*A ZRÍNYI MIKLÓS NEMZETVÉDELMI EGYETEM KIADVÁNYA*



# Kommunikáció 2005
# Communications 2005

6




# Innovációk világhálózata

**Zrínyi Miklós Nemzetvédelmi Egyetem**
Budapest, 2005. október 27.

*A tudományos kiadványt szerkesztették:*
Dr. habil. Sándor Miklós nyá. ezredes, egy. docens
Dr. Rajnai Zoltán mk. alezredes, egy. docens
Dr. Fekete Károly mk. alezredes, egy. docens
Szöllősi Sándor okl. mk. őrnagy, egy. adjunktus

*Lektorálta:*
Dr. Fekete Károly mk. alezredes, egy. docens

*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 7060 11 1

**TARTALOMJEGYZÉK**


I. FEJEZET 15
Dr. LINDNER Miklós 17
A HONVÉDELMI MINISZTÉRIUM HONVÉD VEZÉRKAR HÍRADÓ ÉS INFORMATIKAI CSOPORTFŐNÖKSÉG MEGALAKULÁSÁNAK 60. ÉVFORDULÓJÁRA 17
BOZSÓ Zoltán 27
A RENDŐRSÉGI TEVÉKENYSÉGIRÁNYÍTÁS, A TÖRZS MŰKÖDÉSE 27
CSER Ádám 39
KÉPI INTEROPERABILITÁSI PROBLÉMÁK ÉS MEGOLDÁSOK A NATO-BAN 39
DOBÁK Imre 45
A KÉSZENLÉTI SZERVEZETEK VÁLTOZÓ KOMMUNIKÁCIÓS RENDSZEREI - PÉLDÁK A KÖZÉP-EURÓPAI TÉRSÉG ORSZÁGAIBÓL 45
DOBOS Attila 53
GENERÁCIÓVÁLTÁS A HONVÉDSÉGI TÁVKÖZLÉSBEN 53
EGRI Gábor 57
DÖNTÉSI FOLYAMAT FORMALIZÁLÁSA 57
FARKAS György 77
ÚJ KOMMUNIKÁCÓS KIHÍVÁS A SPAM 77
FEHÉR Gábor, KORN András, SZENTGYÖRGYI Attila, SZŰTS Péter Lóránt 101
BIZTONSÁGOS VEZETÉKNÉLKÜLI SZUPERHÁLÓZAT 101
FREGAN Beatrix 111
DOKTRÍNA, STRATÉGIA, TAKTIKA – A FRANCIA MINTA 111
GÁCSER Zoltán 115
AZ INFOKOMMUNIKÁCIÓS ESZKÖZÖK ÉS A DIGITÁLIS KATONA SZEREPE A XXI. SZÁZAD HADVISELÉSÉBEN 115
Dr. HAIG Zsolt 127
AZ INFORMÁCIÓS MŰVELETEK TERVEZÉSÉNEK KÉRDÉSEI 127
HÓKA Miklós, HORVÁTH Attila 145
A BÉKETÁMOGATÓ ÉS VÁLSÁGREAGÁLÓ MŰVELETEK HÍRADÁSA – ITTHONI SZEMMEL 145
HORVÁTH Zoltán 153
A KIS- ÉS KÖZEPES MÉRETŰ PILÓTA NÉLKÜLI REPÜLŐ ESZKÖZÖK, VALAMINT A FÖLDI IRÁNYÍTÓPONT KÖZÖTTI

KOMMUNIKÁCIÓ HATÉKONYSÁGÁNAK NÖVELÉSI LEHETŐSÉGE, SZABÁLYOS RASZTERES ÁLLOMÁNYÚ DIGITÁLIS DOMBORZAT MODELL ALKALMAZÁSÁVAL 153
KASSAI Károly 161
AZ ELEKTRONIKUS ADATKEZELŐ RENDSZEREK VÉDELMÉNEK FONTOSABB TENDENCIÁI (KIEMELTEN A SZABÁLYOZÁSI TERÜLETTEL KAPCSOLATOS FELADATOK) 161
KERNER Menyhért 171
INFORMÁCIÓVÉDELEM A KORMÁNYZATI ÉS A VÉDELMI SZFÉRÁBAN 171
KERNER Menyhért 179
AZ INFORMATIKA HAZAI JOGI KÖRNYEZETÉNEK INFORMÁCIÓBIZTONSÁGI SZEMPONTBÓL VALÓ VIZSGÁLATA 179
Dr. KOVÁCS László 187
A TERRORIZMUS VESZÉLYE ÉS A MAGYAR KÖZTÁRSASÁG KOMMUNIKÁCIÓS INFRASTRUKTÚRÁJA 187
Magyarné KUCSERA Erika 199
A TELJES INTEGRÁCIÓ FONTOSSÁGA A MH ZÁRTCÉLÚ INFOKOMMUNIKÁCIÓS HÁLÓZATAINAK MENEDZSMENTJÉBEN 199
MAROS Dóra, MÉSZÁROS Árpád 203
A MAGYAR TÁVKÖZLÉSI RENDSZER ANOMÁLIÁI A LONDONI TERRORTÁMADÁS TÜKRÉBEN 203
MÁTÉ József 209
A KATASZTRÓFAVÉDELEM INFOKOMMUNIKÁCIÓS TÁMOGATOTTSÁGA 209
Dr. habil MEZEY Gyula 225
A KRITIKUS IT INFRASTRUKTÚRA VÉDELMÉRŐL 225
Dr. NAGY Tamás 229
A MAGYAR LÉGVÉDELEM INFORMÁCIÓS HÁLÓZATÁNAK JELLEMZŐI 1945 – 1955 KÖZÖTT 229
NÉMETH András 243
MOBILTELEFON HÁLÓZATOK ALKALMAZÁSA A KATASZTRÓFAVÉDELMI KOMMUNIKÁCIÓ TERÜLETÉN 243
NÉMETH András, Dr. OSVÁTH Zoltán 256
MÚLT –JELEN – JÖVŐ… AVAGY VILLAMOS- KONTRA „HADMÉRNÖK” A HÍRADÓTISZT-KÉPZÉSBEN 256

Dr. PÁNDI Erik 269
A KORMÁNYZATI KOMMUNIKÁCIÓT KISZOLGÁLÓ RENDSZEREK LEHETSÉGES INTEGRÁCIÓJA 269
RÉVÉSZ Gyula 291
A HÍRADÓ KIKÉPZÉS MÚLTJA, JELENE ÉS JÖVŐJE 291
TESSEDIK Tamás 299
SZOLGÁLTATÁSMENEDZSMENT EGY TÁVBESZÉLŐ SZOLGÁLTATÓ INFORMÁCIÓ BIZTONSÁGI KÖVETELMÉNYEINEK SZEMSZÖGÉBŐL 299
Dr. VÁNYA László 305
FORRADALMIAN ÚJ ELJÁRÁSOK A RÁDIÓ- ÉS RÁDIÓTECHNIKAI ZAVARÁSBAN 305
Dr. VASS Sándor 315
AZ INFOKOMMUNIKÁCIÓS BERENDEZÉSEK BIZTONSÁGOS ÜZEMELTETÉSÉNEK NÉHÁNY AKTUÁLIS KÉRDÉSE 315
II. FEJEZET 327
Károly FEKETE 329
THE MULTI-NATIONAL MISSIONS AND THE NETWORK ENABLED CAPABILITY 329
Károly FEKETE 334
TOWARDS A NEW GENERATION OF WLAN IN MILITARY COMMUNICATIONS 334
Károly FEKETE 341
SECURE BASED WIRELESS IP PROTOCOLS WITH REGARD TO CLOSED NETWORKS 341
Gyula MIKÓ, András MAGYAR 347
C-BAND ADAPTIVE RADIO DIRECTION FINDING SYSTEM 347
Sándor MUNK 361
INTEROPERABILITY INFRASTRUCTURE IN MILITARY INFOCOMMUNICATION SYSTEMS 361
Erik PÁNDI 371
UNIFICATION OF THE HUNGARIAN GOVERNMENTAL COMMUNICATIONS SYSTEMS 371
Zoltán RAJNAI, Beatrix FREGAN 377
NOUVELLES STRATEGIES DE TECHNOLOGIES ET ART DE LA GUERRE 377
Zoltán RAJNAI, László TREMBECZKY 383
LE CIMENT DES ARMEES: LA COHESION 383
Gyula RÉVÉSZ 387
INFORMATION OPERATION IN THE “INFORMATION AGE” 387

Roland VIDA, Attila VIDÁCS 391
A SURVEY ON ENERGY EFFICIENT COMMUNICATION SCHEMES IN WIRELESS SENSOR NETWORKS 391
WB Electronics 401
BATTLEFIELD MANAGEMENT SYSTEM TROP FOR BRIGADE AND BELOW – IRAQ FREEDOM MISSION EXPERIENCES 401
Zoltán SZENTPÁL, László ZÖMBIK 405
ATTACKS AGAINST ANONYMIZER NETWORKS 405
III. FEJEZET 421
A NEMZETKÖZI TUDOMÁNYOS SZAKMAI KONFERENCIA HÁTTÉR INFORMÁCIÓI 422
ALCATEL 423
END TO END NETWORK-CENTRIC SERVICES, THE NEEDED "BIG PICTURE" APPROACH TO DEFENSE NETWORKING 423
ANTÓK Péter 441
HÍRKÖZLŐHÁLÓZAT - HÁLÓZATBIZTONSÁG 441
CISCO Systems Magyarország Kft. 453
INTELLIGENS INFORMÁCIÓS HÁLÓZATOK - BIZTONSÁG ÉS HATÉKONYSÁG 453
ERICSSON Magyarország Kft. 463
ERITAC POINT TO MULTI-POINT 463
Károly FEKETE 489
THE BENEFITS OF HIGH PERFORMANCE WIMAX SOLUTIONS IN MULTINATIONAL MISSIONS 489
FERCOM Kommunikációs Kft. 503
MOTOROLA VEZETÉKNÉLKÜLI ADATKOMMUNIKÁCIÓS RENDSZEREK 503
KAPSCH Telecom Kft. 517
VIDEÓ MEGFIGYELÉS EGY KICSIT MÁSKÉPPEN 517
MÁTÉ József 527
A KATASZTRÓFAVÉDELEM INFOKOMMUNIKÁCIÓS TÁMOGATOTTSÁGA 527
Gyula MEZEY 547
EMERGENCY 2005 SYSTEM 547
József TORJAI 555
OMNIPCX 4400 BENEFITS FOR DEFENSE 555
T-SYSTEMS 575
AZ ELEKTRONIKUS KORMÁNYZATI GERINCHÁLÓZAT (EKG) KÍNÁLTA LEHETŐSÉGEK 575
WB Electronics 583
TACTICAL FIBER OPTIC COMMUNICATION 583

WB Electronics 597
TROP BATTLEFIELD MANAGEMENT SYSTEM 597

**A nemzetközi szakmai tudományos konferencia kommunikációs partnere:**

Magyar Telekom Részvénytársaság

T Systems

**A tudományos konferencia támogatói:**

SIEMENS Rt.

Kapsch Telecom Kft.

Fercom Kommunikációs Kft.

THALES COMMUNICATIONS

CISCO Systems Magyarország Kft.

ERICSSON Magyarország Kft.

WB ELECTRONICS

A rovatlások felolvasása a háttérben található.

*Te, tudod mi az, hogy DVB, PET meg NHH?*
*Hé, egy mobil cég vezetője biztos tudna*
*tanácsot adni. Ismersz egyet?*
*Á, erről biztos lesz valahol egy konferencia,*
*na de hol és mikor. Tudsz valakit, aki ilyeneket szervez?*

*Ha a fenti kérdésekre **igennel** válaszoltál, biztos hallottál már a HTE-ről. Ha **nem,** itt az idő.*

A Hírközlési és Informatikai Tudományos Egyesület várja a szakma, és annak társadalmi hatásai iránt érdeklődő fiatal kollégákat:

- Szakosztályok
- Rendezvények
- Kiadványok: Hírlevél, Híradástechnika folyóirat, Mobil-IT
- Kapcsolatok, ismeretségek

Bővebb információ a weben a ***www.hte.hu*** alatt, vagy pedig e-mailben az ***info@hte.hu*** címről. Addig is ízelítőül:

**AKTUÁLIS RENDEZVÉNYEINK**

Október 19. (szerda), 16.00
*Stúdiótechnikai szakosztály, Digitális Mozgó Világ Klub*
***Látogatás a DUNA Televízióban***
***Beszámoló a FIAT-IFTA éves beszámolójáról***

Október 19. (szerda), 17.00 óra
*HTE TIPIK Klub*
***A szerződések szerepe az építőipari projektekben***

Október 27. (csütörtök), 17.00 óra
*Távközlési Klub*
***Ambiens Intelligencia***

*Az előadásokról részletes információ található a HTE honlapján a **www.hte.hu** címen.*

A Hírközlési és Informatikai Tudományos Egyesület egy több mint 50 éves múltra visszatekintő szakmai szervezet. Tevékenysége közel 20 szakosztályon belül történik, havonta számos rendezvény (konferencia, klub, workshop) gyűjti össze a szakma legjavát. Az Egyesület által kiadott Híradástechnika folyóirat pedig rendszeresen igényes tartalommal várja az olvasókat.

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET
Budapest, V., Kossuth L. tér 6-8. Postacím: 1372 Budapest, Pf. 451
Tel.: (06-1) 353 1027 Fax.: (06-1) 353 0451, www.hte.hu, e-mail: info@hte.hu

# A HTE FELÉPÍTÉSE

## SZAKOSZTÁLYOK

Digitális Mozgó Világ Klub
Digitális Rádió Kör
Dokumentumtechnológia szakosztály
Digital Video Broadcasting kör
e-Magyarországért szakosztály
Energiaipari távközlési szakosztály
Informatikai biztonság és adatvédelmi szakosztály
Informatikai szakosztály
Kábeltelevíziós szakosztály
Közlekedéshírközlési szakosztály
Média Klub
Mikroelektronikai szakosztály
Stúdiótechnikai szakosztály
Számítástechnikai szakosztály
Szenior klub
Távközlési és Informatikai Projektirányítók Klubja
Távközlési Szakosztály
TETRA Szakosztály
Vételtechnikai Szakosztály

## TERÜLETI CSOPORTOK

Győri csoport
Debreceni csoport
Nyíregyházi csoport
Paksi csoport
Salgótarjáni csoport
Siófoki csoport
Soproni csoport
Szegedi csoport

## MUNKAHELYI CSOPORTOK

BME Villamosmérnöki és Informatikai Kar
BMF Kandó Kálmán Villamosmérnöki Főiskolai Kar
Puskás Tivadar Távközlési Technikum
Széchenyi István Egyetem
Zrínyi Miklós Nemzetvédelmi Egyetem

HÍRKÖZLÉSI ÉS INFORMATIKAI
TUDOMÁNYOS EGYESÜLET
1055 Budapest, Kossuth Lajos tér 6-8.
Postacím: 1372 Budapest, Pf. 451.
Tel: (1) 353-1027 Fax: (1) 353-0451
www.hte.hu, info@hte.hu

## VEZETŐSÉG

| | |
|---|---|
| Elnök | Dr. Sallai Gyula, Budapesti Műszaki és Gazdaságtudományi Egyetem |
| Alelnökök | Dr. Huszty Gábor, Entel Kft.<br>Maradi István, T-Mobile Rt.<br>Dr. Pap László, Budapesti Műszaki és Gazdaságtudományi Egyetem |
| Főtitkár | Horváth Pál, Actel Kft. |
| Főtitkár-helyettesek | Ágoston György<br>Dr. Kántor Csaba, Magyar Telekom Rt.<br>Dr. Tormási György, Antenna Hungária Rt. |
| További Intéző-bizottsági tagok | Dr. Cinkler Tibor, Budapesti Műszaki és Gazdaságtudományi Egyetem<br>Bölcskei Imre, Magyar Telekom Rt.<br>Duró Imre, HUNSAT Rt.<br>Dr. Kolláth Gábor, Ericsson Magyarország Kft.<br>Marchhart Pál, Vodafone Rt.<br>Vágujhelyi Ferenc, SzilCom Kft. |
| Ellenőrző bizottsági elnök | Halmi Gábor, Műszaki és Természet-tudományi Egyesületek Szövetsége |
| Ellenőrző bizottsági tagok | Kubinyi Imre, Edusys Rt.<br>Dr. Szecsődi Istvánné, EMITEL Rt. |
| Etikai bizottság elnök | Dr. Gosztony Géza, Pázmány Péter Katolikus Egyetem |
| Etikai bizottsági tagok | Csikász István<br>Mallász Judit, IT-Business |
| Gazdasági bizottság elnök | Csizmadia Attila, Pénzügyminisztérium |
| Díj bizottság elnök | Dr. Bartolits István, Nemzeti Hírközlési Hatóság |
| Külügyi bizottság elnök | Füredi Ágnes |
| Elnökség további tagjai | Antalné Zákonyi Magdolna, Phoebus Kft.<br>Bárányné Dr. Sülle Gabriella, T-Mobile Rt.<br>Dr. Géher Károly, Budapesti Műszaki és Gazdaságtudományi Egyetem<br>Fáy András, Nokia Magyarország Kft.<br>Dr. Halász Edit, Budapesti Műszaki és Gazdaságtudományi Egyetem<br>Halász Miklós, Hungarotel Rt.<br>Hazay István, HUNSAT Rt.<br>Dr. Henk Tamás, Budapesti Műszaki és Gazdaságtudományi Egyetem<br>Dr. Horváth László, Puskás Tivadar Távközlési Technikum<br>Jambrik Mihály, Informatikai és Hírközlési Minisztérium<br>Dr. Lajtha György<br>Dr. Takács György, Pázmány Péter Katolikus Egyetem |
| Oktatási bizottság elnök | Dr. Cinkler Tibor, Budapesti Műszaki és Gazdaságtudományi Egyetem |
| Ifjúsági bizottság elnök | Tóth Gergely, SEARCH-Lab Kft. |
| Híradástechnika főszerkesztő | Dr. Szabó Csaba, Budapesti Műszaki és Gazdaságtudományi Egyetem |
| Híradástechnika szerkesztő-bizottság elnök | Dr. Zombory László, Budapesti Műszaki és Gazdaságtudományi Egyetem |
| Hírlevél főszerkesztő | Máté Mária, Kopint-Datorg Rt. |
| Ügyvezető igazgató | Nagy Péter |

*Privacy Enhancing Technologies*

# BEVEZETŐ

A Tisztelt Olvasó az évenkénti rendszerességgel elkészített „Kommunikáció - Communications” tudományos kiadvány könyv változatát tartja a kezében.

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

A tudományos kiadvány első és második fejezete tudományos cikkek formájában, magyar és idegen nyelven teszi közzé az elmúlt időszak tudományos eredményeit, az aktuális problémákra adható válaszokat, megoldásokat. A cikkek szerzői többségében kutató intézetek, egyetemek, kormányzati és polgári távközlési szervezetek valamint a versenyszféra tudományos munkatársai, fejelsztő szakemberei, oktatói, doktoranduszai.

A könyvben közreadott és vizsgált témák időszerűségét jelzi, hogy a harmadik fejezetben a Zrínyi Miklós Nemzetvédelmi Egyetem Híradó Tanszék, a HVK Katonai Tervezési Főcsoportfőnökség, a Zrínyi Miklós Nemzetvédelmi Egyetem Katonai Műszaki Doktori Iskola és a Hírközlési és Informatikai Tudományos Egyesület ZMNE egyetemi csoportja által rendezett „Kommunikáció 2005” nemzetközi szakmai tudományos konferencián elhangzott előadások egy részének szerkesztett változatát olvashatjuk.

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

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

A szervező bizottság nem titkolt szándéka, hogy az előadásokon elhangzottak minél szélesebb körben ismertté váljanak, ezért a könyv mellett – korlátozott példányszámban – a kiadvány elektronikus változatát is közreadtuk.

*A szervező bizottság*

# I. FEJEZET


09:02_ KEZDŐDIK A HETI IT-ÉRTEKEZLET
09:05_ AZ OSZTÁLYVEZETŐ VISSZATÉR SZABADSÁGÁRÓL, ÉS NEKIKEZD E-MAILJEI ÁTNÉZÉSÉNEK
09:07_ A FÉREGVÍRUS TÁMADÁSBA LENDÜL
09:08_ A HÁLÓZAT MEGSEMMISÍTI A VÍRUST
09:09_ AZ ÉRTEKEZLET MEGSZAKÍTÁS NÉLKÜL FOLYTATÓDIK
Elég csak egy pillanatra hátat fordítania, és számítógépes hálózatát máris támadások érhetik.
Még szerencse, hogy tud magára vigyázni. A Cisco Security Agent az önvédő hálózat legújabb titkos fegyvere.
Felismeri a féregvírusokat, és még azelőtt megsemmisíti őket, mielőtt bármi kárt okozhatnának.
A biztonság a hálózat egészére kiterjeszthető. A támadások visszaverhetők.
Jelszó a megelőzés. A hálózat működik, az értekezlet megszakítás nélkül folytatódik.
További információért kérjük, látogasson el a http://www.cisco.com/hu/security weboldalra.
Cisco Systems
THIS IS THE POWER OF THE NETWORK. NOW.

**Dr. LINDNER Miklós**

# A HONVÉDELMI MINISZTÉRIUM HONVÉD VEZÉRKAR HÍRADÓ ÉS INFORMATIKAI CSOPORTFŐNÖKSÉG MEGALAKULÁSÁNAK 60. ÉVFORDULÓJÁRA

Dr. Lindner Miklós nyá. vezérőrnagy, címzetes egyetemi tanár
a Puskás Tivadar Híradó Bajtársi Egyesület elnöke

Amikor immár évente hagyományosan megtartjuk konferenciánkat, amelynek fókuszában a kommunikáció korszerűsítésére irányuló témák állnak elemi kötelességünk megemlékezni a HM HVK Híradó és Informatikai Csoportfőnöksége megalakulásának 60. évfordulójáról. A Honvédelmi Minisztérium (HM) Honvéd Vezérkar (HVK) Híradó és Informatikai Csoportfőnöksége 60 éves történetének sűrített változata méltán reprezentálja azt a hat évtizedes küzdelmet, amelyet a csoportfőnökség vezetői és személyi állománya, de megkockáztatom az egyeteme híradó szolgálat egésze a katonai vezetés híradásának folyamatos biztosítása érdekében vívtak.

Hat évtizeden keresztül – a politikai széljárások és a költségvetés hektikus változásai közepette – a vezetés által meghatározott általános irányelvek keretei között céltudatos munka folyt egy az adott kor színvonalán álló híradó szolgálat megteremtéséért és folyamatosságának évtizedeken átívelő biztosításáért.

A II. világháború katonai műveleteinek kimenetele már 1944 évben előrevetítette a hitleri Német Birodalom és szövetségesei vereségét.

Kelet-Magyarország felszabadulásával egyidőben a Debrecenben 1944 decemberében megalakult Ideiglenes Magyar Kormány 1945 januárjában, Moszkvában aláírta az ideiglenes fegyverszüneti egyezményt, amelynek keretében vállalata – nyolc hadosztályt magába foglaló – demokratikus magyar hadsereg felállítását és a Szovjet Hadsereg oldalán a németek elleni harcba vetését.

A fegyverszüneti egyezmény figyelembevételével, ideiglenes szervezettel megalakult Honvédelmi Minisztérium megkezdte a hadosztályok szervezését, felállítását és felszerelését.

Az égetően szükséges híradó egységek szervezésére, anyagi- technikai ellátásának biztosítására és valamennyi híradással összefüggő kérdés koordinálására az akkori HM Katonai Csoportfőnökség állományában híradó osztály került létrehozásra.

A létrehozott híradó osztály személyi összetételét azok a Magyar Királyi honvédség állományában szolgált demokratikus érzelmű híradó tisztek és tiszthelyettesek alkották, akik hajlandók voltak szembefordulni a hitleri Németországgal és elkötelezettek voltak egy új demokratikus Magyarország és annak megszervezésre kerülő demokratikus hadserege iránt. Eltökélt szándékuk volt egy új híradó szolgálata alapjainak lerakása.

Ezidőben a legnagyobb gondot a híradó eszközök és anyagok összegyűjtése okozta. A fegyverszüneti egyezményben rögzített 8 hadosztály helyett 2 hadosztály került felállításra. E hadosztályok híradó eszközökkel és anyagokkal való ellátása alig érte el

a szükségszerű szintet, mivel ezen anyagok és eszközök összegyűjtése, javítása az adott körülmények között rendkívül nehéz feladatot jelentett.

Mivel a hadosztályok ütközetbe vetésére nem került sor, a híradó osztály minden erejét és energiáját a híradó csapatok megalakítására, az országos légvezetékes hálózat rombolt részeinek helyreállítására fordította. Mintegy 7000 km vezetéket építettek és az ország hírközlésének meghatározó viszonylataiban helyreállították a távbeszélő és a távíró hálózatokat.

Ezt követően az osztály fő figyelmét a HM közvetlen híradó egységek magját képező 1. és 6. Híradószázadból felállítandó 1. Önálló Híradózászlóalj (Pécs), illetve a szervezés alatt álló határőrség hírrendszerének megteremtése kötötte le. Továbbá erőteljesen dolgozott a korabeli HM hírrendszerének megteremtésén. Már ezidőben is foglalkoztak a híradó eszközök korszerűsítésének megoldásán, azonban erre vonatkozóan szinte semmiféle kézzelfogható lehetőséggel nem rendelkeztek.

A híradó szervezetek fejlesztése az 1947. évi párizsi békeszerződés megkötését követően megtorpant, mivel a politika a hadsereg fejlesztését másodrendű feladatnak ítélte meg.

Az 1948. évi belpolitikai csatározást követő változások, a gyorsütemű balratolódás következtében a hadsereg fejlesztése ismét központi kérdésként merült fel.

A hadsereg fokozott fejlesztését szorgalmazó elgondolások okai között elsősorban a Kommunista és Munkáspártok Tájékoztató Irodája és a Jugoszláv Kommunisták Szövetsége között kölcsönösen kialakult ellentétek álltak, és ezek évtizedre meghatározták annak a fegyverkezési spirálnak létjogosultságát, amelyek a hadseregek intenzív fejlesztése terén a szocialista országokat sújtotta.

A Katonai Főcsoportfőnökség elnevezésű szervezet, amely 1948-ban „kvázi" honvéd vezérkarként működött, átfogta az egész honvédség irányítását. Ezzel egyidőben a HM híradó osztály – mint a katonai főcsoportfőnöknek alárendelt szervezet – a Katonai Főcsoportfőnökség VII. (híradó) osztálya elnevezést kapta.

Az idő tájt a feszült hidegháborús helyzetben, a katonai felső vezetés – ráhangolódva a politikai vezetés téves, külföldről is sugallt helyzetértékelésére – a háborús konfliktus rövid időn belüli kitörésével számolt. E hidegháborús légkörben a híradó osztályra komoly – erejét és lehetőségeit meghaladó – feladatok hárultak. E feladatok közül kiemelkedett a Magyar Postával – mint a hálózatok gazdájával – történő együttműködés megszervezése, a II. világháborúból megmaradt híradó technika alkalmazhatóságának felmérése, a híradó alegységek fokozott szakkiképzésének irányítása.

A híradó osztály gondjait fokozta a káderállomány elégtelensége, utánpótlásának nehézségei.

A híradó eszközök, anyagok és egyéb berendezések – a voluntarista vezetés által meghatározott irreális – mennyiségének elégtelensége a híradás biztosításában – mint hálózati gazdát – a Magyar Postát kulcsszereplővé tette, annak ellenére, hogy erre megfelelő felkészültséggel rendelkezett volna.

A hadsereg nagyarányú fejlesztésének elgondolása a híradó osztályt váratlanul érte. A politika vakrepülésének körülményei között a híradó osztálynak olyan technikai fejlesztés kidolgozásával kellett foglalkoznia, amely sem az ipari tervezés, sem a gyártás területén – a szükséges anyagok, alkatrészek hiányában – nem volt kellően meg-

alapozva. Az ország nyugattól történt hermetikus elzárkózása a fejlesztéshez és gyártáshoz szükséges alkatrészállomány beszerzését meghiúsította, így csak a hazai, gyengébb minőségű alkatrészállományra lehetett hagyatkozni.

Mindezek ellenére a híradó osztály a rendelkezésre álló lehetőségek optimális kiválasztásával a fejlesztést beindította.

A kiképzés és a káderutánpótlás biztosítására honvédelmi miniszteri rendelettel létrehozták az első törzstiszti tanfolyamot, majd 1948-ban megkezdődött a híradó tisztek Honvéd Kossuth Akadémián történő intézményes kiképzése.

Az 1949. évet a honvédség szervezeteinek kialakítása jellemezte. Ennek megfelelően az 1949. évi tavaszi szervezés során a Katonai Főcsoportfőnökség – amely eddig kvázi Vezérkarként működött – hivatalosan felvette a Honvéd Vezérkar elnevezést.

Így a Katonai Főcsoportfőnökség (híradó) Osztályának megnevezése Honvéd Vezérkar 3. (híradó) Csoportfőnökségre változott, lényegesen jobb szervezettel és létszámkonstrukcióval. 1949 júliusában létrejöttek a honvédelmi miniszter közvetlen alárendeltségében a fegyvernemi parancsnokságok, s így a HVK 3. csoportfőnöke egyidejűleg a híradó csapatok parancsnoka tisztét is betöltötte és így valamennyi híradó beosztásban szolgáló katona szolgálati elöljárójává vált.

Ugyanezen évben a Csoportfőnökség közvetlen alárendeltségébe került a 101. Híradóezred (Pécs), valamint a megalakult a Zalka Máté Híradó Tiszti Iskola.

A Zalka Máté Híradó Tiszti Iskola megalakításának időszakában 648 híradó tiszt volt a szolgálat állományában. Jellemző a voluntarista hadseregfejlesztésre, hogy a Csoportfőnökség káderutánpótlási terve 1952-re 2622 fős híradó tiszti állomány meglétét irányozta elő!

Mai szemmel kissé groteszknek hat, hogy a lövészezredek híradó szervezeteiben 12-14 híradó tiszti beosztás volt rendszeresítve, ugyanakkor a tiszthelyettesi beosztások száma minimalizálódott.

Az 1949. év a Csoportfőnökség és a híradó technika fejlesztése szempontjából igen fontos év volt. Ekkor született döntés a magyar fejlesztésű R-10, R-20 és R-40, R-50 típusú rádiók és tábori MH berendezések gyártására, ami a mostoha nemzetközi viszonyok közepette csúcseredménynek számított.

Ez évben került sor a HM átszervezésére, ami a Csoportfőnökséget is érintette. Az átszervezés során a Csoportfőnökség megnevezése VK Híradó Csoportfőnökségre változott, de használhatta az alárendeltek felé a Híradó Csapatok Parancsnoksága megnevezést is. Az átszervezés a Csoportfőnökségen rádiós és vezetékes osztályok szervezetbe állítását eredményezte. A Csoportfőnökség közvetlen alárendeltjeinek száma jelentősen megnőtt.

Jellemző, hogy a Csoportfőnökség közvetlen alárendeltjeinél – a vezetéknélküli eszközök mennyiségének elégtelensége miatt – a vezetékes alegységek domináltak.

A Magyar Posta kezelésében és fenntartásában lévő hírhálózatok állapotának gyengeségeire utalt, hogy a létrehozott vonalépítő zászlóaljak felszerelése és kiképzése kizárólag állandó vezeték építésére és karbantartására korlátozódott.

A Csoportfőnökség nehéz körülmények közötti helytállását beárnyékolták azok a politikai jellegű adminisztratív intézkedések, amelyek sem mivel nem igazolható politikai diszkrimináció fojtogató légkörének kialakulásához vezettek. E légkörben min-

den jogi alap és bírósági ítélet nélkül elbocsátották, internálták a Csoportfőnökségen dolgozó, korábban a magyar királyi honvédségben szolgált tiszteket. Ez a tény, valamint a Csoportfőnökség állományának évi 20-25 %-os fluktuációja nem kedvezett a tervszerű, elmélyült munkának.

A Csoportfőnökség által kidolgozott fejlesztési követelmények és tervek alapján tovább folytatódott a rádiók gépjárművekbe történő beépítése, megkezdődött az első hadsereg típusú mozgó hírközpont komplexum építése, ami az akkori körülmények között lényeges előrelépést jelentett.

Az 1951-ben nagy lendülettel – az objektív lehetőségek figyelmen kívül hagyásával – megindult hadseregfejlesztés 1953-ban megtorpant, ami a fejlesztések visszafogását és a létszám nagyarányú csökkentését eredményezte. A létszámcsökkentést a Csoportfőnökség az alárendeltjeire hárította, ami 450 főben realizálódott.

Ez a létszámcsökkentés egy sor jó felkészültségű híradó tisztet érintett és ennek negatív, nyugtalanító hatása még sokáig érezhető volt. A politika hazárdjátéka, a háborús veszély indokolatlan túlértékelése, majd az egészségtelenül felduzzasztott hadsereg hirtelen leépítése komoly gondokat okozott. Ez indokolatlan mértékben vette igénybe a Csoportfőnökség amúgy is túlterhelt állományát. Megbomlott a követelmények és lehetőségek közötti egyébként is gyenge összhang, ami ismét az ellentmondások kiéleződéséhez vezetett.

Az 1954. év volt a Csoportfőnökség életében az első olyan esztendő, amikor a békehadrendben szereplő híradó eszközök 100%-a állt rendelkezésre.

A Csoportfőnökség megkezdte a szárazföldi hadsereg parancsnokság felállításával kapcsolatos híradó feladatok elemzését és javaslatot dolgozott ki a hadsereg híradó szervezeteire. A hadsereg felállítására – az időközben kitört forradalom és szabadságharc eseményei következtében – nem került sor. A forradalmi események viszonyai között és után a Csoportfőnökség az országos távközlési hálózat kulcsobjektumainak védelmére és biztonságára koncentrált.

A forradalom leverését követően a Csoportfőnökség a napi élethez feltétlen szükséges szolgáltatások biztosításával foglalkozott, a fejlesztéssel kapcsolatos kérdéseket – anyagi keretek hiányában – csak elvi szinten művelte, törzsfoglalkozásokon és hadijátékokon vett részt.

A Varsó Szerződésben viselt tagságunk miatt a Csoportfőnökségnek egyre nagyobb figyelmet kellett fordítani a tagországokban rendszeresített, alapvetően szovjet fejlesztésű és gyártású híradó eszközök iránt, mivel azok paraméterei, szolgáltatásai lényegesen felülmúlták az akkor rendszeresített saját gyártmányú eszközeinket. A Csoportfőnökség irányt vett ezen eszközök hosszabb távon történő beszerzésére, illetve licenc honosítás alapján a magyar híradástechnikai ipar által történő gyártatására. E törekvések eredményeként a magyar ipar nagyvállalatai (Orion, Videoton, Telefongyár, Finom Mechanikai Vállalat, Mechanikai Labor) komoly megrendeléshez jutottak és a partnerek nagy megelégedésére kifogástalan minőséget produkáltak,

1961-ben egy sor változás érintette a Csoportfőnökséget, amely ekkor már nagy gyakorlatot szerzett a sűrű szervezési és szervezeti változások kezelésében.

Ugyancsak ez évben a Csoportfőnökség állományából került felállításra a Szárazföldi Hadsereg Parancsnokság Híradó Osztálya. A berlini válság idejére, a Csoportfőnökség „M” alakulatai közül 8 került tartalékosokkal feltöltésre és összekovácsolásra.

E gyakorlatokon kiütköztek a tartalékos kiképzéssel kapcsolatos gondok, amelyek főleg az anyagellátás minőségében, valamint a szakkiképzés hiányosságaiban jelentkeztek.

1962-ben a Csoportfőnökség a VKF vezetésével először hajtott végre olyan gyakorlatot, ahol a gyakorlat résztvevőjeként szerepelt. E gyakorlaton élesen kiütköztek a képességek területén meglévő – gyors megoldásra váró – gondok és problémák. Itt ismételten felmerült az örökzöld téma, a Magyar Posta által működtetett hírhálózatok katonai felhasználhatóságának korlátai, a szükséges helyreállító képesség gyengeségei.

A Közlekedési és Postaügyi Minisztérium által felállítandó helyreállító alakulatok - minden jó szándék ellenére - nélkülözték a gyors, szakszerű helyreállításhoz elengedhetetlen eszközöket. Nem rendelkeztek mobil mikrohullámú állomásokkal, sokcsatornás mobil vivőfrekvenciás berendezésekkel, speciális gépjárműparkkal, továbbá a szükséges szakértelemmel.

A gyakorlat azt is bebizonyította, hogy a tartalékos híradó állomány előzetes összekovácsolás nélkül még szükségszerűen sem képes feladatának ellátására.

A hatvanas éveket a szovjet katonai híradástechnika térhódítása jellemezte. Ekkor jelent meg a magyar ipar által is gyártott ultrarövid-hullámú (URH) család (R-105, R-108, R-109, R-114), amelyek minőségi javulást hoztak az URH híradásban, az R-403, R-401 rádiórelé-állomások, amelyeket a magyar ipar deciméteres (DM) sávval kiegészítve R-405 típusjelzéssel gyártott és sikeresen exportált. A Csoportfőnökség irányításával és gondozásában került sor egy – az adott időben – korszerű rádiórelé állomás kifejlesztésére és gyártására. Az R-1406 és 1412 típusjelzésű 6 illetve 12 csatornás berendezés rádiórészét (RDM) a csehszlovák ipar, míg a vivőfrekvenciás berendezéseket (H-6, H-12) a magyar híradástechnikai ipar gyártotta.

A technikai rejtjelző eszközök térnyerése – amelyek szoros kapcsolatban voltak a híradó szolgálat által biztosított átviteli utakkal – szükségessé tette a Csoportfőnökség és a VK Önálló 8. (rejtjelző) osztály összevonását.

1971 júliusában életbelépett szervezési rend a Csoportfőnökség elnevezését Magyar Néphadsereg Vezérkar 6. Csoportfőnökségre, az eddigi időszakos tervezés rendjét rövid, közép és hosszú távú tervezési ciklusra változtatta.

Az R-140 rádióállomások rendszerbeállítása, az R-142 rádióállomások beszerzéséről kialakított döntés, valamint a rádiórelé állomások tömeges megjelenése meghatározó jellegű változást eredményeztek a csapatok vezetésében. Ez időben alakultak ki a körvonalai a honi légvédelem hatékonyságát növelő grandiózus beruházások megtervezésének és e beruházások előkészítésének. E beruházások előkészítése a Csoportfőnökségre hihetetlen nagy terheket rótt.

1975-ben a csoportfőnökség megnevezése MN. Híradófőnökségre változott.

A Főnökség megkezdte a területi hírközpontok kialakításának előkészítő munkáit, amelyek összefogták az adott helyőrség béke híradását és így lényegesen jobb hatásfokkal működő béke hírrendszer alakulhatott ki. E hírközpontok alapját képezhették a rendkívüli körülmények között szükséges hírrendszer kialakításának is.

Ezzel egyidejűleg megkezdődött az ötéves fejlesztési tervek részletes kidolgozása, amely magába foglalta az akkori időben korszerű rádió, rádiórelé, mozgó tábori hírközpont elemek, vezetékes eszközök és építő-felszerelések, a sokcsatornás vivőfrekvenciás berendezések, új géptávíró, futár és tábori posta eszközök, továbbá a rejtjelző

és titkosító berendezések beszerzését, gépjárművekbe, objektumokba történő beépítését.

Ez időszak főfeladatait a fejlesztésből származó híradó feladatok végrehajtása jelentette. A fejlesztés eredményeként jelent meg a magyar ipar által gyártott R-107 rádió tranzisztorizált változata, az R-130 korszerűsített változata, amely az R-1340 típusjelzést viselte, továbbá az Orion által gyártott raj-szakasz rádió. A Finommechanikai Művek (FMV) megkezdte a 10 előreprogramozható frekvenciával rendelkező R-140 rádióállomás gyártását és exportálását. A Híradó Főnökség követelményei alapján – az állandó hírrendszerben működő tábori eszközök kiváltására – az Orion megalkotta az első gigaherzes (GHz) sávban digitális jelfolyam alapján működő mikrohullámú berendezést, amely a béke és az előkészített híradás területén hozott korszakos változást. A Híradó Főnökség és az ORION közös sikereként ez volt az ország első digitális mikrohullámú rendszere. A honi légvédelem nagyarányú korszerűsítése nagymérvű híradó beruházások megkezdését igényelte, ami jelentős erőket kötött le.

A Főnökség rendezte a táboriposta megszervezése és biztosítása területén lévő elmaradást.

A Főnökség részt vett a KGST Postai és Távközlési Állandó Bizottságának (POTÁB) munkájában, ahol mérsékletességével támogatta a szükséges – az ország érdekeit szolgáló – fejlesztéseket, és határt szabott a saját érdekeinken túlmutató, nehezen finanszírozható elgondolások megvalósításának.

A kiképzés korszerűsítése során a Főnökség tervei alapján közel fél milliárd forintos ráfordítással létrehozott Híradásipari Műszerész Tiszthelyettes Szaközépiskola (Vác) új gondolatokat és módszereket vitt a híradó tiszthelyettesek kiképzésébe. A tiszthelyettesi állomány minőségi javulását ígérték azok a követelmények, amelyeknek a hallgatóknak meg kellett felelni. Az iskola 4 éves kiképzési idejében – stabil tanári karral és korszerű felszereléssel – az érettségi és a híradásipari szakma mellett tiszthelyettesi rendfokozatot adott a hallgatóknak.

E szervezési ciklusban került sor a hagyományos hadsereg, hadosztály, ezred szervezeti forma, hadsereg, hadtest, dandár, zászlóalj szervezeti formává történő átalakításra, amely a híradó erők és eszközök újraosztását és a híradás-szervezési elvek módosítását igényelte, amit a Híradó Főnökség jó hatásfokkal megoldott.

A rendszerváltás folyamata a Híradó Főnökségnek semminemű gondot nem okozott.

A híradás és informatika között kialakult szimbiózis az adatok távolsági továbbításához a híradó szolgálat által létrehozott átviteli utakat igényelte. Különösen megmutatkozott ez a Tábori Automatizált Csapatvezetési Rendszer (PASZUV) elemeinek áttekintése során. Ekkor került napirendre a két szervezet összevonásának gondolata.

Az MN Híradó Főnökség állományába került a Rendszerszervezési, Vezetésgépesítési és Automatizálási (REVA) szolgálat, amely megtartotta a fejlesztés területén önállóságát. A Főnökség elnevezése ekkor MN Híradó Főnökségről MH Híradó és Automatizálási Csoportfőnökségre változott.

Ez időszakra esik a NATO békepartnerségi rendszeréhez való csatlakozás, valamint elgondolás született az ASOC NATO szabványú légtér ellenőrzési rendszer híradó vonzatainak megítélésére, a Jugoszlávia területén kitört etnikai háború kapcsán szükségessé vált intézkedések foganatosítására.

Először kerültek alkalmazásra katonai céllal az INMARSAT polgári műholdas rendszer eszközei, amelyek a boszniai IFOR magyar kontingens kiszolgálása után szinte valamennyi külföldi kontingens kitelepítésénél a híradás egyik megbízható eszközét képezte.

Első ízben jelentek meg az ISDN rendszerek, amelyek forradalmasították a híradást. Kialakították a hírrendszerek üzemképességének állandó ellenőrzését és üzembiztosságát garantáló hálózat-felügyeleti rendszert. Létjogosultságot kap az IP (Internet) protokollra épülő híradás gondolata, továbbá az irodai alkalmazásban megszokott vezetési eszközöknek tábori körülmények közötti adaptálása, a videokonferenciák gyakorlati megvalósulása, valamint a mobil telefonrendszerek a béke vezetés körülményei közötti tömeges alkalmazása.

A megváltozott biztonságpolitikai helyzetben a Csoportfőnökség nemzetközi kapcsolatai is átalakultak. A Csoportfőnökség közreműködőként és munkatársi szinten aktív szerepet vállalt az európai hagyományos fegyverek csökkentésének ellenőrzését célzó szerződés végrehajtásában, az ENSZ majd később az EBESZ és a NATO vezette békefenntartó missziókban.

Rendszeressé vált a magyar híradó törzsek, alegységek részvétele a nemzetközi NATO gyakorlatokon. A. NATO-hoz történt csatlakozás új, meghatározó fejezetet nyitott a híradó és informatikai szolgálat történetében. Új elgondolások és módszerek kerültek a híradás megszervezésének és biztosításának középpontjába. állományából állandó képviselők jelentek meg a NATO meghatározott szerveinél.

1996 szeptemberében a Csoportfőnökség elnevezése VK Híradó és Informatikai Csoportfőnökségre változott. Időközben a Csoportfőnökség átalakult és a VK Vezetési Főcsoportfőnökség alárendeltségében működött tovább.

2000-ben újból átalakításra került a Honvéd Vezérkar, melynek részeként a Főcsoportfőnökségeket megszűntették. A Főcsoportfőnökség bázisán jött létre a VK Vezetési Csoportfőnökség.

A csoportfőnökség kidolgozza az új hadműveleti elvekhez kapcsolódó híradó elgondolást, amelynek keretében a meglévő híradó technikai eszközöket és rendszereket szükségszerűen az új elvek szerint végrehajtandó hadműveleti feladatokhoz adaptálja. A Csoportfőnökségen a NATO követelményeknek megfelelően kidolgozásra került az MH híradásának részletes hosszú távú fejlesztési terve. A Csoportfőnökség támogatásával a Zrínyi Miklós Nemzetvédelmi Egyetem (ZMNE) Katonai Kommunikációs Rendszerszervező Tanszékén kidolgozásra kerülnek „a Magyar Honvédség állandó telepítésű kommunikációs rendszere továbbfejlesztésének technikai lehetőségei" illetve a „Tábori alaphírhálózat digitalizálásának lehetőségei egyes NATO tagországok kommunikációs rendszereinek tükrében" című értekezések.

A Csoportfőnökség viszonylag csökkentett állománnyal, a híradó, az informatikai, az elvi tervező és az információvédelmi osztállyal, valamint a törzsirodával átfogta a katonai kommunikációval kapcsolatos területek és feladatok egész vertikumát.

Az állandó hírrendszerben és a beszerzésben növelték a költséghatékony gazdálkodást, intenzíven keresték az új eszközök beszerzésének legoptimálisabb ár/érték arányú lehetőségeit.

A Csoportfőnökség felkészült az MH különféle kontingenseinek külföldi működése kommunikációs biztosítására és az eddigi tapasztalatok alapján e feladatainak maradéktalanul eleget tett.

Külön érdeme a Csoportfőnökségnek, hogy a szervezeti változások – és különféle más irányú ráhatások – közepette megóvta azt a fegyvernemi kultúrát és annak emlékeit, amelynek kitörölhetetlen jelei a szolgálat működésében ma is jelen vannak és reprezentálják azt a szakszerű munkát, amit hat évtized alatt a Csoportfőnökség vezetői és munkatársai a katonai vezetés folyamatosságának biztosításáért önzetlenül tettek.

A Honvédelmi Minisztériumot érintő 2005. évi jelentős szervezeti változások a teljes Honvéd Vezérkart érintették. A HVK Híradó és Informatikai Csoportfőnökség feladatrendszere 2005. április 1-jével jelentősen megváltozott.

A csoportfőnökséget képező híradó és informatikai osztály beépült az újonnan megalakított HM HVK Katonai Tervező Főcsoportfőnökségbe, és a VKF közvetlen alárendeltségébe került MH Híradó Parancsnokság.

Amikor a csoportfőnökség dióhéjba sűrített történetének végéhez érünk, megjelennek előttünk névvel és név nélkül azok a nagyszerű emberek, akik életének egy meghatározó darabja, munkája, verítéke a hat évtized folyamán – kötőanyagként - beépült abba az alapba, melyre az egymást követő generációk a Csoportfőnökséget – az adott kor követelményeinek megfelelően – mint felépítményt megalkothatták, és folyamatosan formálják.

Az alkotók között találjuk azokat a hazájukat szerető, a magyar királyi honvédségben szolgált híradó tiszt, tiszthelyettes bajtársainkat, akik a még dúló népirtó háború viszonyai között, egy új Magyarország demokratikus hadseregében képzelték el jövőjüket, akik hatvan évvel ezelőtt a Csoportfőnökséget létrehozták, és erejüket megfeszítve, mostoha körülmények között lerakták az alapokat. Sajnálatos, hogy az alapítók nagy többségét ellehetetlenítették, elbocsátották, többek – koholt vádak alapján – súlyos börtönbüntetést, internálást szenvedtek. Tisztelettel emlékezünk rájuk.

Megbecsüléssel és őszinte tisztelettel emlékezünk azokra a bajtársainkra, akik hittek egy eszmében és a munkapadokat, az eke szarvát elhagyva, katonai előképzettség nélkül, vállalták a tanulást, és nehéz körülmények között igyekeztek megfelelni a velük szemben támasztott erejüket meghaladó követelményeknek, és rövidebb-hosszabb ideig a Csoportfőnökségen szolgáltak döntő többségükben, szakmájuk elhivatott művelőivé váltak.

Megbecsüléssel gondolunk a Honvéd Kossuth Akadémiát, a Zalka Máté Híradó Tiszti Iskola, az Egyesített Tiszti Iskola (ETI), a Bolyai János Katonai Műszaki Főiskola (BJKMF) különböző évfolyamait végzett bajtársaink derékhadára, akik a Zrínyi Miklós Nemzetvédelmi Egyetemen (ZMNE), a külföldi híradó akadémiákon, egyetemeken szerzett felsőfokú képesítésükkel erősítették a Csoportfőnökség – minden szinten elismert – tekintélyét.

A hat évtized munkájának összesítésénél szembetűnő a Csoportfőnökség kifogástalan erkölcsi szilárdsága, magas szintű fegyelmi állapota, személyi állományának áldozatkészsége, kreativitása, a munkához való viszonya, a híradásért viselt személyes felelősségérzete.

Az elöljáró szervek a Csoportfőnökség munkáját, erkölcsi- anyagi szilárdságát folyamatosan magasra értékelték, amit az ellenőrzések eredményei, és az elismerések magas száma fémjelez. A Csoportfőnökség, de az egész híradó szolgálat történetében nem fordult elő, hogy valamely seregtest, magasabb egység, egység – a híradó szolgálat hibájából – nem megfelelő értékelést kapott volna. A Csoportfőnökség összmunkája pozitív megítélését meghatározó eredmények hátterében megtalálhatók az alárendelt híradó szolgálatok, csapatok, tanintézetek vezetői és végrehajtó állományának – ezred, zászlóalj, század és szakaszparancsnokok – a vezetés által kitűzött célok teljesítésére végzett odaadó lelkiismeretes munkája. Társadalmi szervezetekhez kötödésük példaértékű. Így a Budapesti Nyugállományúak Klubja Híradó Tagozatával, valamint a Puskás Tivadar Híradó Bajtársi Egyesülettel élő kapcsolattal rendelkezik. Tisztelettel ápolja – a hosszú időn át méltatlanul agyonhallgatott – a nagy magyar feltaláló és hazafi, Puskás Tivadar emlékét.

A híradó szolgálat ma szolgáló állománya – akik híven követik nevezetes elődeik példáját – meghajtja a tisztelet és elismerés zászlaját a Csoportfőnökségen 60 év alatt szolgált vezetők és valamennyi munkatárs előtt, akik – a politika pillanatnyi széljárásától függetlenül – a haza- és hivatásszeretettől vezérelve kiemelkedő munkájukkal megteremtették annak lehetőségét, hogy a Csoportfőnökség – elnevezésétől függetlenül – hat évtizeden át a Vezérkar elismert szervezeteként folyamatosan szolgálja a honvédelem ügyét.

**BOZSÓ Zoltán**

# A RENDŐRSÉGI TEVÉKENYSÉGIRÁNYÍTÁS, A TÖRZS MŰKÖDÉSE

Bozsó Zoltán rendőr ezredes
Rendőrségi főtanácsos
PMRFK Közbiztonsági Igazgató
Főkapitány-helyettes

Telefon:06-20/444-1260
Fax:01-443-5103
E-mail:bozsoz@orfk.b-m.hu
bozsoz@dunaweb.hu

A rendőrség szolgálati munkájában kiemelt jelentőségük van az összetett rendőri műveletek vezetésének, amelyek előkészítése és végrehajtása a rendőri szervek vezető és beosztott állományától magas fokú szakmai ismereteket, hozzáértést és tervszerűséget igényel. Az Országos Rendőr-főkapitányságon, a rendőr-főkapitányságokon és központi alárendeltségben lévő más területi rendőri szerveknél létre kell hozni a csapaterő vezetésének szerveit, ki kell jelölni állományát és ki kell dolgozni a részletes munkarendjét.

## A törzs

A törzs az Országos Rendőr-főkapitányságon, a rendőr-főkapitányságokon, a Rendészeti Biztonsági Szolgálatnál (REBISZ) a rendőri műveletek vezetésének alapvető szerve. Ideiglenesen működtetett szervezeti elem, amely közvetlenül részt vesz az alárendeltek feladatainak megtervezésében, a végrehajtás szervezésében és irányításában.

## A törzs alapvető feladatai:

- a közbiztonsági és a bűnügyi helyzetre, valamint a rendőri és együttműködő szervek helyzetére vonatkozó adatok állandó ismerete, azok gyűjtése, nyilvántartása, elemzése, értékelése;
- a rendőrfőkapitány elhatározásának meghozatalához szükséges számvetések, javaslatok elkészítése;
- az alkalmazási tervek, írásos intézkedések, parancsok, jelentések, tájékoztatások kidolgozása, a szóban kiadott parancsok okmányolása;
- a feladatoknak az alárendeltekhez való eljuttatása és azok végrehajtásához a felkészülés megszervezése;
- a vezetési pont működtetése;
- a tapasztalatok gyűjtése, tanulmányozása, elemzése, általánosítása, az alárendeltekhez és az elöljáróhoz való eljuttatása;
- az alárendeltek részére megszabott feladatok végrehajtásának segítése és ellenőrzése;
- a mindenoldalú biztosítás feladatainak megtervezése és végrehajtásuk összehangolása;

- a híradás és az együttműködés fenntartása.

A megyei rendőr-főkapitányságokon a törzs vezetője a közrendvédelmi osztályvezető, a Budapesti Rendőr-főkapitányságon a közrendvédelmi főosztályvezető.

Az Országos Törzs vezetője teljes feltöltöttség esetén az ORFK Közrendvédelmi és Közlekedésrendészeti Főosztály vezetője.

A törzs közbiztonsági, bűnügyi, híradó, anyagi-technikai-egészségügyi és összekötő-futár csoportokból álljon. Az Országos Törzsben szükség esetén külön személy- és létesítménybiztosítási csoport is működhet.

A közbiztonsági csoport rendeltetése a közbiztonsági helyzet elemzése, értékelése; a következtetések alapján javaslatok kimunkálása a feladat megoldására irányuló döntéshez; a kidolgozott intézkedéseknek a végrehajtók részére történő eljuttatása; a helyzet adatainak gyűjtése; számvetések kidolgozása; a szomszédos és együttműködő szervek tájékoztatása; a rendőrfőkapitány szóban kiadott utasításainak, parancsainak rögzítése, az elhatározás előkészítése és formába öntése, parancsok intézkedések kidolgozása; az együttműködés megszervezésének előkészítése; a csapatfelderítés és az álcázás rendszabályainak kidolgozása; a rejtett vezetést szolgáló okmányok kidolgozásának irányítása; a vezetési pont telepítésének, áttelepítésének, őrzésének és védelmének a megtervezése; az ügyeleti szolgálat megszervezése a törzsben és a vezetési ponton; az elöljáró számára szóló jelentések összeállítása; az eseménynapló és a nyilvántartó térkép vezetése; az alárendeltek ellenőrzésének és a tevékenységekhez való felkészülésük segítésének a megszervezése.

A bűnügyi csoport feladata a döntéshez szükséges bűnügyi információk beszerzésének megtervezése, megszervezése, a bűnügyi szervek tevékenységének irányítása; a felderítési feladatok, nyomozási cselekmények összehangolása; a beérkező adatok feldolgozása és továbbítása a törzs vezetőjének, illetve a rendőrfőkapitánynak.

A híradó- és informatikai csoport feladata a híradás megtervezése, a híradó és informatikai rendszer üzemkészségének fenntartása; a vezetési pontok települési helyeinek állandó ismerete; az alárendelteknek szóló híradó intézkedések, tervek, okmányok kidolgozása és eljuttatása a hírrendszer telepítésének irányítása; a híradó eszközökön folytatott párbeszédek szabályainak és a híradó-üzemfegyelem rendszabályainak megkövetelése és ellenőrzése; a rádióelektronikai védelem rendszabályainak a kidolgozása; a törzs állományának kiképzése a technikai eszközök kezelésére, a rejtett vezetést szolgáló okmányok alkalmazására; az alárendeltek híradó eszközökkel történő ellátásának biztosítása, azok üzemeltetésének és nyilvántartásának megszervezése; a csapattevékenység informatikai biztosítása.

Az anyagi-technikai-egészségügyi csoport feladata a tevékenység mindenoldalú biztosításának részeként az anyagi ellátás, a technikai eszközök kiszolgálásának és a személyi állomány egészségügyi ellátásának megtervezése, megszervezése; az anyagi, technikai, egészségügyi biztosítás tervének kidolgozása és az abban foglalt feladatoknak az alárendeltekhez történő eljuttatása; a vezetési pont településének, áttelepülésének, anyagi kiszolgálásának közvetlen irányítása.

Az összekötő-futár csoport a feladat jellegétől függően, szükség szerint kerül létrehozásra. Feladata a rendőrfőkapitány, a törzs, valamint az elöljáró és az alárendelt szervek között a parancsok, intézkedések, jelentések továbbítása; a küldemények kézbesítése; az együttműködő szervekkel a folyamatos kapcsolat biztosítása, javaslattétel

a közös feladatok pontosítására, összehangolására, a megerősítő szervek alkalmazásának módjára.

A személy- és létesítménybiztosítási csoport feladata a védett vezetők, delegációk és objektumok biztonságára vonatkozó adatok gyűjtése, elemzése, értékelése; az általános veszélyeztetettségi szint meghatározása; a biztonság megteremtése és fenntartása érdekében szükséges szolgálati követelmények meghatározása; a megelőző, a személy- és objektumvédelmi állomány tevékenységének megtervezése; az erre vonatkozó szolgálati okmányok kidolgozása; a szolgálati ágak közötti koordináció végrehajtása; kapcsolattartás és koordináció az érintett külső szervekkel; javaslattétel a szolgálati ágak, szolgálatok személy- és létesítménybiztosítási feladataira.

A közbiztonsági csoport 3-5, a többi csoport 2-3 fős lehet. Ettől a rendőrfőkapitány a feladatok jellegétől függően eltérhet, a csoportok létszámát növelheti. A törzs állományát ki kell egészíteni a gépíróval, rajzolóval. Az összekötőfutár csoportot más rendőri szervtől vezényelt összekötő tiszttel akkor kell kiegészíteni, ha azt a feladat jellege igényli; századnál nagyobb alegységgel a rendőr-főkapitányság erőit megerősítették, illetve a művelet keretében speciális szolgálat (pl.: a REBISZ speciális erői) vagy a Köztársasági Őrezred is működik.

Amennyiben a végrehajtandó feladat jellege szükségessé teszi, hogy a vezetést más, rendőrségen kívüli szervek döntési jogkörrel rendelkező képviselői is segítsék, úgy ezek a személyek általában nem a törzsben, hanem a rendőrfőkapitány (rendőri szerv vezetője) mellett működő külön tanácsadó, segítő testületben (operatív bizottságban, vezetői válságkezelő csoportban) tevékenykednek.

A törzsek működtethetők az illetékes rendőrfőkapitány (parancsnok) döntése alapján, az adott feladattól függően teljes vagy a feladat jellegétől függően részleges állománnyal. Részlegesen működtetett törzs esetén az adott feladat időtartamára a törzs vezetőjének a meghatározottaktól eltérő személy is kijelölhető.

A törzs eredményes munkája elérhető az oda beosztott állomány magas szintű szakmai felkészítésével, a törzs folyamatos és szilárd vezetésével; a rendőrfőkapitány intézkedéseinek és az elöljáró törzs által meghatározott feladatoknak a pontos és időbeni végrehajtásával; a közbiztonsági és bűnügyi helyzet, valamint a rendőri szervek feladatainak, a végrehajtás feltételeinek és lehetőségeinek pontos ismeretével; a feladatok törzsön belüli helyes elosztásával, a kölcsönös helyettesítések biztosításával; a törzs és az alárendeltekkel szembeni magas fokú követelménytámasztással és a kiadott intézkedések végrehajtásának szigorú ellenőrzésével; a híradás megbízható fenntartásával; a vezetés automatizálásra szolgáló informatikai rendszerek és eszközök hozzáértő alkalmazásával.

A rendőri feladatok hatékony vezetésének leglényegesebb feltétele az elöljáró és alárendelt törzsek, valamint más vezetési szervek közötti helyes kapcsolat kialakítása, összehangolt munkájuk biztosítása. Ennek érdekében:

Az elöljáró törzsek kötelesek időben meghatározni az alárendeltek feladatait, tájékoztatni őket a kialakult helyzetről, az őket érintő rendszabályokról és elhatározásokról; megbízható híradást szervezni és fenntartani az alárendeltekkel; kidolgozni és eljuttatni azokhoz a szükséges okmányokat; meghatározni a jelentések és más okmányok felterjesztésének rendjét; szükség esetén javaslatot tenni az alárendeltek vezetési pontjainak helyére, áttelepülésük rendjére; segíteni az alárendelt törzsek munkáját és

ellenőrizni azok tevékenységét; szükség esetén ellátni az alárendelteket térképpel és egyéb anyagokkal.

Az alárendelt törzsek kötelesek végrehajtani az elöljáró törzs utasításait; a meghatározott időre a követelmények szerint, illetve saját kezdeményezésre jelenteni a helyzetre vonatkozó adatokat, a rendőrfőkapitány elhatározását és az alárendeltjeik részére kiadott intézkedéseket; időben felterjeszteni a jelentéseket, a kidolgozott tervek, intézkedések és más okmányok meghatározott számú példányát; az összeköttetés megszakadása esetén kihasználni minden lehetőségét annak helyreállítására.

### A törzsbe beosztottak feladatai

A törzsben a munka fő szervezője a törzs vezetője. Közvetlenül a rendőrfőkapitánynak, vagy az általa a csapaterő vezetésére intézkedésben kijelölt parancsnoknak (továbbiakban együtt: parancsnok) van alárendelve, szolgálati elöljárója a törzsbe beosztott személyi állománynak.

### A törzs vezetője:

### Felelős:

- a törzsre háruló valamennyi feladat végrehajtásáért;
- a kiadott intézkedések okmányolásáért és továbbításáért;
- a vezetés folyamatosságának fenntartásáért, a híradás megszervezéséért;
- a vezetési pont működési feltételeinek megteremtéséért és fenntartásáért.

### Köteles:

- felkészíteni a törzsbe beosztott állományt feladataik végrehajtására;
- összehangolni a törzs csoportjainak tevékenységét, tájékoztatást adni részükre a helyzetről és a kapott feladatról;
- meghatározni a feladatok végrehajtásának rendjét a törzsön belül;
- ismerni a rendőri tevékenység tervét, az alárendelt szervek helyzetét, állapot, lehetőségeit, feladatait, rendelkezésre álló erőket és eszközöket;
- következtetéseiről, javaslatairól soron kívül jelentést tenni a parancsnoknak;
- ellenőrizni az alapvető fontosságú intézkedések, parancsok végrehajtását.

### Jogosult:

- az alárendelt törzsektől, szervektől, ügyeleti szolgálatoktól adatok, javaslatok, jelentések bekérésére;
- tájékoztatást kérni és adni más rendőri és együttműködő szervek részére a végrehajtott, illetve tervezett feladatokról, a helyzetről;
- meghatározni a mindenoldalú biztosítás részletes rendszabályait.

A közbiztonsági csoport vezetője a törzs vezetőjének helyettese. Egy személyben felelős a csoportra háruló feladatok maradéktalan végrehajtásáért, a törzs vezetőjének időben történő tájékoztatásáért; a helyzetről és az alárendeltek állapotáról szóló, valamint a megszabott feladatok végrehajtására vonatkozó adatok gyűjtéséért és feldolgozásáért. Jogosult a tervokmányok kidolgozása érdekében a munkába bevonni a törzs más csoportjainak, valamint a szolgálati ágak, szolgálatok, szakszolgálatok tisztjeit.

A bűnügyi csoport vezetője felelős a közbiztonsági és bűnügyi helyzetre vonatkozó adatok folyamatos gyűjtéséért, elemzéséért, értékeléséért; a szükséges adatok

lehetőség szerint időben történő beszerzéséért; a nyílt és operatív adatgyűjtés érdekében alkalmazott bűnügyi és más felderítő szervek felkészítéséért, tevékenységük összehangolásáért, irányításáért; az információk ellenőrzéséért.

A híradó- és informatikai csoport vezetője felelős a csoport szakmai munkájáért; a törzsön belüli, az alárendelt és együttműködő szervekkel, a szomszédokkal a híradás és az informatikai kapcsolatok megszervezéséért és folyamatos fenntartásáért; az informatikai biztosítás megszervezéséért; a híradó- és informatikai állomány feladat-végrehajtásra való állandó készenlétért; a híradó- és informatikai eszközök szakszerű alkalmazásáért és üzemeltetéséért; a biztosító és kiszolgáló szervek felkészítéséért és tevékenységük koordinálásáért.

Az anyagi-technikai-egészségügyi csoport vezetője felelős az anyagi ellátás, a technikai eszközök kiszolgálásának és a személyi állomány egészségügyi ellátásának megtervezéséért, megszervezéséért; a szállítási, utánszállítási feladatok megszervezéséért és irányításáért; az anyagi, technikai, egészségügyi biztosítás tervének kidolgozásáért és az abban foglalt feladatoknak az alárendeltekhez történő eljuttatásáért; a vezetési pont településének, áttelepülésének, anyagi kiszolgálásának közvetlen irányításáért.

Az összekötő-futár csoport vezetője felelős az oda beosztottak fegyelméért, feladat-végrehajtásra való állandó készenlétért. Ismerje kit, mikor, milyen feladattal bíztak meg, hová indítottak útba, mikor várható visszaérkezése, illetve a feladat befejezése. Távollétében helyettesét a törzs vezetője jelöli ki.

A személy- és létesítménybiztosítási csoport vezetője felelős a csoportra háruló feladatok maradéktalan ellátásáért; a törzs vezetőjének időben történő tájékoztatásáért; a szükséges belső és külső koordinációk végrehajtásáért; a nyílt és operatív védelmi-biztonsági intézkedések megtételéért.

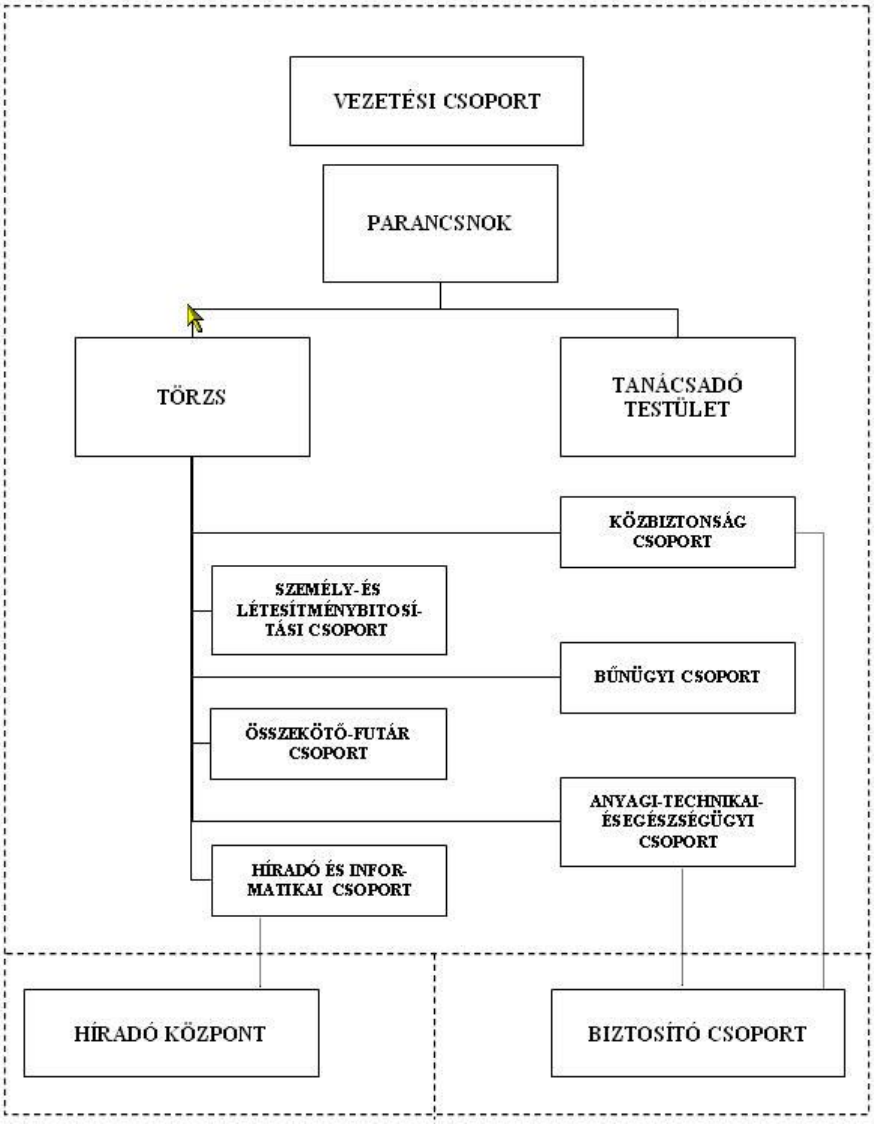
### A törzsbe beosztott tisztek kötelesek:

- folyamatosan bővíteni szakmai és vezetési ismereteiket;
- jól ismerni a rendőri műveletekben alkalmazható szolgálati formákat és taktikai eljárásokat, azok előkészítésének és végrehajtásának rendjét, az alárendeltek szervezetét, eszközeit és lehetőségeit;
- pontosan végrehajtani a beosztásukkal járó feladatokat;
- készen állni egymás helyettesítésére; sokoldalúan értékelni a helyzetet és ennek alapján megalapozott javaslatokat tenni; gyorsan és pontosan elkészíteni a szükséges számvetéseket, okmányokat;
- pontosan és röviden jelenteni a helyzetre vonatkozó adatokat és a számvetések eredményeit, a következtetéseket és javaslatokat; áttekinthetően és pontosan vezetni a munkatérképeket és más nyilvántartó okmányokat; ismerni a híradó és az automatizált vezetési eszközök kezelését;
- szigorúan betartani a rejtett vezetés szabályait, a híradó és más vezetési eszközök alkalmazásának biztonsági rendszabályait;
- betartani a titokvédelem követelményeit.

### A vezetési pont

A vezetési pont az a meghatározott kiterjedésű, technikai és más eszközökkel berendezett terület, amely a feladatok előkészítése és végrehajtása időszakában egy-

aránt biztosítja a vezető szervek (személyek) folyamatos működéséhez szükséges feltételeket, lehetővé teszi az alárendeltek tevékenységének közvetlen irányítását. A vezetési pont általában rendőrségi vagy más objektumban, szükség esetén a terepen hozható létre (1. ábra).




1. ábra A Vezetési Pont felépítése

A vezetési pont vezetési csoportra, híradóközpontra és biztosítócsoporta tagozódik

A vezetési csoport a vezetési pont alapvető eleme, amely a parancsnokból, a tanácsadó testületből (operatív bizottság), valamint a törzsből áll. Rendeltetése a kü-

lönböző munkahelyen lévő szolgálati személyek összehangolt, tervszerű munkájával az elhatározás megalkotása, a döntések meghozatala, a törzsszolgálati feladatok ellátása, az alárendelt szervek vezetése.

A híradóközpont rendeltetése a folyamatos és megbízható összeköttetés biztosítása a vezetési ponton belül az elöljáróval, az alárendeltekkel és az együttműködő szervekkel. A híradó és informatikai eszközöket és azok kezelőállományát foglalja magában.

A biztosítócsoport rendeltetése a vezetési pont személyi állománya munkájához, pihenéséhez, ellátásához a megfelelő feltételek biztosítása, a vezetési pont őrzése. Állományába őrség, szállító részleg és ellátó részleg tartozik. A biztosítócsoport általában a vezetési csoporttól elkülönítve helyezkedjen el.

Lakossági tájékoztató, információs szolgálat működtetése a biztosítás vezetési pontján. Külön városi telefonszámok megadása a tömegkommunikáció részére, ahová bármilyen felvilágosításért lehet fordulni. A tájékoztató szolgálat folyamatos, kapcsolatot tart a biztosítás rendvédelmi szervei, illetve a tömegkiszolgálásban résztvevő más szervek (mentő, tömegközlekedés, kommunális létesítmények, egészségügyi létesítmények, stb.) ügyeleteivel.

A vezetési pont létrehozásának (településének) helyét és idejét a parancsnok határozza meg. Helyét csak azok ismerhetik, akiknek szolgálati feladataik ellátásához az feltétlenül szükséges.

A vezetési pont megszervezéséért a törzs vezetője a felelős, aki meghatározza a vezetési pont állományát, a munkavégzés, az ügyeleti szolgálat ellátásának, a pihentetésnek a rendjét, a vezetési pont őrzés-védelmével kapcsolatos rendszabályokat és szükség esetén az áttelepülés feladatait.

A vezetési pont helyének pontos kijelölése és annak berendezése érdekében előkészítő részleg kerülhet kijelölésre. Az előkészítő részleg vezetőjének meg kell határozni:

- a vezetési pont létesítésének helyét;
- a berendezéssel kapcsolatos feladatokat, követelményeket;
- a híradást milyen rendszerben kell kiépíteni;
- az őrzés szabályait;
- a végrehajtás határidejét;
- az előkészítő részlegbe beosztott erőket és eszközöket.

Szükség esetén gondoskodni kell a vezetési pont álcázásáról és a polgári személyektől (a lakosságtól) történő elszigeteléséről. A vezetési pont körzetében szabályozni kell a személyi állomány és a szállító eszközök mozgásának rendjét. A vezetési ponton tartalék alegység, előállító hely, sajtóközpont nem helyezhető el.

A vezetési pont őrzésére és védelmére tervet kell készíteni, amely szöveges, rajzos és táblázatos formában tartalmazza:

- vezetési pont elemeinek elhelyezkedését;
- az őrzendő objektumokat, az őrzésre kijelölt erőket;
- az őrök felállítási helyét, a járőrök menetvonalait, feladataikat;
- a tüzelőállásokat;
- a riasztás, értesítés rendjét, jeleit, jelzéseit;
- az áttelepüléssel kapcsolatos feladatokat és az egyéb szükséges rendszabályokat.

Őröket kell felállítani a vezetési pont bejáratához, a vezetési csoporthoz, a híradóközponthoz és szükség esetén azokba az irányokba, ahonnan egy erőszakos fellépés, illetéktelen behatolás valószínűsége a legnagyobb. A rendőri művelet vezetőjét mozgása során a kialakult helyzettől függően fedező csoporttal kell biztosítani.

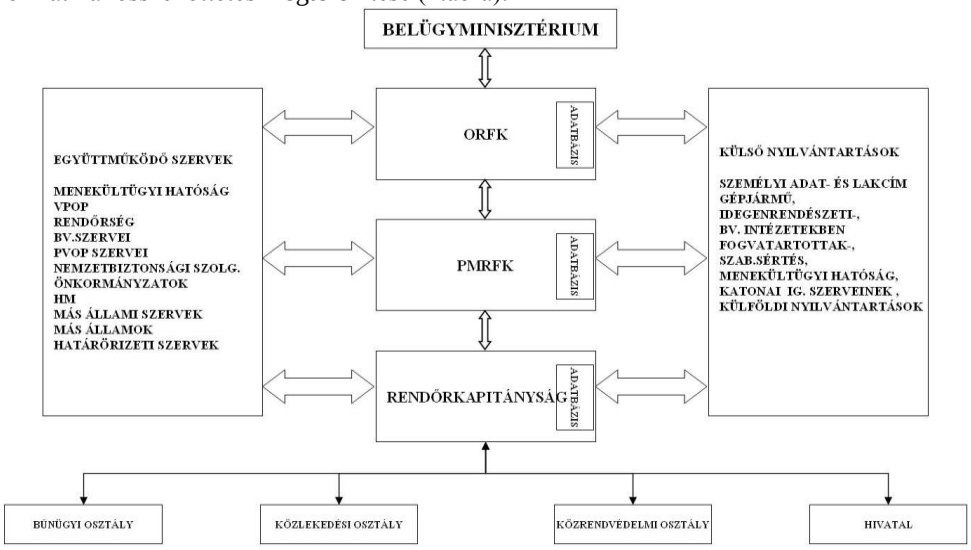
A vezetési ponton vezetési pont ügyeletest kell kijelölni. Az ügyeletes ismerje a kialakult helyzetet, az alárendeltek tevékenységét, vezetési pontjai helyét, a vezetési pont munkarendjét, az ellenőrzés és a pihentetés tervét, az őrzés és a védelem tervét, a műveletet irányító parancsnoknak, helyetteseinek, a törzs vezetőjének és a törzs csoportjai vezetőinek tartózkodási helyét; az értesítés és riasztás jeleit, jelzéseit.

A rendőri művelet körzetén belül, a fő feladat végrehajtásának körzetében a parancsnok részére figyelőpont is berendezhető. A figyelőpont rendeltetése a fő feladatot végrehajtó alárendeltek tevékenységének közvetlen megfigyelése és azok vezetése a végrehajtás legfontosabb időszakban. A vezetési pont állományából a figyelőponton csak a legszükségesebb szolgálati személyek tartózkodhatnak. Amikor a parancsnok a figyelőponton van, helyettesének minden esetben a vezetési ponton kell tartózkodni.

A vezetési pont mellett, attól legfeljebb 2 km távolságra helikopter-leszállóhely is kijelölhető. A helikopter-leszállóhely őrzéséről külön gondoskodni kell.

### A rendőri műveletek híradó- és informatikai biztosításának végrehajtása

A rendőri műveletek eredményes végrehajtásának egyik alapvető feltétele a tevékenységet irányító parancsnokok, a törzsek, a végrehajtó állomány, valamint az együttműködő szervezetek között a vezetékes, és/vagy vezeték nélküli híradó- és informatikai összeköttetés megteremtése (2.ábra).




2. ábra Városi rendőrkapitányság informatikai kapcsolatrendszere /vázlat/

Az országos jelentőségű, vagy a területi szervek által önállóan végrehajtott feladatok híradó- és informatikai biztosításának zavartalansága érdekében:

- a rendőri szervek szervezeti, vezetési rendszeréhez;

- forgalmazási sajátosságaihoz;
- területi elhelyezkedéséhez rugalmasan igazodó (igazítható) híradó- és informatikai rendszert kell létesíteni.

**A híradó- és informatikai biztosítás elemei**

A telepített és mobil vezetékes, valamint vezeték nélküli eszközök, amelyek részegységeit

- hírközpontok;
- különböző hírhálózatok;
- híradópontok;
- az állandó hírrendszer (vezetékes, vezeték nélküli);
- és a feladatok végrehajtásához létrehozott ideiglenes híradó rendszerek alkotják.

Rendőri műveletek végrehajtása során az összeköttetés biztosítható jelzőeszközök felhasználásával és futárok indításával is.

**A híradó- és informatikai összeköttetéssel szemben támasztott követelmények**

- feleljen meg a rendőri művelet parancsnokának a feladat végrehajtására hozott elhatározásának;
- biztosítsa a vezetési, értesítési, együttműködési híradást;
- biztosítsa a folyamatos, megbízható, többcsatornás összeköttetés feltételeit;
- a feladat végrehajtásában, a vezetésben beállt változásoknak megfelelően legyen rugalmas és gyorsan átszervezhető;
- biztosítsa a művelet parancsnokának a vezetési pontjáról történő eltávozásakor az összeköttetést a vezetési ponttal, az elöljáróval, az alárendeltekkel, valamint az együttműködő szervekkel;
- biztosítsa a feladat jellegének megfelelő rejtett vezetés feltételeit;
- alkalmazkodjon a terep sajátosságaihoz;
- biztosítsa a feladat végrehajtásához szükséges központi adatbázisokhoz történő hozzáférést, az információk gyűjtésének az értékelő-elemző munka végzésének informatikai feltételeit;
- biztosítsa a követelményeknek megfelelő kép- és hanginformációk dokumentálásának feltételeit.

A híradó és informatikai biztosítás megszervezése, valamint az erre vonatkozó terv elkészítése a csapatszolgálati törzs híradó- és informatikai csoport vezetőjének a feladata.

**A csapatszolgálati törzs híradó- és informatikai csoportjának vezetője**

A parancsnoki elhatározás alapján értékelje:

- a rendőri művelet híradó- és informatikai igényét;
- a működési terület infrastrukturális ellátottságát;
- a terep sajátosságait;
- a szolgálati csoportok információ igényét;
- a híradó- és informatikai biztosítás megszervezésének és létesítésének időszükségletét;
- a feladat végrehajtásához szükséges központi adatbázisok és azok felhasználóinak körét;

- a vezetési pontok, átjátszóállomások működtetéséhez szükséges erő- és eszköz szükségletet;
- a kép- és hangdokumentáció követelmények feltételrendszerét, a rendelkezésre álló, illetve bevonható technikai eszközök mennyiségét.

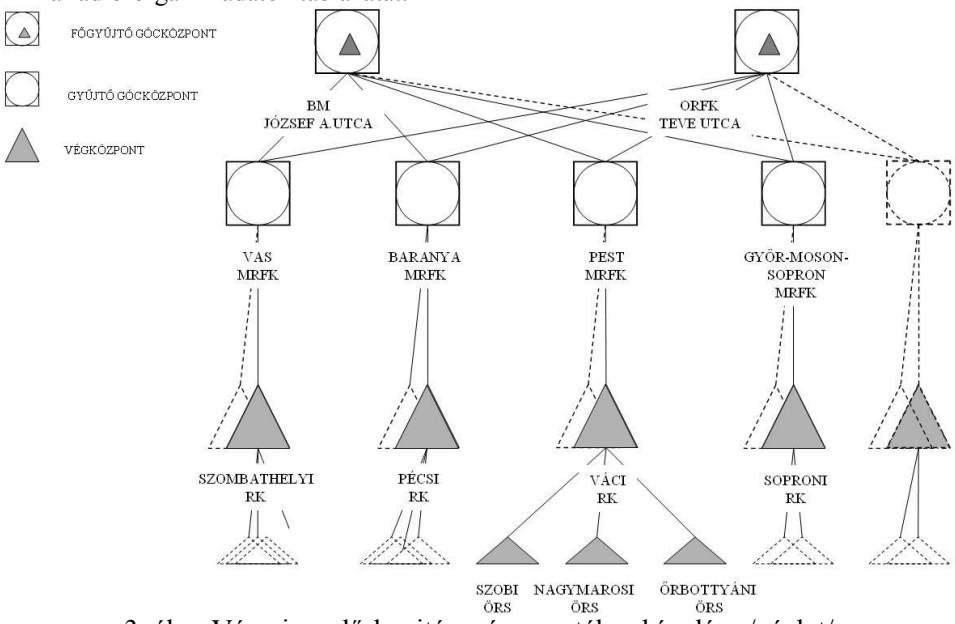
A meghatározottak alapján a rendőri művelet híradó- és informatikai biztosítására, a tevékenység dokumentálására hozott elgondolását jelentse a törzs vezetőjének, tegyen javaslatot a vezetési pont(ok) telepítési helyére, híradórendszer felépítésére. A jóváhagyott híradó- és informatikai elgondolás és a törzs vezetőjétől kapott utasítások figyelembevételével intézkedjen a híradó- és informatikai biztosítás tervének kidolgozására, illetve a híradórendszer telepítésének előkészítésére.

A híradó- és informatikai biztosítás megszervezésekor vegye figyelembe:

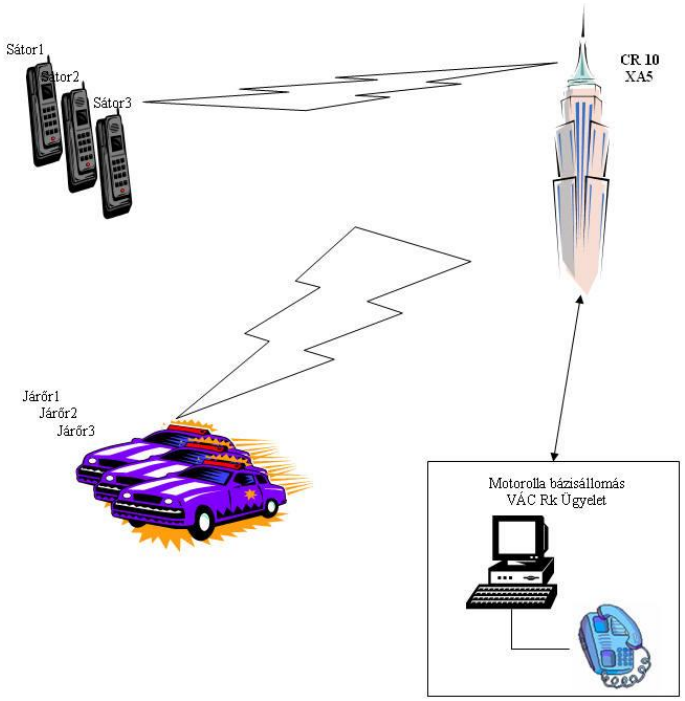
- a vezetési pontok telepítésénél az elöljáróval, az együttműködőkkel, az alárendeltekkel történő kapcsolat tartásához meg kell teremteni - az állandóan üzemelő, vagy ideiglenesen kiépített távbeszélő hálózatok (zárt és közcélú vezetékes, illetve vezeték nélküli) felhasználásával - a távbeszélő összeköttetés feltételeit. Biztosítani kell az írásos anyagok továbbításának lehetőségét, a központi adatbázisokhoz történő hozzáférést, valamint a feladatban résztvevő erők informatikai kiszolgálását;
- a híradó- és informatikai összeköttetést az állandóan üzemelő rádió hírrendszerek (megyei, ügyeleti és mozgószolgálati, őr-járőr szolgálati) mellett - a szolgálati csoportok feladatához és területi elhelyezkedéséhez igazodó - ideiglenes rádióforgalmi rendszerek létesítésével kell megoldani;
- a megyei ügyeleti és mozgószolgálati rádióforgalmi rendszereket elsősorban a vezetési, valamint az együttműködési híradás megszervezéséhez kell felhasználni;
- az alegységeken, illetve szolgálati csoportokon belüli zárt hírrendszerek létesítéséhez ideiglenes rádióforgalmi csatornák kerüljenek alkalmazásra. A csatorna kiosztásnál kerülni kell az érintett rendőrkapitányságok állandó rádióforgalmi rendszereivel történő kölcsönös zavarást;
- az ideiglenes rádióforgalmi hírrendszerek megbízható üzemeltetését kisegítő hírközpontokkal, átjátszó, illetve közvetítő állomásokkal kell biztosítani;
- a feladat jellegének megfelelően a rejtett vezetés érvényesítéséhez, illetve a megbízható vezetés fenntartásához alkalmazni kell a teljes, vagy részleges rádiótilalmat, a rendszeresített rejtjeltechnikai eszközöket, a tevékenység fedésére kidolgozott szolgálati közlemények táblázatát;
- a megyei ügyeleti és mozgószolgálati rádióforgalmi rendszerekbe történő kölcsönös bekapcsolódással kell biztosítani a szomszédos megyékkel történő együttműködést;
- az együttműködő szervekkel a rádióhíradás megszervezéséhez elsősorban az erre a célra kijelölt közös frekvenciát (csatornát) kell felhasználni, szükség esetén kezdeményezni kell készülék átadásával, az egymás rádióforgalmi rendszerébe történő bekapcsolódás feltételeinek biztosítását;
- feladathoz a szervezetnek kiutalt állandó, illetve ideiglenes hívóneveket kell alkalmazni.

**A rendőri művelet végrehajtására készített híradó- és informatikai biztosítási terv tartalma**

- a rendőri művelet célját, a létrehozott alegységek, szolgálati csoportok feladatát, összetételét;
- a vezetési pont(ok) telepítésének helyét, idejét, valamint a vezetési pont részére telepítésre kerülő kommunikációs, informatikai és dokumentációs feltételek biztosítását;
- a távbeszélő híradás tervét;
- a feladat végrehajtásához szükséges központi adatbázisokhoz történő hozzáférés megvalósításának módját, az adatbázisok várható felhasználói körét, a lekérdező hely és a felhasználói állomány közötti összeköttetés rendjét, a törzs működéséhez biztosított informatikai eszközök meghatározását;
- a tervezett rádiórendszerek biztosításának, működtetésének tervét, az átjátszóállomások telepítésének helyét, idejét, áttelepítésének rendjét, a működtetésének személyi, anyagi, technikai feltételeit;
- a híradó és informatikai biztosítás személyi és technikai támogatásának rendjét;
- a biztosítási terv melléklete tartalmazza;(3.ábra)
- vezetékes híradás vázlatát, ha ideiglenes vezetékes hírás kerül kiépítésre;
- a rádióhíradás vázlatát;(4.ábra)
- a fontosabb távbeszélőszámok jegyzékét;
- a rádióforgalmi adatok táblázatát.




3. ábra Városi rendőrkapitányság vezetékes híradása /vázlat/




4. ábra Városi rendőrkapitányság rádióhíradása /vázlat/

A jóváhagyott híradó- és informatikai tervet tájékoztatásul meg kell küldeni az állandóan üzemelő rendszerek országos műszaki felügyeletét végző:

- ORFK Híradástechnikai Szolgálat igazgatójának;
- Központi informatikai adatbázisok alkalmazása esetén a BM Központi, Adatfeldolgozó, Nyilvántartó és Választási Hivatal vezetőjének.

Az előre nem tervezhető, azonnali rendőri beavatkozást igénylő esetekben a híradó és informatikai feltételek biztosítása az állandóan üzemelő rendszereken alapul. A híradó- és informatikai biztosítást, a feladatot irányító parancsnok szóbeli utasítása alapján, a változó helyzethez igazodva, a feladat végrehajtásának folyamatában kell megszervezni, különböző rendszabályok bevezetésével, ideiglenes hírrendszerek létesítésével.

A rendőri műveletekhez alkalmazott megyei ügyeleti és mozgószolgálati rádióforgalmi rendszer működőképessége kiemelt műszaki felügyeletének biztosításához az érintett rádió távközlési központ ügyeletét az igénybevett rádióforgalmi rendszerekről távbeszélőn tájékoztatni kell.

Az együttműködésre kijelölt szervek vezetői, parancsnokai az illetékes híradó- és informatikai csoportvezető tervének figyelembevételével saját híradó- és informatikai erőivel, eszközeivel biztosítsák a feladatba bevont állomány tevékenységéhez szükséges híradó- és informatikai feltételeket.

**CSER Ádám**

# KÉPI INTEROPERABILITÁSI PROBLÉMÁK ÉS MEGOLDÁSOK A NATO-BAN

## Aktualitás

A Védelmi Képességek Kezdeményezése a világon megváltozott fenyegetésekre és védelmi kihívásokra kíván választ adni. Ebben kiemelkedő szerep jut a felderítésnek, az együttműködésnek és az ezeket támogató informatikai rendszereknek.

„Védelmi Képességek Kezdeményezése (DCI) úgy lett megtervezve, hogy biztosítsa a szövetséges erők együttműködő képességének megőrzését, és a szövetség tagjai folyamatosan fejlesszék és frissítsék erre való képességüket, hogy szembenézhessenek az új biztonsági kihívásokkal" - mondta General Lord Robertson főtitkár 1999-ben Washingtonban, a Védelmi Képességek Kezdeményezésének (Defense Capabilities Initiative, DCI) bemutatásakor.

A NATO növekvő hangsúlyt fektet a tagok védelmi eszközei közötti együttműködési képesség megteremtésére és fenntartására, 1999-óta kiemelt módon kezeli az informatikai eszközök – köztük a felderítési és képalkotó eszközöket– kompatibilitását, interoperabilitását.

## Együttműködő képesség keretrendszere

A NATO Együttműködő Képesség Keretrendszeréhez (NATO Interoperability Framework, NIF) szorosan kötődve a IV. Légi Csoport (Air Group IV.) dolgozik a felderítési képalkotó rendszerek együttműködő képességén, elsősorban a légi felderítés szemszögéből közelítve. Ugyanakkor a felderítés és hírszerzés szakmai közösségének nyomására kiterjesztették látókörüket a légi felderítésen kívül eső általánosabb felderítési és hírszerzési információk befogadására, a rendszerbe történő integrálására is.

Ennek a munkának a eredménye a NATO Képi Információk Együttműködésének Architektúrája (NATO Imagery Interoperability Architecture, NIIA). Ez a keretrendszer az együttműködési képesség négy szintjét határozza meg :

- szint : strukturálatlan adatok cseréje – ember által értelmezhető strukturálatlan adatok cseréje pl: folyó szövegek átadása úgymint jelentések és analízisek;
- szint: strukturált adatok cseréje – ember által értelmezhető strukturált adatok cseréje kézi vagy gépi adatkezeléssel, de kézi összeállítást és átvételezést igényel;
- szint: akadálymentes adatcsere – adatok automatikus cseréje és megosztása egy egyezményes adatcsere modellre alapozva;
- szint: akadálymentes információ csere – a harmadik szint egyfajta kiterjesztése, mely lehetővé teszi az egységes értelmezést együttműködő alkalmazások között.

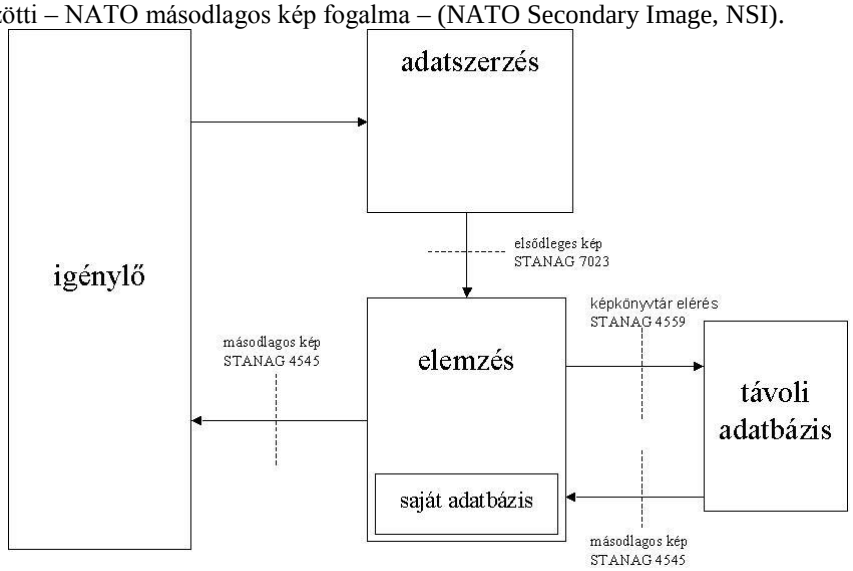
Az NIIA célja a II. szintű együttműködési képesség megteremtése néhány speciális III. szinthez tartozó kapcsolódási felület kialakításával . Az NIIA az ISO hét rétegű adatközlési modelljére épül és igyekszik minél több már létező ipari szabványra támaszkodni, ezzel is elősegítve a fejlesztés és telepítés meggyorsítását kulcsrakész komponensek beépítésével (Componens Off The Shelf, COTS).

