portée à la technologie JAVA et aux extensions potentielles de la couche d'abstraction définie par le SCA. Le second objectif est de définir une architecture logicielle conforme au standard SCA afin d'évaluer quelles sont les limitations à l'indépendance entre la plate-forme matérielle et l'applicatif logiciel (forme d'onde).

Enfin, le dernier objectif est de tester matériellement cette architecture logicielle. Deux plateformes conformes au standard SCA sont développées par deux industriels différents. Ces derniers développent indépendamment trois formes d'ondes qui seront portées sur chacune des plates-formes matérielles. Cette étape permettra de valider le concept clé de portabilité des formes d'onde dans un contexte de radio logicielle.

Des essais d'interopérabilité seront également menés avec le démonstrateur MMR. Cette étude s'achèvera fin 2005.

Enfin, il faut mener des études sur l'utilisation de produits civils avec des modifications mineures (pour en augmenter la portée par exemple).

Ces produits ont l'avantage d'un coût bas, mais comme ils ne couvrent pas complètement le besoin militaire, ils ne pourront être utilisés que dans les conflits de basse intensité.

Une série de défis techniques doit être relevée pour que les radios de la future génération constituent la brique de l'avant du système de communication de l'espace de bataille. Cette génération par des démonstrateurs comme DRHD, MMR, ou architecture logicielle, qui permettent de valider les résultats des recherches et vérifier, dans des conditions représentatives de la réalité, que les niveaux de performance espérés sont accessibles. Cette levée de risque servira à lancer un programme dans des conditions de risques moindres sur les coûts et les délais pour une mise en service à l'horizon 2010.

Enfin, il convient de noter la part importante que prend la coopération dans les études et les démonstrateurs. Souhaitons que cette coopération sur les études amont soit les prémices et le prélude à une coopération pour le développement et la production de la prochaine génération de radios.

A HÍRADÓ KIKÉPZÉS AZ ÁTALAKÍTÁS TÜKRÉBEN

A Magyar Honvédség állományába a 2004-es esztendőben vonulnak be utoljára a sorkatonák, kiknek a helyét a jövőben az önkéntes, szerződéses és hivatásos állományúak foglalják el.

Hosszú ideje élő gyakorlatot, valamint a hozzá kapcsolódó kialakult kiképzési rendszer változását eredményezi ez a folyamat.

Tanulmányomban a híradó kiképzés átalakítását kívánom bemutatni az átalakítás tükrében.

A téma megközelítése pedagógiai szempontból

Társadalmunk a gyökeres átalakulások korát éli. Egész társadalmunk fejlődésének egyik kulcskérdése és nélkülözhetetlen feltétele a tudati viszonyok gyorsabb ütemű fejlesztése, az emberek gondolkodásának erősítése, erkölcsi arcukat megváltoztatása, műveltségük gyarapítása. A mai „rohanó” világ, gyors ütemű fejlődésének – mind a számítástechnikai, a híradó és informatikai fejlődésének –, szinte azonos ütemben való követése.

Ezen kihívásoknak szakmailag jó felkészültségű, megfelelő oktató, nevelő és pedagógiai módszerek alkalmazásával felelhetünk meg. Itt kell hangsúlyozni a megfelelő nevelői, pedagógiai módszerek alkalmazását, mely nélkül eredménytelen lenne a csupán szakmai oldalról való megközelítés.

A nevelőmunka hatékonysága jórészt a nevelők tudatosságán múlik. Mennyire ismerik fel és értik meg a gondjaikra bízott katonák gondolkodását, mennyire ismerik személyiségeik sajátos ismertetőjegyeit, valamint ismerik-e a nevelés útját, módját, a nevelési célok irányát, a nevelő munka eszközeit, eljárásait, törvényszerűségeit?!

Nem mindegy, hogy parancsnok és beosztott viszonyának bonyolult kölcsönhatásban, a pedagógiai törekvések nyomán mi lesz a végeredmény. Társadalom, pszichológia, pedagógia sajátos katonai elemek egymásra hatóan rendeződnek el, s az erőteljes fókuszában ott van az a bizonyos legnemesebb anyag, az ember, mint személyiség és nembeli lényegénél fogva humanizmust, egyéni bánásmódot, nevelői tapintatot követel.

Korunkban nagy fontosságú a pedagógiai tudományos, gyakorlati és elméleti kérdéseinek vizsgálata. Egyrészt fokozódnak a személyi állomány kiképzésének követelményei, másrészt a társadalmi, a tudományos-technikai fejlődés, a harcászat minőségi változásai a pedagógia folyamatában, sok új elképzelést, lehetőséget hoztak felszínre.

A pedagógiai kategóriák alapjának megváltozása és bővítése együtt jár a tudomány fejlődésével. Korunk szakirodalmában pedagógiai jelenségek leírásán, magyarázatán, valamint a tevékenységgel kapcsolatos ajánlások kidolgozásán túl, már megjelent a pedagógia prognosztikai funkciója is. A kérdés a társadalmi és tudományos-technikai haladás következtében került napirendre.

A katona személyisége nem megosztottan, hanem egységes egészként fejlődik ki, ezért a csapatoknál és különböző más katonai szervezeteknél folyó nevelőmunkát összeforrott, céltudatos rendszerként kell vizsgálni. A rendszer körvonalai a nevelés távlati terveiben jutnak kifejezésre. Nagyon fontos széles körben alkalmazni azokat a tapasztalatokat, amelyek a nevelőmunka tervezésénél, az oktatási programok kidolgo-

zásánál és a kiképzés ideje alatt összegyűlnek. A nevelőmunkára fokozott figyelmet kell fordítani, amelynek meghatározásakor a következő feladatokat kell elsősorban megoldani:

a./ a nevelési folyamat céltudatosságának, szervezésének, ellenőrzésének, a vezetési folyamat sajátosságának és struktúrájának vizsgálata,

b./ a személyi állomány vezető tevékenységében az eljárók módszereinek vizsgálata.

Az oktatás, nevelés minősége nagymértékben függ a tiszt (parancsnok) személyiségétől, pedagógiai felkészültségétől, tevékenységétől és képességeitől. Személyi példamutatásával beosztottjait pozitív irányba befolyásolhatja, valamint a feladatok alkotó megoldására készítheti.

Különös figyelmet kell fordítani a tisztok pedagógiai tudásának vizsgálatára, a kiképzés és nevelés folyamatában képességeik számára kedvező társadalom-pszichológiai feltételek megteremtésére, hogy a hadsereg tagjaiba pozitív érzelmeket alakítsanak ki, serkentsék őket az alkotóképesség kifejlesztésére, valamint hogy az alárendeltek szellemi színvonalát kellőképpen felismerjék és azt emelni tudják.

Az oktatás és a nevelés egységét képező elv különös jelentőségét az adja, hogy a tiszteknek, parancsnokoknak sajátos hivatásuk van. Nem csupán a személyi állomány oktatásáért, kiképzéséért, szakértelmük kialakításáért, hanem erkölcsi-pszichológiai felkészítésükért is.

Híradó kiképzés lehetséges változata

1. A program célja:

- A tanfolyam keretében szerzett ismeretek elmélyítése, bővítése, a gyakorlati készségek megszilárdítása. A kijelölt személyi állomány felkészítése a rajban háborús és béke kiképzési időszakban, alap híradó és informatikai feladatok végrehajtására.
- Ismertetni a beiskolázott állománnyal az azonos és különmű híradótechnikai eszközök együttes, komplex hírendszemben történő üzemeltetését.
- Az egyénenkénti kiképzéssel szembeni elvárásoknak megfelelő, alapfokú szakmai és módszertani jártasságokkal bíró másodlagos híradó és informatikai kezelő biztosítása a Magyar Honvédség alakulatai részére.
- A programban kiképzendőként résztvevők számára olyan ismeretek és módszerek adása, amelyek a beosztásuk mellett járó feladatok elvégzéséhez meghatározott célok elérését és a követelmények teljesítését biztosítják.

2. A tanfolyam elvégzésével szerzett képesítés követelményei:

Szakmai követelmények:

- **Az előmeneteli tanfolyam tagjai** ismerjék meg a rendszeresített állomások, eszközök rendszerttechnikai alkalmazásával összefüggő feladatokat, a fő- és segédbe-rendezések technikai adatait, jellemzőit, az állomások táplálási, kommunikációs és antennarendszerét. Ismerjék meg a hangolás, a távbeszélő üzemmódok létesítésének szabályait, illetve távvezérlés módjait. Ismerjék a rendszeresített eszközeik

kezelői szintű bevizsgálásának, önellenőrzésének szabályait. Az alkalmazás szintjén ismerjék az életvédelmi és balesetelhárítási rendszabályokat.

- **Híradó állomás és forgalmi szolgálati ismeretekből** a kezelők, távbeszélők, rádiótávírási eszközök el a technikai eszközökhöz kapcsolódó forgalmi és szolgálati utasítások szabályait; a kezelők általános és konkrét köteleit; a különböző híradó eszközökön az összeköttetések felvételével és fenntartásával kapcsolatos előírásokat, tevékenységeket a berendezések, eszközök által biztosított üzemmódokban. Válgassanak képessé a megismert előírások, szabályok gyakorlatban történő alkalmazására, a szolgálati és üzemi csatornákon való hírváltás végrehajtására, a közlemények, küldemények továbbítására és kezelésére. Ismerjék meg a természetes és szándékos zavarok elleni védekezés módjait, a REH alapjait és összetevőit. Sajátítsák el a szolgálati közlések táblázatának alkalmazását, a különböző kódokat és rövidítéseket, valamint a forgalmazásban megengedett egyszerűsítéseket. Ismerjék meg az adatlapok, vázlatparancsnok, eseménynaplók és más, az állomásokon rendszeresített egyéb okmányok kezelésével és vezetésével kapcsolatos teendőket.
- **A beiskolázott állomány tagjai** a felkészítés időszaka végére ismerjék meg a híradó technikai eszközök, komplexumok, állomások, stb. alkalmazásának alapelveit; gyakorolják be a kezelői tevékenységeket és fogásokat, amelyek funkcionális köteleikhez kapcsolódnak. Legyenek képesek irányítás mellett (kezdeti jártassági szinten) a telepítési, építési, üzembe helyezési, üzemeltetési és bontási folyamatokban a szaktevékenységek végrehajtására.

A tanfolyamon résztvevő ismerje meg:

- ismerje meg a tevékenységéhez szükséges szabályzókat, a vonatkozó intézkedéseket és a szolgálati szabályzat adott pontjait;
- a híradó és informatikai alaptanfolyam nyújtotta technikai eszközök rendszerteknikai felépítését, eszközök kezeléséhez nélkülözhetetlen szakmai elméleti és gyakorlati feladatrendszert, normatív követelményeket;
- az élet és baleset elleni védelem rendszabályait;
- a híradó eszközökön folytatott – szakágnak megfelelő – hírváltás szabályait;
- Az informatikai berendezések nyújtotta lehetőségeket, felhasználói programok működési elvét.

A tanfolyam befejezéséig sajátítsa el:

- megtanítani és képessé tenni a szerződéses katonákat szakbeosztásuk mellett (vagy helyett) híradó szakfeladatok teljes értékű ellátására, kialakítani és megszilárdítani együttműködési készségüket az alegység előtt álló feladatok megoldásában.
- felkészíteni a szerződéses katonákat a híradó, informatikai eszközök (állomások) telepítésénél és bontásánál egy kezelői feladat irányítás mellett történő ellátására, megtanítani őket az ehhez szükséges alapvető szabályokra, valamint a tevékenységek során betartandó biztonsági rendszabályokra. Felkészíteni a katonákat az eszközök szabályos üzemeltetésére és forgalmazási szakfeladataik ellátására. A rádióelektronikai harc szabályainak betartására.
- megtanítani és begyakoroltatni a funkcionális köteleikhez kapcsolódó tevékenységeket, hogy magabiztosan legyenek képesek az adott vezetési szint híradás biz-

tosítási feladatainak ellátására a harc különböző fajtáiban, a védelmi harc megvívása során jelentkező híradó szakfeladatok végrehajtására.

- a beiskolázott állomány váljon képessé a vezetékek nélküli és vezetékes híradó eszközökön a hírváltási, forgalmazási feladatok – normatívákban szabályozott – végrehajtására, az összeköttetések létesítésére és folyamatos fenntartására, az információk megbízható, gyors és pontos továbbítására a forgalmi szakutasításokban meghatározottak szerint.
- legyenek képesek a híradó állomások, berendezések szakszerű alkalmazásán túlmenően, azok igénybevételének és technikai kiszolgálásának végrehajtására, a technikai berendezések üzemképességének állandó fenntartása érdekében.

A sikeres vizsga letétele után legyen képes:

- a híradó és informatikai eszköz üzembe helyezésére, üzemeltetésére;
- a komplexumokhoz beosztott állomány feladat meghatározására, szakmai irányítására, ellenőrzésére;
- a beosztott állomány szakmai felkészítésének végrehajtására.

4. A felkészítés programja

4.1. Informatikai alapismeretek

1. Tárgykör: Hardware és software

Biztosított óraszám: 2 óra (elméleti)

Tartalma:

A számítógép típusainak ismertetése, rövid összehasonlítása. Perifériák bemutatása, rendszerben történő telepítésének ismertetése. Az adattárolás lehetőségeinek bemutatása, a személyi számítógép felépítésének ismertetése.

2. Tárgykör: Operációs rendszerek

Biztosított óraszám: 2 óra (elméleti)

Tartalma: a Windows típusú operációs rendszer megismerése, egyéb operációs rendszerekkel történő összehasonlítása. Hatékony munka elsajátítása az egérrel, a rendszer elindítása. Programok és adatállományok elindításának és letöltésének gyakorlása. A munkaasztal használatának és az ablakok kezelésének módszerei.

3. Tárgykör: Fájlkezelés

Biztosított óraszám: 2 óra (gyakorlati)

Tartalma: a Windows Intéző tallózó program használatának gyakorlása, fájlok és mappaműveletek végzése. Parancsikonok készítése, felhasználása, átnevezése, törlése. Dokumentumok keresése név és típus szerint.

4. Tárgykör: Word

Biztosított óraszám: 8 óra (gyakorlati)

Tartalma: a Word indítása, a bejelentkező ablak és képernyő felépítése. Alapvető fájlműveletek (új dokumentum készítése, mentése, betöltése) alkalmazása. Dokumentum, bekezdés és karakterformázás végrehajtása. Szöveg nyelvhelyességének ellenőrzése, oldalszámozások végrehajtása. Tabulátorok használata, táblázatok készítése. Nyomtatás menete.

5. Tárgykör: Excel

Biztosított óraszám: 8 óra (gyakorlati)

Tartalma: az Excel indításának lehetséges módjai, képernyőjének felépítése. Az aktív cella mozgatása, adatbevitel végrehajtása. Munkafüzetek ke-

zelése, formázások végrehajtása. Képletkészítés alapjai, függvények, diagrammok lehetőségei. Nyomtatás menete.

6. Tárgykör: Internet

Biztosított óraszám: 2 óra (gyakorlati)

Tartalma: a Világhálóra történő csatlakozás módjai, „Honlap” megnyitásának gyakorlása. Adott állomány, dokumentum keresése, letöltése. Rövid e-mail üzenetek küldése, fogadása.

Javasolt irodalom: *(a képzési követelményekben meghatározottakon túl)*

- ZMNE Vezetés- és Szervezéstudományi Kar, Informatikai Tanszék: A katonai informatika alapjai című egyetemi jegyzet
- A HM HONVÉD Kulturális Szolgáltató Közhasznú Társaság: számítógép kezelői, oktatási tematika és alapismeretek című tansegédlet.

Módszertani ajánlások:

Az ismert anyagot gyakorlati foglalkozások (lehetőleg egy csoportban, az informatikai tanteremben) keretében kell feldolgozni. Az egyes foglalkozások anyagainak oktatása során a hangsúlyt a katonák egyéni felkészítésére kell helyezni. Az oktatás alapvető módszerét az egyszerű, könnyen érthető, példákkal illusztrált előadásmód jellemezze. Törekedni kell a gyakorlatiasságra. Elméleti módszerrel csak a legszükségesebb technikai alapismereteket, a berendezés kezelésével és üzemeltetésével kapcsolatos szabályokat oktasson a foglalkozásvezető.

4.2. Műholdas hírközlési ismeretek

1. Tárgykör: Műholdas távközlési ismeretek.

Biztosított óraszám: 2 óra (elméleti)

Tartalma: a műhold és lefedettségének jelentése. Műholdak és földi állomások kapcsolattartásának rendszere és lehetőségei.

2. Tárgykör: Inmarsat műholdas telefon ismertetése.

Biztosított óraszám: 2 óra (elméleti)

Tartalma: a TT 3060 A mobiltelefon bemutatása, technikai jellemzői. Menürendszerének elmélete, bemutatása.

3. Tárgykör: Inmarsat műholdas telefon működtetése.

Biztosított óraszám: 6 óra (gyakorlati)

Tartalma: az Inmarsat műholdas telefon üzemhez való előkészítése, üzemeltetése. Az üzemeltetés során választható üzemmódok lehetőségei. Hívásindítás és hívásfogadás lépései. A karbantartás szükséges mozzanatai.

Javasolt irodalom: *(a képzési követelményekben meghatározottakon túl)*

- HM Kommunikációs Főigazgatóság által biztosított kiadvány,
- Inmarsat műholdas telefon használati útmutató.

Módszertani ajánlás:

Az ismert anyagot elméleti és gyakorlati foglalkozások keretében kell feldolgozni. Az egyes foglalkozások anyagainak oktatása során a hangsúlyt a katonák egyéni felkészítésére kell helyezni. Az oktatás alapvető módszerét az egyszerű, könnyen érthető, példákkal illusztrált előadásmód jellemezze. Törekedni kell a gyakorlatiasságra. Elméleti módszerrel csak a legszükségesebb technikai alapismereteket, a berendezés kezelésével és üzemeltetésével kapcsolatos szabályokat oktasson a foglalkozásvezető.

4.3. Forgalmi szolgálat

1. Tárgykör: Általános előírások.

Biztosított óraszám: 2 óra (elméleti)

Tartalma:

A rádióhíradás helye, szerepe jelentősége és elemei. A rádióháló és rádió-irány fogalma, a rádióállomások felosztása. Sürgősségi kategóriák elemzése.

2. Tárgykör: Rádióforgalmi szolgálat szabályai rádió távbeszélő üzemmódban.

Biztosított óraszám: 2 óra (elméleti)

Tartalma:

Az összeköttetés felvételének szabályai, ismertetőjel kérés-adás előírásai. Hívások fajtái, frekvencia váltás szabályainak betartása.

3. Tárgykör: A rádióforgalmi okmányok és azok vezetésének rendje.

Biztosított óraszám: 2 óra (elméleti)

Tartalma:

A forgalmi eseménynapló kitöltésének szabályai, módjai. A rádióforgalmi rendszer adatlapja, használatának előírásai. Távirati űrlap alkalmazásának szabályai. A Szolgálati közlések táblázatának kezelése, kitöltésének szabályai.

Javasolt irodalom: *(a képzési követelményekben meghatározottakon túl)*

- Normagyűjtemény híradó katonák osztályos fokozat értékeléséhez;
- Híradó állomás és forgalmi szolgálat utasítás;
- Rádióforgalmi szakutasítás;

Módszertani ajánlás:

Az ismeretanyagot elméleti foglalkozások keretében kell feldolgozni. Az okmányok kidolgozása témakörben célszerű mintaokmányokon demonstrálni az elvárásokat, majd önálló foglalkozás keretében értékelni. A tanfolyamon résztvevők a gyakorlati foglalkozásokon gyakorolják a tanultakat az előírásoknak megfelelően. Az oktatás alapvető módszerét az egyszerű, könnyen érthető, példákkal illusztrált előadásmód jellemezze.

4.4. Típus ismeret

1. Tárgykör: Az élet és balesetvédelem

Biztosított óraszám: 2 óra (elméleti)

Tartalma: A villamos áram élettani hatása az emberi szervezetre. Az elektromos balesetek fajtái, áramütés veszélyei. Tűzoltó eszközök használatának szabályai, betartandó biztonsági rendszabályok. A telepítés, építés, üzemeltetés, bontás valamint málházás során betartandó biztonsági rendszabályok.

2. Tárgykör: R-107 rádiókészülék ismeret

Biztosított óraszám: 1 óra (elméleti)

3 óra (gyakorlati)

Tartalma: A rádiókészülék technikai bemutatója, fontosabb technikai adatok ismertetése. Kezelőszervei, üzemmódjai. A rádiókészülék üzemeltetési és alkalmazási lehetőségei. A vezérlés és távvezérlés lehetősége. A karbantartás rendje. Az áramellátás és antenna rendszere.

3. Tárgykör: R-159, R-1260 rádiókészülék ismeret

Biztosított óraszám: 1 óra (elméleti)

3 óra (gyakorlati)

Tartalma: A rádiókészülékek technikai bemutatója, fontosabb technikai adatok ismertetése. Kezelőszerveik, üzemmódjaik. A rádiókészülékek üzemeltetési és alkalmazási lehetőségei. A karbantartásuk rendje. Az áramellátás és antenna rendszerük.

4. Tárgykör: R-142 rádióállomás ismeret

Biztosított óraszám: 4 óra (elméleti)

18 óra (gyakorlati)

Tartalma: A rádióállomás technikai bemutatója, fontosabb technikai adatok ismertetése. A gépkocsi belső terének felosztása, a beépített híradó- és segédberendezések, továbbá a parancsnoki munkát szolgáló eszközök rendeltetése, elhelyezése. A beépített berendezések kezelőszerve, üzemmódjai. A rádióállomás üzemeltetési és alkalmazási lehetőségei. A vezérlés és távvezérlés lehetősége. A karbantartás rendje. Az áramellátás és antenna rendszere.

5. Tárgykör: Komplex foglalkozás

Biztosított óraszám: 12 óra (gyakorlati)

Tartalma: A rádióállomás (rádiókészülékek) üzemelőtti bevizsgálása, üzembe helyezése. Hangolások, beszabályozások végrehajtása, szolgálati összeköttetések létesítése. Vezérlő vonalak kiépítése. Összeköttetések felvételének gyakorlása a lehetséges üzemmódokban és vezérlési változatokban. Közlemények adás-vételének, a hírváltási feladatok végrehajtásának gyakorlása. Üzemmódokkal, antennákkal, teljesítménnyel való manőverek gyakorlása.

Javasolt irodalom: *(a képzési követelményekben meghatározottakon túl)*

- KÁBESZ,
- Érintésvédelmi utasítás,
- MH-ban hatályos alapvető munkavédelmi jogszabályok gyűjteménye,
- Szakkiképzési program a SZFP alárendeltségébe tartozó híradó katonák és alegységek kiképzéséhez,
- R-142 rádióállomás kezelési utasítása
- R-107 rádiókészülék műszaki leírása és kezelési utasítása,
- TBK-67 tábori távbeszélő készülék kezelési utasítása.

Módszertani ajánlás:

A tárgykör anyagát lehetőleg egy csoportos foglalkozás keretében kell feldolgozni. A tanfolyamon résztvevők a gyakorlati foglalkozásokon gyakorolják a tanultakat az előírásoknak megfelelően. Az oktatás alapvető módszerét az egyszerű, könnyen érthető, példákkal illusztrált előadásmód jellemezze. A telepítés-bontás és üzemeltetés anyagának oktatása során arra kell törekedni, hogy a katonák elsajátítsák a számukra rendszeresített eszközök üzembe helyezési, üzemeltetési folyamatainak és működtetésének technológiai helyes sorrendjét, gyakorlati fogásait, a kezelő kötelmeit. Valamennyi gyakorlati foglalkozás megkezdése előtt a vonatkozó életvédelmi és baleset elleni védelem rendszabályait is oktatni kell.

Szigorúan tilos a katonákkal olyan foglalkozásokat végrehajtani, amelyekre nem lettek előzőleg kioktatva, olyan gyakorlati foglalkozást levezetni, amelynek biztonságos végrehajtásához szükséges rendszabályokra nem lettek megtanítva, a balesetmentes ténykedésre való képesség nem lett a foglalkozásvezető által ellenőrizve.

4.5. A tantárgyak kapcsolódása más tantárgyakhoz

A tárgykörökre biztosított óraszámot ajánlasként kell kezelni. A képzési ágak és tárgykörök tartalmi összefüggéseit a képzés tematikus tervének elkészítésénél figyelembe kell venni. Minden képzési ág és tárgykör ismeretanyagát a kiképzés folyamatában, gyakorlati foglalkozásokon ötvözni kell. Törekedni kell arra, hogy a képzés végére minden beiskolázott képes legyen az ismeretek ötvözésével önállóan végezni a híradó tevékenységgel járó kötelmeit.

5. A képesítés vizsgakövetelményeinek meghatározása

A képesítő vizsga során alapvetően figyelembe kell venni a szakmai vizsgáztatás általános rendjéről szóló – a 4/1996. (V.24.) MÜM rendelettel módosított – 10/1993. (XII. 30.) MÜM rendelet előírásait, valamint a HM OTF 1997-ben a szakmai vizsgáztatás megszervezéséhez kiadott útmutatóját.

A vizsgán számon kell kérni a képzési programban meghatározott ismeretanyagot.

A másodlagos híradó és informatikai kezelői felkészítés tantárgyaiból írásbeli, gyakorlati vizsgát kell tenni.

5.1. A vizsga részei:

- Írásbeli
- Gyakorlati

5.2. Írásbeli vizsga:

Az írásbeli tételek az informatikai alapismeretek, a műholdas hírközlés, a forgalmi szolgálat és a típusismeret témaköreiből összeállított kérdéseket tartalmazza. A gyakorlati vizsga tárgyát képező foglalkozás mindenoldalú biztosítását e helyszínen biztosított anyagokból történő szelektív válogatás útján a vizsgázó végzi el.

A biztosított idő: 50 perc

5.3. Gyakorlati vizsga:

Gyakorlati vizsgafeladat az írásbeli anyaggal összefüggésben egy meghatározott híradó csatorna működtetése, forgalmazásának okmányolása a kijelölt híradó berendezéssel

A vizsgára történő felkészülés ideje: 30 perc

A vizsga időtartama: 30 perc

5.4. A vizsga értékelésének meghatározása:

5.4.1. A vizsgázó által levezetett kiképzési foglalkozás, értékelési szempontjai:

- a. A vizsgázó szakmai felkészültsége. A foglalkozási anyag ismereteinek elsajátítása, alkalmazása.
- b. A foglalkozás anyagi-technikai biztosítása, a foglalkozási hely berendezése, a biztosított eszközök-anyagok ismerete, előírás szerinti alkalmazása, felhasználása.
- c. A foglalkozás hatékonysága, intenzitása, az időkihasználtság, a hasznos idő aránya.
- d. A foglalkozás milyen mértékben érte el a célját.

5.4.2. Értékelés:

Az értékelés a fent leírt értékelési szempontok figyelembevételével történik, annak elbírálásával, hogy azok milyen mutatók formájában jelentkeznek a foglalkozás során.

5.4.3. Értékelési mutatók:

a.) A beiskolázott állomány felkészültsége:

- **5-ös** = teljesen átfogja - uralja - az anyagot;
- **4-es** = egyes - nem lényegbevágó - részek elmaradtak;
- **3-as** =, az anyag tartalmának megfelelően egy, vagy több fontos tevékenység - anyagrész - nem kerül végrehajtásra;
- **2-as** = az anyag tartalmának megfelelően a fontos tevékenységek több mind fele nem kerül végrehajtásra;
- **1-es** = a foglalkozás hatékonyságát meghatározó lényegi tevékenység - tevékenységek - nem kerülnek végrehajtásra.

b.) A gyakorlati vizsga anyagi-technikai biztosítása, az eszközök alkalmazása:

- ha minden biztosított, az eszközök alkalmazása szabályos = **kiváló**;
- ha minden biztosított, de az eszközök alkalmazása hiányos = **jó**;
- csak a főbb eszközök vannak biztosítva = **megfelelő**.
- a főbb eszközök nincsenek biztosítva = **nem megfelelő**.

c.) A gyakorlati feladat intenzitása, a hasznos idő aránya:

- **kiváló**, ha- 50 %-nál kisebb az időkihasználás;
- **jó**, ha- 60-70 %-os az időkihasználás;
- **megfelelő**, ha- 80-90 %-os az időkihasználás.
- **Nem megfelelő**, ha- 100%-nál nagyobb az időkihasználás.

d.) A gyakorlati vizsga hatékonysága:

- **Kiváló** = az előírt tevékenység végrehajtásra került, a rádióhálóban megfelelően ténykedett a katona;
- **Jó** = egyes feladatok végrehajtása hiányos (okmányolás);
- **Megfelelő** = összeköttetést létesített, de a forgalmazás nem történt meg
- **Nem megfelelő** = nem került sor az összeköttetés végrehajtására.

A vizsga összértékelését az értékelési mutatókra adott osztályzatok számtani középátlagja adja. Ezek alapján:

- **5-ös** ha az egyes mutatókra adott osztályzatok számtani középátlagja 4,51, vagy ennél több (ezen belül a b.,c.,d., mutató kiváló);
- **4-es** ha az egyes mutatókra adott osztályzatok számtani középátlagja 3,51-4,50 (ezen belül az a., c., d., mutatók legalább jó);
- **3-as** ha az egyes mutatókra adott osztályzatok számtani középátlagja 2,51-3,50 (ezen belül a c., d., legalább megfelelő).
- **2-es**, ha egyes mutatókra adott osztályzatok számtani középátlagja 1,51-2,50 (ezen belül az d., legalább megfelelő).
- **1-es** ha az egyes mutatókra adott osztályzatok számtani középátlagja nem éri el az 1,50-t.

Az érdemjegyeket az ötfokozatú skálának megfelelően kell megállapítani:

- o jeles (5),
- o jó (4),
- o közepes (3),
- o elégséges (2),

-
- elégtelen (1).

A MEGBÍZHATÓ, INTELLIGENS ÉS BIZTONSÁGOS HÁLÓZAT RECEPTJE

Kapsch TeleCom Kft.



A megbízható, intelligens és biztonságos hálózat receptje

Nortel LAN/WLAN portfólió a Kapschtól

Szabó Zoltán
tervező mérnök

Kommunikáció 2004



Kapsch TeleCom Kft.

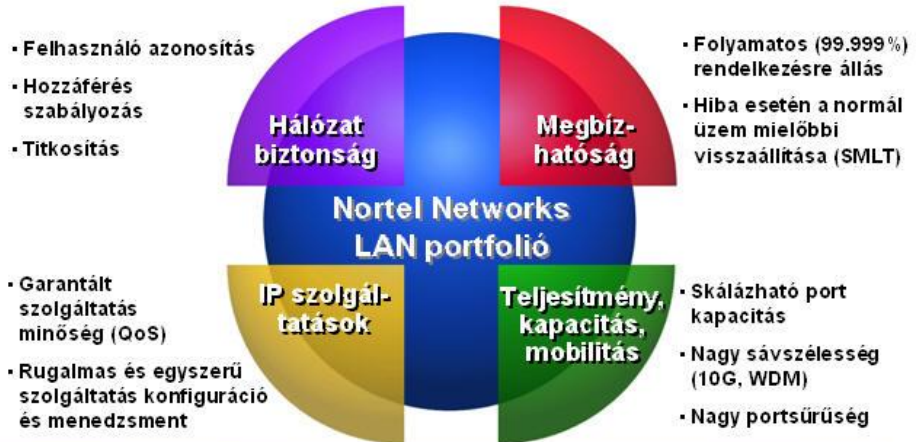


Hozzávalók



- Teljes körű termékskála
 - Vezetékes (LAN)
 - Vezeték nélküli (WLAN)
 - Hálózat felügyelet
- A legkorszerűbb hálózati technológiák alkalmazása
- Dinamikus termék- és technológiai fejlesztés
- Elsőrangú támogatói szolgáltatások
- Versenyképes ár
- Meggyőző referenciák

Korszerű hálózati technológiák – avagy hogyan szolgáljuk ki a legfontosabb igényeket?



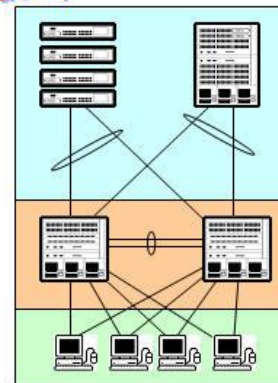
A Nortel válasza: BayStack és Passport LAN kapcsolók

Split MultiLink Trunking (SMLT)

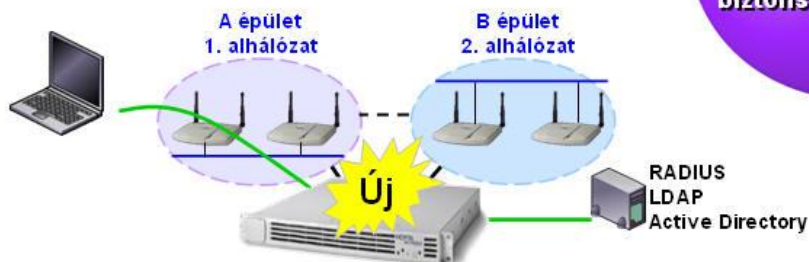
Megbízhatóság

- Jobb, mint 99.999% rendelkezésre állás
- Terhelésmegosztás
- <1 mp átállás
- Hogyan csinálják mások?
 - Spanning Tree (~40 mp)
 - Rapid Spanning Tree (~8 mp)

Minden port AKTÍV



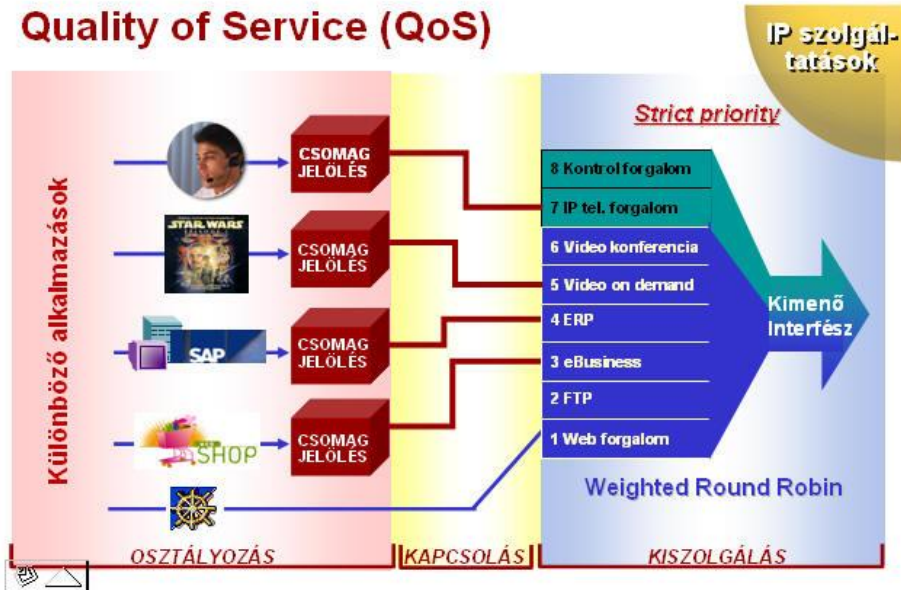
WLAN Security Switch 2250



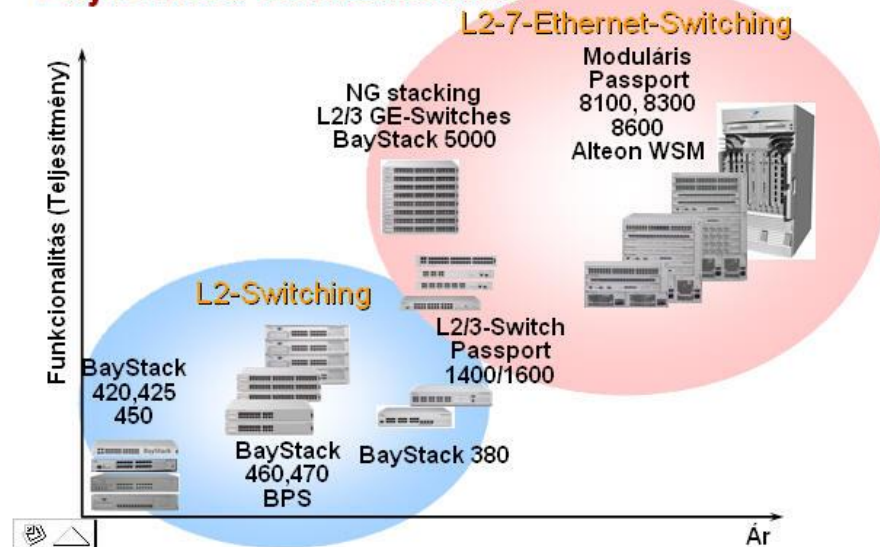
WLAN Security Switch 2250

- 802.1x, SSL, IPSEC alapú hálózat biztonság
- Felhasználó azonosítás, hozzáférés szabályozás, titkosítás
- Alhálózatok közötti roaming
- Forgalom szabályozás
- Központosított WLAN menedzsment

Quality of Service (QoS)



Teljes körű termékcsalád



Gigabit a számítógépekhez – BayStack 5510

- 24 és 48 portos 10/100/1000 kapcsoló
 - A két utolsó port 1000Base-T vagy SFP GBIC
- 8 eszközig szteckelhető
 - 384 db 10/100/1000 port 8 RU magasságban
- Hamarosan 802.3af Power over Ethernet funkcionalitással
- DMLT, SMLT, QoS
- Fejlett hálózat biztonsági funkcionalitás
 - 802.1x alapú felhasználói azonosítás (EAP)
 - SSHv2 – biztonságos CLI konfigurálás
 - SNMPv3, RADIUS támogatottság



BayStack 5510-48T



BayStack 5510-24T





Passport 8300 – munkacsoporti szerepre

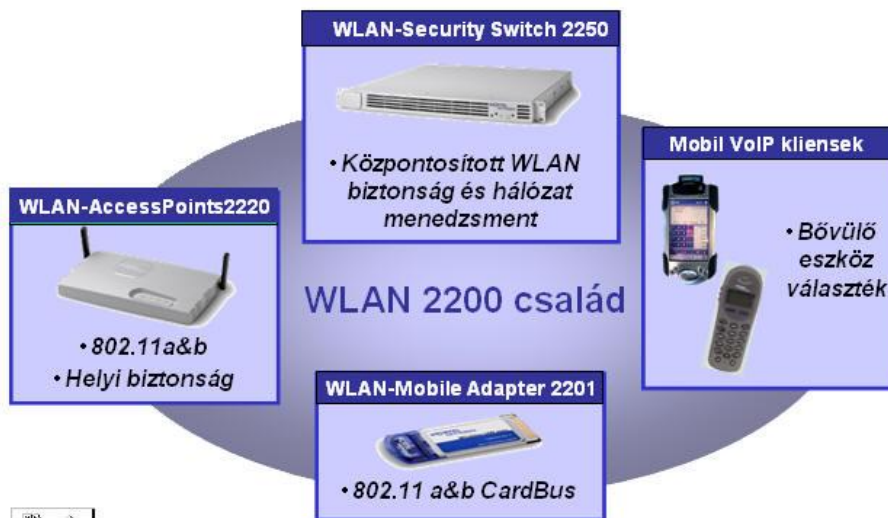
- Fokozott megbízhatósági jellemzők
 - Redundáns SF modul, táp és ventilátor (+hot-swap)
 - DMLT, SMLT
- 8 db Gig SFP port az SF modulokon, QoS
- Jelenleg 48x10/100 és 24x10/100/1000 modulokkal (+802.3af PoE)
- 8306, 8310 (4 és 8 I/O modulós szekrények)
- Fejlett hálózat biztonsági funkcionalitás
 - 802.1x alapú felhasználói azonosítás (EAP)
 - SSHv2 – biztonságos CLI konfigurálás
 - SNMPv3, RADIUS támogatottság



Passport 8310



WLAN portfólió – biztonság, QoS és roaming



És a referenciák – például HSBC központ



- 8500 felhasználó
- 16,000-20,000 port
- 116 db Passport 8600
- 3 db Passport 7K
- 1 db Passport 15K
- 13 db Alteon WSM
- 2 db Meridian1
- DECT
- Symposium
- Konferencia

Köszönöm a figyelmet!