**Képalkotó rendszerek együttműködő képessége**

A korábbi képi jellegű felderítési rendszerek alapvetően film alapúak voltak, így az együttműködő képesség megteremtése gyakorlatilag kimerült az alkalmazott termékek és eljárások szabványosításában. Az elektronikus képkezelés elterjedése rengeteg új lehetőség mellett számos szabályozatlan elemet is bevezetett. Ezeket az alábbi területeken határozhatjuk meg:

- szenzorikus adatok formátumának szabályozása
- elektronikus átviteli csatorna szabályozása
- fizikai hordozó kiolvasási lehetőségeinek szabályozása

A NATO két illeszkedési felület kialakításával foglalkozik kiemelten. Az egyik a képalkotó és az feldolgozó eszköz közötti – ez a NATO elsődleges kép fogalma -(NATO Primary Image, NPI), a másik az elemző eszközök és az adatbázisok közötti – NATO másodlagos kép fogalma – (NATO Secondary Image, NSI).




1. ábra STANAG 4545 és 7023 helye a felderítési ciklusban

Mind a két elérési ponttal kapcsolatban a NATO kidolgozta azok különböző aspektusait szabályozó ajánlásokat:

Elsődleges kép elérési pont:

- STANAG 7023, NATO elsődleges képformátum (NATO Primary Imagery Format, NPIF). Az NPIF szabvány feldolgozatlan szenzorikus adatok átvitelére szolgál a szenzor és a feldolgozó eszköz között. A szabvány univerzális és tartalom- független. Rendeltetése az egy vagy több forrásból származó szenzorikus adatok elhelyezése térben és időben, hogy a rögzített adatokat térben és időben össze lehessen vetni más helyen egy későbbi időpontban.
- STANAG 4575, NATO fejlett adattárolás (NATO Advanced Data Storage, NADS). Az NADS szabvány fejlett digitális adathordozók elérését és kiolvasását szabályozza, mint például memória modulok és lemez egységek. Ennek segítségével a felderítési adatok fizikailag kiolvashatók a felderítő eszközből, bármely

ezzel kompatíbilis NATO eszköz által. Az elemző eszközhöz az adatot eljuttatva megkezdődhet az érdemi elemzés.

- STANAG 7085, NATO együttműködő képes adatcsatorna képalkotó rendszerekhez (Interoperable Data Links for Imaging Systems). Ez a szabvány 3 osztályban definiál fizikai átviteli csatornát: analóg, digitális pont-pont átvitel, és digitális műsorszórás.

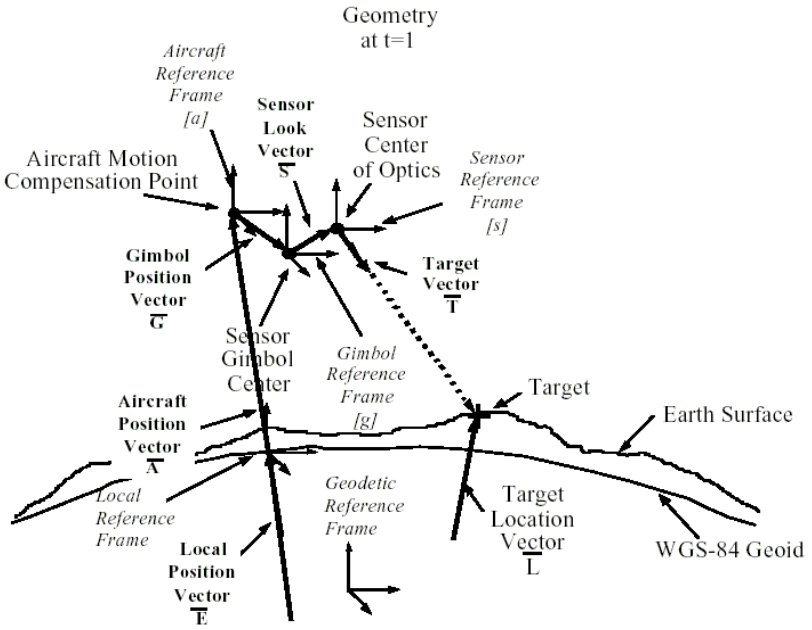
Másodlagos kép elérési pont

- STANAG 4545, NATO másodlagos képformátum (NATO Secondary Imagery Format, NSIF). Az NSIF szabvány a feldolgozott, emberi értelmezésre alkalmassá tett képek és járulékos információk cseréjét biztosítja. Egy NSIF képegység tartalmazhat egy vagy több képet, képsorozatot, hozzá kapcsolódó grafikát és kiemeléseket, illetve elemző, magyarázó szöveget egyaránt.
- STANAG 4559, NATO szabványos képkönyvtár elérési ú (NATO Standard Imagery Library Interface, NSILI). Az NSILI szabványos elérési és keresési lehetőséget biztosít a NATO képi adatbázisai között. A kiválasztott konkrét kép átviteli módját nem rögzíti, ábrázolásra az NSIF formátumot ajánlja.

A következő két fejezetben az elsődleges és másodlagos képformátumokat fogjuk részletesebben megvizsgálni.

**NPIF**

A NATO elsődleges képformátuma az adatgyűjtő eszköz – szenzorrendszer és hordozója – és az elemző állomás közötti adatátadást szabályozza.




2. ábra A szenzor helyét és irányultságát leíró vektor rendszer

Forrás: STANAG 7023

Az NPIF önleíró, általános célú formátum. Önleíró abban az értelemben, hogy az elemzést a felderítés célja, módja, vagy a használt eszközök előzetes ismerete nélkül, kizárólag az NPIF adatcsomag alapján el lehet végezni. Ezeket a hatékony elemzéshez elengedhetetlen információkat a formátum kiegészítő információs szegmensei az adat elidegeníthetetlen részét képező módon hordozzák. A formátum általános célú, mivel felderítési formától, hordozótól, és szenzor típustól független. (megjegyzendő, hogy a formátum elsősorban légi felderítésre szánt, de általános jellege miatt alkalmazható egyéb felderítési formákra is).

Egy NPIF struktúra két fő komponense a szenzor adat és a kiegészítő adatok. A szenzor adat tartalmazza a képalkotó eszköz által érzékelt és rögzített képi információt (Szenzor képi adat) és a szenzor leíró adatokat, melyek segítségével a képi adat képpontjai időben és térben elhelyezhetőek a való világban. A kiegészítő adatok a felderítéssel kapcsolatos műveleti adatokat tartalmaznak.

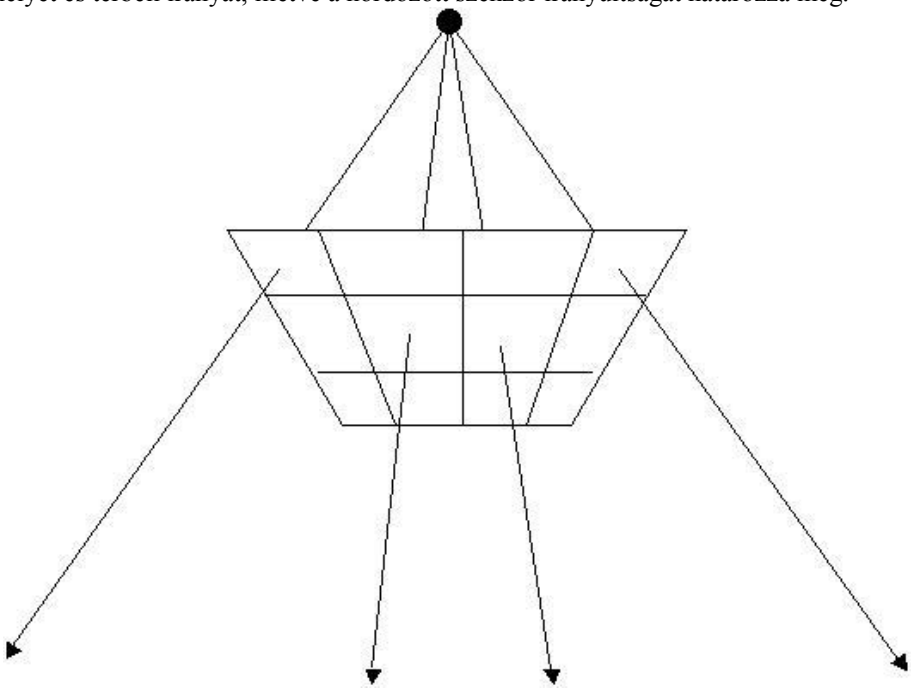
Szenzor adat:

- Szenzor képi adat (Képi információ)
- Szenzor leíró adat (A képi információ képpontjait helyezi el térben és időben)

Kiegészítő adatok:

- Formátum leíró, feladat leíró, cél adatok, hordozó adatok

NPIF kapcsán fontos kiemelni, hogy mind térben, mind pedig időben megvalósítja a képpontok hozzárendelését a valós tér pontjaihoz. A térbeli hozzárendelést két vektor rendszeren keresztül valósítja meg. Az első vektor rendszer a hordozó eszköz helyét és térbeli irányát, illetve a hordozott szenzor irányultságát határozza meg.



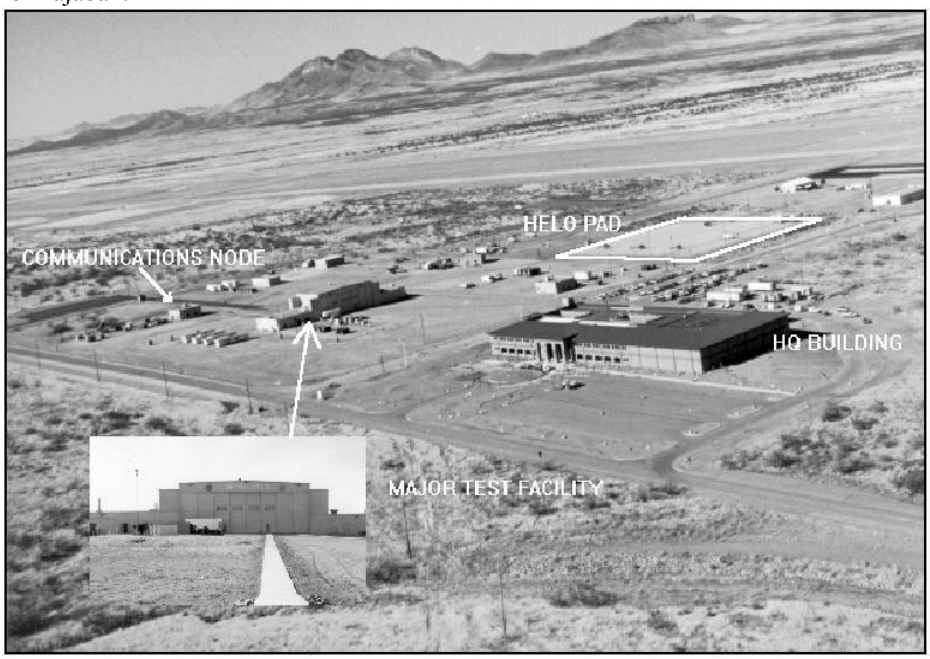
3. ábra A szenzor képpontjai irányvektorát leíró vektor rendszer

A másik vektor rendszer az alkalmazott szenzor képalkotási geometriája alapján adja meg az egyes képpontok irányvektorát a szenzor optikai közép vonalához képest.

**NSIF**

A NATO másodlagos képformátuma az elemzett és értelmezett képek cseréjét segíti elő. Ezért az NSIF nem a térinformatikai kérdésekre helyezi a hangsúlyt, hanem fő feladata biztosítani a komplex képi információval támogatott felderítési jelentések sokrétű információ tartalmának kezelhetőségét.

Egy NSIF kép egy fejlécen kívül három fő szegmensből áll: képi, grafikai és szöveges. A képszegmens magát a felderítési képet vagy képeket tartalmazza, kalibrált és javított formában. A grafikai szegmens, képi kiemeléseket, kontúrokat, nyilakat és egyéb az elemzés során hozzáadott képi jelölő elemeket tartalmaz. A szöveges szegmens a kép elemzése során nyert helyzetismereti tudást tartalmazza szöveges jelentés formájában.




4. ábra Kompozit NSIF kép, grafikai kiemelésekkel
Forrás: STANAG 4545

A kompozit kép kezelésén kívül az NSIF másik fő feladata a felderítési adatok életciklusának támogatása, melyet a fejlécben hordozott adat mezőkön keresztül valósít meg. Itt találhatóak a fájl eredetére, minősítésére és kezelésére vonatkozó adatok.

**Összefoglalás**

Elmondhatjuk, hogy mind az NSIF, mind pedig az NPIF igen összetett formátum.

Az NPIF esetében a komplexitás a probléma jellegéből adódik. Egy mozgó platformra szerelt változó geometriájú és működési elvű képalkotó eszköz képpontjainak a való világhoz rendelése igen komplex probléma.

Az NSIF esetében az alapprobléma nem ennyire komplex. Itt az alapproblémán kívül a komplexitást jelentősen növeli, hogy a szabvány nem előíró, hanem leíró jellegű.

Egy előíró protokoll pontosan meghatározza, milyen adatokat, hol, milyen reprezentációban, hosszban, dimenzióban köteles a protokollt alkalmazó fél megadni. Alternatív, redundáns ábrázolás számára nem hagy helyet, épp ezért többnyire egyszerű, egyértelmű és kompakt. A leíró jellegű protokollok adatok alternatív ábrázolására adnak lehetőséget, melyek értelmezését leíró mezők vezérlik. A leíró jellegű protokolloknál gyakoriak az opcionális illetve feltételesen kötelező mezők, a mezők közötti függőségek. Előnyük, hogy általában könnyen írhatóak, mivel a mezőket kitöltő fél a saját natív ábrázolásának megfelelően, átváltás és számítások nélkül tudja kitölteni, míg ezek olvasása, a függőségek, és a megengedett adatok sokfélesége miatt néha roppant bonyolult.

Ennek az eredménye, hogy míg NSIF fájlt előállítani elég egyszerű, a szabványnak megfelelő állományok olvashatóságát garantálni – a sok alternatív ábrázolási mód miatt – igen költséges. Ebből következik, hogy az NSIF kompatíbilis képolvasók ára igen magas ( >>1000$ ), amely az elterjedésnek, így a szövetségen belüli interoperabilitás megteremtésének komoly gátakat szabhat.

## Felhasznált irodalom


[1] NATO Imagery Interoperability Architecture (NIIA), North Atlantic Council, Document AC/224(AG/4)D/104

[2] NATO MILITARY AGENCY FOR STANDARDIZATION, STANAG on Air Reconnaissance Primary Imagery Format (NPIF), 2004 Szeptember

[3] NATO MILITARY AGENCY FOR STANDARDIZATION, STANAG on NATO Secondary Imagery Format (NSIF), 1998 November

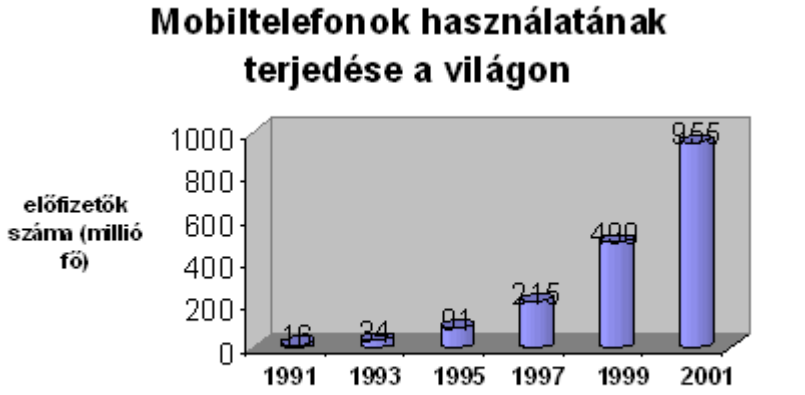
**DOBÁK Imre**

# A KÉSZENLÉTI SZERVEZETEK VÁLTOZÓ KOMMUNIKÁCIÓS RENDSZEREI - PÉLDÁK A KÖZÉP-EURÓPAI TÉRSÉG ORSZÁGAIBÓL

PhD hallgató

Napjaink veszélyhelyzetei (természeti katasztrófák, ipari balesetek, tömegszerencsétlenségek, terrortámadások) kapcsán Európában is előtérbe került a készenléti szolgálatok rádiókommunikációs igényeinek kérdésköre. A kelet-európai térség országai nyugati szomszédaikhoz képest bizonyos mértékig lemaradva, azonban nem elmaradva igyekeztek és igyekeznek fejlődő gazdasági lehetőségeik közepette megteremteni azoknak a „készenléti-veszélyhelyzeti" távközlési rendszereknek az alapjait, melyek használata áttételesen a társadalom széles rétegei biztonságát növelheti.

Természetes emberi igény, hogy veszélyhelyzetekben információt kapjunk az eseményekről, a szükséges teendőkről, amelyet a rendelkezésünkre álló kommunikációs csatornán próbálunk megszerezni. Elvárjuk azt is, hogy a mentésben, veszélyhelyzetek kezelésében résztvevők a lehető leghamarabb a helyszínre érjenek, munkájukat szervezetten, egymással összehangoltan végezzék, amely tevékenységnek szintén alapvető része az általuk használt kommunikációs eszköz. Egyértelműen következik, hogy feladatvégzésük hatékonyságát nagymértékben kihat kommunikációs rendszereik fejlettsége, illetve adott szakfeladatra való megfelelősége.




Forrás: ITU - Key Global Telecom Indicators 2001

Felmerül a kérdés, hogy a mobiltelefonok hihetetlen, a társadalom egészét érintő elterjedésnek korában a GSM mobiltelefonok, és maga a technológia miért nem alkalmas az érintett szervezetek feladatainak ellátására, a veszély-, és katasztrófahelyzetekben történő alkalmazásra. A GSM rendszer amellett, hogy a területi lefedettséget biztosítani tudja, egyéb szempontokban (pl. rövid hívás-felépítési idő, csoporthívási

funkció, prioritással kezelt hívások, titkosítási lehetőség, DMO - direkt módú rádiókapcsolat - üzemmód) azonban nem teljesíti a készenléti rendszerekkel szemben támasztott követelményeket.

Számos nemzetközi példa (pl. a New York-i és washingtoni terrortámadások) mutatja, hogy a GSM rendszerek - megnövekedett kommunikációs igény okozta – hirtelen túlterhelése miatt sem képes a készenléti szervezetek speciális kommunikációs igényeit kielégíteni.

A mentésben-elhárításban résztvevő szervezetek rádiórendszereinek létjogosultsága vitathatatlan, hiszen megfelelő kommunikáció (távközlés) megléte nélkül, a mentésben, illetve a katasztrófa elhárításban-felszámolásban résztvevő szervezetek tevékenységében zavarok lépnének fel.




A régi elavultnak tekinthető, felhasználó szervezetenként elkülönülő, tetemes fejlesztési és fenntartási összegeket felemésztő analóg rendszerek digitális technológiát alkalmazó készenléti kommunikációs (Public Safety and Security) rendszerekkel történő felváltását számos érv támasztja alá:

- A készenléti-biztonsági szervek által alkalmazott jelenlegi rádiós eszközök a sávtartományra jellemző terjedési sajátosságokból adódóan nem képesek biztosítani egy országos, összes szervezetet magában foglaló egységes rendszert. Az elhasználódott analóg rendszerek általában csak hangátvitelre voltak használatosak.
- Természeti katasztrófa, tömegszerencsétlenség, ipari balesetek bekövetkezésekor vagy terrortámadás esetén biztonságos, a civil távközlési rendszerektől teljesen elkülönített hálózat kell, hogy a hatóságok rendelkezésére álljon.
- Alapvető fontosságú a rövid időn belüli hatékony válaszlépések megtételéhez a kommunikációs rendszerre jellemző gyors kapcsolási idő és az időszakos, eseményhez kötött csúcsrajáratás lehetősége.
- A korszerű digitális rendszerek korábbi analóg rádiórendszerekkel szembeni előnye, a rendszereken továbbított adatok illetéktelen személyek általi hozzáférésének kizárása is.

Az „emberéletek” mentésében közvetlenül résztvevő szervezetek (mentők, tűzoltóság) mellett vitathatatlan azon kormányzati szervek kommunikációjának fontossága is, melyek nem elsődlegesen a veszélyhelyzetek kezeléséhez kapcsolódóan folytatnak híradást, hanem kiemelt biztonsági feladatokat látnak (pl. kormányőrségek) vagy akár a társadalom széles rétegei biztonságához köthető tevékenységet végeznek (pl. rendőrség).




A távközlés fejlődésével párhuzamosan, kialakultak azok az európai alapszabványok, illetve azzal egyenrangúnak tekinthető specifikációk is, melyek a készenléti rendszereket működtető többnyire állami szervek kommunikációs rendszerei alapját megteremtették.

**Szabványok**

A készenléti szervek rádiókommunikációs igényeinek kielégítésére Európában – egyenrangú megoldásként - elfogadott standard, a Tetrapol és a TETRA, mint digitális, cellás, rádiórendszer specifikációk. A TETRA (TErrestrial Trunked Radio) az ETSI (European Telecommunications Standardisation Institute) által kidolgozott, korszerű, digitális, TDMA (Time Division Multiple Access) technológia. A TETRA mint nyílt trönkölt rádiós standard1 a '90-es évek közepétől indult útjára az European Commission és ETSI által, amely nem csak beszéd, hanem adatok átvitelének megoldására is irányult.

A Tetrapol néven ismert „specifikáció" néhány gyártó (főként a francia Matra cég) tevékenysége kapcsán vált ismerte és elterjedtté. A TETRA-12-t nevezték át Tetrapol-lá, ami igazából a TETRA és a „police" kifejezések összetételéből adódott, mivel a francia Belügyminisztérium a Tetrapol-t választotta a rendőrségi hálózat[2] kiépítésére. A későbbi kísérletek a Tetrapol elfogadtatására hosszú utat tettek meg 1996-ig, amikor is a TETRAPOL technológia Európa szerte elfogadásra került, mind az ITU (International

1 TETRA alapszabvány (ETS 300 392-1), Air Interface - ETS 300 392-2, Peripheral Equipment Interface - ETS 300 392-5, Gateways - ETS 300 392-4, Inter System Interface - ETS 300 392-3, DMO - ETS 300 396 szabvány

2 1992 - az első működő hálózat a Rubis, a francia csendőrség hálózata

Telecommunications Union), European Police Co-operation Council, CEPT, ETSI Board (1999 ETSI accepted the Tetrapol Publicly Available Specification), MESA (Mobiltiy for Emergency and Safety Applications) által.

A Schengeni / Rendőrségi Együttműködési Tanács végrehajtó bizottság döntése[3] felismerte, hogy az Európai Uniós, illetve tagjelölt országok vegyesen alkalmazzák a TETRA-t, illetve Tetrapol-t, így azokat a rendszerek kiépítése szempontjából egymással egyenlőként elfogadva kimondta, hogy szükségesnek tartja közöttük a kompatibilitás megteremtését, illetve továbbfejlesztését. Az európai szabályozás alapján az egyes országok digitális kommunikációs rendszereinek kiépítéséért folyó harcban a TETRA és a Tetrapol így egyenrangú félként indulhatnak.

A Scehngeni Egyezmény 44. cikkelye deklarálta, egy egységes rádióhálózat létrehozásának szükségét Európában. A két szabvány (Tetra, illetve Tetrapol) valamelyikének alkalmazásával az egyes tagországok kiépített digitális rádiórendszerei alkalmassá válnak arra, hogy a schengeni előírásoknak is megfeleljen.

A két szabvány, és az időközben rohamosan terjedő GSM hálózatok tükrében, európai szinten is számos elvárás fogalmazódott meg a készenléti szervezetek kommunikációs rendszereinek kialakítását illetően:

- folyamatos kommunikációt tegyen lehetővé (akár különböző csoportok között is),
- rendkívüli-, és katasztrófahelyzetben is megbízhatóan működjön,
- a felhasználó szervezetek speciális igényeit kielégítse,
- rugalmas feladatirányítási képességekkel rendelkező legyen, hierarchikus felépítésű,
- a korábbi analóg rendszerekkel képes legyen együttműködni,
- minél szélesebb területi lefedettséget biztosítson,
- biztonságos kommunikáció követelménye,
- adatátviteli lehetőség,
- a végfelhasználói készülékek egyedi igényeknek megfelelő széles választéka,
- a felhasználó szervezetek között elkülöníthető, illetve együttműködni képes rendszer legyen,
- növelje a szervezetek hatékonyságát és együttműködési képességét (akár nemzetközi együttműködési lehetőség is),
- költséghatékonyan, a felhasználói igények alapján bővíthető, továbbfejleszthető legyen.

Az elmúlt tíz év során a két szabványra alapozva, mintegy a mögöttük álló vezető távközlési cégek piaci harcaként Európában egymás után építették ki (vagy folyamatban van) az országos, a kisebb térségeket lefedő (pl. főváros), illetve az adott „célfeladatra” (pl. repülőterek, közlekedési vállalatok) telepített digitális rádiókommunikációs rendszereket.

Európában napjainkban már több mint 60 Tetrapol hálózat működik, melyek közül számos országos lefedettséget biztosít[4]. A TETRA hálózatokat érin-

3 Schengen SCH/I (98) 17 REV 4. sz.

4 Franciaország (ACROPOL, RUBIS), Svájc (POLYCOM), Csehország (PEGAS), Szlovákia (SITNO), Románia (PHOENIX), Koszovo (NATO erők), Spanyolország (SIRDEE)

tő szerződéskötések száma csak Európában 330, melyből 61 a kelet-európai régióra vonatkozik[5]. A telepített rendszerek használhatósága számos természeti katasztrófa felszámolása (árvizek, erdőtüzek, madridi terrortámadás), sport és politikai rendezvények (athéni olimpia, NATO csúcs) kapcsán bebizonyosodott.

**Néhány példa a térség digitális rádiórendszereire**

A közép-európai térség országai is már a '90-es évek közepén felismerték a váltás szükségességét, majd az Európai Uniós csatlakozás, illetve annak folyamata erősítették meg a közös európai technológiákra alapozott rendszerek létrehozását. Az érintett országok eltérő szabványokat választva azonban időben közel párhuzamosan kezdték meg rendszereik kiépítését. A rendszerek kiépítésének elmaradását, a projektek elhúzódását gyakran pénzügyi és politikai okok, nem a készenléti szervek igényeinek változása, vagy a technológiák közötti döntésképtelenség okozta.

Csehországban, habár a készenléti rádiórendszer szükségességére vonatkozó döntés még 1993-ban megszületett, az országos kiépítés megkezdése után (1999) a projekt befejezésig (2003 második félév) tíz év telt el. A PEGAS digitális rádiókommunikációs hálózat Tetrapol specifikáción alapul, és a cseh biztonsági erők országos hálózataként funkcionál.

A PEGAS első regionális része Prágában épült ki 2000 őszére az IMF és a Világbank konferenciájának időpontjára. A részrendszer sikere az országos hálózat kiépítésének lehetőségét erősítette. A prágai rendszer később is jól vizsgázott a prágai árvíz, illetve 2002. novemberében a NATO csúcs idején, amikor – a terrorista cselekmények elleni küzdelem légkörben – a fővárosban már telepített PEGAS rendszeren, több mint 7 ezer terminál állt kapcsolatban a rendőrség bevetésirányító központjával, összeköttetést teremtve ezzel a cseh belügyminisztérium és a védelmi minisztérium egyéb szervei között. A rendszer 2003 második félévére 14 régiót lefedve, 20 ezer terminál kommunikációját biztosítani képes (42 kapcsolóközpont, 218 bázisállomás) rendszerré vált. Kiépítését a különböző szervekhez kötött analóg rendszer elavultsága[6], és annak fenntartási költségei indokolták. Az új digitális rendszer használatán azonban már a Belügyminisztérium mellett (mint operátor) a rendőrség, a tűzoltóság, a polgári védelem szervei, a Védelmi Minisztérium, és az Egészségügyi Minisztérium (pl. mentőszolgálat) szervei is osztoznak.

A rendszer alkalmazása, - amely közel 95%-os területi lefedettséget biztosít - nem csak a képességek (pl. központi adatbázis elérése), hanem minőségi mutatók tekintetében is a cseh rendőrségi szervezet hatékonyságának növeléséhez vezetett. A rendszer beszéd és adatátvitelt biztosít a 380-400 MHz közötti frekvenciatartományban, a kommunikációs igények biztosítására Európában kijelölt sáv felhasználásával.

5 Forrás: Konferenciaanyag - a professzionális mobil távközlésről - 2004 június, TETRA FORUM HUNGARY, Tetrapol Presentation – 2004 szeptember, HTE, Bp.

6 a cseh rendőrség 30 éves analóg „TESLA" rendszere

A folyamatosság fenntartása érdekében a rendszer alkalmas a létező analóg rendszerekkel való együttműködésre. A kialakított infrastruktúra támogatja a PEGAS rendszert felhasználó szervezetek azonos idejű, egymástól független kommunikációját, ugyanakkor vészhelyzetben (pl. balesetek, árvizek) a különböző felhasználói csoportok számára biztosított az együttműködési, mentési és elhárítási feladatok közös, szervezett végrehajtása.

A Schengeni követelményeknek megfelelő ausztriai rendszer megvalósításának kezdete 2001. júliusára tehető. Az ADONIS (Austrian Digital Operating Network for Integrated Services) országos lefedettséget biztosító (1288 bázis állomást tartalmazó) rendszerként indult, 4 kivitelezési fázisban.

A tervezett felhasználók (szövetségi és állami rendőrség, haderő, vámszervek, tűzoltóság, mentési feladatokat ellátó szervek, stb.) igényeit kiszolgáló rendszer befejezési határidejét 2006. első negyedévére tervezték, azonban a TETRA hálózat megvalósítása 2003-ban - próbaüzemet követően - leállításra került, amelyet pénzügyi és tervezési problémák, a várt 120 ezer felhasználó elmaradása indokoltak, azonban a készenléti rendszer szükségességét azóta is fenntartják. A projekt problémáiról megjelent cikkek szerint a tervezett állami felhasználókat és magánvállalatokat, mint előfizetőket a rendszer használatának tetemes költsége riasztotta el.

Romániában a térség egyéb országaihoz hasonlóan az elavultnak tekinthető távközlési rendszerek napjainkra elérték gazdaságossági fenntartási ciklusuk végét és természetes igényként jelentkezett rendszereik korszerű TETRA, vagy Tetrapol rendszerrel történő felváltásának igénye.

A Tetrapol szabványra alapozott Phoenix rendszer kiépítését 1998-ban kezdték és a (40 kapcsolóközpontot, 94 bázisállomást magában foglaló) 10 ezer rádióterminál alkalmazását biztosító rendszer kiépítése négy évig tartott. A rendszer felhasználói között biztonsági szervezeteket (pl. hadsereg) találunk. A Phoenix rendszer több alkalommal is eredményesen igazolta létrehozását, például II. János Pál Pápa 1999. májusi romániai, majd az Egyesült Államok elnökének 2002. novemberi bukaresti látogatása során. Az esemény ideje alatt a Phoenix rendszerhez telepített néhány ezer terminál alkalmazása eredményesen támogatta az elnöki védelmét ellátó szolgálat tevékenységét.

A szlovákiai SITNO digitális rádiórendszer, a Szlovák Köztársaság biztonsági erői számára létrehozott országos méretű hálózat. Felhasználói többek között a rendőrség, a mentők, a tűzoltók, a polgári védelem szervei. A rendszer kiépítésére a kezdeti lépéseket 1998-ban tették, és 2005. év végi teljes kiépítésére (8 kapcsolóközpont, 88 bázisállomás) 8 ezer végfelhasználói terminállal számoltak.

A rendszer képes a létező analóg rendszerekkel együttműködni megkönnyítve ezzel a korábbi rendszerekről való átállást, és biztosítva az egyéb, továbbra is üzemben maradó analóg hálózatokkal való közös alkalmazást. A korábbi, főként hangátvitelt biztosító rendszerekkel szemben hang és adatátvitelre is egyaránt használható.

Lengyelországban a Szczytno-i rendőr akadémián építettek ki (2003. elején) TETRA alapú „Command & Control” rendszert, amely a rendőrség és egyéb készenléti szervezetekhez tartozó szakemberek oktatására alkalmas. Az oktatás mellett a rendszert Szczytno-i kerületi rendőri parancsnokság vezetés-irányítási feladatokra is használja, illetve tervben van regionális készenléti központként való alkalmazása is. A bevetésirányítási központ és diszpécserei több ezer rendőr tevékenységének, és gép-

jármű mozgásának az irányítását teszik lehetővé. Intelligens számítógépes bevetésirányítási rendszer működik a varsói rendőrségen is, amely több mint kétezer rendőr és TETRA terminálokkal felszerelt gépjármű irányítását képes ellátni.

Magyarország.

A több évtizedes magyar rendőrségi, tűzoltóság, illetve mentőszolgálat által alkalmazott kommunikációs hálózatot véve összességében elmondható, hogy nem felel meg a mai európai követelményeknek, és a készenléti szolgálatok átalakul(t)ó feladatai új, magas színvonalú, országos szintű rendszer kiépítését teszik szükségessé. Magyarországon a készenléti szervezetek jelenlegi rendszerei szervenként széttagoltak, fenntartásuk költséges. Analóg rádióik mellett (helyett) egyes szervezetek GSM alapú mobiltelefonokat is alkalmaznak, melyek használata jelentős kiadásokat jelentenek.

Magyarországon a technológiai változtatás szükségessége már a ’90-es évek közepén megfogalmazódott, és a rendelkezésre álló fejlett digitális rádiórendszereket gyártó nyugati cégekkel közösen, lehetséges piacként helyi mintarendszereket[7] hoztak létre. Ezt követően 2001. nyarán megalakították a százszázalékos állami tulajdonban levő Magyar Posta Rt.-t, megbízva a készenléti Tetra-hálózat kiépítésével, azonban a pályázatot technikai okokra hivatkozva 2002. januárjában fel is függesztették.

A kormány újabb döntése 2003-ra tehető, amikor is szolgáltatásvásárlási modellt elfogadva újabb projekt előkészítése kezdődött meg[8]. A végleges pályázati anyag 2004. év végére készült el, majd kiírásra került az EDR (Egységes Digitális Rádiórendszer) pályázata. A fordulók eredményeként 2005. augusztus 15-ig a pályázók megtették ajánlatukat, amelyek elbírálását követően októberben döntés születhet. A tervek szerint az érintett szervezetek (a Kormány a 279/2001. (XII. 23.) Korm. rendelet hatálya alá tartozó szervezetek, az Országos Mentőszolgálat, valamint az Országos Vízügyi Főigazgatóság) Budapest 2006. elején történő lefedése után, 2007 végére az országos hálózatot is birtokba vehetik, teljesítve ezzel a schengeni elvárásokat is.

## Felhasznált irodalom


[1] Ivan Vlasich es Roland Leimer- Migration strategies from – Konferencia a professzionális mobil távközlésről - 2004 június, TETRA FORUM HUNGARY

[2] John Cox - TETRA market place and its successes – Konferencia a professzionális mobil távközlésről - 2004 június, TETRA FORUM HUNGARY

[3] Jonathan Dolby - Double success for TETRAPOL during the NATO summit in Prague (Czech Republic) and US President's visit to Romania - http://www.tetrapol.com

[4] Mallász Judit -Kísérlet a rendőrségnél - Computerworld 2000/15.Mobile Europe – 2003/04 december/január – The wireless Communication Magazine for Europe

[5] Mobile Europe –2005 április– The wireless Communication Magazine for Europe

[6] Mobile Europe –2004 április– The wireless Communication Magazine for Europe


7 pl. 2000-ben budapesti Tetrapol rádiókommunikációs pilothálózat - Belügyminisztérium - Matra Nortel Communications

8 1031/2003. (IV. 9.) Korm. határozat az egységes digitális rádió-távközlő rendszer kialakításáról

[7] News from Rohde & Schwarz 2003/II 178.- TETRA radio systems
[8] News from Rohde & Schwarz 2004/IV 184.- TETRA radio systems
[9] Pándi Erik-Nyaka József-Nagy Lajos-Tatárka István - Gondolatok az integrált, országos hatáskörű katasztrófavédelmi szervezet rádióhíradása kialakításának lehetőségeiről - http://www.zmka.hu
[10] Simon Gyula - A civil TETRA technológia bevezetésének szabályozási kérdései – Konferencia a professzionális mobil távközlésről - 2004 június, TETRA FORUM HUNGARY
[11] Soós Krisztián - Motorola TETRA IP a Világ biztonságért – Konferencia a professzionális mobil távközlésről - 2004 június, TETRA FORUM HUNGARY
[12] TETRA news – 3-4/2003
[13] Várkonyi Iván - 2005. május – Népszabadság - Új készenléti távközlési rendszer Népszabadság
[14] 2003. április 29. - Magyar Nemzet - Drága és hiányos a távközlési rendszer
[15] 2003. április 22. - Népszabadság - Új rádiórendszer rohammunkában
[16] 2003. április 18. - Magyar Hírlap - Az EDR 2005-ben már működhet Magyarországon
[17] 2003. március 28. - Világgazdaság - Takarékos készenléti telefon
[18] 2003. március 26. – Index - Egységes digitális rádiórendszer a készenléti szerveknek
[19] 2003. március 21. - Magyar Nemzet- Teher az államnak a rádiótávközlő rendszer
[20] 2005. augusztus 16. - Népszabadság - Még nem szól, de már olcsóbbnak ígérkezik a készenléti telefon
[21] www.posta.hu
[22] www.dmeurope.com
[23] www.bretschneidernet.de
[24] www.tetrapol.com
[25] www.tetramou.com
[26] www.tetrapol.com
[27] www.tetrawatch.net

**DOBOS Attila**

# GENERÁCIÓVÁLTÁS A HONVÉDSÉGI TÁVKÖZLÉSBEN

## A jelenlegi távbeszélő hálózat kialakulása

A Magyar Honvédség 1997-ben kezdte meg telekommunikációs hálózatának modernizációját. A több lépcsős, folyamatos beruházások eredményeképp kialakításra került az MH Zártcélú Digitális hálózata, teljes egészében kiváltva az analóg központokból felépített gerinchálózatot, s az analóg központok (közel 50 db) analóg trönkökön kapcsolódnak a hálózathoz. A digitális központok (Hicom 300H) tervezett száma az év végére megközelíti a 60-at, a kapcsolódó mellékállomások száma pedig a 25 000-et.

## Az MH Intranet hálózata

Az intranet hálózat kialakításával új lépcsőhöz érkezett a telekommunikációs hálózat modernizációja. A meglévő központokban szoftverbővítéssel (HiPath 4000) biztosítható IP alapú trönkkártyák alkalmazását, a meglévő mellékoldali és trönkkártyák, valamint analóg és digitális végkészülékek változatlan felhasználása mellett. Ez lehetővé teszi a központok felcsatlakoztatását az Intranet hálózatra, valamint a központok hálózati forgalmának átterhelését az IP hálózatra. A nagy kapacitású (45-90 csatorna) IP trönkkártyákon keresztül korlátozás nélkül biztosított a meglévő szolgáltatások alkalmazása. Ebben az esetben a központok egy-vagy több Ethernet csatlakozáson keresztül kapcsolódnak az intranet hálózat switch elemeihez, így a transzport hálózat router elemeiben tervezett, a telefonközpont fogadását biztosító 2Mb/s-os kártyák teljes egészében megtakaríthatók. Továbbá a beszéd kommunikáció számára biztosítandó pont-pont összeköttetések helyett, alkalmazható az Intranet hálózaton keresztül a pont-multipont konfiguráció kialakítása. Bár az egyes telefonközpontok, mint a transzport hálózat felhasználói, fizikailag egy-vagy több trönkkel kapcsolódnak az IP hálózathoz, de logikailag közvetlen összeköttetés építhető fel a hálózathoz csatlakozó bármely telefonközponthoz. A beszédkommunikáció a transzport hálózatra történő átterhelésével biztosítható, hogy kis mellékszámú helyőrségekbe vagy objektumokba kihelyezésre kerüljön egy-egy gócközpont analóg, digitális, illetve IP mellékei, a hálózatban alkalmazott szolgáltatások teljes körű biztosításával, önálló telefonközpont alkalmazása nélkül. Természetesen, mind a Hicom 300, mind a HiPath 4000 központok hálózat-felügyeleti rendszere rendelkezésre áll, azonos felületen, egy rendszerben.

## Az MH Informatikai Transzport hálózat első üteme

A Magyar Honvédség informatikai és híradó rendszerének integrálása érdekében 2003. szeptember és 2004. december között kiépítésre kerültek az MH Transzporthálózatának elemei. A feladatban a HM HVK Híradó és Informatikai Csoportfőnökség végezte a koordinálási tevékenységet és az MH Elektronikai Szolgálatfőnökség, valamint az MH Híradó Parancsnokság irányította a kivitelezés munkáit.

Az alapfeladata volt előkészíteni az MH meglévő HICOM alapú zártcélú rendszerének és az informatikai transzporthálózatnak az integrálását. Ezen a módon a nemzeti és külföldi szerepvállalásból adódó helyszínek is lefedésre kerültek úgy a híradás, mint az informatikai adatforgalom és biztonsági rendszerek vonatkozásában.

A HM HVK HIRICSF-ség informatikai osztálya által kezdeményezet fejlesztés célja a párhuzamos híradó és informatika rendszerépítés felszámolása és új, világszínvonalú Információ technológiai szolgáltatások bevezetése volt. A az Informatikai és híradó rendszerek integrálásával létrejött a katonai követelményeket figyelembevevő nagy túlélő-képességű és széleskörű automatizmussal rendelkező intelligens országos kapcsoló hálózat, melyet az MH transzporthálózatának nevezünk.

Az ütem végén a beszédcélú szolgáltatások két technológián alapulnak. A távbeszélés egyrészt az MH zártláncú hálózatának részeként HICOM ISDN központokon keresztül nagytömegű felhasználó részére biztosított a Magyar Honvédég objektumai között (beleértve a Honvédelmi Minisztériumot és annak háttérintézményeit is). Másrészt az infrastrukturálisan kiépítetlen, de adatátviteli kapcsolattal rendelkező területeken az informatikai eszközök felhasználásával az IP elv alkalmazásával történik a hangátviteli szolgáltatás biztosítása. A távközlő rendszer fejlesztésének további, harmadik ütemében a meglévő technológiák és az MH adatátviteli rendszerének szolgáltatásait felhasználó, közös rendszer kerül kialakításra. Ennek elemeit a SIEMENS HIPATH és Cisco IP technológiák képezik. Ezzel biztosítható egy hosszú időn keresztül rendszerben tartható, magas szolgáltatásokat nyújtó, gazdaságos rendszer létrehozása.

### Az MH Informatikai Transzport hálózat fejlesztése

Az MH Transzporthálózata a tervezett ütem végén az alábbi informatikai rendszerek működését fogja biztosítani:

- MH Levelező rendszer,
- MH Iroda automatizálási rendszer (portál),
- MH Internet (Az érvényben lévő biztonsági előírások alapján!),
- MH Költségvetés Gazdálkodási Rendszer részelemei,
- MH Légierő nemzeti és NATO vezetési, valamint fegyverirányítási rendszerek,
- NATO Irodaautomatizálási rendszer (NIAR),
- Logisztikai rendszerek (Kodifikáció, Vagyontárgy követő, stb.),
- MH Meteorlógiai rendszer,
- MH Vegyivédelmi rendszer részelemei,
- MH Egészségügyi rendszer részadatai.

Az Informatikai rendszer alapját képező gerinchálózat a felkapcsolódó felhasználókkal kiszolgálja a Magyar Honvédséget. A közelmúltban 34 helyszínen átadott transzport hálózati csomópontokkal kialakított egységes rendszer, mint felhordóhálózat megvalósította a gerinchálózathoz történő csatlakozást. A 34 helyszínen történt hálózati fejlesztést és kiépítést valamint a rendszerbe történő integrálás munkálatait a Siemens Rt. végezte. Az összes helyszín egy egységes integrált távfelügyeleti rendszerben egy helyszínről vezérelhető és távfelügyelhető. Ezt az országos felügyeleti rendszert a MH HIP állománya üzemelteti. A meghibásodások mielőbbi elhárítása érdekében fenntartási szerződés formájában a Siemens Rt. szervízhálózata is résztvállal.

Az átadott transzporthálózat mind a 34 helyszínén, a folyamatos működése érdekében egységes áramellátó és vezérlő rendszerrel rendelkezik, amely szintén a távfelügyeleti rendszer részét képezi.

A távközlő hálózat 2005-ben további 18 kapcsolóközponttal bővül és a felügyeletei rendszer egy generációs fejlődésen megy át. Az új felügyeleti rendszer a

legmagasabb technológiai színvonalat képviselő IP alapú rendszer, amely jelentős szolgáltatásai mellett képes integrálni és felügyelni bármelyik gyártó és technológia IP alapú berendezését, rendszerét

A transzporthálózat folyamatos fejlesztés alatt van az egyre bővülő felhasználói igények kielégítése érdekében. A jelenleg is futó fejlesztés az MH irodaautomatizálási rendszer kialakítására kiírt és a Siemens-Synergon konzorcium által megnyert közbeszerzési pályázat folyamata. A fejlesztés magában foglalja az eddigi elkészült rendszer elemeket mind a híradó és informatikai oldalról. A tender eredménye meghatározza a HM tárca egészére történő híradó és informatikai fejlesztés jövőbeni irányait. A pályázat célja, hogy a MH egészére egy átfogó, tervezhető és megvalósítható képet kapjunk az irodaautomatizálás és az integrált hang-adatkapcsolati rendszerekben.

Az irodaautomatizálás első lépcsője a transzporthálózat átalakításával már a 2005. évben kiépül a tender keretein belül. Az alkalmazás területén bevezetésre kerül a PlumTree által fejlesztett portálrendszer jelenleg 15 000 felhasználóval, melyet már most is használ a MH mint tesztportál.

### Integrált távközlő hálózat alkalmazása a NATO-ban és itthon

Az MH kommunikációs rendszereinek csatlakozását a NATO alaphálózathoz (Core Network) szintén egy Siemens HiPath berendezés biztosítja, amelyet a NATO telepíttetett Budapestre. A NATO alaphálózatát szintén a Siemens telepítette és támogatja az üzemeltetést. Az azonos technológiának köszönhetően a rendszerek közötti átjárás problémamentes. A teljes rendszer karbantartását és üzemeltetés a Siemens magyar szakemberei végzik.

Az integrált rendszeren alapuló szolgáltatás kiszolgálásának legjobb hazai példája, a Veszprémben létesített (SEL objektumban) a légierő vezetési és irányítási rendszereit összefogó CRC (Control and Reporting Centre), melynek teljes távközlési és informatikai rendszerét a Siemens létesít NSIP projekt keretében.

Itt a Légierő vezetési és fegyverirányítási rendszere, beleértve a különböző nemzeti és NATO vonatkozású alrendszerek központi irányítása, felügyelete és működtetése valósult meg. Az integrált rendszerek között megtalálhatóak a folyamatos nemzetközi légihelyzetkép; a nemzetközi polgári és katonai radar állomások jelei, információi; nemzetközi katonai és polgári repülési tervek; meteorológiai adatok; légierő hadműveleti vezetési és irányítási rendszere; hasonló funkcióval bíró NATO rendszerekkel a közvetlen kapcsolat. Az említett rendszereken kívül a folyamatos híradó és informatikai kapcsolat az alárendeltekkel valamint a Magyar Honvédség alakulataival.

A központban az alárendeltektől a transzporthálózaton kapott radarjeleket nagy teljesítményű számítógépekkel dolgozzák fel valós idejű légi helyzetképpé. A valós idejű légi helyzetképet - a szövetséges együttműködésből adódóan - elküldik a NATO integrált légvédelmi rendszerébe, a NATINADS kijelölt vezetési pontjára is.

2004-ben helyezték üzembe a MASE elnevezésű radaradat-feldolgozó és fegyverirányító rendszert, melynek telepítési jogát nemzetközi tenderen nyerte meg a Siemens.

A légi irányítás területén elkönyvelt nagy sikernek volt tekinthető, hogy a légierő irányítói első ízben kapcsolódtak össze egy - Magyarország légterében tartózkodó - NATO-tulajdonú AWACS repülőgéppel. A transzporthálózaton keresztül többszörösen kódolt, lehallgatástól védett rádióhullámok segítségével juttatták el a CRC

valós idejű légi helyzetképét a repülőn dolgozó szövetséges katonáknak. "Cserében" a magyarok is megkapták az AWACS-tól az általuk látott radarképet.

A légihelyzetkép-cserék egyébként mindennaposak a légierőnél. Nemzetközi egyezmények alapján ugyanis rendszeresen cserélik ki információikat a magyar, a román és a szlovén katonai légtérellenőrzők.

A NATO által finanszírozott NSIP projekt a földalatti létesítmény teljes rekonstrukcióját tartalmazza. Az új beléptető rendszer, valamint lehallgatásbiztos belső antennarendszer az objektum teljes kommunikációs rendszere átadásra került. Emellett a legmodernebb technológiával felszerelt új légi irányító és vadászirányító termet építettek ki.

A NATO is megkezdte légi vezetési és irányítási rendszerének egységes hardver és szoftver alapra helyezését. A cél az úgynevezett Légi Vezetési és Irányítási Rendszer (Air Command and Controll System/ACCS) megalkotása volt, felváltandó a "toldozott-foltozott" hardver és szoftver környezettel rendelkező AEGIS-t. Az ACCS program késése miatt azonban szükségessé vált átmeneti megoldások keresése, s ekkor születtek meg a különböző PC alapú megoldások, például az AEGIS Site Emulator (ASE).

### A MASE (Multi AEGIS Site Emulator) rendszer.

Az ERCS rendszer biztosítja a NATO repülőgép-fedélzeti felderítő és korai előrejelző rendszer és a földi telepítésű légi vezetési és irányítási rendszer között az azonosított légi helyzetről, harcvezetésről és fegyverirányításról szóló információk zavarvédett adatcseréjét és hangalapú rádiókommunikációs összeköttetését.

A MASE rendszer megvalósítja a földön és a repülőgép fedélzetén telepített radarok és egyéb szenzorok adatainak integrálását, az egységes légi helyzetkép előállítását, valamint a harcászati szintű légi vezetési és irányítási feladatok szövetségi követelmények szerinti végrehajtását.

A CSI rendszer biztosítja a saját és megerősítésre kijelölt NATO-szövetséges földi telepítésű légvédelmirakéta-egységek harcvezetését és az alegységek fegyverirányítását.

Hasonlóan jelentős fejlődést jelent az ICC rendszer beindítása, amely légierős vezetési rendszeréhez szükséges minősített adatok részére biztosít megbízható, biztonságos adat- és beszédátvitelt.

### Összegzés

A fentiek alapján elmondható, hogy a Magyar Honvédség távközlő és informatikai rendszerei egy technológiai generációváltást követően a kor színvonalának megfelelő szinten vannak, és tökéletesen együttműködnek a NATO rendszerekkel. A hálózat megfelelő szolgáltatásokat biztosít a hazai és a nemzetközi törzsek számára.

A hálózat felépítése és a végrehajtott fejlesztések lehetővé teszik, hogy a tervezés alatt lévő tábori rendszer gyártótól és technológiától függetlenül kapcsolódhasson az állandó rendszerhez és egységes integrált rendszert alkossanak.

## EGRI Gábor

# DÖNTÉSI FOLYAMAT FORMALIZÁLÁSA

Egri Gábor r. alezredes
BM Távközlési Szolgálat

### Bevezető

A társadalmi-gazdasági élet valamennyi területén, így a közigazgatásban, vagy a rendészeti igazgatásban is szükség van a megfelelő információk alapján történő döntéshozatalra. Ennek során a rendelkezésre álló adatokat – rendszerint komplex folyamatban – értékeljük, cselekvési változatokat állítunk fel és végül választunk azok közül. Ezen tevékenység-láncolat egyik elemét vesszük most vizsgálat alá, nevezetesen valamely konkrét szempont szerinti értékelést.

Az értékelés komplex jellege egyébként azt feltételezi, hogy előzetesen megfelelő bírálati szempont-halmazt és ehhez rendelt súlyozást, illetve ponthatárokat jelölünk ki. A szempont-halmaz elemeinek egyenkénti értékelése viszont már azonos módszer alkalmazásával végezhető és az alábbiakban ennek felvázolására teszünk kísérletet.

### Határoló pontok kijelölése

Első lépésben célszerű a szemponthoz rendelt értékelő függvény határoló pontjainak felvétele. (Ez matematikai értelemben az adott függvény értékkészletének és értelmezési tartományának meghatározását jelenti.) Ennek azért van különös jelentősége, mert ebből – formálisan is – kiderül az értékelési szempont egyenes, vagy fordított arányosságának jellege. A fentieket az ábragyűjteményben szereplő 1. sz. ábra szemlélteti.

Hétköznapi életből vett példák:

Az arányosságokra szemléletes példát jelentenek általában a sportversenyek mérései. Egyenes arányossággal mérjük például az atlétikából az ugró, vagy dobó versenyeket. Minél messzebbre ugrik (dob) valaki, annál jobb az eredmény.

Fordított arányosságot mutatnak például a futóversenyek esetei, amikor a kisebb idő elérése jelenti az eredményesebb szereplést.

Más területről is hozható szemléltetés: például egy motor minél nagyobb teljesítményű, annál hasznosabb (egyenes arányosság), de minél nagyobb az üzemanyag fogyasztása, annál kedvezőtlenebb az üzemeltetése (fordított arányosság).

A közigazgatás, illetve a rendészet területéről szintén tömegével hozhatók példák, azonban a jelenségek bonyolult összefüggései miatt a „minél …. – annál …" ok-okozati párok értékelése már korántsem egyértelmű. Például a minél több lezárt ügy (nyomozás), annál hatékonyabb (?!) tevékenység, illetve minél hosszabb ideig tartó ügyintézés (nyomozás), annál kevésbé hatékony (?!) tevékenység párosítás is jól szemlélteti az egyenes, illetve a fordított arányosságot. Igen fontos megjegyezni, hogy ez az értékelés így önmagában véve rendkívül egysíkú és sok esetben torzító jellegű, amire éppen a zárójelbe tett írásjelekkel kívántuk felhívni a figyelmet.

A fordított arányosságra nagyon jellemző példát jelent – önmagában – az árak összevetése. (Minél kisebb az ára egy adott terméknek, annál kedvezőbb a vásárló számára.)

### Az értékelő függvény jellege

A határoló pontok közé második lépésként hozzá kell rendelni egy vetítési görbét (függvényt). (2. számú ábra) Általános esetben ez a görbe tetszőleges lehet, azonban a 2. számú ábrából azonnal látszik egy alapkövetelmény, nevezetesen, hogy ez a jelleg egyértelmű legyen. (Az ábrán feltételezett függvény éppen ezt nem teljesíti!)

Mivel ezt a függvényt értékelés céljából vesszük fel, ezért a független- és függő változó közötti hozzárendelésnek ellentmondásmentesnek kell lennie, azaz az egyenes és fordított arányossági jelleg nem lehet egyidejűleg jelen.

Ez a követelmény formalizált matematikai nyelven megfogalmazva a következőket jelenti:

- A változók egymáshoz rendelése kölcsönös és egyértelmű legyen;
- A függvény jellege a határoló pontok között szigorúan monoton növekvő, vagy szigorúan monoton csökkenő legyen.

(A monoton növekvő illetve csökkenő jelleg értelmezése:

A monoton növekvő illetve csökkenő jelleg esetében a független változó értékének növekedésével a függő változó értéke nem változik, vagy nő illetve csökken.

A szigorúan monoton növekvő illetve csökkenő jelleg esetében a nem változik eset nincs megengedve, azaz a független változó értékének növekedésével a függő változó értéke nő illetve csökken.)

### A konkrét értékelő függvény kijelölése

A következő lépésben az adott szempont kiértékeléséhez legjobban illetve legcélszerűbben illeszkedő értékelő függvény konkrét kiválasztását kell elvégezni. Erre a célra tulajdonképpen két alapvető lehetőség kínálkozik:

- Lineáris függvény illesztése;
- Nemlineáris karakterisztika meghatározása.

### 4. a. Lineáris függvény feltételezése

Ebben az esetben a vetítési görbét úgy szerkesztjük meg, hogy a szemponthoz rendelt értékelő függvény határoló pontjaira egy egyenes szakaszt illesztünk. Ilyen általános esetet a 3. sz. ábra szemléltet. Értelemszerűen – az egyenes, illetve a fordított arányosságnak megfelelően – két féle alapeset létezik, az emelkedő, vagy a csökkenő egyenes.

E módszer jelentős előnyökkel, ugyanakkor számos hátránnyal is rendelkezik.

Előnyök:

- A módszer rendkívül egyszerű;
- Matematikai leírása igen könnyen megvalósítható;
- Széles alkalmazói réteg számára közérthető és kommunikálható.
- Hátrányok:
- Csak nagyon erősen leegyszerűsítve írja le a valóságot;
- Nem fejezi ki a leírni kívánt folyamatban rejlő lényeges eltéréseket;
- A kapott eltérések a hétköznapi életben előforduló különbségekkel nem mindig arányosak. (például a kétszer olyan drága…., a kétszer olyan jó….. megállapítások nem feltétlenül a valóságos kétszeres viszonyt fejezik ki.)

(A lineáris vetítési görbe egyenletét az 1. függelékben adjuk meg)

### 4. b. Nemlineáris függvény feltételezése

Az egyenes szakaszból álló vetítési görbe hátrányait értelemszerűen úgy tudjuk kiküszöbölni, ha éppen a lineáris jellegét módosítjuk. Ekkor a határoló pontok közé már matematikai értelemben tetszőleges görbét szerkeszthetünk. Természetesen ebben az esetben a 3. pontban már jelzett (szigorú monotonitás) követelményét teljesíteni kell. Általánosan használható esetet szemléltet a 4. sz. ábra. Az ilyen vonal felvételekor a görbe adott pontjához, vagy szakaszához rendelt meredeksége már – szinte – tetszőlegesen választható és ezzel a valóságot jobban tükröző, illetve ahhoz célszerűen illeszkedő módszert kapunk.

Természetesen ennek az eljárásnak is vannak előnyei és hátrányai.

Előnyök:

- A módszer jobban kifejezi az emberi gondolkodás által kialakított értékítéletet;
- Az értékelési skála rugalmasan illeszthető az adott feladathoz, illetve értékelési szemponthoz;
- Az értékelési skála előzetes kidolgozásával – és kellő nyilvánosságával – biztosítható az adott döntéshozatali eljárás megfelelő átláthatósága (transzparencia).

Hátrányok:

- Kifejezett hátrány, hogy az eljárás leírása bonyolult(abb) matematikai leírást és apparátust igényel.

Az ilyen függvény lényeges tulajdonsága, hogy jobban alkalmazható az emberi gondolkodáshoz, ezért ezt nevezhetjük humán-közeli döntéshez illeszkedő görbének, vagy humán-közeli skálának is. (Az 1. függelékben egy speciális, sin/cos függvénnyel megvalósított nemlineáris vetítési görbe egyenletét is megadjuk.)

A 4. sz. ábrán szemléltetett függvény feltételezése tulajdonképpen önkényes és azon alapul, hogy jellegre az előbb említett humán-közeli tulajdonságot mutatja, ugyanakkor matematikailag viszonylag egyszerűen leírható. E feltételeknek a sin/cos függvény megfelel és ezért szerepeltettük e függvény általánosított matematikai képletét a függelékben.

Hangsúlyozni kívánjuk, hogy adott konkrét esetben tetszőleges (monoton) függvény alkalmazható, kizárólag a felhasználás matematikai apparátus-igénye szab korlátot.

### Finomhangolás

Az előzőekben felvázolt általános jellegű megfontolásokon túlmenően célszerűnek tűnik az eljárás további pontosítása. Ennek keretében a konkrét skálát oly módon célszerű megválasztani, amely az adott feladathoz a lehető legjobban illeszkedik. Ez lényegében matematikai értelemben azt jelenti, hogy a függvény értelmezési tartományában a meredekséget különböző módon (vagy mértékben) határozzuk meg. (Az eltérő jelleg – az adott feladathoz való illeszkedés miatt – általában a szélső illetve a középső tartományokban változik.) Ez a tulajdonság úgy fejezhető ki, hogy rendszerint az intervallum kevésbé fontosnak ítélt szélénél már indifferens a megkülönböztetés.

Hétköznapi értelemben a nyilvánvalóan elégtelen – és elfogadásra nem javasolt – megoldás esetében az értékítélet szempontjából már mindegy, hogy az a változat milyen mértékben rossz. Ilyen általános eset látható az 5. számú ábrán. A szemléltetésen szereplő – a minimális értékelési pontszámot érő – vízszintes szakaszok fejezik ki a „midegy, hogy…” jelleget.

Az alapgondolat a már az előzőekben leírt módon azt fejezi ki, hogy az értékelő személy számára kedvezőtlen tartomány széle felé haladva az értékítéletnek nincs megkülönböztető jelentősége. Ezért abban a tartományrészben az értékelő görbe vízszintes.

Ebben az esetben azonban vissza kell térni a 3. pontban megfogalmazott feltételekre, nevezetesen a függvény szigorúan monoton jellegének szükségességére. A „mindegy, hogy mennyire rossz" szemléletet kifejező vízszintes szakaszok esetén nincs szükség a szigorú monotonitásra, elegendő a függvény monoton jellegének biztosítása.

### Döntési folyamat a gyakorlatban

A fenti formalizált lépések bemutatása után általánosítsuk a döntési folyamatot a gyakorlatban előforduló esetekre. Példaként egy olyan döntés folyamatát és feltételrendszerét elemezzük, amely például valamilyen termék beszerzése során merül fel, a verseny tisztaságának biztosítása érdekében megalkotott közbeszerzésekről szóló 2003. évi CXXIX törvény (kbt.) előírásainak figyelembe vételével.

#### 6. a. A kbt. előírásai, mint a döntések feltételrendszere

A törvény az általános gazdasági- és jogi alapelveken túlmenően részletesen szabályozza az eredményhirdetéshez vezető döntések peremfeltételeit. Az 57. § kimondja az értékelési szempontok, valamint a hozzájuk rendelt súlyozások kialakításának előírását és a pontos meghatározásukra vonatkozó tartalmi követelményeket.

- (1) Az ajánlatkérő az ajánlati felhívásban köteles meghatározni az ajánlatok bírálati szempontját.
- (2) Az ajánlatok bírálati szempontja a következő lehet:
- a) a legalacsonyabb összegű ellenszolgáltatás, vagy
- b) az összességében legelőnyösebb ajánlat kiválasztása.
- (3) Ha az ajánlatkérő az összességében legelőnyösebb ajánlatot kívánja kiválasztani, köteles meghatározni
- a) az összességében legelőnyösebb ajánlat megítélésére szolgáló részszempontokat;
- b) részszempontonként az azok súlyát meghatározó - a részszempont tényleges jelentőségével arányban álló - szorzószámokat (a továbbiakban: súlyszám);

E paragrafus azt is megszabja, hogy az egyes szempontokhoz tartozóan az értékelési skálák azonos határait szükségességes alkalmazni. (Ezen előírást a későbbiekben egy speciális eset – az árak összevetése – kapcsán önállóan elemezzük.)

(az ajánlatkérő … köteles meghatározni)

- c) az ajánlatok részszempontok szerinti tartalmi elemeinek értékelése során adható pontszám alsó és felső határát, amely minden részszempont esetében azonos;
- d) azt a módszert (módszereket), amellyel megadja a ponthatárok [c) pont] közötti pontszámot.

Ezen előírások figyelembe vételével egy feltételezett beszerzésre vonatkozó általános szempont-rendszert és annak értékelési módszereit dolgoztuk ki a 2. függelékben. Az ott leírtakat valamilyen árubeszerzésre lehet vonatkoztatni, de természetesen a konkrét súlyszámokat, ponthatárokat és ennek megfelelően az értékelési skálát a dolgozatban önkényesen választottuk meg, amit a gyakorlatban az adott feladathoz illeszkedő módon célszerű meghatározni. Ennek megfelelően – a konkrét feladatok

következtében – természetesen előfordulhatnak megegyező, azonos értékű súlyszámok, illetve tört értékek is.

6. b. A beszerzési, illetve az ajánlati ár értékelése

Mint azt a 4. b. pontban bemutattuk, az árak összevetésére a fordított arányosság és az emberi gondolkodáshoz jobban illeszkedő nemlineáris skála alkalmazása indokolt. Ez az állítás a következő gondolatmenettel támasztható alá.

Valamilyen termék esetén – kizárólag az árakat figyelembe véve – nyilvánvalóan a legolcsóbb termék nyeri el a legjobb értékelést. Azonban a legolcsóbbtól csupán kismértékben (pl.: 2 – 10 %-kal) drágább termék esetében az értékítélet még nem nagyon csökken. Ugyanez a helyzet áll elő az ár-sáv másik (drága) szélénél is. A „nagyon drága" kategóriában már ismét szinte érdektelen az ár-eltérés, ugyanis az értékítélet ekkor már a minimumtól alig tér el. Az ilyen módon előálló értékelési vetítési görbe tehát a sáv közepén meredekebb, a sáv szélein pedig kevésbé meredek, lankásabb.

Az 1. függelékben megadott sin/cos matematikai képlet viszonylag egyszerűen számszerűsíthető esetet ír le. Adott konkrét feladathoz kapcsolódva sokszor célszerűbb a függvény grafikus megadása, illetve egyenes szakaszokkal való töréspontos közelítése.

A 2. függelékben példaként megadott, a rész-szempontok értékelésére szolgáló eljárásoknál az is szerepel, hogy a (részajánlatoknál) esetlegesen előforduló térítésmentes ellenszolgáltatást 1 Ft-ként kell kezelni. E kikötést csupán azért tettük, hogy a matematikai képletből esetlegesen következő zérussal való osztást, illetve az ebből fakadó számítási hibát elkerüljük.

6. c. Az értékelő pontszámok azonos határainak követelménye

Mint láttuk, a kbt – a verseny tisztaságának érdekében – előírja az értékelő skála ponthatárainak azonosságát. E követelménynek való megfelelés kérdése merül fel azonban a jelenlegi hazai beszerzési gyakorlatban, amikor sok eljárásban az árak értékelése a következő képlet szerint történik:

$$\text{pontszám} = \frac{\text{minimális ár}}{\text{aktuális ár}} \cdot 100$$

Ponthatárnak a 0 – 100 intervallum szerepel, ami igen szemléletes százalékos skálát jelent.

A fenti képlet alapján számított pontszám azonban a hiperbola függvény miatt a 0 (zérus) értéket csak „végtelen" nagy ár esetén éri el, ami nyilvánvalóan a gyakorlatban nem fordul elő. Ennek következtében e képlet gyakorlati alkalmazása – egyszerűsége ellenére – a jelenleg hatályos törvény-szövegnek való megfelelés szemszögéből kérdésesnek tekinthető.

Egyébként a fenti függvény, amely a független változó első hatványával arányos ugyan (de nem lineáris) az ársáv „olcsó" szélénél éppen ellentétes görbületű, mint az előző pontban leírt humán-közeli skála. A görbe meredeksége (esése) pont a legkisebb árnál a legnagyobb, azaz ebben a tartományban csupán kis mértékű árnövekedés is viszonylag jelentős pontszámcsökkenést eredményez. (6. sz. ábra)

## Összefoglalás

A társadalmi folyamatok valamennyi területén, így a közigazgatásban, a rendvédelem terén, vagy a különböző szakigazgatásokban is szükség van az informá-

ciók alapján történő döntéshozatalra. A dolgozat e döntéshozatali eljárás folyamatának egy szakaszával foglalkozik. E tevékenység-láncolatból – kiemelkedő jelentősége alapján – vizsgáltuk az adott információk alapján végzett értékelést, amelyet elemeire bontottunk és ezek matematikai leírását adtuk meg.

Az értékelési folyamatban első lépésként az adott szemponthoz rendelt értékelő függvény határoló pontjait célszerű meghatározni. Ennek azért van különös jelentősége, mert ebből – formálisan is – kiderül az értékelési szempont egyenes, vagy fordított arányosságának jellege. A határoló pontok közé azután hozzá kell rendelni a vetítési görbét. Általános esetben ez a görbe tetszőleges lehet, azonban e függvénynek néhány alapkövetelményt teljesítenie kell. A leglényegesebb ilyen követelmény, hogy a független- és függő változó közötti hozzárendelésnek ellentmondásmentesnek kell lennie, azaz az egyenes és fordított arányossági jelleg nem lehet egyidejűleg jelen.

A következő lépésben az adott szempont kiértékeléséhez legjobban illetve legcélszerűbben illeszkedő értékelő függvény konkrét kiválasztását kell végrehajtani, melyre vonatkozóan két alapvető lehetőség kínálkozik:

- Lineáris függvény illesztése;
- Nemlineáris karakterisztika meghatározása.

A dolgozatban bemutattuk e (kétféle jellegű) függvények meghatározását és alkalmazásuk előnyeit, illetve hátrányait. Az általános jellegű megfontolásokon túlmenően felvetettük az eljárás további pontosításának szükségességét, melynek keretében a konkrét skálát oly módon célszerű kialakítani, amely az adott feladathoz a lehető legjobban illeszkedik. Ez matematikai értelemben azt jelenti, hogy a függvény értelmezési tartományában a meredekséget különböző módon (vagy mértékben) határozzuk meg. Az alapgondolat azt fejezi ki, hogy az adott szempont szerint az értékelő személy számára kedvezőtlen tartomány széle felé haladva az értékítéletnek már nincs differenciáló képessége.

A formalizált lépések bemutatása után általánosítottuk a döntési folyamatot a gyakorlatban előforduló esetekre. E módszert kiterjesztve kimunkáltuk egy termékbeszerzésre vonatkozó általános közbeszerzési eljárás bírálati szempontjait, továbbá azok értékelési módszereit, a közbeszerzésekről szóló törvény előírásainak figyelembe vételével. Példaként egy olyan döntés folyamatát és feltételrendszerét elemezzük, amely valamilyen termék beszerzése során merül fel.

A felvázolt általános módszer elméleti alapjainál kiemeltük, hogy mindenkor az adott konkrét esethez, feladathoz kell a megfelelő matematikai függvényt, vagy közelítést hozzárendelni, melynek matematikai apparátusát is ki kell dolgozni.

## Függelék 1

### Vetítési görbe képletek

A 3. a.) számú ábrán szereplő egyenesen arányos lineáris vetítési görbe képlete:

$$\acute{E} = \frac{\acute{E}_{max} - \acute{E}_{min}}{S_{max} - S_{min}} \cdot \left(S - S_{min}\right) + \acute{E}_{min}$$

ahol:

- $\acute{E}$ az értékelés számértéke;
- $\acute{E}_{max}$ az értékelés legnagyobb számértéke;
- $\acute{E}_{min}$ az értékelés legkisebb számértéke;
- $S$ a szempont számértéke;
- $S_{max}$ a szempont legnagyobb számértéke;
- $S_{min}$ a szempont legkisebb számértéke.

A 3. b.) számú ábrán szereplő fordítottan arányos lineáris vetítési görbe képlete:

$$\acute{E} = -\frac{\acute{E}_{max} - \acute{E}_{min}}{S_{max} - S_{min}} \cdot \left(S - S_{min}\right) + \acute{E}_{max}$$

ahol:

- $\acute{E}$ az értékelés számértéke;
- $\acute{E}_{max}$ az értékelés legnagyobb számértéke;
- $\acute{E}_{min}$ az értékelés legkisebb számértéke;
- $S$ a szempont számértéke;
- $S_{max}$ a szempont legnagyobb számértéke;
- $S_{min}$ a szempont legkisebb számértéke.

A 4. a.) számú ábrán szereplő egyenesen arányos sinusos vetítési görbe képlete:

$$\acute{E} = \frac{\acute{E}_{max} + \acute{E}_{min}}{2} + \frac{\acute{E}_{max} - \acute{E}_{min}}{2} \cdot \sin\left(\frac{2S - S_{max} - S_{min}}{S_{max} - S_{min}} \cdot \frac{\Pi}{2}\right)$$

ahol:

- $\acute{E}$ az értékelés számértéke;
- $\acute{E}_{max}$ az értékelés legnagyobb számértéke;
- $\acute{E}_{min}$ az értékelés legkisebb számértéke;
- $S$ a szempont számértéke;
- $S_{max}$ a szempont legnagyobb számértéke;
- $S_{min}$ a szempont legkisebb számértéke.

A 4. b.) számú ábrán szereplő fordítottan arányos cosinusos vetítési görbe képlete:

$$\acute{E} = \frac{\acute{E}_{max} + \acute{E}_{min}}{2} + \frac{\acute{E}_{max} - \acute{E}_{min}}{2} \cdot \cos\left(\frac{S - S_{min}}{S_{max} - S_{min}} \cdot \Pi\right)$$

ahol:

- $\acute{E}$ az értékelés számértéke;
- $\acute{E}_{max}$ az értékelés legnagyobb számértéke;
- $\acute{E}_{min}$ az értékelés legkisebb számértéke;
- $S$ a szempont számértéke;
- $S_{max}$ a szempont legnagyobb számértéke;
- $S_{min}$ a szempont legkisebb számértéke.

## Függelék 2

### Értékelési szempontok és azok szerinti kiértékelő eljárások, módszerek (mintapélda)

Bírálati szempontok:

Az ajánlatkérő az ajánlatokat az összességében legelőnyösebb ajánlat alapján bírálja el a pénzügyi- és szakmai alkalmassági, továbbá műszaki- és gazdasági tényezők figyelembevételével.

Az ajánlatok minősítése komplex kiértékelő rendszer alapján történik. Az érvényes ajánlatok elbírálása érzékeny a megoldás minőségi paramétereire, a kivitelezés határidejére és a megvalósítás módjára vonatkozó javaslatra, figyelembe véve a jelenleg üzemelő rendszerek folyamatos üzemének fenntartását.

| ***Részszempontok*** | Súlyszám |
|---|---|
| 1. Műszaki paraméterek megfelelősége | 10 |
| 2. Tervezésnek való megfelelőség | 9 |
| 3. Ajánlati ár | 8 |
| 4. Vállalt teljesítési határidők | 7 |
| 5. Referenciák | 6 |
| 6. Az ajánlatban megajánlott opciók | 5 |
| 7. Tartalék-anyag készlet szükséglet | 4 |
| 8. Minőségbiztosításban elért minősítés | 3 |
| 9. Jótállás feltételei és időtartama, szavatosság | 2 |
| 10. Üzemeltető állomány kiképzése, oktatás | 1 |

A részszempont értékelése során adható pontszám: 0 – 10.

**A részszempontok pontozására szolgáló eljárások**

1. A műszaki paraméterek megfelelőségi nyilatkozata szerinti teljes körű egyezés esetén 10 pont.
   Valamely követelmény(ek)nek való meg nem felelés esetén arányosan kevesebb.

2. A tervezésre vonatkozó nyilatkozat szerinti teljes körű egyezés esetén 10 pont.
   Valamely követelmény(ek)nek való meg nem felelés esetén arányosan kevesebb.

3. Az ajánlati ár értékelése az alábbi képlet szerint történik:

$$\text{pontszám} = 7{,}5 + 2{,}5 \cos \left[ \frac{\text{Ár} - \text{m}}{4\,\text{m}} \right] \Pi \qquad \text{ha az Ár} \leq 5\,\text{m};$$

$$\text{pontszám} = 0 \text{ ha az Ár} > 5\,\text{m}$$

Amennyiben csak két ajánlatot kell összevetni és a két ár aránya $\frac{M}{m} < 2$ akkor:

$$\text{pontszám} = 7{,}5 + 2{,}5 \cos \left[ \frac{\text{Ár} - \text{m}}{\text{m}} \right] \Pi$$

ahol: M = legmagasabb ár
m = legalacsonyabb ár
Ár = aktuális pályázati ár
pontszám = két tizedesre kerekítve

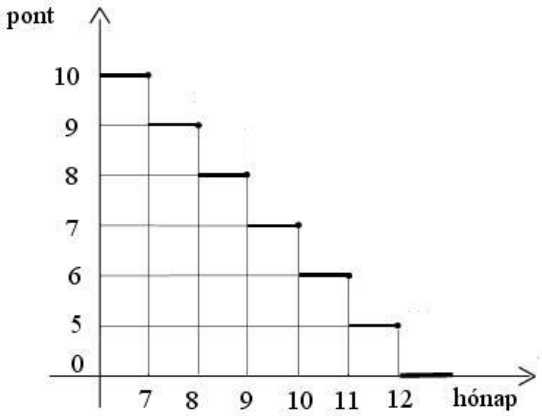
Ha az ajánlati ár értékelésénél az ajánlat térítésmentes ellenszolgáltatást tartalmaz, akkor az értékelési eljárásnál 1 Ft-ként kell figyelembe venni.

4. Teljesítési határidő:

A dokumentációban előírt határidő (például 12 hónap) vállalása 5pont,

1-1 hónappal előbbi határidő vállalása + 1-1 pont,

(max. 10 pont az alábbi diagrammon ábrázolt lépcsős függvény szerint)




(balról nyílt, jobbról zárt intervallum)

5. Az ajánlatban megadott referenciák alapján

| | Pont |
|---|---|
| Legalább 10 BM és alárendeltségébe tartozó referenciahely | 10 |
| Legalább 10 kormányzati referenciahely | 8 |
| Legalább 10 hazai referenciahely | 6 |
| Legalább 10 tetszőleges referenciahely | 4 |
| Kevesebb referenciahely | 2 |
| Nincs referenciahely | 0 |

6. Az ajánlatban megajánlott opciók:

| | Pont |
|---|---|
| Nincs | 0 |
| kért opció megajánlása | 8 |
| többlet opció megajánlása | 10 |

7. A tartalék-anyag készlet szükséglet értékelése az ajánlatban megadott beszerzési árak alábbi képlet szerinti összehasonlításával történik:

$$\text{pontszám} = 6 + 4 \cos \frac{\text{Ár} - \text{m}}{4\,\text{m}} \Pi \qquad \text{ha az Ár} \leq 5\,\text{m};$$

$$\text{pontszám} = 0 \text{ ha az Ár} > 5\,\text{m}$$

Amennyiben csak két ajánlatot kell összevetni és a két ár aránya $\frac{M}{m} < 2$

akkor:

$$\text{pontszám} = 7{,}5 + 2{,}5 \cos \frac{\text{Ár} - \text{m}}{\text{m}} \Pi$$

ahol: M = legmagasabb ár
m = legalacsonyabb ár
Ár = tartalék eszközök ára
pontszám = két tizedesre kerekítve

Ha az ajánlati ár értékelésénél az ajánlat térítésmentes ellenszolgáltatást tartalmaz, akkor az értékelési eljárásnál 1 Ft-ként kell figyelembe venni.

8. Minőségbiztosításban elért minősítés:

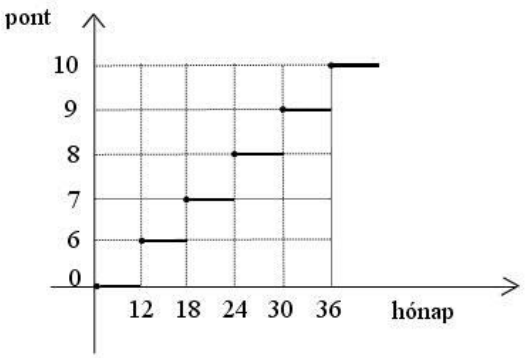
| | Pont |
|---|---|
| Nincs | 0 |
| ISO 9001 | 8 |
| AQAP vagy NATO | 10 |

9. Jótállás feltételei és időtartama, szavatosság

A dokumentációban előírt határidő (például 12 hónap) vállalása 6 pont,

6-6 hónap további garanciaidő vállalása +1-1 pont,

(max. 10 pont az alábbi diagrammon ábrázolt lépcsős függvény szerint)




(balról zárt, jobbról nyílt intervallum)

10. Az üzemeltető állomány kiképzése, oktatása az ajánlatban megadott tematika, óraszám alapján (0-5 pont), valamint az árösszesítőben megadott költségek alábbi képlet szerinti összehasonlításával, valamint összegzéssel történik:

$$\text{pontszám} = 2{,}5 + 2{,}5 \cos \frac{\text{Ár} - \text{m}}{\text{M} - \text{m}} \Pi$$

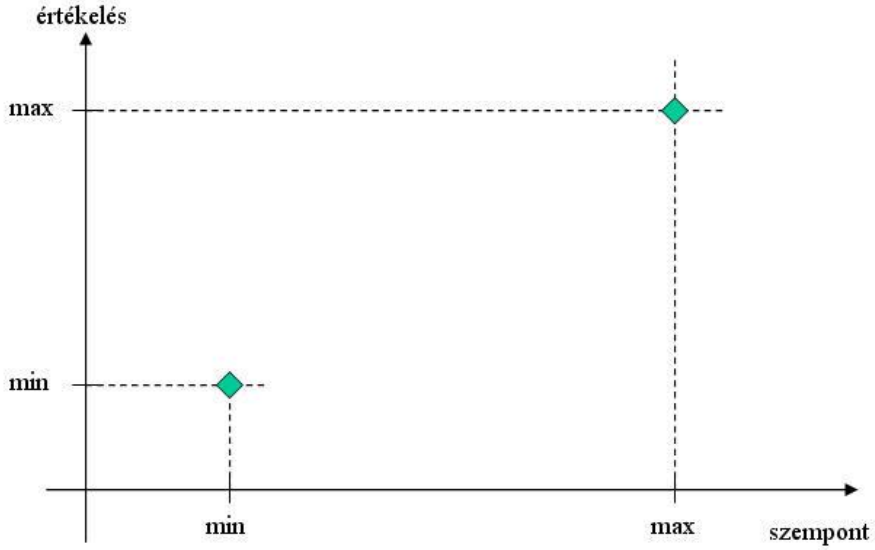
ahol: M = legmagasabb ár
m = legalacsonyabb ár
Ár = oktatás költsége
pontszám = két tizedesre kerekítve

Amennyiben csak két ajánlatot kell összevetni és a két ár aránya $\frac{M}{m} < 2$ akkor:

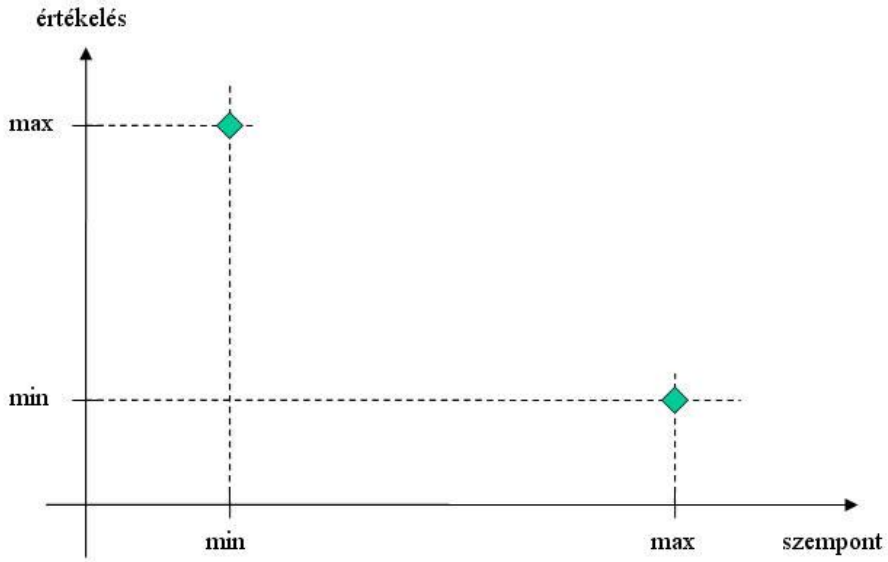
$$\text{pontszám} = 7{,}5 + 2{,}5 \cos \frac{\text{Ár} - m}{m} \Pi$$

I Ha az ajánlati ár értékelésénél az ajánlat térítésmentes ellenszolgáltatást tartalmaz, akkor az értékelési eljárásnál 1 Ft-ként kell figyelembe venni.

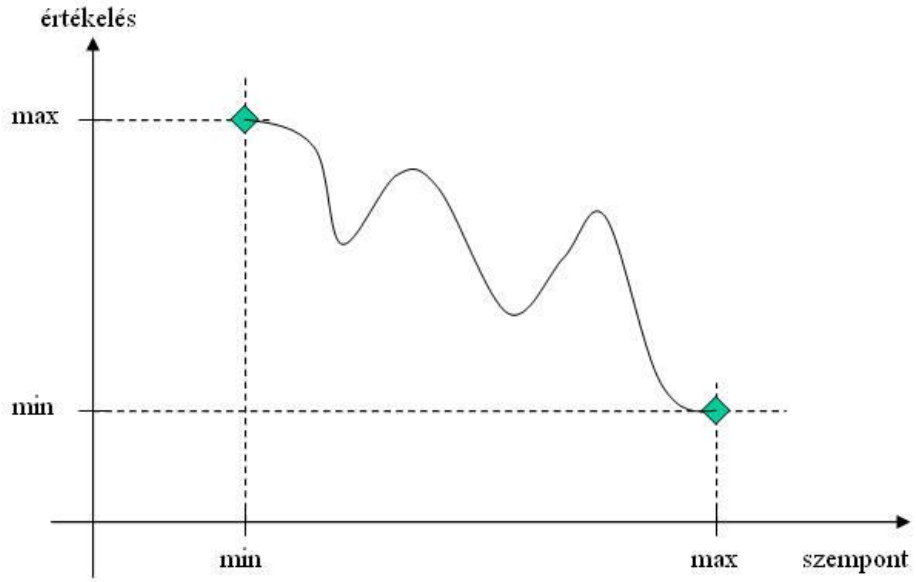
**Ábragyűjtemény:**



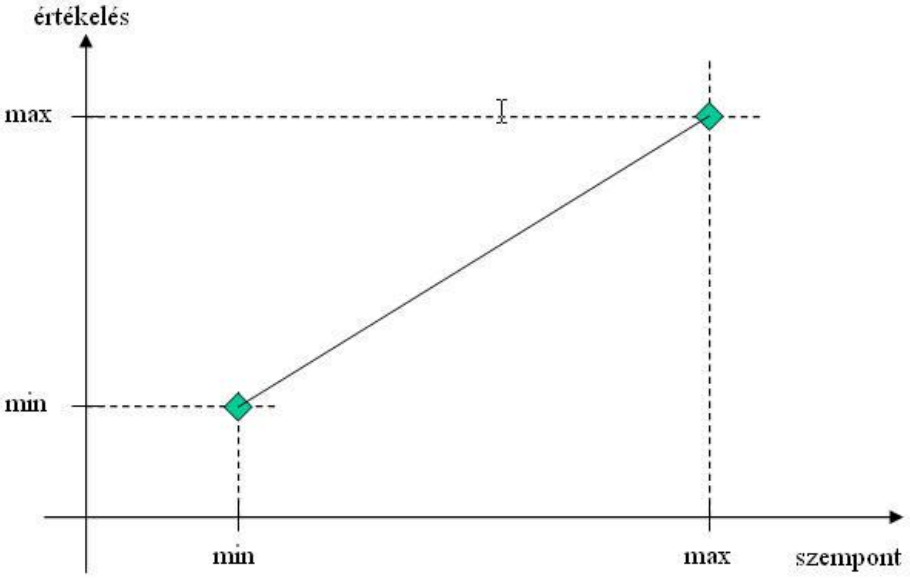

1. számú ábra a.) egyenes arányosság határoló pontjai



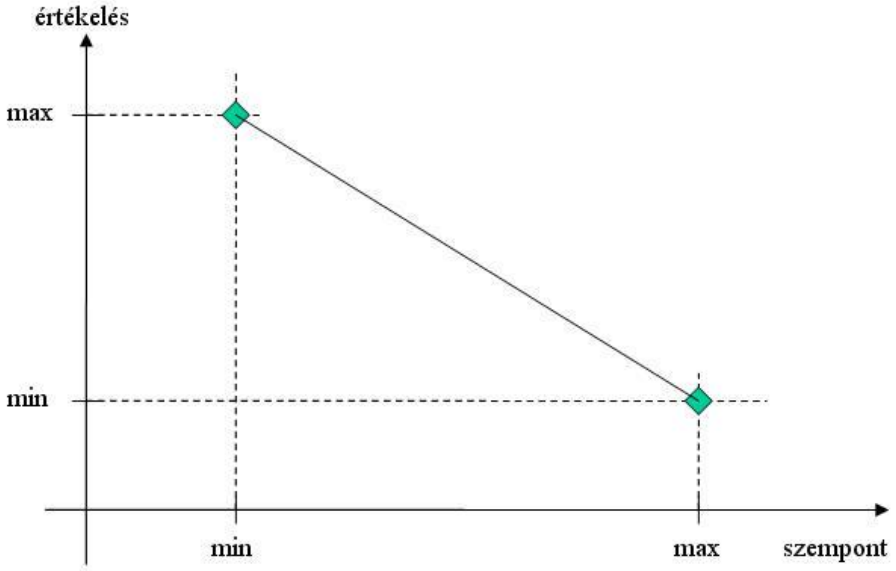

1. számú ábra b.) fordított arányosság határoló pontjai



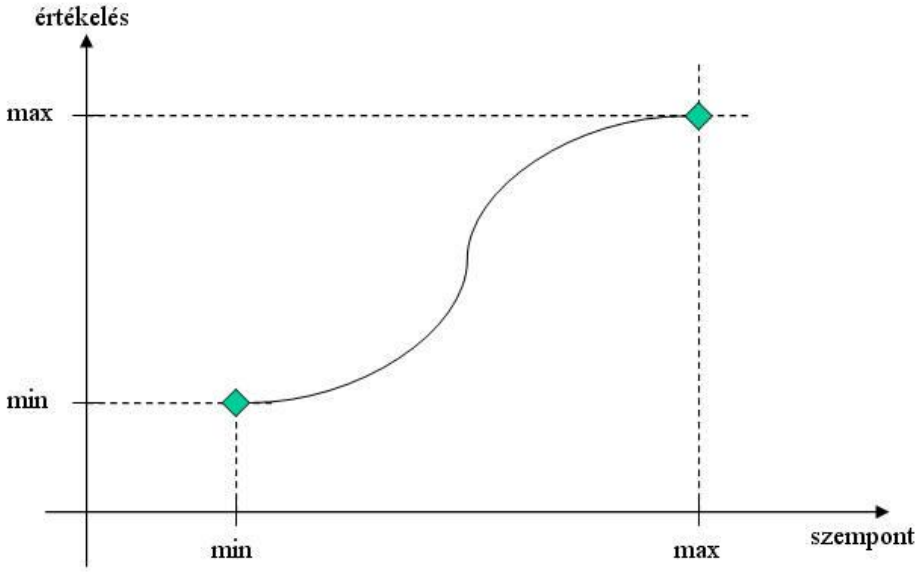

2. számú ábra általános vetítési görbe



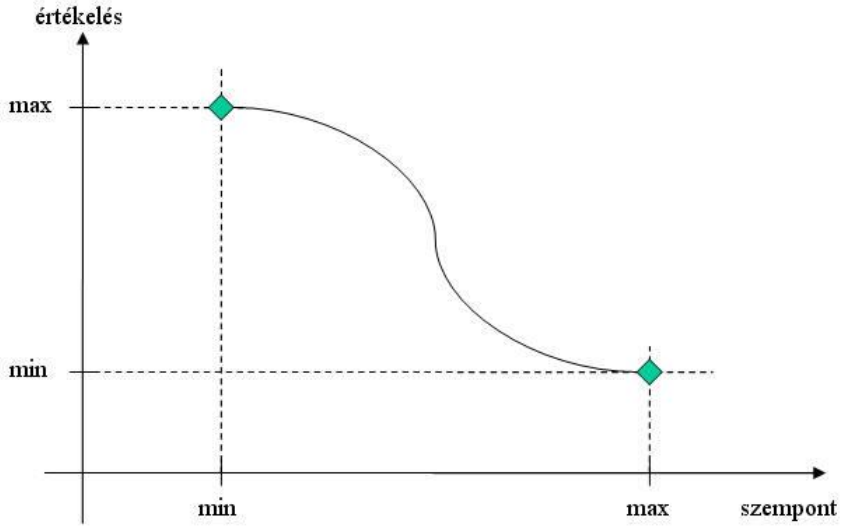

3. számú ábra a.) egyenesen arányos lineáris vetítési görbe



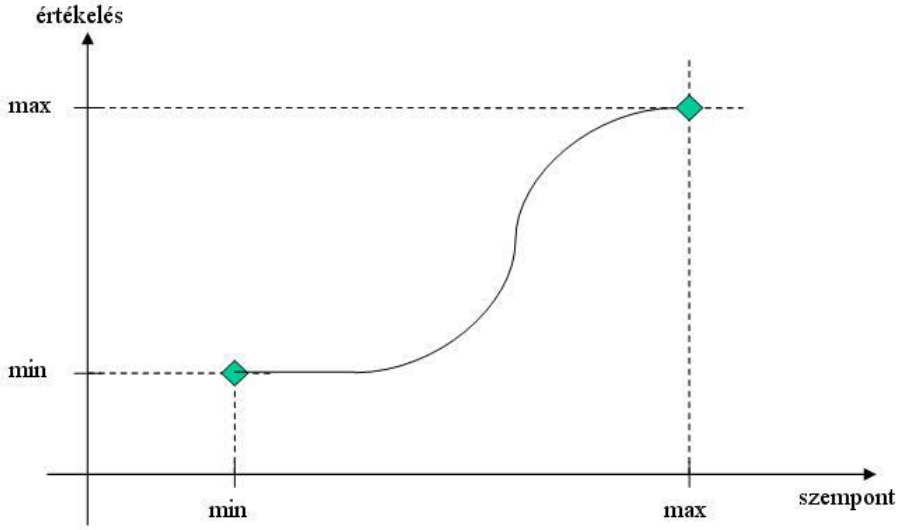

3. számú ábra b.) fordítottan arányos lineáris vetítési görbe



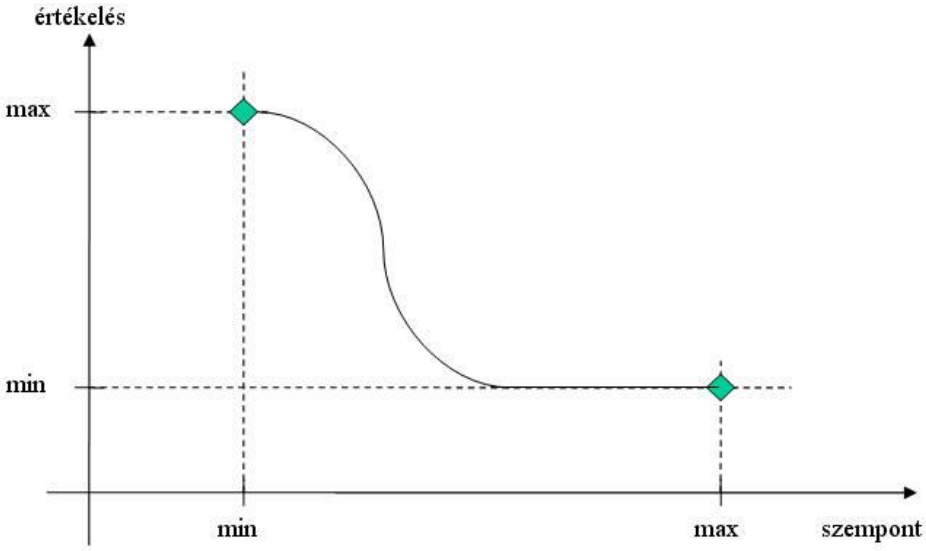

4. számú ábra a.) egyenesen arányos sinusos vetítési görbe



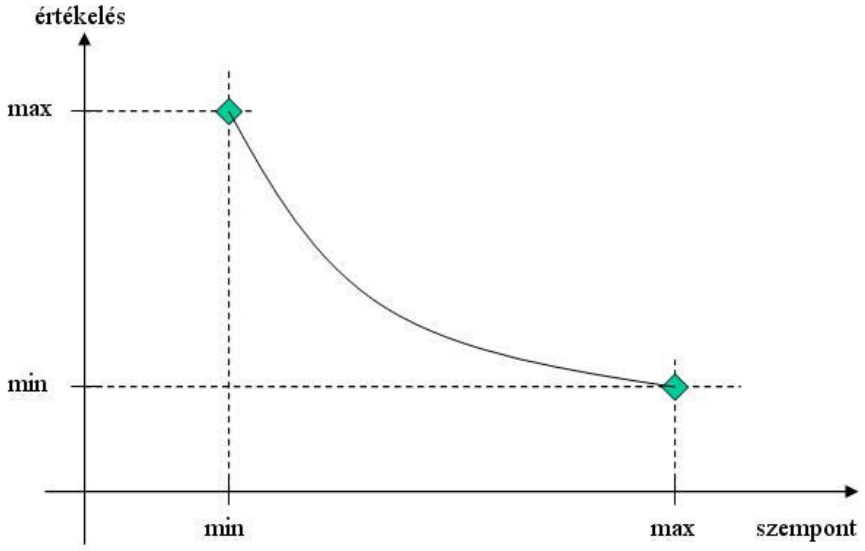

4. számú ábra b.) fordítottan arányos cosinusos vetítési görbe




5. számú ábra a.) egyenesen arányos kiterjesztett sinusos vetítési görbe




5. számú ábra b.) fordítottan arányos kiterjesztett cosinusos vetítési görbe




6. számú ábra hiperbola alakú vetítési görbe

## Irodalomjegyzék


[1] Benesch, H.: Atlasz, Pszichológia. Athenaeum kiadó, 1999.
[2] Csath M.: Stratégiai tervezés és vezetés. Leadership Kft.
[3] Geus, A.: The living Company. Harvard Business Review, 1997. márc.-ápr.
[4] Kindler J.: Fejezetek a döntéselméletből Aula, BKE Budapest, 1991.
[5] Marosi M.: Távol-keleti menedzsment. Közgazdasági és Jogi könyvkiadó, Budapest 1997.
[6] Nováky E (szerk.).: Káosz és jövőkutatás. BKE Jövőkutatási Tanszék, Budapest 1995.
[7] PhD Tanulmányok 2. Pécsi Tudományegyetem Állam-és Jogtudományi Karának Doktori Iskolája, Szerkesztő: Dr Ádám Antal, Pécs 2004.
[8] Simon, H: Korlátozott racionalitás. Válogatott tanulmányok. Közgazdasági és jogi könyvkiadó Budapest, 1982.
[9] Szabó K.: Drótmenedzsment, avagy a káosz irányítása. Társadalmi Szemle, 1995/7.
[10] Vécsey Zsadány: A káosz peremén. BKÁE Vezetőképző Intézet Publikációi Budapest 2000.
[11] 2003. évi CXXIX. Törvény a közbeszerzésekről

**FARKAS György**

# ÚJ KOMMUNIKÁCÓS KIHÍVÁS A SPAM

MK Információs Hivatal
+36-70-317-7630; georg.wolf@csucsposta.hu

## Bevezetés

A cikk az internet széleskörű elterjedésével párhuzamosan kialakult új iparágba, a kéretlen elektronikus üzenetek, a spamek világába nyújt betekintést. Napjainkban a különböző vírusok, férgek után a spamek okozzák a legtöbb bosszúságot az internet felhasználók körében. Először a spam fogalmát, jellemzőit, elterjedésének okát, valamint az okozott problémákat, károkat, majd a spamek elleni védekezés lehetőségeit tekintem át. Világszerte számos intézkedést foganatosítottak a spam megfékezésére a kormányok, az internet szolgáltatók (ISP-k), az email szolgáltatók (ESP-k), az email-reklámozók, kereskedők, antispam szervezetek, fogyasztóvédelmi szervezetek, antispam programozók, stb. Bemutatom a különböző kormányok, és szervezetek intézkedéseit jogi, szabályozási, önszabályozási, oktatási és technikai megközelítésben.

Az utóbbi évtizedek információtechnológiai fejlődés következtében a polgári, a védelmi szféra és a kormányzat különböző szervezetinek működése az alkalmazott informatikai rendszerektől erősen függővé vált. Ennek következtében az informatikai biztonság alapvető nemzetbiztonsági érdekké nőtt, melynek egyik sarkallatos kérdése a kéretlen üzenetek áradatának kontrollálása a folyamatos rendelkezésre állás biztosítása érdekében. Az Internet lassan az élet mindennapos részévé válik. Egyre szélesebb körben alkalmazzuk. Az email az emberek gazdasági és társadalmi életében alapvető kommunikációs eszközzé, és erős médiummá vált a telefon mellett, nem csak az információ- és gondolatcsere, hanem az e-kereskedelem területén is. Az International Data Corporation (IDC) becslése szerint 2006[9]-ban már körülbelül 60 milliárd emailt továbbítanak. Sajnos a vonzó, elérhető, olcsó, platform független szolgáltatások melyeket a világméretű hálózatok, köztük az internet nyújtanak, sebezhetőek. Különös tekintettel a napjainkban módszereiben kiszélesedő globalizálódó, és elharapódzó terrorizmusra, mely minden elérhetőt bevet céljai érdekében. Az internet széleskör[10]ű elterjedésével párhuzamosan kialakult egy új iparág, a kéretlen elektronikus üzenetek, a spamek világa. Napjainkban a különböző vírusok, férgek után a spamek okozzák a legtöbb bosszúságot az internet felhasználók körében. Az alábbiakban meghatározásra kerül a spam fogalma, jellemzői, veszélyei valamint a jelenlegi spam korlátozását célzó szabályozási gyakorlat a világ különböző országaiban. Az intézkedések jogi, szabályozási, önszabályozási, oktatási és technikai megközelítésben kerültek besorolásra. A cikk célja átfogó képet nyújtani a világon előforduló különbö-

9 „E-mail marketing: Consumer choices and business oppurtunities – Discussion paper”. Industry Canada 2003. január; http://e-com.ic.gc.ca/english/strat/e-mail_marketing.html

10

ző spam szabályozási, megközelítési módokról, és ezek korlátairól, ezáltal segítséget nyújtva a saját spam elleni védelmi stratégia kialakításához.

**Mi is a SPAM?**

A spam meghatározása hasznos lenne, viszont úgy tűnik jelenleg nincsen egyetértésen alapuló, használható definíció. A jelenséget különböző módon tekintik a különböző országokban. Számos ország azonban alkotott egy általánosan használható definíciót. Franciaországban a spam alatt a nagyszámú, gyakran gazdasági természetű, ismétlődő kéretlen email-eket értik. Olyan személyek részére, amelyekkel a feladó nem volt korábban kapcsolatban, és akiknek az email címe publikus helyen fellelhető az interneten[11]. Az Európa Bizottsági jelentés szerint a spam általában ismétlődő, tömeges kéretlen kereskedelmi levélküldés, egy olyan feladó által, aki eltakarja, vagy meghamisítja önazonosságát. Ellenben nem minden kéretlen kereskedelmi kommunikáció spam[12]. Az ausztrál értelmezés szerint a spam egy olyan terminus, amelyet általánosságban használnak a kéretlen elektronikus üzenetekre, amelyeket általában nagyszámú címzett kap. Általában – de nem feltétlenül – kereskedelmi tartalmuk van (hirdetni és eladni termékeket vagy szolgáltatásokat); és az alábbi felsorolás közül egy vagy több jellemzőjük van:

- Céltalan és megválasztás nélküli módon kerülnek elküldésre, gyakran automatikus módon
- Tartalmaz, vagy hirdet illegális vagy sértő tartalmat
- Tisztességtelen vagy félrevezető céljuk van
- Személyes adatokat gyűjtenek, amely ellentétes a Privacy Act 1998 National Privacy Principles (NPPs) – el.
- Eltakarja a feladó kilétét
- Nem adnak érvényes és működő címet, ahová a fogadók üzenetet küldhetnek annak érdekében, hogy ne kapjanak további kéretlen üzeneteket13

A jellemzők lehetnek elsődlegesek vagy másodlagosak az alábbiak szerint.

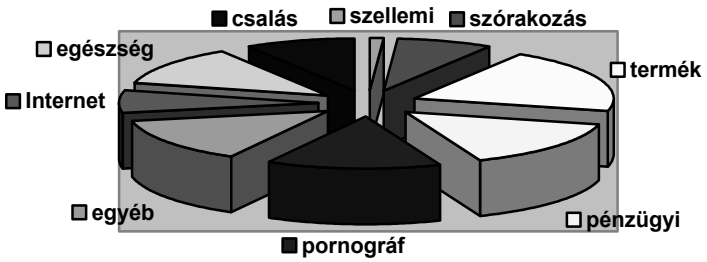
| Elsődleges tulajdonságok | Másodlagos tulajdonságok |
|---|---|
| Elektronikus üzenetek | Beleegyezés és a tulajdonos tudta nélkül gyűjtött címeket használ |
| Nagyszámú | Nem kívánatos |
| Kéretlen | Ismétlődő |
| Kereskedelmi | Célzott közönség és válogatás nélküli |
| | Megállíthatatlan |
| | Anonim és/vagy fedett |
| | Illegális vagy sértő tartalmú |
| | Félrevezető vagy tisztességtelen tartalmú |

11 Comission Nationale de l'Informatique et des Libertés: „Le publipostage électronique et la protection des données personnelles" Madame Cévile Alvergnat jelentése 1999. október 14.

12„Unsolicited Commercial Communications and Data Proptection", Commission of the European Communities, 2001. január; http://europa.eu.int/comm/internal_market/privacy/docs/studies/spamsum_en.pdf

13 www.noie.gov.au/publications/NOIE/spam/final_report/SPAMreport.pdf.

**Spam kategóriák14**




A spam az egyik legellentmondásosabb internet használatot és e-kereskedelmet befolyásoló témává vált. Mi az indítékuk a spam küldőknek az üzeneteik küldésére?

A különböző szofisztikált adatbázisok kifejlődése, egyre népszerűbbé tette a telemarketinget és az email-marketinget, mint a direkt marketing egyik stratégiáját. A direkt marketinget a cégek fontos eszköznek tekintik, hogy megközelítsék, informálják, megtartsák a (potenciális) vevőiket. Az elektronikus üzenetek, beleértve az email-t is, könnyű és olcsó módja egy nagyobb csoporttal való kapcsolatfelvételnek. Ezek az előnyök veszélybe kerülnek a spam folyamatos áradása miatt.

Nehéz dolog beazonosítani a spam-küldőket, akik különböző módszereket használnak a személyazonosságuk elfedésére. Véletlenszerű feladói címeket választanak, a spam-küldő programok automatikusan hamis fejlécet és feladói email-címet generálnak. Más spam-küldők az internetet felhasználva, külföldi országok átjátszóit használják, hogy az üzeneteiket nem lehessen visszakövetni. A spamek 50%-a internetes levelezőrendszereken keresztül érkezik, a világ különböző pontjairól, a másik 50% egy harmadik féltől jön, amely kihasználja a nyitott proxy szervereket és nyitott átjárókat15. Néhány spam-küldő ingyenes email-t nyit, majd elhagyja azt. Olyan programokat használnak, amelyek különböző fiókokat használnak, és az egyik fiók lezárásakor, a másik automatikusan a helyére lép. Sokan egyszerűen átmennek egy másik internet-szolgáltatóhoz, amikor lezárják a számláikat, spam-tevékenység miatt. Mások pedig azt mondják az internet-szolgáltatóiknak, hogy ők is kis szolgáltatók és nem létező ügyfelektől kapják ezeket a spameket16.

A spam-küldők többszázezer üzenetet tudnak küldeni, mindegyik személyre szabott tartalommal és feladói címmel, majd gyorsan kilépnek17. A Spamhaus szerint az összes Észak-amerikai és európai internet-használók által kapott spamek 90%-a

14 Brightmail's Prove Network (2003), „The State of Spam – Impact & Solutions", Brightmail Incorporated, July, www.brightmail.com/press/state of spam.pdf.

15 www.spamhaus.org/sbl/sbl-rationale.html

16 www.spamhaus.org/sbl/sbl-rationale.html

17 Melissa Solomon: „Spam Wars" Computerworld Inc. 2002. november 11. http://computerwordl.com/softwaretopics/software/groupware/story/0.10801.75737.00.html

mindössze egy 180 főnyi csoporttól érkezett, amelyek közül szinte az összes szerepel a ROKSO adatbázisában.

Egy spam-küldő a következő módokon tudja beszerezni az email-címeket:

- Ügyfelektől, akik saját maguk adják meg az email-címüket a spammer-eknek.
- Harmadik felektől, akik beszerezték az email-címeket közvetlenül a magánszemélyektől, és ezeket eladják a spam-küldőknek.
- Publikus helyekről, amelyekből a spam-küldők beszerzik a címeket egy spamwaren keresztül.
- Harmadik féltől, aki spamware-t használ, hogy beszerezze a személyes email-címeket a publikus helyekről és ezeket eladják a spammereknek.

Ezek a források közül a 3. és a 4. a leggyakrabban alkalmazott módszer[18]. Csak az első esetben tudja fogadó azt, hogy spam céljából használják az email-címét. Ahhoz, hogy beszerezzék az email-címeket, a spammer eszközök automatikusan szörföznek a neten. (például: Usenet, a chat-szobák. URL-listák…) Az email-címeket összegyűjtik, majd újra szétküldik különböző listákra, melyeket azért kreálnak, hogy megkerüljék az internet-szolgáltatók által üzemetetett szűrőket.

Létezik más technika az email címlisták beszerzésére. Az egyik egy automatikus véletlenszerű email-cím generátor bizonyos domain címen belül egy programmal véletlenszerű címeket generál betűk kombinálásával. Ennél elegánsabb megoldás a szótári támadás, ahol alfabetikus permutációkat kombinálnak előképzőkkel és családneveket és keresztneveket, vagy rövidítéseket épít be a lehetséges címekbe. A nagyobb internet-szolgáltatók, amelyek nagy email forgalmat bonyolítanak le szervereikkel, nagyon érzékenyek az ilyen szótári támadásokra, hiszen a spamek ebben az esetben nem könnyen felismerhetőek, elvegyülnek a normális forgalomban. Alkalmazott módszer, mikor egy email-szerverrel kiépített kapcsolaton keresztül automatikusan több millió véletlenszerű email-t adnak fel és a sikeres címeket rögzítik egy adatbázisban. Ezeket az email-címeket automatikusan hozzáadják a spam-küldők címlistájához[19]. A spammerek legfőképpen internet-szolgáltatókat és email-szolgáltatókat céloznak meg, de megcélozhatnak cégeket is. A támadás célja ugyan nem a szerverek illetve a személyi számítógépek szolgáltatásainak korlátozása, mégis a támadás hatását tekintve hasonló, mint a „denial of service” (DoS) támadás, ahol a legitimált internet szolgáltatások használata leblokkolódik a nagytömegű illegitim forgalom miatt.

A vezeték nélküli technológia megjelenésével és a harmadik generációs hálózatok fejlődésével, valamint a mobil útján terjedő kéretlen üzenetek megnövekedett használata miatt, egyre nagyobb az igény antispam védelemre. Ahogy a mobiltelefonok és más mobileszközök elterjedésével, egyre több felhasználónak kerül elérhető közelségbe az internet, ezzel együtt válnak a spam-küldők céltáblájává. A szöveges üzenetek eljövetele sebezhetővé tette a mobiltelefonokat a szótár típusú támadásokra, ahol a spammerek telefonszámokat használnak. Ráadásul, ahogy a vezeték nélküli eszközök még inkább multifunkcionálissá válnak, a spam-ek által hordozott vírusok

18„E-mail Address Harvesting: How Spammers Reap What You Sow”, FTC in USA, 2002. november . www.ftc.gov/bcp/conline/pubs/alerts/spamalrt.htm

19„spammers grab MSN Hotmail addresses”, Spamhouse 2003. január 5. www.spamhaus.org/news.lasso?-database=sbl_news&-layout=detail&-response=newsstory.lass&-recordID=13&-search

terjedése elleni védelem, egyre sürgetőbbé válik. Az sms-küldés napról napra nagyobb népszerűségnek örvend. Néhány tipikus sms-spam módszer:

- Sms üzenet egy szolgáltatásra hívja fel a figyelmet, mely egy szám felhívásával érhető el., Ez a szám egy emelt díjas szám, és rendszerint nem kapcsolódik valódi szolgáltatás.
- Sms üzenet szólítja fel az üzenet fogadóját egy emelt díjas szám hívására,
- Sms-spam által egy harmadik fél reklámozza a termékeit és szolgáltatásait egy másik cég ügyfeleinek.

Nem meglepő, hogy a spam egyre népszerűtlenebbé válik az internet használók körében. Az alábbiakban összefoglalásra kerül néhány ok ami miatt a spam ennyire problematikussá vált.

A spam pénzbe kerül az összes internet-felhasználónak. Ezek a költségek növekednek a spam üzenetek növekvő számával. A spam-küldők felhasználják az ügyfelek és a szolgáltatások forrásait, és a hálózatot és számítástechnikai forrásokat, az email-adminisztrátor és az ügyfélszolgálati személyzet idejét kompenzáció vagy beleegyezés nélkül és csökkenti a dolgozók termelékenységét. Nehéz megbecsülni a spam globális költségét, de egy Európai Uniós vizsgálat szerint a globálisan az internet felhasználóknak 10 milliárd eurójába kerül évente20 a spam-tevékenység által okozott kár. A fogyasztók időt pocsékolnak azzal, hogy kitöröljék az ismétlődő, kéretlen, kereskedelmi üzeneteket. Habár a cégek költségei eltérnek a használt módszer függvényében, ezeket meg lehet becsülni, különböző vizsgálatokkal. A Brightmail szerint egy 10 000 fős cég éves spam-költsége körülbelül 675 000 USD21. A Ferris Research becsélése szerint a nem kívánatos kereskedelmi email 8,9 milliárd dollárjukba került az USA-beli cégeknek, 2002-ben. A becslés szerint ez az összeg 10 dollár/fő/hónap22.

A cégek spam költségei az alábbiakból származhatnak.

- A spam-el foglalkozó alkalmazottak termelékenységi visszaesése.
- A plusz költség adódik a hálózat és a számítástechnikai források használatával.
- A humánerőforrásba kerül és pénzügyi teher a technikai eszközök alkalmazása a spam ellen.
- A biztonsági kockázat a spam támadás miatt, mint például a szótári támadások és az email-vírus és férgek miatt.
- A potenciális jogi felelősség.

Az alkalmazotti termelékenység csökkenése szempontjából a költség az idő, amit az alkalmazott azzal tölt, hogy rendszeresen megnézi az email-jét és kitörölje a kéretlen hirdetéseket minden nap. Az Australian National Office23 becslése szerint, az erre fordított idő ára a munkahelyeken átlagosan AUD 960 (kb. USD 620) alkalmazot-

20 Commission of the European Communities, Unsolicited Commercial Communications and Data Protection, Summary of study Findings – 2001 Január, Serge Gauthronet, Etienne Drouard

21 „The state of spam – impact & solutions" Brightmail, 7. oldal, 2003. január, wwwbrightmail.com/press-vpk.html

22 Brian Morrissey: „Spam Cost Corporate America $9B in 2002" Jupitermedia Corporation, 2003. január 7. http://cyberalas.Internet.com/big_picture/applications/article/0,,1301_1565721,00,html

23 „The spam problem and how it can be countered – an interim report by NOIE" 11. oldal The National Office for the Information Economy, 2002. augusztus 1. Ausztrália

tanként évente. Ez nem foglalja magában a hálózati és kapcsolati költségeket és a működésbeli leállásokat a spam-áradat miatt. A hálózatbeli és számítástechnikai források, amelyeket a spam ügyletek miatt használnak, elég magasak. A spam szükségessé teszi, hogy szűrjék a forrásokat, amely lelassíthatja egy cég hálózatait, mert megnöveli a forgalmat és kedvezőtlenül befolyásolja a cég informatikai infrastruktúrájának kihasználtságát. A spam igényli az email-adminisztrátorok és helpdesk idejét és további költségeket jelent az antispam technológiák és a szűrőrendszerek alkalmazása. A nagyobb spam-támadások, mint például a szótári támadás, leállíthatják egy cég hálózatát. Az email-ben hordozott vírusok és férgek szintén komoly veszélyt jelentenek a hálózat számára. Néhányan jogi felelősséget is emlegetnek abban az esetben, amikor a cég nem tudja megvédeni az alkalmazottait a durva anyagoktól, a munkahelyen (pl.: pornó)24.A spam szintén költséget okoz, a legitim email-hirdetőknek. Amint a felhasználók egyre frusztráltabbá válnak a spam-üzenetek miatt és egyre több szűrőt használnak, úgy a legitim hirdetők üzeneteit szintén letörölhetik a spamel együtt. Ennek eredményeként a legitim email-hirdetők elveszíthetik az ügyfeleiket.

Az internet-szolgáltató és az email-szolgáltatók szintén költségeket szenvednek el, hasonlóan a cégekhez. Ezek a hálózati sávszélességek, adattárolás, alkalmazottak ideje, telefonos elérhetőség, az email-áradat kezelésével kapcsolatos költségek, szűrési technológiákba való befektetés és jogi eljárások költségei, melyeket spamküldők ellen indítanak a bíróságokon. Ezen felül az internet-szolgáltatóknak jelentős infrastruktúra bővítési költségei is jelentkeznek a spamek által felhasznált erőforrások kiesésének pótlása miatt. Az internet-szolgáltatóknak és az email-szolgáltatóknak személyi forrásuk is kell legyen, hogy foglalkozzanak a spamekkel technikai szinten és válaszoljanak az ügyfelek panaszaira. Az internet-szolgáltatók által használt spamszűrők hibásan a nem spam üzeneteket is blokkolhatják, mely kényelmetlenséget okoz az ügyfeleknek, akik e miatt szolgáltatót válthatnak. Összességében véve a ráfordított idő és pénz, amelyet erre költenek az internet-szolgáltatók és az email-szolgáltatók, sokkal nagyobb, mint más cégek költségei. Egyes felmérések szerint az internetszolgáltatók az internet-elérhetőségük rezsijének 10%-át fizetik spamre, amelyet belefoglalnak az ügyfél felé kiszámlázott havi előfizetési díjakba25.

Spammelés gyakorlata és különösen az email címek eladása számos kérdést vet fel a magánszféra védelmével az OECD Guidelines on the Protection of Privacy and Transborder Lows of Personal Data (Privacy Guidelines)-val kapcsolatban. Az egyik probléma, a spammel kapcsolatban, hogy magánéletbeli behatolások történhetnek általa. Például a web tűzfal és/vagy spamware programok elhelyezésével a személyi számítógépeken.

A csalásnak és megtévesztésnek számos formája van. A spammerek elfedik az üzenetük eredetét, mivel:

- Tudják, hogy az üzenetük blokkolt vagy szűrt,
- Rá akarják venni az embereket, hogy nyissák meg az üzeneteiket.

24 „The state of spam – impact & solutions" Brightmail, 2003. január 7. oldal wwwbrightmail.com/press-vpk.html

25Rnadolph H. Court és Robert D. Atkinson: „How to Can Spam" 1999. november 1. www.ppionline.org/indol/print.cfm?contentid=1349

Egy jellemző trükk, amit a spammerek használnak, hogy meghamisítják a fejlécet. A spam-küldők gyakran használják az egyéb mail-szerverek átjáróit26. Ezek a problémák magukba foglalják a címzett és a válaszcímek hamisságát, megtévesztő témát (subject) jelölnek meg, és hamis letörlési módokat alkalmaznak. Gyakran a spamek megtévesztő szövegeket tartalmaznak a szövegrészben. Az egyik fajta a „gazdagodj meg gyorsan" típus, mint például a „Nigériai csalás", ahol a küldő meg akarja osztani a millióit az üzenet fogadójával, de előleget kér. Az NSA (National Security Agency) ezt a fajta spamet járványszerűnek ítéli, és azt állítja, hogy több százmillió dollár évente a veszteség27. Néhány spam üzenet piramis játékot mozdít elő vagy rizikó nélküli befektetéseket kínál. Egyéb fajta félrevezető spamek csodadiétákat és egészségügyi terméket hirdetnek, hitelkártya vagy hiteljavítási ajánlatokat, vonzó utazási csomagokat és/vagy üzleti lehetőségeket. Léteznek illegális spam-üzenetek, amelyek prostitúciót, illegális szerencsejátékot, drogot, fegyvereket stb.-t tartalmaznak, illetve népszerűsítenek.

A spam átmenetileg megbéníthatja vagy eldugaszolhatja a számítógépes rendszereket. A nagy terjedelmű spamek interferálhatnak fontos számítógépes infrastruktúrákkal és veszélyeztetik a biztonságot az Interneten. A spamet szintén rosszindulatúan felhasználhatják Denial of Service (DoS) támadásként.

Egy spam tartalmazhat destruktív vírusokat és férgeket. A vírusírók tipikusan olyan programokat írnak, amely letölti a felhasználó címlistáját, és vírusokat küldenek a telefonkönyvben szereplő minden címre. Ezáltal a vírusírók kikerülik a szkennereket és szűrőket, amelyek megállítanák a rossz szándékú programokat. Egyes becslések szerint a vírusok 90%-át email-en keresztül terjesztik, fokozva a bizalmatlanságot az email-el szemben.

A vírusokon és férgeken kívül olyan fájlok, mint például a tűzfalak és spyware, letölthetőek az email-üzenet tartalmaként. A spammerek szintén kihasználják a biztonsági gyengeségeket, amelyeket az email átviteli technikák nyújtanak.

A spam-küldők és a rosszindulatú kódok írói közti összefüggés erősödni tűnik. A spam-küldők vírusírási technológiákat használnak, hogy keresztülvigyék üzeneteiket a szűrökön. A vírusírók szintén hasznát vették a spam-küldők tömeglevelezési technikáinak, hogy megtámadjanak számítástechnikai rendszereket. Vírusokat használva a spam-küldők visszaélhetnek a használók címjegyzékeivel, hogy nagy mennyiségű spam-üzeneteket küldjenek.

Egy másik biztonsági kérdés a spam használatával kapcsolatosan mikor a gyanútlan felhasználónak kémprogramokat töltenek le rejtett módon. A Spyware figyelemmel kíséri a használó internetes tevékenységét és elküldi ezt az információt valaki másnak. Szintén információkat gyűjthet email címekről, jelszavakról és hitelkártyaszámokról.

### Személyiséglopás

Egyre jellemzőbbé válik a személyiséglopás, amely fenyegetést jelent az internet használatra és az e-kereskedelemre, mert leépíti a felhasználó bizalmát. Minden

26 Serge Gauthronet és Etienne Drouard: „Unsolicited Commercial and Data protection" 98. oldal. Commission of the European Communities, 2001. január. http://europa.eu.int/comm/internal_market/en/dataprot/studies/spamstudyen.pdf

27 www.secretservice.gov/alert419.shtml

email tartalmaz információt az eredetére vonatkozóan, de a jelenlegi technológia nem garantálja, hogy a fejlécben való információ hitelességét. Ha a spam-küldő felfedezi, hogy az összes email-e egy bizonyos cégtől keresztülmehet a szűrökön, mivel a cég a „fehér listán" van, akkor a spam-küldők úgy tettetik, hogy mintha arról a címről küldenék az email-eiket. A spammerek általában más cégek IP címeit használják, hogy eltakarják az saját személyiségüket, ellopott vagy hamisan címkézett céges identitásokkal28. Mások, megváltoztatják a fejlécet, meghamisítván a feladót, vagy kreálnak egy nyitott átjárót, nem bebiztosított szervereket használva.

A céges személyiséglopás világszerte megkárosíthatja a cégek image-t. Azok a cégek, amelyek már ilyen támadás áldozataivá váltak, komoly erőforrásokat fordítanak elvesztett arculatuk visszaállítására. Sőt az internet-szolgáltatók feketelistái gyakran tartalmazzák az identitáslopás áldozatainak domain neveit. Következésképpen ezeknek a feketelistáknak az előfizetői nem tudnak többé email-eket kapni, ezektől a legitim cégektől. Napjainkban a domain nevek fontos szerepet játszanak egy cég arculatában.

Személyek ugyan úgy, mint a cégek, szintén a személyiséglopás áldozataivá válhatnak. Sok spammer küldi az üzenetét más címéről engedély nélkül, mivel a spam törvénybe ütközik, vagy az ISP által tiltott tevékenység. Azok az internet-szolgáltatók, akik egy szabványkód szerint működnek, lezárhatják azokat a címeket, amelyeket spam küldésére használnak.

### Csökkenő felhasználói bizalom

Az internet-szolgáltatók és a végfelhasználók által elszenvedett költségeken túl a spam fő problémája, hogy bizalmatlanságot kelt az internet-használók körében, a digitális gazdaságban, amely az e-kereskedelem fejlődésére negatív hatással van.

Több évig az OECD azon munkálkodott, hogy építse a felhasználói on-line bizalmat. 1999-ben az OECD tagországok elfogadták a Guidelines on Consumer Protection in the Context of Electronic Commerce-t. Felismervén a tisztességes üzlet és marketinggyakorlatok fontosságát, ez az útmutatás tartalmaz bizonyos előírásokat a spammel kapcsolatosan előírja, hogy:

Minden kereskedőnek ki kell alakítaniuk egy hatékony és könnyen használható eljárást, mely lehetővé teszi a fogyasztók számára, hogy eldöntsék, hogy kívánják-e vagy sem, a kéretlen kereskedelmi email üzeneteket.

Amikor a fogyasztók azt jelzik, hogy nem akarnak kéretlen kereskedelmi üzenetet kapni, akkor ezt a választásukat tiszteletben kell tartani29.

### Jogi megközelítések

Két eltérő jogi és szabályozási megközelítési mód van világszerte a spam-al kapcsolatosan.

Az egyik esetben a jelenlegi törvényeket és szabályokat, (melyek nem spam-specifikusak), alkalmaznak a spam üzenetek esetében.

A második esetben a meglévő törvényeket és szabályozásokat a alakítják át, illetve új szabályozást alakítanak ki, konkrétan a spam problémával kapcsolatban.

---

28 „Federal, State, and Local Law Enforces tackle Deceptive Spam and Internet Scams, Federal Trade Commission" 2002. november 13. www.ftc.gov/opa/2002/11/netforce.htm

29 www.oecd.org/dataoecd/5/34/1824782.pdf

### Szabályozási megközelítés fajtái

A következő összefoglaló a fő elemekről áttekintést nyújt az olyan OECD tagországokban, ahol a második megközelítést értelmében konkrét szabályozásokat alkottak.

Az opt-in megközelítés tiltja a kéretlen üzenetek küldését, hacsak egy korábbi kapcsolat nem létezett a fogadóval vagy a fogadó kifejezetten nem engedélyezte.

Az opt-out megközelítés a következők egyikét feltételezi:

- Nyílt opt-out nyelvezetet kell az üzenetnek tartalmaznia, vagy letörlési kérést kell megjeleníteni (specifikus opt-out).
- „Spam nélküli lista" felállítása esetén a direkt marketingesek ellenőrizhetik azon ügyfelek listáját, akik nem kérnek kéretlen emaileket (általános opt-out).
- A feladónak egyértelműen beazonosíthatónak kell lennie (például név, zöld szám, elérhetőség, érvényes, a küldő által működtetett email-cím, postai cím vagy utcai cím), mely lehetővé teszi a könnyű opt-out-ot.
- A fogadó kérésével összhangban azonnal meg kell szüntetni irányában a spam-tevékenységet.

Az internet szolgáltatóknak joguk van, hogy megtagadják a spam-küldőktől a szolgáltatást. Az interaktív szolgáltatóknak lehetővé kell tenni, hogy blokkolhassák a kereskedelmi elektronikus fiókokat egy meghatározott módon.

A következő tiltásokat foglalhatja magában:

- Hamis küldő vagy identitás használata
- Hamis fejléc, félrevezető információ a tartalom sorban esetleg egy opt-out kérés figyelmen kívül hagyása, technikai manipulációval
- Engedély nélküli vagy meghamisított router információ, a kiindulási információ meghamisítása
- Harmadik fél az Internet tartományának engedély nélküli használata

A címkézés azt jelenti, hogy egységes címkét teszünk a téma (subject) sorba, vagy a fejlécen, mint például „ADV" (hirdetés) vagy felnőtt (csak felnőttek részére, 18 év felettieknek szánt tartalommal)

Az olyan személyes információ eladása, cserélése vagy lízingelése, amelyet a felhasználó kifejezett egyetértése és tudata nélkül szereztek, betilthatóak.

### Egyéb szabályok a spam-el kapcsolatosan

Jó néhány országnak hasonló gyakorlata van a feladóknak a valódi személyazonosságával, az opt-out lehetőségével az üzenetekben, illetve a fejlécben levő hamis információval kapcsolatban.

A legtöbb ország nem írja elő a „Spam mentes" listákat, mégis opt-out listákat működtetnek bizonyos ipartevékenységi normák alapján.

Megfigyelhető tendencia, hogy a spam-törvények megsértésével kapcsolatosan egyre keményebbé válnak a szankciók. Néhány ország, így például Korea szigorította szabályozását, így jelentősen megnőttek a spammerekre kiróható pénzbüntetések összege. Más országok, mint például Olaszország, nem csak pénzbüntetéseket helyeztek kilátásba, hanem börtönbüntetés kiszabását is lehetővé tették.

A panaszok hatékonyabb kezelése érdekében, néhány ország, mint például Belgium, Franciaország és az Egyesült Államok,30 felállítottak email-címeket, amelyre a felhasználók továbbíthatják a spameket. Ezek a hatóságok jogi lépéseket tudnak tenni, ugyanakkor a statisztikákkal tudnak szolgálni felhasználóknak a spam természetéről.

### Spam esetek jogi kihívásai: a törvénykezés korlátai

A spam-ellenes törvényeknek számos korlátja van:

- Nem költségkímélők,
- Nehéz lenyomozni a spamek eredetét,
- Nehéz a határokon túlról bizonyítékokat beszerezni,
- A szabályozás országonként eltérő.
- A magánszférát védő törvények nehezíthetik hatóságoknak munkáját spammerekkel kapcsolatos információk beszerzésében.

A törvénykezésnek kulcsszerepe van a spam megállításában. Viszont egyedül a jog eszközeivel nem lehetséges megoldani ezt a problémát. Számos szabályozás, mint például a címkézés (néhány állam törvénye megköveteli), nem bizonyult hatékonynak, hiszen a spam-küldőknek csak a 2%-a tartotta be31. Néhány szervezet, ilyen például a Direct Marketing Association (DMA) megítélése szerint, csak a legitim, jogkövető reklámozók fogják betartani a rendelkezéseket. Mások megkérdőjelezik azt Az ePrivacy jelentése szerint (2003. júliusában), az opt-out lehetőségével mindössze 37% élt32.

A spam világméretű probléma, a rendbontók megtalálása komoly problémát jelent, nehéz a nyomozás végrehajtása és az illetékes bíróságok a kijelölése ilyen esetekben. Az eltérő nemzeti szabályozások és az Internet globális természete miatt a hatékony fellépés igen nehéz. A szabályozások mindig adott földrajzi határok között érvényesek és ezzel szemben az Internet természetéből fakadóan nem rendelkezik fizikai határokkal.

Számos nemzetközi kezdeményezés célozta meg a nemzetközi csalások korlátozását.

### Az OECD országok által elfogadott szabályok összefoglalója

2003 júniusában az OECD új előírásokat fogadott el a nemzetközi kooperáció elősegítése érdekében a határokon átnyúló csalások vonatkozásában (OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders). A spam üzenetek, amelyeknek félrevezető a tartalmuk, ennek a kooperációnak a hatálya alá esnek.15 tagországnak van konkrét törvénye vagy rendelete a spamről. Kanada, Csehország és Mexikó a már meglévő törvényeket és szabályaikat alkalmazzák, míg 5 tagország konkrét antispam törvények elfogadását vállalta el 2003-ban. Néhány országnak, mint például Írországnak, Új-Zélandnak és

30 Az FTC kéri a használókat, hogy továbbítsák a spam üzeneteiket (uce@ftc.gov) és létesített egy spam adatbázist a nyomozók részére. A felhasználók naponta körülbelül 105 000 emailt továbbítanak, 2002. májusától.

31 „False Claims ins Spain", Division on Marketing Practises of FTC, 2003 áprlis 30.

32 „2003 Consumer Spam Study" ePrivacy Group, 2003 julius, www.eprivacygroup.net/spamstudy

Törökországnak még nincs spam szabályozása. A következő rész összefoglalja az OECD országok által alkotott szabályokat.

### Ázsiai és Pacifikus OECD országok

Az Ázsia-Pacifikus térség hét országa közül Ausztrália volt az első az opt-in szabályozás bevezetésében. 2003. áprilisában „Final Report of the NOIE Rewiew of the Spam Problem and How It Can Be Countered" javasolt egy opt-in szabályozást és ezt követően az Ausztrál Parlament 2003. december 2.-án elfogadta a Spam Törvény 2003-at.

Kanadában és Mexikóban nincs konkrét szabályozás, habár egy opt-in jellegű korlátozás működik a meglévő törvények közvetítésével.

Koreában és Japánban opt-out szabályozás van. Viszont 2003. október 19.-én az Információs és Kommunikációs Minisztérium (MIC) Koreában bejelentette, hogy bevezeti az opt-in szabályt a mobilszolgáltatásokkal vonatkozásában.

Végül Új-Zélandnak és az Egyesült Államoknak szövetségi szinten nincs szabályozása a spamről. Viszont az FTC monitorozza a spammereket, így ellenőrizve az elektronikus kereskedelmet. 33 állam bevezetett törvényeket a spamről 2003. júliusában. Ezek: Tiltják a feladó eredetének, az útvonal-információnak meghamisítását, harmadik fél email címének annak engedélye nélküli használatát, illetve, a téma rovatban félrevezető információ szerepeltetését. Néhány állam tiltja olyan szoftverek elosztását, eladását, melynek funkciója az üzenet eredetének meghamisítása. Kötelezővé tesznek bizonyos információk szerepeltetését az üzenetben. Előírják a címkézést a téma mezőben, melyeknek jelölnie kell, hogy hirdetést tartalmaz (ADV) vagy pedig olyan anyagot amelyet csak felnőtt nézhet meg vagy birtokolhat (AVD vagy ADULT)33.

Finnország, Franciaország és az Egyesült Királyság nem kötelezi az opt-in-t, amikor a fogadó egy regisztrált jogi személy.

Ausztrália kivételt tesz a kormányszervekkel, a politikai pártokkal, vallási szervezetekkel, jótékonysági szervezetekkel és oktatási intézményekkel, Rájuk nem vonatkozik az opt-in szabályozás.

### Európai OECD országok

A 2004-ben csatlakozott tagországoknak át kell venniük az EU-direktívákat.

Svájcban 2002 októberi nyilvános ülést követően a kormány jelenleg is dolgozik a szabályozás kidolgozásán, mely várhatóan minden spam esetében opt-in szabály lesz. Ugyanakkor kötelezik a telekommunikációs szolgáltatókat, hogy tegyenek meg mindent a spamek felszámolása érdekében.

Nincs szabályozás Törökországban.

### EU tagországok

Az EU elfogadott egy opt-in szabályozást a kereskedelmi email-kommunikációról (beleértve az sms-t) a 2002. július 12.-i 2002/58/EC Direktíva a személyes adatok kezeléséről és a magánszféra védelméről az elektronikus szektorban (Directive and Electronic Communications), amely szerves része egy új, szélesebb EC

33„State Laws relating to Unsolicited Commercial or Bulk E-mail (SPAM)", National Conference of State Legislatures, www.ncsl.org/programs/lis/legislation/spamlaws02.htm

szabályozásnak az elektronikus kommunikációról. Mindezidáig az opt-in a faxokra és az automatahívásokra terjedt ki.

A direktívának három fő eleme van a kéretlen kereskedelmi kommunikációval kapcsolatban. Először is a 13 (1) cikkely szerint, a tagországok kötelesek megtiltani a kéretlen elektronikus üzenetek küldését, kivéve ha az illető előzetesen beleegyezett (opt-in rendszer). Ez a szabály érvényes a magánszemélyek felé történő marketingben (természetes személyek), de a tagországok kiterjeszthetik ezt a cégek felé történő marketingre is. Létezik egy kivétel az opt-in rendszerre, már meglévő ügyfelek esetében [13(2) cikkely], amely személyes adatokat egy értékesítés keretében szereztek, de ezt csak ugyanazon a jogi személy felé használhatják hasonló termékek vagy szolgáltatások nyújtására, ugyanakkor egy egyértelmű opt-out felajánlásával az adatbeszerzés időpontjában és minden egyes üzenettel. A feladó személyazonosságának eltakarása tiltott. A direkt marketing üzeneteknek tartalmazniuk kell egy válasz címet, ahol opt-out lehetőség van („ingyenesen és könnyű módon").

Az elektronikus levelezés széleskörűen értelmezett és az elektronikus kommunikáció bármely formáját magába foglalja, amikor a feladó és a fogadó között nem szükséges az egyidejű részvétel. Ez a definíció technológiailag neutrális és nemcsak az email-t, hanem az SMS-t, MMS-t, stb. is magában foglalja.

A Direktíva szerint a tagországoknak be kellett építeniük a nemzeti szinten új szabályokat, 2003. október 31.-ig a nemzeti törvénykezésekben. Az Európai Bizottság szankcionálási eljárásokat indított számos tagállam ellen, akik ezt elmulasztották megtenni.

A Direktíva konkretizálja és kiegészíti az általános Data Protection Directive-et 95/46/EC. A fentieken túl egyéb Európai Bizottsági előírások vonatkozhatnak a kéretlen kommunikációra, mint például a félrevezető hirdetés begyűjtés és hacking34.

2. Táblázat EU tagok35

| Ország | Kéretlen email-ek |
|---|---|
| Ausztria | Opt-in |
| Belgium | Opt-in |
| Dánia | Módosított Opt-in |
| Finnország | Opt-in |
| Franciaország | nincs |
| Németország | Opt-in |
| Görögország | Opt-in a kéretlen emailekre és hirdetési célokra |
| Írország | Döntés alatt |
| Olaszország | Opt-in |
| Luxemburg | Opt-in törvénytervezet (document parlamtaire 5181) |
| Hollandia | Opt-out |
| Portugália | Opt-out |
| Spanyolország | Opt-in |
| Svédország | Opt-in |
| Egyesült Királyság | Opt-in |

34 2003/31/EC of 8 June 2000 on electric commerce

35 OECD Secretariat and European Comission, „Ninth Report on the Implementation of the Telecommunications Regulatory Package" 19/11/2003, 2/29 p,http://europa.eu.int/information_society/topics/ecomm/doc/all_about/implementation_enforcement/annualreports/9threport/annex2181103.pdf

Megjegyzés: Dánia egy opt-in modellt (Danish Marketing Pracitices Act) alkalmaz, mely előírja, hogy az üzenet fogadója fejezze ki a kérését mielőtt az üzenet megérkezik. 2003. július 25.-től egy új kiegészítés lehetővé teszi a kéretlen emaileket anélkül, hogy a fogadó aktívan kérje ezt, amennyiben számos feltétel teljesül. Az új törvény csak az emailekre vonatkozik.

### Önszabályozó megközelítések

Számos önszabályozási erőfeszítést tettek a spam megállítása érdekében. Néhány a privát szektorban lévő kezdeményezést megemlítünk, beleértve néhány antispam szervezeteket, internet szolgáltatókat, email szolgáltatókat, internet-ipart és emailben reklámozó cégeket, fogyasztóvédelmi szervezeteket és végfelhasználókat.

### Az antispam és az internet-felhasználók szervezeteinek kezdeményezései

Sok antispam szervezet egy listát nyújt, vagy egy linket tartalmaz más antispam-szervezetekhez a weboldalaikon. Ezek a szervezetek információkat, forrásokat, statisztikákat és törvényi útmutatást szolgáltatnak a spamel kapcsolatosan és javaslatokat, hogy hogyan lehet beazonosítani és lecsökkenteni a spamet. A Spamhaus36, technikai eszközöket nyújt, hogy blokkolják a spamet és lenyomozzák a spam-küldőket, úgy, mint egy feketelistát a jól ismert spam-küldőkről. A Coalition Against Unsolicited Commercial E-mail (CAUSE), aktív résztvevői a törvényi vitáknak. A SpamCon Foundation Law Center és a SpamLaws.com, információkat nyújt a meglévő spam-törvényekről és a jogi lehetőségekről a spam-küldőkkel szemben. Vannak szervezetek, melyek panaszközpontokat üzemeltetnek, ahol fogadják a megkereséseket, elemzik és továbbítják a spamet a megfelelő hatóságoknak, további nyomozásra.

Az internetfelhasználói szervezetek szintén küzdenek a spam ellen. A Spanish Internet Users Association egy antispam weboldalt működtet (http://aui.es/contraelspam). Ez a weblap tartalmazza a kezdeményezéseiket a spam elleni küzdelemben, beleértve a spamnek a lenyomozását, információs kampányok, koordinációs központok, eszközök kifejlesztése, amely segít a felhasználóknak elemezni és szűrni a spamet.

### Internet szolgáltatói, email szolgáltatói és Internet-ágazati kezdeményezések

Mint a spamnek a legfőbb áldozatai, az internet szolgáltatók és az email szolgáltatók. Ezen szervezetek többsége preventív, technikai, büntető eszközt vetettek be a spamek ellen, és felhasználók által generált feketelistákat alkottak, hogy megállítsák a spam-áradatot. Valamint megpróbálják elejét venni a forrásaiknak és a sávszélességük a megcsapolásának, és segítik a felhasználók erőfeszítéseit, hogy visszaszorítsák a spameket. A szűrőeszközök használata felveti azt a kérdést, hogy az egyes internet szolgáltatók döntései, miszerint leblokkolnak bizonyos üzeneteket, mennyire legitim. A szűrők nem működnek, amikor a feladó email-címe blokkolt esetleg hamisított. Ugyanakkor az internet szolgáltatók fenntartják a jogot, hogy lezárjanak egy email-címet, ahonnan szabálytalan email-tevékenység történt. Az egyik USA-beli internet

36 A Spamhouse (//spamhause.org)

szolgáltató belevette a szerződésébe, hogy az előfizető 50 dolláros büntetést fizet egy-egy spam-üzenet elküldésekor37.

A Canadian Association of Internet Providers (CAIP) kifejlesztett egy önkéntes szabályt: Az internet szolgáltatók versenyeznek az előfizetőkért, tehát szabadon választhatják meg a belső szabályzataikat és azok alkalmazását az előfizetői szerződésekben. A CAIP szerint a legtöbb internet szolgáltató tag, már tiltja a tömeges elektronikus levelezést, valamint fenntartja a szerződés megszüntetésének jogát, azokkal az ügyfeleikkel szemben, akik ilyen gyakorlatot folytatnak Néhány szervezet különböző technológiák beültetésével, például a küldőfél-azonosítás (CLI) is előmozdítják a személyazonosítást az előre fizetett csomagok esetében.

A spam-küldők általában az elérhető költséghatékonyság miatt látnak okot a spamek alkalmazására. Néhány email szolgáltató gazdasági úton próbálta ezt a problémát megközelíteni. Megpróbáltak anyagi kompenzációt felszámítani a veszteségeikért. Például a Daum, egy koreai email szolgáltató, felállította a „online stamp system"-t 2002 áprilisától, hogy lecsökkentse a használóknak küldött spam-eket. Bevezették, hogy az email küldőknek fizetni kell a spam elküldésért, valamint javasolták, hogy a tömeges kereskedelmi email-küldőknek kell a hálózati infrastrukturális költségeket viselnie.

Az Internet ágazat oktatási, felvilágosítási kampányokat tartott, a felhasználóknak spamről, illetve a spammel szembeni védekezéssel kapcsolatos kérdésekről. Az Internet Industry Association Ausztráliában elindított egy programot, 11 antispam program eladóval közösen, akik vállalták, hogy egy hónapos ingyen használatot nyújtanak a termékeikre, az összes ausztráliai internet-használó számára, 2000. április 16.-án38. Az ausztrál telekommunikációs ágazat kifejlesztett egy gyakorlati normát az SMS spamre, 2002.-ben. A publikus szolgáltatások, mint például a GetNetWise39, amelyet Internet cégek működtetnek, segítik az embereket spam elleni küzdelmükben, hasznos megoldási javaslatok nyújtásával.

A spam-küldők elleni perek száma növekedőben van. Az utóbbi időben több cég is beperelte a spam-küldőket a polgári bíróságokon a veszteségeikért. A Microsoft Corp. 2003 júniusában 15 pert indított az Egyesült Államokban és Nagy-Britanniában olyan cégek ellen, melyek több mint 2 milliárd spam üzenetet küldtek a szoftveróriás ügyfeleinek, amelyek közül sokan az ingyenes Hotmail szolgáltatást használták. Az EarthLink 5 millió dolláros pert indított 100 állítólagos spammer ellen.

### Email (online vagy direct) marketing cégkezdeményezések

Az opt-out listák elterjedése. Az előfizető nem kíván spam üzeneteket fogadni, önmagában egy értékes információ, hiszen így lecsökkenthetők a terméketlen reklámozási költségek és a negatív visszajelzések, panaszok. Néhány európai országban az opt-out listákat egy országos direkt marketing szövetség állítja össze, ilyen például a Federation Direct Marketing (FEDMA) vagy az on-line ipart képviselő újabb szervezetek. A Fédération des Enterprises de Vente á Distance (Direct Marketing Federation – FEVAD) amely 1998-ban Franciaországban alakult és aktívan részt vett ilyen jellegű

37 „Internet and Bulk Unsolicited Electronic Mail (SPAM) Policy", Indutry Canada 1999. július, http://e-com.ic.gc.ca/english/stat/spam.html#Consumer

38 www.iia.net.au/nospam

39 http://spam.getnetwise.org

listák összeállításában 1999 nyara óta. Ez egy lehetséges minta az egyéb országos opt-out listák számára. Aláírásra került egy együttműködést a German Direct Marketing Federation-nal ezzel kapcsolatban. Az Association Belge du Marketing Direct (ABMD) is felállított egy országos, általános opt-out listát.

A Direct Marketing Association (DMA) az Egyesült Államokban bevezetett fogyasztói önszabályozó sémát (opt-out séma), melyet a szövetség működtet. A felhasználók regisztrálhatják magukat, hogyha nem akarnak spamet kapni az e-Mail Preference Service (e-MPS)-re, amelyet a DMA működtet. Akik küldeni akarnak kéretlen leveleket, azoknak az ide feliratkozott személyeket le kell törölniük a listájukról40. Mobiltelefon-számokat szintén regisztrálni lehet ingyenesen az UK Telephone Preference Service-n41.

Opt-in (engedélyhez vagy beleegyezéshez kötött) direct marketing. Egyre több email és direkt marketing cég vette át az engedély alapú marketinget és opt-in email-t. Például 2000. októberében a Finn Direct Marketing Szövetség egy etikai normát dolgozott ki, mely szükségessé teszi az opt-in megközelítést. Az emailcím-gyűjtemény modellje, hogy opt-in formanyomtatványokat kell a webre feltenni. A látogatók ezeket az online kérdőíveket kitöltik arra, hogy kapják a hírlevelet, versenyben vegyenek részt, vagy reklámokat kapjanak, akciókban vegyenek részt, ajánlatokat kapjanak azzal kapcsolatban, ami az érdeklődési körük. Nagyon sok weblap két választási lehetőséget ad a látogatóknak: akarnak-e kereskedelmi üzeneteket kapni, az adataikat átadhatják–e harmadik félnek.

Az opt-in direkt marketing gyakorlat különösen a legitim reklámozók körében növekszik a tagországokban. Ausztráliában és EU- tagországokban is, ahol folyamatban van ennek az átvétele, a direkt marketingszervezetek felállítottak útmutatásokat. Ilyen a DMA-nak az Útmutatása a Kereskedelmi Hirdetésekről, mely a kereskedelmi emailekre vonatkozik42. Egy olyan szervezet, mint a Canadian Marketing Association (CMA) szabályokat és útmutatást állított fel a tagjai számára, az akciós anyagok interneten való szétosztásának módjáról. A Network Advertising Initiative (NAI), amely a hálózati reklámozók egy kooperatív csoportja és Association Interactive Marketing (AIM), amely non-profit kereskedelmi szervezet, kialakított egy magánszférával kapcsolatos alapelvkészletet43. Tanácsot adnak a cégeknek és fogyasztóknak, hogy hogyan lehet lecsökkenteni a spam mennyiségét.

### Önszabályozási módszer korlátoltsága

Az önszabályozási módszerek fontos lépést jelentenek a spam prevencióban, mégis számos korlátjuk van:

- Kevés spammer tagja egy internet-szervezetnek, illetve hajlandó elfogadni szabályait.
- Egy etikai kódex nem nyújt valódi védelmet a rosszindulatú spammerekkel szemben.

40 http://preference.the-dma.org/products/empssubsription.shtml

41 www.tpsonline.org.uk

42„Direct Marketing Association's Online Marketing Guidelines and Do the Right Thing Commentary" 2002. január, www.the-dma.org/guidelines/onlineduidelines.shtml#2

43 www.networkadvertising.org

- A spammerek könnyen megtalálják a módját, hogy elkerüljék a különböző rendszereket és a büntető szabályozásokat.

### Oktatás és felvilágosítás

A felhasználók oktatása és felvilágosítása fontos szerepet játszik a spamek megfékezésében. A felvilágosítás nem csak elővigyázatossá tesz számos spam áldozatot, hanem meg is emeli az email-címgyűjtés költségeit, ezáltal csökkenti a spam költséghatékonyságát. Az oktatás szintén túlmegy a földrajzi határokon, akár maga a spam is, szemben a törvényhozás fölrajzi értelemben vett korlátozottságával. Sok fogyasztóvédelmi szervezet nyújt oktatási és felvilágosító programokat, hogy megerősítsék a fogyasztókat tudatos választásaikban.

Sok fogyasztóvédelmi szervezet tájékoztatja a felhasználókat a spammelési taktikákról és tanácsokat ad nekik, hogy hogyan védekezhetnek ellene. A Center of Democracy and Technology (CDT) egy jelentésében a kéretlen levelek megakadályozásának legsikeresebb módszereit teszi közzé. A jelentés felhívja a figyelmet, hogy az Internet bizonyos területei nem tekinthetők biztonságosnak. Egyéb szervezetek kezdeményezéseket tettek, hogy a weben keresztül segítsék az embereket technikailag a spam kivédésében. Egy érdekes kezdeményezés az „ellenőrzött jel" nevű eszköz kifejlesztése, ami egy „Bizalmas Küldő" üzenet, melynek célja, hogy azonosítsa a küldőt, az üzenet integritását, stb.

Sok kormány a részvénytulajdonosokat ösztönzi arra, hogy önkéntesen kialakítsanak kódexeket és gyakorlatokat. Az Ausztrál Kincstár kialakította az "Australian E-commerce Best Practice Model"-t az összes on-line cégnek, amely előírásokat tartalmaz az internetes direkt marketinggel kapcsolatban44.

Az US FTC működtet egy weboldalt, a spam felvilágosítással kapcsolatban, amely információkat nyújt a használóknak, hogyan reagáljanak a spamre. A Francia Adatvédelmi Hatóság a weboldalán számos információt ad a spam legkülönbözőbb aspektusairól. Az Európai Bizottságnak szintén van egy koncepciója, hogyan szolgáltasson információt az EUROPA weboldalán, beleértve a tagországai szabályozásait, utalásokkal a nemzeti honlapokra, valamint számokat és közeljövőbeli trendeket az EU-spammal kapcsolatban. Az Európai Bizottság létrehozta a Safer Internet Action Plan-t, hogy koordinációt és felvilágosító programokat biztosítson a tagországokban a biztonságos Internet-használatért.

### Technikai megoldások

Amint a spam terjedelme egyre növekedik és a piacra lépési költségek egyre alacsonyabbak, az antispam termékek száma is növekedett. Sok szolgáltatás létezik egyedi használóknak, a legtöbb piacon található új szolgáltatás célcsoportjai: a szolgáltatást nyújtók és szervezetek. A nem kívánatos emailek blokkolására és szűrésére használatos technikai eszközök közül, néhányat megemlítünk.

### Jelenlegi email struktúra

Az egyik fő ok, amiért a spam annyira elterjedt, hogy az SMTP (Simple Mail Transfer Protocol), amelyet a különböző szerverek közti üzenetküldésre használnak (vagy a levelezőklienstől a szerverig), nem ellenőrzi a feladó azonosságát (küldő szer-

44 www.ecommerce.treasury.gov

ver és a feladócímet). Az SMTP-vel és mind a két azonosító meghamisítható. Nincs olyan mechanizmus, amely a levél tartalmának integritását ellenőrizheti. Az emailnek a tartalma, beleértve a téma és az egyéb információk, egy adatblokként továbbításra kerül és nem alkot integráns részt az SMTP kommunikációban45. A tartalom kihagyása magas hatékonysághoz vezet (nagy számú globális email forgalom bonyolítható le) ebben az esetben, de nincs semmi ellenőrzés. Ez felveti a bizalom és a felelősségre vonhatóság kérdését. A felelősségre vonhatóság nélkül a spam virágzik.

Az antispam technikák védik és segítik a cégeket, internet szolgáltatókat, az egyéni használókat, hogy lecsökkentsék az idejüket, amit a spam-üzenetek olvasásával és kezelésével töltenek azáltal, hogy kiszűrik a nem oda való és offenzív tartalmat. Az egyik megoldás a feketelistás szűrők használata, amely a spam-küldők ismert tartomány-neveit és Internet Protokoll (IP-címeket) számukat tartalmazza. A fekete listákat kollektív módon szerzik. Miután elegendő használó kifogásol egy bizonyos üzenetet, az üzenet átkerül a jövőbeni felhasználók spam-mappáiba. Egy másik technikai lehetőség a „fehér lista" vagy a „jóváhagyott küldők listája", amely lehetővé teszi a használóknak, hogy azonosítsák a jóváhagyott és legitim email-címek küldőit. A fehér listák segíthetik kifinomítani a spam-szűrést, mégis ki vannak téve az email-eredet meghamisításának. Jó módszer, az email kliens beállítása, hogy csak digitális hitelesítési hatóság által hitelesített aláírással ellátott üzeneteket fogadjon egy. A digitális aláírási sémák használhatók erre a célra.

Léteznek antispam technikák, melyek olyan viselkedési elemző eszközök, amelyek bizonyos mintákat keresnek. A címellenőrző eszközök azt vizsgálják a tartomány név vizsgálatokkal, hogy a feladó nem próbálja-e eltakarni a személyazonosságát. A digitális ujjlenyomatok, melyeket algoritmusokkal és heuretikákkal alakítanak ki, szintén használatosak a közismert spam minták beazonosítására, leblokkolására és szűrésére.

Az új termékek is megjelentek a piacon amelyek a grafikákat vizsgálják, mint például a bőrszínek, hogy felvegyék a harcot a pornográfia ellen, de ezek az eszközök még gyerekcipőben járnak46. Egy másik technika a Bayes szűrő, azt tanulja és újra tanulja, hogy hogyan szúrja ki a spameket azzal, hogy szkenneli a levelezők által visszautasított üzeneteket és elemzi, hogy milyen közös vonások vannak bennük. Minden új levélnél felhasználva az azt megelőzőkből származó tapasztalatokat dönti el, hogy melyik levelet kézbesítse és melyiket utasítsa vissza. Ez egy életképes megoldás lehet, mert csak a fogadó tudhatja, hogy milyen dolgok érdeklik őt. A pontosságát 99%-ra becsülik. Egy másik új technológia, amely azt a taktikát használja, hogy megköveteli a feladótól, hogy megerősítse a személyazonosságát, mielőtt felkerülne egy fehér listára, amely lehetővé teszi a későbbiekben, hogy korlátlanul küldjön emaileket.

A legtöbb antispam technika különböző kombinációkat tartalmaz, ilyenek a heuretika alapú szkennelés, fehér és fekete listák, tartalmi elemző eszközök és más biztonsági jellemzők, például az SMTP alapú hitelesítés és konfigurálható hálózati alapú frissítéseket tartalmazó, heuretikus kereső modul. Az új szűrők lehetővé teszik, hogy képben legyünk a spammerekről. Ahhoz, hogy beazonosítsunk egy spamet, az antispam eszközök nem csak összehasonlítják az email címeket az ismert spamek

45 „Trsted E-mail Open Standard" 2. és 3. o. ePrivacy Group White Paper, 2003 május

46 Melissa Solomon: „Spam Wars" Computerwordl Inc. 2002.11.11. http://computerwordl.com/softwaretopics/software/gruopware/story/0,10801,75737,00html

listájával, hanem a teljes email tartalmát analizálják közös hirdetési és pornografikus szövegmintákat keresvén. Az antispam programok szintén használnak egy „ködös logika" szűrőt, a használó által megvizsgált minden egyes email-szövegben. Ezen kívül az antispam programokat automatikusan frissítik, mivel a spam technikák gyorsan fejlődnek.

### Technikai szakértői csoportok erőfeszítései

Mind az egyéni cégek, mind a cégek kollektívan együttműködve tesznek erőfeszítést, hogy technikai megoldásokat találjanak a spam-prevencióra, illetve csökkentésére. Ahogy a spam egy fő kérdésé válik, egyre több technológiai cég próbálkozik megoldásokkal, hogy harcoljon a spam ellen. 2003. február 27.-én egy antispam konferencia volt, hogy koordináljanak egy ágazatot felölelő erőfeszítést a problémával kapcsolatban. A konferencián a résztvevők – akik különböző üzleti és technológiai szektorokból jöttek – nagy érdeklődést mutattak a spam iránt, és egy átfogóbb probléma megközelítést vetettek fontolóra. A projekt szerint a technikai ágazat együtt dolgozzon ki egy nyitott, interoperációkra képes antispam protokolt, amely a különböző eredetű email rendszerek között is képes működni, megállítja spameket és egyúttal garantálja a legitim üzenet biztonságos továbbítását 47.

Számos fő technológiai cég, beleértve a Yahoo, Dell Computer, Microsoft és a Sun Microsystem találkoztak 2003. március 14.-én San Franciscóban, hogy megoldást keressenek a spam-re. A JamSpam nevű fórum célja volt, hogy létrehozzon egy nyitott interoperációra képes antispam meghatározást. Amely egy univerzális megoldásként szolgálna a spamre. A találkozón szó esett az email hitelesítési szabványok kialakításáról, amely biztosítaná, hogy a legitim üzenetek felismerhetőek és biztonságosan postázódnak. Az internet szolgáltatók és email szolgáltatók speciális találkozóján a különböző cégek technikai megoldásokat vitattak meg, a nyitott átjátszók bezárására. A cégeket szintén érdekelte egy olyan rendszer kiépítése, ahol átlátszóbb lenne a legitim üzenetek küldése, például az üzenet jellegének a tisztázása. Legyen az email, hírlevél, e-kereskedelmi számla vagy egy baráti levél.

2003 áprilisában a Microsoft, az AOL és a Yahoo bejelentették, hogy együtt dolgoznak a kéretlen levelek leblokkolásán és a spam-küldők megakadályozásában, hogy hamis email-címeket használjanak. Ezen kívül néhány internet szolgáltató szintén összegyűlt, hogy technikai megoldásokat találjanak a spamre. Például Lengyelország legnagyobb Internet portáljai és email szolgáltatói, az Onet, a Wirtualna Polska és az Interia – koalíciót alkotott 2003. májusában, hogy megpróbálják megállítani a rendszerükön keresztül menő spameket. A három cég egy közös akciótervet alkotott, hogy új technológiát alkosson, mely korlátozná az egyéneket és a cégeket a spamküldésben.

Az antispam technológiák vitatása folytatódik. Egy befolyásos Internet szabvány megállapító testület részletes vizsgálatba kezdett, az email spamek növekvő problémáiról, amelynek kihatásai lehetnek az email jövőbeli használatára és a biztonságra. Egy hivatalos antispam kutató csoport48 összejött az Internet Research Task Force égisze alatt, amely szervezet az Internet Engineering Task Force-val (IETF) van

47 David Berlind: „First industry-wide antispam conference shows promise", Oaxaca Lendig Library, 2003 február 27. www.oaxlib.org/v-37.html

48 www.irtf.org/charters/asrg.html

kapcsolatban. Az új csoport egy nyitott kutató testületszabályozási jogosítványok nélkül, viszont a kutatási eredményeik megváltoztathatják az internet szolgáltatók és hálózatok email-kezelési módját. 2003. szeptember 16.-án 40 internet szolgáltató, spam-szűrő és email-küldő cég ügyvezetője és döntéshozója gyűlt össze a San Francisco-i Email Küldhetőségi Csúcstalálkozón, hogy megvitassák a hamis pozitívokat, a legitim email küldhetőségi mutatójának javítását, valamint, hogy képessé tegyék a rendszereket a spam felismerésére. Bemutattak néhány szabványt a kézbesíthetetlen email-kezelésről, leiratkozási kérelmekről, email engedély feltételek publikálásáról és a küldő és fogadó cégek közti kommunikációról49.

### Technikai megoldások korlátai

A spam-blokkoló technológiák többsége jelenleg kulcsszavak vagy feketelista alapján működnek, mely nagyszámú hamis pozitívhoz vezet. A hamis pozitív akkor van, amikor egy legitim emailt spam-ként címkéznek és kiszűrnek. Mindig megvan a lehetősége, hogy az összes üzenetet, amely egy feketelistás lapról ered, szisztematikusan letörlik, kézbesítés nélkül. Ezen kívül az antispam feketelisták gyakran blokkolnak ártatlan internet-használókat, akik blokkolt internet szolgáltatókon keresztül kapcsolódnak. Voltak esetek, amikor egy egész ország domain-neveit blokkolták. Bár néhány felhasználó megerősítve érezte magát ezen szűrők által, sok internet szolgáltató szerint ártatlan embereket tettek áldozattá, beleértve azokat az internet szolgáltatókat, amelyek tudatuk nélkül spam-eket hostoltak, valamint internet-használókat, akiket a spammerek becsaptak, valamint az állítólagos spammerekkel szomszédos email-címeket.

Hogy harcoljanak a probléma ellen, az antispam cégek különböző módszereket ajánlanak, például a heurisztikus szabályon alapuló scanninget és a ködös logikájú szűrőket. Viszont pusztán automata módszerrel nagyon nehéz megállapítani hogy egy üzenet spam-e. A computer algoritmusok amelyek a spameket azonosítják, közel sem tökéletesek. Ráadásul a viszonylag új technológiák, mint például a feladat – reagálás technológiák nagy terhet jelentenek a legitim küldők számára. Sok előfizető listatulajdonosa, mint például a hírlevél küldők (automata reagálás szisztéma) számára nehéz a feladat – reagálás emailek személyes megválaszolása, ezért sok előfizető azt tapasztalhatja, hogy a hírlevelük kézbesítése leállt. Ez a hamis pozitívok egy kategóriája.

A spam-szűrés egy másik megközelítése a konszenzus modell, ahol azok az emberek, akik olyan üzeneteket kapnak amelyet spamnek tekintenek, bejelentik ezt egy koordináló egységnek. Egy komputer programot használnak az összes bejövő levelet koordinálják. Egy helyesen összeállított lista az ismert spammerekről, szintén lényeges javulást jelenthet, a jelenleg használatos szabályozatlan feketelistákban. Ennek ellenére egy tökéletes szűrőrendszert lehetetlen megcsinálni.

A spammerek technikailag eléggé kifinomultak ahhoz, hogy eltakarják nyomaikat, hogy megkerüljék a szűrőket és becsapják az egyéb technológiai sorompókat. Elektronikusan vezényelhetik a védetlen számítógépeket, amelyeket aztán a saját spamelésük eszközévé tesznek. Addig ameddig a spam költségei alacsonyak, a spammereknek nyomós érdekük van, hogy módot találjanak arra, hogy legyőzzék a technológiai korlátokat.

49 http://isipp.com/news.html és http://internetnews.com/IAR/article.php/3-78481

Az antispam termékek kikerülhetetlenül pluszköltséget és lappangási időt jelentenek az internet szolgáltatóknak, email szolgáltatóknak és felhasználóknak. Egy hatékony email-szűrő rendszer jelentős többletköltséget jelenthet a szolgáltatónak és gyakran a kommunikáció hatékonyságának rovására megy. Az üzenetek szűrése az internet szolgáltatóknak időbe és pénzbe kerül, valamint lassítja a hálózat teljesítményét. Néhány internet szolgáltató szerint a szűrőtermékek kifizetődőek, legalábbis felhasználói szinten, de az internet szolgáltató szintjén nem könnyű megtervezni, konfigurálni és installálni.

Az email és az egyéb elektronikus üzenetek globális elterjedése és alacsony ára egy nagyon népszerű és fontos kommunikációs médiummá tette ezeket. A spam gyors növekedése veszélyezteti az elektronikus üzenetek kényelmességét és hatékonyságát, valamint aláássa a használói online bizalmat, általánosságban véve. A fentiekben ismertettem a spamek meghatározásának különböző kísérleteit, hiszen még a definíció terén is komoly eltérések tapasztalhatók a világ különböző részein. Felvázoltam egyes lényeges jellemzőit, elterjedésének okait, a gazdasági élet különböző szereplőinek okozott károkra vonatkozó becslések tükrében. Kitértem a spammelés során alkalmazott módszerek ismertetésére, és a spam-küldéshez szükséges email címek gyűjtési lehetőségeire. Összesítettem, és értékeltem a különböző statisztikák, és információs központok kiadványai alapján, a spamek által okozott kárt. Elemeztem az okozott kár összetevőit, melynek következtében adódik, hogy az általános elégedetlenség elrőrevetíti a szabályozás szükségességét. Összesítettem a világ különböző részein a spamek visszaszorítására tett szabályozási kezdeményezéseket. Az OECD országokban számos intézkedést és kezdeményezést tettek a nem régi spam-rohammal kapcsolatosan, hogy megerősítsék a felhasználók online bizalmát. Úgy tűnik azonban, hogy ezek a szabályozási, önszabályozási és technikai intézkedések nem voltak eléggé sikeresek abban, hogy megállítsák a spamek növekedését. Az újabb erőfeszítéseknek fel kell ismerniük, hogy valószínűleg egyetlen egyedüli megoldás sem lesz képes megállítani a spamet, hanem nemzetközi koordináció szükséges ehhez a problémához, amely nem ismer nemzeti határokat.

Minden spam-probléma megközelítésnek megvannak a maga korlátai. A jogi megközelítésnek szembe kell néznie azzal, hogy a spam-küldők hatékonyan el tudják takarni személyazonosságukat, és határokon keresztül tudnak működni. Az önszabályozási megközelítés esetében szükséges, hogy a spam-küldők saját akaratukból kooperáljanak és betartsák az ágazati működési kódexeket. A közvélemény felvilágosítása és oktatása szükséges ahhoz, hogy biztonságosabb számítástechnikai gyakorlatokat mozdítsunk elő. Ebben az értelemben az antispam stratégiákat össze lehetne kötni általánosabb e-biztonsági kampányokkal. A technikai oldalon a technikai eszközök kifejlesztésének és bevezetésének állandó támogatása szükséges, hogy biztosítsuk azt, hogy a spam ne kerülje el az internet szolgáltatók és mások szűrőit. Összességében véve egy komplex megközelítés nyújtja a spam lecsökkenésének legjobb kilátásait, amely kombinálja a szabályozást, önszabályozást, technikai megoldásokat és felhasználói felvilágosítást.

A spam nem csak egyetlen ország problémája, és nem csak az OECD tagországokra hat ki, hanem egy világméretű probléma. A fejlődő országokban az internethozzáférés és a használat növekedése a spam globális természetét még tovább tágítja.

Egyre világosabb, hogy a hazai erőfeszítéseket nemzetközi együttműködési stratégiákkal kell kiegészíteni, hogy válaszoljon a spamek által jelentett határ nélküli kihívásra.

## Antispam szervezetek honlapjai

[1] www.irtf.org/charters/asrg.html (Internet Research Task Force - Antispam Kutató Csoport)
[2] www.cauce.org/ (Campaign against Unsolicited Commercial Email)
[3] www.euro.cauce.org/ (Euro CAUCE)
[4] www.spamcon.org/
[5] www.mail-abuse.org/
[6] www.mail-abuse.org/swat/
[7] www.spam.abuse.net
[8] www.junkbusters.com/junke-mail.html
[9] www.spamrecycle.com/
[10] www.junke-mail.org/
[11] www.sputum.com/
[12] www.nanae.org/
[13] www.spamsites.org/
[14] www.spamhaus.org/
[15] www.fmp.cpm/spam_patrol/
[16] www.natsma.com/
[17] http://sims.net/massacre/
[18] www.gssnet.com/antispam/spam_index.htm
[19] www.stop-spam.org/
[20] www.caspam.org/
[21] www.ripe.net/ripe/wg/anti-spam/
[22] www.cauce.org/orgmember/org:list.shtml
[23] www.caube.org.au (CAUCE Australia)
[24] http://cauce.ca (CAUCE CANADA) ( korábban: http://cauce-canada.org/)
[25] http://india.cauce.org/ (CAUCE India)
[26] www.spambr.org/ (Brazil Spamharcosok)
[27] www.antispam.ru (Orosz antispam honlap)
[28] http://nospam.spb.ru (Orosz)
[29] www.aui.es/contraelspam/ (Spanyol Internet felhasználók Egyesülete)
[30] www.fabel.dk/ (Dán honlap)
[31] www.spam.org.tr/ (Török antispam honlap)
[32] www.antispam-argentina.8.net/ (Argentin antispam honlap)
[33] www.spamstop.net/ (Japán)
[34] www.cauce.nl/ (Holland)
[35] www.ihatespam.biz/ (koreai)
[36] www.iajapan.org/hotline/ (Japán)
[37] www.spamstop.net/ (Japán)
[38] www.nospamware.it/ (Olasz)
[39] www.uzice.net/yasi/ (Szerb-montenegrói antispam kezdeményezés)

## Irodalomjegyzék


[1] 2003 Consumer Spam Study" ePrivacy Group, 2003 julius, www.eprivacygroup.net/spamstudy
[2] 2003/31/EC of 8 June 2000 on electric commerce
[3] A Radicati Group: „Anti-spam Market Trends 2003-2007", 2003. december 8. www.radicati.com/cgi-local/brochure.pl?pub_id=202&subscr=&back_link=single_report

[4] Brian Morrissey: „Spam Cost Corporate America $9B in 2002” Jupitermedia Corporation, 2003. január 7. http://cyberalas.Internet.com/big_picture/applications/article/0,,1301_1565721,00,html
[5] Commission of the European Communities, Unsolicited Commercial Communications and Data Protection, Summary of study Findings – 2001 Január, Serge Gauthronet, Etienne Drouard
[6] Comission Nationale de l’Informatique et des Libertés: „Le publipostage électronique et la protection des données personnelles” Madame Cévile Alvergnat jelentése 1999. október 14.
[7] CyberAtlas 2003. március 14. szám „Population explosion”; http://cyberatlas.Internet.com/big_picture/geographics/article/0..5911_151151.00.html
[8] David Berlind: „First industry-wide antispam conference shows promise”, Oaxaca Lendig Library, 2003 február 27. www.oaxlib.org/v-37.html
[9] „Direct Marketing Association’s Online Marketing Guidelines and Do the Right Thing Commentary” 2002. január, www.the-dma.org/guidelines/onlineduidelines.shtml#2
[10] „E-mail Address Harvesting: How Spammers Reap What You Sow”, FTC in USA, 2002. november, www.ftc.gov/bcp/conline/pubs/alerts/spamalrt.htm
[11] „E-mail marketing: Consumer choices and business oppurtunities – Discussion paper”. Industry Canada 2003. Január; http://e-com.ic.gc.ca/english/strat/e-mail_marketing.html
[12] „False Claims ins Spain”, Division on Marketing Practises of FTC, 2003 áprlis 30.
[13] „Farkas György: A kéretlen reklámüzenetek (SPAM) fogalma, jellemzői, általa hordozott veszélyek; Kard és Toll, HM Oktatási és Tudományszervező Főosztály, Budapest, 2005. ISSN 1587-558X
[14] „Federal, State, and Local Law Enforces tackle Deceptive Spam and Internet Scams, Federal Trade Commission” 2002. november 13. www.ftc.gov/opa/2002/11/netforce.htm
[15] „Internet and Bulk Unsolicited Electronic Mail (SPAM) Policy”, Indutry Canada 1999. július, http://e-com.ic.gc.ca/english/stat/spam.html#Consumer
[16] „Internet indicators: Hosts, Users and Number of PCs”. International Telecommunication Union; www.itu.int/ITU-D/statistic/at_glance/Internet02.pdf
[17] John Markoff: „Start-up aims to end spam” 2003. március 24. www.nytimes.com/2003/03/24/technology/24PHIL.html
[18] Jonathan Krim: „Spam’s Cost To Business Escalates” Washingtoonpost, 2003. március 13. www.wasinghtonpost.com/wp-dyn/articles/A17754-2003Mar12.html?referrer=e-mail
[19] Melissa Solomon: „Spam Wars” Computerwordl Inc. 2002. november 11. http://computerwordl.com/softwaretopics/software/gruopware/story/0,10801,75737,00html
[20] OECD Communications Outlook 2003
[21] Robyn Greenspan és Brian Morrisey: „Spam Expected to Outnumber Non-Spam”, Jupitermedia Corporation, 2002. december 12. http://cyberatlas.internet.com/big_picture/applications/aricle/0,1323,1301_1555831,00.html
[22] Rnadolph H. Court és Robert D. Atkinson: „How to Can Spam” 1999. november 1. www.ppionline.org/indol/print.cfm?contentid=1349
[23] Serge Gauthronet és Etienne Drouard: „Unsolicited Commercial and Data protection” Commission of the European Communities, 2001. január, http://europa.eu.int/comm/internal_market/en/dataprot/studies/spamstudyen.pdf
[24] „Sobig may be working for spammers” pcwordl.com, 2003. augusztus 29. www.pcwordl.com/news/article/0,aid,112261,00.asp

[25] „Spammers grab MSN Hotmail addresses”, Spamhouse 2003. január 5. www.spamhaus.org/news.lasso?-database=sbl_news&-layout=detail&-response=newsstory.lass&-recordID=13&-search
[26] „State Laws relating to Unsolicited Commercial or Bulk E-mail (SPAM)”, National Conference of State Legislatures, www.ncsl.org/programs/lis/legislation/spamlaws02.htm
[27] Stefanie Olsen: „Net users want law to can spam” 2003. január 3. www.oaxlib.org/spamcost.html
[28] „The spam problem and how it can be countered – an interim report by NOIE” The National Office for the Information Economy, 2002. augusztus 1. Ausztrália
[29] „The state of spam – impact & solutions” Brightmail, 2003. január, wwwbrightmail.com/press-vpk.html
[30] „Trusted E-mail Open Standard”, ePrivacy Group White Paper, 2003 május
[31] „Unsolicited Commercial Communications and data Protection” http://europe.eu.int/comm/internal_market/en/dataprot/studies/spamstudyen.pdf
[32] „Unsolicited Commercial Communications and Data Proptection”, Commission of the European Communities, 2001. január; http://europa.eu.int/comm/internal_market/privacy/docs/studies/spamsum_en.pdf

**FEHÉR Gábor, KORN András, SZENTGYÖRGYI Attila, SZŰTS Péter Lóránt**

# BIZTONSÁGOS VEZETÉKNÉLKÜLI SZUPERHÁLÓZAT

feher.gabor@tmit.bme.hu, korn.andras@tmit.bme.hu, szgyi@alpha.tmit.bme.hu,
sp449@hszk.bme.hu
Budapesti Műszaki és Gazdaságtudományi Egyetem, Távközlési és Médiainformatikai Tanszék

A vezetéknélküli hálózatok újabb biztonsági kihívások elé állítják a hálózatüzemeltetőket: a vezetékes közeghez képest nehéz a hozzáférésvezérlés és a hitelesítés. Cikkünkben egy olyan architektúrát mutatunk be, amely meglevő megoldások integrációja és számos újítás segítségével kezelhetőbbé teszi ezeket a problémákat.

## Bevezetés

A magyar műszaki felsőoktatásban és nagy ipari/kereskedelmi parkokban egyre több hallgató, kutató, oktató és egyéb alkalmazott használ hordozható számítógépet vagy kéziszámítógépet (PDA – Personal Digital Assistant). Ezen eszközök hordozhatóságának előnyei azonban az elérhető vezetéknélküli hálózatok hiányában nem használhatók ki teljesen. A vezetéknélküli hálózatok üzemeltetői általában törekednek arra, hogy a hálózatukat csak a saját szervezetükhöz vagy szervezeti egységükhöz tartozó eszközökkel lehessen elérni. Az átjárás általában még az egymáshoz földrajzilag közel eső hálózatok esetében sem biztosított.

Ennek a problémának a megoldására született meg egy elosztott jellegű biztonságos szuperhálózat koncepciója, majd az Infopark Alapítvány és a Budapesti Műszaki és Gazdaságtudományi Egyetem Távközlési és Médiainformatikai Tanszéke támogatásával a prototípusa is.

A projekt célkitűzése volt, hogy létező, elterjedt megoldások és új kutatási-fejlesztési eredmények integrációja révén olyan szuperhálózat modelljét és prototípusát hozza létre, amelyben a különböző együttműködő szervezetek által üzemeltetett vezetéknélküli hálózatokat a szervezetek valamennyi alkalmazottja a lehető legnagyobb szabadsággal és biztonsággal használhassa. Ezzel kapcsolatban többek között meg kellett oldani a felhasználók hitelesítését, az adatforgalom titkosítását, a virtuális magánhálózatok integrációját, valamint a rendszer üzemeltetési feladatainak szervezethatárok mentén történő particionálását.

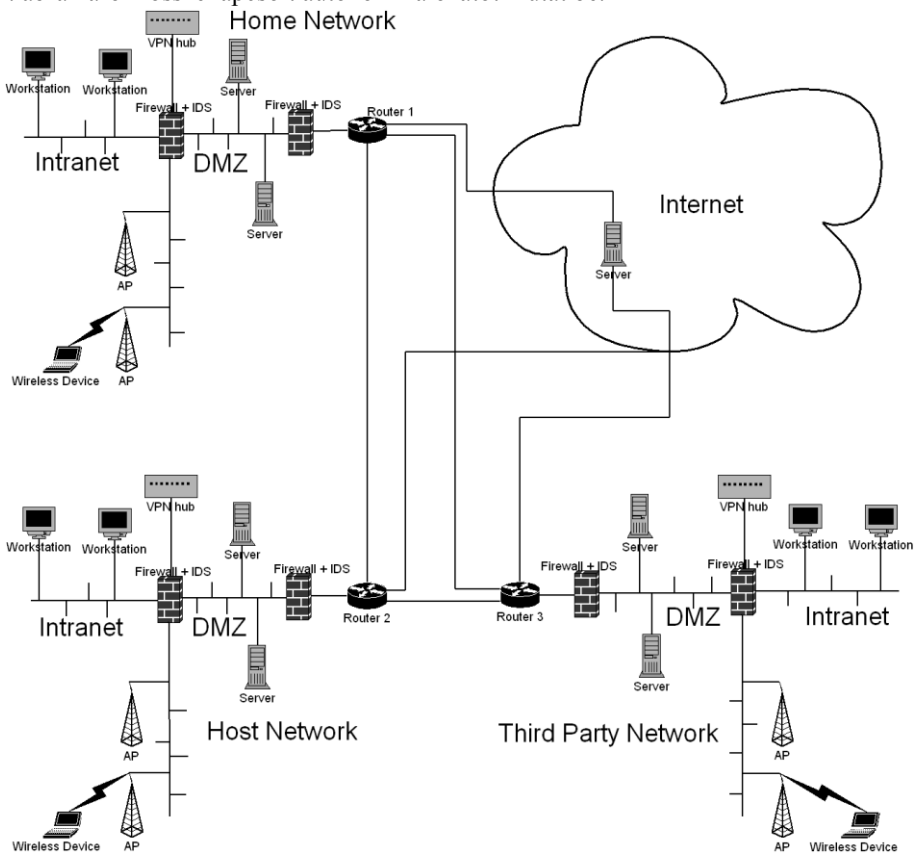
Célként szerepelt a kis teljesítményű vezetéknélküli kliensek támogatása is. Az egyre rohamosabban terjedő kéziszámítógépek processzorainak teljesítménye gyakran nem elegendő a megfelelő biztonságot nyújtó titkosító algoritmusok futtatásához, így olyan hálózatbiztonsági megoldásokat kellett találnunk, amelyek nem veszélyeztetik a PDA-kon futó alkalmazások használhatóságát.

A megalkotott rendszer ezeket a célkitűzéseket részben létező szabványokra, részben új megoldásokra támaszkodva valósítja meg.

## A szuperhálózat

A vezetéknélküli számítógépes hálózatok kialakításának egy újszerű módszere a különböző szervezetek, szervezeti egységek által üzemeltetett vezetéknélküli hálózatok biztonságos szuperhálózatba integrálása. Az így létrehozott szuperhálózat autonóm hálózatok összességéből áll, ahol az egyes autonóm rendszerek egy-egy szervezet, szervezeti egység tulajdonában és irányítása alatt vannak.

Az autonóm hálózatok általánosságban legalább három, egymástól tűzfalakkal elválasztott részre („zónára") bonthatók. Egy zónát alkotnak a vezetékes hálózaton lévő felhasználói számítógépek (intranet), egy másikat a vezetéknélküli hozzáférési pontok és a hozzájuk csatlakozó kliensek. Egy harmadikban, az ún. demilitarizált zónában (DMZ), a nyilvános szolgáltatásokat (is) nyújtó szerverek helyezkednek el. Természetesen ennél összetettebb, pl. több DMZ-t vagy több intranetet is tartalmazó hálózatok is elképzelhetők, ez azonban a továbbiak szempontjából nem lényeges. Az 1. ábra három összekapcsolt autonóm hálózatot mutat be.




1. ábra: A szuperhálózat felépítése

## A felhasználók hitelesítése

A rendszer alapkoncepciója, hogy a vezetéknélküli hálózathoz csak hitelesített felhasználó kapcsolódhat. A hitelesítés folyamata így felhasználható jogosultság-

kezelésre is (bár természetesen lehetőség van további korlátozásokra, lásd később). A rendszerben a felhasználók olyan nyilvános kulcsú titkosításra alkalmas tanúsítványok segítségével hitelesítik magukat; amelyeket a rendszerben résztvevő bármely szervezet vagy szervezeti egység kiállíthat. Ezt a megoldást nevezik nyilvános kulcsú infrastruktúrának (PKI, Public Key Infrastructure, nyilvános kulcsú infrastruktúra).

A szuperhálózatban alkalmazott PKI kétszintű. Egy globális hitelesítő központ (CA, Certification Authority) hitelesíti az együttműködő szervezetek CA-it, ezek pedig saját felhasználóik, szervereik és egyéb eszközeik tanúsítványait. A láncolt hitelesítés használata lehetővé teszi a jogosultságkezelés tetszőleges finomítását is; így megoldható például, hogy egy adott hozzáférési pont csak bizonyos CA-k által aláírt tanúsítványokat fogadjon el.

A tanúsítványok hitelesítése történhet a tanúsítványnak egy tanúsítványláncon keresztüli visszakeresésével vagy a hitelesítési kérés más, illetékesebb hitelesítő eszköznek történő továbbküldésével.

A személyhez kötött hitelesítésnek köszönhetően az esetleges rosszindulatú felhasználók elvileg felelősségre vonhatók; a gyakorlatban ennek természetesen jogi vonzatai is vannak, ezekkel azonban nem foglalkoztunk. A PKI mellett szól az is, hogy néhány egyéb elterjedt jogosultságkezelési megoldással (pl. MAC-szűrés) szemben a rendszer nem eszközöket, hanem személyeket hitelesít.

A PKI használatával a tanúsítványok visszavonására is nyílik lehetőség, így egy kompromittálódott tanúsítvánnyal való visszaélés is megelőzhetővé válik.

A vezetéknélküli kliensek hitelesítését szervezeti egységenként egy-egy RADIUS[14] (Remote Authentication Dial-In User Service) szerver végzi. A WiFi vezetéknélküli hálózatok 802.11i[13] biztonságról szóló szabványban leírtak szerint a kliens először a 802.1X hozzáférésvezérlő protokoll segítségével a vezetéknélküli hozzáférési ponthoz fordul, amely továbbítja a hitelesítési kérést a RADIUS felé. A szuperhálózatban az EAP-TLS[9] hitelesítő módszert írtuk elő, így a RADIUS tanúsítvánnyal hitelesíti magát a kliens felé, illetve tanúsítványok segítségével hitelesíti a klienst. Ha a kliens tanúsítványa rendben van, és a kliens is hitelesnek véli a RADIUS-t, akkor ezt a RADIUS jelzi a vezetéknélküli hozzáférési pontnak, amely ezt követően létrehoz egy titkos csatornát a kliens felé, majd engedélyezi az adatforgalmat a rejtjelezett csatornán.

A vezetéknélküli hozzáférési pont és a kliens között kiépített titkos csatornában az adatok rejtjelezésére a 802.11i a TKIP (Temporal Key Integrity Protocol) protokolljában előírt algoritmust használja. Ez lényeges, hiszen a TKIP-t a legtöbb ma kapható – korábban csak WEP-re tervezett – vezetéknélküli hálózati eszköz támogatja[17].

### Intelligens hozzáférési pontok

A szuperhálózatban intelligens vezetéknélküli hozzáférési pontok biztosítják a vezetéknélküli végberendezésekről csatlakozó felhasználók biztonságát. Olyan hozzáférési pontokat használtunk, amelyek alkalmasak voltak az OpenWRT[22] nevű Linux-alapú operációs rendszer futtatására; mivel a rendszer nyílt forráskódú, könnyű volt új funkciókkal bővíteni.

Az intelligens vezetéknélküli hozzáférési pontok a felhasználók hitelesítésében is részt vesznek. A hitelesítés során szükség van egy olyan szolgáltatásra, amely biztosítja a kapcsolatot a vezetéknélküli kliensek – amelyek hitelesítés hiányában még

nem küldhetnek csomagokat a hálózatba – és a hálózat RADIUS szervere közt. Ezt a feladatot a NAS (Network Access Server) látja el. Az intelligens hozzáférési ponton futó NAS és a megfelelő RADIUS hitelesítő szerver között létezik egy közös titok, amellyel hitelesítés során a kommunikációjukat rejtjelezik, így a hitelesítési üzenetek támadástól védetté válnak.

Az intelligens hozzáférési pontok feladata továbbá az ARP[20] (Address Resolution Protocol) körüli anomáliák detektálása, illetve megfelelő ellenintézkedések foganatosítása. Az ARP elvileg arra szolgál, hogy az egy fizikai hálózaton található, egymással IP-forgalmat lebonyolítani szándékozó állomások felderíthessék egymás adatkapcsolati rétegbeli azonosítóját (pl. fizikai Ethernet-címét). A protokoll két üzenettípussal dolgozik: a „who-has 1.2.3.4” üzenet az 1.2.3.4-es IP-című állomás fizikai címét kéri; erre az adott állomás (ritkábban egy másik, amely tudja a választ) „1.2.3.4 is-at aa:bb:cc:dd:ee:ff” jellegű üzenettel válaszol.

Sajnos az ARP számos visszaélésre ad lehetőséget: egy támadó megteheti például, hogy olyan ARP-válaszokat küld, amelyekben azt állítja, egy bizonyos IP-címmel ő rendelkezik. Ezután lesznek olyan állomások, amelyek az adott IP-címnek szóló csomagjaikat a támadó részére kézbesítik. Az ilyen és hasonló visszaélések ún. ARP-anomáliákkal (tehát a normálistól eltérő jellegű ARP-forgalommal) járnak. Ezek közül az anomáliák közül mi a következőket észleljük:

- multicast- vagy broadcast-címre vonatkozó kérés vagy válasz (normális esetben ARP-csomagok sem broadcast IP-, sem broadcast ethernet-címekre nem hivatkoznak)
- olyan IP címre vonatkozó kérdés vagy válasz jön, amely nem az adott alhálózaton van
- egy válaszcsomag a hozzáférési pont által vezetett IP-hardvercím táblázatban foglalt adatoknak ellentmondó párosítást fogalmaz meg
- válaszcsomag érkezik anélkül, hogy előtte kérdés hangzott volna el.

Anomália észlelése esetén a hozzáférési pont riasztást küld és opcionálisan olyan tűzfalszabályokat léptet életbe, amelyek a csomag feladójának forgalmát kiszűrik. Ezt a forgalomszűrést értelemszerűen csak akkor célszerű alkalmazni, ha a címhamisítást valahogyan kizártuk.

A hozzáférési pont nyomon követi a hitelesítés folyamatát, és annak sikeres befejezéséig az adott kliens által küldött adatcsomagok közül kizárólag a hitelesítéssel kapcsolatosakat továbbítja/fogadja el. A hitelesítés befejezése után kötelezően DHCP-vel (Dynamic Host Configuration Protocol) kapnak IP-címet a kliensek; a hozzáférési pont a DHCP-tranzakciót is nyomon követi, így fel tudja jegyezni, milyen IP-címet kapott az adott (imsert hadvercímmel rendelkező) kliens. Ha a későbbiekben olyan csomag érkezne, amely állítólag erről az IP-ről, de más hardvercímről – vagy fordítva – érkezett, a hozzáférési pont címhamisítási kísérlet miatt riasztást küld, és a hamis csomagot nem továbbítja[21].