Szabó Zoltán

tervező mérnök – adatkommunikációs rendszerek

zoltan.szabo@kapsch.net

A NATO ÚJ KEZDEMÉNYEZÉSE A HÁLÓZAT NYÚJTOTTA KÉPESSÉG

1./ Előszó

A 2001. szeptember 11.-i terroristatámadás alapvetően megváltoztatta a biztonsági környezetünket. Jól definiálható szembenálló felek által kölcsönösen bebiztosított pusztítás veszélye helyett a terrorizmus fenyegetése lépett színre, amely arctalan, és amelyet az esetek többségében nem vagyunk képesek időben azonosítani, és amely kockázati tényezője területhez, földrészhez nem köthető. Reagálásképpen egy új hadászati elrettentés kialakításának igénye merült fel, amely egyrészt a terroristák szponzorainak elriasztásán, másrészt a terroristák meggyőzésén alapul, miszerint a terrorizmusnak nem lehet sikere. Ez a megelőzés szemléletű elrettentés, valamint egy új viselkedésmód kialakítása a civil és a katonai erők másfajta kiegyensúlyozott alkalmazását igényli. A viselkedésmód újraformálása a hatékonyság alapú műveletek kulcsa. Azt az alapvető fontosságú tényezőt, amely ezt az új megközelítést lehetővé teszi - új terminológiával és tartalommal - Hálózat Nyújtotta Képességnek nevezzük. A következőkben röviden tekintsük át a hálózat nyújtotta képesség determinálta összhaderőnemi követelményeket, majd ezt követően vessünk egy pillantást arra, hogy a NATO részéről szűkebb értelemben vett szakterületünkön milyen tevékenységek kezdődtek meg ennek szellemében, és milyen kihívásokkal nézünk szembe, illetve milyen falakat kell a híradás és informatika, különös tekintettel az információvédelem terén lerombolni az áhított végső cél eléréséhez.

Mivel az alap kutatások az Egyesült Államokban kezdődtek, a szakirodalomban először az úgynevezett Network Centric Warfare (NCW), azaz Hálózat Centrikus Hadviselés elnevezés jelent meg először. Amikor a NATO - az NC3B vezetésével - döntést hozott a kutatások NATO égisze alatti történő megkezdéséről, a kutatást finanszírozó tagállamok javaslatára az NC3B NATO Network Enabled Capability, azaz NATO Hálózat Nyújtotta Képesség névre keresztelte (a továbbiakban NNEC) az új képességet, amely kizárólagosan ezen a néven benyomult be a NATO szakirodalomba. Tartalmát tekintve gyakorlatilag nincs különbség a két elnevezés között, ezért napjainkban mindkét elnevezést széleskörűen használják. A NATO elnevezés következetes használata mellett az idézetek, a jobb érthetőség kedvéért vagy csupán csak a stilisztikai kedvéért e mű mindkét elnevezést egyaránt használja.

2./ A NATO hálózat nyújtotta képesség igényének kialakulása

A Prágai Csúcstalálkozón 2002. októberében a NATO vezetői egyetértettek, hogy modernizálják a vezetési struktúrát, egy karcsúbb, eredményesebb, hatékony és bevethető erőt fenntartva, amely a szövetséges műveletek teljes skáláján képes megfelelni bármilyen hadműveleti követelménynek. Szerves részelemeként magába foglalva a NATO Reagáló Erőt -NATO Response Force (a továbbiakban NRF), amely technológiailag fejlett, rugalmas, bevethető, interoperábilis, és fenntartható erő egyaránt tartalmazva a szárazföldi, tengeri és légi erő komponenseket. 2003. októberében a NATO hivatalosan is felállította az NRF kezdeti képességet.

Az iraki háború kapcsán 2003. júliusában egy magas szintű NATO szeminárium került levezetésre, amelyen az USA és az Egyesült Királyság kezdeti tapasztalatait feldolgozva elkészítették a kezdeti tapasztalatok listáját, amelyből a NATO számos előnyös következtetést vonhat le. A legfontosabbnak ítélt első 20 pontból 5 közvetlenül a hálózat nyújtotta képességgel kapcsolatos nevezetesen:

- a NATO döntéshozói folyamata nem elég válaszképes;
- a gyors bevetethetőség és az eredmény elérése meghatározó a képességekben;
- tudásalapú hadviselés;
- hálózat centrikus hadviselés;
- bevetethető vezetési pontok és vezetés – irányítás, illetve híradó és informatikai rendszerek.

A NATO Military Committee azaz a Katonai Bizottság elnöke Kujat tábornok kijelentette: „Az NRF-nek gyorsan bevetethetőnek, hálózat-centrikusnak, gyors eredmény elérésére képesnek kell lenni. Rendelkezzen erre alkalmas vezetés-irányítási, hírszerző, légtér-felügyeleti és felderítő rendszerekkel, amelyek együttműködnek a közös helyzetkép biztosításában. A szövetséggel szembeni katonai kihívás az lesz, hogy átalakítsa jelenlegi erőit és képességeit, hogy szavatolja az eredményesség-alapú műveleteket. Ez kihatással lesz a hadműveleti erők tervezésének és előkészítésének, összeállításának, kiképzésének, bevetésének, alkalmazásának és fenntartásának minden aspektusára.”

Ez a tömör elvi – nevezhetnénk akár követelménytámasztásnak is – megállapítás messze vezet. Gyökerei az elmúlt években - főleg az USA-ban - végzett, az Információs Korszak katonai műveletekre gyakorolt hatását, kihasználását, a jövő hadászati, harcászati tevékenységét kutató projektek eredményeire, megállapításaira nyúlnak vissza. A hálózat nyújtotta képesség kialakítására ható kutatási eredmények, megközelítések új meghatározásokat, kategóriákat, elveket generáltak.

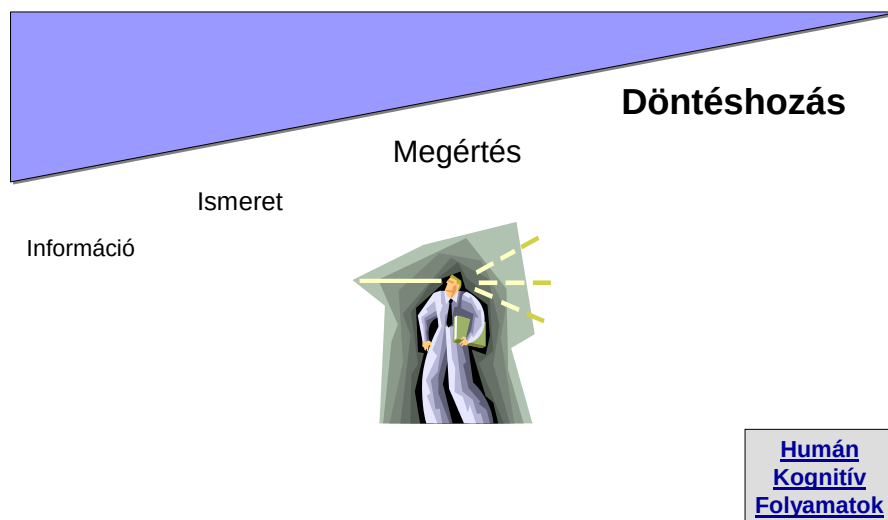
Edmund Giambastiani admirális, mint az Egyesült Államok Összhaderőnemi Erőinek parancsnoka és a NATO Szövetséges Átalakító Parancsnokság főparancsnoka azt mondta:

“Hiszem, hogy az olyan képességek, mint az NNEC a NATO átalakítás hajtómotorjai. De hogy helyesen fejlesszük ki a hálózat nyújtotta képességet szükségünk van a nemzetek hozzájárulására, hogy helyes irányba mozdítsanak el bennünket, és hogy létrehozzunk egy közös keretet a munka elvégzésére, amely a NATO és a tagállamok részvételével kell, hogy kidolgozásra kerüljön. A vezetés-irányítást (C2) a csapatvezetés és az irányítás humán és szervezeti elemeként fogjuk fel, míg a C2ISR-t másnéven Kommunikációt, Számítógépet, Hírszerzést, Légtérellenőrzést, Felderítést, mint aspektusokat, amelyek leírják, hogy az ismereteket technikailag hogyan gyűjtjük össze, hogyan analizáljuk, hogyan jelenítjük meg és digitálisan hangként, adatként vagy képként és hogyan terítjük.”

A hálózat nyújtotta képesség biztosítani fogja az eszközöket, hogy lehetővé tegye a NATO erők számára, hogy gyorsan bevetethető expedíciós erökké váljanak és műveleteket hajtanak végre, amelyek koherensen összhaderőnemieket, együttműködők, hálózatcentrikusak és eredményesség alapúak. Ez az a néhány kulcsfontosságú tényező a hadműveleti követelmények közül, amelyeknek az átalakuló NATO erőknek birtokában kell lenni.

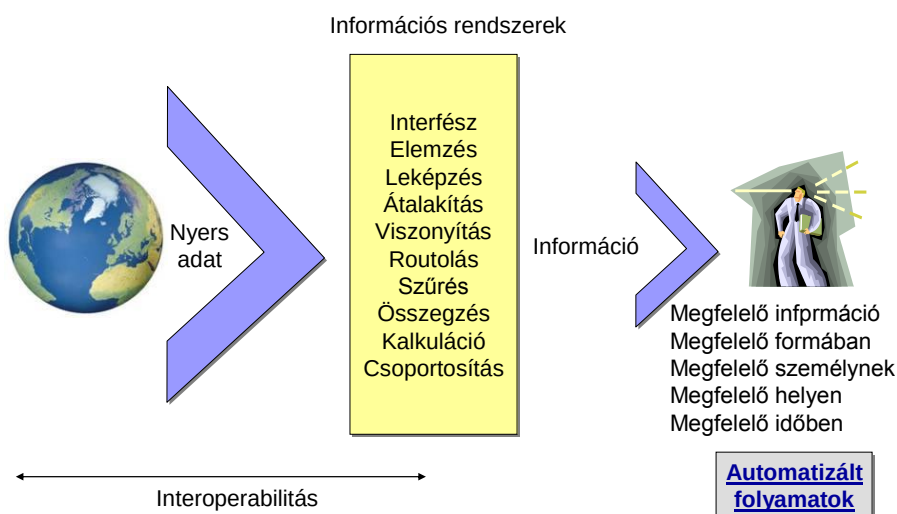
A döntéshozatali mechanizmus leírására egyre inkább a következő egyszerűsített modell válik általánossá a nyugati terminológiában: Megfigyelés, Ismeret, Döntés, Tevékenység. A döntés ciklusa markánsan három fő területen megy végbe. Nevezetesen a fizikai, az információs és a kognitív területeken. Megfigyelünk, keresünk, hogy megértsünk, döntünk és tevékenykedünk ezeken az említett területeken. Kategorizáljuk, fedjük egymásra a négy meghatározó elemet azaz:

- először érzékelni és többet érzékelni, hogy elérjük az **információs fölényt**;
- gyorsabban és jobban megérteni, hogy elérjük a **tudásfölényt**;
- jobban és gyorsabban dönteni, hogy megvalósítsuk a **döntésfölényt**;
- ellentmondást nem tűrően tevékenykedni, hogy eredményesség-alapú műveleteken keresztül elérjük az **eredményesség fölényt**.



1. sz. ábra A döntés folyamata

Egyszerűsítve, az 1. sz. ábra szerinti döntés folyamatát képezhetjük le belölük. Az információs fölény a harctéri adatok hadműveleti és hírszerző szenzorok által történő gyűjtésén, e szenzorok adatainak információvá való fuzionálásán alapszik. Képzeljünk el egy szenzor és információs hálózatot, amely egybekapcsolja az összes vizuális, radar, pilótánélküli felderítő repülőgép továbbított képeket, műholdas képanyagokat, elektronikus és más hírszerző adatokat. A megfelelően kezelt és fuzionált adatok minden szinten növelhetik a csapatok között megosztott helyzetkép pontosságát.



2. sz. ábra Az információfeldolgozása és megjelenítése

Az információs fölény előnyt biztosít az információs versenyben a szövetségeseknek, ami a jövő eredményesség alapú művelet megnyeréséhez szükséges. A 2. sz. ábra az információfeldolgozás és megjelenítés folyamatát mutatja be.

Az információs fölény - az ellenféllel szemben -még több és még jobb minőségű információhoz történő hozzáférést jelenti, birtokolva mindazon eszközöket, technikákat, amelyek a helyes döntéshozatalt támogatják, valamint azon megfelelő vezető szerveket, amelyek e döntés alapján gyorsabban és hatékonyabban tevékenykednek, mint egy lehetséges ellenfél. Ezen felül az információs fölény elérése maga után vonja mindazon tevékenységeket, amelyeket annak érdekében hajtanak végre, hogy minimalizálják (korlátozzák, késleltessék) a szembenálló fél helyzetkép felismerés és döntéshozatali képességét. Az információs fölény elérésének kulcsa egy NATO hálózat nyújtotta képesség kifejlesztése, hogy biztosítsák az információ biztonságos gyűjtését, feldolgozását, és terítését.

A NATO Hálózat Nyújtotta Képesség (NATO Network Enabled Capability - NNEC) átfogja mindazon elemeket, amelyek az információgyűjtők, végrehajtók és a döntéshozók együvé kapcsolásában részt vesznek, hogy lehetővé tegyék egy NATO hálózat centrikus, eredményesség alapú hadműveleti képesség kifejlesztését. Ez magába foglalja azon összhaderőnemi erők bevetését és fenntartását, amelyek képesek az információt megnövekedett harci erővé és hatékony feladat végrehajtássá átalakítani. Az NNEC a teljes harcmezőn keresztül lehetővé teszi a döntéshozás agilitását, kezdeményezőkézségét a műveletek precizitását és koherenciáját.

Hiba! A mezők szerkesztésével nem hozhatók létre objektumok.

3. sz. ábra A koncepció folyamat ábrája

A tudásfőlény biztosítja a parancsnokok és döntéshozók számára a harctér eredményes megértését. Minden arra felhatalmazott egyénnek hozzáférése lesz a lehetséges legjobb információhoz és tudáshalmazhoz, amely a hálózaton található könyvtárban található. Az információ ily módon bármikor, bárhol, bárki számára elérhetővé válik. Képzeljünk el egy „tudáshálózatot”, amely ellátja a felhasználót a harctérre vonatkozó, referenciával rendelkező „használatra kész ismeretekkel”. Ez segíteni fogja a döntéshozókat, hogy jobb és gyorsabb döntéseket hozzanak. 3. sz. ábrán az NNEC koncepció folyamat ábrája látható.

A döntésfőlény magába foglalja a döntéstámogató rendszerekkel felszerelt törzseket, amelyek analízissal és opciók felajánlásával segítik a döntést, így támogatva a döntéshozókat, hogy jobb döntéseket sokkal gyorsabban érjenek el. Egy világos parancsnoki szándékhoz történő könnyű hozzáférés lehetővé teszi az alárendelt parancsnokok számára, hogy megértsék megbízásaikat és teljes kezdeményezőkézséget gyakoroljanak feladataik végrehajtásában. Ez az erők önszinkronizálásának lehetőségében és az eredményesség főlényben fog kicsúcsosodni. Képzeljük el azt a lehetőséget, amikor képessé válunk önállóan új célokat kijelölni a fegyverzetnek, repülőgépeknek akkor is ha nincs várakozási idő új központi csapás tervezési ciklusra, amely megváltoztathatná a célelosztás prioritását.

A tevékenységek középpontjában a hálózat nyújtotta képesség döntő szerepet játszik. A hálózat nyújtotta képességet erő sokszorozóként kell felfogni. A Millennium Challenge 2002. az USA tengerészgyalogság által végrehajtott összhaderőnemi gyakorlat azt bizonyította, hogy a hálózatba kapcsolt erők következetesen legyőzték a háromszoros túlerőben levő ellenfelet. **A konklúzió szöges ellentétben áll, ellentmond a jelenlegi erő-eszköz számvetési gyakorlatnak, azaz többet érhetünk el kevesebb erővel.** A hálózat centrikus képesség amerikai források szerint nem korlátozódik kimondottan csak az információfeldolgozásba bevont elemekre. Szerves egységként magába foglalja a korábban elkülönítve kezelt összes tradicionális katonai területet, amelyet jó amerikai szokás szerint DOTMLPF akronimként aposztrofálnak. A 4. sz. ábra magyarázattal szolgál a mozaikszó tartalmára.

Hiba! A mezők szerkesztésével nem hozhatók létre objektumok.

4. sz. ábra A képesség amerikai felfogása

A hálózat nyújtotta képesség óriási lehetőségeket rejtve mutatkozik be. A NATO-ban elvezet minket egy sokkal hatékonyabb NRF-hez, amely a konfliktus teljes spektrumában sokkal nagyobb hatékonysággal képes kezelni a fenyegetéseket.

Ha gondosan végiggondoljuk - az említett modell alapján a hálózat centrikus megközelítés néhány alapkövével, (információs főlény, tudásfőlény, döntésfőlény, eredményesség alapú végrehajtás) megismerkedve – az új filozófia követelményeit, megállapíthatjuk, hogy a hálózat nyújtotta képesség messze nem csak információs technológiai, hanem annál sokkal messzebbre mutató fájdalmas következményekkel járó komplex átalakulás. Meg kell változtatni szervezeteket és a működést. A hagyományos szervezetek ideje lejárt, le kell váltani őket „hálózatos struktúrákkal”, amelyek nagyobb rugalmasságot, oldalirányú kapcsolatokat, a szervezeti határokon túlnyúló együttműködést biztosítanak. Ez az igazi kihívás!

A NATO is magáévá tette, átvette azokat az elveket, amelyek elvezettek az USA által meghatározott hálózat centrikus hadviselés elveihez. Ezek az elvek teljes

mértékben azonosak. Ezek mindegyike egymásra épülve drámaian fokozza a küldetés hatékonyságát:

- Egy erőteljesen hálózatosított erő, fokozza az információ megosztást;
- Az információmegosztás és az együttműködés erősíti az információ minőségét és a megosztott helyzetképet;
- A megosztott helyzetkép lehetővé teszi az önszinkronizációt.