A sikeres hitelesítésről és IP-címkiosztásról a szuperhálózat menedzsment-modulja üzenetben értesül, és saját adatbázisában tárolja, mikor melyik felhasználó melyik hozzáférési pontra milyen hardvercímű eszközzel jelentkezett be, és melyik IP-címet kapta. Így az üzemeltetők rendkívül egyszerűen ki tudják szűrni egy adott felhasználó hálózati forgalmát, ha a felhasználó viselkedése ezt szükségessé teszi.

Az általunk kifejlesztett RESPIRE[10][11] (Resource Efficient Synflood Protection for Internet Routers and End-systems) algoritmus segítségével a hozzáférési pont képes kölcsönösen megvédeni a vezetéknélküli eszközöket és a vezetékes hálózatot a másik szegmensből érkező esetleges ún. SYN-áradat ellen. A SYN-áradat egy klasszikusnak nevezhető internetes támadás, amely viszonylag alacsony költsége miatt ma is népszerű a támadók körében. A RESPIRE hatásos futtatásához a hozzáférési pontnak az alsó árkategóriában megszokottnál gyorsabb processzorral kell rendelkeznie; a rendelkezésünkre álló Linksys WRT54G hozzáférési pontok sajnos bármilyen elárasztásos támadás hatására a használhatatlanságig lelassultak, akár futott a RESPIRE, akár nem, így a védelem hatásosságát csak személyi számítógépeken tudtuk ellenőrizni, ott azonban kiválóan teljesített.

### Védekezés lehallgatás és adatmódosítás ellen

A szuperhálózatban a lehallgatás és adatmódosítás kivédése érdekében lehetőség nyílik az adatkommunikáció rejtjelezésére, illetve arra, hogy az idegen hálózatot használó kliensek saját hálózatukkal virtuális magánhálózatot alakítsanak ki. Az adatkapcsolati rétegben végrehajtott titkosítással kapcsolatban már említettük a TKIP protokollt, amelynek rejtjelező algoritmusa biztonságot nyújt a vezetéknélküli szakaszon.

Virtuális magánhálózatok (VPN-ek, Virtual Private Network) kialakításának segítségével megoldható, hogy a felhasználók elérhessék azokat a hálózati erőforrásokat, amelyek elvileg csak saját helyi hálózatukon érthetők el, akkor is, ha valójában az Internet (vagy a szuperhálózat) egy más fizikai részéhez kapcsolódtak. Szuperhálózatunkban kétféle VPN-megvalósítást támogatunk: az IPSec-et[18] és az OpenVPN-t[19].

Az IPsec az IP egyik kiegészítése, amely biztonságos adatátvitelt tesz lehetővé az IP-csomagok titkosításával. Az IPsec-kel lehetőség nyílik adatok átvitelére nyilvános hálózaton (pl.: Internet) megfigyelés, lehallgatás, változtatás veszélye nélkül, ezért alkalmazható kiválóan virtuális magánhálózatok kialakítására. Az IPsec a biztonsági szolgálatokat a felsőbb rétegeknek a hálózati réteg szintjén nyújtja, így egyrészt nincs szükség a kliensek és alkalmazásaik átkonfigurálására, másrészt képes bármilyen IP felett futó protokollt és az általa hordozott adatokat megvédeni a lehallgatás és a meghamisítás veszélyétől. Az IPSec előnye, hogy szabványos megoldás, így szinte minden platformra létezik implementációja. Képes tanúsítványokkal hitelesíteni a klienseket, vagyis a PKI-ba is jól integrálódik.

Az OpenVPN az IPSec-hez hasonlóan VPN alkalmazás, amely támogatja a távoli hozzáférést és a virtuális magánhálózatok kialakítását tanúsítványok segítségével. Az OpenVPN és az IPSec között számos különbség van; a legfontosabbak:

- Az OpenVPN TCP vagy UDP fölött valósít meg titkosított adatátvitelt, így tűzfalbarát. A kliens és a szerver közötti teljes kommunikáció ugyanazon az egy adatcsatornán valósul meg.
- Az OpenVPN segítségével virtuális Ethernet is kialakítható, így pl. akár IPX is szállítható vele IP fölött.
- Az OpenVPN képes a VPN-forgalom tömörítésére, így sok esetben jobb átviteli sebesség érhető el vele, mint IPSec-kel.
- Az OpenVPN-t nem szabványosították.

- Az OpenVPN kizárólag az IPSec alagút-üzemmódjához („tunnel mode”) hasonló kapcsolatokkal dolgozik, a transzport-üzemmódot („transport mode”) nem támogatja.

### Behatolás-érzékelés

A szuperhálózatban a hitelesítés és a titkosítás mellett a biztonság növelése érdekében elosztott rendszerű behatolásjelző rendszer[2] (IDS – Intrusion Detection System) is található, amely képes jelezni a hálózatot ért behatolásokat és szokatlan jelenségeket (anomáliákat), és ezekkel szemben intézkedéseket is képes foganatosítani.

A szuperhálózat IDS-e a Snort[1][7] szoftverre épül, amely a legelterjedtebbnek mondható nyílt forráskódú behatolásjelző. Ezt egészítettük ki olyan módon, hogy a riasztásokról multicast-üzenetekben tájékoztassa a szuperhálózat tűzfalait[4][5]; ezek a riasztás súlyosságától vagy gyakoriságától függően a riasztást kiváltó IP-címet ideiglenesen kitilthatják a hálózatból. Természetesen címhamisítás segítségével a rendszer kijátszható (tetszőleges IP-cím kitiltatható vele), így a tiltást csak akkor szabad alkalmazni, ha a címhamisítást kizártuk. A tiltás ellen szól a téves riasztás lehetősége is, így csak olyan támadások észlelése esetén célszerű ehhez az eszközhöz nyúlni, ahol a téves riasztás valószínűsége elhanyagolható.

Olyan algoritmust is kifejlesztettünk, amelynek a segítségével a hálózatban terjedni próbáló vírusok, férgek az általuk okozott forgalmi anomália alapján elosztott módon felismerhetők és forgalmuk kiszűrhető; ez az algoritmus egyelőre sajnos csak szimulátorban létezik. Alapgondolata az, hogy a hálózati vírusok általában valamilyen ismert szolgáltatás (pl. a Microsoft IIS) biztonsági hiányosságát kiaknázva terjednek, és a terjedés során számos különböző hálózatban található számítógép ugyanazon portjával próbálnak kommunikálni rövid időn belül. Ha nyomon követjük, hogy időegységenként hány különböző számítógéppel kezdeményeznek kapcsolatot a mi hálózatunkból bizonyos célportokra, és ez a statisztika ugrásszerűen megnő, akkor általában joggal gyanakodhatunk féregre (különösen, ha a kapcsolatfelépítési kísérletek jelentős része meghiusul).

### Menedzsment-modul

A rendszerben az egyes komponensek működését egy web-alapú menedzsment-felület hangolja össze, ahol az adminisztrátorok a hálózat állapotával kapcsolatos információkat láthatják, illetve a rosszindulatú felhasználókat a felületen keresztül központilag kitilthatják. A hitelesítőrendszer üzemeltetői a tanúsítványok felhasználását és állapotát követhetik; módjuk van a tanúsítványok visszavonására is. A felhasználók saját tanúsítványaikkal kapcsolatos, illetve általános jellegű információhoz juthatnak, valamint kérhetik saját tanúsítványuk visszavonását, amennyiben az kompromittálódott. Itt történik a komponensek által gyűjtött adatok rendszerezése és elemzése is. Természetesen a menedzsment-modul is tanúsítványuk alapján hitelesíti a felhasználókat.

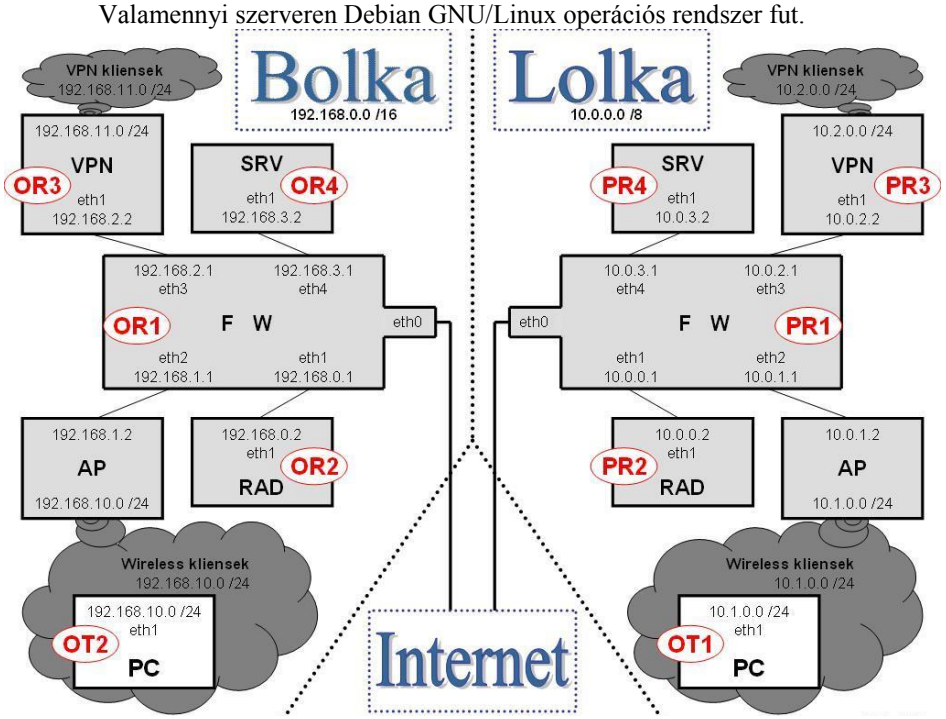
Mivel a szuperhálózatban többféle entitás létezik (vezetéknélküli hozzáférési pontok, behatolásjelző rendszerek, RADIUS, stb.), amelyek beállításait kényelmes lenne egy központi felületen keresztül kezelni, az eszközök a konfigurációjukat és aktuális státuszukat a menedzsment-modul számára elérhetővé teszik (a prototípusban ezeknek a funkcióknak csak a váza található meg).

Az eszközök és a menedzsment-modul kommunikációját a tanúsítvány-alapú hitelesítést nem támogató SNMP[3] helyett saját protokollal oldottuk meg. Esetünkben az eszközök a felhasználókhoz hasonlóan tanúsítványt kapnak, amivel hitelesíteni tudják magukat a menedzsment-modul felé; az adatátvitel a TLS[6] protokoll segítségével kialakított titkosított csatornán történik.

### A szuperhálózat megvalósítása

A szuperhálózat prototípusa a Budapesti Műszaki és Gazdaságtudományi Egyetem Távközlési és Médiainformatikai Tanszékének QoSIP számítógép-laboratóriumában készült el. A prototípus két – „Lolka” ill. „Bolka” névre hallgató – autonóm hálózatot tartalmaz, ahogy az a 2. ábrán látható. Az egyes hálózatok tartalmazzák az intelligens vezetéknélküli hozzáférési pontokat, az Internet felől érkező forgalmat szűrő tűzfalakat, a virtuális magánhálózatok létrehozásában szerepet játszó VPN szervereket, valamint a hitelesítést végző freeRADIUS[23] szervereket. Látható, hogy az egyszerűség kedvéért a DMZ mindkét hálózatban csak egy-egy szervert tartalmaz („SRV”), és hogy egyik hálózatban sincs vezetékes intranet.

Valamennyi szerveren Debian GNU/Linux operációs rendszer fut.




2. ábra: A megvalósított szuperhálózat

A hálózathoz csatlakozó vezetéknélküli kliensek skálája a szabványos megoldásoknak köszönhetően igen különböző lehet. A szuperhálózat képes minden olyan eszközzel együttműködni, amely támogatja a tanúsítványokat, az EAP-TLS hitelest és a 802.11i által felkínált TKIP titkosítási eljárást. Az elkészített mintahálózathoz a tesztek során csatlakoztattunk Linuxot és Windowst futtató, vezetéknélküli hozzáfé-

réssel rendelkező asztali és hordozható számítógépeket, valamint Windows Mobile 2003-at futtató PDA-t is.

A hálózatban lehetőség nyílik kipróbálni a felhasznált létező és az általunk fejlesztett új technológiák együttműködését. Demonstrálható a felhasználók hitelesítése a RADIUS szerver és az intelligens hozzáférési pontok segítségével. Megmutatható az intelligens hozzáférési pont által detektált ARP anomáliák szűrése és jelzése a menedzsment-felület felé, illetve az anomáliát okozó felhasználók kitiltása a rendszerből. Megtekinthető a menedzsment-felület, amint a riasztásokat és a felhasználók bejelentkezését fogadja. Bemutatható a behatolásérzékelő rendszer működése, amint támadást észlelve ellenlépésként üzenetet küldve a tűzfalnak, az blokkolja a támadó forgalmát. Szemléltethető, amint az egyik autonóm hálózatban tartózkodó kliens egy virtuális magánhálózati kapcsolatot létesít a másik autonóm hálózat VPN szerverével.

## Összegzés

A létrehozott szuperhálózattal egy olyan komplex, integrált biztonsági rendszert sikerült megalkotni, amely megfelel a jelen kor magas biztonsági követelményeinek, felhasználóbarát módon támogatja a legújabb technológiákat, leegyszerűsíti az adminisztrátori feladatokat és hatékony módon nyújt biztonságot a hálózati veszélyforrásokkal szemben.

Szeretnénk köszönetet mondani az Infopark Alapítványnak és a Budapesti Műszaki és Gazdaságtudományi Egyetem Távközlési és Média Informatikai Tanszékének, hogy támogatta a biztonságos vezetéknélküli szuperhálózat elméletének és minta megvalósításának kidolgozását, valamint köszönetet mondunk az összes hallgatónak, akik részt vettek a projektben, név szerint kiemelve: Bicskei Alen, Bódis Ákos, Csiszér Ákos, Furucz János, Gyimesi Judit, Kozák Kálmán, Mátyási Péter, Móczó Péter, Zsellér Tamás.

## Irodalomjegyzék

[1] Brian Caswell, Jay Beale, James C. Foster, Jeremy Faircloth, „Snort 2.0 Indtrusion Detection”, Syngress, 2003, ISBN 1931836744

[2] Stephen Northcutt, Judy Novak, „Network Intrusion Detection”, Que, 2002, ISBN: 0735712654

[3] Andrew S. Tanenbaum, „Számítógép hálózatok”, Panem Könyvkiadó Kft., Budapest, 1999, ISBN 9635452136

[4] D. Curry, Merrill Lynch, H. Debar, B. Feinstein, ”The Intrusion Detection Message Exchange Format”, IETF Internet-Draft, 2005, <http://www.ietf.org/internet-drafts/draft-ietf-idwg-idmef-xml-14.txt>

[5] B. Feinstein, G. Matthews, J. White, „The Intrusion Detection Exchange Protocol (IDXP)”, IETF Internet-Draft, 2002, http://www.ietf.org/internet-drafts/draft-ietf-idwg-beep-idxp-07.txt

[6] T. Dierks, C. Allen, „The TLS Protocol Version 1.0”, RFC 2246, 1999, http://www.ietf.org/rfc/rfc2246.txt

[7] Snort, Snort The Open Source Network Intrusion Detection System, http://www.snort.org

[8] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz, „Extensible Authentication Protocol (EAP)”, RFC 3748, 2004. június

[9] B. Aboba, D. Simon, „PPP EAP TLS Authentication Protocol”, RFC 2716, 1999. október

[10] Gábor Fehér, András Korn, „RESPIRE - a Novel Approach to Automatically Blocking SYN Flooding Attacks”, Proceedings of EUNICE 2004
[11] Gyimesi Judit, Korn András, Fehér Gábor: SYN-áradatok automatikus szűrése a RESPIRE algoritmussal, Híradástechnika 2004/9, pp.40-47
[12] G. Bruneau, „The History and Evolution of Intrusion Detection”, SANS Institute, 2001. október
[13] Jon Edney, William A. Arbaugh, „Real 802.11 Security: Wi-Fi Protected Access and 802.11i”, Addison-Wesley, 2003
[14] Jonathan Hassel, „RADIUS”, O'Reilly, 2002
[15] R. Housley, W. Ford, W. Polk, D. Solo, „Internet X.509 Public Key Infrastructure Certificate and CRL Profile”, RFC 2459, IETF proposed standard, 1998
[16] Maxim, Pollino, „Wireless Security”, McGraw-Hill/Osborne, 2002
[17] Wi-Fi Alliance, „Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks”, Whitepaper, 2003
[18] S. Kent, R. Atkinson, „Security Architecture for the Internet Protocol”, RFC 2401, IETF proposed standard, 1998
[19] OpenVPN hivatalos honlap, http://openvpn.net/, 2005
[20] Sean Whalen, „An Introduction to ARP Spoofing”, http://node99.org/projects/arpspoof/arpspoof.pdf
[21] Victor Velasco, „Introduction to IP Spoofing”, http://www.giac.org/practical/gsec/Victor_Velasco_GSEC.pdf
[22] OpenWRT dokumentáció, http://openwrt.org/OpenWrtDocs, 2005
[23] FreeRADIUS projekt honlapja, http://www.freeradius.org/, 2005

**FREGAN Beatrix**

# DOKTRÍNA, STRATÉGIA, TAKTIKA – A FRANCIA MINTA

Az összhaderőnemi szemlélet egyeduralkodóvá válása, mint globális hadművészeti tendencia még nem eléggé jelentkezik tisztképzésünk elméletében és gyakorlatában. 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, ez azt eredményezte, hogy a fegyveres konfliktusba bevont erők nagysága csökkent, ugyanakkor megnövekedett a bevetett kötelékek technológiai fejlettsége. Az alacsony intenzitású konfliktusoknak a fejlett világtól való nagy térbeli távolsága ezzel párhuzamosan csökkentette azt a képzeletbeli szintet, amely a kizárólag egy haderőnem által végrehajtott hadműveleteket az összhaderőnemi szinttől elválasztotta. Az ezredforduló bekövetkeztével minden katonai művelet összhaderőnemivé vált, amiben több haderőnem együttesen vesz részt. Ez logikusan vezet 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 leküzdendő hadászati méretű távolságok miatt – tartósan gyökeret vert harcászati szinten is.

Az összhaderőnemi képességek nyugati mintájú megjelenése a projection-ban, azaz a fegyveres erőknek a hadműveleti területre, körzetbe való átszállításában, utánpótlásában és visszatelepítésében kap szerepet, amely ma a NATO-műveletekben is teret hódított.

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, konkrétabban 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 CID50, egyike azon európai országoknak, ahol elsőként valósították meg az összhaderőnemi képzési formát. Ugyanakkor el kell ismerni azt is, hogy bár Franciaországnak a NATO katonai szervezetétől való sajátos elhatárolódása a fegyveres erők képzésében a legutóbbi időkig is érvényesült, ugyanakkor a közös szövetségi műveletekben (NATO, EU, EBESZ, stb.) mint résztvevő ország, minden szinten igazodik a NATO struktúrákhoz, metódusokhoz. Ugyanez vonatkozik a stratégiai döntéshozatali rendszerre; vagyis a francia módszer valódi NATO döntéshozatali rendszert alkot. Remélhető tehát, hogy a francia modell jelenti a napjainkban fellelhető legnagyobb kontrasztot a tömegessé váló amerikai példákkal szemben.

A francia összhaderőnemi képzés fellegvára a Párizsban található Összhaderőnemi Védelmi Kollégium (CID). A CID 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 tovább folytatják.

A képzési forma főbb tartalmi súlypontját az összhaderőnemi hadműveleti képzés (az oktatott tananyag 50%-a) alkotja, majd fajsúlyát tekintve a menedzsment és tevékenységi technikák (20%), és 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 hadműveleti képzés a haderőnemek és a jelentősebb külföldi hadseregek megismerésén, a különféle hadszínterek és konkrét hadműveleti 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-hadműveleti szinten használt döntéshozatali rendszer, a MARS rendszer51 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 nyújtáson a hallgatók részére, amelyek biztosítják a védelmi szféra környezetének és a katonai műveletek hatásának minél teljesebb körű elemzését. A tananyagrész oktatásának másik kiemelt célja, hogy széles körű globális ismereteket nyújtson az államközi kapcsolatok, a világgazdaság és a nemzetközi együttműködés kérdésköreiben is. A tananyagrész fontosságát jelzi, hogy a hallgatók számára az iskolaév 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 rendelkezé-

[50] CID = Collège Interarmées de Défense: Összhaderőnemi Védelmi Kollégium

[51] **M**éthode interarmées d’**A**ppréciation et de **R**aisonnement sur une **S**ituation **M**ilitaire = katonai helyzetmegítélés és döntéshozatal összhaderőnemi módszere

sükre 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 Francia Köztársaság fegyveres erői összhaderőnemi képzéséből a magyar felsőoktatásra véleményem szerint az alábbi következtetések vonhatók le:

- összhaderőnemi ismeretek mélyebb szintű oktatása, a haderőnemi képzés folytatása, elmélyítése mellett;
- az összhaderőnemi ismereteket a tiszti képzés második-harmadik fázisában célszerű végrehajtani (főiskola – egyetem – vezérkari tanfolyam);
- az összhaderőnemi ismereteket a tiszti karrier szerves részeként, a magasabb beosztásba kerülés feltételeként kell oktatni (azaz a magasabb beosztású tisztek mindegyike eleve összhaderőnemi képzettségű legyen);
- a főtisztek szakterületekre való specializálása megmaradjon, de funkcionálisan működjön. Nincs szükség már összhaderőnemi szakképesítésre, hanem az összhaderőnemi végzettséggel rendelkezők között vannak funkcionálisan specializáltak (pl. nemzetközi kapcsolatok, kommunikáció és média, stb.).

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.

Hagyományaikból és a képzési sajátosságokból adódóan a francia összhaderőnemi tiszt elsősorban magas szintű általános ismeretekkel rendelkező, értelmiségi beállítottságú. Az összhaderőnemi képzés során, mint előző képzése során is mindig, elsősorban gondolkodni tanítják meg, nem terhelik túl adatokkal. (Az amerikaival szemben esetenként talán kevésbé hatékony, mert itt az általános ismeretek dominálnak, nem a specializáció!) Mivel szabályzatai, szakutasításai igen tág teret hagynak az önálló értelmezésnek, esetenként improvizál. A francia tiszt tehát egy nagy hagyományokkal rendelkező európai ország hadseregének tagja; feladatainak végrehajtásakor, munkájában csak a leglényegesebb fázisok végrehajtásában kényszerül aprólékos rendszerességre. Az új iránt az amerikainál fogékonyabb. Nemzetközi törzsekben végzett munkát illetően jelentős tapasztalatai vannak (még a NATO-tól való elhatárolódás mellett is). Ugyanakkor a stratégiai döntéshozatali rendszerben viszonylagos szigorú metódus szabályozza a döntés-elhatározás kialakításának folyamatát.

## FELHASZNÁLT IRODALOM


[1] 1. Ralph Peters: A jövő konfliktusainak kultúrája; Új Honvédségi Szemle, 1997/1. sz., 32-41. o.

[2] 2. Nagy Andrea-dr. Pintér István: Leadership - vezetési stílus, katonai vezetési stílus; Új Honvédségi Szemle, 1997/2. sz., 66-78. o.

[3] 3. Végh Ferenc: Milyen honvédséget akarunk?; Új Honvédségi Szemle, 1997/6. sz., 4-9. o.

[4] 4. Dr. Jeney Géza: A katonai felsőoktatást átfogó képzési rendszer szükségességéről; Hadtudomány, 1996/4. sz., 84-91. o.

[5] 5. Dr. Szternák György: Elgondolás a vezérkari tisztképzés céljáról és tematikai programjáról (középtávú terv); ZMNE Hadtudományi Kar, Budapest, 1997.

[6] 6. Dossier d'enseignement (az Összhaderőnemi Védelmi Kollégium tematikai programja - Kiadvány, Collège Interarmées de Défense, Paris, 2003)

**Interneten elérhető információk:**

[7] 1. Ministre de Défense: http://www.defense.gouv.fr
[8] 2. US Military Academy: http://www.usma.edu
[9] 3. US Armed Forces Staff College: http://www.usma.edu
[10] 4. US Army Command and Staff School: http://leav-www.army.mil
[11] 5. US Army War College: http://carlisle-www.army.mil
[12] 6. UK MOD: http://www.mod.uk

**GÁCSER Zoltán**

# AZ INFOKOMMUNIKÁCIÓS ESZKÖZÖK ÉS A DIGITÁLIS KATONA SZEREPE A XXI. SZÁZAD HADVISELÉSÉBEN

## Bevezetés

A XXI. század biztonságpolitikai és az ebből következő katonai kihívásainak elemzését és értékelését követően levonható az a következtetés, hogy a napjaink és a közeljövő katonai kihívásainak csak a digitális, precíziós hadseregek, szövetséges haderők tudnak megfelelni. Ezek az elekrtonizált, informatizált, hálózatos hadviselésre, információs és hatásalapú műveletek végrehajtására alkalmas, humán és egyre nagyobb számban robot erőkre támaszkodó, precíziós (intelligens) haditechnikai komplexumokat (fegyverrendszereket) felvonultató haderők rendelkeznek csak a sikeres műveletekhez szükséges képességekkel, mint ahogy ezt a II. öbölháború is bebizonyította. A fejlett hadseregek fejlesztési irányai egy ilyen haderő felállítása felé mutatnak. Természetesen ez nem kis pénzt és nem kevés időt vesz igénybe. A digitális, precíziós haderő kialakításában az amerikai hadsereg áll az élen, amely már rendelkezik egy digitális hadosztállyal. Ennek egyik dandárát a II. öbölháborúban sikeresen vetették be a katonai műveletek során. Az amerikai szárazföldi haderő 2005–2010 között egy digitális expedíciós hadtest, tíz digitális hadosztály, egy digitális páncélos felderítő ezred és két digitális dandár (Nemzeti Gárda) felállítását tervezi [1.].

A NATO is az ilyen irányú haderőfejlesztésre kötelezte el magát, 2018-ra el kívánja érni a hálózatos hadviseléshez szükséges képességeket. Ennek első lépéseként 2006-ra felállítja az első digitális szárazföldi dandárát [2.].

## Az infokommunikációs rendszerek

A digitális, precíziós hadseregek, de maga a XXI. század információs (tudás alapú) társadalma sem képzelhető el fejlett infokommunikációs rendszerek, eszközök megléte és működése nélkül.

Látnunk kell, hogy az információs társadalom elsődleges társadalmi értéke (alapvető mozgató rugója) az információ, a kommunikáció és a tudás. A társadalmi, politikai, gazdasági, védelmi és kulturális élet működését ebben a társadalomban az optimális mennyiségű információ biztosítja.

Az információs társadalom működéséhez elengedhetetlenek az úgynevezett általános feladatú és információs rendeltetésű infrastruktúrák[52].

Az általános feladatú infrastruktúrák olyan állandó helyű vagy mobil építmények, eszközök, rendszerek, hálózatok, továbbá az általuk nyújtott szolgáltatások,

[52] Az infrastruktúra nem más, mint egy adott rendszer (termelő vagy elosztó, szolgáltató rendszer, tudományos, állami, magán, nemzeti vagy nemzetközi szervezet, ország, város, vagy régió stb.) rendeltetésszerű működéséhez feltétlenül szükséges intézetek, intézmények, felszerelések és berendezések, továbbá a működtetést ellátó személyzet szabályszerűen működő összessége. Az infrastruktúra a fizikai építményekből és berendezésekből, illetve azokat szakszerűen működtetni tudó szakszemélyzetből tevődik össze. (Forrás: Haig Zsolt – Várhegyi István: Információs műveletek I. Egyetemi jegyzet, ZMNE, Budapest, 2004. p. 124 [5.])

működési feltételek összessége, amelyek valamilyen társadalmi, gazdasági vagy akár katonai funkciók és rendszerek feladatorientált, zavartalan és hatékony működését teszik lehetővé. Ilyek lehetnek például a közigazgatási, szállítási, hírközlési, vezetési, ellátási, tájékoztatási funkciók.

Az információs rendeltetésű infrastruktúrák olyan állandó telepítésű vagy mobil létesítmények, eszközök, rendszerek, hálózatok, és az általuk nyújtott szolgáltatások összessége, amelyek az információs társadalom működéséhez szükséges információk megszerzését, előállítását, tárolását, szállítását és felhasználását teszik lehetővé.

Az információs infrastruktúrákon belül rendeltetésük (feladatuk) szerint megkülönböztethetünk:

- funkcionális (alap) információs infrastruktúrákat, amelyek feladata –fizikailag– lehetővé tenni a társadalom valamilyen információs funkciójának zavartalan működését, tehát infrastrukturális alapon információs alapszolgáltatásokat végezni. Az információs társadalomban ezek tekinthetők az elsődleges információs infrastruktúráknak, hiszen biztosítják az információk megszerzését, előállítását, továbbítását, feldolgozását és felhasználását. Ezek az infrastruktúrák általában nagykiterjedésű, bonyolult szervezésű hálózatok vagy rendszerek keretein belül működnek;
- támogató információs infrastruktúrákat, amelyek létrehozzák, és folyamatosan biztosítsák az alapvető információs szolgáltatásokat végző funkcionális információs infrastruktúrák zavartalan működéséhez és fejlődéséhez szükséges szellemi és anyagi alapokat, valamint támogató háttereket.

Célszerűnek tartom felvázolni az első csoportba sorolható elemeket, hiszen ezek egyes elemei jelentős szerepet töltenek be a katonai műveletek támogatásában, illetve részét képezik a digitális katona eszközrendszerének.

A funkcionális információs infrastruktúrák közé az alábbiak sorolhatók:

- a nyílt előfizetői távközlési hálózatok;
- a közszolgálati, közüzemi és közellátási érdekből üzemeltetett zárt távközlési különhálózatok;
- a műsorszóró és tájékoztató hálózatok;
- a vezetési rendszerek, hálózatok (országos hatáskörű kormányzati, közigazgatási, rendőrségi, határőrségi, vámőrségi, honvédségi stb. hálózatok);
- a légi forgalmat, repülésirányítást és légi navigációt biztosító rendszerek;
- a légvédelmi fegyverirányítást biztosító rendszerek;
- a távérzékelést, távellenőrzést biztosító rendszerek;
- a távirányító- és robotok vezérlését biztosító rendszerek;
- az informatikai hálózatok.[53]

Az információs társadalom információs infrastruktúráinak alapját az informatikai alapú távközlési rendszerek, vagyis az infokommunikációs rendszerek képezik. Az információs társadalomban az informatikai hálózatok nem különíthetők el a távközlési hálózatoktól, hiszen azok nélkül működésképtelenek. Az információs hálózatok tehát nem értelmezhetők a kommunikációs csatornát, és az ezen belüli információ-

[53] Forrás: Haig Zsolt – Várhegyi István: Információs műveletek I. Egyetemi jegyzet, ZMNE, Budapest, 2004.
p. 129 [5.]

átvitelt biztosító eszközök nélkül. A korszerű távközlési rendszerekben felhasznált számítógépes hardver és szoftver környezet egyértelműen az informatika és a távközlés konvergenciáját jelenti. Mindezek indokolják, az „infokommunikáció” mint kifejezés és technológia megjelenésének létjogosultságát.

Tehát a korszerű információs eszközök, rendszerek joggal nevezhetők infokommunikációs eszközöknek, rendszereknek.[5].

## A katonai műveletekben alkalmazható infokommunikációs eszközök (rendszerek)

Napjaink katonai műveleteiben nem csak a katonai célra létrehozott infokommunikációs rendszereket alkalmazzák, hanem támaszkodnak a polgári (infokommunikációs) rendszerekre is. A modern infokommunikációs rendszerek nélkülözhetetlenek a korszerű hadviselés megvívása során, hiszen elképzelhetetlen a siker kivívása ezen eszközök alkalmazása nélkül. Nagy szerepük és jelentőségük van ezeknek az eszközöknek (rendszereknek) az információs és a vezetési fölény megszerzésében, fenntartásában.

Az infokommunikációs rendszerek, hálózatok biztosítják a pontos, tartalomban és időben valós, időszerű adatok és információk megszerzését az ellenségről, továbbá lehetővé teszik ezek feldolgozását, archiválását és értékelhető formában történő megjelenítését.

A katonai műveletekben alkalmazható –fontosabb– infokommunikációs rendszerek (eszközök) az alábbiak lehetnek:

- különböző számítógép-hálózatok;
- harcászati internet és az Internet;
- különbözö vezetékes és vezeték nélküli távközlő (információs) rendszerek, eszközök;
- műholdas távközlési rendszerek;
- műholdas navigációs rendszerek;
- felderítő eszközök, rendszerek (optikai, elektrooptikai, multispektrális, lézer, infravörös, rádiólokációs, rádió-, rádiótechnikai, akusztikai és hidroakusztikai, mágnesesség mérésén alapuló, továbbá szeizmikus felderítő eszközök, rendszerek);
- harctéri (közvetett és közvetlen) azonosító rendszerek;
- térinformatikai alapú katonai információs rendszerek;
- katona-földrajzi információs rendszerek;
- katonai vezetési- és irányítási rendszerek;
- katonai szimulációs rendszerek.

Az infokommunikációs eszközök, rendszerek előnyös tulajdonságai nagymértékben növelhetők összekapcsolásuk, vagyis információs (infokommunikációs) hálózatba kötésük révén.

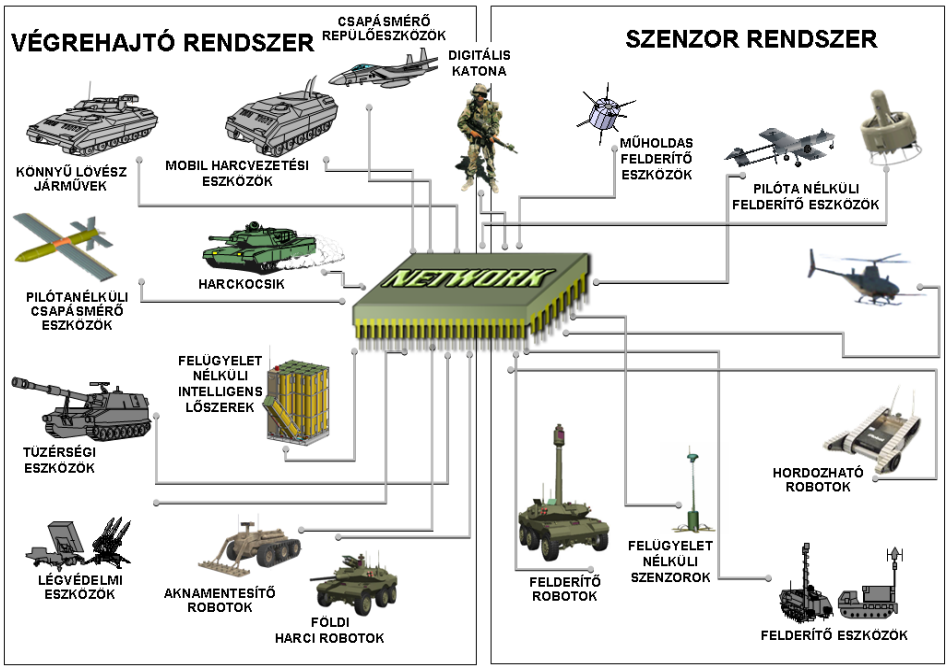
## Az információs hálózatra épülő hálózatközpontú hadviselés

Az úgynevezett magas intenzitású hadműveletekben résztvevő szárazföldi csapatok hatékony alkalmazása megköveteli az egyidejű támogatást a levegőből, az űrből, a tengerről és a távoli harcvezetési központból. Mindehhez olyan, egymással haderőnemi szinten is összekapcsolt számítógép–hálózatokra épülő integrált érzékelő–döntéshozó–végrehajtó információs (infokommunikációs) rendszerre, vagyis számító-

gépes információs hálózatra van szükség, amely lehetővé teszi az ilyen támogatást. Ez a hálózat képezi a hálózatközpontú hadviselés54 gerincét.

A korszerű katonai műveletekben igényként jelent meg, hogy a saját erők, a feladatuk végrehajtásához szükséges valamennyi fontos információhoz valós időben, a megfelelő tartalomban és felhasználható formában legyenek képesek hozzáférni. Ezzel az új gondolkodásmóddal jellemezhető a hálózatközpontú hadviselés, amelyben a hatékonyságot leginkább meghatározó tényezők: az információ, a valós idejű információk áramlást biztosító infokommunikációs eszközök (rendszerek), a humán és szenzor alapú precíziós felderítés, a precíziós tűzerő, a manőver, a sebesség, a tudás és a tudomány.

A hálózatközpontú hadviselés a decentralizált vezetési hálóra, amely minden döntéshozó számára biztosítja a felelősségi és érdekeltségi körébe tartozó fontos adatokhoz, információkhoz való hozzáférést, kiértékelést és ezek hatékony felhasználását; a valós idejű és biztonságos kommunikációra az érzékelők, a döntéshozók és a végrehajtók között; továbbá a szükséges harcászati és harctéri környezeti adatok valós idejű megszerzését, továbbítását, fúziós adatfeldolgozását és megjelenítését biztosító komplex rendszerekre támaszkodik. A hálózatközpontú hadviselés elemeinek rendszerét (1. ábra) három, egymással összeköttetésben és összhangban lévő egységre –az információs hálóra, a felderítő szenzorhálóra és a végrehajtói hálóra– lehet tagolni.




1. ábra. A hálózatközpontú hadviselés elemeinek rendszere55

54 Ezt a korszerű hadviselési elvet követték a szövetséges erők a II. öbölháborúban (2003, Irak).

55 Forrás: Haig Zsolt – Várhegyi István: Hadviselés az információs hadszíntéren. Zrínyi kiadó, Budapest, 2005. p. 175 [1.]

A felderítő, vagy más néven érzékelő (szenzor) hálózat biztosítja a saját és az ellenséges erőkről, valamint a harctér környezetéről és annak változásairól szóló valós idejű és tartalmú információk megszerzését, továbbá eljuttatását a hálózat számára. Ez a rendszer a földi, a tengeri, a légi, a kozmikus és a kibertér alapú érzékelőkből, infokommunikációs eszközökből épül föl.

Az információs, vagy más néven vezetési hálózat adja meg a hálózatközpontú rendszer globális felépítését és biztosítja az ehhez szükséges infrastruktúrát. A katonai és a polgári információs, infokommunikációs infrastruktúra elemeit kihasználva behálózza a hadszíntér minden dimenzióját. Ide sorolható minden olyan eszköz és rendszer, amely érzékeli, összegyűjti, feldolgozza, továbbítja (ideiglenes vagy folyamatos és állandó hang, adat és videojel típusú információáramoltatást biztosít), tárolja és védi az adatokat és információkat.

A végrehajtó, alkalmazói hálózat az adott katonai művelettel összefüggésbe hozható saját oldali harci erőt (élő erőt, technikai eszközt és fegyverrendszert) foglalja magában. Látni kell azt, hogy ezek az elemek feladat végrehajtásuk során értékes információkat gyűjthetnek be és juthatnak el a vezetési hálózathoz.

A hálózatközpontú hadviselés választ adhat a XXI. század katonai kihívásaira az alábbi előnyös tulajdonságai miatt:

- a szenzoroktól a döntéshozón át a végrehajtóig a műveletben résztvevő elemeket egységes hálózatba rendezi;
- a műveletben résztvevő elemek közötti digitális jelformátumú információáramlás alkalmazásával az információk egyik ponttól a másik pontig történő eljutása nagymértékben felgyorsul (kevesebb időt vesz igénybe);
- a végrehajtó nemcsak a saját szenzorai (érzékelői) által nyert információkra tud támaszkodni, hanem más felderítési forrásból származókra is;
- a döntéshozó valós időben képes átlátni a kialakult helyzetet, és így megalapozottabb döntéseket tud hozni.

A fentiek is igazolják, hogy a hálózatba kapcsolt haderő képességei jelentősen megnőnek, hiszen növekszik, és pontosabbá válik a harctéri helyzetismeret (a kialakult harctéri helyzet valós ismerete), melynek következtében a digitális katona szintjétől egészen az összhaderőnemi szintig nő a reagáló képesség, a hatékonyság, a túlélőképesség és az interoperabilitás. A valós idejű információk révén pedig jelentős mértékben lerövidül a döntési időciklus.

A NATO terminológia a hálózatközpontú hadviselés (Network Centric Warfrae – NCW) helyett a hálózat nyújtotta képesség (Network Enabled Capability – NEC) fogalmat használja. A hálózatközpontú hadviselést elemezve beláthatjuk, hogy találóbb a hálózat nyújtotta képesség kifejezés, hiszen ez jobban tükrözi a filozófia lényegét. Miszerint a hálózatba bekapcsolt elemek erőforrásainak összehangolt kihasználása sokkal hatékonyabb, mint ezek önálló, elkülönült alkalmazása. Tehát a képesség növekedést a hálózat által biztosított lehetőségek adják meg.

Két ok indokolta a hálózatközpontú hadviselés (a fentiekben vázolt) rövid elemzését és értékelését. Az egyik az, hogy a digitális katona létezésének egyik alapját a hálózat képezi, a másik, hogy NATO tagként a Magyar Honvédségnek is számítania kell a közeljövőben a hálózatközpontú elv szerint megtervezett és végrehajtott katonai

műveletekben való részvételre. Hiszen a NATO is elkötelezte magát a hálózatos hadviselési képesség kialakítására.

### A digitális katona fogalmi meghatározása[56]

A digitális katona[57] hallatán nem szabad egy fantasztikus filmbe illő robot katonára gondolnunk. Ez a kifejezés ugyanis nem a Terminátor filmek kibernetikus katonáját (robotját), hanem „hús-vér" katonát foglal magában, aki rendelkezik azokkal a –csúcstechnikát képviselő– digitalizált (elektronizált) eszközökkel és rendszerekkel, amelyek biztosítják számára, a XXI. század kihívásaihoz igazodó katonai műveletekben a sikeres feladat végrehajtáshoz szükséges képességeket.

A digitális katonára jelenleg nincs egységes definíció. Betudható ez részben a tématerület újszerűségének és a fejlődés gyors ütemének. A magyar szakirodalomban a digitális katona definícióját – az elsők között – Várhegyi István és Makkay Imre adta meg. Ők az alábbi meghatározást alkalmazták: „A digitális katonák (vagyis összfegyvernemi manőverező erők) a digitalizált harcmezőn, elektronizált és informatizált fegyverrel, digitális vezérlésű, igen nagy találati pontosságú un. precíziós fegyverzettel harcolnak az általános hadműveleti terv alapján. Kiképzésükbe és felkészítésükbe beletartozik a számukra rendszeresített számítógépek (palmtopok, laptopok, törzsmunkaállomások, digitálisan vezérelt híradó eszközök, ellenőrző és felderítő eszközök, fegyverek és fegyverrendszerek stb.) kezelésének mesterfokú elsajátítása.

A digitális katonák tehát azok a korábbi, hagyományos fegyverekkel harcoló összfegyvernemi katonák (lövészek, harckocsizók, felderítők, tüzérek, stb.), akiket átképeztek digitális alapú fegyverek, harc– és vezetési eszközök kezelésére.

A digitális katonákat hamarosan ellátják olyan személyi számítógép-hálózattal, amelynek segítségével egyrészt jelenteni tudja helyzetét, egészségügyi és mentális állapotát, továbbá harci igényeit, másrészt információkat kaphat az elöljárótól, a szomszédaitól a változó helyzetről, újabb veszélyekről.

Az ilyen harci képességű digitális katonák minősítő elnevezése: a hálózatos katona lesz."[58]

Ezek a fogalmi meghatározások az akkori viszonyok között teljesen helytállóak voltak.

A technikai fejlődés és a hálózatos hadviselési elvek térhódításának hatására napjainkban már máshogy értelmezendő a digitális katona. A kutatások jelenlegi állása szerint megváltozott a két fogalom mögötti tartalom. A digitális katona napjainkra már más tartalommal bír, nem a digitális fegyverek, harci és vezetési eszközök kezelésére alkalmas összfegyvernemi katonát értjük alatta, hanem az idézet szerinti hálózatos katonát. A hálózatos katona és a digitális katona jelenleg szinonim fogalomként értelmezhető. Azért nem célszerű külön definiálni a digitális katonát és a hálózatos katonát,

[56] Forrás: Gácser Zoltán: A digitális katona. Tavaszi szél 2005 konferencia kiadvány, Debrecen, 2005. p. 100-102 [6.]

[57] A digitális katona alatt értendő speciális eszközrendszerrel rendelkező katonát az angol szakirodalomban digital soldier (digitális katona), net soldier (hálózatos katona), land warrior (földi harcos), future warrior (jövő harcosa) kifejezések alatt találhatjuk meg.

[58] Forrás:Várhegyi István – Makkay Imre: Információs korszak, információs háború, biztonságkultúra. OMIKK, Budapest, 2000., p. 133 [3]

mert a digitális katona nem létezhet hálózat nélkül. A digitalizált eszközrendszerének működése és az információáramlás sem képzelhető el a hálózat nélkül. Ezenkívül a katona képességnövekedésre is a személyi és a harctéri hálózatba kapcsolt infokommunikációs eszközök működése révén tesz szert.

A digitális katona egy speciális személyi és a harctéri hálózatba kapcsolt digitalizált-elektronizált eszközrendszerrel (egyéni felszerelés csomaggal) rendelkező katona, aki harcát a digitalizált harctéren a hálózatközpontú hadviselési elvek alapján vívja meg. Ezt a katonát a korszerű eszközei és a magas szintű kiképzettsége alkalmassá teszik a háborús és válságreagáló műveletekben való részvételre, valamint speciális, nagy fontosságú feladatok ellátására59.

A digitális katonák harci hatékonysága a megnövelt képességeiknél fogva kb. három-négyszerese a hagyományos katonák harci teljesítményének. A legjelentősebb képesség növekedést az infokommunikációs eszközei és ezek hálózatba kapcsolása, továbbá a személyi robotok alkalmazása adja a katonának.

A digitális katona létrejöttét a XXI. század katonai kihívásai generálták és a technológiai, technikai fejlettség nyújtotta lehetőségek biztosítják. Az új katonai kihívások igényelték a hagyományos katonák ellátását a kor színvonalának megfelelő digitalizált eszközökkel, és felruházását a hálózat nyújtotta előnyös képességekkel, hiszen ezek nélkül nem voltak képesek megfelelő sikereket elérni. Példaként hozható erre az afganisztáni és az iraki misszió is. Ezekben a műveletekben egyre nagyobb szerepet kaptak a digitális katonák, és az infokommunikációs eszközeik, robotjaik alkalmazásával megszerzett, továbbított valós idejű információk. A digitális katonák szárazföldi robotjai derítették fel például az al-Kaida bunkerek jelentős részét.

Alkalmazkodva korunk kihívásaihoz minden fejlett hadsereg modernizációs programjában fontos szerepet kap a katona eszközrendszerének korszerűsítése. E korszerűsítési folyamat kulcskérdése a katona feladat végrehajtó és túlélési képességének növelése. Ez a két paraméter csak úgy fokozható jelentős mértékben, ha a katona rendelkezik korszerű döntéstámogató rendszerrel.

## A digitális katona döntéstámogató infokommunikációs rendszere

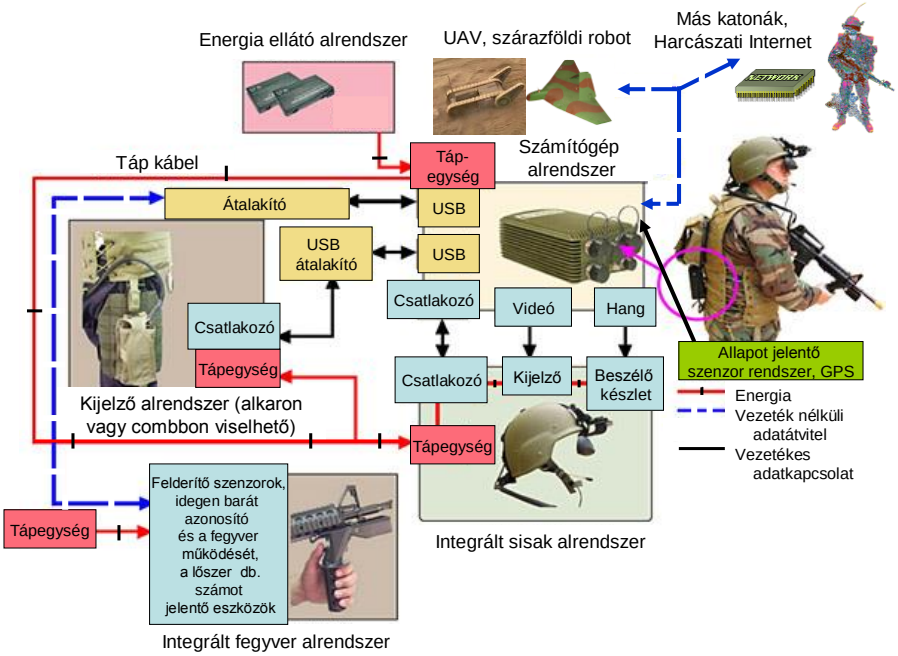
A digitális katona tevékenységét segítő döntéstámogató infokommunikációs rendszert vizsgálva meg kell különböztetni két hálózati szintet, amely egymáshoz kapcsolódva és egymást kiegészítve segíti a katona tevékenységét, és biztosítja számára a releváns döntések meghozatalához szükséges tartalomban és időben valós információkat.

Az egyik szint a helyi hálózat szintje. Ide tartoznak azok az eszközök, amelyek a katona saját eszközrendszerének részeként közvetlenül őt látják el információkkal, feldolgozzák ezeket, és értékelhető formában megjelenítik számára, ezzel alapozva meg a döntéseit. Ide sorolhatók a katona különböző érzékelői (a robotokra telepítetteket is ide értve), kamerái, helymeghatározó egysége, közvetlen idegen-barát azonosító rendszere, –szem elé hajtható, szemüvegre vagy szemüvegbe integrált, testfelületre rögzíthető– megjelenítő egysége és ezeket összehangoló számítógépe (esetleg számítógépei), továbbá ezek között az információáramlást és adat kommunikációt biztosító

[59] Ezek közé tartozhatnak többek között a terrorista csoportok elleni bevetések, a különös fontosságú személyek, célok felderítése, helyzetének megadása, szükség szerinti megsemmisítése.

eszközök. Ezek az eszközök egy rendszert alkotva közvetlenül támogatják a digitális katona tevékenységét, ezért ezt a katona közvetlen döntéstámogató infokommunikációs rendszerének, vagy a katona saját információs hálózatnak célszerű definiálni.

A másik csoportba azok a külső (azaz nem a katona eszközrendszerének részét képező eszközök, rendszerek) hálózatok sorolhatók, amelyek információkkal tudják ellátni a katonát a helyes döntések meghozatalához. Ebbe a rendszerbe tartoznak a harcászati szintű harcvezetési rendszerek, a helymeghatározó és jelentő rendszerek, a földi és légi harcászati rádióhálók (kommunikációs rendszerek és csatornák), adatszerző és feldolgozó rendszerek, a harcászati adatterminálok (közös harcászati adatbázisok), a műholdas helymeghatározó rendszer, és a más katonák közvetlen döntéstámogató rendszerei. Ezen eszközök hálózatba kapcsolt rendszerét a katona közvetett döntéstámogató infokommunikációs rendszerének, vagy a hálózatokon alapuló harctéri információs hálózatnak célszerű definiálni. Egyes szakirodalmakban ezt az integrált kommunikációs hálózatot Harcászati Internet (Tactical Internet60) kifejezéssel illetik.




2. ábra. A digitális katona eszközrendszerének elemei között fennálló kommunikációs kapcsolat rendszer[61]

Ettől a rendszerből kérhet a katona –a feladata alapján kapott jogosultsága alapján– akár magasabb szintű (például tűztámogatási, felderítési) támogatásokat, együttműködési információkat, de adhat is információkat a rendszernek. Továbbá e rendszer kommunikációs eszközein keresztül a katona kapcsolatot tarthat a harcveze-

[60] Forrás: Tactical Internet. http://www.fas.org/man/dod-101/sys/land/internet-t.htm

[61] Az ábrát a [10.] és a [11.] forrásanyagok felhasználásával szerkesztette a szerző.

tési központtal, vagy egy magasabb szintű elöljáróval. Ez a harctéri információs hálózat természetesen elsősorban nem az egyes harcos (digitális katona) érdekében tevékenykedik, de a katona (mint felhasználó) kihasználhatja a rendszer nyújtotta lehetőségeket. Ezáltal a rendszer a katona támogatási feladatát is képes ellátni, így részét képezi támogatási rendszerének.

A digitális katona közvetlen döntéstámogató infokommunikációs rendszernek egyes elemei közötti kommunikációs kapcsolatot, továbbá a hálózathoz (Harcászati Internethez) és a társaihoz való kapcsolódás egy változatát szemlélteti a 2. számú ábra.

Mindkét szinten, továbbá a két rendszer összekapcsolásában is 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 a számítógép fő feladata.

Figyelembe véve a katonai kihívásokat és a katona jövőbeni várható feladatrendszerét, összeállítható egy digitalizált eszközrendszer, amely alkalmassá teszi a katonát a XXI. század harctevékenységeinek sikeres végrehajtására. Ez a katona egyéni felszerelésének részeként jelentős képességnövekedést és jobb túlélési esélyeket teremt számára.

## A digitális katona eszközrendszere

Az elmúlt néhány évet jellemző katonai műveletek tapasztalatai egyértelműen rávilágítottak arra, hogy sikeres tevékenységet a katona csak modern elektronizált, informatizált eszközökkel tud végrehajtani.

Egy elektronizált felszereléscsomagba azokat az eszközcsoportokat célszerű integrálni, amelyek nélkül a katona nem képes a kor színvonalának megfelelő, és sikeres katonai műveletet végrehajtani. Az ilyen speciális eszközrendszert használó katonák bevethetőek szakasz, raj kötelékben, de képesek önálló feladat végrehajtásra is. A digitalizált eszközrendszerrel szemben alapvető elvárásként jelentkezik a vízhatlanság.

A digitális katonának rendelkeznie kell az alábbiakkal (az elektronizált eszközrendszer egy változata):

- speciális ruházat;
- egyéni helymeghatározó (nagy felbontású digitális térképadatbázissal ellátott GPS[62] vevő egység) és helyzetjelentő rendszer;
- egyéni idegen-barát felismerő rendszer;
- nagy felbontású megjelenítő egység képi és írásos információk kijelzésére;
- mikrofon és beszélő készlet;
- felderítő eszközrendszer[63];
- nagy teljesítményű, viselhető számítógép;

[62] GPS: Global Positioning System = globális helymeghatározó rendszer

[63] A digitális katona felderítő eszközrendszere magában foglalja a látható fény tartományában működő (nappali) digitális kamerákat és fényképezőgépeket; az infravörös tartományban működő kamerákat; az ultraibolya tartományban működő felderítő eszközöket; a meglévő fény felerősítésének elvét alkalmazó éjjellátó eszközöket; a lézer besugárzás érzékelőket; a hangfelderítésre és rögzítésre alkalmas eszközöket; a lézer tartományban működő távolságmérővel ellátott távcsövet; az akusztikai változásokat érzékelő műszereket; a külső hőmérséklet változását érzékelő műszereket, továbbá a vegyi, biológiai és radioaktív harcanyagot érzékelő műszereket.

- nagy zavarvédettségű személyi rádió;
- folyamatos védett infokommunikációs kapcsolat;
- egyéni egészségi állapot ellenőrző és jelentő rendszer;
- folyamatos energiaellátást biztosító rendszer;
- hordozható szárazföldi és légi robot;
- elektrooptikai eszközökkel ellátott speciális fegyver.

A digitális katona eszközrendszerének elemei úgy lettek kifejlesztve, hogy ezeket a katona a testfelületén, ruházatán és a hátizsákjában képes legyen magával vinni a bevetésekre. Az eszközök elhelyezésének egy változatát a 3. számú ábra szemlélteti.




3. ábra. A digitális katona és eszközrendszere[64]

Az előzőekben ismertetett felszereléscsomag néhány előnyös tulajdonsága az alábbiakban foglalható össze. A katona a digitalizált eszközrendszer segítségével többek között alkalmas[65]:

- valós (közel valós) idejű audiovizuális felderítési adatok megszerzésére a nap bármely szakaszában;
- ellenséges területek, objektumok felderítésére biztonságos távolságból;

[64] Az ábrát a [9.] és a [10.] forrásanyagok felhasználásával szerkesztette a szerző.

[65] Forrás: Gácser Zoltán: A XXI. század katonájának elektronizált eszközrendszere. Kard és toll 2004/2. Budapest, 2004. p. 156-157 [7.], illetve Gácser Zoltán: A digitalizált katona kommunikációs és információs igénye. Kommunikáció 2004 konferencia kiadvány, ZMNE, Budapest 2004. p. 114-115 [8.]

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

A felszereléscsomag hozzájuttatja a katonát a feladat sikeres végrehajtása szempontjából nélkülözhetetlen valós idejű információkhoz, 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.

## Összegzés

A közelmúlt tapasztalatai egyértelműen rávilágítottak arra, hogy napjainkban sikeres katonai műveleteket nem lehet végrehajtani korszerszerű infokommunikációs rendszerek, eszközök támogatása és a hálózatközpontú hadviselés elveinek alkalmazása nélkül. Ezt felismerve, egyre több nemzet haderejének átalakítása folyik ezen elvek figyelembevételével.

A Magyar Honvédségnek –mint szövetséges haderőnek– is részt kell tudni vállalni a hálózatos hadviselés képességeinek megteremtésében. Megítélésem szerint: képesnek kell lennie részeivel (raj, szakasz, későbbiekben maximum század erővel) szövetséges keretek közötti hálózatközpontú műveletekben tevékenykedni. Ennek konstruktív lehetőségét a digitális katonákból álló kis alegység (raj vagy szakasz erőben) felállításában látom. A digitális alegység képes lenne szövetséges keretek között, akár egy többnemzetiségű digitális zászlóalj, vagy dandár részeként hálózatközpontú katonai műveletek végrehajtására. Ennek megfelelően a magyar digitális alegység katonáinak eszközrendszerét úgy kell megválasztani, hogy ez interoperabilis –tehát együttműködő– legyen a NATO rendszerrel.

## Felhasznált irodalom


[1] Haig Zsolt – Várhegyi István: Hadviselés az információs hadszíntéren. Zrínyi Kiadó, Budapest, 2005.

[2] Haig Zsolt – Várhegyi István – Ványa László: A hatásalapú műveletek és céltervezésük elvi kérdései. Témafeltáró és bevezető tanulmány a MH Légierő 2004. évi tudományos kutatási tervéhez, Budapest 2004.

[3] Várhegyi István – Makkay Imre: Információs korszak, információs háború, biztonságkultúra. OMIKK, Budapest, 2000.

[4] T J Gander, E H Biass, J Keggler: Tomorrow's infantry warrior. Armada International, 5/2003.

[5] Haig Zsolt – Várhegyi István: Információs műveletek I-II. Egyetemi jegyzet, ZMNE, Budapest, 2004.

[6] Gácser Zoltán: A digitális katona. Tavaszi szél 2005 konferencia kiadvány, Debrecen, 2005.

[7] Gácser Zoltán: A XXI. század katonájának elektronizált eszközrendszere. Kard és toll 2004/2. HM OTF, Budapest, 2004.
[8] Gácser Zoltán: A digitalizált katona kommunikációs és információs igénye. Kommunikáció 2004 konferencia kiadvány, ZMNE, Budapest 2004.
[9] Warrior of the future. http://www.businessweek.com/magazine/content/03_30/b3843084.htm
[10] Nic Robertson: Meet Packbot: The newest recruit. CNN.com, 2002. augusztus 01. http://archives.cnn.com/2002/TECH/science/08/01/packbot/
[11] Embedded Training for Dismounted Soldiers Science and Technology Objective. http://www.quantum3d.com/stories/daggers.htm
[12] Combat ID Dismounted Soldier. http://www.fas.org/man/dod-101/sys/land/cidds.htm
[13] Land warrior. http://www.fas.org/man/dod-101/sys/land/land-warrior.htm
[14] Tactical Internet. http://www.fas.org/man/dod-101/sys/land/internet-t.htm
[15] Arthur K. Cebrowski - John J. Garstka: Network-Centric Warfare: Its Origin and Future. http://www.usni.org/Proceedings/Articles98/PROcebrowski.htm

**Dr. HAIG Zsolt**

# AZ INFORMÁCIÓS MŰVELETEK TERVEZÉSÉNEK KÉRDÉSEI

## Bevezetés

Az információs kor kezdetével párhuzamosan kialakuló katonai információs forradalom az információt, mint a társadalom jövőjét meghatározó alapértéket a figyelem középpontjába állította. Ezzel összefüggésben központi szerephez jutott az információból származó tudás és a tudomány legújabb eredményeire támaszkodó tudomány alapú katonai vezetés.

A XXI. században a hadműveleti parancsnok korszerű tudásszintje és vezetési gyakorlata a katonai győzelem kivívásának egyik alapvető feltétele, mely információs fölényre támaszkodik és a vezetési fölényben nyilvánul meg. E fölénytényezők az információs műveletek összehangolt alkalmazásával érhetők el. Az információs műveletek napjainkban egyre nagyobb jelentőséget és szerepet kapnak a katonai műveletek teljes spektrumában.

Az információs hadszíntér kialakulásával az összhaderőnemi hadműveleti parancsnok korábbi hagyományos felelőssége, tervező, szervező, döntéshozó és irányító tevékenysége kibővül az információs műveletekkel kapcsolatos feladatkörökre is. A hagyományos hadművelet keretében végrehajtásra kerülő információs műveletekért a hadműveleti parancsnok személyesen felelős! Ez az újabb felelősség és feladat a parancsnokkal szemben azt a követelményt támasztja, hogy figyelembe kell vennie az információs hadszíntéren jelentkező célpontokat, azok leküzdhetőségének különböző eljárásait, módszereit. Döntéseinél számolni kell az információs műveletek igényeivel és lehetőségeivel. A hadműveleti parancsnoknak nemcsak a hagyományos hadszíntereken (szárazföldi, légi, tengeri, és űrhadszíntereken), de az információs hadszíntéren is győznie kell. A rendelkezésre álló „kemény és lágy" pusztító erőforrások (fegyverek, eszközök és lőszerek) közel 30%-át vagy esetenként ennél még jóval többet is az ellenség információs tevékenységének és vezetési rendszerének bénítására, vagy korlátozására kell fordítani, ami gondos elemző, tervező, szervező törzsmunkát és felelősségteljes döntést igényel.

## 1. Az információs műveletek vezetésének szervezeti struktúrája

A NATO prágai csúcsértekezletén az állam- és kormányfők jóváhagyták a Prágai Képességvállalásokat (Prague Capabilities Commitment - PCC), amely szerint négy képességterületen fejlesztik haderejüket, köztük az információs fölény biztosítása területén. [1] Az információs fölény biztosítása pedig csakis jól szervezett, koordinált a konkrét feladatokhoz illeszkedő információs műveletekkel vívható ki, és tartható meg. Tehát amennyiben a Magyar Honvédség a képességalapú haderő kialakítása mellett kötelezte el magát, akkor meg kell felelnie mind az információs kor, mind pedig a NATO korszerű katonai műveleteiről alkotott elképzeléseinek, és teljesítenie kell a Prágai Képességvállalásokban megfogalmazott célkitűzéseket. Ez tehát azt is jelenti, hogy a Magyar Honvédség keretein belül is meg kell teremteni az információs fölény kivívásához szükséges képességeket, illetve olyan szervezetet, mely képes e tevékenységek tervezésére, szervezésére, koordinálására és irányítására. Békében –

más országokhoz hasonlóan – a Magyar Honvédségben is célszerű létrehozni egy 2-3 fős csoportot, amely az információs műveletek békeidejű feladatainak koordinálásával foglalkozik. Válság és háború időszakában e csoport kiegészíthető mindazon törzstisztekkel, akik az információs műveletek egy-egy területéért felelősek.

Az információs műveletek vezetésére többféle szervezeti struktúrában kerülhet sor. A Magyar Honvédségben jelenleg erre a tevékenységre nincs kialakult szervezet, így itt a NATO és USA elvek adaptálásával ismertetem a struktúra egy célszerű változatát.

Összhaderőnemi szinten az integrált információs műveletek tervezését, szervezését és irányítását az információs műveleti főtiszt vezetésével az Információs Műveleti Koordinációs Csoport (Information Operations Co-ordination Group – IOCG) végzi, amely országoktól és haderőktől függően különböző törzsekben működhet. A legáltalánosabb, és a NATO elveknek is megfelelő struktúra szerint az Információs Műveleti Koordinációs Csoport a hadműveleti törzsben működik. Itt kell azonban megjegyezni, hogy pl. az USA szárazföldi haderejében az információs műveletek tervezéséért, szervezéséért és irányításáért egy önálló törzs az Információs Műveletek Törzs (G-7) a felelős. [2] Az információs műveletek vezetésére haderőnemenként is célszerű szaktörzset létrehozni, mely struktúrájában és feladataiban (a haderőnemi sajátosságok figyelembevételével) hasonlít a fentebb említett szaktörzshöz.

A továbbiakban az összhaderőnemi szintű információs műveleti szaktörzs összetételét, felelősségi körét és feladatait, valamint a hadműveleti szintű információs műveletek tervezését mutatomk be. Ennek megfelelően az itt leírt elvek haderőnemi szinten is adaptálhatók.

### 1.1. Az információs műveleti főtiszt általános feladatai, felelősségi köre

Az Információs Műveleti Koordinációs Csoport élén az információs műveleti főtiszt (Information Operations Officer) áll, aki – az információs műveletekkel kapcsolatos kérdésekben – a parancsnok jóváhagyásával és nevében tárgyal, koordinál, tervez, szervez, irányít, tájékoztat és együttműködik. A parancsnok felé beszámolási kötelezettséggel tartozik, vele állandó kapcsolatot tart. Vezeti a szaktörzs információs műveletekkel kapcsolatos döntés-előkészítő, tervező, szervező, irányító, ellenőrző, együttműködő, és koordináló tevékenységét.

Az információs műveleti főtiszt felelős:

- a parancsnok Hadműveleti Tervének (Operations Plan – OPLAN) mellékletét képező Információs Műveleti Terv (Information Operations Plan – IOPLAN) kidolgozásáért, valódiságáért és időszerűségéért;
- a terv végrehajtását irányító információs műveleti mátrix szinkronizált módon történő, következetes betartásáért, illetve
- az információs műveleti mátrixnak a hadműveleti helyzetben bekövetkezett fontos és lényeges időközi változásokhoz történő igazításáért.

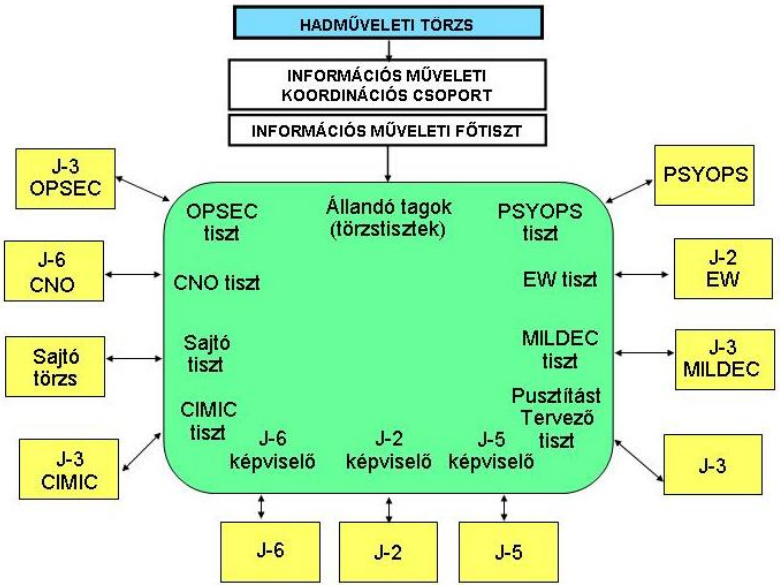
### 1.2. Az Információs Műveleti Koordinációs Csoport összetétele, feladatai

Az információs műveletek sokrétű és egymással szorosan összefüggő tevékenységek (műveleti biztonság, katonai megtévesztés, pszichológiai műveletek, fizikai pusztítás, elektronikai hadviselés, számítógép-hálózati hadviselés, polgári-katonai együttműködés, tömegtájékoztatás, felderítés) integrált és összehangolt végrehajtása.

Ahhoz, hogy az információs műveletek keretében e tevékenységek hatékonyan kerüljenek végrehajtásra, szükséges egy tervezést, szervezést és irányítást végző törzs felállítása és folyamatos működtetése. Mivel az információs műveletek integráns részét képezi mindenfajta katonai műveletnek, ezért elengedhetetlen a széleskörű és alapos tervezés és koordináció a tevékenységi elemek között.

Az Információs Műveleti Koordinációs Csoport összetételét minden esetben a hadműveleti törzs vezetője határozza meg a végrehajtandó feladatok és a parancsnok elgondolása alapján. A csoportot mindazon törzselemek képviselőiből célszerű kialakítani, akik felelősek saját tevékenységük információs műveletekbe történő integrálásáért, tehát alkotó-, kapcsolódó-, vagy támogató elemeit képezik az információs műveleteknek. A szaktörzs összetételének és méretének mindenkor meg kell felelnie az adott feladatnak és a parancsnok ez irányú elgondolásának. Ennél fogva a szaktörzs állandó tagokból (törzstisztekből) és a feladattól függően különböző törzsek (pl.: felderítő, elektronikai hadviselés, CIMIC stb.) képviselőiből (összekötő tisztekből) áll. (1. ábra) A törzsek képviselőinek megfelelő felhatalmazással kell bírniuk saját területük információs műveleteken belüli tervezésével és irányításával kapcsolatosan.

Mint ahogy az előzőekben leírtam e szaktörzs magját már békeidőben célszerű létrehozni, hiszen az információs műveleteknek vannak olyan területei, melyeket ezen időszakban is folytatni kell (pl.: hírszerzés, felderítés, műveleti biztonság, tömegtájékoztatás stb.) Válság és háborús tevékenység időszakában az információs műveleti szaktörzs jelentősen kiegészül, hiszen ekkor az integrált információs műveletek megtervezése és irányítása megköveteli a közvetlen kontaktust, koordinációt az információs műveletek minden egyes elemének képviselői között.




1. ábra: Az Információs Műveleti Koordinációs Csoport összetétele

Válság és háborús tevékenység időszakában a hadműveleti törzs szervezeti alárendeltségében található Információs Műveleti Koordinációs Csoport összetételét feladatorientáltan célszerű kialakítani. Ez azt jelenti, hogy célszerű olyan részlegeket

létrehozni, melyek közös és egy irányba ható tevékenysége jelentősen hozzájárul az információs műveletek sikeres vezetéséhez. Természetesen ez a különböző részlegek közötti, valamint a részlegekben működő törzs- és összekötő tisztek és a többi törzs közti együttműködést is feltételezi. Mind békeidőben, mind konfliktus, vagy háború időszakában az Információs Műveleti Koordinációs Csoport állománya folyamatos kapcsolatot kell, hogy tartson a megfelelő szaktörzsekkel a tervezés és végrehajtás koordinálása érdekében. A munkakapcsolat azt jelenti, hogy az aktuális tervezési adatok folyamatosan megjelennek az Információs Műveleti Koordinációs Csoportnál is, és így azokat összhangba lehet hozni az információs műveletek többi elemével. Ezáltal biztosítható az ellenség vezetési információs rendszerei elleni tevékenység és a saját hasonló rendszereink védelmének az összehangolása, illetve a feladatok szinkronizált végrehajtása.

Egy változatban a csoport felépítése a következő lehet:

- Hadműveleti Részleg (Perception Management Team – PMT);
- Felderítő Részleg (Intelligence Support Team – IST);
- Fizikai Pusztítást Tervező Részleg (Physical Effects Team – PET);
- Számítógép-hálózati Hadviselés Részleg (Computer Network Operations Team – CNOT). [2]

A Hadműveleti Részleg feladata az információs műveletek tervezése és közvetlen irányítása. A részleg koordinálja az információs műveletek különböző elemeinek tevékenységét, az egyes tevékenységeket egy közös információs műveleti tervbe integrálja. A tervezési folyamat során kidolgozza az információs műveletek cselekvési változatait, majd a parancsnok döntése nyomán elkészíti a hadműveleti parancsnok Hadműveleti Tervének információs műveletekre vonatkozó mellékletét (IOPLAN). Folyamatosan követi a hadművelet menetét és irányítja az információs műveletek végrehajtását.

A Felderítő Részleg tartja a kapcsolatot a hadműveleti parancsnokság felderítő törzsével és minden olyan információt és adatot biztosít, amelyek nélkülözhetetlenek az információs műveletek tervezéséhez, vezetéséhez. Azonosítja az ellenség kritikus- és sebezhető információs infrastruktúráit. Meghatározza az ellenség támadó információs műveleti képességeit és a saját erők elleni információs műveletek cselekvési változatait. Értékeli és meghatározza az ellenség információs műveletek általi sebezhetőségét. A részleg végzi a harcterület felderítő előkészítésének (Intelligence Preparation of the Battlefield – IPB) információs műveletekkel kapcsolatos feladatait. Szorosan figyelemmel kíséri az új felderítési adatokat, különös tekintettel az ellenség információs műveleti és vezetési hadviselési képességére, lehetőségére, szándékára, terveire, erőire, eszközeire, módszereire, céljaira, törekvéseire, főerőkifejtésére vonatkozóan.

A Fizikai Pusztítást Tervező Részleg tervezi, szervezi, irányítja és ellenőrzi az információs műveletek keretében alkalmazásra kerülő halálos és nem-halálos (lethal and non-lethal) hatású csapások végrehajtását. Meghatározza mindazon célpontokat, melyeket az információs fölény kivívása és megtartása érdekében pusztítani, illetve működésükben korlátozni kell. A felderítő és hadműveleti törzshöz felterjeszti az információs műveletek érdekében tiltott körzetek és célpontok jegyzékét, amelyek fontos információs műveleti célpontokat, illetve tevékenységi területeket tartalmaznak. Részt vesz a csapások hatékonyságának elemzésében.

A Számítógép-hálózati Hadviselés Részleg tervezi, szervezi, irányítja és ellenőrzi az ellenséges számítógép-hálózatok elleni támadásokat (Computer Network Attack – CNA) és a saját hálózatok védelmét (Computer Network Defense – CND) az ellenség informatikai támadásaival szemben. Szorosan együttműködik a vezetési (híradó és informatikai) törzzsel a saját számítógép-hálózatok védelmi rendszabályainak kidolgozásában.

Természetesen az információs műveletek vezetéséért felelős hasonló struktúrájú szervezetet (békében, illetve válság és háború időszakában egyaránt) mind a szárazföldi-, mind a légierő vezérkarnál is létre kell hozni, megfelelően arányos létszámmal.

## 2. Az információs műveletek tervezése

### 2.1. Az információs műveletek tervezésének általános elvei

Az információs műveletek tervezése – az összhaderőnemi-, összfegyvernemi műveletek tervezéséhez hasonlóan – erősen integrált, bonyolult, komplex feladat, hiszen annak minden elemét kell egy fő műveleti csatornába terelni, miközben ezeket nagyon pontosan kell illeszteni a hadműveleti terv konkrét feladataihoz, ütemezéséhez és határidőihez.

Az információs műveletek tervezését koordinálni kell az érintett magasabb-, alárendelt- és szomszédos parancsnokságokkal, és végül integráltan kell elvégezni a hadműveleti tervezés célkitűzéseivel. A műveletek tervezése során különös figyelmet kell fordítani arra, hogy azok szoros szinkronban kerüljenek végrehajtásra az általuk támogatott hadműveleti erőfeszítésekkel és mozzanatokkal.

Hadászati vezetési szinten az információs műveletek tervezése során az elsődleges feladat a műveletek hadászati politikai és katonai célkitűzéseinek, elérendő céljainak és a kívánt végállapot meghatározása. Ezekre alapozva kell a hadműveleti és harcászati információs műveletek tervezésére vonatkozó irányelveket meghatározni és eljuttatni az érintett törzsekhez.

Hadműveleti vezetési szinten a hadászati tervezési irányelvek figyelembe vételével elvégzik az információs műveletek részletes tervezését, koordinálását, majd végrehajtását és értékelését.

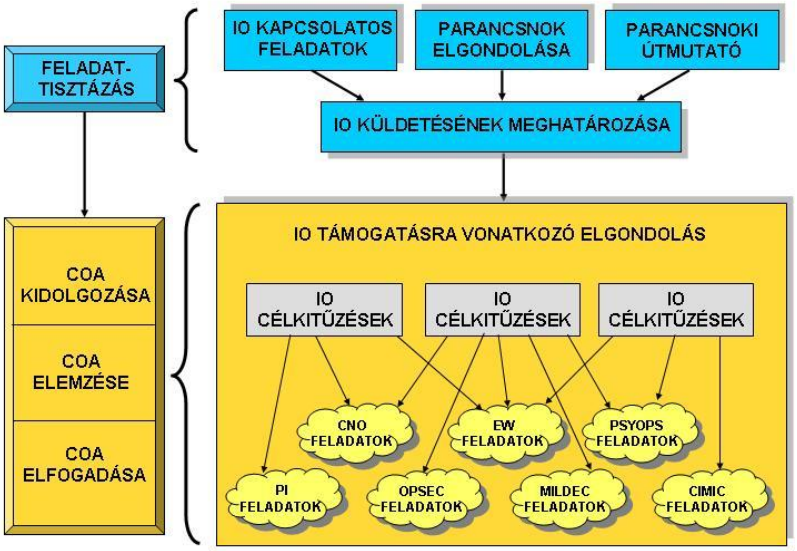
A harcászati vezetési szint felelős a hadműveleti vezetés által meghatározott támadó és védelmi feladatok végrehajtásáért, valamint fontos feladatot hajt végre az információs műveletek eredményességének ellenőrzésében, amelyet megfigyeléssel és csapás utáni felderítéssel old meg. A harcászati szintű parancsnokok főleg katonai információs műveleti képességekkel rendelkeznek, de hozzáférhetnek a helyi polgári közigazgatás és lakossági erőforrásokhoz is, amelyeket eredményesen lehet felhasználni az információs műveletek végrehajtása folyamán.

### 2.2. Az információs műveletek tervezésének folyamata

Az információs műveletek tervezési folyamata szorosan kapcsolódik a katonai művelet tervezési folyamatához. Néhány információs műveleti elem és képesség - úgymint a pszichológiai műveletek, műveleti biztonság, katonai megtévesztés, stb. – hosszantartó tervezést, előkészítést igényel. Egyes feladatok (pl.: felderítés) végrehajtását jóval korábban kell megkezdeni, mint magát a katonai műveletet.

Az információs műveletek tervezésének első lépéseként a parancsnok törzsével megkezdi a kapott feladatok elemzését, és a lehetséges cselekvési változatok (Course of Actions – COA) mérlegelését. Kialakítja saját nagybani elgondolását és az információs műveletek stratégiáját (küldetését), melyekben meghatározza a tevékenységek főerőkifejtésének irányát. Ez a nagybani elgondolás az elhatározás meghozataláig – a törzs elemző munkájának eredményeképpen – még számos finomításon megy keresztül.

A parancsnok az információs műveletek küldetésének meghatározása (Mission Statement), a katonai műveletek információs műveleti támogatására vonatkozó elgondolása (IO Concept of Support), célkitűzései (IO Objectives) és konkrét feladatai (IO Tasks) alapján irányítja az információs műveleteket. (2. ábra) [3]




2. ábra: Az információs műveletekre vonatkozó elgondolás, célkitűzések és feladatok kapcsolatrendszere [3]

Az információs műveletek küldetésének meghatározása röviden leírja, hogy a parancsnok mit vár el az információs műveletek végrehajtásától.

Az információs műveleti támogatására vonatkozó elgondolás tömören de egyértelműen meghatározza, hogy a küldetés sikeres teljesítése érdekében a parancsnok hol, mikor és hogyan kívánja összpontosítani információs képességeit. Az Információs Műveleti Koordinációs Csoport a cselekvési változatok kidolgozása (COA Development) során minden egyes kidolgozott cselekvési változatra kialakítja a katonai művelet információs műveleti támogatására vonatkozó elgondolást.

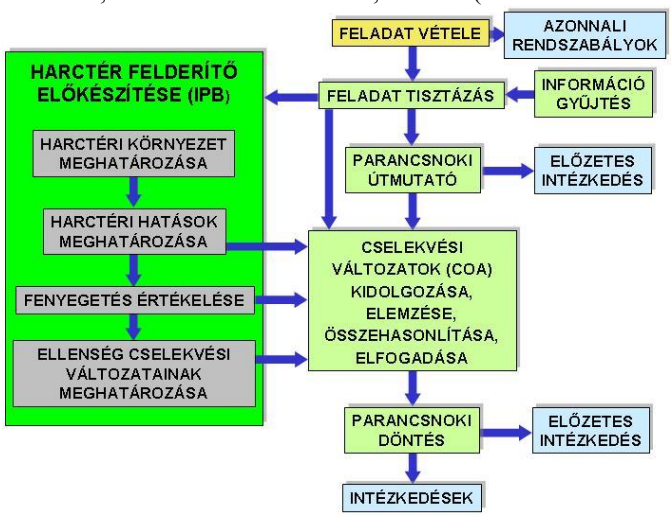
Az információs műveletek célkitűzései egyértelműen meghatározzák azokat a célokat, melyeket a parancsnok az információs műveletek elemei, és képességei alkalmazásával el kíván érni. Ennek kidolgozása során mindazon tényezőkre, feladatokra kell összpontosítani, melyeket végre kell hajtani az információs műveletek küldetésének sikere, illetve a parancsnok szándékának és a katonai műveltre vonatkozó elgondolásának támogatása érdekében.

Az információs műveletek konkrét feladatai mindazon feladatok, melyeket egy, vagy több információs műveleti célkitűzés teljesítésének érdekében kell végrehajtani. Egy konkrét feladat egy információs műveleti elemhez vagy képességhez kapcsolódik (pszichológiai műveletek feladata, elektronikai hadviselés feladata stb.). Az információs műveletek konkrét feladatait a cselekvési változatok kidolgozása során határozzák meg, véglegesítésükre azonban a cselekvési változatok elemzése és elfogadása során kerül sor. [3]

A tervezés során az információs műveleteket számos más tevékenységgel kell integrálni. Így többek között mindig figyelembe kell venni a harcterület általános felderítési tervét és a harctér felderítő előkészítését valamint a céltervezési folyamatot (Targeting Process). Ennek érdekében a felderítő törzs és a tűztámogató elem képviselői aktívan részt vesznek a tervezési folyamatban annak érdekében, hogy az információs műveletek teljes mértékben szinkronban legyenek saját tevékenységeikkel, illetve a teljes katonai művelettel.

Az információs műveletek tervezése – kapcsolódva a hadművelet tervezési folyamatához – az alábbi egymásra épülő fázisokban valósul meg:

- feladat vétele (Receipt of Mission);
- feladat tisztázása (Mission Analysis);
- cselekvési változatok kidolgozása (COA Development);
- cselekvési változatok elemzése (COA Analysis);
- cselekvési változatok összehasonlítása (COA Comparison);
- cselekvési változat elfogadása és jóváhagyása (COA Approval);
- tervek, parancsok, intézkedések elkészítése, kiadása (Orders Production). (3. ábra)




3. ábra: A műveletek tervezésének általános folyamata

A feladat vétele során a parancsnok és törzse megkezdi a kapott feladat előzetes értékelését és különböző azonnali rendszabályokat adhat ki a feladatra való felkészülés érdekében. Ebben a tervezési fázisban az Információs Műveleti Koordinációs Csoport képviselője (általában az információs műveleti főtiszt):

- részt vesz a parancsnok előzetes értékelő tevékenységében;
- megkapja a parancsnok előzetes útmutatóját a feladat végrehajtására;

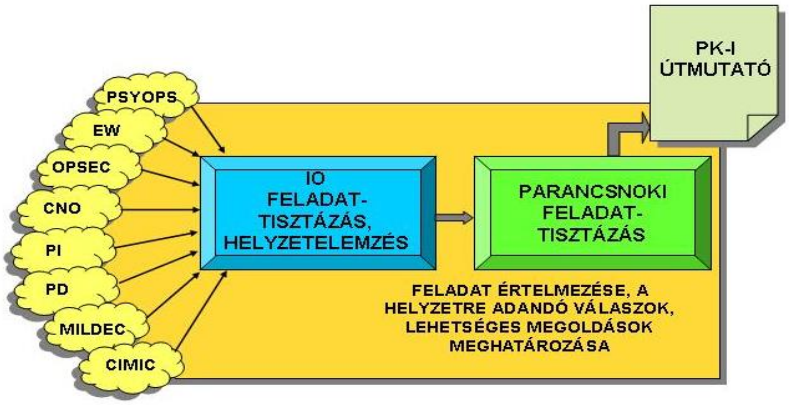
- megkezdi az előzetes információs műveleti értékelést;
- felkészül a tervező munkára.

Béketámogató műveletekben, vagy egyéb helyzetekben, ahol az információ a harcképesség kiemelt elemei közé tartozik, a parancsnok külön az információs műveletekre vonatkozó előzetes útmutatót is kiadhat.

Információs műveletek szempontjából az azonnali rendszabályok az alábbiakat tartalmazhatják:

- az alárendeltek részére előzetesen jóváhagyott feladatok meghatározását, különös tekintettel a katonai megtévesztésre és a pszichológiai műveletekre;
- a kritikus információkat, melyek megkönnyítik a védelmi információs műveletek tervezését, és ami által megkezdődhet a műveletei biztonság tervezésének folyamata;
- az információs műveletekkel kapcsolatos ismert bizonytalansági és kockázati tényezőket;
- a katonai megtévesztésre vonatkozó irányelveket;
- az információs műveleti prioritásokat.

A feladat tisztázása során a törzs elemzi a hadműveleti helyzetet és meghatározza a helyzetre adandó válaszokat és a lehetséges megoldásokat.



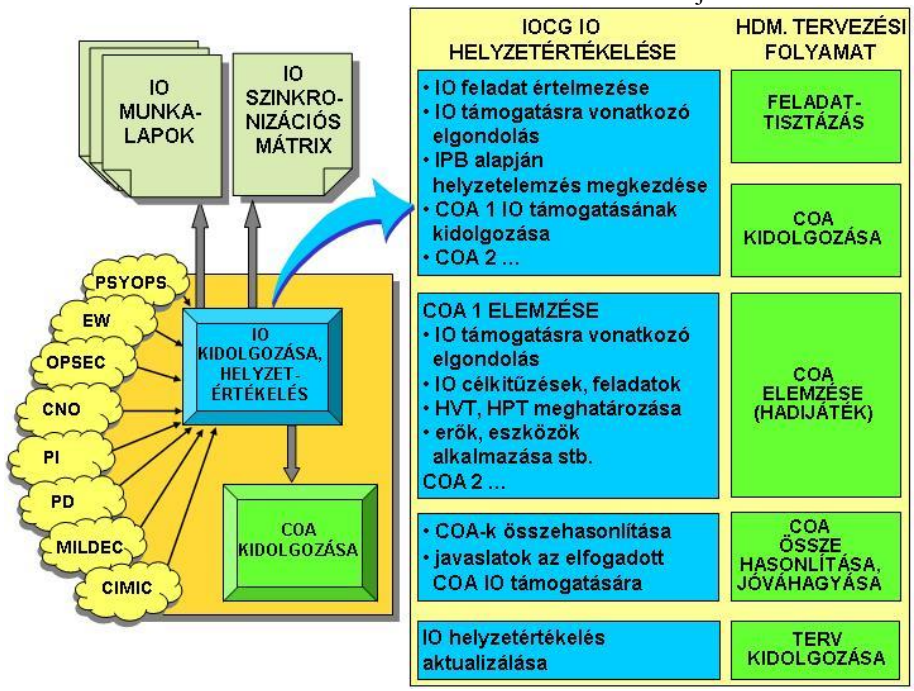

4. ábra: Feladattisztázás és eredménye [3]

E fázisban az Információs Műveleti Koordinációs Csoport megkezdi az információs műveleti helyzetelemzést (Information Operations Estimate). A feladat tisztázása és elemzése során az Információs Műveleti Koordinációs Csoport:

- az információs műveletek szempontjából értelmezi az elöljáró elgondolását, a meghatározott feladatokat;
- részt vesz a harctér felderítő előkészítésében;
- meghatározza és felülvizsgálja az információs műveletekbe bevonható rendelkezésre álló saját és megerősítő eszközöket;
- meghatározza az információs műveletek tervezése és végrehajtása során felmerülő korlátozó tényezőket (pl. amelyek a műveleti biztonságot veszélyeztethetik);
- megkezdi mindazon kockázatok elemzését, melyek kapcsolatba lehetnek a védelmi célú információs műveletekkel, különös tekintettel a műveleti biztonságra;

- meghatározza mindazon kritikus információs igényeket, melyekre a parancsnoknak szüksége van az információs műveletek irányításához;
- meghatározza az információs műveletek tervezésére rendelkezésre időt;
- folytatja az információs műveletek tervezését befolyásoló információk (saját, ellenség, semleges érintettek, harctéri környezet) gyűjtését. (4. ábra)

A cselekvési változatok kidolgozása során az Információs Műveleti Koordinációs Csoport – a harctér felderítő előkészítésének eredményeit felhasználva – folytatja az információs műveleti helyzetértékelést. (5. ábra) Szintén e fázisban kezdődik a céltervezési folyamat, melynek során meghatározzák a nagy értékű- és nagy fontosságú célokat (High Value Target – HVT, High Payoff Target – HPT), valamint az ellenük alkalmazott erőket és eszközöket és azok alkalmazási sorrendjét.




5. ábra: Cselekvési változatok kidolgozása és az információs műveleti helyzetértékelés [3]

Az információs műveleti helyzetelemzés során a szaktörzs elemzi az:

- ellenség információs helyzetét;
- a saját erők információs helyzetét;
- a különböző semleges érintettek (pl. polgári lakosság) helyzetét, és mindezekkel párhuzamosan
- a harctéri környezet, idő, időjárás és egyéb tényezők információs műveletekre gyakorolt hatását.

A helyzetelemzés során – együttműködve a törzs többi elemével – számos cselekvési változat kerül kidolgozásra. A cselekvési változatok számát a harctér felderítő előkészítésének eredményei, vagyis az ellenség várható cselekvési változatainak száma határozza meg. Az információs műveleti helyzetelemzés során valamennyi saját

cselekvési változatra ki kell dolgozni az információs műveleti támogatásra vonatkozó elgondolást.

Ebben a munkafázisban az Információs Műveleti Koordinációs Csoport:

- kidolgozza a különböző cselekvési változatok információs műveleti támogatásának elgondolását;
- meghatározza az információs műveletek céljait;
- fontossági sorrendben meghatározza a támadó és védelmi információs műveletek feladatait;
- meghatározza az információs műveletekben alkalmazható elemek és képességek szerepét és feladatait, valamint az egyes elemeket összehangolja egymással;
- kiválasztja és meghatározza azon nagy fontosságú célokat (HPT), melyeket az információs műveletek sikeres végrehajtása érdekében támadni kell;
- azonosítja a saját erők kritikus információit, a műveleti biztonsági sebezhetőséget és azok védelmét szolgáló műveleti biztonsági intézkedéseket;
- kidolgozza és előkészíti a cselekvési változatoknak megfelelő információs műveleti támogató vázlatokat, mint pl. az információs műveleti szinkronizációs mátrixot (Information Operations Syncronization Matrix) és az információs műveleti munkalapokat (Information Operations Work Sheets).

Az információs műveleti szinkronizációs mátrix minden egyes kidolgozott cselekvési változatban bemutatja minden egyes konkrét feladat végrehajtásának kezdeti időpontját és időtartamát. Megmutatja, hogy mely konkrét feladatok végrehajtása biztosítja az információs műveletek egyes célkitűzésinek elérését. (1. Táblázat)

1. Táblázat: Információs műveleti szinkronizációs mátrix (változat) [2]

| H - 48 | H - 24 | H - 5 | H - 1 | D - NAP<br>H - ÓRA | H + 24 | H + 48 | IO<br>CÉLOK |
|---|---|---|---|---|---|---|---|
| PI-01<br>CIMIC-01<br>OPSEC-01<br>MILDEC-01<br>CND-01<br>PSYOPS-01 | PSYOPS-01 | PD-01 | EW-01 | | | | IO CÉL#1<br>Biztosítani a saját erők műveleti elgondolásának és feladatainak teljesítését |
| PI-02<br>CIMIC-02<br>OPSEC-02<br>MILDEC-02<br>CNO-02<br>PSYOPS-02 | EW-02 | | | | | | IO CÉL#2<br>Megvédeni a saját erők C2 rendszereit |
| PI-03<br>CIMIC-03<br>OPSEC-03<br>MILDEC-03<br>CNO-03<br>PSYOPS-03 | PSYOPS-03 | | EW-03<br>EW-04<br>PD-02<br>PD-03 | | | | IO CÉL#3<br>Megbontani a másik fél ISR és C2 rendszereit |
| EW-05<br>PI-03<br>CIMIC-03<br>OPSEC-03<br>MILDEC-03<br>CNO-03<br>PSYOPS-04 | | | | | | | IO CÉL#4<br>Minimalizálni a polgári zavargásokat |

Ez az okmány a tervezés utolsó szakaszában a cselekvési változat elfogadását és jóváhagyását követően a kidolgozandó terv részét képező információs műveleti mátrix (Information Operations Matrix) alapját képezi. [3]

A cselekvési változatok elemzése során hadijáték módszerével (War-Gaming) elemzik, és meghatározzák, hogy – a legkisebb veszteség mellett – melyik cselekvési változat végrehajtása eredményezi a legnagyobb sikert.

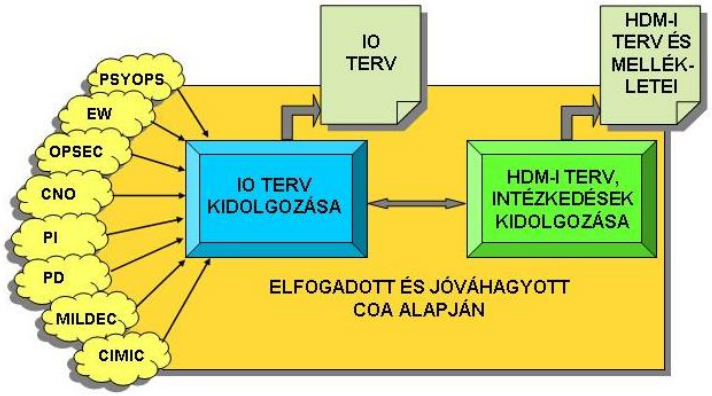
Az Információs Műveleti Koordinációs Csoport az elemzés során alkalmazhatja az előzőekben kidolgozott különböző információs műveleti munkalapokat, melyek tartalmazzák a cselekvési változatok számát, a katonai művelet információs műveleti támogatásra vonatkozó elgondolását, az információs műveletek célkitűzéseit, valamint meghatározzák az információs műveletek elemei és képességei szerinti bontásban, hogy ki, mit, milyen célból, hol és mikor fog végrehajtani.