3./ A NATO C3 Board felelős szakmai szerveinek tevékenysége

A NATO szakmai, technológiai tevékenysége sokkal korábban kezdődött és valószínűleg hatással volt a Katonai Bizottság ösztönzésére is. 2002. novemberében az NC3B felismerte egy NATO NNEC koncepció kialakításának szükségességét. Kilenc ország, nevezetesen Kanada, Franciaország, Németország, Olaszország, Hollandia, Norvégia, Spanyolország, Egyesült Királyság és az Egyesült Államok részvételével (2004.-ben csatlakozott Törökország és Belgium is) megkezdődött az NC3B égisze alatt a felkészülés, hogy nemzeti erőforrásokból pénzalapot hozzanak létre egy NNEC tanulmány finanszírozására. 2003. novemberében a nevezett kilenc ország egyetértési nyilatkozatot írt alá, amely eredményeként 2004. januárjában megkezdődött egy megvalósíthatósági tanulmány kidolgozása, amelynek elvégzésével az NC3A lett megbízva.

A tanulmány menedzselésére egy operatív bizottság került felállításra, amely harmonizálta a koordinációt a nemzetek, valamint az olyan érintett NATO testületek között, mint az ACT, ACO, CNAD és a NACMO. A tanulmány célja, hogy kialakítsa az NNEC funkcionális területét és jövőképét, valamint kimutassa a szükséges összefüggéseket - NATO terminológiával élve - az NNEC C3 aspektusai között. Az NCW vagy NNEC kérdésének kezelésére egy "NEC Capability Team" azaz NEC Képességcsoport került felállításra a NHQC3STAFF állományában. A Katonai Bizottság felkérte az NHQC3STAFF vezetőjét az NC3B és az ACT nevében egy tájékoztató megtartására 2004. év februárjában, aminek következményeként a Katonai Bizottság döntést hozott az NNEC feletti felelősség átvételére, mivel világosan megértette, hogy egy ilyen koncepció a katonai műveletek minden aspektusára kihatással van. A Katonai Bizottság megbízta az ACT-ot, hogy alakítsa ki a koncepciót, mivel az ACT alapvető rendeltetéséből adódóan a legjobb helyzetben van egy minden katonai aspektust figyelembe vevő koncepció kidolgozására. A Katonai Bizottság elismerte, hogy az idevonatkozó C3 kérdéseket érintően az NC3B-e a vezető szerep.

Röviden tekintsük át milyen NNEC-el kapcsolatos tevékenység folyik az NC3O égisze alatt. Rögtön az elején megállapíthatjuk, hogy a koncepció kidolgozása az egy dolog, a koncepció alkalmazása és a valós képesség kifejlesztése az egy másik dolog, talán a legfontosabb kérdés. Leszögezhetjük, hogy a C3, még pontosabban a híradó és informatikai rendszer szempontjából az információs technológia és a híradó és informatikai rendszer a meghatározó az NNEC és a hálózatközpontú műveletek számára. Híradó és informatikai rendszer nélkül nem lehet semmiféle NNEC koncepciót megvalósítani.

Az első említésre méltó projekt, az úgynevezett Overarching CIS Architecture kifejlesztése volt. Ez az architektúra hadműveleti, rendszer és technikai perspektívából legmagasabb szinten írja le, hogy milyen NATO és a nemzeti CIS rendszerek szükségességek, amelyek összeegyeztethetők a NATO vezetésre - irányításra és konzultációra vonatkozó igényével. Arra tervezték, hogy keretet adjon a NATO finanszírozta rend-

szerek referencia architektúráinak tervezéséhez és lehetővé tegyék a nemzetek számára, hogy NATO kompatibilis rendszereket fejlesszenek ki. Ezt a projektet az NC3B kezdeményezte, az NC3 képviselők, valamint az NHQC3S állománya közösen fejlesztette ki, és az NC3A hajtotta végre.

A jelenlegi tevékenység arra összpontosít, hogy hogyan illessze össze az NRF követelményeket, és úgy tervezzük, hogy a küszöbönálló, eljövendő továbbfejlesztése átfogja majd az NNEC aspektusait, mihelyt azok ismertté, lehetségessé válnak.

Az NHQC3S állományába tartozó „Architecture and Interoperability Branch” keretei között folyik a „Joint CIS Concept for NNEC” kezdeményezés kidolgozása. Ez a koncepció hivatott meghatározni az összhaderőnemi kapcsolatok rendszerét és azok információcsere követelményét hálózat centrikus műveletekre. Meghatározza az összeköttetésekre, információval történő ellátásra és az információ kivonására vonatkozó követelményeket és szabványokat, így módon nyújtva segítséget a nemzetek számára, hogy kifejlesszék és integrálják a nemzeti hálózat nyújtotta képességet a NATO keretébe. Amennyiben a koncepció elkészül valószínűleg szabványosítási eljárás alá vetik. A fejlesztés beillesztésre kerül az „NC3B Joint Concepts and Requirements Sub-committee” munkaprogramja közé.

A létező kriptográfiai termékek legnagyobb hiányossága talán nem meglepő módon az interoperabilitás hiánya. Az INFOSEC Sub-Committee, amely az elmúlt évben egyfolytában ezen az alapvető kérdésen dolgozott, egy Norvégia által kezelt kriptográfiai munkaterv alapján alapegyezményt ért el, úgy a NATO-ban, mint koalíciós környezetben egyaránt alkalmazható újgenerációs interoperábilis fejlesztés számára. Ez az alapegyezmény magába foglalja például a NATO és a partnerek szabványos kriptográfiai és kulcsmenedzsment algoritmusait. Ezt az alapegyezményt követően az INFOSEC Sub-Committee elindította a Kriptográfiai Modernizálási Kezdeményezés elnevezésű programját megcélózva a következő tevékenységeket:

- A NATO követelmények meghatározása, harmonizálása és priorizálása az újgenerációs kriptográfiai termékek számára, amelyek interoperábilisak és kiadhatók a partnerek részére
- A nemzeti kriptográfiai programok harmonizálása, amelyeket olyan kezdeményezések számára indítottak, mint az NCW vagy NNEC és a TACOMS Post-2000

Az információvédelem anomáliáit a következő fejezetben részletesen kifejtem.

Az NC3-Technikai Architektúra (a továbbiakban NC3TA) biztosítja a szükséges iránymutatást és technikai komponenseket a NATO CIS fejlesztések támogatására azzal a céllal, hogy:

- a technikai iránymutatás elsődleges forrásaként szolgáljon a NATO CIS projektekhez és;
- nyomonkövesse a technológiai fejlődést.

Előre látva, de anélkül, hogy az NNEC tanulmány végső megállapításait befolylásolnák az NC3TA 6.0 verzió már tartalmazza:

- a legújabb architektúra modellt és;
- már összegezte a Web Szolgáltatás technológiát, valamint;
- már számos Web szolgáltatás szabványt azonosított.

Az NC3TA fejlesztésének vezető testülete a NATO NC3B Információs Rendszerek Albizottságának, Nyílt Rendszerek Munkacsoportja. Az NC3TA naprakészségének tartása során különös tekintettel ügyelnek arra, hogy a polgári fejlesztésekkel összhangban legyenek és figyelembe veszik az NC3B, valamint a CNAD alrendszeréből érkező észrevételeket. Az NC3TA frissítése évente történik. Az NC3TA-t ADatP-34 formátumban tartják, amelyből a 6. verzió jelenleg nemzeti jóváhagyás alatt van.

Az Összhaderőnemi C3 Információcsere Adatmodell (a továbbiakban JC3IEDM) - a Multilaterális Interoperabilitási Programmal (a továbbiakban MIP) és a NATO Adat Adminisztrációs Csoporttal (a továbbiakban NDAG) együttműködésben lesz kifejlesztve. A JC3IEDM célja minden szinten kezdve a hadtesttől a zászlóaljig, illetve a megfelelő legalacsonyabb szintig a vezetési - irányítási információs rendszerek szemantikai interoperabilitásának elérése, hogy támogassák a többnemzetiségű, illetve NATO többnemzetiségű összhaderőnemi műveleteket. A jövőben ez a modell lesz az NNEC meghatározó eleme. A vezető testület ebben az együttműködésben az NDAG. A MIP és az NDAG egyetértési memorandumot írtak alá az együttműködés érdekében ez év februárjában. A két csoport most egy közös úgynevezett MIP-NDAG Adatmodellezési Munkacsoportban dolgozik együtt és jelenleg analizálják a MIP C2IEDM v6.1 és a NATO 4.0-ás Referencia Modelljét azaz a JC3IEDM első verzióját. A két csoport a modellt két éves tervezési ciklusra alapozva fogja kifejleszteni.

Az eXtensible Mark-up Language (XML) - egy metanyelv, amely az adatról strukturális és szemantikus információt ír le – polgári technológiát használó rendszerek közötti magasabb szintű interoperabilitás elérése érdekében eszközöket biztosít. Az XML-t ezért lehetséges tényezőként veszik figyelembe az NNEC fejlesztésénél. Azzal a céllal, hogy közvetlen általános menedzsment útmutatást biztosítsanak, az Information Systems Sub-Committee irányelvet és direktívát dolgozott ki a NATO-ban az XML regisztrációs menedzsmentre, amelyet az NC3B jóváhagyott. Ezzel párhuzamosan az Information Systems Sub-Committee most tekinti át az XML webes környezetben történő használatára vonatkozó további NATO irányelv szükségességét.

Az NNEC fényében megállapíthatjuk, hogy felfokozott hadművelleti követelmény fog napvilágot látni a CIS rendszereken keresztül történő információcserére vonatkozóan. A követelmény, hogy támogassuk a nagy bevethetőségű erőket, amelyeknek már alapvetően nagy frekvencia és sávzsélesség igényük van előreláthatóan növekedni fog az összetételüknek és a feladatuknak köszönhetően. A frekvenciáknak rendelkezésre kell állni, és használhatónak kell lenni bármikor és bárhol. Ezért a bevethető CIS erőket támogató rádiófrekvencia menedzsment eljárásait és elveit ki kell dolgozni. A NATO Frequency Management Sub-Committee éppen most tekinti át a már létező Combined Joint Task Force, NATO Response Force és az Early Entry Forces számos szintjének irányelveit és dokumentumait azzal a céllal, hogy analizálja a spektrummenedzsment következtetéseit. A cél az, hogy minden spektrummenedzsment lehetőséget és követelményt egyetlen átfogó integrált koncepcióban dolgozzanak ki.

Most nézzük át a berendezésekkel kapcsolatos tevékenységeket. Először a harcászati kommunikációt a TACOM Post 2000-t (a továbbiakban TP2K). A tagállamok harcászati kommunikációs hálózatai csak korlátozott mértékben interoperábilisak. Egy projekt csoport került felállításra, hogy ezzel a kérdéssel foglalkozzon. Ebből alakult ki a TP2K szervezet, úgy, ahogy ma is van. Magába foglalja 13 nemzet prog-

ramirodáját egy vállalkozóval (TACONE). Az a céljuk, hogy STANAG-et bocsássa ki, amely növeli a szárazföldi harcászati rendszerek interoperabilitását. Mint ilyen az NNEC számára fontossággal bír. Az alapító szervezetek formálják a TP2K International Project Office-t (Párizs), egy Felsőszintű Irányító Csoport által felügyelve. A STANAG-ek kibocsájtója a vállalkozó, a TACONE. A TP2K végeredményét a NATO nemzetekkel történő koordinálás céljából átadják a Communications Systems Sub-Committee-nek. A NATO jelenleg aktívan bevonásra került a TP2K projektbe, miután részt vett annak 16. ülésén. A 13 nemzet egyetértett abban, hogy a NATO az elkövetkezőkben is részt vehet az üléseken. Az eredményt, amely STANAG-ekből fog állni 2004/2005.-ben fogják átadni jóváhagyás és ratifikálás céljából a NATO-nak. Az már most előrelátható, hogy az ezzel kapcsolatos munkát a Communications Systems Sub-Committee és alárendelt struktúrája nem képes elvégezni és kiegészítő forrásokra, illetve szervezeti változásokra van szükség. A jóváhagyáson és ratifikáláson túlmenően a prototípus kialakítására és tesztelésére is figyelmet kell fordítani.

Napjainkban a NATO és a NATO nemzetek különböző hálózatokat (civil/katonai) használnak. Az alkalmazott és alkalmazásra felajánlott kriptó berendezések nem mindig, igazán szólva alig interoperábilisek. A SCIP - Secure Communications Interoperability Protocol – egy projekt NATO neve, amely szándéka szerint azon van, hogy interoperábilis titkosító végberendezést biztosítson ennek a problémának a megoldására. Így az NNEC látókörében fontos szerepe lehet. A project az USA FNBDT programjára alapoz (Future Narrow Band Digital Terminal). Magába foglalja a jelzésátvitelt, a kriptó-grafikus protokollt, amely a megkövetelt interoperabilitást biztosítja. A NATO ki fogja fejleszteni az FNBDT szabványokon alapuló SCIP jelzésátviteli és kriptográfiai szabványok sorozatát.

4./ Az NNEC megvalósíthatósági tanulmány

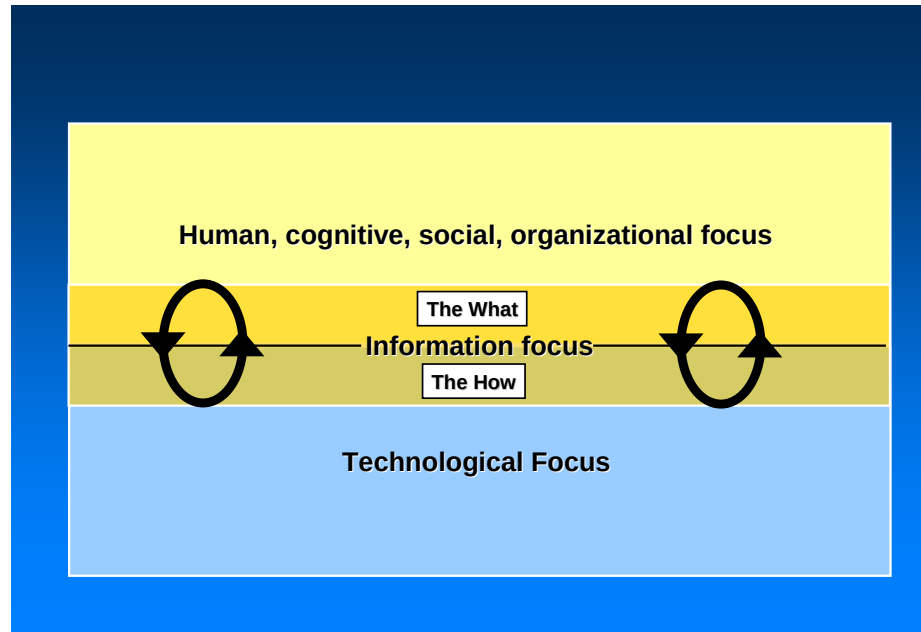
Mint korábban már említettem az NC3B égisze alatt az NC3A 11 nemzet által finanszírozott NNEC megvalósíthatósági tanulmány elvégzését rendelte meg. A tanulmányt készítő csoportot Tom Buckman az NC3A főmérnöke vezeti, aki az NCW, illetve NNEC koncepció jelenleg az egész világon elismert három szaktekintélyének egyike. A következőkben a tanulmány eddigi megállapításainak rövid kivonatát kívánom ismertetni. Azzal a céllal, hogy egy általános tartalmi összefüggést alakítsunk ki az NNEC számára kezdjük egy megállapítással, amely az NC3A-nál megkezdett tanulmány előszavában található.

„NATO Hálózat Nyújtotta Képesség - Network Enabled Capability (NEC) - egy a kulcsfontosságú koncepciók közül, amely a NATO átalakítás középpontjában áll. Sokkal inkább emberekről, szervezetekről és új sokkal dinamikusabb, rugalmasabb, hatékonyabb módon együttműködésre képessé tett nemzetekről szól, mint technológiáról. Mégis technológia, amely az információt nagy sebességgel, a szükséges bőséggel biztosítja, amely lehetővé teszi, hogy az átalakulás megtörténjen. Alapvető természete folytán az NEC és az Átalakítás sokkal inkább egy utazásról szól, mintsem egy végállomásról. Egy utazásról, ahol a szervezeti és technológiai innovációnak és változásnak az átalakulás érdekében kéz a kézben kell együttműködni.”

Az NC3A hajtja végre az NC3B által szponzorált tanulmány elkészítését. Fontosnak tartom megemlíteni, hogy az NNEC sokkal inkább emberekről, szervezetekről és országokról mintsem technológiáról szól. Azonban mégis csak a technológia felhasználása is, hogy nagyobb bőséggel, eléréssel és sebességgel információt biztosít-

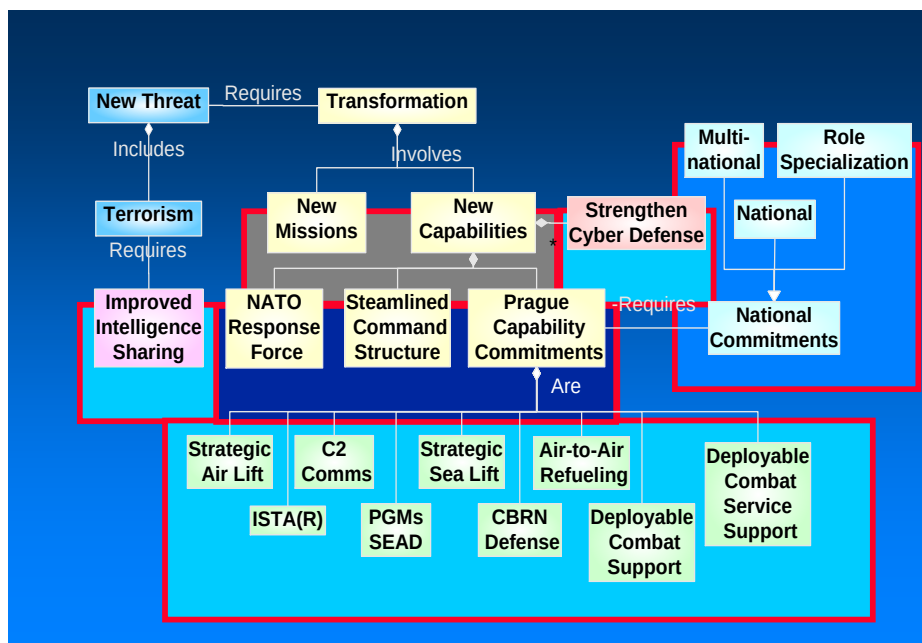
ának a felhasználó számára, mint ahogy az alapvető fontosságú a hálózat centrikus műveleti képességek megvalósításában. Mint azt a megállapítás sugallja két alapvetően fontos aspektusa van a tanulmány kidolgozásának.

Először is vannak az NNEC-nek humán, kognitív, társadalmi és szervezeti aspektusai, valamint van a technológia, a híradó és informatikai rendszer. Van valami közös, amin mindketten megosztóznak és ez nem más, mint az információ. A dolgok humán oldaláról az a kérdés merül fel, hogy milyen információt akarunk, milyen információra van szükségünk, illetve milyen szeretnénk, hogy végrehajthassuk a feladatunkat. Az 5. sz. ábra mutatja be a kettő viszonyát, ahogy Tom Buckman azt prezentálta.



5. sz. ábra Az NNEC humán és technológiai oldalának viszonya az információhoz

A technológia oldaláról viszont azt kérdezhetjük magunktól, hogyan biztosítuk a megfelelő információt a megfelelő embernek a megfelelő időben és a megfelelő helyen. Fontos, hogy lássuk az információs követelmények hálózat centrikus műveletekre vonatkozó „milyen és hogyan” változatainak kialakulását. Az ideális szituáció az lenne, amikor a műveletekben jártas személy az információfeldolgozásban jártas személlyel közösen alakítaná ki a hadművelet információs igényének „milyen és hogyan” alkotóelemeit.