A cselekvési változatok elemzése során az Információs Műveleti Koordinációs Csoport:

- kidolgozza minden egyes cselekvési változat információs műveleti értékelési kritériumait;
- összehangolja az információs műveleti feladatokat a különböző elemek tevékenységével;
- beintegrálja az információs műveleti támogatására vonatkozó elgondolást minden egyes cselekvési változat hadműveleti elgondolásába;
- meghatározza az ellenség információs műveleti képességeit és várható tevékenységeit;
- hadijáték módszerével modellezi a saját információs műveleti támadó képességeket az ellenség információs rendszereivel szemben;
- pontosítja a nagyfontosságú célok listáját, összehangolja a támadó képességekkel és elosztja a célokat a csapást végrehajtók számára;
- elemzi, hogy a hadijáték során cselekvési változatokban történt változások menynyiben vannak hatással a saját kritikus információkra, műveleti biztonsági sebezhetőségre, és amennyiben igen, javaslatokat tesz a megváltozott műveleti biztonsági intézkedésekre, rendszabályokra.

A cselekvési változatok összehasonlítása, majd elfogadása, jóváhagyása fázisokban a kidolgozott és elemzett változatokat a törzs különböző szempontok szerint összeveti egymással annak érdekében, hogy megállapítsa, melyik biztosítja a legnagyobb valószínűséggel a siker elérését. Az összehasonlítás során mindegyik változatnak meghatározzák előnyeit és hátrányait. Az Információs Műveleti Koordinációs Csoport ennek során azt vizsgálja, hogy a hadijáték alapú elemzés során melyik cselekvési változat támogatható a leghatékonyabban az információs műveletekkel.

Az összehasonlítást követően a törzs sorrendet határoz meg a cselekvési változatok között, és javaslatot tesz a parancsnoknak a legkedvezőbb változat elfogadására. A parancsnoki döntést követően a véglegesített hadműveleti elgondolást a parancsnok rendszerint felterjeszti az elöljárónak, majd annak jóváhagyását követően a törzs megkezdi a Hadműveleti Terv kidolgozását és a harcparancs elkészítését. Az Információs Műveleti Koordinációs Csoport is ezt követően már csak az elfogadott változatra dolgozza ki az információs műveletek vezetésére szolgáló okmányokat. (6. ábra)




6. ábra Tervek, okmányok kidolgozása [3]

### 2.3. A céltervezés folyamata

A céltervezés a hadműveletek tervezésének lényeges része, egy logikus folyamat, amely összehangolja a halálos és nem-halálos csapásokat az egyéb harctéri hadműveleti rendszerek hatásaival. A parancsnok céltervezési útmutatója és célkitűzései alapján a céltervező csoport meghatározza, hogy mely célpontokat hol, hogyan és mikor kell támadni. E folyamat során az ellenséges célpontokhoz hozzárendelik azokat a legalkalmasabb ellentevékenységi rendszereket, amelyek a kívánt hatás eléréséhez legmegfelelőbbek. Az Információs Műveleti Koordinációs Csoport folyamatosan részt vesz a céltervező csoport munkájában, javaslatokat tesz az információs műveletek célpontjaira és beintegrálja az információs műveletek sajátos tényezőit a céltervezési folyamatba. A céltervezés támogatja mind a támadó, mind védelmi jellegű információs műveleteket. Természetesen a céltervezési folyamatnak a támadó jellegű tevékenységekre van nagyobb hatása.

Az információs műveletekkel összefüggő céltervezéssel kapcsolatban az információs műveletek célpontjai a következő fajtájúak lehetnek:

- fizikai célpontok (Physical Target), melyek lehetnek állandóhelyűek vagy mobil célpontok, és melyeket gyakran „hardware” célpontoknak (Hardware Targets) is neveznek;
- információs célpontok (Information Target), melyek lehetnek pl. kommunikációs központok közötti összeköttetési vonalak, számítógép-hálózati kapcsolatok, stb. és melyeket gyakran „software”, vagy elektronikai célpontoknak (Software Targets, Electronic Targets) is neveznek;
- tudati célpontok (Perception Target), melyek az ellenfél döntéshozóinak gondolkodásával kapcsolatban levő, tudatos döntéshozatalt befolyásolni képes célpontok, és amelyeket gyakran „wetware” célpontoknak is neveznek (politikai és katonai vezetők, döntéshozók, vagy katonai, illetve lakossági célcsoportok).

A céltervezési folyamat négy azonos fontosságú feladat végrehajtásán alapul, úgymint:

- döntési folyamat;
- célok felderítése és pontosítása;
- célok szétosztása és a

- csapások eredményeinek felmérése.

A döntési folyamat párhuzamosan folyik a tervezési folyamattal. A célok felderítése és pontosítása az előkészítés és végrehajtás időszakában zajlik. A célok szétosztása elsősorban a feladat végrehajtása során jelentkezik, azonban néhány információs műveleti célpont lefogása már a katonai művelet tervezésének időszakában is megtörténhet. Ennél fogva a csapások eredményeinek értékelése folyamatosan zajlik, de legintenzívebb a végrehajtás időszakában. (2. táblázat)

2. táblázat: A céltervezés folyamata [2]

| MŰVELETEK FOLYAMATA, TEVÉKENYSÉGEK | | CÉLTERVEZÉSI FOLYAMAT ELEMEI | CÉLTERVEZÉSI FELADATOK |
|---|---|---|---|
| Értékelés | Tervezés | Döntési folyamat | Feladattisztázás:<br>▪ HVT-k kidolgozása;<br>▪ IO bemeneti adatok a céltervezéshez.<br>Cselekvési változatok kidolgozása:<br>▪ potenciális IO HPT-k meghatározása;<br>▪ közreműködés a célérték elemzésben.<br>Cselekvési változatok elemzése, összevetése:<br>▪ nagy fontosságú célok listája (HPTL);<br>▪ csapásmérési útmutató mátrix (AGM);<br>▪ célpont szinkronizációs mátrix (TSM);<br>harctéri csapások értékelés követelményeinek meghatározása |
| | Előkészítés Végre-hajtás | Célok felderítése és pontosítása | ▪ Adatgyűjtési terv végrehajtása<br>▪ Felderítési követelmények pontosítása<br>HPTL és AGM pontosítása |
| | | Célok elosztása | Csapások végrehajtása az AGM szerint |
| | | Csapások eredményeinek felmérése | ▪ Csapások hatásainak elemzése<br>Nem-halálos IO csapások eredményeinek figyelése |

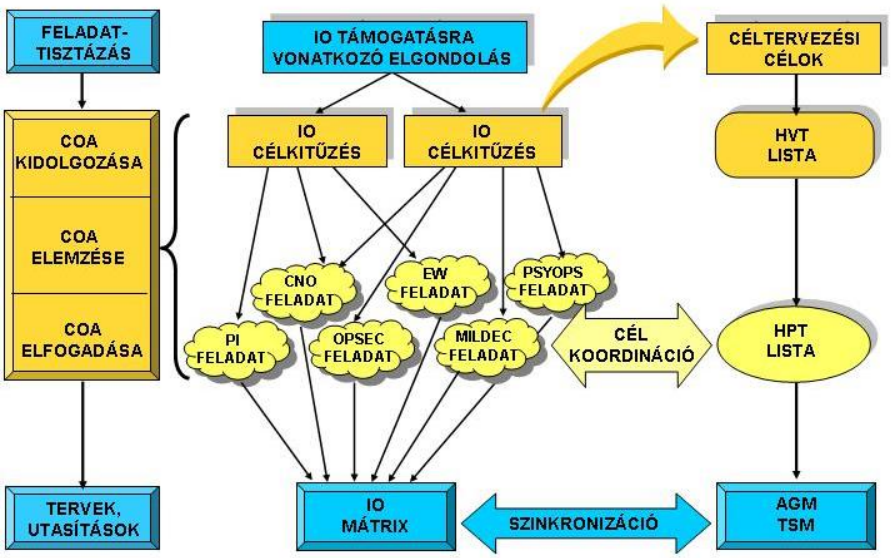
A céltervezési folyamat egy ciklikusan ismétlődő tevékenység, melynek gyakoriságát a hadművelet végrehajtásának üteme határozza meg. E tevékenység során az Információs Műveleti Koordinációs Csoport az információs műveletek tervezésével párhuzamosan végzi a céltervezést.

A döntési folyamat során a céltervező csoport a felderítési adatgyűjtés és csapásmérés tervezésére összpontosít. A parancsnok hadműveletre vonatkozó elgondolása

alapján a céltervező csoport a hadművelet minden egyes kritikus fázisaira céltervezési prioritásokat határoz meg. A feladattisztázás és a cselekvési változatok kidolgozása során az Információs Műveleti Koordinációs Csoport meghatározza az információs műveletek nagy értékű célpontjait (HVT), a célokkal és feladatokkal összhangban kidolgozza a nagy fontosságú célpontokat (HPT). A nagy fontosságú célpontok kiválasztására a cselekvési változások során kerül sor.

A hadijáték alapú cselekvési változatok elemzése után a céltervező csoport minden egyes cselekvési változatra kidolgozza:

- a nagy fontosságú célok listáját (HPT List – HPTL);
- a csapásmérési útmutató mátrixot (Attack Guidance Matrix – AGM) és
- a célpont szinkronizációs mátrixot (Target Synchronization Matrix – TSM). (7. ábra)




7. ábra: Információs műveleti célpontok tervezése [2]

A nagy fontosságú célok listája a célpontok prioritási sorrend szerinti felsorolása, amely a hadművelet minden fázisára tartalmazza azokat. A listában a célpontok célérték, megjelenési sorrend, fontosság és egyéb kritériumok alapján vannak felsorolva.

A csapásmérési útmutató mátrixban mind a halálos, mind pedig a nem-halálos pusztító képességek is felsorolásra kerülnek, így pl. a pszichológiai műveletek és elektronikai hadviselés. Ennek érdekében képesség elemzést kell végezni, melynek során – a kívánt hatás elérése érdekében – szinkronba hozzák a rendelkezésre álló fegyverek, fegyverrendszerek és egyéb ellentevékenységi eszközök mennyiségét, típusát és hatásait a nagy fontosságú célpontokkal. Gondosan felmérik és összehasonlítják a célpont sebezhetőségét, a tervezett fegyver és eszköz várható hatásait, a találati pontosságot, a csapás körülményeit, az időjárási viszonyokat, a célpont védettségének minőségét és a tervezett eredményeket. A képesség elemzést mind a halálos hatású,

mind pedig a nem-halálos hatású fegyverek, eszközök alkalmazása esetén egyaránt el kell végezni.

A célpont szinkronizációs mátrix kategóriánként felsorolja a nagy fontosságú célpontokat és mindazon képességeket, amelyek azok felfedésében, elhelyezkedésük pontosításában, támadásukban és a csapások eredményeinek értékelésében szerepet kapnak. Ez az okmány a nagy fontosságú célok listájának, a felderítőadat gyűjtési tervnek (Intelligence Collection Plan – ICP) és a csapásmérési útmutató mátrixnak az adatait összesíti. A céltervező csoport minden egyes cselekvési változatra kidolgozhat célpont szinkronizációs mátrixot, vagy az előbbiekben említett három okmány (HPTL, ICP, AGM) felhasználásával csak az elfogadott cselekvési változatra készíti el azt.

A célok felfedése és pontosítása – mint a céltervezési folyamat következő fázisa – magába foglalja a nagy fontosságú célpontok pontos helymeghatározását, amely elengedhetetlen a hatékony támadásokhoz. E tevékenység alapvetően a felderítőadat gyűjtési terv végrehajtását jelenti, amelynek ellenőrzését a felderítő törzs végzi. A célok felfedésében és pontosításában nem csak a felderítő törzs felügyelete alá tartozó erők és eszközök vesznek részt. Minden egyes törzs, így az Információs Műveleti Koordinációs Csoport is a hatáskörébe tartozó erőkkel és eszközökkel részt vesz e tevékenységben, és a megszerzett információkat átadja a felderítő törzsnek. Ez viszont is érvényes, vagyis a felderítő törzs által megszerzett információk, amelyek az információs műveletek célpontjaira vonatkoznak, átadásra kerülnek az információs műveleti szaktörzs részére. Ez az információ megosztás lehetővé teszi a csapások eredményességének időbeli értékelését, az információs műveletek hatékonyságának meghatározását és új célpontok kidolgozását.

A célok szétosztása időszakában kerül sor a nagy fontosságú célpontok elleni tevékenységre a csapásmérési útmutató mátrix és a cél szinkronizációs mátrix szerint. Mivel az összes nagy fontosságú célpont azonosítása és helyének meghatározása nem lehetséges, ezért a végrehajtás során folyamatosan követik és pontosítják a célok helyzetét, és ennek megfelelően a célok prioritását – ha szükséges – megváltoztatják.

A csapások eredményeinek felmérése a teljes katonai művelet során folyamatos. Az információs műveletek célpontjaira mért halálos csapások eredményességének felmérése megegyezik más tűztámogató tevékenységek vagy elektronikai csapások eredményeinek felmérésével. A csapások eredményességének felmérését elsődlegesen képi felderítési információk alapján végzik, amikor azt értékelik, hogy a felhasznált fegyver eltalálta-e vagy sem a kijelölt célpontot. Ez kiegészül további hírszerzési információkkal, amikor is megállapítják, hogy a célpont még folytat-e aktív tevékenységet, vagy már nem működik. Ezen kívül arra keresik a választ, hogy a csapásmérés milyen hatást váltott ki a célpont rendszeri környezetében és kapcsolódásaiban.

Az információs műveletek célpontjaira irányuló nem-halálos csapások eredményességének felmérését is folyamatosan kell végezni. Az információs műveletek egyes tevékenységei (pl. pszichológiai műveletek, elektronikai támogató tevékenység, polgári-katonai kapcsolatok, stb.) hatékonyan képesek információkat gyűjteni a nem-halálos csapások eredményeinek kimeneteléről. Ezen értékelés eredményeképpen az Információs Műveleti Koordinációs Csoportnak lehetősége van dönteni arról, hogy folytatja a meghatározott célpontok lefogását, beszünteti azok támadását, vagy a célok lefogásába más információs műveleti elemeket von be.

A céltervezés során a fent említetteken kívül az alábbi okmányokat (listákat, jegyzékeket célszerű kidolgozni és folyamatosan karbantartani:

- tiltott célpontok jegyzéke (Prohibited Target List – PTL), amely olyan célpontokat tartalmaz, amelyeket tilos támadni (pl.: templomok, kórházak, iskolák vagy más kiemelt fontosságú építmények, körzetek, stb.);
- korlátozott célok jegyzéke (Restricted Target List – RTL), amely olyan célpontokat tartalmaz, amelyeket csak külön engedéllyel lehet támadni, mivel a saját csapatok későbbiek folyamán felhasználásra tervezik az építményt, vagy szolgáltatást (pl. állandóhelyű hírközpontok, egyes közúti hidak, TV és műsorszóró állomások, stúdiók, stb.);
- korlátozott frekvenciák jegyzéke (Restricted Frequency List – RFL), amely a saját elektronikai eszközök azon fontos frekvenciáit tartalmazza, melyeken elektronikai ellentevékenység folytatása tilos, vagy csak korlátozottan alkalmazható. [3]

## 2.4. Az információs műveletek vezetésének okmányai

Az információs műveletek vezetésének számos okmánya van, amelyek közül elsősorban az állandó jellegű – mindenütt megtalálható – okmányokat sorolom fel. Ezek az okmányok a NATO feladatokkal összhangban további okmányokkal egészíthetők ki a vezetés hatékonyságának növelése érdekében. Az információs műveletek tervezése során kidolgozandó munkaokmányokat az előzőekben ismertettem, itt külön már nem térek ki rájuk.

A katonai műveletek tervezése során a parancsnoki döntést követően (cselekvési változat elfogadása és jóváhagyása) hadműveleti törzs megkezdi a hadművelet tervének kidolgozását. A Hadműveleti Terv egy olyan integrált vezetési okmány, amelyben valamennyi résztvevő feladata, ütemterve megtalálható. A Hadműveleti Terv mellékletét képezi az Információs Műveleti Terv, amelynek alapján a parancsnok információs műveleti főtisztje koordinálja az információs műveletek erőfeszítéseit. Az Információs Műveleti Terv az információs műveletek vezetésének alapvető okmánya, mely:

- meghatározza, hogy az információs műveletek hogyan tud közreműködni a katonai művelet sikeres végrehajtásában;
- a kidolgozott információs műveleti feladatokat hozzárendeli azokhoz az elemekhez, melyek felelősek azok végrehajtásáért;
- szinkronizálja a konkrét feladatok végrehajtását, amely funkciót az információs műveleti mátrix tartalmazza. (3. táblázat)

Az Információs Műveleti Terv elkészítése során figyelemmel kell lenni arra, hogy az információs műveletek, azok fázisai, feladatai szorosan illeszkedjenek a Hadműveleti Terv fő feladataihoz, fázisaihoz, mivel azok támogatását szolgálják.

Az Információs Műveleti Terv grafikus és szöveges részből áll, és egy változatban az alábbiakat tartalmazhatja:

- a kialakult helyzet értékelését, ezen belül:
- az ellenség helyzetének elemzését (vezetési folyamatok, információs infrastruktúrák, távközlési és információs hálózatok, adatbázisok, információs műveleti képességek, stb.);
- a sajt erők helyzetének elemzését (információs műveleti erőforrások, azok képességei, korlátai; vezetési csomópontok, információs rendszerek, illetve azok sebezhetősége) és

- a harctéri környezet (az információs műveletek megvívását elősegítő vagy hátráltató terep, időtényezők, időjárás, stb.) elemzését;
- az információs műveletek küldetésének meghatározását;
- a információs műveletek végrehajtásának tervét (az információs műveletek megvívására vonatkozó elgondolás, fő célkitűzések, támadó és védelmi információs műveletek konkrét feladatai, az információs műveletek elemeinek és képességeinek összehangolása, stb.);
- a vezetés, együttműködés feladatait (ki, honnan, hogyan vezeti az információs műveleteket, kivel kell folyamatos együttműködést fenntartani, stb.).

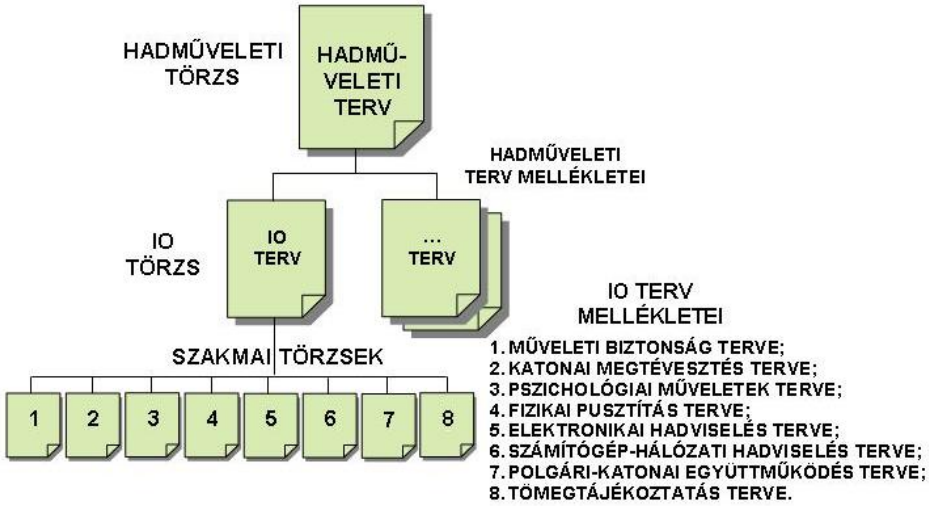
3. táblázat: Információs műveleti mátrix tartalma [2]

| Információs Műveleti Terv Függelék (Információs műveleti mátrix) | | | | |
|---|---|---|---|---|
| Végrehajtó | IO feladat | Idő | Elhelyezkedés | Megjegyzés |
| Egység megnevezése<br>Felderítő rendszer<br>Csapásmérő rendszer<br>stb. | Az IO elemeinek megfelelően a végrehajtandó feladatok felsorolása | Végrehajtás kezdete, időtartama | Célpont megnevezése, helyzete, koordinátája (ha ismert) | |
| Speciális intézkedések, utasítások | | | | |

A hadászati szintű információs műveletek kapcsán – melyben kormányzati, nem kormányzati, és más szervek, intézmények, esetenként vállalatok is részt vesznek – a tervben ki kell térni azok alkalmazására is.

Az Információs Műveleti Tervnek egyrészt részét képezik a már említett munkaokmányok egyes fajtái (pl.: IO mátrix), másrészt pedig azok a mellékletek, amelyek az információs műveletek résztevékenységeinek terveit tartalmazzák. (8. ábra).

Az információs műveletek elemeinek szaktörzsei a kapott tájékoztatások és parancsok alapján készítik el saját szakterveiket, és azokat egyeztetik. Ezek a tervek annyiban térnek el az Információs Műveleti Tervtől, hogy saját szakfeladataikra koncentrálnak, és részletekre menően lebontják a támadó és védő fajtájú információs műveletek rájuk háruló feladatait.




8. ábra. Az információs műveletek vezetési okmányai

## Összegzés

Napjainkra az információs műveletek a korszerű katonai műveletek szerves részévé vált mind a háborús, mind pedig a nem háborús katonai műveletekben. A Magyar Honvédségnek is fel kell készülnie azokra az új kihívásokra, melyek a katonai műveletek információs dimenziójából érkeznek. Ennek egyik fontos lépése, ha megteremtjük a szervezeti kereteit egy olyan törzsnek, amely képes e szerteágazó terület összefogására, a különböző típusú információs tevékenységek koordinálására. A bemutatott törzs és az információs műveletek tervezési folyamata figyelembe véve a Magyar Honvédség feladatait és sajátosságait megfelelően adaptálható annak béke és minősített időszaki vezetési rendszerébe.

## Felhasznált irodalom

[16] Védelmi Felülvizsgálat. Úton a XXI. Század hadserege felé. http://honvedelem.hu/cikk.php?cikk=13776
[17] Joint Information Operations Planning Handbook. Joint Forces Staff College, National Defense University, Norfolk,Virginia. 2002
[18] FM 3-13 Information Operations: Doctrine, Tactics, Techniques, and Procedures. Headquarters, Department of the Army, Washington, DC. 2003

**HÓKA Miklós, HORVÁTH Attila**

# A BÉKETÁMOGATÓ ÉS VÁLSÁGREAGÁLÓ MŰVELETEK HÍRADÁSA – ITTHONI SZEMMEL

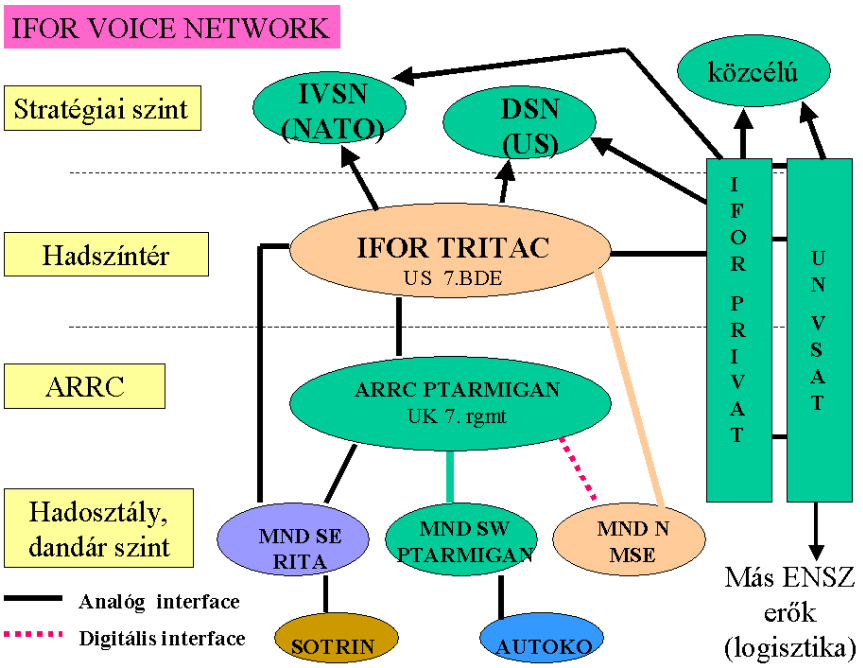
A béketámogató műveletek híradásával kapcsolatosan 1993-ban megtartott munkaértekezleten elfogadott javaslatok eredményeként az Észak-Atlanti Együttműködési Tanácsnak (North Atlantic Cooperation Council - NACC) a békefenntartás területén történő együttműködést koordináló ad-hoc bizottsága (Ad Hoc Group on Cooparation in Peacekeeping - AHG) 1993 novemberében megalakította a Híradó Szakértői Csoportot (Expert Group on Communications - EGC), amely Csoport a vizsgálatok alapján a következő fontos megállapításokat tette [1]:

- a békefenntartó műveletek mérete jelentős mértékben kihat a híradás koncepciójára,
- a békefenntartó műveletek mérete és vezetésének szintje határozza meg a szükséges híradás kapacitását.

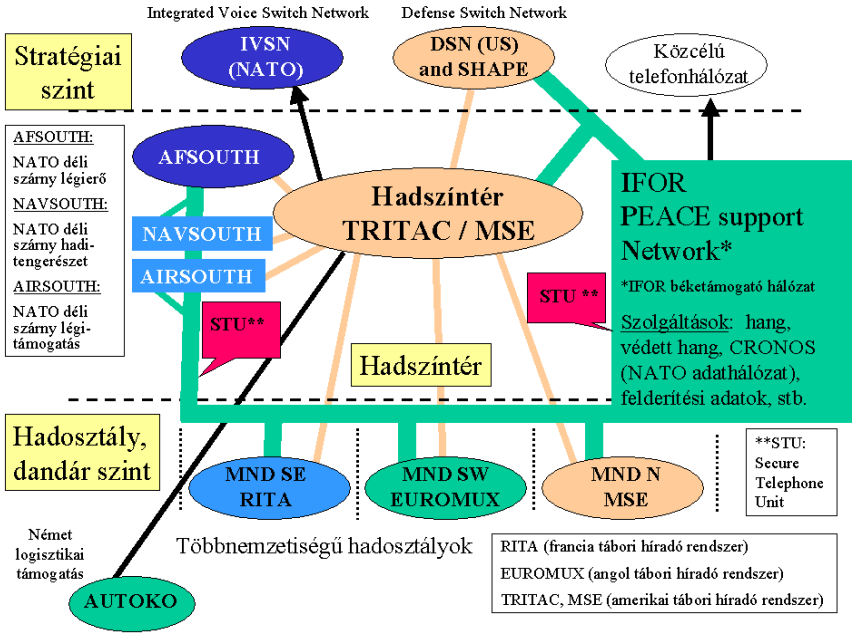
A fentieken túlmenően figyelembe kell venni, hogy a béketámogató műveletek többnemzetiségi jellege jelentősen befolyásolja a vezetési-irányítási (C2) szervezet kialakítását, valamint azt a tényt, hogy az ilyen műveletek általában a politikai, katonai és civil tevékenységek olyan sajátos, előre meg sem határozható keverékét tartalmazzák, melyek mindegyike hatékony koordinációt és integrációt igényel a vezetés valamennyi szintjén.

A korszerű híradó és informatikai rendszerek lehetőséget biztosítanak a béketámogató műveletek parancsnoka számára egy, a teljes alkalmazási területet behálózó, megbízható, sokcsatornás, bármilyen típusú adat gyors továbbítására alkalmas hírhálózat létrehozására. Egy jelentős nagyságú területen megvalósuló béketámogató művelettel összefüggésben várhatóan jelentkező nagy kiterjedésű, bonyolult és összetett híradó feladatok alapján valószínűsíthető, hogy a hadszíntér teljes területét, a hátországi és csatlakozó irányokat is lefedő hírrendszer létesítésére - a korábbi gyakorlattal ellentétben - a továbbiakban egyetlen ország híradó szolgálata sem vállalkozhat önállóan. Ezen túlmenően is szükséges a hadszíntéren fellelhető infrastrukturális források felhasználása mind az alkalmazási területen belül, mind pedig a katonai és a politikai felső szintű vezetési szervek C2 hierarchia szerinti csatlakoztatásához. A számítások szerint egy nagyobb területre kiterjedő béketámogató művelet során egy jelentősebb erőforrásokkal bíró szervezet, mint például a NATO, biztosítja a hadszíntéri híradás alaphálózatát és a fő csatlakozási lehetőségeket, és az így létesített vázat, rendszert lehet más, nemzeti források felhasználásával továbbfejleszteni.

A hírrendszer kialakításának talán a legmegfelelőbb módja a moduláris felfogás, vagyis elsőként a rendszer alapvető elemeit („építőkockákat") kell megtervezni, majd ezt követően szükséges meghatározni az erre igénybe vehető forrásokat. Ezt az elvet követve került kialakításra például az IFOR alaphíradása, míg az SFOR feladatra ez átalakult.




1. ábra: IFOR Voice Network (1995. jan. – 1996. márc.)




2. ábra: SFOR Integrált Hálózat (1996. ápr. – 2002. márc.)

## A béketámogató és válságreagáló műveletek

A „béketámogató műveletek” szakkifejezést a leggyakrabban olyan értelemben használjuk, amely lefedi a tevékenységek széles skáláját, beleértve a konfliktus megelőzést, béketeremtést, békefenntartást, béke kikényszerítést, békeépítést és a humanitárius segítséget adó feladatokat.[2]

Válságreagáló művelet alatt olyan tevékenységet értünk, mely során a katonai képességeket a hagyományos értelemben vett hadszíntéri műveletektől eltérő céllal alkalmazzák, olyan helyzetben, amikor a békés körülményeket egy lehetséges összecsapás, vagy konfliktus veszélye fenyegeti. Ilyen helyzetekben a béke helyreállítására vagy a helyzet stabilizálására – ha lehetséges, akkor a fegyveres beavatkozást kerülve – katonai erőt alkalmaznak. [3]

A nemzetközi szervezetek által irányított válságreagáló és béketámogató műveletekben történő részvétellel kapcsolatos feladatok végrehajtásának részletes szabályairól a Honvédelmi Minisztérium közigazgatási államtitkárának és a Honvéd Vezérkar főnökének együttes intézkedés (a publikáció írásának idején csak tervezet) került kidolgozásra.

Az intézkedés szerint új felkérések, vagy új hazai vállalási kezdeményezések, továbbá a már folyamatban lévő missziókban a magyar szerepvállalást jelentősen befolyásoló változások esetén vizsgálat kerül végrehajtásra. A vizsgálat során különösen a nemzetközi politikai hátteret, a nemzeti érdekeket és a nemzetközi jogi hátteret kell értékelni a művelet indítását elhatározó nemzetközi szervezetben betöltött tagságunk és más meglévő nemzetközi elkötelezettségünk összefüggésében. A vizsgálat alapján javaslattétel kerül kidolgozásra, amelyet a nemzeti érdekek, a kockázati tényezők, valamint a rendelkezésre álló humánerőforrások és pénzügyi források figyelembevételével teszik meg, minden esetben jelezve az alternatív döntési lehetőségeket az országgyűlés felé.

## Békeműveletek híradásának magyar vonatkozásai

A Magyar Köztársaság, és ezen belül az MH szerepvállalása a délszláv válság rendezésében elsőként az IFOR feladat kapcsán jelentkezett. Az évtized közepén megjelenő IFOR békeépítő feladatokhoz csatlakozó Magyar Műszaki Kontingens a meglévő híradóeszközökkel került vezénylésre: R-142 rádióállomás, ennek BTR-60 páncélozott harcjárműbe épített változata, az R-145, kiegészítve a felhasználóbarát automatikákkal ellátott, Videoton gyártmányú R-1340 RH rádiókészülékkel (az R-130 utódja), illetve a BTR-80 páncélozott harcjárművekbe is ez a típus került beépítésre. Személyi rádióként Motorola MT-300 típusú többcsatornás kézirádiókat alkalmaztak, némely esetben kiegészítve az R-159 hátirádiókkal a feladatvégzésekben. A szolgálati távbeszélő viszonylatok ALCATEL digitális központban végződtek, a Horvát Telecom-hoz való csatlakozással. A műholdas híradás viszonylatában az INMARSAT M és C típusú műholdas terminálokat használták: az M típus hordozható, kézitáskás változat, beszéd- és faxátvitelre alkalmazva, míg a C típus gépjárműbe épített, menetközbeni kommunikációra képes változat volt, elsősorban adatátviteli kapacitással felvértezve.

Az SFOR feladat befejezése után, az Okucaniban állomásozó Magyar Műszaki Kontingens kivonásra került a térségből, viszont a szarajevói főparancsnokság védelmére egy magyar őrző-védő század került felállításra, amely napjainkban is ott teljesít szolgálatot. A koszovói válság rendezésében résztvevő magyar kontingens

Pristinában állomásozik, és ott lát el őrző-védő, illetve járőrözési feladatokat; mindkét alegységünk hasonló eszközökkel rendelkezik, mint az IFOR-SFOR feladatban résztvevő Műszaki Kontingens, kiegészítve műholdas eszközökkel.

Napjainkban a szarajevói katonai rendfenntartó kontingens (KRK); a koszovói őr- és biztosító zászlóalj, az iraki szállító zászlóalj; az afganisztáni Nemzetközi Biztonsági Közreműködő Erő (International Security Assistance Force, ISAF) kötelékében szolgálatot teljesítő magyar egységek; valamint a NATO reagáló erőkhöz (NATO Reaction Force, NRF) beosztott egységeink már el vannak látva a következő táblázat szerinti IRIDIUM és INMARSAT mini-M műholdas telefonokkal.

| | KRK Szarajevó | KFOR Pristina | MH SZZ* Irak | NRF** | ISAF | |
|---|---|---|---|---|---|---|
| | | | | | Törzstiszti csoport | KGYSZD |
| IRIDIUM műholdas telefon | - | - | 15 db | 1 | - | 16 db |
| INMARSAT műholdas telefon | 7 db | 7 db | 8 db | 1 | 2 db | 2 |
| *: A kontingens befejezte feladatát, eszközeit 2005. augusztusában leadta. Az új Kiképzésbiztosító Század híradása szervezés alatt.<br>**: NRF-5 váltás végrehajtó elemeinek híradása a konkrét feladatnak megfelelően kerül megszervezésre, a fenti eszközök a központgépjárműbe kerülnek beépítésre. | | | | | | |

1. táblázat: Műholdas telefonok békeműveletekben, 2005. (Forrás:[4])

| Felhasználás viszonylata | | *KFOR* Pristina – HM II. | *MH SZZ* Al-Hillah – HM II. | *MH KGYSZD* Kabul – HM II. |
|---|---|---|---|---|
| Szolgáltatás | Hangátvitel (HICOM bontja le) | 8 db tömörített hangcsatorna (8x8 kbps) | 8 db tömörített hangcsatorna; 1 db tömörítetlen hangcsatorna (8x8 kbps és 1x64 kbps) | 5 db tömörített hangcsatorna* |
| | Adatátvitel (ideértve az Internet, Intranet, IP-telefon és videotelekonferencia-adatforgalmat) | - (terv 192 kbps, az ETHERNET kiépítés alatt) | 320 kbps (ETHERNET) Ebből 192 kbps dedikált adatátviteli kapacitás, 128 kbps igény szerint IP-telefon forgalomra használható | 256 kbps (ETHERNET) |
| Összkapacitás | | 64 kbps | 442 kbps | 352 kbps |
| * Az afganisztáni misszióban 3 hangcsatornát Panasonic kisközpont bont le analóg végződéssel, 2 közvetlenül készüléken végződik | | | | |

2. táblázat: VSAT szolgáltatások külföldi missziók felé, 2004. (Forrás: [4])

Ugyancsak békeműveletekben kerülhet alkalmazásra a civil/üzleti műholdak adatátviteli kapacitásának kihasználása. Az MH békeműveleteinek kommunikációs támogatásában is megjelenik ez a lehetőség, VSAT csatornák bérlése formájában, amit a 2. táblázatban foglalok össze.

A szolgáltatások alapvetően adatátvitelt biztosítanak, de a rugalmas csatornakezelés lehetővé teszi a digitális hangátvitelt, az internet telefont (Voice over IP,

VoIP), és a videotelekonferencia kapcsolatokat is, a szolgáltatótól történő megrendelés után. Felkészülve a jövő békeműveleteire, továbbra is kiemelt figyelmet célszerű fordítani a műholdas rendszerekhez való hozzáférések biztosítására, mivel ez a műveleti forma várhatóan egyre gyakoribb lesz az MH feladatai között.

## A béketámogató és válságreagáló műveletek hazai kommunikációs felkészítése

A béketámogató és válságreagáló műveletbe bevont MH erők hazai felkészítésének koordinálását és a célfelkészítés végrehajtásának szakmai felügyeletével kapcsolatos feladatokat – a felkészítésért felelős szervezettől függetlenül – a HM HVK Műveleti Főcsoportfőnökség végzi. A gyakorlati felkészítés több helyszínen történik, a híradó felkészítést az MH 43. Vezetésbiztosító zászlóalj (rádiós kiképzés), valamint – az MH SZFP felkérése alapján – az MH Híradó Parancsnokság végzi (műholdas és informatikai kiképzés).

2005. első negyedévében – a politikai döntésnek megfelelően – került felállításra az Iraki Kiképzést Biztosító Század (MH IKBSZD), amely alegység híradó és informatikai szakemberei felkészítése során oktatásra kerültek az Inmarsat, az Iridium és a VSAT technikai eszközök használata, valamint a konténerbe épített HICOM központ (a 2004 decemberében Irakból kivont szállító zászlóalj eszköze) telepítési, konfigurálási és üzemeltetési tudnivalói.

| Kontingens | | MH IKBSZD | ISAF váltás | KFOR váltás | NRF-6 váltás | MH ÖBSZ váltás |
|---|---|---|---|---|---|---|
| Felkészítés ideje | | 01. 09. - 11. | 05. 02. - 04 | 04. 18. – 20. | 05. 30 | |
| Technikai eszközök | Híradó | IRIDIUM, INMARSAT, HICOM kp., VSAT, HARRIS RF-5200 rádió (1) | IRIDIUM, INMARSAT, PANASONIC kp., VSAT, HARRIS RF-5200 rádió (1) | INMARSAT, HICOM kp., VSAT, HARRIS RF-5200 rádió (1) | IRIDIUM, INMARSAT, HARRIS RF-5200 rádió (1) | IRIDIUM, INMARSAT, HARRIS RF-5200 rádió (1) |
| | Informatikai | | Router programozás elmélete (2) | | | |
| Megjegyzések:<br>A HARRIS RF-5200 rádiók kezelésére való felkészítést az MH SZFP saját hatáskörben végezte.<br>A routerek típusának tényleges ismeretének hiányában csak alapfelkészítés történt. | | | | | | |

3. táblázat: Béketámogató és válságreagáló műveletek kommunikációs felkészítése (2005. I. félév). (Forrás: [5])

## Következtetések

Napjaink katonai műveleteiben, mind a béke-, mind a hadműveletekben jelentősen megnőtt az információszükséglet. A parancsnokok, döntéshozók számára időben rendelkezésre álló információ alapján lehet csak a hatékony reagálóképességet kialakítani és fenntartani. Bár a Magyar Köztársaság katonái hadműveletekben nem vesznek részt, de a béke- és válságreagáló műveletekben való részvételünk megköveteli, hogy jól felkészült hivatásos és szerződéses katonák lássanak el külszolgálatot – hazánkat képviselve.

A kontingensek több (legalább 2), egymástól független műholdas átviteli eszköztípussal is el vannak látva, ami minden körülmények között biztosítja a megbízható

kapcsolatot Magyarországgal. Mindeddig nem történt olyan, hogy egy kontingens híradása teljesen megszakadt volna, és az egymástól független rendszerek miatt ez a jövőben sem várható. Meghibásodások vagy előre tervezett karbantartások miatt egy átviteli út kieshet, de a többi segítségével biztosított a vezetés folyamatossága.

A hazai felkészítés egyik lényeges sarokköve a híradó és informatikai üzemeltető állomány felkészítése, hiszen feszített ütemben, folyamatos vezetéstámogatási képességgel felvértezve kell helytálljanak, sokszor ellenséges környezetben. A korszerű, bonyolult működésű információs eszközök hadszíntéri alkalmazása, üzemeltetése nem sajátítható el az iskolapadban – ott legfeljebb az elméletet lehet elsajátítani -, a gyakorlati kiképzés minden esetben terepen történő felkészítéssel kell párosuljon. Ehhez jól felkészült, a gyakorlati életet ismerő szakemberekre van szükség, az oktatói állomány oldaláról is. Szerencsére rendelkezünk ilyen szakemberekkel, amit mi sem bizonyít jobban, mint a békemissziók gyakorlatilag folyamatos kommunikációs támogatása, és a híradó és informatikai feladatok zömében problémamentes végrehajtása.

Ugyanakkor a hazai felkészítésekben célszerű a blokkosított és összevont felkészítésekre törekedni. A váltások dátumainak ismeretében összevonható a szakállomány felkészítése, ami adott esetben költségmegtakarítást jelenthet. Az egyes kontingenseknél felhasznált VSAT végponti eszközök különbözősége miatt ez a felkészítés (amely a legdrágább, mert a MH saját erőből nem tudja végrehajtani) nem blokkosítható, de a műholdas mobiltelefonok és a rádiók oktatása igen. A műholdas mobiltelefonok tényleges használóit (kontingensparancsnokok, járőrparancsnokok, hadműveleti ügyeletesek) is be kell vonni a kiképzésbe. Jelenleg a kontingens híradó erői készítik fel a tényleges használó állományt. Mivel cél az, hogy a külföldi szolgálatra szervezetszerű alegységek kerüljenek kiküldésre, ezt a felkészítést a békekiképzés rendszerébe is be lehet integrálni. Így a konkrét feladatra való felkészítés időszakában csak az ismeretek felfrissítésére van szükség.

A korábbiakban említett, a Honvédelmi Minisztérium közigazgatási államtitkárának és a Honvéd Vezérkar főnökének együttes intézkedés (tervezet) meghatározza, hogy a szakterület felelősök a béketámogató és válságreagáló műveletek tapasztalatainak feldolgozására szervezzenek konferenciákat, készítsenek tanulmányokat, kiadványokat és a levont következtetések alapján dolgozzanak ki megoldási javaslatokat a problémás területekre. Ennek alapján lehetővé válik a váltások hatékonyabb felkészítése, de akár a következő katonageneráció számára is hasznos útmutatások kerülhetnek rögzítésre és bemutatásra.

A nagy kontingensek mellett egyre fontosabb a nemzetközi műveletekben egyéni beosztásokban való részvétel. Példaként említhető, hogy a szudáni Darfur tartományban dúló polgárháború következményeit felszámoló AMIS-II misszióban is szolgál magyar katona. Ekkor is biztosítani kell a folyamatos, megbízható beszédkapcsolatot (Iridium műholdas telefonnal), de egyre inkább előtérbe kerül a nagysebességű adatkapcsolat igénye is. A technikai fejlődés hamarosan lehetővé teszi ezen igény kielégítését is.

A békefenntartás nem korunk „terméke”. Az idén első ízben, 2005. május 29.-én megtartott Békefenntartók Napjának megemlékezései során többször elhangzott: a XIX. század végének, a XX. század elejének háborús gócpontjainál már megjelent ez a fajta katonai tevékenység, és – sajnos – várhatóan még jó ideig számolnunk kell vele. Az információs társadalomban a katonai erők tevékenységét is alapvetően

befolyásolja az elérhető információ. A béketámogató és válságreagáló műveletek jellege miatt ez fokozottan jelentkezik, emiatt kiemelten fontos a legjobb és leghatékonyabb (ideértve a költséghatékonyságot is) hírrendszerek biztosítása.

## Felhasznált irodalom


[1] Az Észak-atlanti Együttműködési Tanács (NACC) híradó szakértő csoportjának jelentése a NACC közreműködésével végrehajtott békefenntartó műveletek híradásának koncepciójáról. (1993)

[2] AJP-1. Szövetséges közös hadműveletek doktrínája. 19. fejezet. Békebiztosító hadműveletek (1994)

[3] A Honvédelmi Minisztérium közigazgatási államtitkárának és a Honvéd Vezérkar főnökének együttes intézkedése a nemzetközi szervezetek által irányított válságreagáló és béketámogató műveletekben történő részvétellel kapcsolatos feladatok végrehajtásának részletes szabályairól (tervezet) (2005)

[4] Az MH Híradó Parancsnokság Távközlési Központ nyilvántartásai. (2004)

[5] Az MH Híradó Parancsnokság hadműveleti és kiképzési főnökség nyilvántartásai. (2005)

**HORVÁTH Zoltán**

# A KIS- ÉS KÖZEPES MÉRETŰ PILÓTA NÉLKÜLI REPÜLŐ ESZKÖZÖK, VALAMINT A FÖLDI IRÁNYÍTÓPONT KÖZÖTTI KOMMUNIKÁCIÓ HATÉKONYSÁGÁNAK NÖVELÉSI LEHETŐSÉGE, SZABÁLYOS RASZTERES ÁLLOMÁNYÚ DIGITÁLIS DOMBORZAT MODELL ALKALMAZÁSÁVAL

Zrínyi Miklós Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Kar
Híradó Tanszék
Katonai Távközlési Szakcsoport

A kis- és közepes méretű pilóta nélküli repülő eszközök (továbbiakban UAV) alkalmazása számos előnyt rejt magában. Felderítő, vagy kutató feladatok végrehajtását végezhetik el nehezen megközelíthető, vagy veszélyes terepen az alkalmazók épségének veszélyeztetése nélkül. Az irányítás a célterülettől biztonságos távolságban telepített földi irányítópontról valósítható meg.

Az üzemeltetés és az üzemben tartás lényegesen költségkímélőbb a hagyományos repülőeszközök alkalmazási költségéhez viszonyítva. A bevetéshez az előkészítés, bevetés után a karbantartás gyorsabban elvégezhető. Az alkalmazói alkalmasság nincs a légi üzemeltetéshez szükséges egészségügyi követelményekhez kötve. Az alkalmazói képzés lényegesen kevesebb időt, valamint olcsóbb és kevesebb üzemórát vesz igénybe.

Az irányítás és az értékelés „földön történő elhelyezése" lehetővé teszi az UAV méretének drasztikus csökkentését. Az UAV a kis méret és a kevés „árulkodó jel" miatt nehezen felderíthető és megsemmisíthető eszköz.

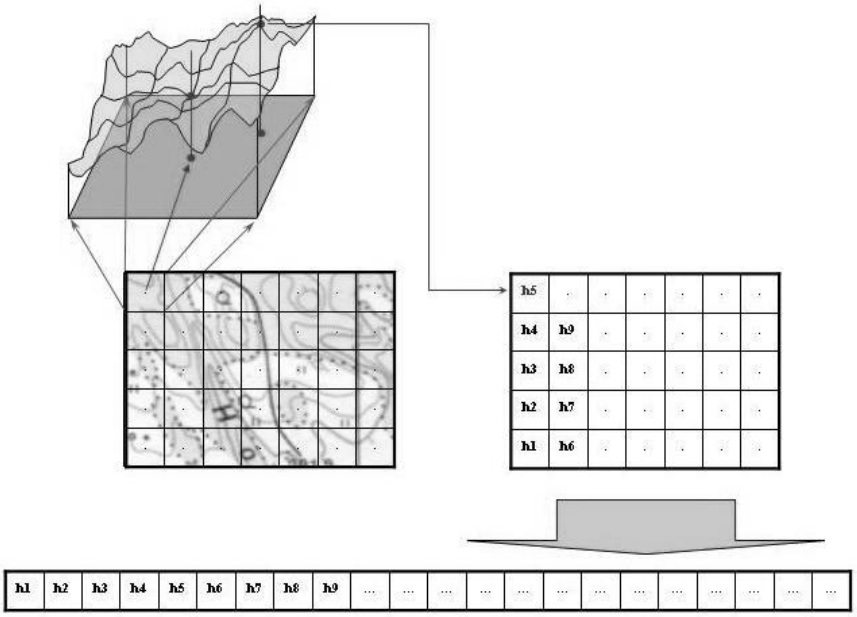
Az UAV alkalmazásának viszont vannak hátrányai is. Az UAV alkalmazása során probléma forrása lehet, hogy az UAV és a hozzá tartozó földi irányítópont csak rádiócsatornán keresztül képes kommunikálni. A földi irányítópontról a szükséges manőverek végrehajtásához parancsokat kell továbbítani az UAV fedélzetére, ezzel egyidejűleg az UAV a megfigyelési és felderítési adatokat szintén rádiócsatornán továbbítja a földi irányítópont részére. A kommunikáció folyamatos. Ez megkönnyíti a felderítést, az információ lehallgatását, az információs csatorna zavarral történő lefogását.

Kis magasságon, ami a kis- és közepes méretű UAV jellemző repülési magassága, a terepdomborzat jelentősen befolyásolhatja a rádiócsatornán keresztül létesített összeköttetés minőségét. Ha az UAV a domborzat árnyékoló hatása következtében kialakult „árnyékzónába" repül, az irányítás kiesése miatt az UAV elvész, és az UAV által szolgáltatott információk vételére a földi irányítópont sem képes.

Célkitűzésem olyan számítógépen megvalósítható algoritmusok bemutatása, amelyek – a szabályos raszteres állományú Digitális Domborzat Modell alkalmazásával – egyrészt képesek az „UAV - földi irányítópont" közötti rádiókapcsolat megvalósíthatóságának értékelésére a rádiókapcsolat területi ellátottságának vizsgálatán keresztül, másrészt képes az UAV részére repülési útvonal tervezésére, mely útvonalat az UAV, a rádiókapcsolat kiesésétől a helyreállásáig önállóan, biztonsággal berepülhet.

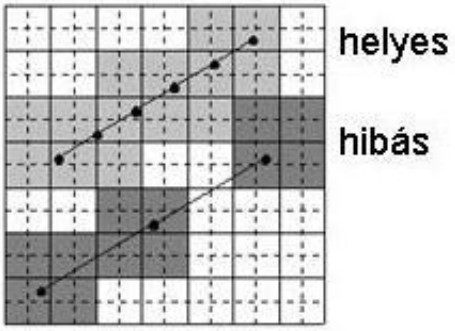
### A szabályos raszteres állományú Digitális Domborzat Modell

A szabályos raszteres állományú Digitális Domborzat Modell (továbbiakban DDM) a vizsgált terület magassági adatait tartalmazza, rendezett formában. Az adatbázis magassági adatainak létrehozásához a vizsgált területet lefedik egy rácshálóval. Az így létrejövő elemi területeken (cellákban) mért maximális magasságértékeket rendre hozzárendelik egy, a rácsháló méretével azonos sor- és oszlopméretű tömbhöz. Ezt a tömböt oszlop-, vagy sorfolytonosan kiolvasva, háttértárolón szekvenciálisan tárolva megkapjuk a DDM-et. Ha ismert a cellaméret, az alapfelület magassága, a tárolás szekvenciája, egy támpont koordinátája, ez esetben a vizsgált terület adott pontjának magassága koordinátái alapján visszakereshető (1. sz. ábra).




1. sz. ábra: A DDM létrehozása

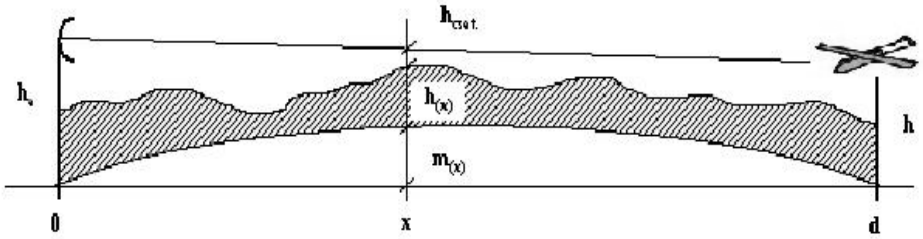
### Optikai átláthatóság vizsgálata DDM alapján




2. sz. ábra: Terepmetszés helyes és hibás végrehajtása

Megfelelően választott lépésközzel a DDM-en vertikális terepmetszet készíthető. A lépésközt úgy kell megválasztani, hogy a metszetkészítés során ne legyen a metszet mentén olyan cella, melynek magassági adata nem kerül feldolgozásra, mivel ez információveszteséghez vezet (alul-mintavételezés). Ennek elkerülése érdekében a cella élhosszánál minden esetben kisebb lépésközt kell választani. A metszetkészítés során a kérdéses pont (osztópont) magassága az őt körülvevő cellanégyes magassági adatainak lineáris interpolációjával állítható elő (2. sz. ábra).

A földgörbülettel korrigálva a magassági adatokat a pont-pont kapcsolat vizsgálata során egyértelműen eldönthető, hogy megvalósul-e az optikai átláthatóság (3. sz. ábra).

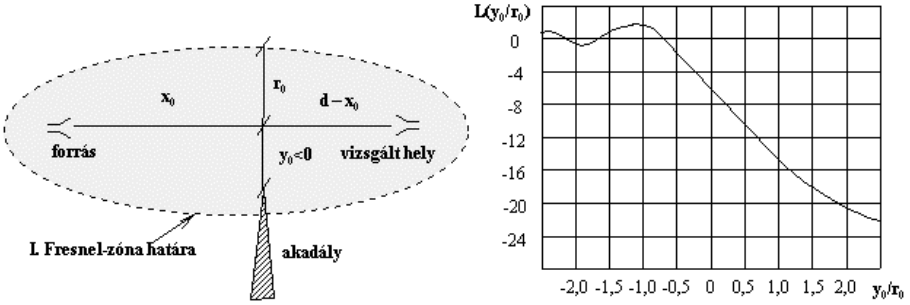



3. sz. ábra: Magasságkorrekció a földgörbültség figyelembevételével

**Összeköttetés minőségi modellezése**

Az UAV-k az irányítás megvalósítására és az információk közlésére többnyire a VHF és az UHF frekvenciasávokat alkalmazzák. A pont-pont összeköttetés vizsgálata során nem elég az optikai átláthatóság ellenőrzése, figyelembe kell venni az I. Fresnel-zóna lefedettségét, mely a terepdomborzat takarásából adódhat.

Egy ismert helyzetű, elhanyagolható szélességű akadály (4. sz. ábra) minőségrontó hatása számítható. Rendszerint a rádiócsatornát nem egy, hanem több akadály terhel. Számos modell született, mely több akadályt figyelembe véve próbálja a rádiócsatorna csillapítását becsülni.

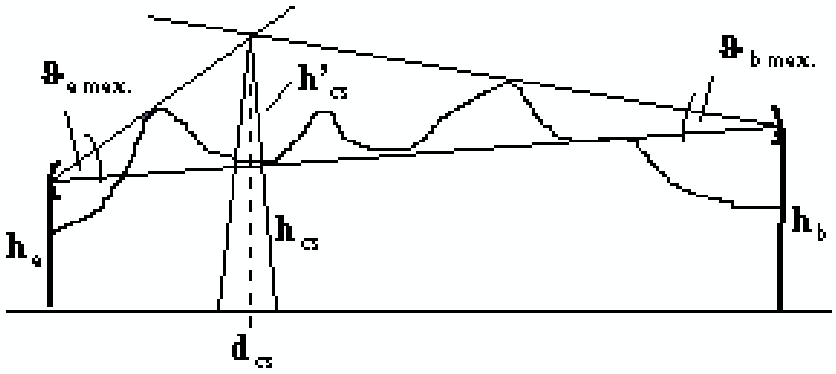



4. sz. ábra: Egy késél okozta diffrakciós fading

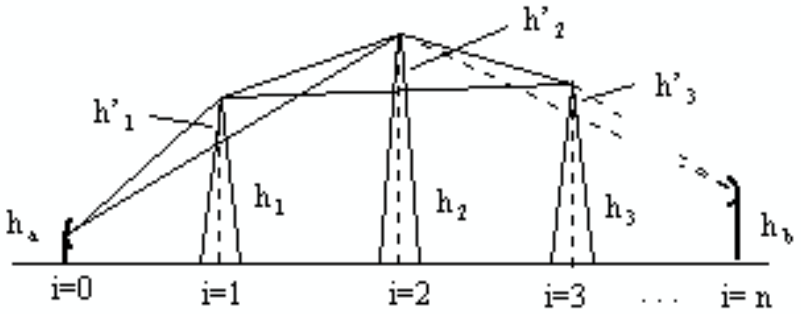
A további ismertetésre kerülő modellek közös jellemzője a több akadály összegzett hatásának számítása az egyes akadályok egymásra hatása alapján, az egyes késélek okozta diffrakciós fading algoritmizált összegzése. Az alkalmazások sarkköve a terepen található, a rádiócsatorna tengelyét legjobban megközelítő csúcsok meghatározása.

A Bullington modell (5. sz. ábra) a rádiócsatorna két végpontjából a legmagasabb helyszög alatt látható két akadály felhasználásával, egyeneseket fektetve az adó és hozzá közeli akadály csúcsára, valamint a vevő és hozzá közeli akadály csúcsára, az egyenesek metszéspontja jelöli ki egy virtuális akadály helyét és csúcsát.

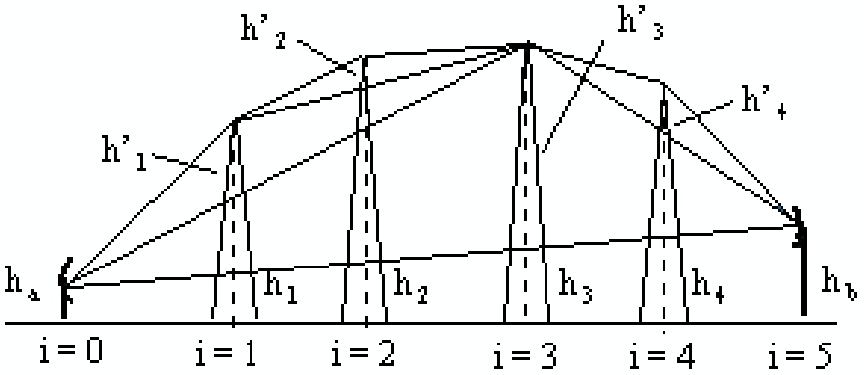
Az Epstein-Peterson modell. (6. sz. ábra) A rádiócsatorna egyik végpontjából a másik irányba haladva az egyes akadályok okozta minőségromlás a szomszédos akadályokra, mint virtuális adó-, illetve vevőpontokra vonatkoztatott hatások összege.




5. sz. ábra: A Bullington modell



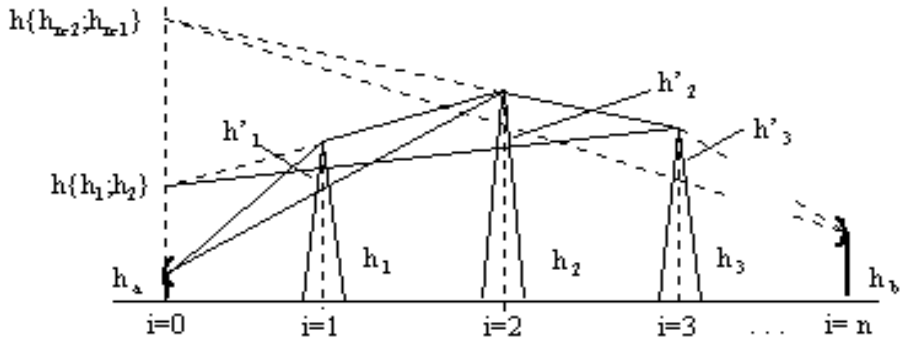

6. sz. ábra: Az Epstein-Peterson modell




7. sz. ábra: A Deygout modell

A Deygout modell. (7. sz. ábra) a rádiócsatornában kiválasztja a legdominánsabb akadályt, ezt követően – kiszámítva hatását – a domináns akadálynál kétfelé választja a rádiócsatornát. Az algoritmus az adó-, illetve a vevőantenna felé mindaddig folytatódik, míg a virtuális rádiócsatornák akadályokat tartalmaznak.

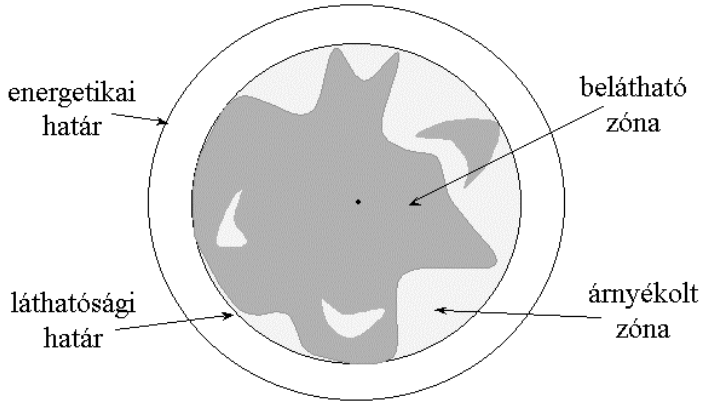
A gyakorlatban még a Japán modell (8. sz. ábra) használatos. Epstein-Peterson módszeréhez hasonlóan a rádiócsatorna egyik végpontjától (adó) indul a másik végpont (vevő) felé. Az egyes akadályok okozta minőségromlási mutatót úgy határozza meg, hogy a virtuális vevőt a vizsgált akadályt sorrendben követő akadályra helyezi. Az adó pozícióját nem változtatja, viszont az adó virtuális magasságát a vizsgált és az azt sorrendben megelőző akadályokra fektetett egyenesnek az adó antenna helyén kimetszett magassága adja.




8. sz. ábra: A Japán modell

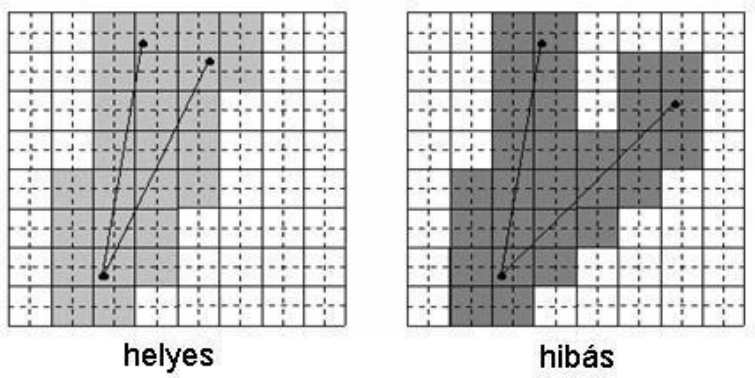
**Ellátottsági- és árnyékdiagram készítése**

Ha az átláthatóság vizsgálata és az összeköttetés minőségi modellezése pont-pont viszonylatban megvalósult, innen már csak egy lépés a pont-terület viszonylat vizsgálata, az ellátottsági- és árnyékdiagramok készítése (9. sz. ábra).




9. sz. ábra: Ellátottsági- és árnyékdiagram

Az információvesztés elkerülése érdekében továbbra sem szabad elfeledkezni arról a szempontról, hogy a kérdéses terepszakaszon található valamennyi terepelemet érinteni kell az analizálás során (10. sz. ábra).




10. sz. ábra: Területvizsgálat helyes és hibás végrehajtása

**A területi ellátottsági- és árnyékdiagramok értékelése**

Ezek alapján belátható, hogy a misszióba küldött UAV feletti kontroll, valamint az UAV által szolgáltatott információk vételének folyamatossága nagy valószínűséggel biztosítható abban az esetben, ha az operátor csak az ellátott területek felett üzemelteti az általa irányított UAV-t. Az UAV elvesztése az árnyékzónák felett előre láthatóvá válik, és nem hat a meglepetés erejével.

**Az UAV - földi irányítópont rádiókapcsolat ideiglenes megszűnésének problematikája**

Az előbbiekben felvázoltak alapján meghatározhatóvá válnak azok a területek, mely területek felett a rádiókapcsolat folytonossága nagy valószínűség szerint nem biztosítható. Ha az UAV ezen területek fölé „téved", vagy egyéb előre nem látható ok miatt a folyamatos rádióösszeköttetés megszakad, az UAV fedélzetére helyezhető számítógép segítségével a rádiókapcsolat helyreállásáig az UAV önállóan kell, hogy biztonságos körülmények között repüljön. Főleg kismagasságú repülés esetén a domborzat komoly veszélyt jelent az UAV számára.

**A repülés biztonsága**

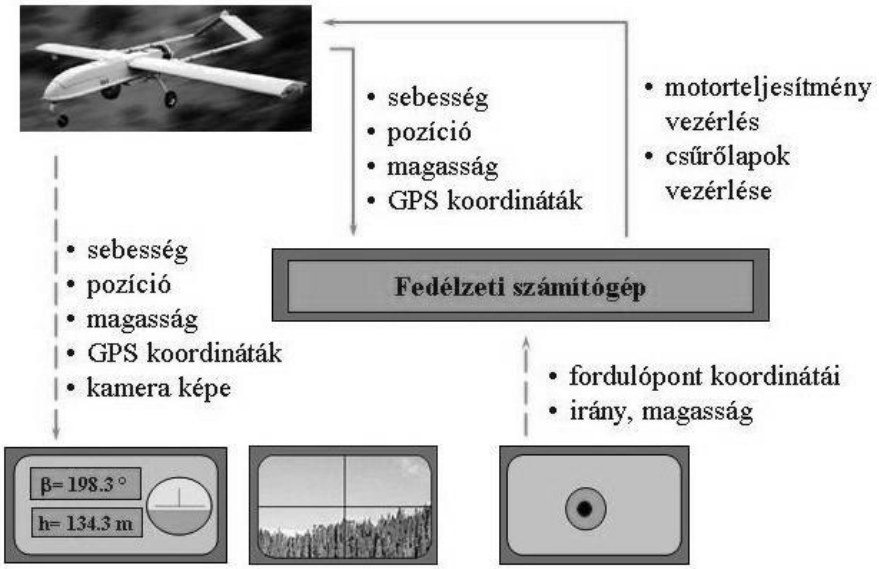
Repülés közben biztonságos magasságot kell tartani a terep felett. Szem előtt kell tartani a repülőgép repülési paramétereit (fordulási sugár, maximális emelkedési, süllyedési képesség stb.). Ügyelni kell arra, hogy az UAV egy meredek hegyoldal mellett biztonságos oldaltávolságban repüljön el, nehogy kisodródjon, vagy egy erős széláramlat nekisodorja. Az emelkedési képesség meghatározza, hogy egy hegyorom biztonságos átrepüléséhez legalább milyen távolságra kell megkezdeni egy emelkedést, maximum mekkora lehet a süllyedés mértéke, hogy a repülési sebesség ne lépje túl a kritikus értéket.

**UAV irányítási modellje DDM alkalmazásával**

Lehetséges megoldás, a fedélzetre telepített, terepkövetést biztosító eszközök alkalmazása, de ez mérete, tömege miatt nem kivitelezhető.

Mivel a fedélzet és a földi irányító pont is tartalmaz számítógépet, a megoldás a számítógépen tárolható terepet leíró adatokban és az azokat feldolgozó eljárásokban rejlik, melyeknek nincs fizikai mérete és súlya.

Egy lehetséges irányítási modellt mutat be a 11. sz. ábra.

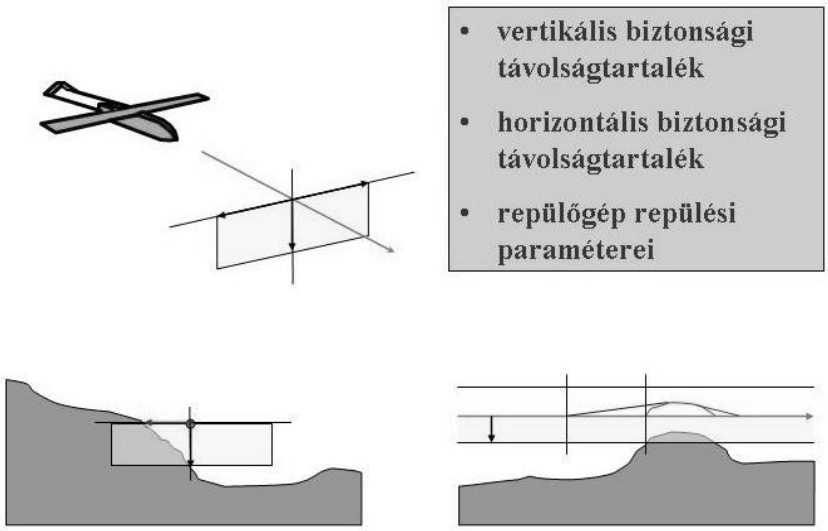



11. sz. ábra: UAV irányítása fedélzeti számítógép támogatásával

A földi irányítási pont utasításai leegyszerűsödnek repülési irányt, vagy elérendő koordinátát meghatározó paranccsá. A fedélzeti számítógép ennek alapján – figyelembe véve a repülés paramétereit és az UAV lehetőségeit – tartja a repülési sebességet, irányt, kivitelezi a manőverek végrehajtását, megcélozva a sorra következő fordulópont elérését. Az UAV fedélzetéről a földi irányító pontra sugárzott repülési paraméterek inkább tájékoztatják a kezelőt, mint alátámasztják a közvetlen irányítást.

Ha megszűnik az irányítás folyamatossága, a fedélzeti számítógép ideiglenesen átveheti az UAV irányítását. A fedélzeten rendelkezésre állnak az UAV repülési paraméterei, az elérni kívánt fordulópont(ok) koordinátái, a pillanatnyi helyzet és egyéb, a manőverek kivitelezéséhez szükséges adatok. A fő feladat, hogy a számítógép képes legyen egy olyan légifolyosó tervezésére, mely térbeli helyzetét vizsgálva biztonságos távolságra van a domborzattól, valamint keresztmetszete biztosítja, hogy az UAV képes folyamatosan a légifolyosón belül tartózkodni.

A fenti követelmények teljesítése DDM-en végzett terepmetszet készítésével megvalósítható. Kiindulásként létre kell hozni egy adatfolyamot, melynek adattartalma megegyezik a tervezett fordulópontok között mérhető felszín magasságával (vertikális terepmetszet). Ezeknek a magassági adatoknak az értékét meg kell növelni a kívánt repülési magassággal. Az adatfolyam magassági adatait szükség szerint meg kell növelni annak érdekében, hogy az UAV rendelkezzen oldalirányú biztonsági távolságtartalékkal (légifolyosó szélessége). Utolsó lépésként az emelkedési és a merülési képességek figyelembevételével tovább növelve a légifolyosó adott elemeinek magasságát biztosítható, hogy az UAV képes legyen ezen manőverek végrehajtása során a légifolyosón belül tartózkodni. Ha nem terepkövető módról van szó, a légifolyosó magassága alulról limitálható (12. sz. ábra).




12. sz. ábra: Útvonalterv két fordulópont között, DDM alapján

A fenti eljárással biztosítható, hogy a folyamatos rádióösszeköttetés megszakadása esetén az UAV nem vész el, képes önállóan folytatni feladatának végrehajtását.

## Összegzés

Összességében megállapítható, hogy a DDM-ek alkalmazásának ez egy új területe. Az UAV-k misszióba küldése során az ellátottsági- és árnyékdiagramok nagyban segíthetik az operátori munkát, növelik a misszió sikeres végrehajtásának lehetőségét. Ellenőrizhetővé válik azon terepszakaszok összessége, mely területek felett a folyamatos összeköttetés fenntartása nem biztosítható. Ha mégis valami ok folytán megszakad a rádióösszeköttetés, az UAV és a földi irányítópont megfelelően kialakított rendszere képes biztosítani, hogy az UAV az összeköttetés helyreállásáig – biztonságos körülmények között – képes önállóan folytatni feladatának végrehajtását.

## Felhasznált irodalom

[1] J. D. Parsons,
[2] The Mobile Radio Propagation Channel. (Pentech Press London 1992)
[3] OMFB,
[4] A térinformatika és alkalmazása (Tanulmány, Budapest 1993. június)
[5] Fenyves Erzsébet,
[6] A térinformatika térhódítása
[7] Dr. Detrekői Ákos – Dr. Szabó György,
[8] Bevezetés a térinformatikába, Nemzet Tankönyvkiadó, Budapest, 1995
[9] Zentai László,
[10] Számítógépes térképészet, ELTE Eötvös kiadó, Budapest, 2000
[11] Micropilot UAV autopilots homepage,
[12] http://www.micropilot.com/
[13] UAV Flight Systems homepage,
[14] http://www.uavflight.com/

**KASSAI Károly**

# AZ ELEKTRONIKUS ADATKEZELŐ RENDSZEREK VÉDELMÉNEK FONTOSABB TENDENCIÁI (KIEMELTEN A SZABÁLYOZÁSI TERÜLETTEL KAPCSOLATOS FELADATOK)

A honvédségnél a civil szférához hasonlóan egyre hangsúlyosabban jelentkeznek a korszerű adatkezelő szolgáltatásokra vonatkozó igények, ami a katonai szervezeteknél a korszerű adatkezelő képességek iránti igényekben és a szervezetek közötti magas szintű kommunikációs szükségletekben mutatható ki.

Az igények kielégítése széttagoltan, a katonai szervezetek önállónak tekinthető erőforrásaira támaszkodva elképzelhetetlen, így a gyakorlatban egyre jobban erősödik az MH szintű, egységes szolgáltatások kialakítására vonatkozó igény.

A korszerű szolgáltatások egy része védelmi területen is olyan technikai megoldásokat követel, amelyek nagyobb fejlesztés nélkül nem valósíthatók meg (pl. az MH Iroda-automatizálási Programon belül kialakítandó elektronikus ügyintézés tartalmasan elektronikus aláírás szolgáltatás nélkül elképzelhetetlen), így elektronikus információvédelmi szakterületen is érzékelhető a kérdések MH szintű, egységes rendezésére vonatkozó szükséglet.

Az egységes hálózati szolgáltatások biztosítása központi hálózat menedzselést igényel, ami a zártcélú hálózat központi hálózatfelügyeletéhez hasonlóan megköveteli a tervezett informatikai hálózat központi menedzselését (beleértve a biztonsági alkalmazásokat) is.

A meglévő, eltérő technológiát alkalmazó kommunikációs eszközök eltérő szolgáltatásokat biztosítanak, ami értelemszerűen megjelenik az elektronikus információvédelem területén is. Automatizált védelmi megoldások csak a korszerű eszközök esetében valósíthatók meg, míg az egyéb eszközök vonatkozásában a személyi felügyeleten és ellenőrzéseken keresztül lehet a biztonsági kérdéseket kézben tartani.

A NATO csatlakozást követő néhány év után látható, hogy a katonai szervezetek egy része az összetett információkezelési szükségleten belül egyre nagyobb arányban igényel NATO adatokat, amelynek vonzata a NATO minősített adatkezelésre feljogosított hálózat magyarországi kiterjedésének bővítése, illetve a helyi adatfeldolgozási képességek kialakítása.

A Magyar Köztársaság légterének védelme, a szövetségesi kötelezettségek teljesítése, a NATO egységes légtér menedzselésének szükségessége megköveteli, hogy a légierő különböző funkcionális rendszerei rendelkezzenek a szükséges kommunikációs csatlakozásokkal, illetve képesek legyenek a NATO adatbázisok használatára (adatok fel-, illetve letöltése).

A NATO prágai és isztambuli csúcsértekezletek követelményei alapján a megjelenő, egyre súlyosabb fenyegetések ellensúlyozása érdekében prioritással rendelkező feladat az informatikai hálózatok biztonságának erősítése.

A megvalósítás egyik részfeladata katonai vonalon az un. CIRC (Computer Incident Response Capability) képességek kialakulása, ami a felkészülési, detektálási,

reagáló és a szükséges helyreállítási műveleteket támogató rendszerelemek kialakítását és folyamatos üzemeltetését teszi szükségessé.

Ezt a feladatot támogatja kormányzati szinten a Nemzeti Hírközlési Hatóság által üzemeltetett Főközpont a kommunikációs szolgáltatások állapotfigyelésével, a támogató információk gyors cseréjével és különböző munkacsoportok értesítésével, támogatva a biztonsági eseményekre történő gyors reagálást és az adatbiztonsági fenyegetések gyors kezelését.66 Hasonló célú, inkább az informatikai területen történő megelőzést és helyreállítást célzó szakmai támogatást lát el a – még csak korlátozott képességekkel rendelkező – nemzeti CERT (Computer Emergency Response Team) szervezet is.

Más feladatok kapcsán olyan infrastruktúrákra van szükség, amelyek képesek két-, vagy többoldalú nemzetközi szerződés alapján átvett külföldi adatok (pl. a Grippen rendszerbeállítással kapcsolatosan svéd minősített adatok) feldolgozását és védelmét ellátni.

Az Európai Uniós csatlakozás már az első pillanatban megkövetelte, hogy a Magyar Köztársaság csatlakozzon az uniós döntéshozatali rendszert támogató informatikai hálózathoz, amely folyamat a magyarországi alrendszerért felelős Külügyminisztérium koordinálásával a honvédséget is érintette.

A Magyar Honvédség adatkezelő rendszerei nem lehetnek függetlenek az általános üzemeltetési és a jogszabályi környezettől, így a technikai fejlődés okozta változások, illetve a felhasználói igények változása mellett a várható tendenciák bemutatásához további segítséget nyújt a kormányzati szintű helyzetértékelés és jogszabályi környezet rövid áttekintésére.

A Nemzeti Biztonsági Stratégia a veszélyeztetésre vonatkozóan kijelenti, hogy a hosszú távú lemaradás hátrányos következményeinek elkerülése érdekében Magyarország számára kiemelt feladat a felzárkózás a fejlett világ információs és telekommunikációs színvonalához. Ügyelni kell a rendszerek védelmére és a megfelelő tartalékok képzésére, mert a számítógépes hálózatok és rendszerek sebezhetősége, túlterhelése, az információlopás, a vírusterjesztés és a dezinformáció kockázati tényezőt jelent az ország számára.

A védelemmel kapcsolatban a stratégia megállapítja, hogy a technológia rohamos fejlődésének korában új feladatként jelentkezik a korszerű és biztonságos informatikai infrastruktúra kialakítása és a kormányzati információs rendszerek védelme.

A kormányzati információs rendszert fel kell készíteni a kibernetikai támadások megelőzésére és kivédésére.

A védelem sikere érdekében szoros koordináció szükséges mind a szövetségesekkel, mind az informatikai és távközlési szolgáltatók, valamint kutatóközpontok között.67

A Magyar Információs Társadalom Stratégia (MITS) a külföldi megfogalmazásokkal összhangban megállapítja, hogy a fejlődés következtében a kormányzati szektor és a gazdálkodó szervezetek függősége az informatikai rendszerektől megnőtt.

---

[66] 27/2004. (X. 6.) IHM rendelet 3, 4 és 10. §.

[67] A Magyar Köztársaság nemzeti biztonsági stratégiája, 2073/2004. (III. 31.) Korm. határozat, II. 1. 6. és III. 3. 7. pontjai. A stratégia az ágazati stratégiák (benne: informatikai és információvédelmi stratégia) elkészítését 2004. szeptember 30-ig határozta meg.

Az előrelépés érdekében – többek között – a kritikus infrastruktúrák kiemelt védelmére, az információbiztonsági tudatosság és az ismeretek fejlesztésére van szükség.

A célok megvalósítása érdekében megfelelő jogszabályi és intézményi környezetet kell kialakítani, ki kell dolgozni a biztonsági követelményeket, honosítani kell a nemzetközi szabványokat, kockázatkezelési módszereket kell kifejleszteni, biztonságos információs rendszereket kell kialakítani, támogatni kell fenntartásukat, valamint részt kell venni a nemzetközi IT biztonsági szervezetek munkájában.68

A MITS Informatikai Biztonsági Részstratégia (IBRS) a Nemzeti Informatikai Biztonsági Stratégia számára célként a kritikus rendszer és infrastruktúra elleni támadások megelőzését-, a sebezhetőségek csökkentését-, és a károk és a helyreállítási idő minimalizálása.

Megvalósítandó célkitűzés a technikai infrastruktúra stabilitása (kockázatkezelés, védett alkalmazások és szolgáltatások, a kritikus infrastruktúra kiemelt védelme, átfogó biztonsági szemlélet kialakítása (biztonság-tudatosság, biztonsági szabványok), a biztonsági tanúsítási rendszer működtetése, a számítógépes vészhelyzeteket kezelő sürgősségi csoportok, az érintett szereplők alapvető jogainak védelme.

Ennek érdekében stratégiai célnak kell tekinteni a hatékony nemzetközi és nemzeti együttműködés kialakítását, a biztonságos, hatékony kormányzati információs rendszerek működését, a kritikus infrastruktúrák kiemelt védelmét, a rendszerekbe és hálózatokba vetett bizalom erősítését és a biztonsági tudatosság fejlesztését, valamint az informatikai rendszerek alanyainak tájékoztatását és a rájuk vonatkozó alapjogok védelmét.69

Az eddigiek kiegészítésére szolgáló információ a 2094/2004. Korm. határozatban meghatározott feladatrendszer, amely megfogalmazza, hogy a minősített adatok védelme érdekében egységesítésre van szükség a nemzeti, NATO, EU (és egyéb külföldi minősített adatok) védelme érdekében.

A kormányzati szintű kezdeményezések jól mutatják, hogy a Magyar Honvédség különböző adatkezelő rendszerei, folyamatai változó környezetben vannak és olyan kihívások előtt állnak, amelyeket az eddigi szabályozó mechanizmussal nem lehet kézben tartani.

A rendelkezésre álló HM szintű jogszabályok, és állami irányítás egyéb jogi eszközei körébe tartozó nem minősített szabályozók áttekintésével gyorsan megállapítható, hogy a Magyar Honvédségnél nem található egy olyan hivatalosnak tekinthető állásfoglalás, amely átfogóan meghatározná a honvédség által kezelt információk védelmi rendszabályainak alapelveit.

A törvények és kormányrendeletek által meghatározott rendszabályok természetesen valamilyen formában kialakítottak (pl. a 79/1995. (VI. 30.) Korm. rendelet végrehajtását szolgálja az MH Titokvédelmi és Ügyviteli Szabályzat, a 43/1996. (III. 19.). Korm. rendelet végrehajtására az MH Rejtjelszabályzata).

Az MH Informatikai Szabályzat a minősített adatok védelmére vonatkozó általános jogszabályok végrehajtása érdekében információvédelmi szakkérdések is szabályoz, és meghatározza, hogy minden katonai szervezetnél számítástechnikai titokvé-

[68] A 1214/2002. (XII. 28.) Korm. határozat 3. pontja szerinti MITS III. fejezet, az ágazati stratégiák összefoglalója, az informatikai biztonság, és a minőség fejezetek.

[69] IBRS II. 1. 6, III. 3. 7, 3. 4, 5. 1. 3. bekezdések, a jövőkép alapelvei fejezet, 83. o. és a stratégiai célok fejezet, 85. o.

delmi felelős (vagy adatvédelmi tiszt) segítse a parancsnok (vezető) munkáját és a védelmi rendszabályokat helyi Számítástechnikai Titokvédelmi Szabályzatban kell rögzíteni.

Egy-egy részterület szabályozására megjelentek HM utasítások, amelyek jól érzékelhetően vagy egy jogszabály végrehajtását célozták (pl. a 4/2000. (II. 29.) HM rendelet és a 13/2000. (HK 6.) HM utasítás az 56/1999. (IV. 2.) Korm. rendelet végrehajtását szolgálta a NATO/NYEU Központi Nyilvántartó és a nyilvántartási rendszer üzemeltetésével kapcsolatban), vagy a felelősségi rendet próbálták szabályozni (169/2000. (HK 19.) MHPK intézkedés a katonai szervezetek biztonsági megbízottainak kijelöléséről, vagy a 33/2002. (HK 13.) HM utasítás az elektronikus információvédelemről) vagy egy rendszerrel kapcsolatos feladatokat határoztak meg (pl. a NATO Irodaautomatizálási Rendszer (NIAR) biztonságával kapcsolatos feladatokról szóló 82/2002. (HK 26.) HM utasítás).

Az így kialakított szabályozók – az összes előnyük mellett – nincsenek összhangban, nem követik a szervezeti változásokat, vagy esetenként nem felelnek meg a korszerűség követelményének.

Az említettek alapján bizonyítható, hogy a Magyar Honvédségnél az információ biztonsággal kapcsolatos felső szintű követelmények és alapelvek egységes, politika[70] szintű meghatározása még nem történt meg úgy, hogy arra támaszkodva az egyes szakterületeken (és folyamatoknál) ki lehessen alakítani a biztonsági követelmények megfelelő védelmi rendszabályokat, és tervezni lehessen az azok érvényesüléséhez szükséges erőforrásokat.

A „biztonság politika" kifejezésre nincs általánosan elfogadott meghatározás, általános értelmezése: a szervezet vezetésének hivatalos döntése a biztonsági követelményekkel kapcsolatban (pl. az ISO/IEC 15408 szabvány (Common Criteria) megfogalmazása szerint: a biztonság politika szabályok, eljárások és irányelvek összessége).

A fent hivatkozott és egyéb kormányzati szintű dokumentumok, jogszabályok áttanulmányozása alapján kijelenthető, hogy hazánkban nincs olyan egyértelmű követelmény, amely meghatározná, hogy a Magyar Honvédségnél milyen szinten, milyen formájú és tartalmú információ biztonság politikát kell kialakítani.

A nemzetközi/nemzeti szabványok, ajánlások nem egyforma nyelvezetet használnak, más-más megközelítéseket alkalmaznak, de megállapításaik mérlegelésével, összegzésével, a katonai sajátosságok beépítésével és a gyakorlati tapasztalatok korrekcióival kialakítható a biztonság politikára vonatkozó alapvető követelmény.

[70] A „security policy" kifejezésből a nemzetközi szabványok fordításakor gyakran „biztonsági szabályzat" válik (pl. az MSZ ISO 15408, az MSZ ISO 17799:2002). Ugyanez előfordul a Nemzeti Biztonsági Felügyeletről szóló 1998. évi LXXXV. törvényben (1. §. 1. pont), és a Központi nyilvántartó, a nyilvántartó és az ellenőrző pontok működéséről szóló 4/2000 (II. 29) HM rendeletben (2.§. 3. pont) vagy az IBRSZ 5. 2. 3. fejezetében, vagy Király Imre 2002-es cikkében. Más esetben (pl. az MSZ ISO 7498-2 esetében a kifejezés magyar fordítása „biztonság politika". A BS 7799 brit szabvány magyar megfelelője pl. az első kötetben „szabályzat"-ot említ míg a második a „politika" kifejezést alkalmazza.

Az információ biztonságra vonatkozó többféle értelmezés megértéséhez jó támpont az amerikai és kanadai megközelítés, amely alapján a biztonság politikának[71] három csoportja különíthető el:

- a szervezeti politika;
- a szervezet egy-egy kiemelt információs területével foglalkozó feladat-specifikus politika (issue-specific policy);
- egy-egy rendszerre vonatkozó, un. rendszer-specifikus politika (system-specific policy).

A különböző források politika alatt általában csak rendszer-, hálózat-, vagy IT politikát értenek, de részletes tartalmi vizsgálat során kiderül, hogy a politikának tartalmaznia kell fizikai-, személyi és dokumentumvédelmi kérdéseket is. Emiatt formailag a felsorolás első és harmadik csoportjának megnevezéséhez az „információ biztonság politika" kifejezést tartom elfogadhatónak (a továbbiakban: politika), és megállapítom, hogy az MH felső szintű szakmai politikának – összhangban a NATO, EU Biztonság Politikával és nemzetközi szabványokkal – az információvédelem mind a négy területét le kell fednie, és ki kell jelölnie a közös menedzselés rendjét.

Az általános követelmények meghatározása csak „fentről-lefelé" történhet, így a továbbiakban a szervezeti információ biztonság politikával kapcsolatos alapvető követelményekre koncentrálok, nem feledve azt az alapvető tényt, hogy a logikus, összefüggő szabályozási hierarchia érdekében a szervezeti politikának ki kell jelölnie a feladat-specifikus politikák területeit és a rendszer- specifikus politika általános feladatát is.

A szervezeti politika tartalmi elemeinek összeállításához alapként a nemzetközi/nemzeti szabványokat (MSZ ISO/IEC 15408, MSZ ISO/IEC TR 13335-3, MSZ ISO 7492-2 és CCITT X.800, MSZ ISO/IEC 17799:2002, MSZE 17799:2004) és az EU Biztonság Politikát tekintem.

A szabványok ajánlásait kiegészítem más nemzeti ajánlásokban foglaltakkal (ITSEC, DoD 5200-28 (TCSEC), The Canadian Handbook on Information Technology (IT) Security, Generally accepted Principles and practies for securing IT systems (NISP SP 800-14), Introduction to Computer Security: The NIST Handbook (NISP SP 800-12), National Training Standard for system administrators in information systems security (INFOSEC); (NSTISSI), Australian Communications-Electronic Security Instruction 33 (ACSI 33), illetve a nemzeti, NATO és EU rendszerek üzemetetése során szerzett tapasztalatokkal.

A fentiek alapján a szervezeti politika felépítését az alábbiak szerint tartom célszerűnek:

Az információ biztonsági célok kijelölése és a politika hatályának azonosítása.

Kiemelendő kérdések:

- azon nemzeti, nemzetközi, szövetségi és MH szintű követelmények (jogszabályok, állami irányítás egyéb jogi eszközei, politikák, stratégiák) és ajánlások azonosítása, amelyek követelményeit a politikának – és az általa szabályozott védelmi rendszabályoknak – ki kell elégítenie;

[71] Az Egyesült Államok NISP 800-12, és 800-14, valamint a Canadian Handbook on IT Security szerint.

- az információ biztonsági célok kijelölése (a bizalmasságra, sértetlenségre és rendelkezésre állásra (és esetleg más célra) vonatkozó általános követelmények);
- annak a követelménynek megfogalmazása, hogy a politika a teljes szervezetre (Magyar Honvédség) vonatkozik (szervezet és személyek, rendszerek, külső együttműködők, a szervezet kikülönített elemei), és melyek azok a szempontok, amelyek a politikától történő eltérést szabályozzák;
- azon szabályozók (dokumentumok) azonosítása, amelyekbe kötelező a politika általános követelményeinek bedolgozása, illetve az esetleges ellentmondások feloldásának módja (pl. szakmai stratégiák, együttműködési megállapodások).

Az információ biztonságért való szervezeti és egyéni felelősségek meghatározása.

Kiemelendő kérdések:

- a strukturált információ biztonsági menedzsment felépítése, beleértve azon szervezeti elemek (funkciók) azonosítását, amelyeket a MH szövetségi kötelezettség teljesítésére kormányzati kijelölés alapján lát el (pl. NATO/NYEU Rejtjelelosztó, NATO/NYEU Központi Nyilvántartó, NATO TITKOS WAN magyarországi alhálózat üzemeltetése) vagy amelyeknek központi üzemeltetés biztonsági feladata van, és a működéshez szükséges szakmai alá- és fölérendeltségi viszonyok meghatározása;
- a szakirányítás általánostól eltérő feladatai;
- a rejtjeltevékenység illeszkedése az elektronikus információ biztonsági menedzsmentbe, beleértve az elkülönítésre vonatkozó általános követelményeket;
- az MH-n belüli, valamint a nemzeti és nemzetközi (szövetségi) szervekkel való együttműködés rendje;
- az információ biztonság érdekében az összeférhetetlenségek meghatározása (pl. az üzemeltető és a biztonságért felelős személy, a biztonsági funkciót megvalósító paraméter mérése és értékelése), illetve az egy személy által nem végezhető tevékenységek meghatározása;
- a védelmi rendszabályok megsértése esetén alkalmazandó alapelvek (szankciók, fegyelmi eljárás), beleértve a nem szándékosan elkövetett eseményekkel kapcsolatos eljárásrendet is.

Az információk, információ kezelő rendszerek és az azokhoz kapcsolódó objektumok érzékenység szerinti besorolásának alapelvei.

Kiemelendő kérdések:

- a személyes adat, az orvosi titok, a nyílt vagy minősített közérdekű adat, a közérdekből nyilvános adatokra vonatkozó kategóriák és az alkalmazott kezelési jelzések;
- az elektronikus adatkezelő rendszerek védelmi szintjeinek meghatározása;
- az üzemeltetési környezetre vonatkozó kategóriák és a rájuk vonatkozó általános követelmények (pl. adminisztratív zóna, biztonsági terület, speciális kiszolgáló létesítmények és a velük szemben támasztott követelmények).

A kockázatkezelésre vonatkozó alapelveket és a maradvány kockázatok kezelésével kapcsolatos általános követelmények. Kiemelendő kérdések:

- a sebezhetőség, fenyegetettség és a kockázatok megállapítására vonatkozó alapvető felelősségek és követelmények;

- a maradvány kockázatok kezelésére vonatkozó tervezési és végrehajtási feladatok (vészhelyzeti és helyreállítási tevékenység);
- a kockázatok felmérésével kapcsolatos feladatok a tervezés, kialakítás és üzemeltetés fázisában, beleértve az ismétlődő vizsgálatok rendjét és feladatait.

A fizikai-, személyi-, dokumentum és elektronikus információ biztonság megvalósításához szükséges védelmi rendszabályok alapjai.

Kiemelendő kérdések:

- a vizsgálati rend meghatározása, amely biztosítja, hogy információ biztonság szempontjából érzékeny beosztásba ne kerülhessen nem megfelelő személy;
- a személyi biztonsági tanúsítvánnyal kapcsolatos követelmények, illetve a speciális beosztásokra vonatkozó eltérő rendszabályok (rejtjeltevékenység, rendszer szintű hozzáférési jogosultság);
- a hozzáférésre történő feljogosítás rendje és a jogosultságok törlésének követelményei beosztásból történő távozáskor;
- a szerződéses partnerek, látogatók belépési jogosultságának megszerzése, valamint az MH rendszerekhez történő hozzáférési jogosultság megszerzése;
- a fizikai védelem alapvető követelményei az infrastruktúra (elhelyezés, épületgépészeti követelmények, védelmi elemek), a technikai rendszer (érzékelők, zárak, riasztók, beléptető rendszerek) az őrzés (járőrözés/ellenőrzés, reagálási normaidők) területén;
- a dokumentumok teljes életciklusán keresztül a védelemmel kapcsolatos rendszabályok alapelvei (pl. készítés, nyilvántartás, minősítés, tárolás, továbbítás, sokszorosítás, betekintés, megsemmisítéssel kapcsolatos minimális követelmények), beleértve a különböző adatkategóriákra vonatkozó speciális rendszabályok lényegét is;
- az elektronikus adatkezelő rendszerek és adatok védelmével kapcsolatos rejtjelzési kötelezettség, kompromittáló kisugárzás elleni védelem, átviteli biztonság, számítógép és hálózati biztonság alapvető követelményei, beleértve a rendszerek tervezésével, kialakításával és jóváhagyásával, az eszközök és adathordozók kivonásával kapcsolatos-, valamint a magán- és harmadik fél tulajdonában lévő elektronikus adatkezelő eszköz alkalmazásával kapcsolatos követelményeket, a távoli elérés és az otthoni munkavégzés rendszabályait is;

A védelmi rendszabályokat megvalósító infrastruktúrákkal, eszközökkel és anyagokkal kapcsolatos erőforrás tervezési feladatok.

Azon területek, amelyeket feladat-specifikus politikával kell lefedni. E területen pontos ajánlások szintén nincsenek, így logikailag összetartozó és valamilyen jellegzetesség miatt fontosnak tekintendő területek kijelölését javaslom:

- az Internet csatlakozással és a szolgáltatás igénybevételével kapcsolatos általános biztonsági követelmények;
- a szervezeten belüli és a más szervezetekkel/személyekkel történő elektronikus levelezés rendszabályai;
- a nyílt forráskódú programok alkalmazásával kapcsolatos előírások;
- az elektronikus adatkezelő rendszerek összekapcsolásának biztonsági követelményei;
- az elektronikus adatkezelő rendszerek behatolással történő tesztelése;
- a web-site szolgáltatással kapcsolatos biztonsági követelmények;

- az elektronikus adatkezelő rendszerek biztonsági vizsgálata és értékelése;
- az elektronikus adatok törlésének-, és az adathordozók megsemmisítésének általános követelményei, beleértve azokat a speciális eseteket (minősítési jelzés vagy kezelési utasítás), amikor elektronikus adathordozó minősítési szintje nem csökkenthető;
- az elektronikus adatkezelő rendszerek biztonsági felügyeletével és monitorozásával kapcsolatos követelmények;
- a rejtjelző eszközök, eljárások és TEMPEST eszközök beszerzésével és rendszerbe állításával kapcsolatos követelmények;
- a szoftverfejlesztés, tesztelés, és rendszerbe állítás biztonsági irányelvei;
- a hozzáférés védelemre (felhasználói és rendszer szintű hozzáférések) vonatkozó általános irányelvek.

A nemzeti és szövetségi (nemzetközi) rendszerek magyarországi alrendszereire vonatkozó akkreditálás, jóváhagyás rendje és követelményei, beleértve a tanúsítványokra, vizsgálatokra, biztonsági tervekre és dokumentációkra vonatkozó követelményeket.

Az információ kezelő rendszerek ellenőrzésének és auditálásának követelményei.

A biztonsági események jelentésével és kivizsgálásával kapcsolatos általános követelmények.

A biztonsági képzés és továbbképzés általános rendje, a biztonság tudatosságra vonatkozó programok.

A szervezeti politika végrehajtására szolgáló szabályozási rend meghatározása.

Kiemelendő kérdések:

- az MH szintű szabályzatok körének meghatározása;
- a védelmi rendszabályok megvalósulására szolgáló dokumentumokkal (irányelvek, kézikönyvek, segédletek) kapcsolatos követelmények;
- a helyi szabályozók körének meghatározása és a rájuk vonatkozó általános követelmények.

A szervezeti politika felülvizsgálatára vonatkozó követelmények.

Kiemelendő kérdések:

- a felülvizsgálatért felelős szervezet;
- a felülvizsgálat gyakorisága;
- a felülvizsgálattal és a változtatási javaslatokkal kapcsolatos egyeztetési követelmények, és
- az eseti felülvizsgálatot kiváltó okok.

Az érvényben lévő nemzeti ajánlással (ITB 12. ajánlás), illetve a felváltását célzó ajánlat tervezettel (Információs Társadalom Koordinációs Tárcaközi Bizottság ajánlása (tervezet) az informatikai biztonsági irányításának követelmény rendszere (IBIK) v 0. 95; 2005. 02. 20.), valamint a „bevált gyakorlat” elv alapján kialakított Informatikai Biztonsági Kézikönyv biztonság politikára vonatkozó ajánlásával történt összehasonlítás alapján állapítható meg, hogy a fenti minimál követelmények szerint kialakított információ biztonság politika kielégíti-e a nemzeti ajánlásokat.

A szinopszis által meghatározott, kidolgozott szervezeti információ biztonság politika megfelelőségének korlátozott ellenőrzésére alkalmas:

- a COBIT Keretrendszer; Tervezés és Szervezet szakterület, P 06 jelzésű Kontroll Célkitűzés (a vezetői célok és irányvonal kommunikálása) szerinti-,
- az MSZ ISO 9001:2000 szabvány 5.6 fejezet (vezetőségi átvizsgálás) szerinti-,
- az MSZE 17799:2004 szabvány 6. fejezete (az információvédelem irányítási rendszere vezetőségi átvizsgálása) szerinti vizsgálat.

Mivel a vázolt szervezeti politika a Magyar Honvédség teljes szervezeti keretei között érvényes, így nem kétséges, hogy formailag miniszteri utasításként kell megjelennie. Ez a követelmény automatikusan tartalmazza azt is, hogy kiadás előtt az érintett szervezetek – beleértve a speciális felügyelet és irányítás alatt álló szervezeteket is – áttanulmányozzák, és véleményezik a tervezetet.

A tartalmi kérdések fontossága miatt szót kell ejteni a szabályozó hosszáról is, mert esetenként előfordul egy-egy témában előzetes követelmény meghatározása egy tervezet hosszúságára vonatkozóan (tipikus indoklás, hogy 2-3 oldalnál hosszabb szabályozót nem szabad írni, mert azt hosszúsága miatt „nem olvassák el", vagy az, hogy „az előző utasítás is két oldalas volt".

Az ilyen korlátozások súlyosan megkötik a szabályozót előkészítő kezeket, amelynek eredménye később egy félig sikerült szabályozó. A hasonló vélekedés megelőzése érdekében leszögezem, hogy a jogalkotásról szóló törvény a jogszabályok vagy az állami irányítás egyéb eszközeivel szemben támasztott követelményei között nem szerepel hosszúságra vonatkozó adminisztratív korlátozás.

Szakmai érdekesség, hogy az Egyesült Államok kormányzati információvédelmet szabályozó direktívája valóban csak néhány oldalas, ami azért lehetséges, mert a részletesen kidolgozott szabályozók miatt az általános alapelvek és követelmények azonosításakor a Védelmi Minisztériumnak elégséges volt a területet szabályozó egyéb direktívákra történő hivatkozás.

A szabályozási rend alacsonyabb szintjén az említett rendszer-specifikus információ biztonság politika feladata egy adott rendszer számára a biztonsági követelmények meghatározása.

A biztonsági követelmények a rendszer sajátosságait (az üzemeltetési környezet a lehetséges fenyegetésekkel együtt, az üzemeltetési sajátosságok és a rendszer sebezhető pontjai, a felhasználói kör, a vezetés döntése a maradvány kockázatokkal kapcsolatban) figyelembe véve alapot adnak az üzemeltetők, a biztonságért felelős személyek és a felhasználók számára készítendő helyi rendszabályok kialakításához.[72]

Összefoglalásként elmondható, hogy Magyar Honvédség a korszerű elektronikus adatkezelő képességek kialakítására irányuló erőfeszítések során olyan helyzetbe került, amikor nem halasztható tovább egy új, a környezethez-, az igényekhez- és az alkalmazott technológiához illeszkedő, rugalmas szabályozási rend kialakítása.

A NATO csatlakozás az infrastruktúrák, a rendszabályok területén olyan párhuzamosságot alakított ki a szakterületen[73], ami az erőforrások korlátozottsága miatt

[72] A rendszer-specifikus politikára jó példa a NATO és EU Biztonság Politikákban megalapozott System- specific Security Requirement Statements (SSRS), ami a 179/2003. (XI. 5.) Korm. rendeletben „Rendszer Biztonsági Utasítás"-ként nevezve jelent meg (63. §.).

[73] Annak ellenére, hogy az integrált kezelésnek egyértelmű támogatói voltak. Pl. Király Imre 2002-es cikkében a helyi szabályozás kapcsán a dokumentum biztonság területén úgy foglalt

napjainkban már nehezen finanszírozható, esetenként működési zavart okozó tényező, így ki kell használni a NATO, EU és nemzeti védelmi rendszabályok egységesítésére vonatkozó kormányzati szándékot, amelynek szervezeti, infrastrukturális és eljárási vonzatai lényegesen egyszerűsítik a védelmi rendszerek kialakítását és fenntartását.

Szervezeti síkon meg kell kezdeni a katonai szervezeteknél eddig széttagolt felelősök tevékenységének összehangolását és egy korszerű, felügyeleti elembe történő integrálását. Ezen a területen kidolgozásra szorul, hogy a felügyeleti elem hogyan kapcsolódik a vezetés általános felelősségi rendjéhez annak érdekében, hogy a biztonsági kérdések súlyuknak megfelelően kezeltek és azonnal parancsnoki (vezetői) reakciót kiváltók legyenek.

Jogszabályaink, szabványok, ajánlások és szövetségi követelmények egyaránt megfogalmazzák, hogy az információk (adatok) biztonsági felügyeletére ott van szükség, ahol az adott művelet történik. A széttagolt elhelyezkedésű, nagy létszámúnak tekinthető Magyar Honvédség esetében mindenképpen ki kell alakítani egy olyan biztonsági felügyeleti struktúrát, amely minden helyszínen képes a biztonság szempontjából lényeges kérdések reális időn belül történő kezelésére. Már nem tartható az a nézet, hogy egy, az adatkezelési képességek biztonságáért felelős személy kijelölésével (az érvényben lévő MH szabályzat szerint: a számítástechnikai titokvédelmi felelős) egy szervezetnél megnyugtatóan rendezhető a biztonság kérdése. Ezen a területen a legnagyobb kihívás a haderő-átalakítással kapcsolatos létszámcsökkentés és személyi változások, illetve az egyre korszerűbb eszközök biztonsági felügyeletéhez szükséges képzett és gyakorlott állomány mielőbbi kialakulása.

Elsőként megoldandó kérdés a szervezeti információ biztonság politika sürgős kialakítása, amelyben le kell rakni azokat az alapokat, amelyek a további szabályozáshoz szükségesek.

Ennek a politikának olyan alapelveket kell rögzítenie, amelyek egységes követelményeket tűznek a minisztérium szervei-, a Magyar Honvédség katonai szervezetei- és a miniszter irányítása és felügyelete alatt álló szervezetek elé.

A szervezeti információ biztonság politikában az egyik legfontosabb teendő annak kijelölése, hogy az MH különböző szervezetei (és azok információvédelmi szervezeti elemei) milyen szabályozókat-, mi alapján és mire vonatkozóan készítsenek el a „fentről lefelé" elv alapján. Ezzel megszüntethető az a jelenlegi helyzet, hogy a helyi – kötelezően készítendő szabályozók – csak felesleges kivonatai legyenek MH szabályzatoknak, illetve megszűnhet a szabályozók átfedésének jelensége is.

Szakítani kell a vastag, a teljes szakmai tevékenység részletes szabályozását célzó szabályzatok kialakításának hagyományával, a szabályzatokban a szervezeti elemek azonosításával, vagy a kiadáskor hatályos jogszabályok szövegeinek ismétlésével, mert az élet a szabályozók változtatásának sebességénél lényegesen gyorsabban változik.

állást, hogy „a katonai szervezetek szintjén nem célszerű külön-külön szabályzatban rögzíteni a nemzeti és a NATO adathordozók kezelésével kapcsolatos helyi eljárási szabályokat" (ÚHSZ 2002/9 85. oldal).

**KERNER Menyhért**

# INFORMÁCIÓVÉDELEM A KORMÁNYZATI ÉS A VÉDELMI SZFÉRÁBAN

Magyar Köztársaság Információs Hivatala

## Kivonat

A cikk betekintést nyújt a magyar információvédelem törvénykezési hátterébe. Rövid áttekintés ad a minősített információkkal, az információs társadalommal, az elektronikus kormányzattal és az elektronikus aláírással kapcsolatos törvényekről, rendelkezésekről. Bemutatja az információvédelemmel kapcsolatos ajánlások szerepét, információbiztonsági szempontból elemzi a Magyar Köztársaság nemzeti biztonsági koncepcióját, végül értékeli a magyar információbiztonság általános helyzetét.

## Bevezetés

Századfordulónk információtechnológiai eredményei lehetővé teszik a kormányzati és a védelmi szféra hatékonyabb működését. A kormányzat az egyes szervek szorosabb együttműködésének eredményét élvezi, továbbá az állampolgárok számára szolgáltatásokat tud biztosítani a rendelkezésére álló informatikai eszközök felhasználásával. A védelmi szférával kapcsolatban e technológiai fejlődés eredménye az egyes szervek, egységek közötti gyorsabb, nagyobb volumenű kommunikáció, ezáltal jobb együttműködés, valamint a speciális IT eszközök felhasználásával hatékonyabb feladatellátás.

Az elektronikus berendezések megjelenéséig az információvédelem gyakorlatilag rezsimintézkedéseket és fizikai biztonsági elemek használat jelentette. Az elektronikus berendezések megjelenésével szükségessé vált a kommunikációs eszközök, módszerek és a jeltovábbításra használt csatorna védelme. Az informatikai eszközök és hálózatok elterjedésével már nem volt elegendő a pont-pont kapcsolatok, valamint a papír alapú dokumentumok védelmére kialakított eljárásrend. Ezért szükségessé vált a technológiai fejlődést követtő információvédelmi ajánlások és jogszabályok kidolgozása. Mivel az információtechnológiai fejlődés igen gyors és gerjesztője nem a kormányzati és ma már a védelmi szféra sem, hanem a civil igények, ezért a szükséges információvédelmi rendelkezések a technológiák megjelenése után, csak késve születhetnek meg.

Az utóbbi évtizedben lezajlott változások, valamint hazánk NATO és EU csatlakozása szükségessé tette az információvédelemmel, adatbiztonsággal kapcsolatos hiányzó jogszabályok megalkotását, ajánlások kidolgozását. Ez alapvetően EU, NATO és egyéb nemzetközi jogszabályok átvételét, nemzetközi ajánlások (pl. Common Criteria) lefordítását, adaptációját jelenteti. A védelmi szférával kapcsolatban a törvénykezési munkán túl szükséges volt a szervezeti háttér megteremtésére is. Így jött létre például a Nemzeti Biztonsági Felügyelet (NBF), mely a NATO, az EU illetékes szervezeteivel kapcsolatos követelmények betartatásáért felelős. E jogharmonizáción kívül a magyar kormányzat erőfeszítéseket tesz hazánk informatikai lemaradásának csökkentése érdekében (optimista becslés szerint is a lakosság 15-20% használja csak a világhálót [1]). A stratégiai cél a nyugati fejlett gazdaságokhoz való felzárkózás,

amit nem lehet elérni informatikai fejlesztés nélkül. Az információs társadalom elérése érdekében kialakították a szükséges intézményi hátteret, jogi környezet.

A kormányzati munka eredményeként megszülettek információs társadalommal, azon belül az elektronikus aláírással, elektronikus közigazgatással kapcsolatos törvények és rendelkezések. Az információbiztonság területének felértékelődését jelzi az új magyar nemzeti biztonsági stratégia, mely kiemelten foglakozik az informatikai kockázatokkal.

## Minősített információk védelme

Az információvédelemmel kapcsolatos törvények, kormányrendeletek [2-5] csak lassan születtek meg, ahogy másutt is a kormányzat csak lassan tudja követni a gyors informatikai technikai fejlődést. Ezt a folyamatot gyorsította fel hazánk a NATO-hoz, majd az EU-hoz való csatlakozása.

A követezőekben részletezem az információvédelemmel kapcsolatos főbb hatályos törvényeket, rendeleteket.

Az 1995. évi LXV., valamint az ezt módosító 2003. évi LIII. törvény, az államtitokról és a szolgálati titokról, szabályozza a külföldi minősítés jelölését, besorolásuk szempontjait. Külföldi minősítéseket és jelöléseket tartalmaz a Magyar Kormánya által az információbiztonság tárgyában kötött nemzetközi szerződések alapján. A NATO, a Nyugat-Európai Unió, az Európai Tanács, az Európai Bizottság és az Európai Atomenergia Közösség által használt minősítéseket és a magyar megfelelőit tartalmazza. A védelmi szféra számára a NATO-val kapcsolatos rendelkezések a kiemelten fontosak, mert szabályozza az illetékes NATO szervekkel való kapcsolattartás követelményrendszerét. A minősítési jelölést jól átgondolt szempontrendszer alapján kell megállapítani, amit e törvény részletesen tárgyal. A törvény mindamellett, hogy némileg módosította a használt minősítési megjelöléseket, minősítési szempontokat, rendelkezik a Nemzeti Biztonsági Felügyelet (továbbiakban: NBF) létrehozásáról, melynek feladata a NATO, a NyEU, az Európai Unió Tanácsa, az Európai Bizottság és az EURATOM Biztonsági szabályzatában előírt követelmények érvényesítése. Az NBF a Miniszterelnöki Hivatal szervezeti keretében működő, önálló feladattal és hatósági feladattal rendelkező szervezet.

A 179/2003. (XI. 5.) kormányrendelet a nemzetközi szerződés alapján átvett, vagy nemzeti kötelezettségvállalás alapján készült minősített adat védelmének eljárási rendjéről szól. A rendelt hatálya azon minősített adatokra és az őket kezelő szervekre terjed ki, melyek esetén a nemzetközi szerződést kihirdető törvény biztonsági hatóságként az NBF-et jelöli ki. Ugyanez a rendelet alkalmazásában értelmezi a használt kifejezéseket, melyek közül számunkra az elektronikus adatkezelés, az elektronikus biztonság, a rendszer, nemzetközi hatáskörű rendszer, NATO, rendszer, összekapcsolt rendszer fogalmai fontosak. A rendelet részletesen kitér a rendszer elemeivel kapcsolatos biztonsági követelményekre, ezen belül kiemelten foglalkozik a fizikai biztonság és az adatkezelés adminisztratív kötelezettségeivel. Informatikai szemszögből a használt adathordozókra, operációs rendszerekre, működtető programok installációjára általánosságban, az azonosítás, jelszóhasználat, naplózás adminisztratív kérdéseire részletesen tér ki. Informatikai rendszerekre, velük kapcsolatos információbiztonsági kérdésekre a kormányrendelet nem tér ki. Az előírás szerint külföldi minősítéssel és jelöléssel ellátott adat "Bizalmas!" minősítési szintig nemzeti rejtjelző eszközön továbbítható, valamint a "Bizalmas!" és alacsonyabb minősítéssel ellátott külföldi minő-

sítéssel és jelöléssel ellátott adat védelmére a NATO, NYEU, illetve az EU illetékes szerve vagy az Országos Rejtjelfelügyelet által jóváhagyott rejtjelző eszköz alkalmazható. A "Titkos!" vagy "Szigorúan titkos!" külföldi minősítéssel és jelöléssel ellátott adat rejtjelzéssel történő védelmére kizárólag a NATO, NYEU, illetve az EU illetékes szerve által jóváhagyott rejtjelző eszközök alkalmazhatóak. Vagyis ebben az esetben az Országos Rejtjelfelügyelet csak a rejtjelző eszközök rendszeresítését, használatbavételét engedélyezi.

A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény meghatározza a nemzetbiztonsági szolgálatok feladatait. A nemzetbiztonsági szolgálatok rendeltetése, hogy az e törvényben meghatározott feladatok elvégzésével, a nyílt és a titkos információgyűjtés eszközrendszerével elősegítsék a Magyar Köztársaság nemzetbiztonsági érdekeinek érvényesítését, ezáltal közreműködjenek az ország szuverenitásának biztosításában és alkotmányos rendjének védelmében. A törvény az Információs Hivatal számára a hírszerzéssel kapcsolatos feladatai mellet feladatául teszi a rejtjeltevékenység szakirányítását, hatósági engedélyezését, felügyeletét és rejtjelkulcs előállítását (Országos Rejtjelfelügyelet).

Vagyis a nem NATO és EU minősítésű adatok esetén, míg a fizikai biztonság és az adatkezelés eljárásrendje részletesen szabályozott és a rejtjelzés kérdése is megoldott, addig az informatikai rendszerek információvédelmével kapcsolatos kérdések nem szabályozottak.

A NATO jellegénél fogva kiemelten kezeli az információvédelemmel kapcsolatos feladatokat. A NATO-n belül bizottságok jöttek létre az információvédelem egy-egy területének lefedésére.

Továbbiakban a NATO illetve az EU információvédelemmel kapcsolatos rendelkezéseit tekintem át [6-9], informatikai szemszögből.

A NATO C-M(2002)49 rendelkezés, mely NATO-n belüli biztonságról szól, AC/35-D/2002 NATO Biztonsági Bizottsági direktíva, az AC/35 – D/2004 Elektronikus Információbiztonsági (INFOSEC) Eljárásrend, valamint az AC/35 – D/2005 CIS rendszerek INFOSEC Menedzsment Eljárásrendjéről szóló utasítások rendezik a NATO-n belüli elektronikus információvédelmi kérdéseket. A NATO-n belül az INFOSEC biztonsági intézkedések alkalmazását jelenti a kommunikációs, informatikai vagy más elektronikus rendszerben feldolgozott, tárolt illetve továbbított információk védelme érdekében, melyek biztosítják a rendszerben az információ bizalmasságának, integritásának és rendelkezésre állásának védelmét. Továbbá rendelkezik Nemzeti Biztonsági Felügyelet létrehozásáról minden tagországban, melynek feladata a NATO minősített információk védelme. Részletezi a tagországonkénti Nemzeti Biztonsági Felügyeletek feladatait.

A NATO szervezetén belüli információbiztonság fontosságát jól szemlélteti, hogy NATO Biztonsági Bizottságot (NSC) állított fel, mely közvetlenül az Észak – Atlanti Tanácsnak van alárendelve. A NATO Biztonsági Hivatalát (NOS) a NATO Nemzetközi Törzsén belül hozták létre. A NOS feladata a NATO biztonságának vizsgálata, azon eszközök meghatározása, melyeken keresztül a NATO biztonságát lehet javítani, koordináció a többi szerv között, valamint a NATO minősített információk védelmét ellátó biztonsági rendszerek rendszeres ellenőrzése. A direktíva részletesen rendelkezik a tekintetben, hogy milyen esetekben kell rejtjelzést alkalmazni az adatok

védelme érdekében, a rejtjelző módszereit a NATO Katonai Bizottsága (NAMILCOM) hagyja jóvá (NS vagy magasabb minősítések esetén).

A NATO biztonsági szabályzatai részletesen rendelkeznek a minősített adatok fizikai biztonságát, illetve a vele kapcsolatos adminisztratív eljárásrendről, rezsim intézkedésekről. Foglalkozik ez elektromágneses kisugárzás és továbbítás körével, de kerüli az informatikai rendszerekkel kapcsolatos információvédelem kérdését.

Az Európai Unió kevésbé részletesen szabályozza az információbiztonság területét, de mutat némi átfedést a NATO vonatkozó direktíváival.

Az Európai Unió Tanácsának 2001/264/EK számú biztonsági szabályzata írja le a tagállamok információbiztonságával, EU minősített anyagok kezelésével kapcsolatos rendelkezéseket. A minősített dokumentumok kezelésének szabályozása mellett foglalkozik az IT és kommunikációs rendszerekben kezelt információk védelmével is. Külön kitér az információbiztonság fogalmára, de további segítséget nem ad. A szabályzat értelmében csak akkreditált kommunikációs központok és hálózatok és/vagy terminálok és rendszerek továbbíthatnak CONFIDENTIEL UE és SECRET UE minősítésű információkat. Vagyis a kommunikációs csatorna minden elemének akkreditáltnak kell lennie.

### Elektronikus aláírás

Egy-két évvel a vonatkozó USA és EU jogszabályok megszületése után tették közzé a magyar elektronikus aláírásról szóló törvényt. A 2001. évi XXXV. törvény az elektronikus aláírásról annak érdekében született, hogy a meglévő hiányt pótolva, megteremtse a hiteles elektronikus nyilatkozattétel, valamint adattovábbítás jogszabályi feltételeit az üzleti életben, a közigazgatásban és az információs társadalom által érintett más területeken.

Az elektronikus aláírással kapcsolatos szolgáltatás lehet elektronikus aláírás hitelesítés, időbélyegzés, aláírás-létrehozó eszközön aláírás-létrehozó adat elhelyezése és elektronikus archiválás.

E jogszabály esetén újdonság, hogy a törvény technológiakövetést ír elő, mely során a Hatóság figyelemmel kíséri az elektronikus aláírással kapcsolatos technológiák és kriptográfiai algoritmusok fejlődését, határozatba foglalja a szolgáltatók által szolgáltatásaik nyújtása során használható biztonságos kriptográfiai algoritmusokat és az azok meghatározott paraméterekkel történő alkalmazására vonatkozó követelményeket. A törvény szerint az elektronikus aláírással kapcsolatos termékek tanúsítását nem valamely szerv, vagy hivatal végzi, hanem az erre kérelmet benyújtott szakértelemmel rendelkező szervezet vagy személy. Ez a megoldás különbözik a rejtjeltevékenységgel kapcsolatos eljárástól, amikor a rejtjelzéssel kapcsolatos hasonló feladatokat az Országos Rejtjelfelügyelet végzi. Ezt azért érdemes kiemelni, mert az elektronikus aláírás, mint eljárás ugyanúgy kriptográfiai módszereket használ.

Új elem az informatikával kapcsolatos szabályozások esetén, hogy az IHM közleményt adott ki, melyben a 20/2004. (IV. 21.) PM rendelet 5. § (3) bekezdése alapján az elektronikus aláírással ellátott számlák kiállításához és azokra vonatkozó megőrzési kötelezettség teljesítéséhez alkalmazott elektronikus aláírás és időbélyegző használatához biztonságos kriptográfiai algoritmusokat (valamint paramétereire vonatkozó követelményeket) határozott meg, amit táblázat formájában közzétett. Ez az elektronikus aláírással foglalkozó törvény technológiakövetéssel kapcsolatos rendel-

kezésének következménye. Felmerül a kérdés, hogy kriptográfiai kérdésekben az IHM a legmegfelelőbb (pedig illetékes) szerv, miután rejtjelzéssel kapcsolatos szakértői munka nem tartozik alapvetően a tevékenységi körébe.

A 40/2004. (XII. 21.) IM rendelet az elektronikus cégbejegyzési és cégnyilvántartásról rendelkezik.

Az 151/2001. (IX. 1.) és a 47/2002. (III. 26.) kormányrendeletek helyébe a némileg finomított 45/2005. (III. 11.) kormányrendelet lépett, mely a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással kapcsolatos feladat- és hatásköréről, valamint eljárásának részletes szabályairól a Nemzeti Hírközlési Hatóságnak az elektronikus aláírásról szóló 2001. évi XXXV. törvénnyel kapcsolatos feladatait és hatáskörét határozza meg. A rendelkezés az Európai Parlament és a Tanács, az elektronikus aláírásra vonatkozó közösségi keretfeltételekről szóló 1999/93/EK irányelvének való megfelelést szolgálja.

### Elektronikus közigazgatás

Az Európa Tanács 2002-es lisszaboni célkitűzése az EU a tudásalapú gazdasági területté való alakítása volt. Az Unióban ennek következtében elkezdődött az E-Europa program kidolgozása. Az információs társadalom elérése érdekében hazánkban is megszülettek a hiányzó törvények és kormányrendeletek.

A 1039/1993. (V.21.) kormányhatározat alapján alakult meg a Miniszterelnöki Hivatalon belül az Informatikai Tárcaközi Bizottság, melynek feladata az információs társadalommal kapcsolatos célok elérésének támogatása volt. A bizottság felügyelete alatt a hazai informatikai szakma számára fontos ajánlásokat tettek közzé.

A stratégiai célok megvalósítása érdekében a kormányhatározatok (1188/2002. (XI. 7.), 1214/2002. (XII. 28.)) születtek az Elektronikus Kormányzati Gerinchálózat (továbbiakban EKG) és az Informatikai Közháló (továbbiakban KözHáló) létrehozásával kapcsolatban. A programot az Európa tervben meghatározott legfontosabb célkitűzések elérése érdekében indították el és az Informatikai és Hírközlési Minisztérium felügyelete alá rendelték.

A kormányhatározatok a kormányzati, közigazgatási adatbázisok és informatikai rendszerek nagysebességű országos elektronikus kormányzat alapinfrastruktúrába való összekapcsolása érdekében születtek. Az EKG-ba be nem vont, a kormányzati informatikába nem tartozó helyi közigazgatási szervek, közintézmények, közfeladatot ellátó egyéb szervek, civil szervezetek informatikai ellátásának biztosítására ki kell alakítani az EKG-val együttműködésre alkalmas Informatikai Közhálót.

Információvédelmi szempontból fontos, hogy a határozatok, habár csak általánosan de foglalkoznak az információbiztonság kérdésével. A törvényhozó szándéka szerint az EKG nagy sebességű, nagy üzembiztosságú és magas biztonsági követelményeknek megfelelő, egységes architektúrájú hálózati infrastruktúra. A gerinchálózat kialakításával párhuzamosan létre kell hozni a gerinchálózat és a kapcsolódó hálózatok átfogó biztonsági rendszereit, valamint ki kell dolgozni a biztonsági szabályzatokat.

Fontos még megemlíteni az eTár-at, mely egy adatbázis, amelynek segítségével bármilyen katasztrófa vagy krízis után újra lehet indítani a nagy közigazgatási és államigazgatási rendszereket, ennek a rendszernek az alapjait 2005 folyamán szeretnénk lerakni.

A 184/2004. (VI. 3.) és a 1053/2004. (VI. 3.) kormányrendeletek az elektronikus közigazgatási ügyintézés megvalósítása érdekében születtek. A Kormány e sza-

bályozásokat az információs társadalom célkitűzései közé sorolható elektronikus közigazgatási ügyintézés lehetőségének biztosítása érdekében hozta meg.

A 1066/2004. (VII. 6.) kormányhatározat az IDA programban (Interchange of Data between Administrations, Kormányzati szervezetek közötti adatcsere) történő részvételről és a kormányzati szervezeteknek az EKG-n keresztüli TESTA (Trans European Services for Telematics between Administrations, Kormányzati szervezetek közötti páneurópai telematikai szolgáltatások) hálózathoz való csatlakozásáról rendelkezik. Továbbá felhatalmazza a kormányzati informatikáért felelős kormánymegbízottat, hogy készítse elő a Magyar Köztársaságnak az IDABC (Interoperable Delivery of pan-European eGovernment Services to Public Administrations, Businesses and Citizens, Páneurópai e-kormányzati szolgáltatások nyújtása közigazgatási szervezetek, üzleti vállalkozások és állampolgárok számára) programban való részvételét. Evvel lehetővé válik európai kormányzati rendszerekbe való integrálódás.

### Információbiztonság és a Magyar Köztársaság nemzeti biztonsági stratégiája

A Magyar Köztársaság nemzeti biztonsági stratégiája (2073/2004. (III. 31.) kormányhatározat) [10] az országgyűlés 94/1998. (XII. 29.) OGY a Magyar Köztársaság biztonság- és védelempolitikájának alapelveiről szóló határozat alapján született meg, mely kimondja, hogy a Magyar Köztársaság kormánya a felelős a nemzeti biztonsági stratégia, valamint a nemzeti katonai stratégia kidolgozásáért. A magyar nemzeti biztonsági stratégia összhangban van a NATO 1999. évi Stratégiai Koncepciójával és az EU által 2003-ban elfogadott Európai Biztonsági Stratégiával.

A koncepció II.1. cikkelye, mely a globális kihívásokkal foglakozik, megállapítja, hogy a globalizáció eredményeként új típusú biztonsági kockázatok jelentek meg, különösen az információs technológia, a közlekedés, a kereskedelem és a pénzügyek területén. Az USA elleni 2001. szeptember 11-ei terrortámadás jelezte a terrorizmus növekvő stratégiai fenyegetéssé válását az euró-atlanti térség biztonságára. (A 2005. év júliusi londoni terroresemények ezt a megállapítást tovább erősítik.)

Új elemként jelent meg a dokumentumban az információs társadalom kihívásai (II.1.6.), az ezt részletező fejezetben kitér hazánk a fejlett világ információs és telekommunikációs színvonalához való felzárkózásának, az oktatás színvonala emelésének szükségességére.

„Az informatikai infrastruktúra technikai és szellemi feltételeinek biztosítása mellett ügyelni kell e rendszerek védelmére és a megfelelő tartalékok képzésére is. Az informatika számtalan lehetőséget teremtett a társadalom számára, de fokozta annak veszélyeztetettségét. A számítógépes hálózatok és rendszerek sebezhetősége, túlterhelése, az információlopás, a vírusterjesztés és a dezinformáció kockázati tényezőt jelent az ország számára."

A fenti idézet alátámasztása annak a folyamatnak, mely az információvédelem általános felértékelődését jelzi. A kormányzatok (itthon és külföldön egyaránt) egyre inkább kezdik felismerni azt, hogy az információvédelem nemzeti érdek, a nemzetbiztonságot érintő terület.

Az információs rendszerek védelme (III.3.7.) jelenti a korszerű és biztonságos informatikai infrastruktúra kialakítását és a kormányzati információs rendszerek védelmét.

„A kormányzati információs rendszert fel kell készíteni a kibernetikai támadások megelőzésére és kivédésére. A védelem sikere érdekében szoros koordináció szükséges mind a szövetségesekkel, mind az informatikai és távközlési szolgáltatók, valamint kutatóközpontok között." Vagyis közös erőkifejtésre van szükség a szövetséges államokkal, valamint a kormányzanak a civil szférával együtt.

A nemzeti biztonsági stratégia végrehajtásának hátterét a tartósan növekedési pályán mozgó nemzetgazdaság adja.

Végezetül a stratégia a rendvédelmi szervek fokozott együttműködésében és szervezeti korszerűsítésében nevezi meg biztonsági kihívások eredményes kezelésének módját. Ez természetesen az informatika területére is érvényes megállapítás.

## Információvédelemmel kapcsolatos kritériumrendszerek, ajánlások

A fent említett törvények, rendelkezések csak a keretet adják az információvédelemmel kapcsolatos munkának, valamint a civil szféra igényei mások, mint a kormányzati, illetve a védelmi szférának. A hiányt információvédelemmel kapcsolatos ajánlások, kritériumrendszerek alkalmazása töltheti ki.

Az informatikai rendszerek egyre szélesebb elterjedése során igény mutatkozott olyan eljárásokra, kritériumrendszerekre, melyekkel azonos feltételek között lehet vizsgálni a rendszereket, a vizsgálat eredménye csak a rendszerek paramétereitől függ (pl. nem függ a vizsgálatot lefolytató személytől, helytől, időponttól). Egymástól függetlenül hoztak létre több követelményrendszert is, Európában és az USA-ban. Az egymástól többé-kevésbé függetlenül kidolgozott kritériumrendszerek, az európai ITSEC, az amerikai TCSEC és FC, valamint a kanadai CTCPEC ajánlások hibáit, hiányosságait kiküszöbölendő jött létre 1996-ban az ISO által is támogatásával Common Criteria for Information Technology Security Evaluation (továbbiakban: CC) [11]. Létrehozói felismerték az egységes kritériumrendszer létrehozásának szükségességét. Célként tűzték ki a technikai fejlődésnek inkább megfelelő, nemzetközileg elfogadhatóbb, ellentmondásoktól mentes követelményrendszer megalkotását.

A CC nem foglalkozik a speciális biztonsági mechanizmusok értékelésével, mint például az országonként változó kriptográfiai eljárások, de megnevezi a fenyegetettségeket, amit ezek felhasználásával lehet kivédeni.

## Összefoglalás

Megszületett az elektronikus aláírással kapcsolatos törvény, az információs társadalom és az elektronikus közigazgatással összefüggő kormányhatározatok alapján kormányzati informatikai fejlesztések zajlanak. Míg a minősített anyagok kezelésével összefüggő törvényi háttér mára teljessé vált, addig az informatika témakörében az információbiztonsággal kapcsolatos jogszabályok, kormányrendeletek még csak kialakulóban vannak. Ezért jobb híján a dokumentumokkal kapcsolatos rendelkezések adaptálására kell szorítkozni, valamint a nemzetközileg elterjedt szabványok, ajánlások a helyi viszonyok közötti használatára.

Látható az Internet alapú szolgáltatások gyors fejlődése, melyet alapvetően a civil szféra igényei gerjesztenek. A védelmi szféra, tekintettel a tárolt, valamint az egyes szervek között áramló információk fontosságára (jelentős része minősített), érzékeny az információvédelem kérdéseire. A védelmi szféra számára alapvetően fontos a hitelesség, rendelkezésre állás és bizalmasság együttes megőrzése.

A gyors informatikai, technológiai fejlődéssel együtt, mely hatékonyabbá teszi a kormányzat és a védelmi szféra működését, együtt kell, hogy járjon az információbiztonság fejlődése is. Ezért az információbiztonság növelése érdekében a kormányzatnak, a védelmi és a civil szférának is egyaránt erőfeszítéseket kell tennie. Az erőfeszítések nem csak új módszerek, technológiák fejlesztését jelentik, hanem rendelkezések, nemzetközi ajánlások kidolgozását is.

## Felhasznált irodalom


[1] http://www.hte.hu/kiadvanyok/hirlev2005/hirlevel_2005jan02.html, 2005. 06. 29.

[2] A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény

[3] Az 1995. évi LXV., valamint az ezt módosító 2003. évi LIII. törvény az államtitokról és a szolgálati titokról, Magyar Közlöny 2003/83. szám, 6552. oldal

[4] A nemzetközi szerződés alapján átvett, vagy nemzeti kötelezettségvállalás alapján készült minősített adat védelmének eljárási rendjéről szóló 179/2003. (XI. 5.) kormányrendelet, Magyar közlöny 2003/126. szám, 9454. oldal

[5] Az elektronikus aláírásról szóló 2001. évi XXXV. törvény

[6] NATO C-M(2002)49 direktíva

[7] NATO Biztonsági Bizottság: Az információk Biztonságáról szóló utasítás, 2002. június 17., AC/35-D/2002

[8] AC/35 – D/2004 Elektronikus Információbiztonsági (INFOSEC) Eljárásrend

[9] NATO Biztonsági Bizottság: A Híradó és Informatikai Rendszerek (CIS) Információs Bizottsága (INFOSEC) által kiadott menedzsment direktívája, 2002. június 17., AC/35-D/2005

[10] 2073/2004. (III. 31.) kormányhatározat a Magyar Köztársaság nemzeti biztonsági stratégiájáról

[11] Computer Security Criteria: Security Evaluations and Assessment, http://www.oracle.com/technology/deploy/security/seceval/pdf/seceval_wp.pdf , 2005. 01. 13.

**KERNER Menyhért**

# AZ INFORMATIKA HAZAI JOGI KÖRNYEZETÉNEK INFORMÁCIÓBIZTONSÁGI SZEMPONTBÓL VALÓ VIZSGÁLATA

Magyar Köztársaság Információs Hivatala

## Kivonat

A cikk betekintést nyújt a magyar informatikai törvénykezés hátterébe, foglakozik az információvédelem témakörével. Rövid áttekintés nyújt az információs társadalommal, az elektronikus kormányzattal és az elektronikus aláírással kapcsolatos törvényekről, rendeletekről. Információbiztonsági szempontból elemzi a Magyar Köztársaság nemzeti biztonsági koncepcióját, és értékeli a magyar információbiztonság helyzetét.

## Bevezetés

Az ezredforduló kihívásaira válaszul egyre hangsúlyosabbá vált a magyar kormányzat azon törekvése, hogy csökkentse hazánk informatikai lemaradását (optimista becslés szerint is a lakosság 15-20% használja csak a világhálót [1]). Cél a nyugati fejlett gazdaságokhoz való felzárkózás, amit nem lehet elérni informatikai fejlesztés nélkül. A kormányzat felismerte, hogy ennek elérése aktív kormányzati támogatás nélkül nem lehetséges, ezért célul tűzte ki az információs társadalom elérését. Az információs társadalom elérése érdekében kialakították a szükséges intézményi hátteret és a szükséges jogi környezetet. Ezt a folyamatot felgyorsította a NATO és az EU követelményeknek való megfelelés kényszere, valamint az E-Europa programmal kapcsolatos hazai elvárások. A kormányzati munka eredményeként megszülettek az elektronikus aláírással, elektronikus közigazgatással kapcsolatos törvények és rendelkezések. Az új magyar nemzeti biztonsági stratégia kiemelten foglakozik az informatikai kockázatokkal, mely e terület növekvő súlyát jelzi.

## Elektronikus aláírás

Egy-két évvel a vonatkozó USA és EU jogszabályok megszületése után tették közzé a magyar elektronikus aláírásról szóló törvényt. A 2001. évi XXXV. törvény az elektronikus aláírásról annak érdekében született, hogy a meglévő hiányt pótolva, megteremtse a hiteles elektronikus nyilatkozattétel, valamint adattovábbítás jogszabályi feltételeit az üzleti életben, a közigazgatásban és az információs társadalom által érintett más területeken.

A törvény részletezi az elektronikus aláírással kapcsolatos szolgáltatások körét, mely elektronikus aláírás hitelesítés-szolgáltatás, időbélyegzés, aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése és az elektronikus archiválás szolgáltatás lehet.

E jogszabály esetén újdonság, hogy a törvény technológiakövetést ír elő, mely során a Hatóság figyelemmel kíséri az elektronikus aláírással kapcsolatos technológiák és kriptográfiai algoritmusok fejlődését, határozatba foglalja a szolgáltatók által szolgáltatásaik nyújtása során használható biztonságos kriptográfiai algoritmusokat és az

azok meghatározott paraméterekkel történő alkalmazására vonatkozó követelményeket.

Tanúsító szervezetek kapcsolatban a következőket rendeli el:

„Az aláíró eszközök és egyéb elektronikus aláírási termékek tanúsítására jogosult tanúsító szervezetként a miniszter azokat a természetes személyeket és szervezeteket jelöli ki, amelyek erre vonatkozó kérelmet nyújtanak be, és rendelkeznek az aláíró eszközök és egyéb elektronikus aláírási termékek tanúsításához szükséges szakértelemmel."

Vagyis az elektronikus aláírással kapcsolatos termékek tanúsítását nem valamely szerv, vagy hivatal végzi, hanem az erre kérelmet benyújtott szakértelemmel rendelkező szervezet vagy személy. Ez a megoldás különbözik a rejtjeltevékenységgel kapcsolatos eljárástól, amikor a rejtjelzéssel kapcsolatos hasonló feladatokat az Országos Rejtjelfelügyelet végzi. Ez azért is érdekes, mert az elektronikus aláírás, mint eljárás ugyanúgy kriptográfiai módszereket használ.

Végül a törvény utal előzményeire, melyek az Európai Parlament és a Tanács 1999/93/EK irányelvével az elektronikus aláírások közösségi programjáról, továbbá az Európai Parlament és a Tanács 2000/31/EK irányelvének az információs társadalom szolgáltatásai bizonyos jogi szempontjairól a Belső Piacon, különös tekintettel az elektronikus kereskedelemre („Elektronikus kereskedelmi irányelv") 9. Cikke 2. bekezdésével.

Új elem az informatikával kapcsolatos szabályozások esetén, hogy az IHM közleményt adott ki, melyben a 20/2004. (IV. 21.) PM rendelet 5. § (3) bekezdése alapján az elektronikus aláírással ellátott számlák kiállításához és azokra vonatkozó megőrzési kötelezettség teljesítéséhez alkalmazott elektronikus aláírás és időbélyegző használatához biztonságos kriptográfiai algoritmusokat (valamint paramétereire vonatkozó követelményeket) határozott meg, amit táblázat formájában közzétett. Ez az elektronikus aláírással foglalkozó törvény technológiakövetéssel kapcsolatos rendelkezésének következménye. Persze felmerül a kérdés, hogy kriptográfiai kérdésekben az IHM a legmegfelelőbb (pedig illetékes) szerv, miután rejtjelzéssel kapcsolatos szakértői munka nem tartozik alapvetően a tevékenységi körébe.

A 40/2004. (XII. 21.) IM rendelet az elektronikus cégbejegyzési és cégnyilvántartásról rendelkezik.

Az 151/2001. (IX. 1.) és a 47/2002. (III. 26.) kormányrendeletek helyébe a némileg finomított 45/2005. (III. 11.) kormányrendelet lépett, mely a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással kapcsolatos feladat- és hatásköréről, valamint eljárásának részletes szabályairól a Nemzeti Hírközlési Hatóságnak az elektronikus aláírásról szóló 2001. évi XXXV. törvénnyel kapcsolatos feladatait és hatáskörét határozza meg. A rendelkezés az Európai Parlament és a Tanács, az elektronikus aláírásra vonatkozó közösségi keretfeltételekről szóló 1999/93/EK irányelvének való megfelelést szolgálja.

### Hazai elektronikus közigazgatás

Az Európa Tanács 2002-es lisszaboni célkitűzése az Unió tudásalapú gazdasági területté való alakítását tartalmazta. Az Unióban ennek következtében elkezdődött az E-Europa program. Az információs társadalom létrehozása érdekében hazánkban is megszülettek a hiányzó törvények és kormányrendeletek.

A 1039/1993. (V.21.) kormányhatározat alapján alakult meg a Miniszterelnöki Hivatalon belül az Informatikai Tárcaközi Bizottság, melynek feladata az információs társadalommal kapcsolatos célok elérésének támogatása volt. A bizottság felügyelete alatt a hazai informatikai szakma számára fontos ajánlásokat tettek közzé.

A stratégiai célok megvalósítása érdekében Kormány a 1188/2002. (XI. 7.) kormányhatározatban fogadta el az Elektronikus Kormányzati Gerinchálózat (továbbiakban EKG) és az Informatikai Közháló (továbbiakban KözHáló) létrehozásáról szóló javaslatot. A programot az Európa tervben meghatározott legfontosabb célkitűzések elérése érdekében indították el és az Informatikai és Hírközlési Minisztérium felügyelete alá rendelték.

E kormányhatározatot követte a 1214/2002. (XII. 28.) kormányhatározat, mely a Magyar Információs Társadalom Stratégia (a továbbiakban MITS) készítéséről, a további feladatok ütemezéséről és tárcaközi bizottság létrehozásáról rendelkezik. A bizottság feladata koordinálni a Magyar Információs Társadalom Stratégiába beépülő ágazati stratégiákat és operatív intézkedési terveket, továbbá biztosítani azok összhangját a Nemzeti Fejlesztési Tervvel és az Európai Uniós irányelvekkel. Az ágazati részstratégiák kidolgozásával, a teljes program koordinációjával, valamint a távközlési szolgáltatások biztosításával az Informatikai és Hírközlési Minisztériumot (továbbiakban IHM) bízta meg a kormányhatározat. A kormányzati, közigazgatási adatbázisok és informatikai rendszerek összekapcsolására ki kell alakítani egy nagysebességű országos elektronikus kormányzat alap-infrastruktúrát. Az így kialakított EKG, és az ahhoz csatlakozó központi közigazgatási szervek nagysebességű külső Internet-csatlakozással kell, hogy rendelkezzenek. Kimondja, az EKG-ba be nem vont, a kormányzati informatikába nem tartozó helyi közigazgatási szervek, közintézmények, közfeladatot ellátó egyéb szervek, civil szervezetek informatikai ellátásának biztosítására ki kell alakítani az EKG-val együttműködésre alkalmas Informatikai Közhálót.

Az EKG kialakításának első fázisában a budapesti gerinchálózatot kell működtetni, amelyet - az illetéktelen hozzáféréssel szembeni védelem biztosítása mellett - elsődlegesen bérelt vonali szolgáltatás igénybevételével kell létrehozni.

Az EKG kialakításának második fázisában a megyei végpontokat a központtal összekötő területi gerinchálózatot kell kialakítani, szintén bérelt vonali szolgáltatás igénybevételével.

Meg kell határozni az EKG-val összefüggő biztonsági és védelmi követelményeket, feltételeket. A törvényhozó szándéka szerint az EKG nagy sebességű, nagy üzembiztosságú és magas biztonsági követelményeknek megfelelő, egységes architektúrájú hálózati infrastruktúra. A gerinchálózat kialakításával párhuzamosan létre kell hozni a gerinchálózat és a kapcsolódó hálózatok átfogó biztonsági rendszereit, valamint ki kell dolgozni a biztonsági szabályzatokat.

A KözHáló az állampolgárok és a közcélú (az Elektronikus Kormányzati Gerinchálózatba be nem vont) intézmények összekapcsolása, az Interneten keresztül. A rendszer a felhasználók számára információk és szolgáltatások elérését teszi lehetővé. Az életre hívó szándéka szerint a KözHáló program elősegíti a szélessávú Internet elérés elterjedését. A KözHáló nem állami magánhálózat, hanem igénybe veszi a piaci szereplők hálózatait és szolgáltatásait. Cél a közeljövőben az összes hazai közcélú intézmény szélessávú Internet kapcsolattal való ellátása.

2005-ben közel 40 milliárd forintból gazdálkodhat az IHM, ebből a KözHáló program folyatására, a Nemzeti Audiovizuális Archívum (NAVA) és a Nemzeti Digitális Adattár létrehozására, és újabb négyezer közösségi internetpont, e-Magyarországpont kiépítésére is jut pénz. A 2005 végétől 2008-ig tartó második szakaszban újabb 3200 ponton épül ki a szélessávú kapcsolat.[2] A közösségi Internet-hozzáférést szolgáló e-Magyarország-programra esetén a meglevő kétezer mellé újabb négyezer e-pontot építenek ki az országban. Fontos még megemlíteni az eTár-at, mely egy adatbázis, amelynek segítségével bármilyen katasztrófa vagy krízis után újra lehet indítani a nagy közigazgatási és államigazgatási rendszereket, ennek a rendszernek az alapjait 2005 folyamán szeretnénk lerakni.

A 184/2004. (VI. 3.) kormányrendelet az elektronikus közigazgatási ügyintézés megvalósítása érdekében jött létre. A Kormány e szabályozást az információs társadalom célkitűzései közé sorolható elektronikus közigazgatási ügyintézés lehetőségének biztosítása érdekében hozta meg.

A 44/2005. (III. 11.) kormányrendelet a Kormány irányítása és felügyelete alatt álló központi közigazgatási szervek kormányzati informatika koordinációjáról rendelkezik, a nemzetbiztonsági szolgálatok kivételével. (A nemzetbiztonsági szolgálatok a Nemzetbiztonsági törvény hatálya alá esnek.) Elrendeli az informatikai fejlesztések MITS-el való összhangját. Többek között előírja az informatikai biztonság elérhető legmagasabb szintjét, valamint a kormányzati informatikai rendszerek együttműködését. A MITS részét az „eKormányzat 2005 Elektronikus Kormányzat Stratégia és Programterv és az eEurope 2005 akciótervben a szolgáltató állam létrehozásához kapcsolódó reformfolyamatok képezik.

A fenti rendeletekhez kapcsolódik még a 1126/2003. (XII. 12.) kormányhatározat a Magyar Információs Társadalom Stratégiáról és Programtervről.

A 1053/2004. (VI. 3.) kormányhatározat az elektronikus közigazgatási ügyintézés és a hozzá kapcsolódó szolgáltatások megvalósításával kapcsolatos feladatokról szól. A Kormány célja olyan elektronikus közigazgatási ügyintézési környezet kialakítása, mely a szolgáltató államot jeleníti meg az elektronikus kormányzat költséghatékony megvalósítása által. Az elektronikus közigazgatási ügyintézés központi rendszerének működtetéséhez kapcsolódó informatikai szolgáltatásokra, a kormányzati portálra és az elektronikus kormányzati gerinchálózat üzemeltetésére tér ki.

A 1066/2004. (VII. 6.) kormányhatározat az IDA programban (Interchange of Data between Administrations, Kormányzati szervezetek közötti adatcsere) történő részvételről és a kormányzati szervezeteknek az EKG-n keresztüli TESTA (Trans European Services for Telematics between Administrations, Kormányzati szervezetek közötti páneurópai telematikai szolgáltatások) hálózathoz való csatlakozásáról rendelkezik. Továbbá felhatalmazza a kormányzati informatikáért felelős kormánymegbízottat, hogy készítse elő a Magyar Köztársaságnak az IDABC (Interoperable Delivery of pan-European eGovernment Services to Public Administrations, Businesses and Citizens, Páneurópai e-kormányzati szolgáltatások nyújtása közigazgatási szervezetek, üzleti vállalkozások és állampolgárok számára) programban való részvételét. Evvel lehetővé válik európai kormányzati rendszerekbe való integrálódás.

A 1113/2003. (XI. 11.) kormányhatározat a közigazgatási szolgáltatások korszerűsítési programjáról rendelkezik.

A 1126/2003. (XII. 12.) kormányhatározat a Magyar Információs Társadalom Stratégiáról és annak végrehajtásáról rendelkezik. A MITS részét is képező „eKormányzat 2005 Elektronikus Kormányzat Stratégia és Programterv csatlakozik eEurope 2005 akcióprogramhoz, valamint az EU tagállamainak az elektronikus kormányzat keretében nyújtott alapvető közszolgáltatásokat felsoroló ajánlásában megjelölt e-kormányzati szolgáltatások megvalósítására. A MITS-ben foglalt feladatok megvalósítása során a koordinációt az Információs Társadalom Koordinációs Tárcaközi Bizottság látja el. A szolgáltató állam létrehozásához kapcsolódó reformfolyamatok felgyorsítása érdekében a közigazgatási szolgáltatások korszerűsítésével kapcsolatos feladatokat összehangoló Koordinációs Bizottság (2124/2003. (VI. 6.) kormányhatározat) irányítása alatt E-kormányzat Operatív Bizottságot hoz létre.

### Információbiztonság és a Magyar Köztársaság nemzeti biztonsági stratégiája

A Magyar Köztársaság nemzeti biztonsági stratégiája (2073/2004. (III. 31.) kormányhatározat) [3] az országgyűlés 94/1998. (XII. 29.) OGY a Magyar Köztársaság biztonság- és védelempolitikájának alapelveiről szóló határozat alapján született meg, mely kimondja, hogy a Magyar Köztársaság kormánya a felelős a nemzeti biztonsági stratégia, valamint a nemzeti katonai stratégia kidolgozásáért. A magyar nemzeti biztonsági stratégia összhangban van a NATO 1999. évi Stratégiai Koncepciójával és az EU által 2003-ban elfogadott Európai Biztonsági Stratégiával.

A koncepció II.1. cikkelye, mely a globális kihívásokkal foglakozik, megállapítja, hogy a globalizáció eredményeként új típusú biztonsági kockázatok jelentek meg, különösen az információs technológia, a közlekedés, a kereskedelem és a pénzügyek területén. Az USA elleni 2001. szeptember 11-ei terrortámadás jelezte a terrorizmus növekvő stratégiai fenyegetéssé válását az euro-atlanti térség biztonságára. (A 2005. év júliusi londoni terroresemények ezt a megállapítást tovább erősítik.)

Új elemként jelent meg a dokumentumban az információs társadalom kihívásai (II.1.6.), az ezt részletező fejezetben kitér hazánk a fejlett világ információs és telekommunikációs színvonalához való felzárkózásának, az oktatás színvonala emelésének szükségességére.

„Az informatikai infrastruktúra technikai és szellemi feltételeinek biztosítása mellett ügyelni kell e rendszerek védelmére és a megfelelő tartalékok képzésére is. Az informatika számtalan lehetőséget teremtett a társadalom számára, de fokozta annak veszélyeztetettségét. A számítógépes hálózatok és rendszerek sebezhetősége, túlterhelése, az információlopás, a vírusterjesztés és a dezinformáció kockázati tényezőt jelent az ország számára."

A fenti idézet alátámasztása annak a folyamatnak, mely az információvédelem általános felértékelődését jelzi. A kormányzatok (itthon és külföldön egyaránt) egyre inkább kezdik felismerni azt, hogy az információvédelem nemzeti érdek, a nemzetbiztonságot érintő terület.

Az információs rendszerek védelme (III.3.7.) jelenti a korszerű és biztonságos informatikai infrastruktúra kialakítását és a kormányzati információs rendszerek védelmét.

„A kormányzati információs rendszert fel kell készíteni a kibernetikai támadások megelőzésére és kivédésére. A védelem sikere érdekében szoros koordináció szükséges mind a szövetségesekkel, mind az informatikai és távközlési szolgáltatók,

valamint kutatóközpontok között." Vagyis közös erőkifejtésre van szükség a szövetséges államokkal, valamint a kormányzanak a civil szférával együtt.

A nemzeti biztonsági stratégia végrehajtásának hátterét a tartósan növekedési pályán mozgó nemzetgazdaság adja.

Végezetül a stratégia a rendvédelmi szervek fokozott együttműködésében és szervezeti korszerűsítésében nevezi meg biztonsági kihívások eredményes kezelésének módját. Ez természetesen az informatika területére is érvényes megállapítás.

### Minősített adatok védelme

A minősített dokumentumokkal kapcsolatos jogalkotás alapját az államtitokról és a szolgálati titokról szóló 2003. évi LIII. törvény adja, mely az információbiztonság tárgyában kötött nemzetközi szerződések alapján használt külföldi minősítésű dokumentumokkal foglalkozik. Tartalmazza a NATO, a Nyugat-Európai Unió, az Európai Tanács, az Európai Bizottság és az Európai Atomenergia Közösség által használt minősítéseket, valamint magyar megfelelőit. E törvényt egészíti ki a nemzetközi szerződés alapján átvett, vagy nemzeti kötelezettségvállalás alapján készült minősített adat védelmének eljárási rendjéről szóló 179/2003. (XI. 5.) kormányrendelet.

A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény kitér a rejtjeltevékenység szakirányítására (hatósági engedélyezés, felügyelet és rejtjelkulcs előállítás), amivel az Információs Hivatalon belül működő Országos Rejtjelfelügyelet bízza meg.

2112/2004 (V. 7.) kormányhatározat a Terrorizmus Elleni Nemzeti Akciótervről, mely a titkosszolgálatok együttműködésének bővítését, minősített adatok továbbítására alkalmas adatátviteli kapcsolat kiépítését célozza meg.

Továbbá az eKormányzattal kapcsolatban új védelmi szükségletek merültek fel, melyek kiterjednek a hálózat, a minősített adatok, adatbázisok, a külföld és a belföld közötti kapcsolattartás biztonságára.

### Egyéb informatikával kapcsolatos törvények

A 2004. évi CXXXIV. törvény a kutatás-fejlesztésről és a technológiai innovációról rendelkezik. A törvényt Országgyűlés annak érdekében hozta, hogy elősegítse a magyar gazdaság versenyképességének és jövedelemtermelő képességének a tudásra, valamint a technológiai innovációra épülő és a fenntartható fejlődést szolgáló növekedését.

A 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatásokról rendelkezik. Az EU jogszabályokkal összhangban rendelkezik az elektronikus kereskedelem fejlődése érdekében. A törvény célja az elektronikus kereskedelem, valamint az információs társadalommal összefüggő szolgáltatások támogatásával a magyar gazdaság nemzetközi versenyképességének javítása.

Az információs technológia fejlődési üteme kikényszeríttette a vonatkozó jogszabályok megalkotását. Ez a jogalkotó munka csak késve tudja követni az e területen jelentkező kihívásokat. Míg az elektronikus aláírás szabályozása teljes, használata napi gyakorlat, addig az információvédelem más területeit csak általánosságban érintik egyes kormányhatározatok. Az elektronikus aláírással kapcsolatban új elem jelent meg a jogalkotásban, a technológiakövetés, mely valószínűleg más információvédelmet érintő területen is megjelenhet a jövőben.

Az információs társadalom kiépítésének felgyorsítása érdekében létrehozott Elektronikus Kormányzati Gerinchálózat és az Informatikai Közhálóval, valamint a kormányzati portállal kapcsolatos fejlesztések nagy ütemben folynak, a jelentős beruházásoknak köszönhetően. A beruházások súlyának megfelelően ezek a projektek jól szabályozottak, de itt is az információvédelem csak, mint egy elérendő cél bukkan fel.

Az információvédelem súlyának felértékelődését jelzi viszont, hogy az új nemzeti biztonsági stratégia külön felsorolja az informatikai rendszerekkel kapcsolatos kockázatokat, mint a nemzeti biztonságot veszélyeztető fontos tényezőket.

## FELHASZNÁLT IRODALOM


[1] http://www.hte.hu/kiadvanyok/hirlev2005/hirlevel_2005jan02.html, 2005. 06. 29.

[2] http://www.magyarorszag.hu/hirek/gazdasag/negyven20041109.html, 2005. 07. 9.

[3] http://www.kulugyminiszterium.hu/kum/hu/bal/Kulpolitikank/Biztonsagpolitika/Nemzeti_biztonsagi_strategia.htm, 2005. 07. 9.

[4] 1188/2002.(XI.7.) kormányhatározat rendelkezik az Elektronikus Kormányzati Gerinchálózatról (továbbiakban EKG) és az Informatikai Közhálóról

[5] 1214/2002. (XII. 28.) kormányhatározat rendelkezik a Magyar Információs Társadalom Stratégia (a továbbiakban: MITS) készítéséről, valamint a KözHáló részletes koncepciójáról

[6] 184/2004. (VI. 3.) Kormányrendelet az elektronikus közigazgatási ügyintézésről és a kapcsolódó szolgáltatásokról

[7] 45/2005. (III. 11.) kormányrendelet lépett, mely a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással kapcsolatos feladat- és hatásköréről, valamint eljárásának részletes szabályairól

[8] 44/2005. (III. 11.) kormányrendelet a kormányzati informatika koordinációjáról

[9] 1113/2003. (XI. 11.) kormányhatározat a közigazgatási szolgáltatások korszerűsítési programjáról

[10] 1126/2003. (XII. 12.) kormányhatározata a Magyar Információs Társadalom Stratégiáról

[11] 1214/2002. (XII. 28.) kormányhatározat a Magyar Információs Társadalom Stratégia készítéséről

[12] 1053/2004. (VI. 3.) kormányhatározat az elektronikus közigazgatási ügyintézés és kapcsolódó szolgáltatások megvalósításával összefüggő feladatokról

[13] 1066/2004. (VII. 6.) Kormányhatározat az IDA Programban történő részvételből és a TESTA hálózathoz való csatlakozásból eredő feladatok végrehajtás

[14] 2004. évi CXXXIV. Törvény a kutatás-fejlesztésről és a technológiai innovációról

[15] 40/2004. (XII. 21.) IM rendelet az elektronikus cégbejegyzési eljárás és cégnyilvántartás egyes kérdéseiről

[16] 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről

[17] 2073/2004. (III. 31.) kormányhatározat a Magyar Köztársaság nemzeti biztonsági stratégiájáról

[18] A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény

[19] Az 1995. évi LXV., valamint az ezt módosító 2003. évi LIII. törvény az államtitokról és a szolgálati titokról, Magyar Közlöny 2003/83. szám, 6552. oldal

[20] A nemzetközi szerződés alapján átvett, vagy nemzeti kötelezettségvállalás alapján készült minősített adat védelmének eljárási rendjéről szóló 179/2003. (XI. 5.) kormányrendelet, Magyar közlöny 2003/126. szám, 9454. oldal

[21] Az elektronikus aláírásról szóló 2001. évi XXXV. törvény

**Dr. KOVÁCS László**

# A TERRORIZMUS VESZÉLYE ÉS A MAGYAR KÖZTÁRSASÁG KOMMUNIKÁCIÓS INFRASTRUKTÚRÁJA

*Az írás a Magyar Tudományos Akadémia Bolyai János Kutatási Ösztöndíjának támogatásával készült.*
*This paper was supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences*

Zrínyi Miklós Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Kar
Informatikai tanszék
kovacs.laszlo@zmne.hu

## Bevezetés

A 21. század elején a társadalmi fejlődés egyik fő meghatározójává vált a távközlés, a számítástechnika és az elektronikus média, azaz az információs technológia széleskörű, egyre átfogóbb alkalmazása, mely áthatja a társadalom minden rétegét, ezek kapcsolatát, elősegítve a hatékony működéshez, a dinamikus fejlődéshez szükséges információk teljeskörű biztosítását, az információszolgáltatás korszerű eszközeinek alkalmazását, a döntés előkészítési és végrehajtási feladatok megvalósítását. Az információs technológia és az új kommunikációs technológiák konvergenciája eredményeként kialakuló, úgynevezett infokommunikációs technológia az alapja az információs hálózatokra épülő új társadalmi rendnek, az információs társadalomnak. Globális kommunikációs – vagy a ma oly divatos névvel illetett infokommunikációs – hálózatokat, illetve eszközöket használunk az ipar, a kereskedelem, az oktatás a kutatás-fejlesztés, és számtalan olyan területen, amely felsorolása is igen-igen hosszadalmas lenne. E rendszerek által nyújtott egy-egy szolgáltatást nagyon sokszor olyan természetesnek veszünk, hogy azt már szinte észre sem vesszük. Magától értetődő, hogy van villamos energiaszolgáltatás, a csapból folyik a víz, a korházakban gyógyítanak, működik a közlekedés, a szállítás, a kereskedelem, a tőzsde és folytathatnánk a sort. Gyakorlatilag ma már a fejlett nyugati társadalmak mindennapjaiban nincs olyan terület, ahol ne lenne meghatározó tényező a hálózat, illetve az ezekre épülő valamilyen szolgáltatás.

Mindezek azonban komoly veszélyforrást is jelentenek, hiszen – amennyiben elfogadjuk azt az állítást, miszerint ezek a rendszerek mindennapjaink részévé váltak – , akkor ezek teljes, vagy részleges hiánya, illetve működésképtelensége is igen komoly veszélyeket idézhet elő. Abban az esetben például, ha az információs infrastruktúráink közül a villamos energiaszolgáltatás hosszabb-rövidebb időre megszűnik, vagy csak akadozva működik, akkor kis képzelőerővel is komoly – akár katasztrofális következményekkel járó – események bekövetkezése jósolható meg.

Az említett – gyakran teljesen a mindennapjaink részévé vált – információs infrastruktúrák jelentős hányada egy, vagy több hálózat része, az esetek döntő többségében az irányítás, a felügyelet, vagy monitoring számítógépes hálózaton keresztül valósul meg.

A hálózatok fejlődéstörténetét tekintve látható, hogy kezdetben a technikai megvalósíthatóság kötötte le a fejlesztők figyelmét, így a hálózatok biztonsága nem játszott kulcsszerepet. Napjainkban azonban, amikor számtalan szolgáltatást veszünk igénybe a hálózatok segítségével, így óriási fontosságú a megbízható, stabil működésű – és nem utolsó sorban biztonságos adatátvitelt megvalósító – hálózat megteremtése. A banki szolgáltatásoktól kezdve a hálózaton folytatott kereskedelmen keresztül, egészen az egyéni felhasználó számítógépéig naponta támadják a hálózatokat, keresnek olyan biztonsági réseket, amelyeken keresztül az adatokhoz hozzáférve különböző mértékű károk okozhatók.

Ma már szinte valamennyi nagyobb hálózat kapcsolódik az Internethez, igénybe veszi annak szolgáltatásait, vagy valamilyen szolgáltatást biztosít az Internet felé. Az Internet felől azonban fel kell készülni az esetleges támadásokra, amik lehetnek betörési kísérletek, de a belső hálózat tönkretételére irányuló próbálkozások is. A védelem tehát alapvető fontosságú.

A hálózati biztonság megteremtése azonban nem lehet csak egyetlen személy feladata egy adott szervezeten, illetve annak számítógépes hálózatának tekintetében. A biztonság itt is olyan komplex módon valósítható csak meg, amely felöleli a szervezet tevékenységének valamennyi szegmensét. Mindezeken túl egy adott ország esetében meghatározó tényezők a biztonság vonatkozásában azok a kormányzati tevékenységek is – jogszabályi háttér megteremtése, szabályzók, irányelvek, auditálási szabályok megfogalmazása –, amelyek az adott ország számítógépes hálózatainak a biztonságosabbá tételére irányulnak.

Jelen írás célja nagyon röviden felsorolni azokat az információs infrastruktúrákat, amelyek – akár ideiglenes, akár hosszabb távú – leállása veszélyezteti a társadalom normális működését, illetve behatárolni azokat a pontokat, ahol ezek az infrastruktúrák támadhatók. Természetesen elengedhetetlen a vizsgálódás szempontjából annak körvonalazása, hogy vannak e, és ha igen milyen terrorista veszélyek, amelyek potenciálisan fenyegetést jelenthetnek ezekre az információs infrastruktúrára.

## 1. Információs infrastruktúrák – kritikus információs infrastruktúrák

Infrastruktúrán azoknak a rendszereknek, illetve ezek elemeinek az összességét értjük, amelyek biztosítják az adott szervezet rendeltetésszerű működését. A fontosság, feladat, rendeltetés és felépítés alapján számtalan infrastruktúrát különböztethetünk meg. Ezek közül azonban ki kell emelni azokat, amelyek részleges, időleges, vagy teljes leállása olyan következményekkel jár, amelyek más infrastruktúrák működésképtelenségét is magukkal vonzzák. Azokat az infrastruktúrákat, amelyek ezek alapján a legfontosabbak, a legsebezhetőbbek, folyamatos és rendeltetésszerű működésük elengedhetetlen a többi infrastruktúra működéséhez kritikus infrastruktúráknak nevezhetjük.

A teljesség igénye nélkül néhány e kritikus infrastruktúrák közül:[74]

- az energiatermelő, -tároló és -szállító infrastruktúrák: a szén- és olajtüzelésű, gázüzemű, vízi-, szél-, nap-, biogáz- és atomerőművek, földgáz és kőolajtermelő és -finomító vállalatok, szénbányák, villamos energia átalakítók, távvezetékek, kőolaj- és földgázszállító vezetékek, stb.;

[74] Forrás: Haig – Várhegyi: Információs műveletek, Egyetemi jegyzet, Budapest, 2004.

- a banki és pénzügyi infrastruktúrák: banki hálózatok, kereskedelmi központok, érték- és árutőzsdék, egyéb pénzügyi szervezetek;
- a vízellátó rendszerek: víztisztítók, víztározók, vízvezeték- és csatornahálózat, stb.;
- a távközlési és kommunikációs rendszerek: távközlési és kommunikációs eszközök, amelyek számítógép alapú hálózatokat, szoftvereket, stb., is magukba foglalnak;
- a szállító infrastruktúrák: nemzeti légitársaság, repülőterek, közúti személy- és teherszállító vállalatok, út- és autópálya hálózatok, vasúti társaságok, vasúthálózatok, vízi szállító eszközök stb.;
- a vészhelyzeti és katasztrófavédelmi infrastruktúrák: mentőszolgálatok, rendőrség, tűzoltóság, egészségügyi intézetek, katasztrófa elhárító szolgálatok, stb.;
- a kormányzati és önkormányzati szervek.

Napjainkban ezek az infrastruktúrák mindegyike jórészt számítógépes hálózatra, vagy ezek egyes elemeire épül. Ezek önmagukban is sérülékenyek, de mivel ezek a számítógépes hálózatok nagyon sok esetben természetszerűleg – pont az általuk elvégzendő feladatok miatt – nem zártak, nem a külvilágtól hermetikusan elzárt hálózatok, hanem számos helyen kapcsolódnak más hálózatokhoz. Mivel vannak külső kapcsolódási pontjaik – az esetek jelentős részében ezek számának a meghatározása, illetve a kapcsolódási pontok behatárolása is komoly nehézségekbe ütközik (komplexitás, feladatok sokrétűsége, fizikai kialakítás, területi lefedettség, stb. miatt) –, így az egyébként is sérülékeny hálózatok kívülről is támadhatóvá válnak.

### 1.1. Távközlési és kommunikációs hálózatok:

Amennyiben a Magyar Köztársaság esetében megvizsgáljuk a kritikus információs infrastruktúrák közé tartozó távközlési és kommunikációs hálózatokat, akkor ezeket az alábbi három nagy csoportra oszthatjuk:

- közcélú hálózatok;
- különcélú hálózatok;
- zártélú hálózatok.

A közcélú hálózatok ma már alapvetően piaci alapok nyugvó, liberalizált szolgáltatásokat és infrastruktúrákat jelentenek. E hálózatok fejlődési üteme követi a világ fejlődési tendenciáit. Ma már több vezetékes és mobil távközlési szolgáltató hálózata lefedi az ország egész területét. A szolgáltatók egyebek mellett vezetékes távközlési szolgáltatásokat, GSM, vagy most startoló UMTS szolgáltatásokat, ISDN elérhetőségeket, VoIP lehetőségeket, különböző optikai illetve hagyományos hálózatokon szélessávú adatátviteli szolgáltatásokat, rádió és televízió műsorszórást biztosítanak.

A különcélú hálózatok valamely szervezet, vagy vállalat funkcionális feladatait támogatni, illetve irányítani hivatottak. Ilyen különcélú hálózat többek között a MÁV Rt., a MOL Rt., vagy az MVM Rt. saját, vagy vállalkozásokban a részükre biztosított irányító, ellenőrző adat és távbeszélő hálózatai.

A zártcélú hálózatok körébe a védelmi, illetve a nemzetbiztonsági feladatokat ellátó szervezetek saját kommunikációs és adathálózatait sorolhatjuk. Ilyenek a BM, a Határőrség, az OKF, vagy a HM különböző hálózatai.

## 2. A terrorizmus réme a XXI. században és az információs terrorizmus

A XXI. század elején a legnagyobb veszélyforrásának a terrorizmust tartjuk. Ennek ellenére azonban nincs olyan egyértelmű meghatározás, amely pontosan leírná a terrorizmus fogalmát. A különböző definíciók aszerint határozzák meg a fogalmat, hogy az adott terrorista csoport vagy szervezet milyen célt kíván elérni, illetve, hogy e szervezetnek feltételezhetően kik a tagjai és milyen motivációval rendelkeznek. Ebből kiindulva – ha nem is hivatalosan – született meg az információs terrorizmus kifejezés. Ezzel a jelzővel azokat a szervezeteket illetve tevékenységeket illetik, akik, vagy amelyek kihasználják, illetve felhasználják azokat az információs infrastruktúrákat, amelyek közül néhány az előzőekben bemutatásra került. Természetesen itt azonban felmerül a kérdés, hogy ezeket az infrastruktúrákat a hagyományos terrorista szervezetek is felhasználhatják működésük során. A különbség mégis abból adódik, hogy az információs terrorizmus nemcsak, hogy felhasználja ezeket az infrastruktúrákat, hanem ezeken keresztül támad, illetve fennáll a veszélye, hogy ezekben a rendszerekben komoly károkat is okoznak a rajtuk keresztül megvalósított támadásokkal. Meg kell azonban jegyezni, hogy az információs terrorizmus is sok esetben használhat „hagyományos" terrorista eszközöket, hiszen egy hagyományos robbanóanyaggal végrehajtott fizikai támadás egyes információs infrastrukturális elemek vagy rendszerek ellen szintén komoly – időszakos, vagy végleges – működésképtelenséget, és így komoly károkat okozhat.

Az információs terrorizmus tehát célját tekintve felhasználja, és így közvetett módon a társadalom egészét, vagy egyes csoportjait, „terrorizálva" – félelemben, bizonytalanságban tartva – kihasználja az információs infrastruktúrákat.

Mielőtt az információs infrastruktúrákon keresztül végrehajtható esetleges támadások módjait elemeznénk fontos hangsúlyozni azt a tényt, hogy a fejlett nyugati társadalmak visszavonhatatlanul függővé váltak az információs infrastruktúráktól, illetve ezek szolgáltatásaitól. Ezek jelentik a fejlődőképes gazdaság, és nyugodtan kijelenthetjük, hogy a normális társadalmi működés alapjait. E rendszerek nélkül nem képzelhető el hatékony gazdaság, és kiegyensúlyozott társadalmi működés. A védelem tehát létérdekünk.

A továbbiakban e rendszereken keresztül bekövetkezhető támadások és azok lehetséges módjai kerülnek röviden bemutatásra.

### 2.1. Információs támadás:

Az információs támadás jelenthet egyaránt hagyományos – fizikai – támadást, például információs rendszerek ellen elkövetett hagyományos robbantással végrehajtott támadást, de ugyanakkor jelenthet az információs rendszereken – főként a hálózatokon – keresztül végrehajtott információs támadást is. Vizsgáljuk meg a hálózatok támadásának lehetőségeit.

A számítógép-hálózati támadás szoftveres, vagy hardveres úton való behatolást jelent a szembenálló fél számítógépes- rendszereibe, illetve hálózataiba, azzal a céllal, hogy tönkretegye, módosítsa, manipulálja vagy hozzáférhetetlenné tegye az adatbázisaiban tárolt adatokat, információkat, illetve magát a rendszert vagy hálózatot. A támadás a számítógép-hálózati elemekben való fizikai károkozást is jelentheti, amelyet a szoftverek módosításával vagy manipulációjával lehet elérni. A hatékony véde-

lem megvalósításához mindenekelőtt fel kell mérni azokat a pontokat, illetve módszereket, ahol, és amelyekkel ezek a rendszerek támadhatók vagy sebezhetők

## 2.2. Veszélyek, gyenge vagy támadható pontok:

A támadási formák ma már olyan sokrétűek, hogy a felsorolásuk gyakran reménytelen vállalkozásnak tűnik. Még a teljesség igénye nélkül is szélmalomharcnak tűnik felsorolni a DoS támadásoktól kezdve a backdoor attack-ig, vagy a flood-okig azokat a formákat, amelyekkel a hálózatok, illetve az azokban működő számítógépek támadhatók. Naponta értesülhetünk a különböző médiumok segítségével, hogy újabb és újabb támadási formák jelennek meg, amelyek hatásaikat – és az általuk okozott károkat – tekintve hol kisebb, hol nagyobb veszteséget, károkat okoznak.

Néhány általános következtetés azonban levonható e támadási formák tanulmányozásából. Ezek közül az egyik, hogy felmérjük, melyek azok a veszélyek, amelyek az információs infrastruktúrákat illetve a hálózatokat fenyegetik. Ezek a következők lehetnek:

- az információ és az erőforrások megsemmisítése;
- az információ meghamisítása vagy módosítása;
- az információ vagy az erőforrások eltulajdonítása, elmozdítása vagy elvesztése;
- az információ felfedése, nyilvánosságra hozása;
- a szolgáltatás megszakítása.

A veszélyeket tovább csoportosíthatjuk, kategorizálhatjuk. A kategóriák részben át is fedik egymást. Az első csoportba a humán eredetű, a második csoportba technikai jellegű veszélyforrások sorolhatók. Ilyen humán jellegű veszélyforrás, amely rögtön egy kis átfedést is mutat a technikai eredetű veszélyforrásokkal, az az információk szabad áramlása, illetve az információkhoz való hozzáférés relatíve könnyű módja. Nagyon sok technikai eszköz és rendszer (hardver és szoftver egyaránt) adata, műszaki leírása és paramétere mindenki számára viszonylag könnyen elérhető. Ez egyrészről természetes, hiszen például a szabványok, vagy a protokollok esetében pont a cél, hogy mindenki tudja azt az egységes álláspontot, amely lehetővé teszi a kompatibilitást és az együttműködést. Másrészről, pedig ez komoly veszélyeket is rejt magában, mert így ezek elemezhetőek, megkereshetőek a gyenge vagy támadható pontok, felületek.

A következő ilyen humán jellegű veszélyforrás az információk ellenőrizhetetlenségének ténye.75 Vannak ugyan kísérletek, például az Interneten folyó információáramlás bizonyos fokú ellenőrzésére, de ezek rendszerint csak célzottak lehetnek – hiszen a hatalmas napi adatforgalommal szemben gyakran csak kis ellenőrző erő, illetve apparátus áll – ugyanakkor ennek az ellenőrzésnek a törvényi és jogszabályi háttere is gyakran hiányzik. Az ellenőrzés egyik példája az FBI törekvése a Skype ingyenes Internetes telefon (VoIP) szolgáltatás lehallgatására.76 Egy másik ilyen törekvés Nagy-Brittaniában a terrorista gyanús weboldalak blokkolása, illetve szűrése.77

Összességében humán oldali veszélyforrásokról elmondható, hogy a legfontosabb megválaszolandó kérdés az a probléma, hogy mi a fontosabb az alapvető embe-

[75] Ez alapvetően nem technikai kérdés, mert a technikai feltételek elvben megteremthetőek lennének.

[76] http://index.hu/tech/biztonsag/skyp9489/

[77] Terrorizálják a terroristák weboldalait, http://it.news.hu

ri jogok – szabad véleménynyilvánítás, információhoz való szabad hozzáférés, stb. biztosítása –, vagy a biztonság, amely megteremtése sok esetben az előzőek bizonyos mértékű csorbításával jár együtt.

A technikai jellegű veszélyforrások száma ma már naponta ugyanúgy nő, mint ahogy növekszik az új technika és technológia eredményeit felhasználó és alkalmazó rendszerek száma. Gyakorta elhangzó vélemény, hogy a védelem még nagyon sok ideig csak a támadások mögött lemaradva tudja követni a fejlődést és az eseményeket. E technikai fejlődés nyújtotta veszélyforrások közül emeljünk ki kettőt:

- Mobil hálózat elérés:

WIFI és W-MAX: Óriási ütemben növekszik a népszerűsége és az elterjedése a vezeték nélküli hálózati elérésnek. Mivel ezekben az esetekben az elektromágneses jelek átviteli közege a levegő, ezért nehéz jól körülhatárolható korlátokat szabni a hotspot-ok elérésének, azaz a konkrét fizikai kapcsolódás nélkül (mint ahogy az a vezetékes elérés esetén nyilvánvaló) elég egy hordozható számítógépet bizonyos távolságra elhelyezni a hotspot-tól, és máris kivitelezhető a támadás. Felmérések és gyakorlati tesztelések78 bizonyították, hogy átlagosan a wifi felhasználók 35-40%-a bármilyen támadás előtt nyitott rendszert használ. Ez nagyon sok esetben abból adódik, hogy a felhasználók gyakorlatilag újrakonfigurálás nélkül, azaz alapbeállításokkal üzemeltetik és használják a hálózatot. Ez több támadási felületet is adhat. Az első ilyen támadási felület az adatlopás. Mivel könnyen, például az utcáról, egyszerű technikai eszközökkel „látható az adatforgalom", az könnyen rögzíthető. Amennyiben a kényelem együtt jár még olyan könnyelműséggel, mint az a tény, hogy nagyon gyakori hiba a felhasználók részéről, hogy nem, vagy csak nagyon ritkán változtatják a különböző jelszavaikat, így a jelszavakhoz való hozzáférés is meglehetősen leegyszerűsödik. A másik igen nagy veszélyeket magába foglaló támadási felület a rosszindulatú szoftverek bevitele az ily módon nyitott hálózatokon keresztül, de ide sorolhatjuk a feltört gépről más hálózatokba irányuló támadásokat is.

- Kéziszámítógépek biztonsága:

Szintén robbanásszerűen terjednek a kéziszámítógépek. Ezek azonban a kényelem mellett szintén jelentős veszélyforrásokat hordozhatnak magukban. Ezeket a gépeket sokkal könnyebb elveszíteni, vagy akár ellopni, mint a nagyobb gépeket, amellyel megnő az adatlopás – illetéktelen adathozzáférés – veszélye. A kéziszámítógépek általában vezeték nélküli adatkapcsolatot tesznek lehetővé, amely – ahogy az előzőekben láttuk – szintén jelentős veszélyforrás. A kéziszámítógépek sem védettek a vírusokkal szemben, így egy vírustámadás után könnyen az egész hálózatba bejuthat egy-egy rosszindulatú program.79

A technikai veszélyforrásokat elemezve meg kell vizsgálnunk, hogy a támadók hogyan férhetnek hozzá a hálózathoz, illetve az azon lévő adatokhoz. Erre három megoldás kínálkozik:

- valamilyen, a szervezet felügyelete alatt nem álló, tehát publikus, vagy harmadik fél kezelésében álló hálózatról;

[78] Szentesi Kálmán: Védtelen wifi hálózatok, http://prohardver.hu/

[79] Krasznay Csaba: A kéziszámítógépek biztonsága, Hactivity 2004, http://hacktivity.hu/folia/eloadas_5.ppt

- a szervezet saját kezelésében álló hálózatról, rendszerint arra legálisan csatlakoztatott számítógépen keresztül. Ennek egy speciális esete, amikor egy az 1. módszer szerint elért gépen keresztül támadják meg a szervezet további rendszereit;
- az adatokhoz (érzékeny információt tároló számítógépekhez, adattároló médiumokhoz, nyomtatásokhoz) közvetlenül hozzáférve.

(A harmadik eset javarészt a fizikai biztonság ill. a klasszikus adatvédelem területe).

Amennyiben a támadásról beszélünk azt is meg kell vizsgálnunk, hogy ki az, aki a támadást végrehajtja. A hacker olyan személy, aki pl. az Internet segítségével hozzá tud férni védett adatokhoz más számítógépeken. Komoly hacker egy egész rendszert az irányítása alá vonhat. A hacker általában nem akarja rosszindulatúan megváltoztatni a programokat. A hacker-eket olykor szándékosan kérik fel arra, hogy próbáljanak meg betörni valamilyen védett rendszerbe, evvel feltárva annak hiányosságait. A cracker (programfeltörő, szoftverkalóz) olyan személy, aki megpróbál illegálisan a védőkódok megkerülésével bejutni más számítógéprendszerekbe (pl: bankok) manipuláció vagy kártevés céljából. Ellentétben a hacker-ekkel, ezek mindig rosszindulatú betörők. Általában különböző operációs rendszerekre és platformokra specializálódnak. Addig próbálgatnak, kísérleteznek, amíg valamire nem találnak. Először interaktív kapcsolatot (login) akarnak megszerezni. Ezt lehet továbbfejleszteni root, vagy superuser jogkörré, aki egy gép legfőbb adminisztrátora. A phreak-ek csoportjai telefonvonalat lopva jutnak anyagi előnyökhöz. A phreak-ek a telefonközpontok vezérlő számítógépeinek, a távközlési vonalak ingyenes igénybevételének és általában a telekommunikációnak a szakértői. Rendelkeznek azzal a tudással, ami a központok átprogramozásához szükséges. Emellett a mobil telefonhálózat forgalmának, belső adatainak lehallgatásához is van megfelelő eszközük. A megszerzett információ segítségével õk maguk, vagy akiknek ezt lehetővé teszik, képesek mások költségére telefonálni. A jerk (enyhe fordításban: semmirekellő), vagy másképpen számítógépes vandál. Ugyanúgy viselkedik, mint a jól ismert utcai vandál, vagyis saját szórakozására, értelmetlenül tör és zúz. A weboldalak átírásától egészen a törlésig akármire képes.

Természetesen az előbb felsorolt csoportok tagjaiból nem lesz azonnal és egyenesen információs terrorista. Azonban a „szakmai" tudásuk a hálózatok támadásához rendelkezésre áll, rendelkeznek bizonyos mértékű gyakorlattal, így valamely ideológiai, vagy csak egyszerűen gazdasági (anyagi) megfontolások, vagy előnyök potenciálisan rávehetik őket, hogy eszközként felhasználják tudásukat és tapasztalatukat egy-egy támadásnál.

Visszatérve a támadásokhoz, megvizsgálva azokat megállapítható, hogy ezek az alábbiak lehetnek:

- illetéktélen hozzáférés az információkhoz (adatlopás):

Az adatbázisokban rendszerezett információk nagyon sok esetben mind anyagi mind erkölcsi értelemben sokat érnek. Annak érdekében, hogy ezeket az adatbázisokat, információkat a felhasználók el tudják érni, valamilyen szintig hálózaton keresztül is elérhetővé kell tenni. Ebben az esetben azonban megnyílik az út az illetéktelen felhasználók számára. Az illetéktelen felhasználók (adatlopók) a hálózaton található biztonsági rendszerek hiányosságait, vagy a legális belépéshez szükséges kritikus információk jogosulatlan megszerzésével megnyílt lehetőségeket használják ki annak érdekében, hogy az adott helyen meglévő információt megszerezzék. Ezek lehetnek

jelentéktelenek, de lehetnek akár hosszú és költséges kutatások eredményei, vagy akár nemzetbiztonsági szempontból kritikus katonai, vagy polgári adatok is. Nemzetbiztonsági szempontból különösen veszélyes az illetéktelen adathozzáférés, mivel a hírszerzés számára nincsenek jelentéktelen, vagy értéktelen adatok. A hálózatok lehallgatása rendkívül jelentős veszély, mivel ezúton tömegével lehet a hálózati belépéshez szükséges jelszavakat illetéktelenül megszerezni. A hálózatokon, kapcsolt vonalakon haladó adatforgalom többé-kevésbé könnyen lehallgatható. Különösen a helyi hálózatok adatforgalma hallgatható le könnyen, az itt szokásos üzenetszórásos technika jóvoltából (egy hálózati szegmens minden egyes munkaállomásához a többi munkaállomás minden üzenete eljut). A hálózatok lehallgatásra alkalmasak a szabadon elérhető olyan szoftverek, melyeket a hálózati menedzserek hálózatmonitorozásra, a forgalom analizálására fejlesztettek ki. A hálózat topológiája erősen befolyásolja a lehallgatás lehetőségeit, azonban ez idáig a lehallgatás elleni védelem nemigen volt szempont a hálózattervezéskor. Számos adatátviteli mód nehezen hallgatható le (ISDN, GSM, optikai átvitel, vagy a szinte felderíthetetlen és lehallgathatatlan szórt spektrumú jelátvitel), de a tökéletes megoldást csak a teljes adatforgalom titkosítása jelentheti. Az információkhoz való illetéktélen hozzáférés egy különleges módja a Van Eck-féle sugárzás kihasználása. A Van Eck-féle sugárzás azt jelenti, hogy minden fajta elektromágneses rendszer, pl. a számítógép képernyője, kábelei, hardver elemei bizonyos mennyiségű és intenzitású elektromágneses sugárzást bocsátanak ki. Ezek érzékeny vevőkkel detektálhatók és értékelhetők.

- illetéktelen adatbevitel:

Az adatbázisok megbízhatósága gyakran csak utólag mérhető – illetve a használat során a felhasználó megbízik az adatok valóságtartalmában és ezeknek az adatoknak a felhasználása során, feltételezi azok helytállóságát. Azonban, ha illetéktelen adatbevitel történt – legyen szó szándékos, vagy nem szándékos adatbevitelről – és ezek az adatok a valóságostól eltérőek, információ tartalmuk más, mint a tényleges, és a felhasználók ezt megbízható, hiteles információnak tartják – hiszen a korábban felhasznált információk megbízhatóak voltak – óriási anyagi károk keletkezhetnek. Az anyagi károkon kívül az adott információs rendszer, vagy annak egy eleme - például a hamis információkat szolgáltató adatbázis – irányában egy olyan nagyfokú bizalmatlanság alakul ki, amely túl az anyagi károkon további károkat okozhat.

- rosszindulatú szoftverek bevitele:

Minden olyan szoftver rosszindulatúnak tekinthető, amely nem az információs rendszer működésének a biztosítására, vagy azzal közvetlenül kapcsolatban kerül az információs rendszerbe, és amelyek valamilyen módon az adott információs vagyon ellen irányulnak. A rosszindulatú programokat összefoglaló néven az angolból átvett malware szóval írjuk le. Általában ezeket a szoftvereket az információs rendszer működésének akadályozására juttatják be a rendszerbe, de különösen veszélyesek a meglévő adatvagyon rombolására, pusztítására irányuló szoftverek. Ezek a szoftverek szisztematikusan rombolják, módosítják, használhatatlanná teszik az adott információs vagyont.

A mindennapi gyakorlatban az alábbi, egymástól sokszor nehezen megkülönböztethető malware-kategóriákat határozhatunk meg[80]:

[80] Dr. Nagy Gábor: Phishing, pharming - mi jöhet még?, http://it.news.hu - alapján

*Program típusú malware:*

- számítógépvírusok és programférgek:
- vírusfejlesztő kitek;
- trójai és backdoor programok;
- dialerek;
- dropperek;
- kémprogramok;
- keyloggerek;
- egyéb kártékony programok.

*Szöveg típusú malware:*

- spam;
- hoax;
- holland és spanyol lottónyeremény levelek;
- nigériai csalások;
- phishing, pharming;
- egyéb, szöveges típusú kártékony tartalmak.

- információs környezetszennyezés:

Az adatvagyon területén megnyilvánuló környezetszennyezés elsősorban nem fizikai környezetszennyezés. Ez elsősorban olyan adatoknak és információknak az információs rendszerekbe való bejuttatását jelenti, amelyek egyrészt nagyságrendjüknél fogva (pl.: tömeges nemkívánatos reklám, ismertető, „spam") fizikailag bénítják a hálózatot, ezáltal elérhetetlenné téve a fontos, valódi információkat. Másrészről ideológiai, politikai, vallási, vagy egyéb tartalmuknál fogva károsan befolyásolhatják az információs társadalom tagjait, hiszen ezen a módon sokkal hatékonyabban és szélesebb körben eljuttathatók az információk, mint bármikor azelőtt.

Összefoglalva: láthatjuk, hogy az információs rendszereknek mind a technikai mind a humán oldalát tekintve számtalan olyan felülete és pontja van, amelyek komoly veszélyforrásként jelentkezhetnek e rendszerek működésére, közvetett módon, pedig az egész társadalom egészére nézve.

## 2.3. A védelem

Ha a támadások elhárításának megtervezésével és megszervezésével foglalkozunk, előre meg kell becsülni a támadás valószínűségét. Egy rendszer sokféleképpen sebezhető, de ezeknek anyagi vonzatát is mérlegelni kell. Ha egy támadás nehezen kivitelezhető, akkor a kockázati tényező lényegesen kisebb. Természetesen a biztonságnak ára van. A biztonság nagyobb költséget, gyengébb hálózati teljesítményt és bonyolultabb elektronikus adatcserét jelent.

Az adott szervezetnek a rendelkezésre álló pénzügyi keretek, a szükséges hálózati teljesítmény és az elektronikus adatcsere követelmények ismeretében kell döntenie a megvalósítandó biztonságról.

Az informatikai biztonság nem csak műszaki kérdés – mint, ahogy azt a veszélyforrások bemutatásánál láttuk –, hanem humán probléma is. Egy az Egyesült Államokban készült felmérés szerint az összes számítógépes bűnesetek 81%-át a szervezet saját alkalmazottja által elkövetett illegális adatmanipuláció teszi ki. A külső támadás sokkal kevésbé valószínű, a statisztika szerint ez 17%.