6. sz. ábra A Buckman féle NNEC összefüggések

Ez a párbeszéd különböző módon megtörténhet kezdve a katonai műveletektől a gyakorlatokon keresztül a levont tanulságokat feldolgozó tevékenységig úgy, hogy a mérnököket és végrehajtókat egy terembe gyűjtjük, hogy közösen gondolkozzanak egy feladatterv fölött. A fontos az, hogy ezt a tevékenységet ne hagyományosan követelmény specifikus, rendszerszállító szemszögből nézzük, ahol megkérik a hadműveleti embert, hogy írja le a követelményeit, és a mérnökök fogják ezeket, és elmennek megoldást találni az igényre. Ez a hagyományos lineáris modell kialakítás – amerikai zsargonnal „vizesés” megközelítés –egyszerűen nem tudja szállítani az igényelt megoldást.

Az 6. sz. ábrán látható diagram kiinduló pontja annak a képességnek a megértéséhez, amelyet hálózatközpontú képességnek nevezünk. Ez a koncepció diagram lefedi a legtöbb alapvető gondolatot, amely az államfők Prágai Csúcsértekezletét követően megjelent deklaráció tartalmaz. Megállapításaikban úgy összegezték az Átalakítást, mint új küldetést, új tagországokat, a partnerekkel való új kapcsolatot magába foglaló folyamatot. Ez a diagram a NATO átalakítás új küldetésére és az új képességek szempontjaira fókuszál. Ezek azok a képességek, amelyek azoknak az új küldetéseknek a támogatásához szükségesek, amelyeket hálózat nyújtottnak tekintünk.

Sokkal pontosabban kifejezve ez magába foglalja a NATO modernizált vezetési struktúrája alatt működő - a Prágai Képesség hozzájárulásban kiemelt - képességek birtokában levő jövő NRF-jét. Ha egy lépéssel előre megyünk, eljutunk azokhoz a platformhoz és képességfajtákhoz, amelyek még világos képet adnak az elképzelt műveletekről. Hangsúlyozni kell az új információforrások kritikus fontosságát, különösen a hírszerzés terén, valamint a jövőbeni kibernetikus képességeink védelmének alapvető fontosságát. Nem engedhetjük meg magunknak, hogy olyan információs

rendszerre támaszkodjunk, amit nem védünk, vagy nem bízunk meg benne. Végezetül számolnunk kell a ténnyel, hogy át kell alakítani azt az utat és módot, ahogy a jelenlegi képességeket kialakítjuk, és ahogy az érintettet ellátjuk vele. Sokat tehetünk a prototípus és kísérleti tevékenységgel, de amit fenntartható átalakításnak hívnak, az a régi falak lerombolását igényli. Mint ahogy már az előzőekben említésre került a lineáris fejlesztési modell a továbbiakban nem tartható.

5./ Az NNEC információvédelmi kihívásai

Az NNEC koncepció realizálásának egyik legellentmondásosabb területe az információvédelem. Nem könnyíti a koncepció kezelését az a tény, hogy információvédelmi berkekben még elfogadott definíciója sincs az NNEC-nek. Ezért a jelenlegi állás szerint az információvédelem egy integrált, méretezhető és teljes mértékben telepíthető híradó és informatikai rendszer keretein belül marad, amely a szövetséget konzultációs, vezetési és irányítási rendszerrel látja el.

Számos változás tapasztalható, hogyan hajtják végre napjainkban a katonai műveleteket, amelyek óriási hatással vannak az információvédelemre. Három markáns területre hívom fel a figyelmet:

- **A koalíciós környezet.** A katonai műveletek rendszerint a szövetség – azaz a NATO vezetésével mentek végbe, míg ellenben most rendszerint egy Szövetség (vagy a NATO vagy az EU), illetve egy nemzet (pl. az USA) viseli a vezető szerepet, vezeti a műveleteket, amelyek mind kihatással vannak a biztonsági irányelvekre, valamint a védett információ és védett technológia kiadására különös tekintettel a partnerekre;
- **A katonai erők összetétele.** A múltban a katonai műveletek olyan nagyságrendű nemzeti erők kompozíciójával kerültek végrehajtásra, mint a hadtest és a hadosztály. Napjainkban a nemzeti hozzájárulás észrevehetően változó és a formációk ezred, zászlóalj és nem ritkán alacsonyabb szinteket érnek el. Ennek nyilvánvaló hatása van a biztonságos interoperabilitásra, amelyet a vezetési irányítási lánc mentén ki kell nyújtani;
- **Az iram és szinkronizáció.** Ha megnézzük a jelenlegi iraki műveletet, könnyen felismerhetjük, hogy a múlttal összehasonlítva miként nőtt meg a műveletek irama és a szinkronizációja egy teljesen összhaderőnemi környezetben végrehajtott művelet során. Ezt szintén súlyosbítja az tény, hogy biztonságos interoperabilitást ilyen körülmények között - még ha polgári technológiát alkalmaznának is egy integrált, méretezhető, teljes mértékben telepített híradó és informatikai rendszer esetében, ahol bármilyen erő-hozzájárulás korlátozás nélkül „plug in” módon bekapcsolható lehet, anélkül hogy nyomást gyakorolnánk az adott nemzetre, hogy feleljen meg specifikus szabványoknak - egyáltalán nem könnyű elérni.

Egy integrált, méretezhető, teljes mértékben kitelepített híradó és informatikai rendszerben a hadműveleti és információcsere követelményeket a következő tényezők határozzák meg:

- az összekapcsolandó, de különböző klasszifikációs szinten levő hálózatok technikai topológiája;
- a biztonsági irányelvek és az információcsere megvalósító felhasználó szervezetek és érdekközösségek biztonsági szintjei;

- a cserére kerülő információ érzékenysége;
- a hálózatok földrajzi elhelyezkedése;
- a hálózatok mérete;
- a rendelkezésre álló idő, beleértve a technikai és adminisztratív szempontok elvégzését, mint pl. a földrajzilag széttagolt hálózat akkreditációja.

Kétségtelenül az interoperabilitás az egyik legnagyobb kihívás, amellyel ma szembesülünk. Az integrált, méretezhető, teljes mértékben telepített híradó és informatikai rendszer koalíciós környezetben még súlyosbítja is a jelenleg alig megoldott helyzetet. Amikor a biztonság interoperabilitásáról beszélünk a következő korlátokkal szembesülünk:

- különböző biztonsági irányelvek, úgy NATO, nemzeti, mint EU. Például a jelenlegi irányelvek nem engedik meg a Szövetségen belül használt kriptográfiai termékek kibocsátását a Szövetség területén kívülre;
- fejlett nemzeti technológiák kiadásának nemzeti irányelvek által történő tilalma;
- különböző technológiák használata található meg harcászati szinten, - kezdve az analógtól a Voice over IP-ig, ISDN, MSE vagy EUROCOM szabványokon továbbítva – és amelyek úgynevezett „vörös gateway-eket” igényelnek, hogy együttműködjenek.

Egy integrált, méretezhető, teljes mértékben telepített híradó és informatikai rendszer esetén - koalíciós környezetben - az összekapcsolt rendszerek biztonsági profilja lehet, hogy uniformizálható. Három fő figyelembe veendő kérdés merül fel:

- minden hálózatnak van egy sebezhetőségi foka és egy hálózat által elfogadott kockázat minden más hálózatra ugyanazzal a biztonsági kockázattal jár;
- vannak szigorú követelmények a különböző klasszifikációs szinteken levő (koalíciós és nem kormányzati) hálózatok összekapcsolására, valamint különösen koalíciós környezetben, különböző megbízhatósági szinten levő (NATO és partner nemzetek) hálózatokra;
- a földrajzilag széttagolt dinamikus hálózatok összekapcsolásának akkreditációja. Az akkreditáció ma egy formális állandó eljárás, ami nagyon dinamikus környezetben nem biztosítható.

A biztonságos információcsere a hálózat centrikus környezet alapvető tárgya. Az információ sokrétű formában, tartalommal, kategóriával lesz jelen és a rögtön rendelkezésre álló információ teljes méretét a szó szoros értelmében lehetetlen mennyiségileg meghatározni. Vegyünk számba néhányat az alapvető kérdések közül:

- hogy biztosítani tudjuk a tárolt, feldolgozott, és hálózaton keresztül továbbított információ bizalmasságát, sértetlenségét és rendelkezésre állását, az információ menedzsment élettartamával összefüggésben minimum olyan alapelvek meglétére van szükség, mint a tulajdonjog, az érzékenység, elszámoltathatóság, valamint a „szükséges, hogy tudja” elv;
- az információ megosztási szabályokat és eljárásokat minden szervezeten belül világosan meg kell határozni;
- az olyan technikai kérdéseket, mint a megbízható hozzáférés ellenőrzés és a hitelesítés meg kell oldani.

Amikor a biztonságos információcseréről beszélünk nem mehetünk el amellett, hogy néhány nem közvetlen információvédelmi kérdést ne érintsünk.

Az első az információ biztonsága. A jelenlegi információbiztonság mind irányelv, mind megvalósítási direktíva értelemben:

- papírientelt. Szabályok és eljárások az elektronikus környezetre nincsenek;
- nehezen megvalósítható a NATO vezette CJTF-ban.

Ráadásul a valós probléma az, hogy NATO-nak nincs Információ Menedzsment irányelve és nincs megvalósítási direktívája, útmutatási dokumentációja. Az INFOSEC közösségnek nincs egyetlen bázisa sem, amelyen ellenrendszabályokat foganatosítana, a saját védelme érdekében, valamint a biztonságos információterítésre. Az információ teljes élettartamát lefedő világos szabályok és eljárások nélkül hálózat centrikus környezetben az információcsere teljes biztonsággal az információ engedély nélküli kiáramlásához vezet.

Most pedig pár példán keresztül nézzük meg milyen kulturális változásra van szükség ezen a területen. Az első példán keresztül az INFOSEC – t általában gátnak tartják, hogy egy fontos feladatnak megfeleljen. Ebben a sajátos esetben az interoperabilitási feladatnak. Van, aki arra a következtetésre juthat, hogy amennyiben új technológiákat alkalmazunk információvédelmi korlátok nélkül, máris elértük az interoperabilitást. Természetesen ez a megközelítés teljes mértékben hibás. Erre nézve Augusto Pistoia ezredes az NHQC3STAFF Információvédelmi Osztály vezetője, egyben az NC3B Információvédelmi Albizottság elnöke azt mondta:

„Senki sem fog egy harckocsiba Ferrari motort beépíteni, amely vitathatatlanul a legjobb, leggyorsabb és technológiailag legfejlettebb a világon. Ehelyett felállítanak egy csoportot, amely kiegyensúlyozott módon kialakítja egy tank fejlesztési tervét, legkevesebb szem előtt tartva a motort, a harckocsi súlyát és alakját, a fegyverrendszerét, valamint az aktív és passzív védelem mértékét. Ugyanezt az elvet kell alkalmazni a hálózatainkban is. **Az INFOSEC többé már nem egy fekete doboz, amelyet már egy korábban kiválasztott technikai megoldáshoz hozzáadhatnak. Meg kell állítani a „kályhacső fazonú” tervezést, amelyben az egyik közösség tervezi a kommunikációs rendszert, a másik az információs rendszert és még egy másik az információvédelmi rendszert.**” Ezt neveztük korábban lineáris fejlesztési modellnek.

A másik példa az összhaderőnemi követelményekből fakadóan szimpatikus lehet, azonban nagyon félrevezető. Kétségtelen, hogy a hálózat centrikus környezetben az információmegosztás egy közös helyzetkép érdekében elvitathatatlan fontosságú követelmény. Napjainkig viszont a „need-to-know” elv alapján korlátoztuk az információhoz történő hozzáférést. Az információmegosztásnak azonban ennek nem a „need-to-know” elv szab gátat. Az információmegosztás és a need-to-know” elv nincsenek egymással konfliktusban. Amit meg akarnak velem osztani az a minden, amit tudnom kell. Az igazi probléma az, hogy a NATO-nak nincs Információ Menedzsment Irányelve és információmenedzsment eszköze, lehetővé téve a felhasználónak, hogy kreálja vagy azonosítsa, vagy kiválassza az információt, amit meg akar osztani.

6. Összegzés

Az NNEC kivonatos, általános ismertetését, valamint az összhaderőnemi követelmények teljesítésével kapcsolatos szakmai tevékenységek rövid leírását próbáltam

átnyújtani a híradó és informatikai közösségnek. Szándékom volt amellet, hogy a NATO-ban folytatott erőfeszítésekre rámutassak, egy látens kérdés felvetése, nevezetesen: Nem kellene már ebben az ügyben valamit kezdeményeznünk? Remélem a szakmai körökben az NNEC terület rövidesen részletesebben feldolgozásra kerül és erős szakma tevékenység veszi kezdetét.

A 2,5 G ÉS AZ UMTS 3. GENERÁCIÓS MOBIL SZOLGÁLTATÁS INFORMÁCIÓ BIZTONSÁGI FELADATAI

Bevezetés

A digitális technika gyakorlati alkalmazása évtizedeken keresztül a műszer és irányítástechnika valamint a számítástechnika területére korlátozódott. Ennek egyszerűen az anyagtechnológia viszonylagos fejletlenségének volt betudható.

A telekommunikáció számára – természetesen – készen álltak az elméleti megvalósítási formák, mint például az impulzus kód moduláció, vagy a digitális adatátvitel számos más matematikai megoldásai, viszont a rendelkezésre álló fizikai hordozók nem voltak képesek megfelelő szintű hatásfokkal az elméletet gyakorlattá váltani. A hetvenes évek végétől a technológiában fokozatosan bekövetkező fejlődések eredményeként forradalmi változások álltak be mind a lapkákra történő integrálhatóság, mind pedig a az adathordozók terén. Ezzel a kezdetleges néhány MHz-es frekvenciákról át lehetett térni a több száz illetve több ezer MHz-es átvitelekre és közel zaj mentes sáv-szélességekre.

Ez tette lehetővé, hogy az első generációs analóg átviteleket felválthatták a digitális jeltovábbítások. A digitális adatátvitel a műszaki lehetőségek egész tárházát sorakoztatta fel. Ezek közé tartozott többek között a második generációs digitális hírközlés, közismert nevén a GSM rendszer. A laboratóriumi és a gyakorlati teszt eredmények műszakilag biztatóak voltak, viszont költséges üzemeltetése miatt az elemzők az első időben inkább státusz szimbólumnak ítélték, sem mint tömeges fogyasztási cikknek. Az első GSM rendszer megjelenésétől jó néhány év telt el míg a penetráció robbanásszerűen megváltozott. Ez alapvetően két dolognak volt köszönhető:

- Egyrészt a szolgáltatók belátták, hogy rendszereik működtetése során általános költségeik, melyek a penetrációtól függetlenül megvannak, jóval magasabbak, mint az üzemi költségeik.
- Másrészt a készüléktámogatásos kínálat illetve a pre-pay ajánlatok rövid idő alatt ugrás szerűen megnövelték a keresletet.

A '90-es évek második felétől néhány év leforgása alatt a második generációs GSM rendszer alkalmazása soha nem prognosztizált penetrációt eredményezett. E tapasztalatok feldolgozása és napjainkra kibővült szolgáltatások tárházára alapozva vizsgálom meg az UMTS jövőbeli lehetőségeit.

A telekommunikációs piac és az UMTS jelenlegi és várható jövőbeli helye

Az UMTS-hez (Universal Mobile Telecommunications System), a harmadik generációs műszaki megoldáshoz fűzik mindazokat a reményeket amelyek képesek lesznek kielégíteni minden olyan igényeket, melyekkel már a 2G rendszerek esetében is bevezetésre kerültek, viszont a kapott eredmény nem vagy alig közelítette meg az integrált telekommunikációs igények elvárásait.

Ahhoz, hogy a tartalomszolgáltatás piaci vizsgálatát, valamint az integrált telekommunikáció alakulását vizsgálni lehessen, rendszerezni kell a műszaki gazdasági trendek alakulását az elmúlt évekre vonatkoztatva.

Műszaki irányvonalak:

Néhány évvel ezelőtt mikor az UMTS rendszerek gyakorlati megvalósíthatósága reális közelségnek tűnt, számos fejlesztő és szolgáltató cég fogott hozzá az új technológiai rendszerek fejlesztéséhez. Azonban a 3G-be vetett kezdeti innovatív lelkesedés több gyártó és szolgáltatónál megtorpant. Rövid idő leforgása alatt két fő irány rajzolódt ki:

- az egyik a meglévő mobil rendszereken alapuló tovább fejlesztett változatok, ezek a ma 2,5 vagy 2,75G jelű EDGE rendszerek,
- míg a másik egy merőben új, a korábbtól technikailag is eltérő rendszerében is újszerű távközlési hálózat bevezetése. (Nagyon fontos piaci hátránya, hogy hálózatan más, pl. GSM rendszer nem üzemelhet, tehát ma, ha valaki UMTS-t akar használni, akkor egy GSM készüléket is magánál kell, hogy hordjaon.

Természetesen mindkét irányzat célkitűzésében ugyan azok az alapelvek kerültek meghatározásra, amelyeket korábban a 2G rendszerek esetében már felmerültek. Ezek közé tartoztak a:

- integrált telekommunikáció,
- mobil computer alkalmazás (RAS, GPRS),
- integrált handset-ek,
- multi funkciós média eszközök,
- bővített, széleskörű ipari alkalmazhatóság (helymeghatározások, regisztrációk, speciális adatbázisokkal történő kommunikációk, stb.)

A két műszaki megoldás fejlesztési területe – első sorban a technológiai területeken – ugyanazokat a specifikumokat írta elő, ezek, pedig az alábbiak voltak:

- nagy sebességű és tárhatalmú processzorok fejlesztése, (2002-ben és 2003-ban az Intel és az AMD egymást túlszárnyalva léptek elő a 200 és 220 MHz-es processzorokkal, míg a múlt év végén az Intel zinte minden típusú igényt kielégítő processzorát mutatta be, melynek sebességét már a 320MHz-es órajele határozta meg. Egyéb paraméterei pedig teljesen megfelelnek mind a két műszaki irányelvek elvárásainak.)
- egységesített, globális szabványok alkalmazása,

Ugyanakkor a két fejlesztési irány számos pontjában el is tér egymástól. Ezeket az alábbiak szerint lehet csoportosítani:

A 2G (2,75G) rendszerek fejlesztési koncepciója:

- Kiaknázni a meglévő távközlő rendszerekben rejlő kapacitásokat;
 - Növelni az átviteli sebességet,
 - Törekedni a rendelkezésre álló spektrumok teljes kihasználására.
- Olyan új típusú processzorok kifejlesztése, melyek képesek a fenti sebességek biztosítására.
- Viszonylag alacsony ráfordítással biztosítani az alapcél megvalósítását.

A 3G UMTS rendszerek fejlesztési koncepciója:

- Kiaknázni a technológiai rendszerek nyújtotta valódi szélessávú átviteli lehetőségeket,
- Habár a merőben új technológia költséges új átviteli hálózat kiépítését igényli, jövőbeli megtérülése minden bizonnyal garantált hiszen ezek az eszközök már nem csak a földi jel továbbításban, hanem a műholdas rendszerekben is

továbbítani képesek. Ezzel teremtve meg a szélessávban működő univerzális jelfeldolgozás és hírközlés teljes kiépítettségét.

A műszaki fejlesztések és a korszerű gyártástechnológiai kapacitások már évek óta nem korlátozzák az igények kielégítésének. A továbbiakban a az egyes műszaki megoldások keresleti-kínálati trendjének nemzetközi piacon való alakulásával foglalkozom.

Az egyes műszaki generációs irányelvek alakulása és várható trendjeik

A nemzetközi trend alakulásával számos szakcikk foglalkozik melyeket az alábbiak szerint lehet csoportosítani:

- Az UMTS hálózatok kiépítése és a hálózatok üzemeltetése az operátorok számára 200 és 2002 között nem hozta azt a fogyasztói penetrációt, ami alapján a további beruházások indoltak lettek volna, (Hazánkban is látva a nemzetközi piaci kereslet pangását a 2002-re tervezett licence kiírást elhalasztották 2004-re)
- A hálózatok tovább építése, a rendszer elemek fejlesztése, gyártása csak nagy fokú globális integrációkkal vált lehetségessé. Néhány példa az elmúlt évek konzorciumai közül:
 - Motorola-Simens készülék gyártás,
 - Fujitsu-Sagem technológiai fejlesztés,
 - Ericson-Texas technológiai fejlesztés,
 - NEC-Simens együttműködés,
 - IBM-AT&T-Intel teljes együttműködés,
- Néhány cég, akik egyedül próbálták hálózataik kiépítését megvalósítani, mint pl. a német Mobilcom vagy a finn Sonera súlyos adósság állományt halmoztak fel. Ugyanakkor voltak olyan a telekommunikációs piac nagyjai közé tartozó, mint például a japán NTT DoCoMo vagy a norvég Telenor – az ingyenes állam által felajánlott licence ellenére is - látva a piac nehéz mozgását, inkább kivárt.
- Mindkét generációs rendszer bevezetését tovább nehezíti a mobil piac mélyrepülése, melynek két magyarázata lehet:
 - a GSM annak ellenére, hogy nem szélessávú szolgáltatás, bőven rendelkezik annyi kapacitással, hogy az általános fogyasztói körben nem tartják indokoltnak az UMTS-ből eredő többlet költség megfizetését,
 - a másik, hogy a penetráció lassan telítődik és mindössze kb. 900 millió új előfizetőt prognosztizálnak a következő évekre.
- Piac elemzők prognózisai a korábbi elemzésekhez képest 2003-as vizsgálataikban már korábbra teszik az UMTS megtérülésének várható idejét.

A továbbiakban az ismertetett piaci viszonyok és a stratégiai megfontolások mellett működő biztonsági elveket foglalom össze.

Biztonsági alapelvek a 2.75 és 3G rendszerek bevezetése során

Mindenek előtt ki kell jelteni, hogy a műszaki technikai fejlettség korszerű technológiai megvalósításai nem generálnak merőben új biztonsági feltételrendszereket. Ugyanakkor viszont két alapvető elem jövőbeli alakulásával kell foglalkozni, ezek az alábbiak:

- Védelmi rendszerek sebezhetőségének felderítése, új típusú védelmi rendszerek kialakítása,

-
- A fejlett technológia sajátos eszközrendszeréből adódó bővített védelmi felkészítések rendszere.

Az első gondolat arra terjed ki, hogy az adat és információ biztonságot rendszerező szabványok és előírások mellett a szándékos támadó mindig újabb és újabb eljárásokkal törekszik célja elérésére.

A másodikban azokat az új típusú fenyegető kockázati elemeket kell számba venni, amelyek az új generációs telekommunikáció kiépítettsége és más egyéb adottságai miatt alaphelyzetben jelen lehetnek. A meghatározó modulokat Porter stratégiai elvei alapján lehet rendszerezni:

- Szállítói modul
- A szolgáltatásokat igénybe vevők rendszerhasználati vonzereje,
- A támadó szándékúak belépési korlátai
- A legkülönbözőbb szolgáltatók telekommunikációs rendszereinek transzparens átjárhatósága.
- Az új típusú szolgáltatók műszaki rendszereinek biztonsági és védelmi elveinek kialakítása, ennek pedig meg kell felelni a hármas alapkövetelménynek:
 - Biztonságosság,
 - Sérthetlenség
 - Rendelkezésre állás.

A teljes rendszer alapelveit az alábbiak szerint lehet csoportosítani:

- Stratégiai feltételek
 - Vállalati adottságok,
 - A menedzsment stratégiai elvei.
Ebbe a kérdéskörbe tartoznak a kiemelt vállalatok kettős funkciójának kezelése. Ez a gazdálkodó szervek piaci funkciója és a biztonsági fenyegetettséget kezelni képes megítélések rendje.
 - Környezeti hatások
 - Társadalmi viszonyok
 - Törvények és rendeletek rendszere
 - Jogsabályok,
 - Szabványok,
 - Működési szabályok
- Biztonság stratégiai feltételek
 - Objektumi feltételek
 - Védelmi rendszerek és szabályzók rendje,
 - A védelem személyi feltételei
 - Humán rendszerek
 - Törvényi elvárások,
 - A gazdálkodó szerv biztonsági személyi feltételei
 - Személyi adottságok
 - Folyamatszervezési feltételek
 - Adatvédelem (titok védelem, ahol arra szükség van),
 - Információ kezelés biztonsági aspektusai,
 - Műveleti elvek, szabályzatok, stb.
 - Biztonság szervezési elvek:

-
- A biztonsági szervezeti egység helye a gazdálkodó szervezetben belül:
 - Hatáskör
 - Méretgazdaságosság,
 - Funkcionális megosztás
 - Biztonsági stratégiai menedzsment a cél meghatározástól a tervezésen át, a végrehajtási elvek meghatározásán keresztül az eredmények kiértékeléséig illetve a szükséges korrekciók bevezetéséig.

Összességében tehát a biztonsági alapelveket egy olyan koordináta-rendszerbe kell elképzelni, amelynek egyik tengelyére transzformáljuk a már bevezetett és szabályzókkal koordinált fenyegetettségeket (X tengely), a másik tengelyre kerülhetnek az új kockázati tényezők (Y tengely) és a harmadik tengelyre a kockázati tényezők általános fenyegetettségét lehet skálázni. A skála mértékeket súly értékekkel lehet meghatározni. E témakör részletezésére más publikációmban fogok kitérni, a módszer lényege, hogy segíthet a biztonsági stratégia kialakításában.

Befejezés

A 2.75 és 3G biztonsági stratégiáinak meghatározásához nem azért van szükség megkülönböztetett új elvekre, mert a már jól bevált szabványok nem tudnák lefedni az elvárt igényeket, hanem azért mert gyarapodnak az elkövetők tapasztalatai és az új technológia új sebezhetőségeket is tartalmazhat. Ami viszont lassúbb változáson megy keresztül azok a szervezési alapelvek, mint

- a célmeghatározás,
- a szervezési, tervezési, elemzési lépések,
- kockázatanalízis.

A KAPCSOLAT MEGSZAKADT... REPÜLŐTRAGÉDIA EGY PSZICHOLÓGUS SZEMÉVEL

MH Kapos Bázisrepülőtér (MH KBRT)

Bizonyára mindannyian találkoztunk már azzal az igen bosszantó jelenséggel, amikor felemeljük a telefonkagylót - hogy valami igen fontos dolgot közöljünk a szeretteinkkel – és ahelyett, hogy rögtön belevágnánk a tárcsázásba csak sistergést hallunk a vonal túlsó végén. Még bosszantóbb az a helyzet, ami minden év utolsó napján megtörténik velünk, amikor a szilveszteri káoszban, az év legeslegutolsó perceiben szeretnénk boldog új évet kívánni barátainknak és ismerőseinknek. Hosszú percekig nem tudunk velük kapcsolatot teremteni. Ezek azonban csak egyszerű, ámbár felettébb idegesítő hétköznapi szituációk, melyek próbára teszik türelmünket.

Mi történik azonban egy olyan helyzetben, ha a kapcsolat megszakadása a másik oldallal nem egy jelentéktelen hétköznapi szituációban történik, hanem egy éles, emberéleteket is kockára tevő helyzetben?

*„20 óra 9 perc: az összeköttetés még megvan a másik irányítóponttal
20 óra 28 perckor fordulnak a cél mögé*

.

.

20 óra 31. 35 perckor a céltávolság 1. 5 km

20 óra 31. 36 perckor: összeütközés...”

(TOP GUN 1996/10)

Előadásomban a fent idézett repülőtragédiát szeretném pszichológus szemmel bemutatni, mely pár évvel ezelőtt minden repülős szakember életét felkavarta.

Az általam feldolgozott eset 1995 szeptemberében történt. Az MH Légvédelmi Parancsnoksága módszertani repülést tervezett, melynek célja a „légtér és szabálysértő repülőgépek elleni tevékenység begyakorlása éjjel, vizuális elfogással”. A téma azért lehetett aktuális, mert az ICAO szigorú előírásokat rögzített a polgári légi járművek ellen foganatosítható rendszabályokkal kapcsolatosan, és előírta azok jelzéseit.

A feladat végrehajtására az intézkedés szerint az alakulatok legképzettebb hajózó-állományát kellett kiválasztani. A célrepülő szerepére SZU-22M3 és AN-26 típusú repülőgépeket jelöltek ki. Az elfogó gépek szerepére pedig MIG-21UM, MIG-23UM és MIG-29UB típusok kerültek kiválasztásra. Ezek közül egyedül a MIG-29UB volt képes hőpellengátorral kedvező időjárási viszonyok között felderíteni a célt.

A feladat végrehajtása előtt összevont felkészülésen és eligazításon vettek részt a feladatot végrehajtók Veszprém-ben, ahol ismertették velük a módszertani repülés tárgyát. Ezt a fajta feladatot a rendelkezésre álló repülőgépekkel lokátor nélkül rendkívül nehéz volt végrehajtani. Akik már valaha is részt vettek hasonló feladatban, azok tudták, hogy a repülőgép személyzetének igen korlátozott lehetőségei vannak az oktató típusból a légi célok felderítésére még nappal is, nem beszélve arról, hogy ezt a feladatot éjszaka kellett végrehajtatniuk a pilótákkal.

A másik problémát az jelentette számukra emlékeik szerint, hogy nem volt összevont felkészülés a hajózó állománnyal, tehát személyre menően nem volt lehetőség a

feladat átbeszélésére és a közös felkészülésre. Egy speciális feladat végrehajtását nagymértékben megkönnyíti a személyes kontaktus és annak lehetősége, hogy a repülés folyamán az összes számításba jöhető szituáció átbeszélésére van lehetőség még a repülés megkezdése előtt. A közös felkészülés egy ilyen feladat végrehajtása előtt kiemelt jelentőségű, mert így a résztvevők tudják, hogy ki van az adott hívószám mögött, megismerhetik a repülőgép-vezetők képzettségét, felkészültségét, váratlan helyzetekre való reagálását és ez nagyon fontos körülmény volt. A feladat pontos átbeszélése valószínűleg megkönnyítette volna a feladat végrehajtását, hiszen a gyakorlat kritikusabb pontjainak átbeszélése, a közös gondolkodás elmélyítése, az elméleti begyakorlás pszichés szempontból kiemelkedő jelentőségű. Hétköznapi helyzetekben is nagyon fontos számunkra, hogy félelmeinket és aggályainkat megosszuk a másik emberrel, ugyanilyen fontosságú lett volna az említett gyakorlat esetében is. A együtt eltöltött idő hatására könnyebben fel tudtak volna készülni a váratlan helyzetekre (bár tudjuk, hogy nem lehet mindenre felkészülni), mégis jobban megismerték volna egymást, a másik reakcióit és munkamódját, vélekedését a feladatról. Kiszámíthatóbbá váltak volna a váratlan szituációk, mely megnöveli a belső biztonság érzetét, csökkenti a vélt vagy valós szorongásokat a feladattal kapcsolatban, növeli a koncentrálóképességet, összpontosíthatóbbá teszi a figyelmet, így a katonák energiája a feladatra orientálódik, nem pedig a belső feszültségre. A Top Gun 1996/10 számának erről az esetről szóló cikke utal az egyik életét vesztett pilóta lelki állapotára. A pilóta ugyanis zaklatottan hívta fel a gyakorlat előtt a vadászirányító megfigyelőt, hogy legyenek nagyon figyelmesek. Pedig azelőtt nem tett ilyet. Szorongásokkal a lelkében, stresszes és feszült állapotban ült be gépébe. Természetesen a stressznek is van egy egészséges mértéke, amely még serkenti teljesítményünket, de ha elhatalmasodik az emberen, akkor teljesítménye romlani kezd, a hirtelen döntést kívánó helyzetben pedig bizonytalanná válik.

Az ilyen és ehhez hasonló veszélyes gyakorlatok előtt nagyon fontos lenne a közös konzultáció, illetve pszichológus szakember segítsége. Világhírű sportolóink már évek óta pszichológus segítségével készülnek fel a fontosabb versenyekre, ami segít nekik a koncentrálásban és a feszültség oldásában. Az eredményekre pedig –valljuk be őszintén – büszkéek lehetünk. A Magyar Honvédség keretein belül is kiválóan lehetne alkalmazni a sportolóknál már bevált pszichológiai eszközöket, de ez napjainkban sajnos csak kis mértékben valósul meg.

Visszatérve történetünkre, a gyakorlat kezdetére következőképpen emlékszik vissza az akkor szolgálatban lévő harcálláspont parancsnok:

„Hozzákezdünk. Az első kört nappal csináltuk, jó látási viszonyok között. Csak arra kellett odafigyelnem, hogy megfelelő oldalra vezessem ki a repülőgépet, hogy az esti lemenő napsugarak ne szemben legyenek, hanem a cél felé világítsanak. Megfelelő irányon és távolságon átadtam a helyettesemnek (továbbiakban B) az elfogót a végső megközelítéshez és a cél elfogásához, azonosításához.

Az első kört sikeresen megcsináltuk, nem volt semmi gond. Következett az éjszakai sorozat.

20 óra 31 perc és 20 óra 31 perc 36 mp: az útvonalazó jelenti, hogy leállt a hajtóműve! Abban a pillanatban felkaptam a mikrofont és jelentését követően azonnal utasítottam a katapultálásra. A repülési magassága 2450 m volt.

*Rögtön beszóltam a hangosba és utasítottam B-t, hogy azonnal válassza ki az elfogót, de már hallottam is a rádión, hogy azonnal kifordította az elfogót, amely északi irányra fordult és elkezdett emelkedni. Furcsa volt, hogy **nem igazolt vissza**, csak végrehajtotta a parancsot.”*

A történet vége azt hiszem mindenki számára ismert, melyben a korabeli sajtó elég negatív fényben igyekezett feltüntetni a két szárazföldről irányító katonát.

*„Ekkor belémnyilalt valami, csak nem? **Miért is nem rádiózt?** Hallott engem, hiszen a parancsot végrehajtotta, hallotta B-t, hiszen megkezdte az emelkedést is. **ÜTKÖZTEK VOLNA?** De hát a SZU-22 pilótája nem jelentette, pedig tudott rádiózni, csak azt mondta, leállt a hajtóműve, nem mondta, hogy ütköztek, pedig, ha így volt, azt észre kellett vennie!!!*

*Hibáztunk? Hibázhattunk? Hibázhattam? Valamit nem vettem észre? Valamit kihagytam a számításból? Tudott vajon **rádiózni** a másik gépszemélyzet? Vagy csak hallották, amit mondtunk nekik, vagy nem is hallottak semmit és esetleg sebesülten, sérült géppel vonszolták magukat hazafelé, amíg a technika vagy az ember fel nem adta? De hát már ott voltak! Már csak 8 km választotta el őket a biztonságos földtől! **Miért nem jelentette a gép pilótája, hogy ütköztek? Tehettem volna ennél többet? Volt egy - két álmatlan éjszákám. Többször végiggondoltam, újra éltem az egészet. Tudtam, hogy az adott helyzetben a legjobban cselekedtünk, és nem követtünk el hibát.”***

A repülőgépen lévő személyzet pszichés állapotát mindannyian el tudjuk képzelni. Ők maguk azonban már nem tudnak nyilatkozni az eseményekről. Óriási hibát követnénk el azonban akkor, ha egy ilyen embert próbáló szituációban megfedkeznenk a másik oldalról. Hogyan élték meg a tragédiát azok a tapasztalt és jól képzett katonák, akiknek a szárazföldről, a „vonal másik végéről” kellett átélniük - a repülőgépekkel tartott kapcsolat megszakadása miatt -, ahogy az általuk irányított gépek balesetet szenvedtek.

A történet felidézése - még a mai napig, tíz év távlatából is - mindannyiuk számára megterhelő dolog. Átélni a tehetetlenség érzését, a káoszt, a pánikhelyzetet, amelyben gyorsan és hideg fejjel kellett másodpercek alatt komoly döntéseket hozni, minden halandó embert próbára tenne.

Az ilyen és ehhez hasonló traumák átélése hihetetlen módon megterheli az egészséges ember lelkét. Sokszor csak hetekkel a tragédia után tudjuk felfogni azt, mi is történt valójában. Gyakran találkozom kollégákkal, akik pár hónap elteltével jelzik, hogy már feldolgozták a velük történt megrázó eseményeket, mégis beszámolnak arról, hogy a történetek, a katasztrófa kínos pillanatai visszatérő álmokként zaklatják őket. Freud szerint az álmainkban olyan képeink és emlékeink kerülnek előtérbe, amelyek túl fájdalmasak vagy bűntudat-ébresztők ahhoz, hogy tudatosan szembenézzünk velük. Vagyis a trauma, a tragédia képei még mindig mélyen foglalkoztatják őket. Benne vannak mindennapjaikban, csökkentik koncentrációs képességüket, munkaképességüket, zavarják pihenésüket. Gyakran olyan mindennapi panaszokkal jelentkeznek, mint egy egyszerű, de egyre gyakrabban visszatérő fejfájás, alvászavarok, hirtelen vérnyomás-emelkedés, -ingadozás, gyomorbántalmak, jelentős mértékű fogyás vagy éppen súlygyarapodás. „Katona dolog”, mondhatnánk. De mi munkálkodik vajon a

hátterben? – leginkább akkor merül fel ez a kérdés, mikor az összes orvos szétjárja a karját, és tűnődik a negatív leleteken, holott a tünetek egyértelműek.

A pszichológiában létezik az úgynevezett poszttraumás stressz szindróma (PTSD), mely a vietnami háború után vált igazán elfogadott diagnosztikus kategóriává. Az Egyesült Államok Tisztiorvosi Hivatala szerint a veteránok 15%-a szenvedett leszerelés után PTSD-ben, illetve a hozzá kapcsolódó alkalmazkodási zavarban. Ehhez a betegséghez gyakran kapcsolódik alkoholizmus, kábítószer-élvezet, erőszakosság valamint magánéleti problémák. A Vietnámban harcolt katonák, mint tudjuk, túlságosan fiatalok voltak, egyes kutatások szerint az átlagéletkoruk alig haladta meg a 19 évet. Számukra a háborús körülmények szokatlanok voltak: nem voltak világosak a frontvonalak, a támadások sorrendje és időszerűsége bejósolhatatlan volt, ami az emberi pszichét igencsak megterheli.