A biztonság megteremtése nem elsősorban technikai kérdés, sokkal inkább rendszerszintű fogalom. Ezt a rendszert módszeresen, az alapoktól kezdve kell felépíteni. Ennek folyamatát megvizsgálva a következő lépések megtétele elengedhetetlen:

*Kockázatelemzés (Risk analysis)*

Külső konzulens (rendszerintegrátor vagy auditáló) cég szakemberei a szervezet informatikai szakembereivel együttműködve felmérik, hogy a szervezet számítógépes rendszerét mely területeken fenyegeti veszély, hogyan lehet az értékkel és a kockázattal arányos költségű védelmet kialakítani.

*Biztonsági politika kialakítása (Security & Access Policy)*

Irányelvek, eljárási szabályok kialakítása, etikai elvárások, hozzáférési, jogosultsági, naplózási rendszerekkel szembeni követelmények meghatározása, ellenőrzési rendszer kidolgozása, felelősségi körök rögzítése, stb.

*Fizikai védelem*

A gépekhez és információhordozókhoz való fizikai hozzáférés csak az arra jogosult személyek részére biztosított.

*A felhasználó személyazonosságának és hitelességének megállapítása (Authentication)*

Csak az arra felhatalmazott személyek, és csak alapos azonosítás után léphetnek be a rendszerbe.

*Jogokkal történő felruházás (Authorization)*

A felhasználók számára a tevékenységükhöz minimálisan szükséges felhatalmazások biztosítása.

*Rejtjelzés (Encipherment)*

A belső és külső lehallgatás elleni védelmet a kritikus állományok, adatbázisok kódolt tárolása, bizonyos tranzakciók, illetve forgalom titkosítása és az Interneten összekapcsolt helyi hálózatok közötti forgalom titkosítása (VPN – Virtual Private Network) biztosítja.

*Ellenőrzés, vizsgálat (Accounting/Auditing)*

Az események folyamatos figyelése, a felhasználók tevékenységének naplózása, a napló fájlok elemzése.

*Rendszeres felülvizsgálatok, módosítások*

A biztonsági rendszer félévenkénti átvilágítása javasolt, a gyenge pontok, konfigurációs hibák feltárása a legfrissebb betörési technikák ismeretében. A vizsgálati módszerek leírását, a talált hiányosságokat és kiküszöbölésük módját közzé kell tenni a szervezetben, és ezt a továbbiakban a hiányosságok megszüntetésénél alapul kell venni.

A biztonság megteremtése során a cél: a dinamikus biztonság megteremtése. Mivel állandóan változó környezetről beszélhetünk nincsenek örök időkre szóló megoldások, a rendszert folyamatosan tökéletesíteni kell, hiszen a támadók is egyre újabb, fejlettebb módszerekkel és eszközökkel rendelkeznek.

*A védelem lehetséges megvalósítása az alábbi területeken kell, hogy megtörténjen:*

- fizikai biztonság megvalósítása:

Fizikai őrzés: zárt helyet jelent, a fizikai beléptetés során a jogosultság ellenőrzését, megfelelő tűzvédelmet, szükség esetén légkondicionálást feltételez. Elektroni-

kus őrzés: folyamatos tápellátást, időszakos vagy folyamatos háttérmentést, illetve a hozzáféréshez biztonságos fizikai közeg biztosítását foglalja magába;

- határterületi biztonság:

A határterület az a terület, ahol a hálózatok összekapcsolódnak. Sok esetbe ez a helyi hálózat kapcsolódási pontjait jelenti az Internethez. A külső, vagy más hálózatokból érkező támadások ellen védeni kell a saját hálózatunkat. Erre szolgáló módszerek és alkalmazások: tűzfalak, hálózati forgalomelemzők, behatolás érzékelők, támadásszimulálók, de ide tartozik például az authentikáció, vagy a kriptográfia is.

- belterületi biztonság és a munkaállomások védelme:

A munkaállomások védelme az egyik leggyakrabban hangoztatott védelmi megoldás, hiszen az előzőekből is látható volt, a munkaállomások jelentik a legkönnyebben támadható célokat. A megfelelő vírusvédelem – folyamatos, ma már naponta frissülő vírusadatbázis – mellett ugyanilyen fontos az authentikáció vizsgálata.

### 2.4. Hadseregek

Amennyiben információs terrorizmusról beszélünk, meg kell említenünk a hadseregek helyzetét, illetve az azok által használt információs infrastruktúrákat is. A terjedelmi korlátok miatt jelen írás csak vázlatosan veti fel az ezzel kapcsolatos kérdéseket.

- A hadseregek a vezetésben is és a végrehajtásban is egyre inkább előtérbe kerülnek, és egyre inkább nélkülözhetetlenné válnak azok az információs rendszerek, amelyeket a polgári életben, vagy akár mindennapjainkban használunk. Itt természetesen speciális célra – az esetek többségében integráltan – használnak adatszerző, feldolgozó, továbbító (C4ISR – Command, Control, Communication, Computer, Intelligence, Surveillance, Reconnaissance) valamint döntés-előkészítő – számítógépre alapozott rendszereket.
- Az elmúlt 4-5 év hadviselésben bekövetkezett változásai – a XXI. század kihívásainak való megfelelés: gyorsaság, hatékonyság, mobilitás, a minél pontosabb és megbízhatóbb információk minél rövidebb időn belül való megszerzése és elemzése –, azt követelték, hogy egy hálózathoz tartozzanak mindazok, akik ebben a folyamatban részt vesznek, azaz a parancsnoktól kezdődően a végrehajtókig mindenki egy hálózat része legyen. Ezt hálózat központú hadviselésnek hívják, amely lényege éppen a hálózat nyújtotta előnyök minél hatékonyabb kihasználásában, és végső soron, ezen előnyökön keresztül, ezek mintegy hadműveleti előnnyé alakításában rejlik. De rögtön adódik a kérdés, vajon az ilyen hálózatok megfelelően védettek-e a külső beavatkozásoktól? Lehetnek-e ezek a hálózatok terrorista célpontok?
- Sok a hasonlóság és az analógia a civil információs infrastruktúrákkal, amely felveti azt a kérdést, hogy függővé válnak-e a modern hadseregek is ─ a társadalom többi részéhez hasonlóan ─ az információs rendszerektől?
- A mobil hálózatok ─ hálózati eszközök, mobil hálózati elérés, mobil adatbázisok ─ védelme kielégítően megteremthető-e a harctéren?

### Összefoglalás, következtetések:

Napjainkban egyre több – szociológiai, gazdasági, politikai – háttérelemzés születik arról, hogy nemcsak óriási előnyei vannak a forradalmian új technika és technológia alkalmazásának, hanem ezek olyan árnyoldalakat is magukban rejtenek, ame-

lyek potenciális veszélyforrásként jelentkezhetnek, és amelyek kezelésére minden – az információs társadalom kialakítását, vagy fejlesztését célul maga elé tűző – országnak fel kell készülnie.

A jelen írásban bemutatott megoldásokkal és alkalmazásokkal támadhatók a felsorolt információs infrastruktúrák.

Mivel a Magyar Köztársaság kommunikációs infrastruktúrája hasonló módon épül fel, ezért kijelenthető hogy hazánk kommunikációs infrastruktúrája hasonló eszközökkel és módszerekkel támadható. Az, hogy egy-egy különálló vagy komplex támadásnak milyen következményei lehetnek természetesen további elemzéseket kívánnának. Jelen írás a Magyar Köztársaság távközlési és kommunikációs infrastruktúráját éppen, hogy csak felvillantotta, de ebből is világosan látható, hogy ezek a hálózatok, rendszerek és szolgáltatások az egész ország gazdaságát és működését alapvetően befolyásolják. Így a leírtakból az is kiderül, hogy e rendszerek információs támadásával komoly anyagi károk, és igen komoly humán katasztrófák következnének be hazánkban is.

A védelem megteremtése és folyamatos dinamikus fenntartása olyan elsődleges érdek, amely kormányzati, és széles gazdasági, valamint társadalmi összefogást követel. Ebben szerepet kell, hogy kapjanak a kormányzati szervek, a nemzetbiztonságért felelős szervezetek és a civil szervezetek egyaránt.

## Felhasznált irodalom


[1] Haig – Várhegyi: Információs műveletek, Egyetemi jegyzet, Budapest, 2004.
[2] Terrorizálják a terroristák weboldalait, http://it.news.hu
[3] Szentesi Kálmán: Védtelen wifi hálózatok, http://prohardver.hu/
[4] Krasznay Csaba: A kéziszámítógépek biztonsága, Hactivity 2004, http://hacktivity.hu/folia/eloadas_5.ppt
[5] Dr. Nagy Gábor: Phishing, pharming - mi jöhet még?, http://it.news.hu

**Magyarné KUCSERA Erika**

# A TELJES INTEGRÁCIÓ FONTOSSÁGA A MH ZÁRTCÉLÚ INFOKOMMUNIKÁCIÓS HÁLÓZATAINAK MENEDZSMENTJÉBEN

## Bevezetés

A MH zártcélú távközlési és informatikai célú hálózat központosított menedzsmentjének alapjai már lehelyezésre kerültek, a hálózatmenedzsment alapvetően magas szinten működik. A haderőátalakítás keretében a humánerőforrás lehetőségek egy kezdeti egységes szervezet kialakításához megteremtődtek. Kiemelten fontos feladat azonban ezen alapokra építkezve a felügyeleti szerv egy olyan szolgáltatás-, megbízhatóság- és biztonságorientált integrált menedzsmentté történő továbbfejlesztése, mely már a távközlési és informatikai hálózati elvek időszerű megközelítésének figyelembevételével annak új irányvonalában fejlődik. A hatékony üzemeltetés és fenntartás egyik kiemelt szegmense a menedzsment, mely optimális működéssel magas színvonalú szolgáltatásokat képes nyújtani mind a felhasználói, mind az üzemeltetői állomány irányába.

Nem lehet eléggé kihangsúlyozni annak fontosságát, hogy a napjainkban mind inkább összekapcsolódó hang- és adatszolgáltatások eszközparkját és szolgáltatásait rendszerszinten szükséges kezelni. A különböző hálózati típusok és különböző célú adatátviteli szolgáltatások elkülönített üzemeltetése és menedzsmentje bizonyítottan nem célra vezető. Ezen kölcsönös integráció nem egyenértékű a szakterületenkénti teljesen független üzemeltetéssel, mely információcserét hajt végre a nap adott szakaszaiban. Az integrált menedzsmentnek a helyzetek pillanatnyi változására azonnal reagálnia szükséges, mely csak egységes, egymásba kapcsolódó integrált adatbázisrendszeren alapuló összehangolt, szigorúan szabályozott tevékenységek útján valósulhat meg.

A sikeres üzemeltetés és menedzsment már említett egyik feltétele a szolgáltatási és funkcionális területek teljes, időben azonnali, közös adatbázisalapú megvalósulása. A beszéd és adatcélú forgalmazás funkcionális szétválasztása -mint felügyelet alá csoportosítandó részelem- átgondolást igényel, hiszen a MH zártcélú hálózatában a hordozófelületek felügyeletének és üzemeltetésének nagy múltja van és a mindennemű szolgáltatások ezen hordozóhálózatra épülnek. Ezt figyelembe véve érdemes egy alapjaiban új felügyeleti funkcionális szisztéma kidolgozásának lehetőségét számba venni.

## Integráció hiányának problémái

A Magyar Honvédség adat- és beszédforgalmi célú távközlő hálózata igen sokrétű mind a szolgáltatásai, alkalmazásai mind az alapjait alkotó hordozófelületek tekintetében. A hálózat részenkénti (elemcsopotonkénti) kezelése nem adhatja meg a teljes hálózat forgalmi és biztonsági optimalitását, mivel így az egyes részterületek esetleges rejtett hibáiról- amennyiben ezek az éppen vizsgált összetevőknél nem okoznak problémát- nem értesülnek időben az ezzel közvetett kapcsolatban lévő részterületek szakállományai. Ezen jelenséggel a hálózat egészében olyan üzemeltetési és biztonsági rések keletkezhetnek, melyek teret engedhetnek a hálózati szintű, vagy speciális problémák generálódására.

## Feladat újraszervezés elvei

Az egyik kiemelten fontos terület a hálózat és menedzsmentbiztonság megszilárdítása a MH zártcélú hálózatában. A jelenleg megalakuló szervezeti elem a hálózati eszközök és szolgáltatások fenntartói állományának széttagoltsága miatt komoly nehézségekkel találják szemben magukat, hiszen a teljes egységben történő kezeléshez szükséges háttérbiztosítást nyújtó szervezeti elemek egyes részei az átszervezés következtében éppen most alakulnak újjá.

Tudomásul kell vennünk, hogy a MH zártcélú hálózatán belül támadások érik az adatátviteli szolgáltatásokat igénybevevő kommunikációs eszközöket, az aktív elemeket, valamint a menedzsmentben részt vevő eszközöket, továbbá ezeken keresztül ezek használóit. A Magyar Honvédség érdeke, hogy ezen támadásokat, illetéktelen hozzáféréseket visszaszorítsuk, kontrolálni tudjuk. Ehhez mind a menedzsment szakállomány (mely már rendelkezésre áll) képzése, mind a szakmai elöljárói rend és rendszer aktualizálása szükséges.

Mivel ezen terület nem kapott mindig a kor kihívásainak megfelelő figyelmet, ezért az itt dolgozók szakmai irányító szerveinek, valamint a menedzsmentterületnek jelenleg igen nagy lemaradást kell kompenzálnia, mivel egy megbízható, biztonságos zártcélú hálózat üzemeltetése elképzelhetetlen napjainkban védelem nélkül az egyre nagyobb számú és jelentősebb információszerzést, dezinformálást célzó támadásokkal szemben.

A védeni kívánt hálózatok, adatok biztonsága nem garantálható folyamatos felügyelet, ellenőrzés, tesztelés nélkül. Már nem elegendő az, hogy megvásárolunk egy védelmet szolgáló hardver és szoftver rendszert, hiszen az informatika és technológia fejlődésével lehet, hogy ez a jövő hónapban már elavulttá válik és nem lesz képes a támadások kivédésére. Mivel a Magyar Honvédség gazdálkodási kerete szűkös, ezért javaslom, hogy a már meglévő alap biztonságot nyújtó technológiára alapozva egy jó szintű biztonsági rendszer kombinációt alakítsunk ki melyet lépcsőzetesen a kor színvonalának megfelelő kihívások szerint tökéletesítsük. Ezen részekből álló rendszer folyamatosan, kisebb ütemekben, kisebb anyagi ráfordítással fejleszthető és saját szakállománnyal kontrolálható, tesztelhető.

A biztonsági oldal szorosan együtt kell, hogy működjön az adatátviteli célú szolgáltatási hálózatok felügyeletével, valamint a hordozófelületek menedzsmentjével. Az adatátviteli hálózatok menedzsmentje nem elkülöníthető a többi menedzsmentterülettől, mivel az egyes szolgáltatási területek célját szolgáló beállítások esetlegesen hátrányosak lehetnek a zártcélú hálózat egészét vizsgálva egy másik részterületen. Ezen hálózatoptimalizálási problémák kiszűrése csak centralizált menedzsment megvalósításával lehetséges, melyben közös koordináció alatt zajlik a hordozófelületek, valamint az ezeken futó alkalmazások, szolgáltatások felügyelete, a zártcélú hálózat biztonságát szavatoló menedzsmenttevékenység. A felsoroltak által megfelelő szakmai irányítás alatt megvalósítható egy védett, magas szolgáltatási színvonalú, a forgalmi szituációk változásához alkalmazkodó költséghatékony hálózat.

## Menedzsmentbiztonság

A menedzsmentbiztonság kiemelten fontos, hiszen szinte minden szolgáltatás, valamint az alapjait biztosító eszközrendszer ezen keresztül, elérhető, módosítható, vagy csak egyszerűen ezeket felhasználva információ nyerhető ki a szolgáltatás fel-

használójáról, vagy az általa bonyolított hang- illetve adatforgalmazásról. Ezért is kiemel feladat a menedzsment védelmének szilárdítása az alábbi területeken:

- Védeni szükséges egy felöl a hálózatot az ellen, hogy a menedzsment tevékenység rejtése alatt esetleg illetéktelen hozzáféréssel szabadon átjussanak a hálózat biztonsági akadályain;
- Védeni szükséges a menedzsment által használt hozzáférési pontokat és lehetőségeket;
- Védeni szükséges a menedzsment központi szerverét;
- A gyűjtőszerver duplikálása, élő adatbázissal ellátása szükségszerű;
- Védeni szükséges a jelszóállományt illetéktelen kézre kerüléstől;
- Szükséges a log-file védelme az illetéktelen behatoló nyomainak eltüntetését megakadályozása céljából;
- Szükséges a menedzsmenttevékenység szigorú írásos szabályzása;
- Rendszeres feladatként meg kell jelennie az alábbi tevékenységeknek:
- A felhasználónevek, jelszavak rendszer ellenőrzése;
- A rég nem használt jelszavak ellenőrzése;
- Váratlan időpontú, területű belépések ellenőrzése (hétvége, munkaidőn kívül);
- Biztonságossági vizsgálatok végzése, betörési tesztek végzése szigorúan ellenőrzött keretek között;
- Bejárások alkalmával az eszközök, átviteltechnika biztonsági szempontok szerinti vizsgálata;
- Esetleges illetéktelen felhasználás nyomon követése, jelentése;
- A log-file folyamatos elemzése biztonsági szempontok szerint.

Ezen feladatok töredék részét a már rendelkezésre álló jogosultságok és adatok birtokában a hálózatfelügyeleti szerv végzi, azonban a szervezeti váltásokat követően javasolt megfelelő szakmai irányítottság alatt működő szolgáltatási –, eszközpark összekapcsolódási lehetőségeket és ezek problémáit figyelembe vevő menedzsmentfunkció létrehozása, melyhez elengedhetetlenül szükséges a szakmai elöljáró egységes feladatszabása és együttműködése.

### Saját menedzsment fontossága

Általánosságban elmondható, hogy a technika fejlődésének következtében az elkülönített hang- és adatkapcsolattal rendelkező telekommunikációs hálózatok költséges megoldásnak tekinthetők.

A Magyar Honvédség zártcélú hálózatában biztosított hang és adatszolgáltatásokon keresztül azonban olyan védett, vagy bizalmas információk kerülnek továbbításra, melyek illetéktelen kézbe jutva veszélyeztethetik a Magyar Honvédség és ez által az ország érdekeit. Hasonló okokból nem kerülhet az Egységes Kormányzati Gerinchálózat kötelező érvényű szabályzása alá a Magyar Honvédség zártcélú hálózata, bár az IP használata költséghatékonysága miatt saját hálózatunkban saját felügyelettel mind indokoltabbá válhat. Érdemes megfontolni, hogy mind a már titkos vagy bizalmas információhalmaz, mind a hálózatokból kinyerhető elsődlegesen nyílt, de adatbányászat útján teljes pl. állománytáblát feltérképezést adó adatbázis kikerülése veszélyes lehet. Ezeket figyelembe véve az elsődlegesen a biztonságos üzemeltetés és menedzsment belső, MH alárendelt állománnyal történő megvalósítása javasolt. A menedzsmentfeladatok tervezésénél nem csak a békeidejű tevékenységre szükséges tervezni, hanem az esetleges nem béke idejű tevékenységekre is. Tapasztalat, hogy a

civil cégekkel kötött fenntartási szerződések Vis Major kitételnél - egyes speciális szerződésektől eltekintve - a szolgáltató érdekei érvényesülnek túlnyomó részben. Ez viszont ellent mond azzal a ténnyel, hogy ezen szituációkban kiemelten szükséges az adott szolgáltatást biztosító infrastruktúra áldozatos, fegyelmezett, profi üzemeltetése és szükség szerinti hibaelhárítása a fenntartó állomány által. Ez a civil szférában nem szavatolható oly szinten, mintha ezen funkciókat jól felkészült és hivatását gyakorló MH alárendelt állomány látná el. A védelmi szféra területén súlyozottan szükséges arányba állítani a biztosítandó szolgáltatások fontosságát a fenntartó saját állomány mindennemű költségvonzatával szemben. A távközlés a vezetést, különböző szakcélú információcserét (légiirányítás, pénzügyi-, humán információk forgalmazását) biztosítja zártcélú hálózatunkban, mely hálózati szolgáltatások biztonságos folyamatos üzemeltetése saját MH alárendelt állománnyal valósítható meg magas szinten és biztonságosan béke és mozgósítási állapotban is.

## Összegzés

A Magyar Honvédség jelenlegi zártcélú hang és adatátviteli célú távközlő hálózata a hordozófelületek, eljárások, valamint szolgáltatások oly széles skáláját sorakoztatja fel, melyeken egy a célszerűségi szempontokat figyelembe vevő hálózatoptimálási-, felügyeleti-, biztonsági-, valamint üzemeltetési feladatköröket ellátó központosított, új feladatrendszer szerint összehangolt menedzsment megvalósítása igen bonyolult feladatnak ígérkezik. Hosszú távon azonban mind anyagi-, mind humán- és technikai erőforrás tervezés szempontjából egy központosított, feladatköreiben újracsoportosított, kibővített menedzsment irányításával, ellenőrzésével, üzemeltetésével magas hálózat-, menedzsmentbiztonság szavatolása mellett a hálózattervezési, útvonalirányítási valamint üzemeltetési feladatkörök optimalizálása is megvalósulna.

A szolgáltatásokkal szembeni elvárások változását figyelembe véve időszerűvé vált egy a hálózattípusok sokszínűségétől független közös platformon dolgozó hálózatoptimálást célzó rendszer megvalósítása a Magyar Honvédség zártcélú távközlési hálózatán, mely a jelenleg alrendszer típusok szerinti területenkénti hálózattervezésből következő hiányosságokat, hibákat küszöbölné ki az IT ajánlások figyelembevételével, ezzel a hálózat működését szolgáltatási és anyagi szempontok szerint optimalizálná és a pontos globális hálózattervezés lehetőségét megteremtené.

## Irodalomjegyzék


[1] Ávéd Zoltán: Üzleti szintű rendszerfelügyelet Coputerworld 2005. 07. 12. pp 16-18.

[2] Szőllősi Lóránd, Marosits Tamás: A biztonságos információkezelés (secure processing) alapjai Híradástechnika 2005/7 pp.28-33.

[3] Híradástechnika LXI. 2004/9 Takács Attila, Császár András, Szabó Róbert, Henk Tamás: Forgalommenedzsment többszörös kapcsolatú állományoknál pp.19-25.

[4] Kassai Károly- Magyar Sándor: A zártcélú hálózat felügyeletének biztonsági kérdései Új Honvédségi szemle 2002/11

[5] Góbor Balázs: „Technológia-független, univerzális azonosítók” PKI közlemények 2004/48 pp.127-140.

**MAROS Dóra, MÉSZÁROS Árpád**

# A MAGYAR TÁVKÖZLÉSI RENDSZER ANOMÁLIÁI A LONDONI TERRORTÁMADÁS TÜKRÉBEN

## Bevezetés

2005. július 7.-én Londonban négy terrorista robbantás történt egy órán belül. A merényletsorozat halálos áldozatainak száma meghaladta az ötvenet, a sebesültek száma több száz volt.

Ilyen esetekben emberek ezrei próbálnak meg kapcsolatot teremteni telefonon keresztül, és van, amikor a kapcsolat sikerességén emberi életek múlnak. Mivel a mobiltelefon a legkézenfekvőbb és leggyorsabban használható segélykérő eszköz, ezért a bajbajutottak és a mentőalakulatok is elsősorban, és legelőször a mobil hálózatokat veszik igénybe. Ez egy természetes reakció, hiszen a mobilok bárhol és bármikor használhatóak – legalábbis a marketingkampányok ezt sulykolják az előfizetőikbe. Tehát ha az előfizető nem tud telefonálni, azt a következtetést vonja le, hogy a hálózatot egyszerűen lekapcsolták. Képzeljük magunkat egy olyan áldozat bőrébe, aki valahol beszorulva, súlyos – talán életveszélyes sérülést – szenvedve kétségbeesetten próbál mobiljáról segítséget kérni. Amíg rá nem találnak – ami hosszú órákat, esetleg napokat is igénybe vehet – a mobilon kívül semmi más lehetősége nincs a segítségkérésre. Vagy képzeljük el, hogy részt veszünk a mentésben és nem tudjuk kihívni a mentőket, vagy a tűzoltókat, mert semmilyen kommunikációs lehetőségünk sincs: nem működnek a mobilhálózatok, a vezetékes vonalak emiatt már túlterheltek, és még olyan egyéb megoldás sem áll rendelkezésre, amely speciálisan a mentésben résztvevők számára biztosított (pl. egy TETRA hálózat). De létezhet, hogy gyermekünk éppen arra indult, ahol az esemény történt.

Mit lehet ilyenkor tenni, hiszen a távközlési hálózatok nem arra lettek tervezve, hogy az átlagosnál 5-10-szer nagyobb forgalmat lebonyolítsanak. A hálózatok kapacitását és a szolgáltatás minőségét elsősorban a profitorientáltság határozza meg, ezért olyan szükséghelyzetekre, amikor a meglévő csatornakapacitás többszörösére lenne szükség, a távközlési szolgáltatók nem készülnek fel. A szükséghelyzet, a katasztrófa, a terroristatámadás már nem magánügy, hanem sok embert és szervezetet érintő közügy. A mentés és annak szervezettsége nem lehet okozati összefüggésben az egyéni érdekekkel.

## A londoni terrortámadás távközlési vonzatai

A terrortámadások következtében – mint minden ilyen esetben – ugrásszerűen megnőtt a telefonhívások száma. Az első rémület után tapasztalható igen nagy mennyiségű hívás először a mobil hálózatokat érintette. A robbantások helyszínét érintő cellákban nagyon rövid időn belül túlterhelés következett be, amely még a nagyon fontos segélyhívásokat is lehetetlenné tette. A jelentések először arról szóltak, hogy központi utasításra lekapcsolták a mobil hálózatokat, egy esetleges újabb robbantástól tartva. Madridban ugyanis mobiltelefon segítségével hozták a robbanószerkezeteket működésbe. Ezek a hírek később valótlannak bizonyultak. A mobil szolgáltatók azonnal tapasztalták a hálózatukban bekövetkező túlterhelést, ezért azonnali lépéseket tettek a kapacitásnövelésére. Ennek egyik módja volt a kódolás megváltoztatása. A

teljes sebességű (Full rate) beszédcsatorna ugyanis 13 kb/s csatornasebességű beszédkódolási eljárást használ a hangátvitelre normál esetben. A mai GSM technikában lehetőség van egy olyan kódolás használatára is, amely a csatornák sebességét csupán 6,5 kbit/s-ra redukálja, így a cellában található csatornakapacitás a duplájára növelhető. Habár az adattömörítés és fading jelenségek ilyen esetben érzékenyebben hatnak az átviteli minőségre, szükséges helyzetekben ez mégis jó megoldás a megnövekedett forgalom kiszolgálására, a túlterhelés enyhítésére. Ugyancsak probléma volt, hogy a segélyhívások sikertelenségi aránya a cellák túlterhelése miatt jelentősen megnőtt. Ennek megoldására a londoni szolgáltatók korlátozták a nem segélyhívást kezdeményező felhasználók hozzáférését a hálózathoz. A mentésben résztvevő alakulatok emberei is csak olyan módon tudták használni a nyilvános hálózatokat, hogy egy speciálisan meghatározott kódot használtak a híváskezdeményezéskor, amely azonosítás után elsődleges prioritást biztosított a számukra a kapcsolat felépítésekor. A hírek alapján az derült ki, hogy még így is sok volt a probléma a mentésben résztvevők közötti kommunikációval, hiszen a már elkészült TETRA rendszert szerződés hiányában sem a mentők sem a tűzoltók nem tudták használni.

A mobil hálózatok túlterheltsége rövid időn belül a vezetékes hálózatokra is hatással volt, hiszen második lehetőségként a legtöbben a vezetékes telefonokat próbálták meg igénybe venni. A vonalak túlterhelése itt is rövid időn belül jelentkezett, amely komoly torlódásokat okozott nemcsak a belföldi, hanem a külföldre irányuló és onnan bejövő forgalomban is. Elindult tehát az a dominóeffektus, amely ilyen esetekben megbénítja a távközlési hálózatok működését. A tapasztalt túlterhelések természetesen hatással voltak az Internet forgalomra is, hiszen a telefonvonalak használhatatlansága miatt nagyon sokan e-mailben próbálták felvenni a kapcsolatot hozzátartozóikkal, barátaikkal. Tovább növelte az Internet forgalmat, hogy nagy mértékben megugrott a különböző hírportálok látogatottsága, hiszen az emberek minél aktuálisabban és gyorsabban kívántak értesülni a fejleményekről. Az Internet szolgáltatók a tapasztalatok szerint jól kezelték a csúcsforgalmat. Ez a dominó – ha kicsit meginogva is – de állva maradt.

A londonihoz hasonló helyzetekben, a fentiekkel összefüggésben számos kérdés merül fel a szerzőkben:

- Hogyan reagálna a magyar távközlési rendszer hasonló helyzetekben?
- Milyen eszközök állnak rendelkezésre a felmerülő többletkapacitás igény
- kielégítésre, vagy a kapacitásproblémák azonnali enyhítésére?
- Ki hozza meg ilyen esetben a döntéseket és azt kik hajtják végre?
- Mennyi idő kell a végrahajtáshoz?
- Milyen szabályozási és végrehajtási háttér szükséges?
- Ki és milyen módon finanszírozza a felmerülő költségeket?
- és végül…
- Kiknek fontosak a fenti kérdések és a válaszok?

## A magyar szabályozási háttér kérdései

A fenti kérdések tekintetében először megvizsgáltuk, hogy jelenleg milyen jogszabályokat vonatkoznak a fentekben felvetett problémákra.

Meghatározónak tekintettük a következő jogszabályokat:

- 2003. évi C. törvény az elektronikus hírközlésről.

- 100/2004. (IV. 27.) Kormányrendelet az elektronikus hírközlés veszélyhelyzeti és minősített időszaki felkészítésének rendszeréről, az államigazgatási szervek feladatairól, működésük feltételeinek biztosításáról.
- 24/2004 IHM rendelet a védelmi feladatokban résztvevő elektronikus hírközlési szolgáltatók kijelöléséről, és felkészítési feladataik meghatározásáról.
- 27/2004. IHM rendelet az informatikai és hírközlési, továbbá a postai ágazat ügyeleti rendszerének létrehozásáról, működtetéséről, hatásköréről, valamint a szolgáltatók bejelentési és kapcsolattartási kötelezettségeiről.

A fenti jogszabályok közül irányadónak tekintettük a 100/2004 kormányrendeletet, amely részletesen meghatározza az elektronikus hírközlési szolgáltatók és hatóságok feladatait veszélyhelyzeti feladatait és a védelmi felkészítés céljait. E szerint:

„3. § A védelmi felkészítés célja, hogy minősített időszakban az elektronikus hírközlő hálózatok:

a) a jogszabályoknak megfelelően képesek legyenek egységesen működő rendszert alkotni;

b) alkalmasak legyenek a kormányzati szervek, a nemzetgazdaság, a fegyveres erők és a rendvédelmi szervek kommunikációs igényeinek kielégítésére, valamint a lakosság légiriasztásával, tájékoztatásával, élet- és vagyonbiztonságával, védelmével és ellátásával összefüggő elektronikus hírközlési feladatok teljesítésére;

c) biztosítsák az elektronikus hírközlési szolgáltatások folyamatosságát a védekezésben és a katasztrófa elhárításban részt vevő szervezetek kommunikációs igényeinek előtérbe helyezésével;

d) felkészültek legyenek az elektronikus hírközlés működését súlyosan befolyásoló természeti vagy emberi tevékenység következtében fellépő események kezelésére;

e) alkalmasak legyenek a Magyar Köztársaság NATO tagságából és a távközlési erőforrások biztosításáról katasztrófa elhárítás és mentés céljára tárgyú Tamperei Egyezményből adódó nemzetközi kötelezettségek ellátására."

A rendelet 18 esetben hivatkozik külön jogszabályokra, amelyek a kapcsolódó területeket vonatkozásában tartalmaznak szabályozásokat. Az alábbiakban csak azokat emeljük ki, amelyek – véleményünk szerint – a londoni merényletek kapcsán felmerült kérések megválaszolásában irányadóak lehetnek:

- „…..A helyreállító szervezetek kijelöléséről, illetőleg a helyreállítás érdekében a külön jogszabály szerinti szerződés megkötéséről - az elektronikus hírközlési szolgáltatókkal egyeztetve - az ágazati miniszter gondoskodik, amelynek során a helyreállítás költségeit a felkészítés összesített szükséglete keretében tervezi…."
- „…..elektronikus hírközlési korlátozások bevezetése külön jogszabályok szerint…."
- „….szükség esetén a különböző hálózatok külön jogszabályok szerinti összekapcsolására, a kerülő átviteli lehetőségek kialakítására az együttműködési igények kielégítése érdekében…."
- „….rombolás, tömeges üzemkiesés, forgalmi torlódás esetén az országosan rendelkezésre álló erők, eszközök, tartalékok külön jogszabályok szerinti igénybevételével és összefogásával a helyreállítási, illetőleg kapacitás növelési munkák végrehajtására, segítésére és irányítására….."

- „…Ha az elektronikus hírközlési szolgáltatás gazdaságmozgósítási, illetőleg védelmi igénybevétele miatt az elektronikus hírközlési szolgáltatónak vagyoni hátránya keletkezik, részére kártalanítás jár külön jogszabályok alapján….”

A fent hivatkozott „külön jogszabályok” eddigi vizsgálataink alapján még nem születtek meg annak ellenére, hogy pontosan ezek a legrelevánsabb kérdések egy veszélyhelyzeti időszakban.

## Tapasztalatok a Magyar Telekom hálózatában

Az előzmények alapján felmerült a kérdés, milyen minőségben és mennyire vagyunk felkészültek – szakmai szemmel vizsgálva – egy adott katasztrófahelyzet kezelésére, a legnagyobb hazai távközlési szervezet adatai és szemszöge alapján. E – nem minősített helyzetre vonatkozó - vizsgálat vezérvonalát a 24/2004. (VIII. 16.) IHM rendelet adta, amely – egyebek mellett - a védelmi feladatokat határozza meg az egyes távközlésben részt vevő távközlési szervezetek részére.

A vizsgálat során először az ország és a külföld – esetünkben kimondottan Londont célzó – összeköttetési rendszert tekintettük át. Megállapíthatóak voltak az alábbiak:

- Az országot elhagyó teljes, ill. bejövő trunkrendszerre nincs áttekintő adatsorunk, s várhatóan egyéb távközlési szolgáltató sem rendelkezik országos rálátással. Így a vizsgálatot a T-Com adataira korlátozottan kellet lefolytatni.
- Nem sikerült egyetlen távközlési szolgáltatónál sem olyan kapcsolatra találni, ahol a jelen vizsgálatban érdemben használható adatokat rendelkezésre bocsátottak volna. Ez feltehetőleg arra utal, hogy a vélt vagy valós vállalati titkok őrzése erősebb, mint egy esetleges veszélyhelyzetben az egymást kisegítő – az ország biztonságát támogató – megoldás keresése.
- A hazai generált forgalom, ill. a tranzitált forgalom pillanatnyi – vagy akár hosszú távú átlagolt - helyzetét feltehetően nem vizsgálja senki, hiszen beavatkozásra alkalmas adatokat senki sem adja tovább, de nem is kér senki. Legalább is ezt kell feltételezni az információink alapján.
- Az egyes távközlési szolgáltatók – minden bizonnyal – a legjobb gazdasági érdekeiknek megfelelően kezelik a forgalmukat, hiszen azt a megismert részletek alapján a pillanatnyi profit, és nem a rövid, vagy hosszú távú biztonság vezérli.

Áttekintettük a 24/2004. IHM rendeletben előírt – katasztrófahelyzetekre vonatkozó – követelmények teljesülését mindazon esetekre, amelyekhez hozzáfértünk. A megismert állapotokat úgy tekintettük, mintha a londoni események miatt nálunk is katasztrófa helyzet alakult volna ki. Ezzel kapcsolatban a korábbi tapasztalatok szerint várható volt, hogy a forgalom kezelésekor az átviteli utak közötti irányítás során az egy kábelben futó párhuzamos trunknyalábokat külön átviteli iránynak veszik. Ez a gyakorlat természetesen a biztonság rovására megy, hiszen ha egy optikai kábel megsérül, akkor többnyire minden szála elszakad, vagyis valamennyi nyaláb sérül. A valóságban az alábbiakat találtuk:

- Közel fél éve a Matáv Rt. a legfrekventáltabb irányokban befejezte a nyomvonalfüggetlen trunkirányokra való átállást, vagyis a tartalék átviteli irányok az első esettől független nyomvonalú kábelekben valósulnak meg. Ez a tény mérsékli a forgalom lebonyolítás sebezhetőségét.
- Nem egy irányban többszörös elérési lehetőség is megvalósult, lehetőleg mindannyiszor harmadik, sőt negyedik kábelirányt felhasználva.

- A fenti megállapítások belföldre igazak, a külföldi szakaszok ez irányú adatai homályban maradtak.
- A londoni robbantások időszakában megnövekedett forgalom lebonyolítását említésre érdemes – magyar beavatkozást kívánó – kábelkiesés, átviteli irány lehetetlenülés vagy berendezéshiba nem zavarta meg.

A Magyar Telekom hálózatán London felé irányuló távközlési forgalom fogadására több ottani szolgáltató és trunkcsoport felhasználásával – kerülő irányokat is igénybe véve - került sor. A forgalom rögzített adataiból nagyon pontosan meg lehetett állapítani a terrorcselekmény hazai bejelentésének időpontját, hiszen onnantól kezdve meredeken emelkedett a kimenő hívások száma. Egy átlagos naphoz képest (esetünkben az előző naphoz viszonyítva) a forgalom csaknem minden szolgáltató felé az ötszörösére ugrott. A nagy forgalmi felfutás lecsengése kissé lassabb volt, mint a felfutás, késő estére, másnap hajnalra közelítette csak meg az átlagos forgalmat.

A forgalmi adatok grafikonjain alig lehetett megkülönböztetni a beszélgetésben végződő hívásokat a londoni trunkelfogásokat a híváskezdeményektől, ami azt bizonyítja, hogy a hazai megugrott forgalom kezelése – legalább is a Magyar Telekomnál – elfogadható volt a kismértékű túlcsordulás miatt.

Ha tovább vizsgáljuk a forgalmi adatokat, megállapítható, hogy a hívások sikertelenségének döntő hányada külföldre esik. Ennek mindenek előtt az az oka, hogy a kinti (London) szolgáltatóknál torlódás merült fel, amelyet innen nem lehetett befolyásolni, pontosabban csak gerjeszteni lehetett. A műszakilag sikeres, ám mégsem beszélgetésben végződő hívások meddőségében a döntő szerep a hívott félen múlott: nem vette fel, nem volt bekapcsolva, ill. a helyi szolgáltató nem érte el.

A hívásadatok további vizsgálatánál megállapítható volt, hogy a normál napoknál sokszorta nagyobb forgalom lebonyolítása nem okozott különösebb műszaki feladatokat, emberi beavatkozásra sem volt szükség.

Mind ezek mellett figyelemfelkeltő jelenségek az alábbiak:

- A kimenő hívásirányok ötszöröződése mellett a vissza irányú forgalom közel 15 %-al csökkent, ami akár a kinti torlódás miatti nehéz kinti beszélgetés kezdeményezés, akár a szükséges kapcsolatteremtések hazai indításával is magyarázható. (Kérdés: ez a tapasztalat mennyiben általánosítható, s használható-e hasonló helyzetekben trunkirányok szükség-váltására?)
- A központtorlódás (külföldön) és a szabad átviteli utak hiánya (torlódás a központ előtt illetve után) a csúcsterhelések időszakában a hívások több, mint felét hiúsította meg. (Kérdés: érdemes-e ezen jelenséget figyelni és beavatkozást tervezni hasonló esetekre, vagy egyedi esetként csak tudomásul kell venni ezen állapotot?)

## Következtetések

Felvetődik tehát a kérdés, hogy a példa mennyire igazolja felkészültségünket egy éles helyzetre. A jogszabályi háttér hogyan biztosítja (vagy miért nem biztosítja) a szükséges szabályozásokat, és mi a felelőssége a hatóságoknak és a szolgáltatóknak ezek megalkotásában illetve betartásában? Vajon rendben lévőnek lehet-e tekinteni, hogy a jelenlegi forgalomkezelési felkészültségünk országos szinten teljesen az üzleti szféra érdekei szerint alakuljon a továbbiakban is? Esetleg el kéne gondolkodni egy – kissé a biztonság felé is irányuló – alternatív megoldás vizsgálatán, ami szabályozási, beruházási kérdéseket is felvet, s szorosabb együttműködésre késztetheti a társszolgáltatókat az ország polgárai érdekében?

Vajon országos szempontból elegendő-e az, hogy minden szolgáltató a saját pillanatnyi érdekeit pátyolgatva így-úgy megoldja az adott forgalmi helyzetét, ám a horizontális összeköttetések mérete és szerepe – legalábbis becslési szinten – nem biztos, hogy alkalmas lenne egy komolyabb forgalmi probléma kezelésére. Ezek a felemásnak tekinthető üzleti megoldások kimerítik-e a 2003. évi C. törvény (az elektronikus hírközlésről) 86. § d) pontjában előírt azon követelményét, mi szerint minősített időszakban együtt kell működni más szolgáltatókkal?

Eleget tesznek-e a hétköznapokra méretezett átviteli rendszerek egy katasztrófa okozta extra forgalomra, amilyenre, pl. a 100/2004. (IV. 27.) Korm. rendelet az elektronikus hírközlés veszélyhelyzeti és minősített időszaki felkészítésének rendszeréről, az államigazgatási szervek feladatairól, működésük feltételeinek biztosításáról szóló elvárásoknak, avagy erre csak egy nálunk bekövetkezendő éles helyzet utáni elemzéskor kaphatjuk meg a választ? Mivel a szilveszteri forgalmi helyzet némileg emlékeztet egy katasztrófa okán megugró forgalmi állapottal, feltehetően sokunkban ugyanaz a válasz erősödik meg. Csupán az az eset már emberéletre, vérre megy!

Soha ne kelljen megtapasztalnunk, hogy feleslegesen hívtuk fel a figyelmet a távközlésünk egy gyenge pontjára! Reméljük, hogy az általunk feltárt problémákra és a felmerült kérdésekre minél előbb választ kapunk? De kitől és mikor?

**MÁTÉ József**

# A KATASZTRÓFAVÉDELEM INFOKOMMUNIKÁCIÓS TÁMOGATOTTSÁGA

A Magyar Köztársaság lakosságának biztonsága, a nemzetgazdaság és a nemzeti örökség javainak védelme minden állampolgárnak és szervezetnek kiemelt feladata. A „humanitárius segítségnyújtások" korában felértékelődött a katasztrófák megelőzésének és gyors felszámolásának szerepe. Az elmúlt években bekövetkezett jelentős számú katasztrófa- és veszélyhelyzetek „eredményeként" fokozott figyelem kíséri a katasztrófavédelem mindennapi tevékenységét.

Az 1996. évi XXXVII. törvény a Polgári Védelemről, valamint a 1999. évi LXXIV. Törvény (továbbiakban: Kat. Tv.) IV. fejezete, továbbá az érvényben lévő kormányhatározatok és rendeletek pontosan meghatározzák a katasztrófavédelem feladatrendszerét és tevékenységi körét. Mindezen feladatok és a katasztrófavédelemre felruházott hatósági és szakhatósági elvárások jelentős kihívás elé állították a BM Országos Katasztrófavédelmi Főigazgatóságot és területi szerveit.

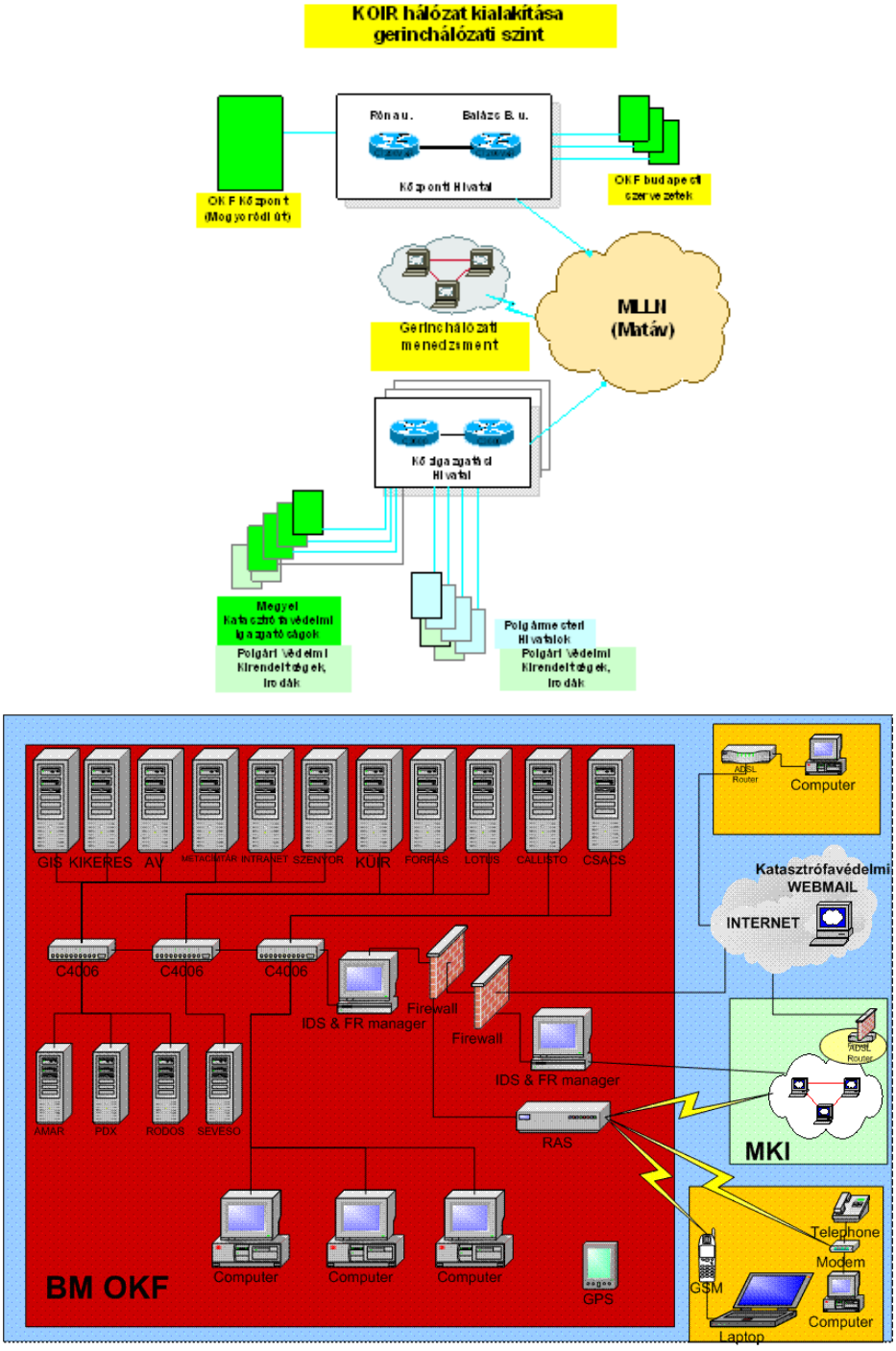
A Kat. Tv. 14. paragrafusa határozza meg a katasztrófavédelmi célú távközlési és informatikai rendszerek egységes irányítási rendszerbe történő kialakítását és működtetését). A Kat. Tv. 5.§ e. pontja kimondja, hogy a Kormány feladata a katasztrófavédelmi információs rendszer létrehozása.

## KOIR - Katasztrófavédelmi Országos Információs Rendszer

A katasztrófavédelmi célú távközlési és informatikai rendszerek egységes irányítási rendszerben történő működtetésének alapfeltétele volt a Katasztrófavédelem Országos Információs Rendszerének (KOIR) kialakítása. A KOIR megvalósításával az igazgatóságok nemcsak analóg kapcsolt vonalon, hanem a belügyi INTRANET hálózatra való felfűzéssel tudják elérni a főigazgatóság informatikai hálózatát. A megfelelő adatátviteli sávszélesség biztosításával elérhetővé váltak a levelező rendszerek, a térinformatikai adatbázis, a vírusvédelmi rendszer által nyújtott lehetőségek, a HTML alapú hírcsatorna és egyéb, a mindennapi munkát megkönnyítő, a hatékonyságot növelő alkalmazások. A fax, a telefon és az adatátviteli költségek csökkentése szintén indokolta a KOIR megvalósítását. A megvalósítás legfontosabb állomásai:

- Az OKF és a megyei igazgatóságok helyi hálózatának (LAN) kiépítése.
- A LAN-ok integrálása országos kiterjedésű adatátviteli hálózatba (WAN).
- Virtuális magánhálózat létrehozása a BM meglévő adatátviteli rendszerein.
- A hálózat csomópontjain az alkalmazott átviteli módszernek (TCP/IP) megfelelő útválasztó, kapcsoló és hálózati kiszolgáló eszközök telepítése.

A KOIR megfelel a Belügyminisztérium hosszú távú hálózatfejlesztési koncepciójában meghatározott követelményeknek, multi-protokoll alapú adatátvitelt biztosít, ahol a vonalak és a rendszer aktív elemei egy központból menedzselhetőek. Nagy megbízhatóságú, nagy hibatűrő képességű rendszer (a rendelkezésre állás 99% fölötti), amelyben a hálózat virtuális magánhálózatként kezelhető. A kommunikációs sávszélességet optimálisan használja ki, a megjelölt minimális sávszélesség (128kbps) rugalmasan bővíthető, a végpontok száma igény szerint rugalmasan növelhető, az adat- és hangátvitel integrálása megvalósítható.

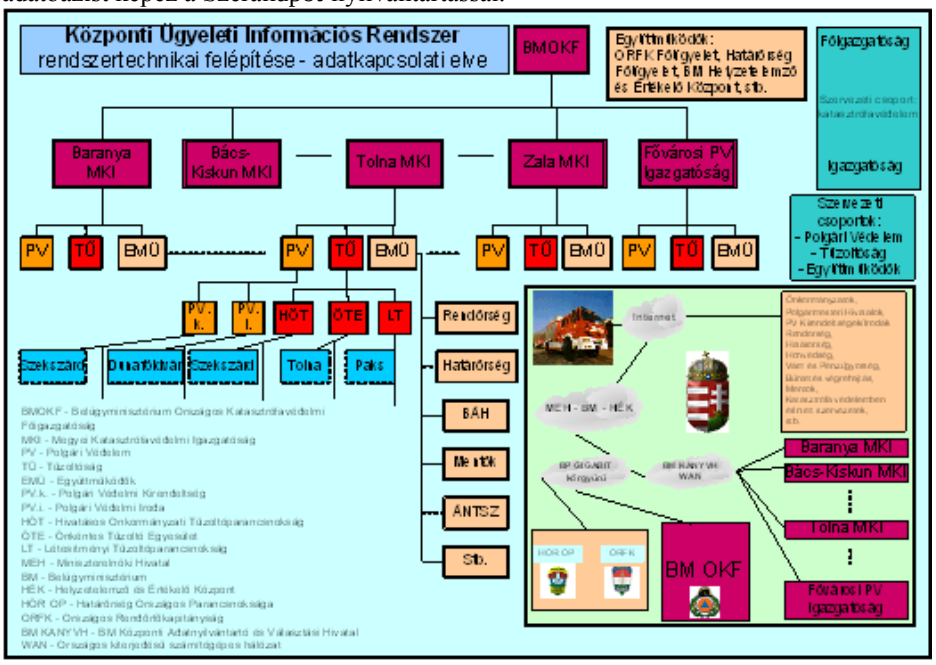

KOIR hálózat kialakítása
gerinchálózati szint
Rónai u.
Balázs B. u.
Központi Hivatal
OKF Központ
(Mogyoródi út)
OKF budapesti
szervezetek
Gerinchálózati
menedzsment
MLLN
(Matáv)
Kódigazgatási
Hivatal
Megyei
Katasztrófavédelmi
Igazgatóságok
Polgári Védelmi
Kirendeltségek,
Irodák
Polgármesteri
Hivatalok
Polgári Védelmi
Kirendeltségek,
Irodák
GIS
KIKERES
AV
METACIMTÁR
INTRANET
SZENTYOR
KÜIR
FORRÁS
LOTUS
CALLISTO
CSACS
C4006
C4006
C4006
IDS & FR manager
Firewall
Firewall
IDS & FR manager
AMAR
PDX
RODOS
SEVESO
RAS
BM OKF
Computer
Computer
Computer
GPS
ADSL
Router
Computer
Katasztrófavédelmi
WEBMAIL
INTERNET
MKI
Telephone
Modem
GSM
Computer
Laptop

A rendszeren belül kialakítható a hálózati adat- és rendszermenedzsment, a napi munkavégzés hatékonyságának növelésére Intranet alapú hírcsatorna, komplex levelező-, illetve ügyviteli rendszer üzemeltethető, az OKF és a területei szervek munkatársai valamennyi szakterület által alkalmazott rendszer adatállományához jogosultság szerinti hozzáféréssel rendelkeznek. Az eszközpark biztosítja az adat útvonalakon a titkosított kommunikációt (3DES/IPSec), a csomag- és csomagtípus-prioritást biztosító védelmi megoldást (QoS), a hardveres tűzfalat, a VPN kliens autentikációt, a hardver elemek menedzselhetőségét, az erőforrások távoli elérését.

### KÜIR – Központi Ügyeleti Információs Rendszer

A KÜIR egy infokommunikációs rendszer, amely a katasztrófahelyzetben, veszélyhelyzet-kezelésben érintett és együttműködő szervezetek számára könnyíti meg az elektronikus kapcsolattartást, az információk áramlását. Megvalósítja az információk gyors elektronikus cseréjét, a csoportmunkát, s a rendszerbe foglalt egységes megjelenésre az Internetet használja fel virtuális magánhálózat kialakításával.

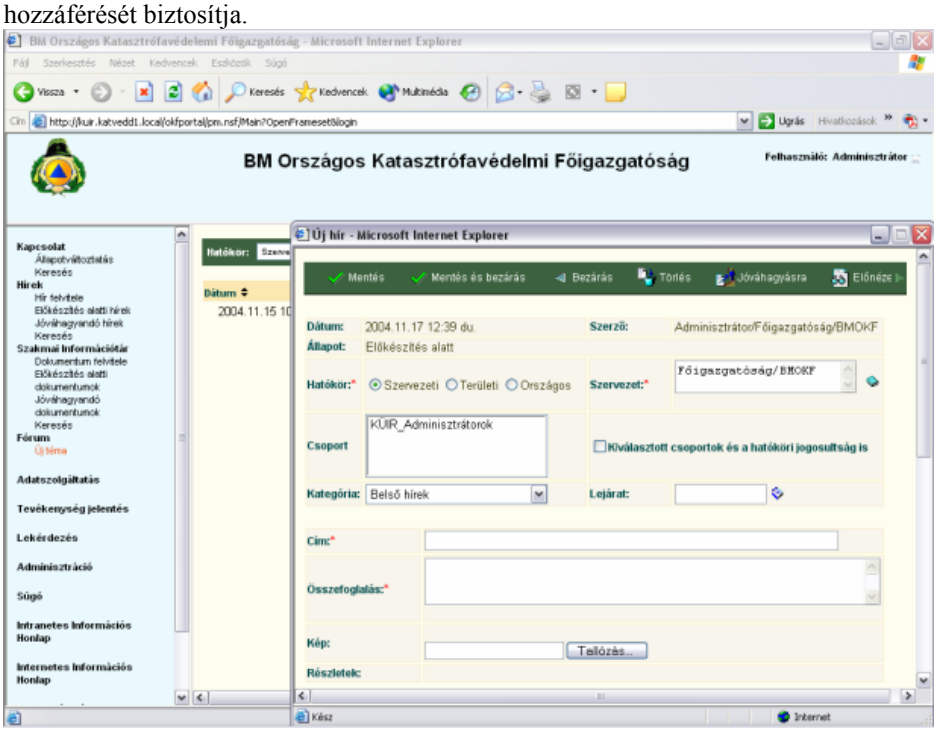
A KÜIR megvalósításával az Internet hozzáféréssel rendelkező helyi és területi katasztrófavédelmi szervezetek számára olyan információs rendszer alakult ki, amelynek segítségével - űrlap alapú adatszolgáltatások feldolgozását és összesítését követően - országos és területi szinten bármely időpillanatban meghatározhatók a veszélyhelyzet kezelésére mozgósítható erők és eszközök, s nyomon követhető valamennyi adatszolgáltatást teljesítő szervezet tevékenysége. A rendszerbe integrálásra került az Riasztási és Segítségnyújtási Tervek elektronikus változata, amely relációs adatbázist képez a Szerállapot-nyilvántartással.



## Intranet Portál

Az intranet portál egy tartalmi és jogosultsági hierarchia szerint gyorsan elérhető, adatbázis megjelenítést (szerkesztést), és a felhasználók hierarchikus azonosítását ellátó rendszer, szigorú hozzáférési adminisztrációval. Egységes felhasználói felület létrehozásával megoldja a különféle információforrásokból származó adattartalmak egy képernyőn való megjelenítését, a belső hírek előállítását és terjesztését, lehetőséget teremt a biztonságos távmunkára, ösztönzi a dolgozók közötti információcserét. Az Intranet Portál előnye, hogy a szervezet logikai belső hálózatára épít, azaz külső, idegen személyek részére egyáltalán nem, vagy csak korlátozottan elérhető.

A KÜIR megvalósításával együtt készült a Katasztrófavédelmi Intranet Portál, melynek bevezetésével elérhető, hogy valamennyi szakterület, valamennyi szervezet önállóan szerkesztett információs oldalakkal jelenhessen meg. Lehetőség nyílt az űrlap alapú adatszolgáltatás kidolgozására és megvalósítására. A kialakításra került Intranet Portál a könnyen és gyorsan kereshető információtárolást helyezi fókuszba. Tekintve, hogy a portálon nemcsak publikus információk jelennek meg, kiemelten fontos feladata, hogy a tárolt adatokhoz csak jogosultsággal rendelkező személyek hozzáférését biztosítja.

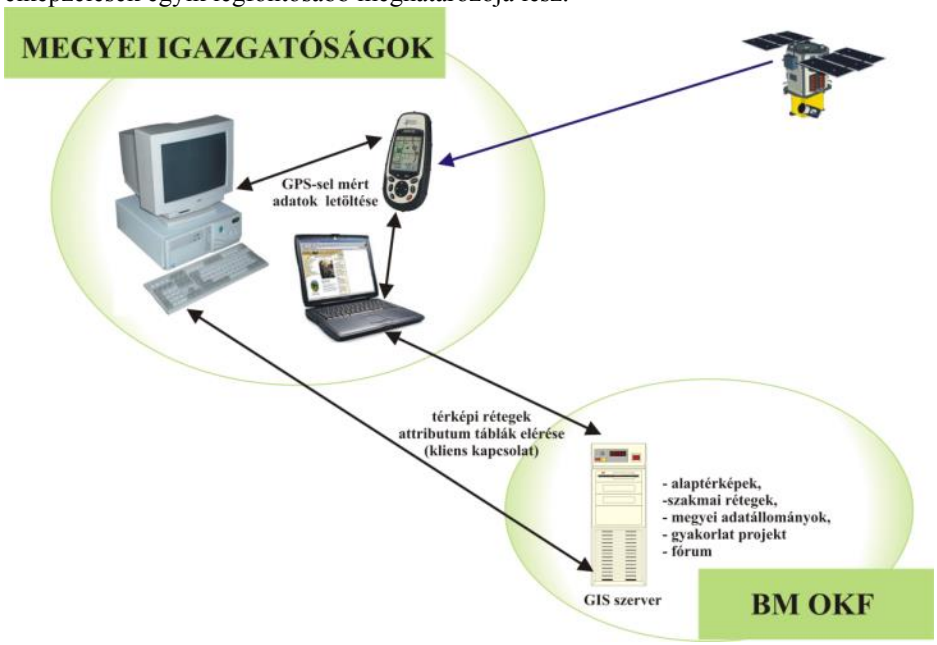



## KATIR – Katasztrófavédelmi Térinformatikai Rendszer

A katasztrófaveszélyt jelentő folyamatok térben és időben zajlanak le, ezért a katasztrófavédelmi szervek irányítási, koordinációs és ellenőrzési feladatainak hatékony ellátása integrált térképi szemléleten alapuló gyakorlatot követel. A KATIR kialakításának célja egy olyan térinformatikai rendszer létrehozása és üzemeltetése, mely lehetővé teszi a térbeli adatok pontos és automatikus áramoltatását, s megfelelő

leválogatással rövid idő alatt képes döntési információkat szolgáltatni a veszélyhelyzet-kezelés irányítójának.

A KATIR nem egy elkülönített informatikai rendszer, a KOIR szerves részét képezi, s fejlesztése szorosan összefonódik a KÜIR és az Intranet Portál fejlesztésével is. A KATIR jelenleg a megyei igazgatóságok szintjéig került kiépítésre. Mind az OKF-en, mind az igazgatóságoknál rendelkezésre állnak a rendszert kiszolgáló alapvető hardver és szoftvereszközök, s a katasztrófavédelmi továbbképzési rendszerben is fokozott hangsúlyt kapott a személyi állomány térinformatikai képzése. A technikai eszközfejlesztések eredményeként mára nemcsak asztali, hanem mobil eszközök is a térinformatika szolgálatába lettek állítva. Jelenleg a térinformatikai rendszer adatbázisának tervezése folyik, amelynek meghatározása és kialakítása a jövőbeli fejlesztési elképzelések egyik legfontosabb meghatározója lesz.




### Térinformatikai MetaAdattár

A katasztrófavédelmi térinformatikai rendszer adatminőségének kezelése megköveteli a rendszer adatintegráló képességének szabályozását. E célból kerül meghatározásra a térinformatikai metaadattár, ami egy adattárház az adatbázist alkotó adattáblák fontosabb jellemzőinek és tartalmilag azonos adattípusainak meghatározásával. Feladata, hogy az adatfeldolgozás helyétől és helyi sajátosságaitól függetlenül országos szinten biztosítsa az információk egységes rendszerbe szervezését és megjelenítését. A metaadattár nem más, mint a rendszer adatbázis tartalmának egyfajta (kapcsolati szintek nélküli) statikus leírása.

A metaadatbázis tartalma érvényét tekintve két osztályba sorolható:

Kötelező – az OKF által központilag meghatározott adatgyűjtések esetében az országos adattáblák létrehozása miatt a metaadattárban meghatározott adatstruktúra használata.

Ajánlás - a kötelezően előírt adatgyűjtéseken túl a megyei igazgatóságok a helyi sajátosságok figyelembevételével maga dönthet a feldolgozásra kerülő leíró adatok köréről.

Tekintettel azonban arra, hogy egyazon adatgyűjtés több igazgatóság estében is igényként merülhet fel, célszerű, ha az adatgyűjtés már kezdettől fogva azonos formai és tartalmi jellemzőkkel történik meg. Ezért a megkezdett, vagy újólag elrendelt adatgyűjtéseket tájékoztatás céljából ajánlás szinten a központi metaadattárban szerepeltetni kell.

Alap digitális térképek és adatbázisok:

- DTA-50 2.0 – Magyarország digitális alaptérképe (EOV).
- DSM-2003 / 10 – Magyarország valamennyi települését tartalmazó digitális utcatérkép.
- DDM-200 – Magyarország digitális domborzati térképe.




## Katasztrófavédelmi MetaCímtár

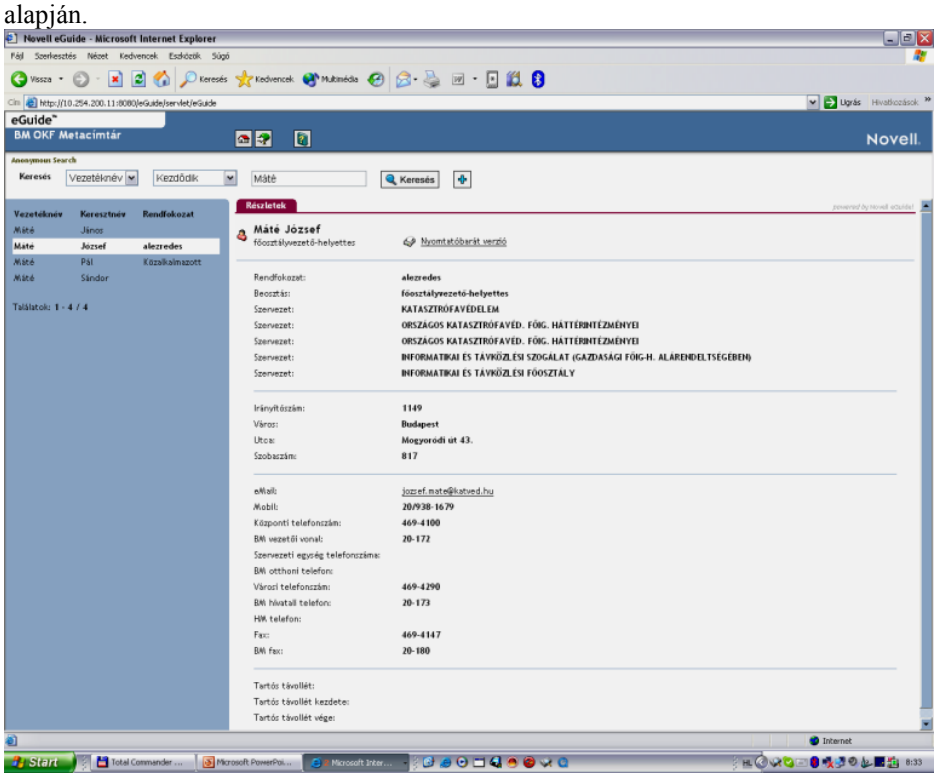
A MetaCímtár lehetőséget biztosít valamennyi katasztrófavédelemben érintett szerv, illetve személy elérhetőségi adatainak HTML alapú nyilvántartására és megjelenítésére, egységes szerkezeti keretbe foglalására, csoportos lekérdezésére.

A MetaCímtár az alapadatokat a SZENYOR személyügyi nyilvántartó rendszer publikus címtár interfészéből kapja, az adminisztrátor részére WEB-es felületet biztosít a vezetékes és mobil telefonszámok, valamint az elektronikus levelező fiókok aktualizálására.

A MetaCímtár kialakítása teremti meg a hálózati erőforrás kiosztás jogosultsági szintmeghatározásához szükséges peremfeltételeket. A bevezetés alatt álló ZenWorks - hálózatmenedzsment a jogosultsági szintek függvényében fogja engedi, illetve korlátozni a számítógépes hálózat központi erőforrásainak és a menedzsment alá vont személyi számítógépek szolgáltatásainak elérését, a központi futtatású alkalmazások és adatbázisok elérhetőségének mértékét.

A Katasztrófavédelmi MetaCímtár közel 1900 fő elérhetőségi adatait tartalmazza az OKF, a katasztrófavédelmi igazgatóságok, a polgári védelmi kirendeltségek és irodák, valamint a Megyei Védelmi Bizottságok személyi állományából.

A felvitt adatok alapján személyi és hierarchikus (szervezeti) keresés kezdeményezhető. A személyi keresés esetén további relációs keresési lehetőségek (kezdődik, egyezik, tartalmaz, végződik) adottak a vezetéknév, a keresztnév és a beosztás alapján.

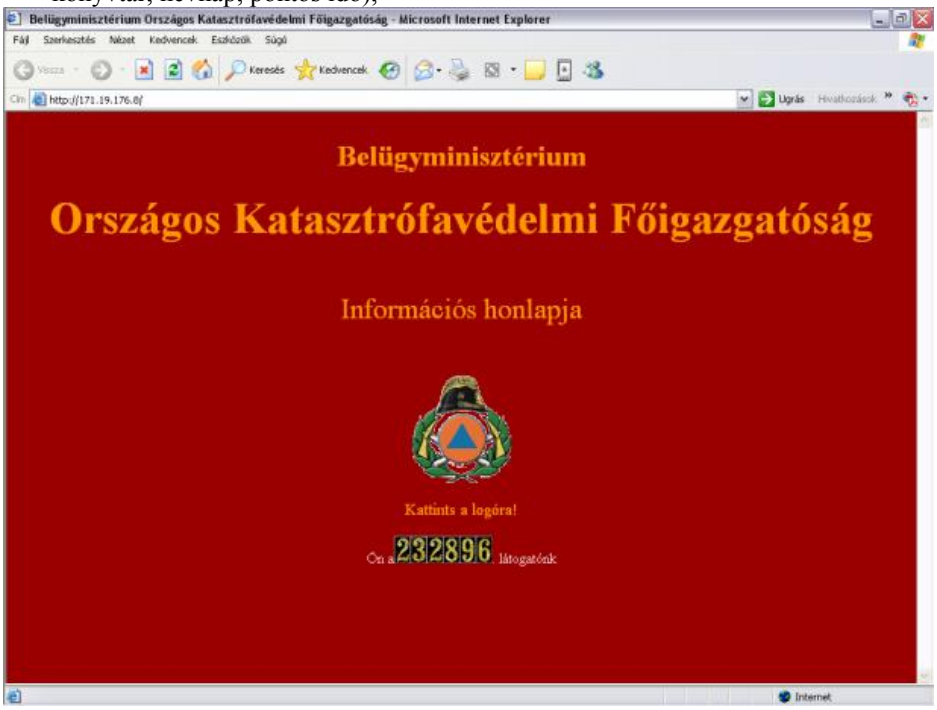



## Információs honlap

A BM OKF információs honlapja – a katasztrófavédelmi intranet - a helyi hálózaton a 171.19.176.8 IP cím alatt érhető el. A honlapról több, a napi munkában fel-

használható, illetve információs jellegű oldal érhető el. Ezek (a teljesség igénye nélkül):

- számítógépes alapismeretek,
- aktuális hírek (napi hírek, belső információk, tőzsde, hírek a nagyvilágból, újságos stand, időjárás és vízállás adatok, Balaton információ),
- a megyei igazgatóságok és a Közbeszerzési Tanács honlapjai,
- levelező szolgáltatás,
- KIKERES kormányzati keresőrendszer,
- AMAR és Káreset Adatszolgáltatási Program adatok,
- információs oldalak (kormányzati címtár, telefonszám tudakozó, menetrend, könyvtár, névnap, pontos idő),




### Nukleáris baleset-elhárításhoz kapcsolódó rendszerek

A veszélyhelyzetek elhárításával kapcsolatos eddigi tapasztalatok szerint a megelőzés egységes rendszerének megteremtése az egész világon nagymértékben felértékelődött az elmúlt időszakban. A megelőzést, a védekezést és a következmények felszámolását a különféle döntéstámogató, országos és nemzetközi szintű folyamatos információs és adatcsere, valamint védekezési rendszerek összehangolásával lehet biztosítani.

A szennyezőanyagok légköri kibocsátásával nukleáris események, veszélyhelyzetek esetében fontos szempont, hogy a légköri terjedés-számítási eredmények tovább feldolgozhatóak, és beépíthetők legyenek az ilyen esetekben rendkívül felelősségteljes döntések meghozatalát segítő alkalmazásokba, amelyek leginkább szolgálják a lakosságvédelmének és az állampolgárok biztonságát. Ezt az elvárást nagymértékben

kielégíti az Európai Unió által EU Phare program keretében a BM OKF-en telepítésre került, jelenleg a magyarországi megvalósítás (honosítás) fázisában lévő Valós idejű Online Nukleáris Döntéstámogató Rendszer (röviden: RODOS / Real-time On-line Decision SuppOrt System, illetve Nemzetközi Regionális Radiológiai Adatcsere Központ (röviden: PDX / Prototype Data eXchange system) rendszerek.

## 1. A Nemzetközi Regionális Radiológiai Adatcsere Központ (PDX rendszer)

A PDX rendszer lehetővé teszi a rendszerben levő országok radiológiai és meteorológiai monitoring, környezeti fix laboratóriumi rendszerének, továbbá a területén működő atomerőművek adatainak elérését normál, illetve veszélyhelyzeti időszakban a Közép-Európai (magyarországi) és a Kelet-Európai (oroszországi) regionális PDX központokon át. Az adatok elérése ISDN2 adatvonalon keresztül, nemzetközileg egységes EURDEP (EURopean Data Exchange Platform) formátumban történik. Az EURDEP formátumú adatok kezelése, rendszerezése Oracle adatbázis kezelő rendszer segítségével történik.

Ez az információ és adatcsere folyamatos információt, adatbázist biztosít a tagországok számára az európai térség országainak radiológiai, meteorológiai, levegő, talaj és víz szennyezettségének aktuális helyzetéről.

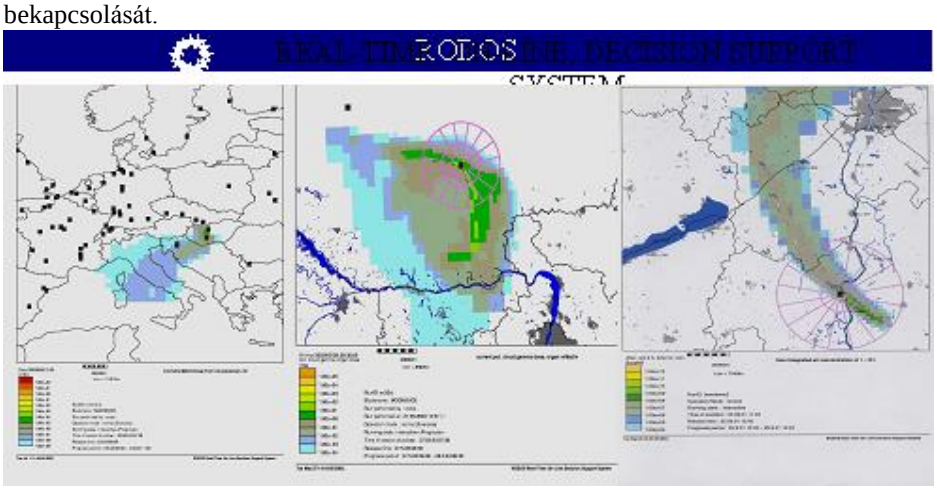
A PDX adatait, a RODOS rendszer közvetve fel tudja használni a több országon átnyúló nukleáris események hatásinak vizsgálatához, értékeléséhez. A RODOS rendszer által készített modellek (grafikus, táblázatos, diagrammos és szöveges típusú) eredmény file-i a PDX rendszer segítségével könnyen, gyorsan eljutathatók a Nemzetközi Regionális alközpontokon keresztül az egyes érintett tagországok Nemzeti alközpontjaiba. A különböző helyzetekben kiválasztott adatok szükség esetén könnyedén beilleszthetők a rendszer által biztosított nemzetközileg elfogadott szabvány EMERCON formátumú táviratokba és megküldhetők az arra érintett országok számára. A beérkező adatok megléte lehetővé teszi a mérési eredményekben jelentkező trendek figyelemmel kisérését, értékelését. A PDX rendszer hazai és nemzetközi adatbázisokból épül fel, melyek jelenleg a következők:

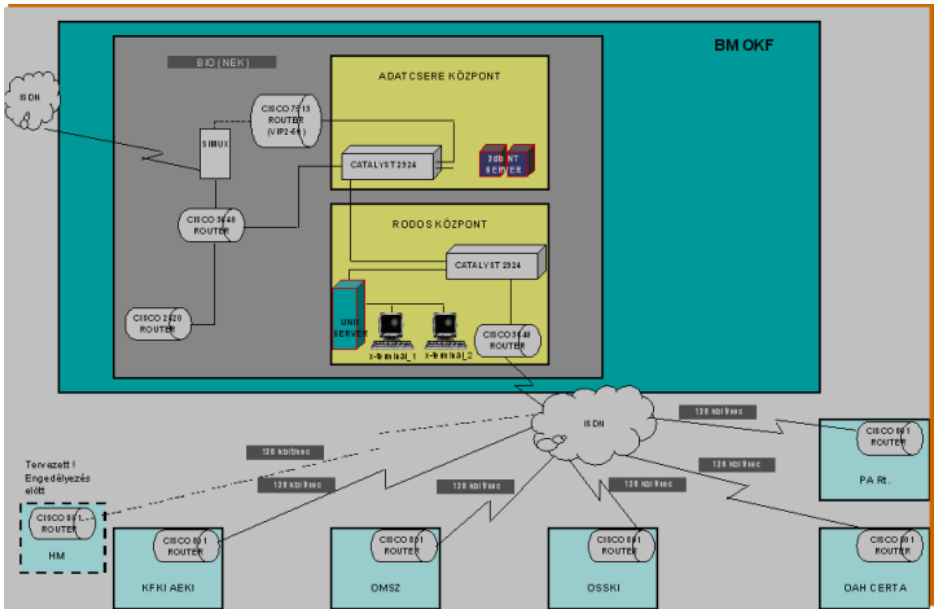
Hazai szintű:

- AMAR rendszer (országos Automatikus radiológiai Mérő és Adatgyűjtő Rendszer) mérési adatai a nukleáris szakterület alhálózatán keresztül
- Az Országos Sugárbiológiai és Sugáregészségügyi Kutató Intézet (OSSKI) által szolgáltatott Országos Környezeti Sugárzásfigyelő és Ellenőrző Rendszer (OKSER) mérési adatai /amely tartalmazza a egészségügyi radiológiai mérő és adatgyűjtő hálózat (ERMAH), a hatósági környezeti sugárfigyelő és ellenőrző rendszer (HAKSER) és a az FM mérőhálózatok és laboratóriumok mérési adatait/ ISDN2 adatvonalon.
- A KFKI AEKI környezeti radiológiai mérőrendszerének mérési adatai ISDN2 adatvonalon.
- OMSZ Paks és Budapest 100 km-es környezetében lévő meteorológiai távmérőállomások mérési adatai ISDN2 adatvonalon.
- Nemzetközi szintű:
- Az obnyinszki (ukrán) kelet-európai regionális radiológiai adatcsere központtal való ISDN adatkapcsolat rendszere révén az orosz, ukrán, belorusz radiológiai, meteorológiai és környezeti laboratóriumi mérési adatokhoz való hozzáférés nor-

mál, gyakorlati és veszélyhelyzeti időszaknak megfelelő, meghatározott gyakorisággal.

Napirenden van a PDX rendszer továbbfejlesztése, melynek keretében a rendszeren belüli nemzetközi adatcsere közeljövőben ki fog bővülni az osztrák, a szlovák, a szlovén és horvát radiológiai, meteorológia és környezeti laboratóriumi adatokkal és későbbiekben további országok nemzeti központjainak is tervezzük a rendszerbe történő bekapcsolását.





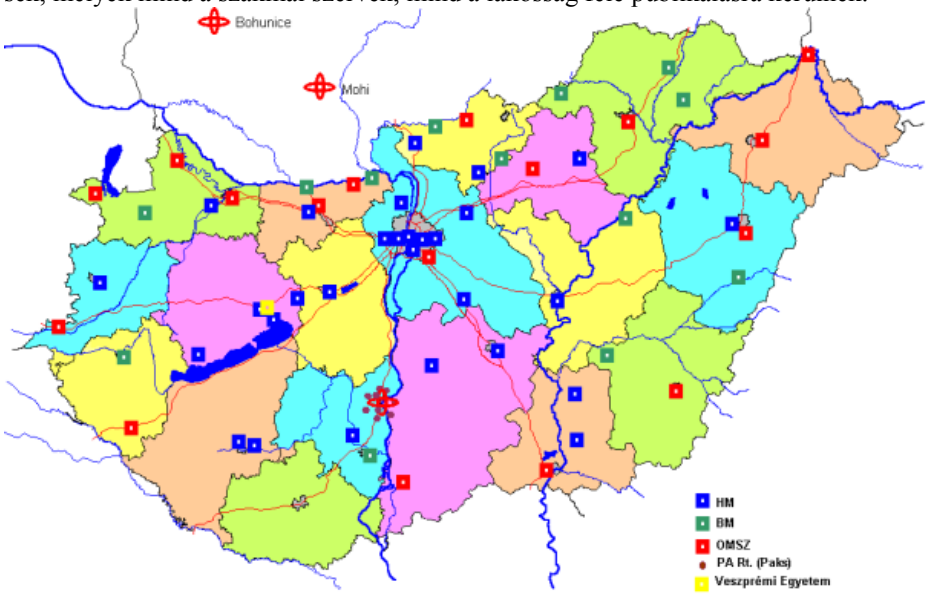

## 2. Az OSJER Országos Radiológiai Távmérő Hálózata (AMAR)

Régóta tudjuk, hogy nap, mint nap együtt élünk az ionizáló sugárzással. A természetes háttérsugárzás eredete kettős: egyrészt a Napból és a világűrből érkező kozmi-

kus sugárzás, másrészt a környezetből érkező talajsugárzás okozza. Ennek köszönhető, hogy a háttérsugárzás térben és időben folyamatosan változik, jelentősen függ a talajszerkezettől, az időjárástól, a Nap tevékenységtől és egyéb kozmikus jelenségektől.

A Magyar Köztársaság területén a háttérsugárzás mérését 1993 óta az Országos Sugárfigyelő, Jelző és Ellenőrző Rendszer részét képező Országos Radiológiai Távmérő Hálózat mérőállomásai végzik. Az Országos Radiológiai Távmérő Hálózat a honvédelmi, belügyi ágazati rendszerekből, az Országos Meteorológiai Szolgálat és a Paksi Atomerőmű Rt. összesen 77 db mérőállomásából áll jelenleg.

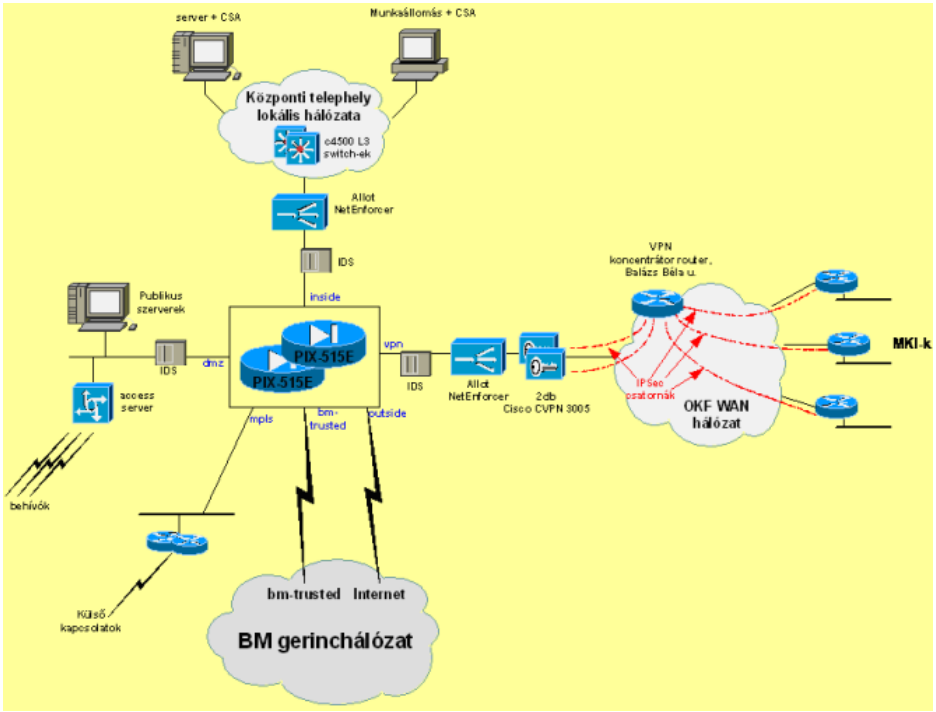
A rendszer a helyi meteorológiai adatok mellett a környezeti gamma dózisteljesítmény értékeket méri. A háttérsugárzás mértéke (a dózisteljesítmény) a Magyar Köztársaság területén 60-180 nSv/óra között változik. Amennyiben a háttérsugárzás valamelyik mérőállomáson meghaladja a riasztási szintet – 500 nSv/óra – az állomás riasztási jelet küld a központba, amelyet kivizsgálnak. Az összegyűjtött adatok az Országos Sugárfigyelő, Jelző és Ellenőrző Rendszer központjaként is működő BM OKF Nukleáris Baleseti Információs és Értékelő Központba érkeznek be. Az adatokat a központ folyamatosan értékeli, ellenőrzi és eltárolja, illetve a többi ágazat felé továbbítja. A mérési adatokból napi, heti és havi rendszerességgel készülnek háttérsugárzási jelentések, melyek mind a szakmai szervek, mind a lakosság felé publikálásra kerülnek.




### Behatolás detektáló (IDS - Intrusion Detection System) és sávszélességmenedzselő rendszer

Az utóbbi években rohamosan nő a számítógépes vírusok, férgek okozta veszélyek bekövetkezésének kockázata. A belügyi hálózat több alkalommal is külső és belső adatkapcsolatokon keresztül megfertőződött, egyes esetekben a központi szolgáltatások szüneteltetését eredményezték e jelenségek. A belügyi fejlesztési tendenciákat figyelembe véve az OKF-en olyan rendszert hoztunk létre, amely részben automatikusan, részben manuálisan képes a nem tipikus hálózati forgalmat kiszűrni, így megelőz-

ni a munkaállomások és adatállományaik, valamint a központi szolgáltatásokat biztosító szerverek károsodását. Az IDS rendszerek napi 24 órás felügyeletet nyújtanak a hálózatnak, figyelve annak forgalmát, valamint elemezve a forgalmi mintákat és a hálózaton fellelhető jeleket. A vizsgálatokból származó adatokat az eszköz menedzsment szoftver komponense felügyeli. A támadás érzékelésekor a rendszer automatikus reakciókat hajt végre. Ilyen reakció lehet – a beállításoktól függően – a menedzsment rendszer felé küldött jelzés, a hálózati eszközök tiltólistáinak átprogramozása illetve a TCP kapcsolat megszakítása. A nem kívánatos aktivitást úgynevezett „signature" alapon ismeri fel, melynek lényege, hogy a hálózatról elkapott csomagokat, bizonyos feltételes csoportoknak felelteti meg az eszköz, és egyezés esetén megteszi a kívánt lépéseket. A Cisco IDS jelenleg több mint 800 signature-rel rendelkezik. Fontos tulajdonsága, hogy mindezt a munkát elvégezve sincsen semmilyen behatással a hálózati forgalomra, számára az IDS láthatatlan marad, és teljesítményét, áteresztő képességét sem csökkenti. Az IDS mellett aktivizálásra került az Allot Netenforcer sávszélesség menedzsment rendszer is, további védelmi eljárások biztosítása érdekében, az Allottal valamennyi hálózati forgalom szabályozható. A rendelkezésre álló kommunikációs vonalakat optimálisan használja ki, priorizál a futtatott alkalmazások között és lehetőséget teremt az URL és tartalomszűrésre, valamint a szokásostól eltérő hálózati forgalmat generáló eszközök (szerverek, munkaállomások – PC-k) felderítésére és a hálózati forgalomból történő kitiltására.



## Elektronikus feladat meghatározó és szöveges üzenetküldési rendszerek

### Marathon

Adatkapcsolatot teremt a minisztérium és valamennyi BM társszerv részére a BM Helyzetelemző és Értékelő Központtal. Aktivizálására országos méretű veszélyhelyzet-kezelés során kerül sor. A BM OKF részéről adatszolgáltatás a Veszélyhelyzet Kezelési Központból történik.

### Calliope

A Calliope a BM vezetői állománya részére, illetve címzetten a társszervek egyes szakterületei (személyügyi és gazdasági terület) között adatkapcsolatot biztosító szoftver.

### Callisto

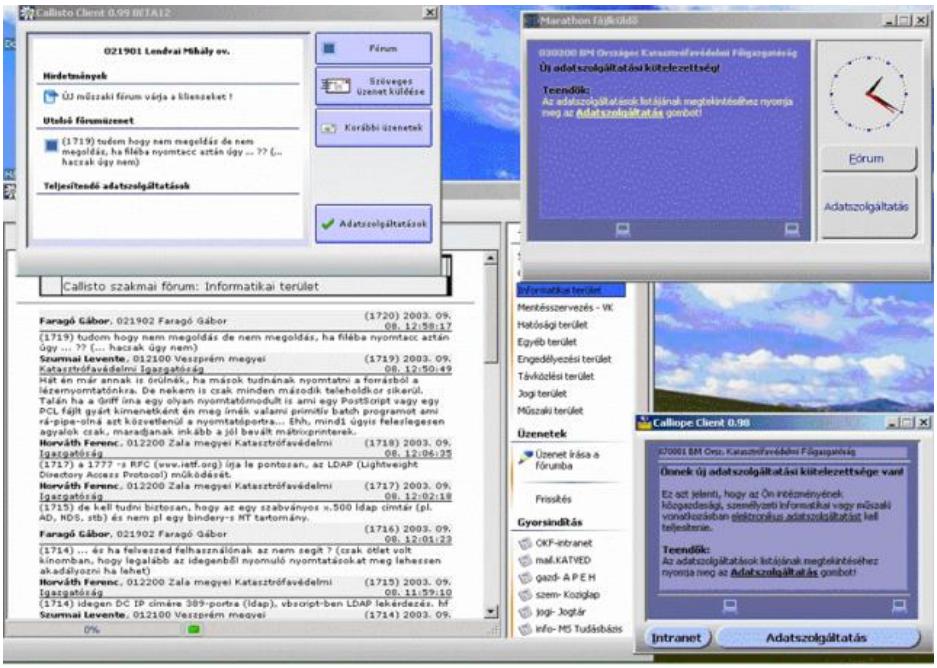
A Calliope és a Marathon szoftverek továbbfejlesztett változata. Irányított feladat meghatározásra, a végrehajtás kontrolljára, továbbá szöveges üzenetküldésre és fájltranszferre alkalmas.

Az IP alapú működést kihasználva a hálózatba kötött személyi számítógépek között a területi elhelyezkedésétől függetlenül (országos szinten) 1-3 perc alatt adatkapcsolat létesít, rajta keresztül üzenetváltás kezdeményezhető, illetve elektronikus úton feladat szabható. Emellett fórumot biztosít szakterületi feladatok hatékony végrehajtására, a felmerült problémák azonnali kezelésére.

A Callisto a BM-ben elfogadott és használt elektronikus feladat-meghatározó rendszerrel teljesen kompatibilis alkalmazás. A program alkalmazása megkönnyíti a BM társszervek irányából jövő adatszolgáltatási kérelem, illetve kötelezettség elektronikus úton történő teljesítését.

A Callisto integrált alkalmazás, a Gyorsindítás menü alól keretet biztosít:

- a Katasztrófavédelmi Információs Honlap,
- a Katasztrófavédelmi WEBMAIL,
- az Adó és Pénzügyi Ellenőrzési Hivatal,
- a BM Közigazgagatásszervezési és Közszolgálati Hivatal,
- az FCROAT-IT (informatikusok részére),
- a NetAkadémia Interaktív Tudástár,
- a Microsoft Magyarország MS Tudázbázis,
- a BM Közgazdasági és Humán Rendszer,
- Scriptum (magyar-angol-német-francia) szótár,
- Térkép – Magyarország,
- CD-Jogtár elérésére és futtatására.




## Levelező rendszerek

### Lotus Notes

A Lotus Notes egy szerver/kliens felépítésű, csoportmunkát támogató, munkafolyamatot figyelemmel kísérni képes zárt levelező és tartalomszolgáltató rendszer.

A központban a Notes szerver áll, melyhez kliensként Notes kliens kapcsolódik. A szerver biztosítja az adatok elérhetőségét a kliensek számára és figyeli a hozzáférési jogosultságokat. A Lotus Notes Domino szerver egyben levelezési rendszer, adatbázis motor, biztonsági rendszer, alkalmazás fejlesztői környezet, hálózatmenedzsment a Notes felhasználók számára, valamint web szerver. Lehetővé teszi a dokumentumok biztonságos tárolását, titkosítását, aláírását, verziók követését, a felhasználók módosítását, ellenőrzését.

Az OKF-en a Lotus Notes elsősorban a vezetők, a vezetői titkárságok és az ügyeletek közötti elektronikus levelezést, illetve dokumentumok küldését biztosítja, valamint csoportmunka támogatási lehetőséget ad. Authentikációs eljárás előzi meg a felhasználói fiók elérését és a szerver-kliens adatbázis szinkronizációját.

### Katasztrófavédelmi WEBMAIL rendszer

A WEB alapú nyílt elektronikus levelezést biztosítja. A WEBMAIL szervert a Rádiós Segélyhívó Országos Egyesület üzemelteti, a szolgáltatás adminisztrátori feladatát az a BM OKF Informatikai és Távközlési Főosztály végzi. Az email fiókok dedikáltan 25 MB-osak, egyébként korlátlan kapacitásúak.




A Lotus Notes-tól eltérően a regisztrált felhasználók a világ bármely pontjáról elérhetik az email fiókjukat SSL kódú titkosítással, autentikációt követően. A regisztrált egyéni felhasználók mellett csoportos (intézményi/szervezeti) email fiókok is működnek. A A Katasztrófavédelmi WEBMAIL szolgáltatás a hagyományos elektronikus levelező rendszer által nyújtotta lehetőségeken túl beépített határidőnaplóval is rendelkezik.

Szervezeti e-mail azonosító:

- ……@katved.hu
- ……@katasztrofavedelem.hu

## Központi szolgáltatások

### Internetes Honlap

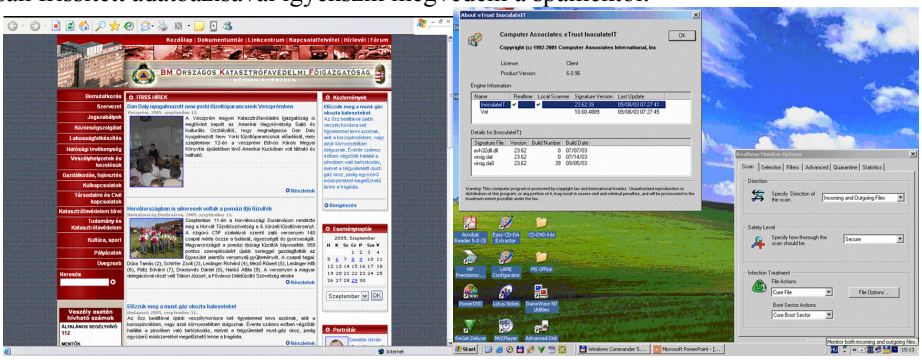
A lakosság tájékoztatásának színvonalasabbá tétele érdekében a belügyi honlapra integrált, a belügyi webmester által karbantartott katasztrófavédelmi weboldal megszűntetésre került és 2003-ban önálló Katasztrófavédelmi Internetes Honlapot hoztunk létre, szerkezeti felépítése, struktúrája, megjelenése (design) véglegesítésre került, az adatokkal történő feltöltése folyamatban van, a fejlesztés során a KIETB 19. sz. ajánlásnak feleltettük meg. Katasztrófavédelmi Portállá fejlesztését követően a jelenleg legszínvonalasabb adatkommunikációs felületet biztosít valamennyi látogató, illetve felhasználó részére. A portál létrehozásával az országos és a regionális katasztrófavédelmi szervezetek és szervek új típusú társadalmi megjelenítésének elősegítését, a szakmai tevékenység új dimenzióinak megteremtését tettük lehetővé az Interneten keresztül. A Portál szolgáltatás igénybe vételével a katasztrófavédelem országos főigazgatósága, a területi szervek, a katasztrófavédelmi szervezetekkel együttműködésben lévő önkormányzatok, karitatív szervezetek, ad-hoc feladatok ellátását végző bizottságok és más közigazgatási szervek vagy a velük kapcsolatban álló szervezetek megtalálják és közzétehetik a tevékenységüket érintő vagy ahhoz szükséges információkat.