Még egy nagyon érdekes jelenséget tartok fontosnak kiemelni itt. A pszichológiában használt tanult tehetetlenség fogalma ebben a helyzetben is igen meghatározó lehetett. A jelenség lényege abban rejlik, hogy állatkísérletek kapcsán kimutatták, hogy ha a kísérleti állat nem tudta bejósolni előre a vele történő negatív dolgokat, egy idő után fásulttá és kiegétté vált. Elvesztette képességét az ön maga feletti kontroll gyakorlására, elfogadta a számára kedvezőtlen helyzetet még akkor is, ha semmi nem akadályozta meg, hogy ellene tegyen. – Gondoljunk mélyen bele! Látunk ilyen eseteket saját környezetünkben? Biztosan. Vannak olyan vietnámi veteránok, akik mind a mai napig átélnek emlékeikben vagy álmaikban a traumatikus és tragikus élményeiket. Az egyik veterán így vélekedik erről: „A történelem szerint már vége a háborúnak. Számomra azonban sosem ér véget!”

A poszttraumás stressz szindróma gyakori tüneteit észlelték magukon az általam említett katasztrófa résztvevői is, azonban nem tudtak mihez kezdeni vele, hisz segítséget nem kaptak a trauma feldolgozásában. Vajon kinek a felelőssége az ellátatlanság? És vajon hogy vélekedett volna az irányítók környezete tudván, hogy pszichológiai segítséget kapnak? „Egy katona nem panaszkodik! Egy katona erős, problémáktól mentes!” – ezek a gondolatok dominálnak. De meddig? Gondolkodásmódunk megváltoztatása közös felelősségünk és lehetőségünk! Ők egyedül dolgozták fel a történeteket, pedig akár segítséget is kaphattak volna.

Egy súlyos trauma, vagy esemény után a következő tüneteket észlelhetjük magunkon, vagy akár barátainkon és munkatársainkon:

- **Nem tudjuk elfelejteni a történeteket** (ami egyébként érthető és természetes)
 - a traumás eseményre való kényszerű, ismétlődő, szenvedést okozó visszaemlékezés: minden gondolatunk a történetek körül forog, és akárhogy próbáljuk is kikapcsolni állandóan dolgozó elménket, mindig ott motoszkálnak a negatív képek a fejünkben.
 - az eseményről való álmodás: mindannyiunk számára nagyon fontos a pihentető alvás. Álmainkban azonban a megtörtént események újra és újra előtérbe kerülnek, ezáltal zavarják pihenésünket.
 - pszichés szenvedés és vegetatív tünetek a traumás élményt szimbolizáló vagy arra emlékeztető aktuális helyzetekben
- **Tagadjuk**

- a traumával összefüggő ingerek, a traumához kapcsolódó gondolatok, emlékek és érzések kerülése, esetleg visszaemlékezési képtelenség

- **Rosszkedv, levertség**

- csökkent válaszkészség, lecsökkent érdeklődés és részvétel fontos tevékenységekben: munkahelyi feladatainkat egy ilyen levert és melankolikus állapotban kevésbé tudjuk ellátni, és családjunk is egyre többször zsörtölődik velünk, hogy valami nincs rendben mostanában

- **Túlzott éberség**

- fokozott készenlét tünetei, alvászavar, felfokozott élnkség, koncentrációs zavarok: akárhogy is próbáljuk azonban leplezni idegességünket, nem mindig sikerül

- **Bűntudat**

- gyakori bűntudat az életben maradás miatt, illetve amiatt, amit életben maradásukért tettek a krízishelyzetben: olyan helyzetek után alakul ki, amikor saját életünk is valamilyen formában kockára volt téve. Ilyenkor gyakran foglalkoztatja az embert, a „mi lett volna ha...?” kérdése, amely gyakorlatilag csak a bűntudatunkat és szorongásunkat növeli.

A felépülés időtartamát is több tényező befolyásolja:

- **Személyes megküzdési képességek, tapasztalatok**

Akik korábban már kénytelenek voltak szembenézni feszült helyzetekkel, valószínűleg gyorsabban alkalmazkodnak az újabb szélsőséges helyzethez. Életünkben mindannyiunknak számos stresszkeltő és szorongással teli eseményt kell átélnie. Ezek a tragédiák, bár megrázóak és sokszor nehezen feldolgozhatóak, mégis növelik abbéli képességeinket, hogy a későbbiekben felmerülő problémákkal könnyebben megbirkózzunk. Növelik megküzdési stratégiáink számát, hiszen vissza tudunk emlékezni arra, hogy a múltban, egy hasonló helyzetben hogyan cselekedtünk, mi az, aminek volt haszna és segített a probléma megoldásában, és melyek voltak azok a tényezők, amik gátolták a felépülést és az események feldolgozását.

- **Az átélt stressz és veszteség intenzitása, mértéke**

Azok az események, amelyek hosszabb ideig tartanak, és nagyobb fenyegetettséget jelentenek, sokkal hosszabb feldolgozási folyamatot igényelnek.

A poszttraumás stressz betegséget azonban sokan nem ismerik fel, pedig mindannyian átéljük enyhébb, vagy fokozott tünetképződéssel járó fajtáit. Gondoljunk csak arra, mit élünk meg egy-egy szeretett családtagunk, barátunk, egy számunkra fontos eszme, közösség elvesztése esetén, és a mai világban, akármennyire is fejlett és modern gondolkodásúnak tartjuk magunkat, mégsem fordulunk szakemberhez segítségért. Az általam említett tragikus helyzetben valószínűleg senkinek sem jutott eszébe az az igen fontos tényező, hogy a traumát átélőket pszichológushoz vagy pszichiáterhez irányítsák. Akármennyire is rettegünk attól, hogy félelmeinket és szorongásainkat megosszuk egy idegennel, nagyon sokszor egy súlyosabb helyzet kialakulását előzhetjük meg vele.

A Top Gun (1996/10) egyik cikke, mely ezzel a tragédiával foglalkozik, a következő kérdéseket és problémákat veti fel:

- „Egyáltalán nem törvényszerű, hogy két repülőgép-vezető ugyanazon a frekvencián tud **pszichikailag ráhangolódni** a feladat különleges jellegé-

re. Ezért befolyásolhatják egymást, ami erősítheti, de gyengítheti is a rendelkezésükre álló információ helyes értékelését!

- Ennek következményeként torzul, bizonytalanná válik a helyes **döntés** meghozatala, a felelősség sem tudatosodik teljes mértékben, mert ketten vannak, számitanak egymásra, ezáltal hibák csúsznak a tevékenység helyes sorrendiségébe, ami az előírt repülési rezsím megsértéséhez vezethet.”

A cikk szerzője rávilágít egy nagyon fontos kérdésre. Ez pedig a döntés, s a döntés meghozatalának nehézsége. Hétköznapi szituációkban gyakran egy igen egyszerű kérdésen is órákig törjük a fejünket, és nem biztos, hogy valóban a legjobb döntés születik. Éles szituációban ez a folyamat megnyúlhat, és a pszichés terheltség miatt nehezebbé válhat az, hogy tisztán lássuk a dolgokat. Hogyan hozunk tehát döntést pánikhelyzetben? Mi is jellemzi valójában a pánikot?

Igen széles spektrumon mozognak azok a tünetek, melyek a pánikroham velejárói. A legfontosabb komponense talán a félelem, melybe beletartoznak konkrét, vagy szimbolikus félelmeink, mint például: félelem a haláltól, a világvégétől, a megőrüléstől, az ájulástól, az ismeretlentől és sorolhatnánk még. Ugyanakkor a zavarodottság, a szétesettség - érzése, irrealitásérzés, a realitáskontroll elvesztése, szédülés, izzadás és ingerlékenység szintén gyakori jelenségek. Egy ilyen, tünetekben gazdag helyzetben hogyan vagyunk képesek egyáltalán tisztán gondolkodni? Képesek vagyunk-e egyáltalán a korrekt és megfelelő ítéletalkotásra. A következő tényezők igen komoly hatással lehetnek döntési folyamatainkra:

- **Fáradtság:**

Az elhúzódó válság halmozott terhelést jelent és emiatt sokszor csak a "döntésért születik döntés". Az elhúzódó, nagy megterhelést jelentő döntési folyamat dühöt, rosszindulatot válthat ki. A meghozott ítéletünket általában felülrétékeljük és minden erőnkkel védeni próbáljuk a bírálatokkal szemben. Festinger elmélete is ezt támasztja alá: ha már meghoztuk a döntésünket, legyen az akármilyen jó vagy rossz, utána már csak olyan érveket veszünk figyelembe, melyek azokat alátámasztják.- hiszen a „mi gyereink”. Johnston, Driskell és Salas (1997) vizsgálatukban arra hívják fel a figyelmet, hogy a figyelem túlzott mértéke, azaz a "nagyon éber" döntési stílus alkalmazása jobb döntési eredményhez vezetett, mint a simán "éber döntési stílus" alkalmazása. Ez azt mutatja, hogy még extrém helyzetekben is lehetséges jó döntéseket hozni, és a túlzott figyelem valamint a stressz nem vezetnek feltétlenül az alternatívák figyelmen kívül hagyásához és kognitív leegyszerűsítésekhez. Fontos kiemelnünk, hogy a stressznek kettős hatása van teljesítményünkre: egyrészt fokozza készségünket, koncentrációnkat, másrészt szorongást kelt bennünk, visszavetve, megbénítva teljesítményünket, így döntési folyamatainkat is. Természetesen ez is több tényezőn áll: szerepet játszanak benne az egyéni különbségek, a kellemetlen ingerek erőssége és az is, hogy az adott szituációt mennyire tartjuk veszélyesnek.

- **Sok közül nehéz választani**

Legtöbbször a szituáció kétértelműsége és nem súlyossága határozza meg a döntés nehézségi fokát. Azonban nagy egyéni különbségek vannak abban a tekintetben, hogy egy adott embert mennyire befolyásolnak a különböző alternatívák, illetve képes-e őket egyáltalán figyelembe venni. Az erkölcs, a jónak és rossznak az ismerete csak nehezíti a helyes út megtalálását, mivel szűkíti az intellektualitás meghatározó szere-

pét. A tisztán racionális döntés ezért akkor lehetséges, ha a döntéshozó nem rendelkezik semmilyen erkölcsi értékkel és ugyanakkor fizikailag nem kimerült, nem frusztrált. Ugyanakkor a mély erkölcsi meggyőződés roppant megviselő lehet bizonyos helyzetekben. Mint Wiegler megjegyzi, előfordulhat, hogy háborús körülmények között jelentkező válságszituációk kevésbé megterhelők, mint a béke idején folytatott diplomáciai manőverezés, ugyanis a hadi események gyakran saját logikájukat követik. Ennek alapján a tényleges háborút megelőző helyzetek sokkal inkább megterhelik a döntéshozók fizikai és pszichológiai erejét.

- **Csoportos döntést kell hozni**

Mivel a lényeges döntések esetében a végső döntés megszületése lényegében csoportos vita eredménye, fontos a csoporton belüli vélemények megoszlásának mikéntje. A csoportgondolkodás tünetének pszichológiai leírásából ismert, hogy a döntést jelentősen eltorzíthatja, ha a csoporttagok többsége egy véleményt képvisel, illetve ha az ellentétes álláspontok kifejtése az erős vezető illetve a többiekhez való erős alkalmazkodási kényszer miatt akadályozott. Wiegler azonban arra hívja fel a figyelmet, hogy a csoporton belüli túlzottan nagy ellentét jelentős stresszt jelenthet a csoportvezető számára.

- **Nem szabad gyengének látszani**

Egy olyan hierarchiára épülő szervezetben, mint a hadsereg, elengedhetetlen az, hogy a vezető szerepet betöltő egyének magabiztosságot sugalljanak akkor is, amikor nincsenek éppen a helyzet magaslatán.

- **Az információval mindig baj van**

Az idők folyamán egyre több információval vagyunk kénytelenek szembesülni. Ez azt eredményezi, hogy a helyzet összetettségének növekedésével egyre intenzívebbé válik az átélt feszültség. Inzana, Driskell, Salas és Johnston (1997) azt találták, hogy egy stresszes helyzetet megelőzően kapott felkészítő információ jelentősen csökkentette az átélt stressz intenzitását. Gondoljunk csak vissza gyermekkori emlékeinkre, amikor anyukánk elvitt minket az orvoshoz, hogy a kötelező védőoltásokat megkapjuk. Vagy idézzük fel első élményünket, amikor fogorvosnál jártunk. Sokkal könnyebben elviseltük a fájdalmat, ha a szüleink felkészítették rá, hogy bizony nem csupa kellemes dolog érhet minket egy fogorvosi székben. Természetesen ez az eredmény a kiszámíthatatlan helyzetekre nehezen alkalmazható, mégis felhívja a figyelmet arra, hogy az információ előkészítő, strukturáló szerepe adott esetben csökkentheti a feszültséget elősegítve így az optimális döntéshozatalt.

Térjünk vissza az előadás elején felvázolt esetre!

Mivel 1995 szeptemberében vélhetően megszakadt a kapcsolat a repülő személyzet és a szárazföld között, nem tudhatjuk, hogy a levegőben feladatot teljesítő személyzet milyen döntéseket hozhatott. Volt-e egyáltalán idejük döntést hozni. Ha végiggondoljuk az általam felsorolt tényezőket, melyek egy pánikhelyzetben jelentkezhetnek, nem volt könnyű feladatuk a levegőben a megfelelő döntés kialakítására. Azt azonban tudjuk, hogy a szárazföldi irányítók a feladat nehézsége ellenére is mindig a leggyorsabb és leghelyesebb módon jártak el. Döntéseikben mindenféleképpen közrejátszott az is, hogy az évek során igen nagy tapasztalatra tettek szert a különböző repülési feladatok végrehajtása révén.

Mi is tehát a tanulság ebből az esetből egy pszichológus szemével nézve? Gyakran adódnak életünkben olyan helyzetek, melyekre valamilyen oknál fogva nem tudunk

felkészülni. Előfordulhat, hogy hibázunk, hiszen emberek vagyunk, nem vagyunk tökéletesek, de ballépéseinkből tanulhatunk is. Egy-egy tragikus esemény után azonban ne szégyeljük szakember segítségét kérni. Nem az a gyenge ember, aki felvállalja az őt nyomasztó problémákat, aki mer beszélni gondjairól és érzéseiről, hanem aki titkolja és szégyenkezik miatta. Problémái márpedig mindannyiunknak vannak. És ez így természetes! El kell fogadnunk, hogy vannak szorongással teli szituációk az életünkben, és fel kell vállalni azt, hogy egyes dolgok igenis mélyen érintenek bennünket. Talán a Magyar Honvédség is némi idő elteltével felfedezi a pszichológusokban rejlő lehetőséget, és ha esetleg felmerül egy hasonlóan megrázó baleset, mint amit én is példaként felhoztam, lesz a traumát átélőknek szakszerű segítsége.

Mi, emberek, a híradás, a kommunikáció fejlődésével, a mobiltelefonok világába belekényelmesedve nem felejthetjük el azt az igen bölcs közmondást, mely szerint „ami el tud romlani, az el is romlik”. Jól tudjuk, hogy vészhelyzetek mindig voltak, vannak és lesznek. Azt gondoljuk, hogy a civilizáció fejlődésével egyre nagyobb biztonságban érezhetjük magunkat, pedig ha jobban belegondolunk, számos veszélyes helyzetet teremtenek számunkra a fejlődő technika csodái.

Irodalomjegyzék:

- [1] Rita L. Atkinson – Richard C. Atkinson – Edward E. Smith – Daryl J. Bem: Pszichológia (Osiris, Budapest, 1995.)
- [2] Dr. Barlai Róbert – Kővágó György: Válság- (katasztrófa) kommunikáció (Petit Reál Könyvkiadó, Budapest, 1996.)
- [3] Shirley Trickett: Csak semmi pánik (Park Könyvkiadó, Budapest, 1995.)
- [4] Sigmund Freud: Álomfejtés (Helikon Kiadó, Szekszárd, 2000.)
- [5] Stephen Barlay: Légikatasztrófák (Széchenyi Nyomda Kft., Győr, 1990.)
- [6] Stephen Barlay: Fekete doboz (K. u. K. Kiadó, Kaposvár, 1996.)
- [7] Háty György: Repülők, Műszerek, Emberek (Műszaki Könyvkiadó, Budapest, 1990.)
- [8] Farkas Gábor – Lajtai János: Székesfehérvár repüléstörténete (Dunatáj Kiadó Kft., Dunaujváros, 1997.)
- [9] John Peters – John Nichol: Tornado század (Borsodi Nyomda Kft.)
- [10] TOP GUN 1996/10 szám
- [11] TOP GUN 1999/4
- [12] Aranyas 2004/1

CYBER WARFARE – VALÓBAN KORSZERŰ KIHÍVÁS A HADERŐKKEL SZEMBEN

Dr. Ványa László okl. mk. alezredes
Zrínyi Miklós Nemzetvédelmi Egyetem, Elektronikai hadviselés tanszék
1101 Budapest, Hungária krt. 9-11.
E-mail: vlaci@zmne.hu

Bevezetés

Az emberiség történelmében mindig fontos szerepet játszott a háború, mint a hatalomért folytatott küzdelem eszköze. Minden kor állama arra törekedett, hogy a rendelkezésére álló legkorszerűbb technikai eszközökkel lássa el a hadseregét, és nemcsak létszámban, de technikailag is fölénybe kerüljön az ellenség felett. Különösen az elmúlt száz évre igaz, hogy a hadviselő felek igyekeztek a tudomány legújabb vívmányait minél előbb hadrendbe állítani, sőt a tudományos kutatás nagy része egyenesen a hadseregek érdekében, a hadseregek megrendelésére folyt, az új és még újabb fegyverek kifejlesztésére irányult. Nincs ez másképpen az információs korban sem, amikor a világ fejlett országai már az információs társadalom létrehozásán dolgoznak. Jelen írás azt kívánja felvázolni, hogy milyen hatással lesz (sőt már van) a legfejlettebb információtechnológia a hadviselésre, milyen új kihívásokkal kell szembenézni a cyber-kor hadseregének, milyen új megoldások várhatók.

A hadviselés színtérének változása az emberiség történelme során

A háborúk történetét vizsgálva végigkövethetjük azt a folyamatot, ahogy fejlődtek a haderők, korszerűsödtek a haditechnikai eszközök, és mintegy ezek következményeként egyre szélesedett a hadműveletek megvívására szolgáló tér. Az 1. ábrán az egyes korok hadviselésének színtereit láthatjuk.

	Ókor	Középkor	Újkor	Legújabb kor
Szárazföldi hadszíntér	●	●	●	●
Tengeri hadszíntér	●	●	●	●
Légi hadszíntér			●	●
Világűr				●
Elektromágneses spektrum			●	●
Cyber-tér				●

1. ábra. A hadviselés színtereinek változása a történelem folyamán

A szárazföldi-, a tengeri-, a légi hadszíntér és a világűr nem igényel különösebb magyarázatot, azonban a két utolsó sornál álljunk meg egy pillanatra.

Az elektromágneses spektrum hadszíntérként való besorolása egyesekben néha még mindig megütközést kelt. Pedig ha belegondolunk, a huszadik század hajnalán megalkotott rádiók, majd a második világháborúban már kulcsszerepet játszó radarok megjelenésük pillanatától gyökeresen megváltoztatták a hadviselést.

A rádiók a katonai vezetés nélkülözhetetlen eszközévé váltak. A jelek, jelzések, közlemények és minden, amit az elektromágneses hullámok „képére” át lehetett formálni fénysebességgel tették meg az utat, leküzdvé a távolságot és nagymértékben kiváltva a kábelek nehézkes és sérülékeny hálózatát. A rádióhírközlés a megjelenését követően igen rövid idő alatt a támadások egyik legfontosabb célpontjává is vált.

A rádiólehallgatással és rádióbeméréssel a sugárzott közlemények tartalmát, valamint a rádióadók helyét is meg tudták határozni, majd csapást tudtak mérni rájuk. A rádióadások zavarására kifejlesztett speciális zavaróadókkal meg tudták nehezíteni, vagy akár teljesen lehetetlenné tudták tenni a forgalmazást. Megkezdődött a rádióháború.

A radarok olyan légi, földi és tengeri felderítési képességeket jelentettek a hadseregeknek, amelyekkel korábban egyáltalán nem rendelkeztek, illetve az információk megszerzésére csak nagy erőforrás ráfordítás, vagy és emberi élet kockáztatása árán volt lehetőség. A technikai fejlesztéssel párhuzamosan azonnal napirendre került a radarok aktív és passzív zavarásának kérdései. A rádióháború tehát kiterjedt a radarokra is, megkezdődött a speciális vevő, pelengátor, analízátor és zavaró eszközök fejlesztése, ami az egyre újabb radarok fejlesztésével párhuzamosan folytatódik napjainkban is.

A korabeli rádióháború elméletének tudományos alapú kidolgozásával létrejött az elektronikai hadviselés, a hadseregek szervezetében pedig rendszeresítették az elektronikai hadviselési egységeket, alegységeket.

Összefoglalva tehát:

- a technika fejlődésének legújabb eredményei igen rövid időn belül megjelennek a hadviselésben és az alkalmazók jelentős fölényre is szert tehetnek mindaddig, amíg meg nem találták az „ellenszert” is;
- kidolgozták az elektromágneses hullámtartományban folytatott hadviselés elméleti és gyakorlati módszertanát, az elektronikai hadviselést¹⁹⁴;
- az elektronikai hadviselésben megtalálható a hadviselés valamennyi tevékenységi formája, a felderítés, az álcázás, a megtévesztés, a csapás, a támadás, a védelem, stb.;
- szervezetszerű erőket hoztak létre és speciális rendeltetésű eszközöket fejlesztettek ki, amelyek ezeket a speciális szakfeladatokat végzik,

ami alapján kijelenthetjük, hogy az elektromágneses hullámtartomány a hadviselés valódi hadszíntérévé vált.

Az 1. ábra utolsó sorában a cyber-tér áll, amelyről azt állítom, hogy a hadviselés hatodik szintere. Ennek igazolása céljából a továbbiakban részletesen megvizsgálom a cyber-tér jellemzőit és a hadviseléssel való kapcsolatát.

¹⁹⁴ Az elektronikai hadviselés nem csak az elektromágneses hullámtartományban folyik, hanem a mechanikus rezgések tartományában is, mint például a szeizmikus és akusztikus hullámok tartománya.

A cyber-tér, mint a hadviselés hatodik színtere

A cyber-tér létét ma már nem vonja kétségbe senki. Mindenki egyetért abban is, hogy a számítógépes hálózatok mind fizikailag, mind logikailag behálózták az egész Földet. Az információs infrastruktúra globálissá vált, az információ pedig elsődleges jelentőségű erőforrássá lépett elő. Mint minden erőforrásnak, az információnak is megvan az a sajátossága, hogy a birtoklása hatalmi kérdés, tehát akinek a birtokában van, az igyekszik védeni azt, aki pedig meg akarja szerezni, az így, vagy úgy harcol érte.

A számítógépek és az őket összekötő távközlési kapcsolatok egy olyan különleges világot hoztak létre, amelyben a belépő felhasználó többé-kevésbé szabadon szörfözhet, a virtuális valósággal mintegy másik dimenzióba léphet át, ahol nincsenek államhatárok, és eredetileg nincsenek szigorú törvények. Ebben a világban a tárolt és felhasznált információ mennyisége egyre nő, egyre több szöveges, képi, hang és más formában tárolt információ válik hozzáférhetővé.

Mi is folyik a cyber-térben? Első ránézésre látható, hogy egyre nagyobb mennyiségű adat és információ halmozódik fel benne, amelyet az alkalmazók egymással cserélhetnek, egymásnak eladhatnak, amelyekhez hozzáférnek. A hálózatoknak köszönhetően az alkalmazók egymás erőforrásaihoz is hozzáférhetnek, amelyeket bizonyos kerektek között használhatnak is. Jó esetben ez lehetővé teszi az oktatást, képzést, kutatást, a kulturális értékek közvetítését, a műsortovábbítást, a kereskedelmi tevékenységet, a munkavégzést és még sorolhatnánk, hogy mennyi hasznos dolgot. Ugyanakkor, ugyanebben a világban, a cyber-térben kémkedés, hírszerzés is folyik, pénzmosás, illegális üzleti tevékenység, de megtalálta a helyét a tiltott anyagokkal való kereskedelem éppúgy, mint a pornóipar.

A világ üzleti életének, az államgépezeteknek, a bankszférának, a vállalatoknak, az önkormányzatoknak, a magánembereknek és többek között a hadseregeknek is egyre jelentősebb része él a számítógépes hálózatok, a cyber-tér nyújtotta szolgáltatásokkal, és egyúttal teszi ki magát a hálózat által jelentett kockázatoknak. Minél jelentősebb ez a részvétel, annál magasabb fokon informatizált a társadalom, ugyanakkor annál kevésbé tud ez a társadalom megenni a cyber-tér nélkül.

A terjedelem szabta korlátok miatt nem kívánom most példák sokaságán bemutatni, hogy milyen hasznos dolgokra képes az emberiség ebben az új közegben, ugyanakkor fel szeretném hívni a figyelmet arra, hogy fizikailag és logikailag ugyanezen eszközökkel dolgoznak a számítógépes bűnözők, a számítógépes rendszerek feltörésére, és azokban illegális tevékenységek folytatására szakosodott személyek, vagy csoportok.

Mint a világ minden szférájában, a cyber-térben is megjelent a politika, a hatalom megszerzéséért, mások befolyásolásáért folytatott harc. Előbb szimpatizánsok, számítógépes hackerek álltak egyik, vagy másik ügy mellé, majd később az egyes országok által folytatott háborúk során mindkét szembenálló fél mellett óriási, több tízezresre tehető csoportok kapcsolódtak be a küzdelembe a saját számítógépes eszközeikkel. Példaként szolgálhat erre az indiai-pakisztáni, a kínai-tibeti, vagy akár az izraeli-palesztin konfliktus. A gyakorta éles fegyverekkel folytatott meleg háborúk mellett a háttérben, a külső szemlélő által nem olyan látványos módon de határozottan megjelent és egyre nagyobb szerepet játszott a számítógépes hálózatokon folytatott harc.

Az első Öböl-háborút a világ első információs háborújaként emlegetik a szakértők. A légi csapások és szárazföldi műveletek mellett, azokat megalapozva, kiemelkedő jelentőséggel bírt az elektronikai hadviselés és a számítógépes rendszerek bénítása. A fő erőfeszítés a vezetés bénítására, a vezetési rendszerek működésének megakadályozására, a csapatok elszigetelésére irányult.

A harc persze nem volt egyoldalú. Az irakiak és a világ velük szimpatizáló hackerei internetes támadások sokaságával bombázták a Pentagon és a NATO számítógépes oldalait, elektronikus levelek ezreivel árasztotta el mindkét fél egymás szervereit. A délszláv háborúban, majd a 2003-as iraki háborúban tovább nőttek a számítógépes hálózatok támadásával okozott károk, a szolgáltatás kiesések által létrejött működési zavarok.

A tapasztalatok tehát azt mutatják, hogy a polgári és katonai rendeltetésű információs infrastruktúrák, az információs rendszerek és a bennük zajló folyamatok kiemelt jelentőségre tettek szert, ezáltal akár már korlátozott katonai konfliktusok esetén a támadások elsődleges célpontjaivá válnak.

Tekintsük a cyber-térben folytatott harc (háború) jellemzőit:

- közel fénysebességgel folynak az akciók;
- speciális a közeg, ahol a tevékenység folyik, speciálisak a műveletek módszerei is, így különleges felkészültséget igényelnek;
- megtalálható benne a hadviselés szinte valamennyi eleme:
 - információszerzés, helymeghatározás;
 - csapásmérés;
 - védelmi tevékenységek;
 - zavaró, megtevesztő műveletek;
- sokkal szélesebb körnek van módja beavatkozni, mint a hagyományos háborúban;
- a támogatók sokasága mobilizálható igen rövid idő alatt, kérésre segítek tünhetnek fel a legváratlanabb pillanatokban;
- folyhat békében, válságban és háborúban egyaránt.

Mi teszi lehetővé a cyber-térben folytatott háborút? A választ még a chipok gyártásánál, a számítógépek és szoftverek fejlesztésénél, kell keresnünk. A chipkebe beépített, nyilvánosan nem dokumentált funkciók és áramkörök lehetővé teszik, hogy akár adott parancsra, vagy külső rádiójelre a chip valamilyen feladatot hajtson végre, vagy csak egyszerűen beszüntesse a normális működést. Ezt chippingnek nevezzük.

A számítógépes programokba akár szándékosan, akár akaratlanul hibák maradnak (bug-ok) amelyek feltárásával lehetőség nyílik azok kihasználására. A programokba beleírt, de nem nyilvános rutinok a fejlesztők számára lehetőséget adnak bármilyen későbbi behatolásra (back door), vagy illegális programrészek futtatására. A biztonsági rések sokasága válik nap, mint nap ismertté a világ legnépszerűbb, legtöbb példányban futó programjaiban is.

Ezek az okok magyarázzák például azt, hogy a világ legnagyobb hadiüzemei a saját fegyvereik, repülőik, vagy rakétaik gyártásához csak saját maguk által gyártott chipkeket, és programokat használnak, semmilyen beszállítótól nem fogadnak el olyan alkatrészt, amiben nem dokumentált funkciók rejtőzhetnek.

A biztonság pedig növelhető lenne. A számítógépes hálózatokban folyó üzenet-, és adatforgalom kódolható lenne, azonban ez úgynevezett „felsőbb érdekek” miatt nem

valósítható meg. Törvények szabályozzák, hogy milyen biztonsági szint használható, holott az annál jóval magasabb fokú biztonság elérésének nincs technikai akadály. A „felsőbb érdekeknek”, azaz az államoknak és a biztonsági szolgálataiknak erősebb az az érdekük, hogy ellenőrzésük alatt tarthassák a számítógépes hálózatokon folytatott forgalmat, mint a hálózatok biztonsága. Ha megvalósulna pl. a közlemények 128 bites titkosítása, akkor a megfejtés gyakorlatilag lehetetlenné válna, ami a kontrol teljes elvesztését jelentené.

A számítógépes hálózatok biztonságát tehát feláldozták a hírszerzés, a lehallgatás, a magánszféra feletti ellenőrzés megtartása érdekében. Ezért nem lesznek biztonságosabbak egy adott szintnél soha a hálózatok és hálózatalapú rendszerek. A fejlődés persze nem áll meg, így látszólag a biztonsági szinteket növelik, de ezt mindig csak a lehallgathatósági határ alatt tartva teszik meg.

A „magasabb érdekek” határai persze nem határozhatók meg egyértelműen, mivel a politika, a hatalom, gazdaság, a világcégek és egyének érdekei napjainkra összemosódtak, kibogozhatatlanul szövevényessé váltak. Így kerülhetett sor arra, hogy a világsajtóban olyan, elsősorban a szövetségeseknél nagy felháborodást kiváltó tények láttak napvilágot, mint az Echelon, vagy a Carnivor rendszer létezésének és feladatainak a ténye. Ezek olyan alapvetően kémrendszerek, amelyek a világ számítógépes hálózatainak forgalmát elemzik, állítólag nemzetbiztonsági, terrorista elhárítási célból, azonban mint kiderült, akár gazdasági hírszerzési feladatokat is végrehajtottak.

Összefoglalva tehát, az államok, és elsősorban a gazdaságilag, műszakilag fejlett országok képesek a cyber-tér felett ellenőrzést gyakorolni, ott végeredményben akár háborús tevékenységet is folytatni.

Ez valóban csak a gazdasági nagyhatalmak privilégiuma? Nem! Ez nem infrastruktúraigényes atomipar, vagy csillagászati árú űrtechnológia. Ez hasonló a vegyi fegyverhez, amire azt mondják, hogy a szegény országok atombombája. Az informatikai eszközök legnagyobb része szabadon hozzáférhető, az áruk folyamatosan csökken. A szaktudás, a hozzáadott emberi szellemi potenciál az, ami ezt a technikát még magasabb szintre képes emelni.

Ha tehát a technológia minden ország számára elérhető, és a tudás is megszerezhető, akkor igen nagy szűklátókörűségre utal, ha abban bízunk, hogy ezzel a fenyegetéssel nem kell szembenéznünk. NATO tagok lévén szélesebb azoknak a köre, akik a NATO valamely tevékenységével, missziójával nem értenek egyet és ennek például a tagországok elleni cyber-támadások eszközével is hangot kívánnak adni. A biztonsági kockázatok köre tehát növekszik.

A cyber-tér biztonsági fenyegetéseire adható katonai válaszok

Kik vesznek tehát részt a cyber-térben folyó, mondjuk ki: harcban? Békeidőben a jogosulatlan felhasználóktól a profi hackerekig terjedő személyek és csoportok, a polgári és katonai nemzetbiztonsági szolgálatok, az internetrendőrség, az ellenzéki és szimpatizáns csoportok. Katonai konfliktusok esetén mindezek részt vesznek a harcban továbbra is, csak hovatartozásuktól, elkötelezettségüktől és vérmérsékletüktől függően különböző célokkal és intenzitással. Bekapcsolódnak ugyanakkor azok a hadseregek szervezetében létrehozott speciális információs harcosoknak nevezhető alegység tagjai, akik speciális eszközeikkel és szaktudásukkal a szembenálló fél rendszereiből képesek információkat gyűjteni, illetve képesek támadni azokat.

Mi kell egy ilyen szervezet létrehozásához?

- szakmai döntés;
- a működés jogi kereteinek megalkotása;
- a feladatra alkalmas személyi állomány kiválogatása;
- speciális oktatás, felkészítés;
- a megfelelő szervezeti struktúra létrehozása;
- technikai, infrastrukturális háttér (fegyverzet);
- az alkalmazás doktrínális elveinek megalkotása;
- intenzív gyakorlás, kutatás és együttműködés a megfelelő hazai és külföldi szervekkel.

Milyen eredmények várhatóak egy ilyen kötelék létrehozásától?

- új hadműveleti képesség létrejötte;
- a legnagyobb eredmény/befektetés arány elérése, ami ma haditechnikai rendszerben elérhető;
- a szembenálló fél rendszereinek sebezhetősége fokozódik, míg a saját rendszerek biztonsága növekszik;
- olyan aszimmetrikus hadműveleti képesség jön létre, ami a koalíciós műveletekben is jól alkalmazható.

Véggövetkeztetések

1. A fent leírtakból látható és véleményem szerint bizonyított, hogy az információk korban a hadviselés egy újabb hadszíntérrel, más szóhasználatban, egy újabb dimenzióval bővült, a cyber-térrel.

2. Az itt folyó tevékenység adott körülmények között minden tekintetben kielégíti a hadviselés fogalmát. A korszerű hadsereg megteremtésén dolgozó döntéshozók számára nyilvánvalóvá kell, hogy váljon, hogy erőket és eszközöket kell erre a színtérre csoportosítani, mert olyan lépéshátrányba kerülünk, amely egyre nehezebben dolgozható le.

3. Szakembereket kell képezni, szervezetet kell létrehozni, gyakorolni kell és együttműködve a saját számítógépes rendszerek üzemeltetőivel fel kell készülni a valódi feladatok végrehajtására, mert az ellenfeleink nem fogják ezt a lehetőséget kihagyni. Az első csapások a katonai és polgári számítógépes rendszereinket, vezetési hálózatainkat fogják érni.

4. Ha ma nem élünk ezzel a lehetőséggel, ha ma nem készülünk rá, meg sem fogjuk érteni, hogy mi történik körülöttünk, amikor kénytelenek leszünk ötven évvel ezelőtti vezetési módszereket alkalmazni, ha valamilyen eredményt el akarunk érni a korszerű eszközeink hiányában.

A csapat létszáma: egy fő

Egy fő-rendszerintegrátorral egyszerűbb a védelem

A Matáv egyedüli infokommunikációs fővállalkozóként összefogja a legjobb informatikai partnereket személyre szabott biztonságtechnikai megoldásához.

A biztonság és a védelem az üzletben mindenkinek mást jelent. A Matáv tagvállalataival – **BCN, SafeCom** – és partnereivel kidolgozott informatikai biztonsági (vírusvédelem, tűzfalmegoldások stb.) és fizikai biztonsági megoldásai (komplex hálózati, videomegfigyelő és épületbiztonsági rendszerek) garantálják a biztonságos üzletmenetet. Személyesen az Ön cégének is.

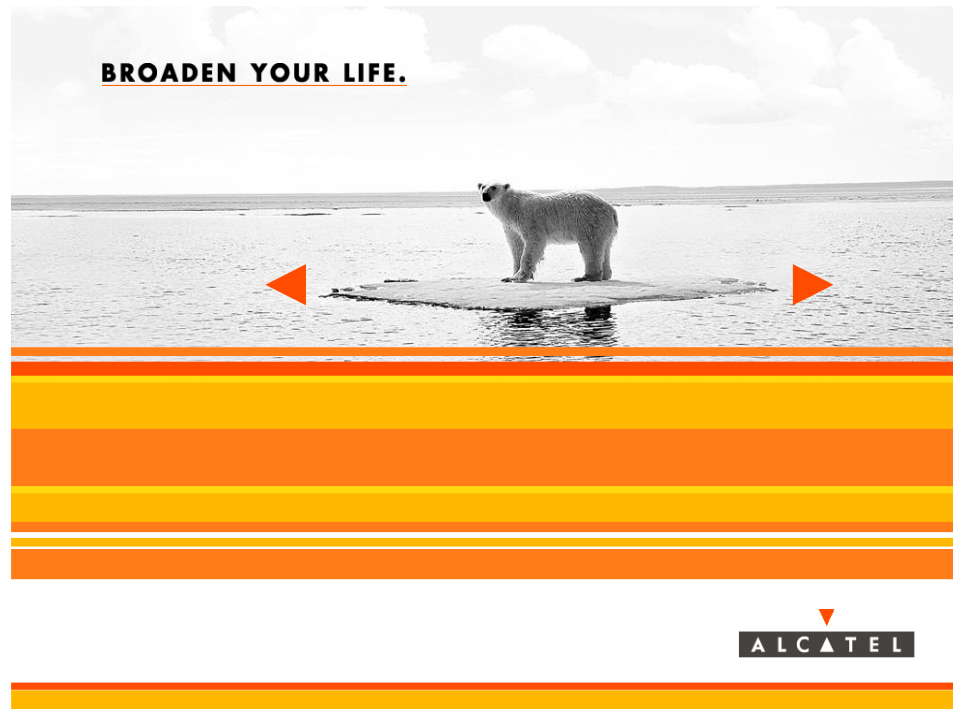





matáv
a szavakon túl

www.matav.hu

Az Alcatel kommunikációs megoldásokat kínál a távközlési, az Internet szolgáltatók és egyéb vállalatok számára, hogy azok hang- adat- és video alkalmazásokat juttathassanak el előfizetőikhez, vagy dolgozóikhoz. Az Alcatel a vezetékes és mobil szélessávú hálózatok, alkalmazások és szolgáltatások terén elért vezető helyét kihasználva teremt értéket üzletfelei számára a nagy sáv szélességek világában.



Alcatel Hungary Kft.

1116 Budapest, [Kondorfa u. 10.](#)

Telefon: (1) 2099500 Telefax: (1) 2099599

www.alcatel.hu

alcatelh@alcatel.hu