## ETRUST Antivírus

A BM OKF-n belül valamennyi felhasználó gépére fel van telepítve, amely a hálózaton lévő gépeket védi a vírusok támadása ellen, valamint a vírusirtó szerver a legújabb antivírus frissítések letöltésével naprakész felügyeletet biztosít a felhasználók részére.

## ETRUST AntiSpam

A nagy mennyiségű kéretlen elektronikus levelek (spamek), tójai és egyéb nem kívánatos alkalmazások, hirdető és felugró ablakok ellen, azok kiszűrésére központi szolgáltatásként került bevezetésre. A tartományba vett valamennyi PC-t automatikusan frissített adatbázisával igyekszik megvédeni a spamektől.



**Dr. habil MEZEY Gyula**

# A KRITIKUS IT INFRASTRUKTÚRA VÉDELMÉRŐL

## A hazai polgári válságkezelésen belül az állami és a magánszféra feladatai

Nem lehet nem figyelembe venni azt, hogy a modern társadalom sebezhetőségét megnövelő szolgáltatások és infrastruktúra gyenge pontjai illetve erősségei nagymértékben a magánszektorban hozott döntések következményei.

Az állami, és magánszektor közötti, az infrastruktúra védelmére vonatkozó munkamegosztásra az USA-ban négy járható utat (modellt) már nemcsak felvázoltak, hanem egyes államokban ezeket ki is próbálták, ezek:81

- Az ún. NICON-modell
- A 'terror-ellenes' modell
- Az ún. CDC-modell (az állam és magánszféra partnersége)
- A 'magánszektor vezetése' modell

Az alábbiakban röviden összevetem a fenti 4 alapmodellt a taktikai jelző-riasztó és válaszreagáló rendszer hatásossága (pl. a reagálás gyorsasága) szempontjából vizsgálva. Megjegyzem, hogy ezek nem egymást kizáró alternatív modellek, divergens fejlődéshez vezető utak, hanem konkrétan mindig valamilyen átmenet, az alapmodellek egy kombinációja jelenik meg a gyakorlatban.

### 1. A NICON modell

Ezt a modellt a nukleáris stratégiai hadviselés USA-beli polgári védelmének régebbi, ún. DEFCON modelljéből vezették le. Eszerint az infrastruktúrát fenyegető veszélyeket jelző és riasztó rendszer tervezésének és kialakításának irányítása az USA védelmi minisztériumának a felelősségi köre.82 A rendszer maga egyébként bármely infrastruktúrának a kormányzat, illetve a magánszektor legkülönbözőbb szervezetei tulajdonában álló hálózataira és elemeire terjed ki.

E rendszer igen lényeges elemei az ún. veszélyhelyzeti válaszreagáló központok.83 A központ állományának egy része köztisztviselő, akik az infrastruktúra védelme végrehajtásának hatósági felügyeletét látják el, másik része a magánszféra által alkalmazott ügyeleti diszpécser, akik a távmérő rendszer jelzései alapján döntenek a szükséges teendőkről (pl. riasztanak). Az információ a közigazgatás hierarchiájában egy szinttel magasabban levő (pl. regionális) adatfúziós elemző központba kerül, amely azért felel, hogy a kritikus infrastruktúrát, vagy folyamatokat érintő szakadásra riasszon.

Habár az infrastruktúra védelmének foka tekintetében az állami felügyelet elvárása és a magánszektor gazdasági érdekei között van eltérés, a döntéshozók emiatti bizonytalanságát egy országos elemző központ hatósági előírásaival (jogszabályok, szabályzatok, válaszreagálási tervek) lecsökkenti.

---

81 R.C.Molander, P.A.Wilson, D.A.Mussington, R.F.Mesic, Strategic Information Warfare Rising,(RAND 1998)

82 DoD Department of Defence USA

83 ERC Emergency Response Center

## 2. A 'terror-ellenes' modell

Ez a közelítésmód azzal a feltételezéssel él, hogy az infrastruktúra veszélyeztetésének kiváltó oka nem egyfajta aszimmetrikus hadviselés - a terroristát nem tekinti hadviselő félnek. Az infrastruktúra rombolását sem az aszimmetrikus hadviselés egy módjának, hanem közönséges bűnténynek minősíti és ebből kiindulva, megoltalmazását elsősorban rendészeti feladatnak tekinti és ezért a titkos-szolgálatok és a rendőrség felelősségi körébe utalja.

A jelző és riasztó rendszer diszpécserei az infrastruktúra professzionális szakemberei, akik egyben hivatásos tisztek. Riasztáskor a készenléti szintet, a kötelező intézkedéseket a hatóság rendeli el. A magánszektor itt adatszolgáltató, amely végrehajtja a központi hatóság által rendelt kötelező biztonsági ellenőrző intézkedéseket (pl. a bankok a pénzmosás tekintetében).

## 3. A CDC-modell

Az állami- és a magánszektor sebezhetőségének csökkentése érdekében a kormányzat katalizátor-hatású koordinációs tevékenységet fejt ki, egyrészt az infrastruktúra gyenge pontjainak feltárására, másrészt a sebezhetőség csökkentésére, végül a hatásosabb válaszreagálásra ösztönzi, mind az állami-, mind a magánszektor egyes szereplőit. A normális működéstől való eltérést felderítő intézkedések nem csak a kritikus, hanem a teljes országos infrastruktúrát célozzák.

Arra, hogy a jelzés-riasztásra, vagy a válaszreagálás, helyreállítás jobbítására mely intézkedések szülessenek, a kormányzat, az egyetemek, és a magánszektor képviselőiből álló testület ad ajánlásokat. A jelzésekre való válaszreagálásról elsősorban az országos lefedettségű infrastruktúra tulajdonosaival állapodnak meg, diszpécsereik ehhez igazodva intézkednek.84 A válaszreagálás céljára a legmagasabb szakmai kompetenciával rendelkező szereplőkhöz telepített regionális veszélyhelyzet-kezelő 'csapatok' - pl. az USÁ-ban az ún. CERT-központok85 az egyetemeken vannak és ezeket a szövetségi kormányzat finanszírozza - végzik. Ezen túlmenően a szakmailag élenjáró szövetséges, illetve nemzetközi szervezetekkel, is minél szorosabb segítségnyújtási együttműködést hoznak létre.86

## 4. A 'magánszektor vezetése' modell

Ez a modell arra az alapfeltételezésre épül, hogy az infrastruktúrát kezelő nagyvállalatok saját érdekükben önként is fellépnek az infrastruktúra megoltalmazása érdekében. Az iparág maga megszervezi ezt a tevékenységet (pl. a vegyipar,87 a tőzsde88az USÁ-ban kialakította az iparág biztonsági szabványait, kockázatelemzési módszereit, sőt ellenőrző szerveit,89az államtól, más nemzetközi szervezetektől pedig

[84] pl. ilyen hazai megoldás az ún. VERIK a Magyar Vegyipari Szövetség ún. Vegyipari Riasztási és Információs Központja.lásd *VERIK Vegyipari Riasztási és Információs Központ, Segítség vegyi anyagok szállítási baleseteinél* (MAVESZ1998)

[85] CERT Computer Emergency Response Team

[86] pl., a WHO, EU, stb.,

[87] VERIK a Magyar Vegyipari Szövetség ún. Vegyipari Riasztási és Információs Központja.lásd *VERIK Vegyipari Riasztási és Információs Központ, Segítség vegyi anyagok szállítási baleseteiné* (MAVESZ1998)

[88] NASDAQ National Association of Securities Dealers

[89] pl. SEC Securities and Exchange Commission

ezután már csak azt várja, hogy ezeket változtatás nélkül fogadja el, esetleg konzultatív (pl. módszertani) támogatást vár.

### Az IT (információ-technológia) infrastruktúrájának egyre növekvő súlya

A szolgáltatások és az infrastruktúra egyre nagyobb része függ az IT-től. Az IT infrastruktúra oltalmát (a védelmi kockázat csökkentését) szolgáló jelző-riasztó és válaszreagáló, helyreállító rendszer szervezeti struktúráját is befolyásolhatja az IT fejlesztésének hazai stratégiája (Nemzeti Információs Társadalom Stratégia), azon belül a HM és a BM, valamint a titkosszolgálatok IT-fejlesztési, és infrastruktúra-fejlesztési stratégiája. Ezek utalnak arra, hogy külső ellenség, vagy belső/esetleg külső ellenfél (pl. terroristák, szervezett bűnözés) elleni védelem céljára milyen képességek, és hol állnak inkább a rendelkezésre, hol van (vagy lesz) a hazai szakmai kompetencia, és annak eléréséhez mely cselekvési változatot választották. Azonban e rengeteg részlet között a 'sok fától' nehéz meglátni 'az erdőt', azaz a feltett védelmi célt.

Véleményem szerint a lehetséges védelmi céljaink:

- A szövetségesek között a vezetési hadviselést (az információs hadviselés katonai változata) magas szinten művelő néhány ország közé kívánunk tartozni.

Ennek a csoportnak a közös célja valószínűleg a vezetési hadviseléstől való kölcsönös elrettentés (mutual deterrence), az elsőként való támadástól való tartózkodás és a csoporton kívüli proliferáció akadályozása, pl. nemzetközi műszaki szabványokkal is.[90]

Nekünk egy ilyen cél azt jelentené, hogy jelentős mértékű közös NATO K+F és hadiipari együttműködésbe kellene invesztálnunk. A fenti jellegű katonai együttműködés vélhetően azt jelentené, hogy nálunk inkább a NICON, vagy a 'terror-ellenes' modell, esetleg a kettő vegyüléke valósulhatna meg.

De vajon reális feltételezésnek tűnik az, hogy hazánkat ilyen szerepre ösztönöznék? Vagy az ország maga ambicionálja ezt a szerepet és tudná is a kutatásokat finanszírozni? Megalapozottan talán egyik sem vélelmezhető, mert ez a 'fegyverkezési' verseny többek között, pl. a rejtjelzés új legkorszerűbb – hálózatvédelmet célzó, illetve a rejtjelfejtés vonatkozó - eljárásait fejlesztené.

- A nem-offenzív információs hadviselést (ez nevével 'hadviselés' ellentétben egyáltalán nem katonai, hanem alapvetően civil tevékenység) magas szinten művelő néhány ország közé akarunk tartozni.

Ennek a csoportnak a közös célja az lehet, hogy a sebezhetőségüket mindahányan csökkentsék, és a támadó beazonosításával, valamint pl. a leszerelés-ellenőrzéshez hasonló nemzetközi szankciókkal a támadástól elrettentsen.

Ez azt jelentené, hogy jelentős mértékű közös, pl. EU IST K+F és információbiztonsági együttműködésbe kellene invesztálnunk.[91] A fenti civil együttműködés vélhetően azt jelentené, hogy nálunk inkább a CDC, vagy a 'terror-ellenes' modell, esetleg a kettő vegyüléke valósulhatna meg. De vajon reális feltételezésnek tűnik az, hogy hazánkat ilyen szerepre ösztönöznék? Vagy az ország maga ambicionálja ezt a szerepet és tudná is a kutatásokat finanszírozni? Az új globális hálózatok (GII) eleve könnyen sebezhetők, az 'e-kormányzás', az 'e-kereskedelem', az 'e-bankrendszer'

[90] Megjegyezzük, hogy az offenzív eszközökről szinte soha, sehol, senki nem beszél

[91] IST Information Society Technology

összeomolhat. Még a bankok információ-biztonsága viszonylag a legerősebb, mert ők ezt képesek finanszírozni.

- A piaci diverzifikáltság 'természetes oltalmában' bizakodunk (és illesztünk, illesztünk, illesztünk…)

Az IT és az információbiztonság termékeinek nemzetközi piacáról vásárolni,92 egyrészt azt jelenti, hogy elfogadjuk az információbiztonság és közvetve az infrastruktúra oltalma tekintetében a mások termékeitől való egyre erősebb függést. Másrészt azonban a diverzifikált, sokirányú függés a katasztrófális hatások terjedésének természetes korlátozása is lehet, illetve reménykedni lehet abban, hogy egyetlen támadó sem képes az infrastruktúra egészére megsemmisítő információs csapást mérni.

Ugyanakkor a mi esetünkben ez azt is jelenthetné, hogy fokozatosan leszakadunk az IT K+F fő vonalától, ami viszont iparunk számára elfogadhatatlan. De tulajdonképpen ez történik ma. Az ország egyszerűen nem tudná kigazdálkodni az információ-biztonság általános magas költségszintjét, következésképpen az infrastruktúra oltalmának magas szintjét sem. Nem is igazán a nemzetállam döntési alternatívájáról, hanem tartós kényszerpályáról van szó.

Kivétel az a néhány 'sziget', ahol az állam és a hazai magánszféra még képes az infrastruktúra védelmébe beruházni. Beruházni viszont a magánszféra nemigen akar majd akkor, ha az EU-ajánlásokon még túlmenő magyar hatósági (vö. ITB-8) szabályozásnak is eleget kellene tenni.93

- Az információs hadviseléssel szembeni sebezhetőség viszonylag alacsony szinten tartása

Ez megvalósítható célnak látszik.

## Megjegyzések és felhasznált irodalom


[1] R.C.Molander, P.A.Wilson, D.A.Mussington, R.F.Mesic, Strategic Information Warfare Rising,(RAND 1998)
[2] DoD Department of Defence USA
[3] ERC Emergency Response Center
[4] pl. ilyen hazai megoldás az ún. VERIK a Magyar Vegyipari Szövetség ún. Vegyipari Riasztási és Információs Központja.lásd VERIK Vegyipari Riasztási és Információs Központ, Segítség vegyi anyagok szállítási baleseteinél (MAVESZ1998)
[5] CERT Computer Emergency Response Team
[6] pl., a WHO, EU, stb.,
[7] VERIK a Magyar Vegyipari Szövetség ún. Vegyipari Riasztási és Információs Központja.lásd VERIK Vegyipari Riasztási és Információs Központ, Segítség vegyi anyagok szállítási baleseteinél (MAVESZ1998)
[8] NASDAQ National Association of Securities Dealers
[9] pl. SEC Securities and Exchange Commission
[10] Megjegyezzük, hogy az offenzív eszközökről szinte soha, sehol, senki nem beszél
[11] IST Information Society Technology
[12] COTS Commercial Off The Shelf
[13] ITB Informatikai Tárcaközi Bizottság


92 COTS Commercial Off The Shelf
93 ITB Informatikai Tárcaközi Bizottság

**Dr. NAGY Tamás**

# A MAGYAR LÉGVÉDELEM INFORMÁCIÓS HÁLÓZATÁNAK JELLEMZŐI 1945 – 1955 KÖZÖTT

## A kommunikációs rendszerek jellemzői a hidegháború kezdeti időszakában

1945-ben véget ért a emberiség eddigi legpusztítóbb háborúja. A harccselekmények befejeztével azonban számtalan olyan kérdés várt megoldásra, amelyben a győztesek ellenérdekeltek voltak. A két szövetséges nagyhatalom a már megszerzett pozíciója birtokában a másiktól várta azokat a gesztusokat, amelyek megadására önmaga nem volt képes. Ennek a folyamatnak az eredményeként fokozatosan nőtt a feszültség a korábbi fegyvertársak között, amely előbb konfrontációhoz, majd később a nyílt katonai szembenálláshoz is elvezetett. Az 1945–1989 között eltelt majd félévszázadot a történeti szakirodalom a Hidegháború időszakának nevezi, amelynek alapvető problematikája a következő volt:

„…az USA attól félt, hogy a szovjetek világhatalomra tesznek szert a jövőben, Moszkvát pedig az aggasztotta, hogy az USA hegemóniája kikezdhetetlen a Földnek azokon a részein, melyeket nem a Vörös Hadsereg foglat el.”94

A háborút győztesen befejező két nagyhatalom rövid idő alatt kiépítette saját érdekszféráját, és tudatosan törekedett annak megvédésére a másikkal szemben.

Az Amerikai Egyesült Államok által ellenőrzött nyugat-európai és a Szovjetunió által kontrolált kelet-európai térségben – végeredményét tekintve – hasonló folyamatok játszódtak le. Mind a két nagyhatalom a vele azonos, vagy legalábbis hasonló nézeteket valló politikai erőket juttatta hatalomra, illetve a saját hatalmi rendszeréhez hasonló helyi változatok kiépülését preferálta. Mindezek eredményeként 1949–1950-reEurópa két olyan egymással ellenséges részre szakadt, amelyek között a kommunikáció csak Washingtonon és Moszkván keresztül valósulhatott meg.

A polgári és katonai információs rendszerek úgy épültek ki kontinensünkön, hogy azok végpontjai a szovjet, illetve az amerikai fővárosban voltak. Így nem csoda, hogy mind a két nagyhatalom elsődleges célja volt, hogy behatoljon a másik fél szigorúan zárt információs rendszerébe, és onnan létfontosságú adatokat szerezzen meg. Ebben az információs harcban a szövetséges kisállamok érdekeit messze háttérbe szorították a nagyhatalmi elvárások. Idővel ugyan ez feszültséget okozott mindkét érdekszférában, de a térséget ellenőrző két nagyhatalom végül is úrrá lett ezeken a nehézségeken. A szovjet és amerikai konfliktus megoldási technikákat alapvetően az adott nagyhatalmak belső hatalmi mechanizmusai, illetve a világról vallott nézeteik határozták meg. Így nem csoda, hogy idővel, hogy az amerikai és a szovjet fél egymástól gyökeresen különböző megoldásokat produkált.

Az információk ebben az időben, első sorban hagyományos eszközökön áramlottak. A földi telepítésű rádióállomások és távvezetékek hálózata biztosította valamennyi állam számára, hogy időben megérkezzenek a létfontosságú információk és utasítások a küldőtől a célállomásig. Így volt ez a korabeli légvédelmi rendszerek-

[94] E.J.Hobsbawm: A szélsőségek kora, A rövid 20. század története 1914—1991. Pannonica Kiadó, kiadási hely és évszám nélkül, 225.o.

ben is. Amíg a hagyományos belsőégésű motorok hajtotta repülő eszközök közlekedtek kizárólag a légtérben, nem is okozott gondot azok mozgásáról szóló információk időbeni célba juttatása. Azonban még ebben a klasszikusnak nevezhető helyzetben is jelentkezhettek problémák. A második világháború időszakában 1940–41-ben lezajlott „Angliai légi csata" példáján kiválóan megfigyelhetőek az információáramlás és az effektív védelmi intézkedések közötti sajátos viszonyrendszer.

Már a második világháború elején valamennyi háborús nagyhatalom rendelkezett napjaink egyik legfontosabb információ szerző eszközével, a radarral. Ezzel a berendezéssel már több mint 100 kilométeres távolságból fel lehetett deríteni a közeledő ellenséges repülőgépeket. A brit légvédelem az angol partvidéken Észak – Dél irányban olyan állandó telepítésű RADAR95 hálózatot hozott létre, amely már kellő információval szolgált a közeledő ellenséges légikötelékekről. A RADAR információk kiegészültek a Brit szigeteken kiépült vizuális rendszertől származó jelentésektől, amelyek együttesen ugyan abba a központba jutottak el, ahol döntöttek a légierő (RAF96) gépeinek bevetéséről. A brit szakemberek ebben a szisztémában olyan sikeresen ötvözték az információgyűjtést a végrehajtás irányításával, hogy a repülőgépek kellő átcsoportosításával adott irányokban, mindig jelentős erőfölényt tudtak elérni a támadó német légierő gépeivel szemben. A brit példában jól látható, hogy mivel az információáramlás sebessége messze meghaladta a céltárgyak sebességét, így a támadó fél eleve hátrányba került védekező féllel szemben.

A technikai fejlődés azonban hamar felborította az információáramlás és a repülőgépek sebessége közötti viszonyrendszert. Már a második világháború végén megjelentek azok a sugárhajtású repülőgépek, amelyek módosították a korábban kialakult egyensúlyt a légierő és a légvédelem között. 1944-ben a világon elsőként Luftwaffe vetett be sugárhajtóművel felszerelt vadászgépeket. A Messerschmitt gyártmányú Me 262 ugyan még csak a hang sebesség alatt tudott repülni, de már jelezte a fejlődés irányát. A második világháború befejeztével ezekből a német gépekből úgy az amerikai, mint a Vörös Hadsereg is elegendő számú darabot szerzett, amelyek megfelelő kiindulási bázisként szolgáltak az új repülőgéptípusok kifejlesztéshez.

## A magyar légvédelmi rendszer jellemzői a második világháborút követő időszakban

Magyarországon a második világháborút követő politikai átrendeződések eredményeként 1948-ra világossá vált, hogy hazánk a szovjetunió érdekszférájának része lesz. Az 1947-es parlamenti választásokat megnyerő Magyar Kommunista Párt 1948 júniusában a Magyar Szociáldemokrata Párttal fúzióra lépve létrehozta a Magyar Dolgozók Pártját (MDP), amely már egyértelműen jelezte a sztálini szovjet modell magyarországi realizálását. Az új párt vezetése elsőrendű feladatának tekintette, hogy Magyarországot a lehető legrövidebb időn belül integrálja a szovjet politikai, gazdasági és nem utolsó sorban katonai rendszerbe.

Ennek a folyamatnak az eredményeként a Magyar Honvédség perifériás helyzete fokozatosan megváltozott az 1948-as politikai fordulat után. A fegyveres erők szerepének felértékelődésével párhuzamosan előtérbe került az ország légvédelmének

[95] RADAR (Radio Detecting and Rainging ) angol betűszó, jelentése, Rádió Figyelő és Jelző Rendszer.

[96] Royal Air Force: Brit Királyi Légierő

megszervezése. 1948 végéig önálló magyar légi felderítés szervezeti keretei nem léteztek. Ennek oka az ország katonapolitikai helyzetében, gazdasági lehetőségeiben és műszaki – technikai adottságaiban keresendők. 1949-ig ugyanis nem létezett „ellenséges" állam Magyarország határai mentén.97

A Magyar Honvédség 1948. október 1-től érvénybe lépő „Pilis-II." hadrendjében először jelenik meg az Országos Légvédelmi Központ (ORLÉKÖZ), amely a Honvédelmi Minisztérium közvetlen alárendeltségébe tartozott. Az ORLÉKÖZ egy légvédelmi rádióbemérő üteg és egy légvédelmi osztály felett diszponált ebben az időben. Az ORLÉKÖZ ekkor kettős funkciót látott el. Egyrészt rendszerezte és értékelte a hozzá beérkező légi információs adatokat, másrészt aktív végrehajtó szervén keresztül - gépvontatású légvédelmi osztály (g.gv.lgv.oszt.) - utasítást adott az esetleges légi ellenség megsemmisítésére. Ez a szervezeti struktúra azonban a következő év tavaszán módosult.

1949. március 16-án életbe lépett a honvédség „Klapka"-hadrendje. Az új szervezeti felállásban az ORLÉKÖZ alárendeltségéből kivették a légvédelmi tüzérséget és így a szervezetnek kizárólagos feladata lett a beérkező légi információk kiértékelése és a Honvéd Vezérkar VII. Alcsoportjának tájékoztatása. Az új feladatok ellátása érdekében két Légvédelmi Központot (LÉKÖZ) állítottak fel a Dunántúlon. Ezzel a lépéssel kezdődtek el az előkészületek egy önálló légvédelem megteremtésére. A LÉKÖZ-ök figyelő őrseiktől érkező információkat miután feldolgozták jelentést tettek az ORLÉKÖZ-nek.

Az 1949. október 1-jén életbe lépő „Petőfi"-hadrend keretében az OLP alárendeltségében működött a légi figyelő- és jelzőrendszer. Ebben a struktúrában az ORLÉKÖZ már négy LÉKÖZ-től összegyűjtött információkat továbbított az OLP felé.98 A rendszer kiépítésénél megfigyelhető, hogy a fő figyelési és felderítési irányt Nyugat és Dél felé határozták meg. A LÉKÖZ-ök közül három a Dunántúlon (Zalaegerszeg, Veszprém, Kaposvár) és egy a Duna-Tisza közén (Kiskunfélegyháza) települt. Az új rendszer kiépítésénél nem mondtak le a határvédelmi szervektől érkező légi információkról sem99, azonban a hangsúlyt alapvetően a felállítandó figyelő őrsökre helyezték. A figyelő őrsökön szolgálatot teljesítő katonák vizuális úton szerezték információikat, amelyeket kiépített telefonvonalakon továbbítottak a LÉKÖZ-eik felé. A jó vizuális felderítés érdekében magasleseket építettek a határ közelében. Az országhatár közelsége azonban sokszor veszélyforrást is rejtett magában. A 2. LÉKÖZ (Zalaegerszeg) 1949-ben kérte az ORLÉKÖZ-től, hogy figyelő őrseit hátrébb telepíthesse a határtól, mert többször is határincidensek fordultak elő, illetve Jugoszláviával szembeni politikai légkör változásával a provokációk megszaporodásától tartottak. A biztonsági szempontok mellett természetesen figyelembe vették a látási és figyelési viszonyokat is.100

---

97 1949-re világossá vált, hogy a Tító vezette Jugoszlávia elutasítja a sztálini szovjet modell adaptálását, és ezért a Szovjetunió vezette szocialista országok tömbje és déli szomszédunk között ellenségessé vált a viszony.

98 Hadtörténeti Levéltár (HL.) Magyar Néphadsereg (MN.) 1949/T. HVK. 4.doboz (dob.) 35000/eln. H.V.K. 5.á. 1949.

99 HL.MN. 1949/T. OLP. 11.dob. 1282/eln.

100 HL.MN. 1949/T. OLP. 10.dob. 1079/eln.

A hírrendszer minősége azonban már ekkor sem felelt meg a kor elvárásainak. A meglévő postai telefon- és telexvonalakat használták, amelyek állapota és sűrűsége idővel egyre inkább elmaradt a kívánatos szinttől. A Honvéd Vezérkar 3.a. osztálya még 1949-ben felmérte a híradó hálózatot és megállapította, hogy a postai telefonvonalakra épített jelentő rendszer nehezen működik, és harci helyzetben megbénulhat. Ezért javasolták a meglévő hálózat átalakítását, illetve újabb híradási rendszer kiépítését, amelynek tervezése ekkor már megkezdődött.101

A meglévő infrastrukturális hiányosságokból adódó problémákat még tovább növelte, a személyi állomány alacsony kiképzettségi szintje. Ezt a tényt megerősítette az 1949. szeptemberében megtartott miniszteri szemle, amely során felmérték a csapatok harcértékét. A szemle tapasztalatait rögzítő jegyzőkönyv arról tanúskodik, hogy a hadseregnél hiányosságok voltak a fegyelemmel, a kiképzettségi szinttel és az anyaggazdálkodással.102

A légvédelem technikai korszerűsítése érdekében megkezdődött a hazai lehetőségek felmérése. 1949. december 22-én a Vezérkar VI. Csoportfőnökségének ülésén meghatározták a légvédelem számára szükséges berendezéseket és azok paramétereit.103 A magyar légvédelem vezetése érzékelve, hogy a vizuális felderítésre épülő felderítési rendszer hatékonysága egyre inkább csökken, halaszthatatlanul szükségesnek tekintette a rádiólokátor állomások üzembe helyezését. Ezzel párhuzamosan a hírrendszer korszerűsítésére is konkrét tervek készültek. Ezek szerint a létrehozandó kommunikációs rendszerben az információk áramlása már nemcsak vertikálisan (alárendelttől elöljáró felé), hanem lehetőség szerint horizontálisan (alárendeltek egymás között) is megvalósult volna.104 Erre egyre inkább szükség is volt, mivel idő közben életbe lépett az 1949. november 25-én Bukarestben megkötött magyar-román katonai egyezmény, amely kölcsönös légvédelmi tájékoztatást – beleértve a diszlokációt is – és a híradás felvételét írta elő a két fél között.105 Hasonló megállapodás jött létre 1950. május 12-én Prágában a csehszlovák féllel is.106 Ezeknek a szerződéseknek az adott különös fontosságot ebben az időben, hogy ekkor Magyarország Tiszától Keletre eső területe feletti légteret nem a magyar légvédelem ellenőrizte, hanem a román és a csehszlovák, mert itt ekkor még nem épült ki a figyelő- és jelzőrendszer.107

1950 tavaszán lépett életbe a Magyar Néphadsereg „Rákóczi”-hadrendje. A légvédelemnél, hasonlóan a szárazföldi csapatokhoz, ekkortól kezdték használni a katonai alakulatok megnevezésére a négy jegyű fedőszámokat.108 1950. november 1-től a Magyar Honvédség ismét újabb szervezeti formát vett fel a „Kossuth”-hadrend keretében. Ebben az új struktúrában került felállításra az 1. LÉKÖZ Budapesten.109 Fontos szervezeti változás volt, hogy az öt légvédelmi központot az ORLÉKÖZ-től áthelyezték az újonnan felállított Légi Figyelő és Jelző Ezred parancsnokság aláren-

101 HL.MN. 1949/T. OLP. 10.dob. 1173/eln.
102 HL.MN. 1949/T. OLP. 10.dob. 1105.
103 HL.MN. 1950/T. OLP. 72.dob. 042/SzT.
104 HL.MN. 1950/T. OLP. 72.dob. 2.cs. 0892.
105 HL.MN. 1950/T. OLP. 72.dob. 024/SzT.
106 HL.MN. 1950/T. OLP. 72.dob. 03027/T.
107 HL.MN. 1950/T. OLP. 75.dob. 0264/SzT.
108 HL.MN. 1950/T. OLP. 72.dob. 01269/SzT. melléklet.
109 HL.MN. 1950/T. OLP. 73.dob. 2.cs. 06735.sz.

deltségébe. Az ORLÉKÖZ ettől kezdve az ezred szakmai tanácsadó feladatait látta el, és hasonlóan a 16. önálló rádiótechnikai osztállyal és az öt LÉKÖZ-zel az ezred alárendeltségében működött. A Légi Figyelő és Jelző Ezred az OLP110 alárendeltségébe tartozott ugyanúgy, mint a légvédelmi tüzér alakulatok.

A lokátorok alkalmazásának még nem volt gyakorlata a légvédelemnél. A kezdeti időkben még nem engedélyezték, hogy a meglévő lokátorok folyamatos üzemben működhessenek. Ezt a magas meghibásodási számmal, az alkatrészek gyors elhasználódásával indokolták. Ezért meghatározták, hogy a berendezéseket csak akkor kapcsolják be, amikor nagyobb légi forgalom tapasztalható az ország légterében és azokra az irányokra figyeljenek, ahol ez a tevékenység zajlik.111 Ezzel a rendelkezéssel az a furcsa helyzet keletkezett, hogy a vizuális figyelési rendszer információit rádiólokátorokkal kontrolálták, és a berendezések biztosította lehetőséget - éjszakai és rossz látási viszonyok közötti felderítést - nem használták ki.

Ezzel a megoldással a légi felderítésnél továbbra is elsőrangú szerep jutott a légi figyelő- és jelzőrendszernek. A rendszer munkájában a katonai vezetés fejlődést tapasztalt ebben az időben. Elrendelték, hogy „a LÉKÖZ-ök kiértékelő tisztjei csak a bejelentett saját gépmozgásokkal nem azonosítható jelentéseket továbbítsák az ORLÉKÖZ-nek”112. A gépek felismerésénél azonban egy sajátos probléma merült fel. A magyar és jugoszláv katonai repülőgépek felségjeleinek ábrája hasonló volt, és csak egy helyen tért el a színezésben. Ezt jelezte az OLP vezetése a Honvédelmi Minisztériumnak, vázolva, hogy milyen problémák adódhatnak:

„... felmerült annak szükségessége, hogy a magyar felségjeleket megváltoztassuk, mert ez kb. 1000 méter magasságban már nem különböztethető meg a jugoszláv felségjelektől és így főleg az O.L.P. figyelő és jelentő szolgálatánál komoly hibákra vezet, ami a déli határunkon lévő feszültséget figyelembe véve súlyos következményekkel járhat”.113 A források szerint be is következett ilyen okból szabálytalan repülés.114

Ebben az időben nem tartoztak az OLP irányítása alá a honi vadászrepülő csapatok, amelyek akkor a Légierő Parancsnokság alárendeltségében működtek. Mai szemmel nézve meglehetősen nehézkesen történt a magyar légtérben zajló repülések irányítása. A figyelőőrsök miután észlelték a saját repülőgépek mozgását a légtérben ezt követően jelentést tettek erről elöljáró légvédelmi központjuknak. Innen a repülőgépekről szóló információ a Légi Figyelő és Jelző Ezreden keresztül az OLP-hez érkezett, ahonnan értesítették a Repülő Parancsnokságot. Miután itt az információt feldolgozták, utasítást adtak annak a repülő hadosztály parancsnokságnak, amelyik alárendelt ezredébe tartozott a gép. Jól látható, hogy a többszörös áttétel mennyire lelassította a légi helyzetről szóló információ sebességét, és a sok áttétel mekkora hibalehetőséget rejtett magában. Ezért fordulhatott elő a későbbiekben, hogy sok szabálytalan (ellenséges) berepülés történt az ország légterébe. Időközben megtörtént a Tökölön települő szovjet légierő parancsnokság és az OLP közötti együttműködés felvétele. Az

110 Országos Légvédelmi Parancsnokság
111 HL.MN. 1950/T. OLP. 75.dob. 02501/OLP. 3.-1950.sz.
112 HL.MN. 1950/T. OLP. 73.dob. 0998/OLP. 3.-1950.sz.
113 HL.MN. 1950/T. OLP. 73/1.dob. 7012.sz.
114 HL.MN. 1950/T. OLP. 75.dob. 02502/OLP. 3.-1950.sz.

OLP parancsnok utasította alárendeltjeit, hogy minden légtérsértést vagy szabálytalan repülést jelezni kell a „Rakéta állomás”-nak Tökölre.115

Az új együttműködési forma életbe lépése után, még bonyolultabb lett a légtér ellenőrzése, mivel most már két légvédelmi központból történt az irányítás. A magyar vizuális felderítő rendszer elavultságát jól tükrözte, amikor sugárhajtású repülőgépet kellett irányítania. „1951. október 25-én a pontatlan rep. bejelentés miatt a Tököli rep. térről szovjet léglökéses vadászok lettek bevetve, melyek szintén nem elég feszesen szabályozott együttműködés miatt a szabálytalanul repülő gép helyett a moszkvai és a pécsi menetrendszerű légi járat repülőgépeit kényszerítették leszállásra.”116

A légi figyelő- és jelzőrendszernél ez nem volt egyedi eset. Előfordult, hogy a kisszámú híradó vonalak telítettsége miatt az információ nem érkezett el a központba és így Magyarország területéről szabadon, minden következmény nélkül repülőgép repülhetett ki.117

A vázolt hibák ellenére azonban a vizuális felderítés 1951-re elérte teljesítőképességének határát. Erről tanúskodik az 1950-51-es kiképzési évről szóló jelentés.

„A kiképzési év kezdetéhez viszonyítva jelző alakulatok az alábbi fejlődést érték el:

- a távbeszélő jelentési átlag 4-5 percről 2, sőt némely esetben még az alá is csökken.
- a rádió jelentés terén a kezdeti 15-20 percről 3-4 percre csökkent a jelentések ideje.”118

A jelentés továbbá 15 külföldi repülőgép berepülésére tesz említést, amelyből 13 esetben jugoszláv, míg kettőben amerikai gép sértette meg a magyar légteret. A magyar légvédelemnek azonban nemcsak a külföldi repülőgépek adták fel a leckét, hanem a hazaiak is. „Népköztársaságunk területe feletti repüléseket szabályozó rendeletet a légierők eleinte nem tartották be. Igen nagy volt a szabálytalan repülések száma, ami azonban javult.”119

A bíztató statisztikák azonban már nem tudták eltakarni a helyzet súlyosbodását. A légvédelmi rendszerben az információk már annyira torzulhattak, hogy 1952. november 28-án a légierő szabályosan bejelentett repülést folytató gépeire az OLP alárendeltségében működő tüzér alakulatok (88.lé.tü.o.) tüzet nyitottak.120 Az incidens során személyi sérülés nem történt és nem keletkezett anyagi kár sem.

1951 folyamán megkezdődtek azok a szervezeti változások, amelyek 1952. október 1-től már új hadrendet eredményeztek. 1951. január 20-án az OLP parancsnoka már új szervezeti megnevezésekről tesz javaslatot a honvédelmi miniszternek.121 Eszerint az ORLÉKÖZ-t beolvasztanák a jelző ezred parancsnokságának állományába. Jelző század megnevezést alkalmaznának a LÉKÖZ helyett, és ennek vezető szerve a századőrs lenne.

---

115 HL.MN. 1950/T. OLP. 75.dob. 05134/OLP. Jelző o.-1950.sz.
116 HL.MN. 1951/T. OLP. 172.dob. 05693/OLP. Jelző o.-1951.sz.
117 HL.MN. 1951/T. OLP. 172.dob. 0285/2.LÉKÖZ.-1951.sz.
118 HL.MN. 1951/T. OLP. 172.dob. 08122/OLP. Titkárság.-1951.sz.
119 U.o.
120 HL.MN. 1951/T. OLP. 181.dob. 09790/T. Jelző o.-1952.sz.
121 HL.MN. 1951/T. OLP. 181.dob. 0451/OLP. Jelző.-1950.sz.

Ugyanebben az évben elkezdődtek a munkálatok a Tiszától Keletre eső területek légvédelmének biztosítására. Debrecenben a 6. és Miskolcon (Lillafüred) a 7. légi figyelő- és jelzőszázadokat kezdték el szervezni. A két újonnan felállítandó század személyi állományának feltöltését későbbre tervezték. Ezért csak a századok vezetései kezdték meg működésüket 1952 tavaszán, de így is elkezdődhetett ezen új alegységek híradó összeköttetésének kiépítése a hozzájuk közel eső szomszédos országokban működő légvédelmi alakulatokkal. Így kívánták tökéletesebbé tenni a légi információk áramlását a térségben.

A honvédség 1952 őszétől életbe lépő szervezetében a repülő alakulatok állományában, a 66. vadászrepülő hadosztály alárendeltségében már megtalálhatóak a MIG-15 típusú sugárhajtású vadászrepülőgépek.122 Az új típusú repülőgépek földi irányításához szükséges rádiólokátorok is megjelentek. A lokátorok által biztosított vadászirányításra már 1952-ben sor került. A lokátorok rendszerbe állítása azt eredményezte, hogy a megnövekedett felderítési távolság mellett, éjszaka és rossz látási viszonyok között is folyamatosan figyelemmel lehetett kísérni a légtérben zajló eseményeket. Ezen berendezések hátránya volt, hogy a kis magasságban repülő célokat nem derítették fel. Ezt a hiányosságot a még működő légi figyelő- és jelző századokkal csökkenteni lehetett. A sugárhajtású repülőgépek elterjedésével a kis magasságban történő repülések száma csökkent, mert igen kockázatos nagy sebességgel a föld közelében repülni. A kis magasságon történő rádiólokációs mező áttörésének elmélete, majd csak bő 30 évvel később a szárnyas (cirkáló) rakéták (robotrepülőgépek) megjelenésével kerül ismét előtérbe.

Összefoglalva elmondható, hogy a légi felderítés rendszere 1952 végére nagyjából kiépült Magyarországon. A döntően vizuális figyelés mellett megjelentek már a rádiólokátorok, bár ezek rendszerbe állított típusai nem a legkorszerűbb technikát képviselték. A légi figyelő- és jelző őrsök három gyűrűt alkotva szerveződtek az országban (országhatár mentén, Budapest körül és a kettő között). Ezen kívül a főbb repülési útvonalak mentén működtek ezek a vizuális felderítési pontok.

Az új típusú repülőgépek megjelenésével párhuzamosan a rádiólokátorok száma is növekedett. Ezáltal ugrásszerűen bővült a légi információk mennyisége, amely továbbításának és feldolgozásának problémáját az elkövetkezendő időszakban kellett megoldani.

## Szervezeti változások a magyar légvédelem rendszerében

1952 áprilisában a Honvéd Vezérkar Szervezési osztálya 0755/1952. számú intézkedésében öt önálló hadműveleti rádiótechnikai század és öt önálló rádiótechnikai szakasz rendszerbe állítását határozta meg.123 1952. október 1-gyel életbe lépő új szervezetben azonban csak három önálló rádiótechnikai század és három önálló rádiótechnikai szakasz kezdte meg a működését. Ezen alakulatoknál 1953 végére összesen 8 darab rádiólokátor állomás üzemelt a tervezett 11-gyel szemben.124 Ráadásul ezek a berendezések már ekkor sem voltak a legkorszerűbbek, hiszen első típusaikat már a II. világháború alatt alkalmazták. A lokátorok rossz technikai állapota ellenére a katonai vezetés azonban ekkor még nem mondhatott le a figyelő rendszerről. A vizuális felde-

[122] HL.MN. 1956/T. MNVK 1.Csfség. 12.dob.
[123] Epresi: 5.o.
[124] HL.MN. 1953/T. H.lé.fi.je.e.pság. 535.dob. 0901. Kimutatás.

rítést folytató figyelő őrsök munkája ekkor már nem felelt meg a megváltozott körülményeknek. Az illetékes szovjet katonai tanácsadó erről 1953-ban jelentést is tett Kána Lőrinc vezérőrnagynak, aki ekkor a Magyar Néphadsereg légvédelmi parancsnoka volt.125 A szovjet tanácsadó a vázolt problémák mellett felhívta a magyar vezetés figyelmét, hogy az ország légvédelmének biztosítása érdekében elengedhetetlenül fontos fenntartani a kölcsönös információs hálót a magyar és a Magyarországon települt szovjet légierő között.

A tanácsadó észrevételeivel egybe csengett az 1953. május 9-én megtartott komplex gyakorlat tapasztalatai, amikor tesztelték az új légvédelmi felderítő rendszert, és megvizsgálták, hogy a rádiólokátorokkal együtt milyen hatékonyságú munkára képes. A gyakorlat során, ugyanazon útvonalon először egy darab, majd 15 perc múlva két darab LI-2 gép repült. A tapasztalatok azt mutatták, hogy a felderítő rendszer (lokátorok + vizuális figyelés) 60-70 %-os hatásfokkal képes működni. A meglévő helyzetet csak rontotta, hogy a rendszer irányításában az 1. honi légi figyelő- és jelző ezred főőrsénél komoly hibák mutatkoztak.

„A Főőrs munkájában komoly hiányosság volt az, hogy a diszpécserek hanyag munkája következtében a célokat nem tudták azonosítani, és így a gépek 32! percig repültek az ország légterében tisztázatlan légi helyzetben.”126

1953 tavaszán ugyancsak miniszteri szemle során ellenőrizték a légvédelem aktív elemét képező légvédelmi tüzérséget.

„ A honi lgv.tü.csap-ok az idén 48 %-ban kerültek ellenőrzésre. Az eredmények így alakultak: 23 % jó, 59 % megfelelő és 18 % nem megfelelő.”127

Ezek a tapasztalatok is azt mutatták, hogy az elért fejlődés ellenére nagyobb figyelmet és több pénzt kellett fordítani a légvédelem fejlesztésére. 1953 őszén a Vezérkar összefoglaló jelentést készített, amely szerint a légvédelem a szükséges tiszti állomány 93,6 %-ával és a tiszthelyettesi állomány 39,4 %-ával rendelkezett. A kimutatás szerint a repülő alakulatoknál valamelyest kedvezőtlenebb volt a helyzet. A tiszti állomány 70,3 %-ában, míg a tiszthelyettesi 38,6 %-ában volt feltöltve. Ezzel szemben a repülőgépek számát tekintve kedvezőbb volt a helyzet. A szükséges vadászrepülőgépek 93 %-a, a csatarepülőgépek 98 %-a és a bombázó repülőgépek 100 %-a állt rendelkezésre.128

Az ismertetett tapasztalatok is nagymértékben hozzájárultak, hogy az OLP vezetése javaslatot tett a magyar katonai vezetésnek a légvédelmi rendszer nagyléptékű fejlesztésére és korszerűsítésére. Eszerint a főváros légvédelmének biztosítására:

„Felállítani tervezünk:

- a.) Budapesten egy lgv.tü.hdt.pság-ot,
- b.) Budapesten egy lgv.tü.ho.pság-ot,
- c.) Budapesten egy köz.lgv.tü.e-t”129

Ez a javaslat a légvédelem aktív elemét 29 ponton tervezte módosítani.130

125 HL.MN. 1953/T. OLP. 92.dob. 002429/1953.sz.
126 HL.MN. 1953/T. H.lé.fi.je.e.pság 534.dob. 1.cs. OLPk. 069.sz. parancsa.
127 HL.MN. 1953/T. MNVK Titkárság 4.dob. 2.cs.
128 HL.MN. 1954/T. MNVK Hdm.Csf. 8.dob. 1.cs. Összefoglaló jelentés.
129 HL.MN. 1953/T. OLP. 92.dob. 09727/1953.sz.
130 U.o.

1953 őszén Kána Lőrinc vezérőrnagy az OLP parancsnoka tájékoztatta a honvédelmi minisztert a légi figyelő- és jelzőrendszer helyzetéről.131 Eszerint a rendszer harckészültségében 1953 október második felében visszaesés volt tapasztalható. A jelentés szerint többször nem észleltek célokat, vagy ha igen, akkor összekeverték azokat. Pontatlanok voltak a jelentésadások, amelyekhez a hadműveleti vezetés kiértékelő munkájának alacsony színvonala társult. Sajátosan szubjektív elemet is tartalmaz ez a dokumentum, mely szerint a jelző ezrednél nagy megelégedettség volt tapasztalható. A tények ismeretében ez kissé meglepőnek tűnik. A jelentés a visszaesés okaként továbbiakban még megemlíti:

„Rátértünk az új jelzőrendszerre, azonban ekkor még nincsenek meg a rád.technikai műszerek. Így hézagos ez a rendszer. Előfordulhatnak belső célok, amelyet egyáltalán a rendszer nem tud észlelni."132

Az OLP parancsnoka hasonló tartalmú beszédet mondott 1953. november 12-én a magasabb parancsnoki értekezleten. Az itt elmondottakban külön felhívta a figyelmet, hogy 1953. november 5-én egy Jugoszlávia felől érkező repülőgép, amely megsértette a magyar légteret a vizuális figyelési rendszer pontatlansága miatt szabadon repülhetett a légtérben, és büntetlenül el is hagyhatta azt.133

A légvédelem parancsnokának helyzetértékelésével némileg ellentmond a Vezérkar Hadműveleti Csoportfőnökségén (VK. Hdm. Csfség) készített összefoglaló jelentés az 1953. évi légi tevékenységről. „A légi határsértések száma 1952-höz viszonyítva az 1953-as évben kb. egyharmadára csökkent.

A légi határsértések száma:

- 1951-ben 16
- 1952-ben 42
- 1953-ban 13

Tehát 1952-ben a légi határsértések száma erősen emelkedett, 1953-ban viszont erősen (!) csökkent."134

A továbbiakban ez olvasható: „A berepülések számának csökkenéséből arra lehet következtetni, hogy a figyelő és jelző, valamint a RT. rendszerben és a Le. harckészültségében fejlődés állt be az elmúlt évhez viszonyítva. Nagymértékben hozzájárult a légi provokációk csökkentéséhez a lefolytatott magyar-jugoszláv tárgyalás és a béketábor országainak erősödése következtében a nemzetközi helyzet feszültségében beállt viszonylagos enyhülés is."135

A Vezérkar anyaga szerint a légvédelemnek az országon belüli szabálytalan repülések igencsak feladták a leckét. Az 1953. évben összesen 241 szabálytalan repülés történt, amelyből a magyar légierő részéről 131, míg a szovjet légierő részéről 110 esetet regisztráltak."136

Az OLP parancsnoka által az 1953/54. kiképzési évre kiadott a 001. sz. utasításában a légi figyelő- és jelző rendszer minden elemének meghatározta az elérendő célt.

131 HL.MN. 1953/T. OLP. 92.dob. 004144/1953.sz.
132 U.o.
133 HL.MN. 1953/T. OLP. 92.dob. 003791.sz.
134 HL.MN. 1954/T. MNVK Hdm.Csf. 8.dob. 2.cs. 00198/1954.sz.
135 U.o.
136 U.o.

A rádiótecnikai őrsöknek:

- 3 nagysebességű cél folyamatos követése,
- azokról tájékoztatás,
- vadászok rávezetése az ellenséges célokra,

Rádiótecnikai századőrsök:

- 6-8 nagysebességű cél repülése esetén a légi helyzet folyamatos kiértékelése
- erről időben és pontosan tájékoztatni
- együttműködés a rádiótechnikai őrsökkel, a vadász, a légvédelmi tüzér és légoltalmi szervekkel
- saját repülések pontos nyilvántartása és erről tájékoztatás

Főőrs:

- 6-8 nagysebességű cél légtérben tartózkodása esetén irányítsa a rádiótechnikai őrsök munkáját és tájékoztasson a saját vadászok helyzetéről

Az intézkedés a légvédelmi tüzér alakulatoknak előírja, hogy a vadászerőkkel és a légi figyelő- és jelző szolgálattal együttműködve legyen képes megsemmisíteni a nagymagasságban, nagysebességgel repülő légi célokat.137

A kitűzött célok megvalósításához halaszthatatlanná vált az OLP hírrendszerének korszerűsítése. A gyengén fejlett infrastruktúra már nem tudta biztosítani a megnövekedett információs forgalmat, az alárendeltek irányítását. Ezért a Vezérkar Hadműveleti Csoportfőnöksége (VK.Hdm.Csf.) intézkedett, hogy az alapvetően fontos kábel és rádióalkatrész hiány ne akadályozza a működést.138 Erre a lépésre különösen nagy szükség volt, mert ez év őszén bekapcsolták a honi légvédelmi rendszerbe a kivonuló figyelő- és jelző rendszer alakulatait. Ezeknek a mobil alegységeknek a szárazföldi csapatok légvédelmét kellett biztosítaniuk. A kivonuló légi figyelő- és jelző alakulatok az illetékes szárazföldi magasabb egységek alárendeltségében maradtak, de a szakmai irányításukat az OLP figyelő- és jelző ezrede látta el.139 Így békeidőben biztosítottá vált a kivonuló alakulatok gyakoroltatása és szakmai ismereteinek korszerűsítése. Természetesen bekapcsolásukkal a honi légvédelmi rendszer is nyert, mert újabb információs forrásokkal bővült.

1954 szeptemberében a VK.Hdm.Csfség. elkészítette a néphadsereg 6 éves perspektivikus átszervezésének tervét. A terv elkészítői a korábbi évek tapasztalatait levonva:

„...a légvédelem szempontjából döntő jelentőségűvé vált a felderítés, elsősorban a nagyhatású lokátorok használata...”140

Ugyancsak a kor színvonalának megfelelő tűzvezető lokátorokkal kívánták felszerelni a légvédelmi tüzérséget, ahol korszerűbb, nagy hatótávolságú lövegek rendszerbe állítását tervezték.141 Ez a dokumentum jól tükrözi azt a hangsúly eltolódást, amely a katonai vezetésben bekövetkezett:

„Hazánk védelmi képességének fokozása és a hadsereg harckészségének fenntartása elsősorban is a légvédelem és a légierő korszerűsítését követeli meg...”142

137 HL.MN. 1953/T. MNVK Titkárság 4.dob 1.cs. 001.sz. OLPk utasítás.
138 HL.MN. 1954/T. MNVK Hdm.Csf. 8.dob. 1.cs. 0484.sz.
139 HL.MN. 1954/T. MNVK Hdm.Csf. 8.dob. 1.cs. 01600.sz.
140 HL.MN. 1955/T. MNVK Hdm.Csf. 8.dob. 1.cs. 04739.sz.
141 U.o.
142 U.o.

Ebben az időben jelentős változások zajlottak le a Magyar Néphadseregen belül, hiszen ekkor kezdődött el a szárazföldi csapatok létszámának drasztikus csökkentése. A légvédelem alakulatait azonban ez a folyamat nem érintette lényegesen. Még 1954-ben megkezdődött a légi figyelő- és jelzőrendszer elemeinek felszámolása a Dunántúlon, de ez nem a létszámcsökkentéssel volt összefüggésben, hanem a rádiótechnikai rendszer kiépítésével állt összhangban.

## Kommunikációs zavarok a magyar légvédelemben

1955 a magyar légvédelemben a fordulat évének tekinthető. A korábban vázolt hiányosságok, a rendszer elavultságából fakadó zavarok ebben az évben robbanásszerűen törtek a felszínre. Ez év tavaszán történt események felhívták az ország politikai és katonai vezetésének figyelmét a légvédelmi rendszer működési zavaraira.

„1955. március 28-ra virradó éjjel egy nagy magasságban repülő gyors, ellenséges repülőgép hazánk határait megsértve, nyugat-keleti irányban átrepülte az ország légterét és 37 perc múlva büntetlenül távozott."143

A történtek fontossága akkor érthető meg igazán, ha figyelembe vesszük, hogy ekkor a NATO arzenáljában már nagy mennyiségben rendelkezésre álltak atomfegyverek és azokat nagy célba juttatni képes hordozó eszközök (bombázó repülőgép). Mindezek alapján a magyar katonai vezetés lépéskényszerbe került. Most már elengedhetetlenül szükségessé vált az ország légvédelmi rendszerének átalakítása. Ezért Bata István honvédelmi miniszter, aki az 1940-es évek végén még a magyar légvédelmet irányította, kiadta a 007. számú tisztiparancsot, amelyben az esemény bekövetkeztének egyik fontos okát személyi mulasztásokban vélte felfedezni. Nem csoda, ha ezt követően szigorú felelősségre vonás következett. A honvédelmi miniszter a szolgálat hanyag ellátásáért megrovással fenyítette az OLP és a Le. teljes vezető állományát, valamint elrendelte 13 személy lefokozását, és alacsonyabb beosztásba helyezését. Megállapítható, hogy főleg azok a tisztek lettek elmarasztalva, akik az esemény idején a harcálláspontokon szolgálatot láttak el. A honvédelmi miniszter ezért jelentős szervezeti változásokat rendelt el.

„Az országos légvédelem harckészültségének gyökeres megjavítása és a rendszeren belüli együttműködés megszilárdítása végett a honi légvédelmet és a Magyar Néphadsereg légierőit az Országos Légvédelmi Parancsnokság /:O.L.P.:/ alatt egyesítem. Az országos légvédelmi parancsnok teendői ellátásával további intézkedésig Hazai Jenő vezérőrnagyot - eddigi munkaköre alóli ideiglenes felmentése mellett - azonnali hatállyal megbízom."144

Ezzel a döntéssel Magyarországon is egyközpontú irányítás alá kerültek a légvédelmet biztosító erők, és ekkor vált összfegyvernemi haderőnemmé a honi légvédelem, valamint elkezdődhetett a légvédelmi információs rendszer korszerűsítése is:

„Az országos légvédelem parancsnoka 1955. május 15-ig tegyen javaslatot a légvédelmi figyelő- és jelző szolgálat összevonására két légvédelmi figyelő- és jelző ezredbe és a 25. és a 66. vadászrepülő hadosztályokkal közös harcálláspontok megszervezésére."145

143 HL.MN. 1955/T. HM. Titkárság 3.dob. 1.cs. MN. HM. 007.sz.tiszti (ti.) parancs (pcs.)
144 U.o.
145 U.o.

A parancs a továbbiakban elrendelte a légvédelmi tüzér egységek új diszlokációjának kidolgozását, a légvédelemnek szükséges infrastrukturális fejlesztési tervek elkészítését, valamint intézkedett a légvédelmi alakulatok személyi állományának átvizsgálásáról.

Még el sem csitultak a március 28-i berepülés keltette hullámok, amikor rövid időn belül ismét működésképtelenségről tett tanúbizonyságot a magyar légvédelem.

„1955. május 1-re virradó éjjel egy alacsonyan szálló ellenséges motoros repülőgép DÉL-ÉSZAKI irányban átrepülte hazánk Déli határát és elérte Sztálinvárost, ahol szárnyával az egyik magasfeszültségű vezeték tartó oszlopába ütközve megsérült, majd visszafordult és büntetlenül elhagyta hazánk légterét. Útközben népi demokráciánkat becsmérlő röpcédulákat szórt. ”146

Ez a két esemény érzékeny csapást mért a honi légvédelmi rendszerre. Bebizonyosodott, hogy a fokozatosan kiépített légvédelmi hálón oly nagyok voltak a lyukak, hogy azon szabad volt a ki- és bejárás.

Néhány nappal az esemény után május 6-án a VK.Hdm.Csfség. elkészítette helyzetértékelését a vezérkari főnöknek:

„Problémák a lgv. területén és a VK.Lgv.alo-nál”.147

Ebben az elemzésben a légvédelmi rendszer valamennyi eleméről lesújtó vélemény tárul az olvasó szeme elé:

„1.) A figyelő- és jelző rendszer még nem képes a légi helyzet állandó folyamatos és megbízható nyilvántartására.

- a nagy magasságban, nagy sebességgel repülő célokról a RT-őrsök nem tudnak folyamatos jelentéseket adni.
- a figyelő- és jelzőrendszer jelenlegi szubjektív és objektív eszközeinek alkalmazása mellett nincs biztosítva az alacsony és kis magasságban repülő célok idejében történő felderítése és megbízható megfigyelése.
- Az OLLEP. nem rendelkezik megfelelő számú és minőségű harcirepülőgép vezetővel...
- A honi és kivonuló lgv.tü. mai technikai eszközeivel rossz látási viszonyok között (éjjel és felhős időben) nem képes légi célok lövésére (Nincs ellátva tüzér lokátorral).”148

A jelentés a továbbiakban szól a személyi állomány alacsony kiképzettségéről és új szervezeti struktúra beállításának szükségességéről. A történtek valóban sokkoló hatással lehettek a magyar politikai vezetésre, amit jól tükröz az MDP Politikai Bizottságának a történtekkel foglalkozó határozati javaslata is. A javaslatban a vezérkari elemzéshez hasonló következtetések figyelhetők meg. Ennél azonban lényegesebb, hogy az ország politikai vezetése az események hatására biztosította a légvédelem korszerűsítéséhez szükséges anyagi eszközöket.149

A megtörtént eseményeket elemezve elmondható, hogy az OLP vezetése tisztában volt a légvédelem hiányosságaival és arról folyamatosan tájékoztatta a katonai felső vezetést. Ennek a két rendkívüli eseménynek kellett bekövetkeznie ahhoz, hogy valóban megkezdődhessen a haderőnem korszerűsítési folyamata. Természetesen a

146 HL.MN. 1955/T. HM. Titkárság 3.dob. 1.cs. MN. HM. 015.sz.ti.pcs.
147 HL.MN. 1955/T. MNVK Hdm.Csfség 3/a.dob. 1.cs.
148 U.o.
149 HL.MN. 1956/T. OLLEP. 40.dob. 2.cs. 01978/1955.sz.

vezetők is felelősek a történtekért, hiszen a légvédelem emberi oldala is hibázott. Érdekesen változott a történések hatására a VK. Hdm. Csfség álláspontja. Amíg az 1953-as évről készített elemzésük pozitívan szól a légvédelemről, addig az 1955. év közepének álláspontja, már gyökeresen eltér a korábbitól. Különösen furcsa ez a változás, ha figyelembe vesszük, hogy a légvédelemben ekkor már több lokátor működését és hatékonyabbá is vált a légi figyelés, legalábbis a fennmaradt dokumentumok tanúsága szerint.

1955 nyarán a honi légvédelmi tüzér magasabb egységek és egységek részére meghatározták az új harcfeladatot. Kijelölték számukra, hogy a kulcsfontosságú közigazgatási-, ipari-, katonai objektumokat és közlekedési csomópontokat mely alakulataiknak kell oltalmazniuk.150 Ennek megfelelően meghatározták az új hadműveleti feladatokat151 és elkészült az új diszlokációs intézkedés is.152

1955. október 1-től ismét új szervezeti struktúrában működött a légvédelem. A struktúra megfelelt a honvédelmi miniszter 067.sz. parancsában meghatározottaknak. Az Országos Légvédelmi és Légierő Parancsnokság (OLLEP) alárendeltségében működő két önálló rádiótechnikai jelző ezred központja, már együtt települt a két vadászrepülő hadosztály parancsnokságával. Az önálló rádiótechnikai jelző ezredek századaitól származó légi információk sokkal rövidebb idő alatt eljutottak a végrehajtókhoz, és ami lényeges, hogy egy kézben összpontosult a magyar légvédelem irányítása. Az új szervezeti keretek között már megtalálhatóak a korábbi lokátoroknál korszerűbb típusok is, amelyeket már a keleti országrészben működő rádiótechnikai századok is használtak.153

## Összegzett tapasztalatok

A felvázolt események fontos és hasznos tanulságokkal szolgálnak napjaink kommunikációs és légvédelmi szakemberei számára. Minden hozzáértő számára könnyen megérthető a korszak egyik alapvető ellentmondása, amely a gyorsan fejlődő haditechnika és annak hatékony alkalmazása között húzódott. Hiába fordított a korabeli magyar katonai vezetés horribilis összegeket az ország légvédelmének kiépítésére, ha a rendelkezésére álló légvédelmi technika és az információáramlást biztosító egykori vezetékes- és rádió hálózatok szűk áteresztő képessége nem volt összemérhető egy esetleges támadó ellenséges repülőgép sebességével. A korszak politikai viszonyiból és katonai vezetés rendszeréből következően a hatékony visszacsatolás, a rendszerek korszerűsítésének lehetősége eleve a minimálisra voltak redukálva.

A kialakult helyzeten majd csak az 1955. május 14-én létrehozott Varsói Szerződés Szervezete (VSZ) változtatott, amikor is ebben a Szovjetunió vezette katona-politikai szövetségben elsődlegesen fontos céllá vált az egységes légvédelmi háló létrehozása. A VSZ államok közös légvédelmi rendszerének alapját az az egyesített információs hálózat biztosította, amelyben már a légtérben lezajló információk is nagy sebességgel áramlottak a tagországok között. A technikai korszerűsítések eredményeként az 1970-es évekre már a VSZ információs rendszerében közel valósidejű információk áramlottak, amely fenntartásában nagy szerep hárult az egyre fejlő automati-

150 HL.MN. 1956/T. OLLEP. 40.dob. 2.cs. 00907/1955.sz.
151 HL.MN. 1956/T. OLLEP. 40.dob. 2.cs.
152 HL.MN. 1955/T. MNVK Hdm.Csfség 3/a.dob. 2.cs. 00974/1955.sz.
153 HL.MN. 1956/T. OLLEP. 40.dob. 2.cs. 00779/1955.sz.

zált adatfeldolgozó rendszerekre. A számítógépek elterjedése, a z egyre korszerűbb rádiólokátorok rendszerbeállítása min-mind hozzájárultak ahhoz, hogy a légvédelem aktív elemei mindig pontos információkkal rendelkezhessenek, feladataik teljesítése érdekében. Természetesen ahol emberek dolgoznak, ott számtalan hiba is jelentkezik, de az informatika térnyerésével egyre inkább csökkenthető azoknak a zavaroknak a száma, amelyek elődeink munkáját oly sokszor megnehezítették.

Napjainkban, mikor hazánk az Észak – atlanti Szerződés Szervezetének Tagja, ismét hasonló problematikákkal kell szembenéznünk. Az előre nem kalkulálható műszaki problémák okozta nehézségeket tovább fokozhatják, a váratlan terrorista támadások. Ezért a jövőben elsődleges feladatunk, hogy kommunikációs rendszerünk működő képességét a rendelkezésünkre álló valamennyi eszközzel, minden körülmények között fenntartsuk. Civilizációnk alapjait védjük, amikor biztosítjuk információs rendszerünk működését. Nem szabad elfelejtenünk az ősi mondást:

**Az információ hatalom!**

**NÉMETH András**

# MOBILTELEFON HÁLÓZATOK ALKALMAZÁSA A KATASZTRÓFAVÉDELMI KOMMUNIKÁCIÓ TERÜLETÉN

A háború első áldozata az igazság,
a katasztrófáé a kommunikáció

## Bevezetés

A XX. század a technikai fejlődés mellett a téves ideológiák szülte véres háborúk százada volt, amely után az emberiség azzal az egyetemes óhajjal tekintett az új évszázad és egyben a III. évezred elé, hogy az hozza meg a békét és nyugalmat a Föld minden polgára számára. Sajnos azonban megint akadtak olyanok, – mint annyiszor a történelem folyamán - akik úgy érezték, joguk van élet és halál fölött dönteniük. 2001. szeptember 11.-e alapjában rengette meg a biztonságba és békébe vetett hitet. Azon a napon több ezren lelték halálukat a World Trade Center két tornya és a Pentagon romjai alatt, valamint a Pennsylvaniában lezuhant utasszállító roncsai közt. (Csak az utasok példaértékű magatartásának köszönhető, hogy ez utóbbi esetben a terroristák nem tudták épületnek kormányozni az utasszállító gépet…) Az Al-Kaida terrorszervezet véres akciójára válaszul az Egyesült Államok és szövetségesei megtámadták Afganisztánt és a helyi ellenzéki erők segítségével megbuktatták a nyugati szemmel nézve illegitim, terrorizmust támogató tálib kormányát…

A különböző eszközökkel végrehajtott, a civilizált Világ ellen irányuló terrorcselekmények azonban folytatódtak, ami arra késztette az amerikai kormányzatot, hogy újabb bűnbakot találjon. Irak koalíciós megszállását követően sorra érkeztek az akcióban résztvevő országoknak szóló fenyegetések, nem kevés munkát adva a titkosszolgálatoknak és más biztonsági szerveknek, rettegésben tartva a polgári lakósságot. A XXI. századi terrortörténet új szakaszába érkezett, amikor 2004. március 11-én pontosan 911 nappal az ikertornyok összeomlása után (09. 11.), az Al-Kaida Európában is letette névjegyét. Madridban tíz pokolgép robbant három különböző pályaudvaron 191 halálos áldozatot követelve (1899 sebesült)...

2005. július 7-én biztossá vált, hogy az idein év sem telik el hasonló akció nélkül, hiszen London félelme is beigazolódott. Egymás után négy pokolgép robbant a metróhálózatban és egy buszon több mint 50 emberéletet oltva ki.[154] (A sebesültek száma meghaladta a 700-at.) A hatóságokat azonban nem értre teljesen felkészületlenül a támadás, így a mentés a körülményekhez képest szervezetten történhetett, nem utolsó sorban az Egyesült Királyság hatóságai részére biztosított fejlett kommunikációs rendszereknek köszönhetően.

A terrorizmus elleni védekezés mellett azonban, egyre jelentősebb erőfeszítéseket követel a nemzeti kormányzatoktól, nemzetközi szervezetektől, különböző hatóságoktól a természeti katasztrófák és azok hatásai elleni egyre gyakoribb fellépés.

[154] 2005. június 21-én az előzőhöz hasonló merényletkísérleteket hajtottak végre, ám azok áldozatokat nem követeltek.

(Emlékezzünk csak a 2004. december 26.-án pusztító délkelet-ázsiai szökőár több mint negyedmillió áldozatára!)

De beszéljünk akár természeti, akár civilizációs katasztrófákról, az ellenük való védekezés, a károk enyhítése, felszámolása, az emberáldozatok mérséklése, egyszóval a katasztrófavédelem komplex és bonyolult feladat, széleskörű összefogást követel a társadalom minden szereplőjétől. Ezek a jelenségek gyakran határokon is átnyúlva fejtik ki káros hatásukat, így az ellenük való védekezésben szükség van átfogó kooperatív és gyakorlati nemzetközi együttműködésre is...

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 elhúzódó védekezési műveletek esetén is képes biztosítani egységei számára az utánpótlást (pl.: nagy kiterjedésű erdőtüzek, tiszai árvizek, hó okozta rendkívüli helyzetek stb.).

A katasztrófavédelemben, mint komplex rendszerben, melynek elemei 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 szervekkel. Az ilyen hírközlő rendszerek esetében, alapvető követelmény az állandó, megbízható rendelkezésre állás, valamint a biztonságos együttműködési képesség (kompatibilitás). [4]

Cikkemben olyan megoldásra kívánom felhívni a figyelmet, mely már a világ több országában is üzemel, és amelynek működését az Egyesült Királyság példáján kísérelek meg bemutatni.

## „Mobilcsend” Londonban

A 2005. július 7.-i robbantások után a brit főváros teljes mobilhálózata megbénult, ami kétféleképpen magyarázható:

1. A mobil hálózatokat (mint minden távközlő hálózatot) különböző forgalmi modellek alapján tervezik meghatározott áteresztő képességűre (egyidejűleg létesíthető összeköttetések száma), előre meghatározott mértékű tartalékolás mellett. A hálózat rendeltetésszerű üzeme mellet előfordulnak azonban igénybevételi csúcsok, melyek meghaladják annak rendszertechnikai (technológiai) képességit, azaz a rendszer egyszerűen összeomolhat. Vannak olyan naptárilag előre meghatározható időszakok, amikor ezzel a jelenséggel nagy biztonsággal számolni lehet, ugyanakkor vannak helyzetek, amelyek előre legfeljebb maximális bizonytalansággal tervezhetők. Előbbire példa az Újév beköszönte, amikor mindenki egyszerre szeretné tolmácsolni jókívánságait szeretteinek, barátainak, ismerőseinek. Utóbbi eset jellemzően olyan váratlan, nagy tömegeket érintő események bekövetkezte után kialakuló információs „vákuum”

eredménye, mint a terrorcselekmények, ipari balesetek, vagy természeti katasztrófák, amikor mindenki a fenti célcsoport biztonságáról kíván a lehető legrövidebb időn belül meggyőződni, vagy segítséget kérni. (Július 7.-vel kapcsolatban értelemszerűen ez utóbbi jöhet szóba.)

2. Számos ország, így Nagy Britannia és Magyarország cselekvési tervei is számolnak a mobil hálózatok szolgáltatásainak részleges vagy teljes felfüggesztésével.155 Többen úgy látják, a júliusi robbantások után ezen felhatalmazások alapján szándékosan, biztonsági okokból állították le a londoni mobilhálózatot, elsősorban azért, hogy mobiltelefonos távirányítással ne lehessen több pokolgépet robbantani.

„Mobilcsend" Magyarországon?

A jogszabályok értelmében a hatóságoknak Magyarországon is lehetőségük van, hogy az ország honvédelmi, nemzetbiztonsági, gazdasági és közbiztonsági (terrorelhárítás és a kábítószer-kereskedelem elleni küzdelem támogatása) érdekében elrendeljék a mobilszolgáltatás szüneteltetését. Ez a jelenlegi gyakorlat alapján egy esetleges terrortámadás vagy katasztrófa esetén komoly fennakadásokat okozhat a mentésben résztvevő szervek tevékenységének koordinálásában, mert a rendőrség, a mentőszolgálat a katasztrófavédelem stb. vezetői is döntően mobiltelefonon tudnak kapcsolatot tartani egymással és beosztottaikkal. A rendőrségi rádiók ugyan a mobilcsend ideje alatt is zavartalanul működnek, azonban azokkal csak a híváskörzetükön belül tartózkodó, azonos forgalmi rendszert használó felhasználók érhetők el. A mentők, rendőrség, tűzoltóság, katasztrófavédelem, határőrség és a mentésre, kárelhárításra alakult szervezetek, szolgálatok rádiórendszerei más-más frekvenciákon forgalmaznak (némely szervezet többön is), ami a rendszerek közti átjárhatóságot csak bonyolult és költséges rendszertechnikai megoldások alkalmazásával tenné lehetővé. A rádiózás azonban a jelenleg rendelkezésre álló technikai feltételek mellet nem csak körülményes, de biztonsági szempontból is aggályos, hiszen a forgalmazás nem, vagy csak erősen korlátozott mértékben titkosítható. Ez a két tényező a gyakorlatban annyit jelent, hogy vészhelyzetben a rendőrség intézkedéseiről a más frekvencián forgalmazó társszervek csak közvetítők útján, saját országos vagy megyei központjuk közbeiktatásával értesülhetnek, a terroristák viszont a rendszerbe történő behallgatással folyamatosan tájékozódhatnak az ellenük foganatosított eljárásokról. A rádióforgalom könnyű lehallgathatósága, és az együttműködési problémák miatt tértek át több hivatalos és egyenruhás szervezetnél az elmúlt években a mobiltelefon használatára…

A mobiltelefon rendszerek hatékonysága krízishelyzetben

A mobiltelefon használat mára nem csak a világ fejlett, hanem fejlődő országaiban is a mindennapok részévé vált, aminek következtében az egyén bárhol, bármikor képes hívást kezdeményezni és bárhol, bármikor elérhető. Ennek (és a megfizethető szolgáltatásoknak) köszönhetően a rádiótelefon sokak számára munkaeszközzé is vált mind a magán, mind az állami szektorban, így a közigazgatásban, a rend-, határ-, hon-, és katasztrófavédelemben is. Számos szervezet esetén tapasztalható súlyponteltolódás ezen kommunikációs forma irányába a mindennapos tevékenységek során. A

[155] Magyarországon két alapvető jogszabály - a 2004. január 1.-étől hatályba lépet a 2003. évi C. törvény az elektronikus hírközlésről, valamint a 100/2004 (IV. 27.) kormányrendelet az elektronikus hírközlés veszélyhelyzeti és minősített időszaki felkészítésének rendszeréről – tartalmazza az ezzel kapcsolatos paragrafusokat.

mobiltelefonok ugyan bizonyítottak és bizonyítanak napjainkban is normál körülmények között, de mi történik, ha valamilyen krízishelyzet alakul ki.

A kommunikációs rendszereket két alapvető jelenség (veszély) fenyegeti krízishelyzetben (például terrorcselekmény, vagy katasztrófa esetén):

- az infrastruktúra elvesztése: amikor a rendszer valamely része, vagy egésze fizikailag megsemmisül (pl.: robbantás, földrengés, elemi erejű vihar következtében), illetve az alapvető működéséhez szükséges valamely tényező nem áll rendelkezésre (pl.: energiaellátás zavara, megszűnése). Ebben az esetben a rendszer által biztosított szolgáltatások elérhetetlenné válnak minden az adott ellátási területen tartózkodó előfizető számára. (Az összeköttetések megszakadnak)
- a túlterheltség (vagy túltelítettség): amikor az igénybevétel nagysága meghaladja a rendszer áteresztőképességét. Ebben az esetben az adott területen rendelkezésre álló csatornák száma kisebb, mint a híváskezdeményezési próbálkozásoké. (pl.: Újév első percei, vagy bekövetkezett katasztrófát követően)

A gyakorlatban természetesen a két tényező ok-okozati összefüggésben is állhat, illetve egymás hatását erősítve akadályozhatja az információáramlást.

### A 2001. szeptember 11.-ei terrortámadás tapasztalatai

A támadás előtti és utáni időszakban is számos alkalommal lehetőség nyílt a telekommunikációs rendszerek extrém terhelés mellett történő vizsgálatára, melyek során a szolgáltatók és távközlési szakemberek információkat kaphattak a rendellenes működés esetén fellépő jelenségekről akár az infrastruktúra egy részének elvesztése mellett is, ugyanakkor a legszélesebb körben és értelemben tanulmányozott eseménynyé a mindmáig precedens értékű New York-i terrortámadás telekommunikációra gyakorolt hatása vált. Ez a hatás rendkívül súlyosnak bizonyult. Fizikailag megrongálódott az infrastruktúra jelentős része, aminek következtében szinte teljesen megszűnt az információáramlás. A tornyok összeomlása például óriási fennakadást okozott a West Street 140-es szám alatti központban, ahol 200 000 telefon-, 150 000 hivatali vonal, és közel 4 000 000 adatátviteli áramkör némult el. A 911-es segélyhívó rendszer azonnal a készenléti tartalékkörökre kapcsolt így biztosítva a rendszer működőképességét. 38000 segélyhívást kezelt, ami 71 %-kal több volt, mint normális üzem esetén. A vezetékes kapcsolatok megszakadását követően a város egyik mobilszolgáltatója a forgalom 1300 %-os növekedését tapasztalta. Az infrastruktúra sérülései, valamint az ugrásszerűen megemelkedett forgalom miatt 11 órára a mobiltelefonos hívások 90 %-a blokkolódott New York körzetében. Az energiaellátási problémák csak tovább súlyosbították a kialakult helyzetet. A fenti problémák ellenére a mobilhálózat nem omlott össze teljesen, sőt mobilizálható (szállítható) bázisállomások telepítésével a rendszer működése hamarabb helyreállt, mint a vezetékes összeköttetéseké, ezzel bizonyítva, hogy vészhelyzetben ez az egyik legmegbízhatóbb kommunikációs csatorna.

A rendszer leghatékonyabb szolgáltatásai az SMS156 és az e-mail küldési lehetőség, hiszen ez terheli legkevésbé a hálózatot, továbbá ezek segítségével lehet az információkat (utasításokat) a legrövidebb időn belül, akár nagy tömegekhez is eljuttatni. Ezért annak ellenére, hogy az Egyesült Államokban korábban közel sem volt olyan népszerű a szövegküldés, mint például Nagy-Britanniában, a mentés idején sikeresen alkalmazták az információtovábbításnak ezt a formáját.

[156] Sort Message Service – rövid szöveges üzenet

**Mobil hálózatok irányítása krízis idején Nagy-Britanniában**

A kormány jogosult intézkedni a mobiltelefon hálózatok szolgáltatásainak korlátozására, vagy felfüggesztésére válsághelyzetben, azonban az eljárás gyakorlati alkalmazása a hálózatokat üzemeltető, piaci alapon működő szolgáltatók üzleti érdekei miatt meglehetősen korlátozott. Minden GSM rendszer esetében alkalmazható a hozzáférés vezérlése, ami 15 hozzáférési szintet definiál. Ebben a rendszerben a 10-15. sorszámú szint a sürgősségi (készenléti) szolgálatok számára van fenntartva. A hozzáférés irányítását krízishelyzetben az úgynevezett ACCOLC157 vezérlő program végzi, amelyet a mobiltelefon szolgáltatók aktiválnak a rendőrség, vagy a kormányhivatal utasítása alapján. A program működtetésének célja, hogy veszélyhelyzetben prioritást biztosítson a közbiztonságért felelős szervezetek és más kiemelten fontos hatóságok számára a hálózatokhoz való hozzáférés tekintetében. Ez a megoldás megakadályozza a kevésbé fontos felhasználók tömegesen kezdeményezett hívásai miatt esetlegesen bekövetkező forgalmi torlódásokat, ami veszélyhelyzet esetén megnehezítené, vagy lehetetlenné tenné a hálózat használatát a mentésben résztvevő szervek számára. Normál helyzetben (nem minősített időszakban) a rendőrség „incidens" parancsnoka jogosult az ACCOLC program aktiválására utasítást adni, míg kivételes esetekben ez a felelősség a kormányhivatalra hárul. Előbbi esetben a hozzáférés vezérlése általában a hálózat ellátási területének korlátozott részére tejed ki (néhány bázisállomás), és elsősorban a szervezett bűnözés elleni harc (pl.: kábítószer-, fegyverkereskedelem) kommunikációs támogatásában segíti a hatóságokat.

A második megoldásra olyan kiterjedt válsághelyzet (terrortámadás, katasztrófa stb.) esetén kerülhet sor, amely a központi kormányzat közvetlen beavatkozását igényli. (Ekkor a mobiltelefon szolgáltatások teljes szüneteltetése is lehetséges. Véleményem szerint ezen eljárás alkalmazására került sor a 2005. július 7.-i terrorcselekmények után Londonban.)

*Az ACCOLC jelentése*

Az ACCOLC tehát egy az Access Overload Control szavakból képzett betűszó, melynek magyar fordítása „hozzáférés vezérlés túlterheltség esetén" lehetne. Ez tulajdonképpen olyan vezérlési metódust takar, amely rendkívüli helyzetekben (pl.: jelentős mértékű ipari, vagy közlekedési balesetet, természeti katasztrófát, terrorcselekményt követidőszakban) a lehető legrövidebb időn belül biztosítja a mobiltelefon szolgáltatók hálózataihoz való elsőbbségi hozzáférést a mentésben résztvevő szervezetek (pl.: rendőrségi szervek, tűzoltóság, mentőszolgálatok stb.) és személyek számára. Ha ez a hozzáférés vezérlés aktív, a hálózatot nem terhelhetik túl a prioritással nem rendelkező felhasználók hívásai.

Az ACCOLC rendszer aktiválásának felelőssége

Nagyobb baleset körzetében, vagy a szervezett bűnözés illetve terrorizmus elleni küzdelem jegyében a rendőrség „incidens" parancsnoka utasíthatja a szolgáltatókat, hogy az érintett cellák esetében aktiválja ezt a hozzáférés irányítási rendszert. Terrortámadásokat, nagykiterjedésű, nagy tömegeket érintő ipari, vagy természeti katasztrófákat követően, amennyiben a kialakult helyzet a központi kormányzat közvetlen beavatkozását igényli, a rendszer aktiválására a Kormányhivatal intézkedhet.

[157] Access Overload Control - hozzáférés vezérlés túlterheltség esetén

(Amíg az ACCOLC inaktív, minden forgalmi igény azonos prioritással kerül kielégítésre, ekkor a készenléti szervek hívásai sem élveznek elsőbbséget a „civil” hívásokkal szemben.)

Az ACCOLC rendszer igénybevételének feltételei

A rendszer szolgáltatásait igénybe vehetik mindazon szervezetek és szakemberek, akiknek a készüléke regisztrálásra került, és olyan körzetben tartózkodnak, ahol az ACCOLC–ot aktiválták.

Erre az intézkedésre csak extrém esetekben kerülhet sor, általában amikor valamilyen okból kifolyólag a saját hálózatok működőképessége korlátozott, vagy ha komplex mentési műveletek végrehajtása során olyan együttműködésre van szükség, melynek koordinálása más kommunikációs csatornákon nem biztosítható, továbbá a hálózat normális üzemben előreláthatóan nem képes kiszolgálni a növekvő védelmi igényeket a tartalékok bevonása mellet sem. (Az ACCOLC általában kommunikációs tartalék szerepet tölt be krízishelyzetek kezelése során.)

Másik eset, amikor a rendszer aktiválásának célja a mobiltelefon hálózatok forgalmának korlátozása, például a szervezett bűnözés, vagy terrorizmus elleni harc folyamán a feltételezett elkövetők kapcsolattartásának akadályozása (pl.: ne tudják értesíteni egymást az ellenük foganatosított intézkedésekről), vagy robbantásokat követően további pokolgépek mobiltelefonok útján történő aktiválását megelőzni.158

Az elsőbbségi hozzáférésre jogosultak körét szigorúan szabályozzák (korlátozzák), hogy ne fordulhasson elő a rendszer túlterhelése, a prioritással rendelkezők nagy száma miatt. A rendszerbe történő regisztrációt különböző kormányzati szerveken keresztül kell kérvényezni. Az engedélyt csak a krízishelyzetek megoldásában kulcsszerepet játszó szervezetek és személyek kaphatják meg, mint például az érintett körzetekbe vezényelt rendőrök, tűzoltók, katonák, mentőtisztek, esetkocsik, orvosok, és különböző specialisták (bombaszakértők, ABV szakemberek, égési specialisták stb.) Az engedélyezést követően a kérelem átkerül az érintett mobiltelefon szolgáltatókhoz, akik ezután kezdeményezik a készülék regisztrációját. (A szolgáltatás térítésköteles!) Ezt követően az érintett készülékeket el kell vinni a szolgáltatóhoz, ahol elvégzik a regisztrációt, a készüléket ellátják egy speciális SIM kártyával és átkonfigurálják.

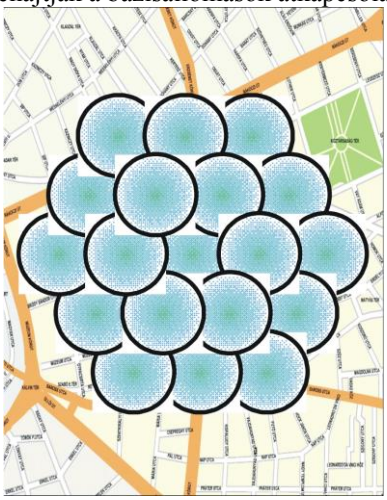
Az ACCOLC rendszer működése

A mobiltelefon hálózatok cellás rendszerek, azaz a szolgáltatási terület teljes lefedését különböző méretű cellák (városban kisebb, ritkán lakott területeken nagyobb) egymásmellé helyezésével oldják meg (a hatékony frekvenciakihasználtság- újrafelhasználás miatt). Minden cella rádiófrekvenciás kiszolgálásáért egy-egy bázisállomás felelős, amelyek egymástól függetlenül programozhatók, kapcsolhatók, vezérelhetők.

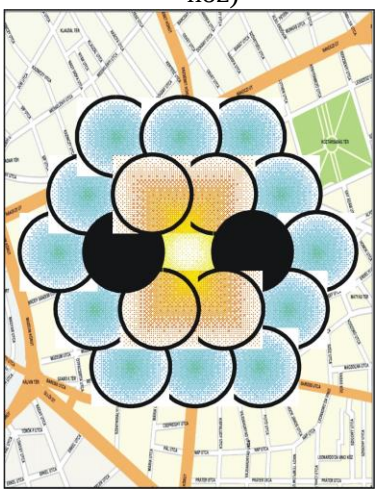
Ha egy területen valamilyen rendkívüli állapot alakul ki (robbanás, tömegbaleset, katasztrófa stb.), a rendőrség illetékes „incidensparancsnoka” a kialakult helyzetet értékelve dönthet úgy, hogy szükséges a hozzáférés vezérlésének alkalmazása (mobiltelefon szolgáltatás szüneteltetése). Ekkor utasítja a szolgáltatókat (Cellnet, Vodafone, Orange, ...) az ACCOLC rendszer aktiválására, amihez megadja az érintett terü-

158 Azzal a veszéllyel kell számolni, hogy az elkövetők az első robbantásokat követően a kiérkező mentőalakulatok ellen újabb támadást hajtanak végre.

letet és a várható időtartamot. Ezt követően az érintett alhálózatok üzemeltetői a meghatározott cellákban végrehajtják a bázisállomások átkapcsolását.



1. ábra: Normál működésű cellák (minden előfizető hozzáférhet a hálózathoz)



2. ábra: A középső 7 cellában aktív ACCOLC (csak regisztrált felhasználók férhetnek hozzá a hálózathoz

A rendszer visszaállításáig a fenti területeken csak a regisztrált (priolizált) felhasználók férhetnek hozzá a hálózatok szolgáltatásaihoz, míg az innen telefonálni kívánó egyéb felhasználók a ”rendszer foglalt”, vagy a „szolgáltatás nem hozzáférhető” jelzést hallanak. (Ekkor természetesen ezek a készülékek nem is hívhatók.) Ezalatt a normál működésű cellákban tartózkodó minden felhasználó azonos prioritással férhet hozzá a hálózathoz, tehát a regisztráltak sem élveznek elsőbbséget az átlagos előfizetőkkel szemben. (Itt torlódás is előfordulhat, ezért fontos nagy körültekintéssel eljárni a zóna kijelölésekor.) A válsághelyzet megszűntetését követően a rendszer visszaáll

normál üzemre. Az 1. ábrán a krízishelyzet előtti és a felszámolását követő, míg a 2. ábrán a krízishelyzet alatti állapot látható sematikus térképvázlaton fiktív cellákkal. (A kék cellák normál működést, a pirosak aktivált ACCOLC rendszert jelentenek.)

*Ellentételezés*

Az ACCOLC rendszer alkalmazásában (extrém helyzeteket leszámítva) sem a készenléti szervek, sem az előfizetők, sem pedig a szolgáltatók nem érdekeltek. Előbbiek azért nem, mert az többnyire saját kommunikációs csatornáik hiányát jelenti, míg az előfizetők a rendszer aktivált állapotában nem tudják igénybe venni a hálózat szolgáltatásait. A szolgáltatókat egyértelműen gazdasági veszteség éri, hiszen ebben az időszakban nem keletkeznek bevételeik, ezért őket anyagi kártalanítás illeti meg a kiesett forgalom miatt. (A készenléti szervek a hálózat használatáért természetesen fizetik forgalmi díjakat.)

**A mobil hálózatok alkalmazásának lehetősége krízis idején Magyarországon**

Magyarországon jelenleg tehát a kormány jogosult felfüggesztetni a mobil szolgáltatásokat az ország honvédelmi, nemzetbiztonsági, gazdasági vagy közbiztonsági érdekeinek védelmében. Egy ilyen intézkedés azonban a hatóságok munkáját is ellehetetlenítené, hiszen a gyakorlatban a készenléti szolgálatok is jobb híján a mobiltelefont használják mind a szervezetek közötti, mind a szervezeteken belüli kommunikáció biztosítására. (Pl.: nagy hadgyakorlatok, árvízi védekezés stb.) Katasztrófahelyzetben jelen pillanatban is a mobiltelefon jelenti a mozgósítás leghatékonyabb, a kapcsolattartás legmegbízhatóbb lehetőséget a Rendőrség, Mentőszolgálat, Katasztrófavédelem, Honvédség és más a krízis felszámolásában résztvevő szolgálatok vezetői, szakemberei és beosztott állománya számára. (Nincs ez másként a Határőrség, Rendőrség, Vám- és Pénzügyőrség közös akciói során sem.) Bár minden fent említett hatóság rendelkezik saját rádiókommunikációs rendszerrel azok megbízhatósága, információvédelmi és együttműködési képessége meglehetősen korlátozott, így a nagyfokú együttműködést igénylő, komplex feladatok végrehajtására alkalmatlan. (És még nem is beszéltünk a nemzetközi együttműködések esetleges kommunikációs igényeiről…)

A fenti anomáliák miatt a kommunikációs (híradó) szakemberek évek óta sürgetik az egységes digitális rádiotávközlő rendszer (EDR) országos kiépítését, amelyen keresztül természeti katasztrófa, tömegszerencsétlenség vagy terrortámadás esetén biztonságosan, a polgári telekommunikációs hálózatoktól függetlenül, illetéktelenek számára hozzáférhetetlenül (lehallgathatatlanul) tarthatnák a kapcsolatot a különböző hatóságok. A kormányzati döntés előkészítése csaknem tíz éve tart, és csak 2005-ben született meg a véglegesnek tekinthető elhatározás. A Budapesti rendszer átadásának tervezett időpontja 2006. kora tavasza, míg az országos rendszer várhatóan 2007 végétől (schengeni követelmény) áll üzembe. Az előző kormányzati ciklusban kiírt tendert az eredményhirdetés előtt lefújták. Az akkori elképzelésben, az szerepelt, hogy „technikát” vásárolnak és a projekt lebonyolítására állami céget hoznak létre.

Ez a megoldás közel 50 milliárd forintos egyszeri befektetést igényelt volna, míg a rendszer éves üzemeltetési költségei évi 12 milliárd forintot tettek volna ki. Az új tender értelmében a kormány a piaci megoldás mellett döntött, így a kiírásban nem technológia, hanem szolgáltatás megvásárlása szerepel. Ennek köszönhetően fordulhat elő, hogy nagy valószínűséggel a NOKIA fogja szállítani a szükséges berendezéseket, hiszen a három talpon maradt konzorcium mindegyike (T-Mobile Rt. - Magyar Telekom Rt., Magyar Villamos Művek Rt. - Saab AB, Antenna Hungária Rt. - a Siemens Rt.) a skandináv multinacionális vállalatot jelölte meg alvállalkozóként. (A szolgáltatás ellentételezéseként mindhárman évi 10 milliárd forint feletti összeget jelöltek meg.) Minden pályázó rendelkezik már többé-kevésbé a rendszer kiépítéséhez elengedhetetlen alapinfrastruktúrával, mégis a T-Mobile lépéselőnyben van a többiekhez képest, hiszen jelenleg is rendelkezik piaci alapon működő vezetéknélküli rendszerrel.

A kiépülő hálózat várhatóan a TETRA technológián fog alapulni és becslések szerint több mint 40 ezer felhasználó számára biztosít folyamatos, biztonságos kommunikációs lehetőséget. (Ennek legnagyobb jelentőssége nagyobb katasztrófák esetén mutatkozik meg a különböző szervezetek együttműködése során.)

De térjünk vissza a jelenlegi gyakorlatra és vizsgáljuk meg, miként tudjuk a mobiltelefon szolgáltatók hálózataiban rejlő lehetőségeket nagyobb mértékben kiaknázni rendkívüli helyzetek során, abból az alapfeltevésből kiindulva, hogy ez nem alternatívát jelent az EDR-rel szemben, hanem kiegészíti azt, illetve szükség esetén tartalékként állhat rendelkezésre. Induljunk ki a fent említett, Nagy-Britanniában üzemelő ACCOLC rendszerből, amely krízishelyzetben biztosítja a kiemelt fontosságú felhasználók számára az elsőbbségi hozzáférést a mobiltelefon hálózatokhoz.

Amennyiben hazánkban bevezetésre kerülne a rendszer, és a készenléti szervezetek (Rendőrség, Honvédség, Katasztrófavédelem, Polgári védelem, Tűzoltóság, Határőrség, Mentőszolgálat stb.) szolgálatban lévő tagjait és vezetőit ellátják ilyen speciálisan programozott készülékekkel[159], olyan kommunikációs platform állna rendelkezésünkre, amely minden körülmények között biztosítja az együttműködés lehetőségét, minden szervezeti szinten.[160] Ez a megoldás jelentősen csökkentheti a készenlétiek reakcióidejét, ami emberéleteket jelenthet. Természetesen új eljárási- és rendszabályokat szükséges kidolgozni, és azok alkalmazását együttműködési gyakorlatokon gyakoroltatni, hogy a rendszerben rejlő lehetőségeket maximálisan kiaknázhassuk. Ugyanazon technológiára épülő szabványosított rendszerben ugyanis nagyságrendekkel gyorsabb az információ áramlása, mint különböző megoldásokat al-

[159] Akár többnormás EDR/GSM/GPS készülékekkel

[160] Ehhez azonban arra is szükség van, hogy a katasztrófahelyzetben kivonuló állomány is felszerelhető legyen az érintett hatóságok erre a célra kialakított „híradó" raktáraiból ilyen telefonokkal.

kalmazó, különböző fejlettségű telekommunikációs rendszerek erőszakos összekapcsolása, történjen akár valamilyen automatizmus, akár diszpécser útján.

A jelenleg működő korszerű mobiltelefon rendszerek azonban a beszédkommunikáció mellett számtalan kiegészítő szolgáltatást nyújtanak a felhasználók számára, amelyek alkalmazása további támogatást nyújthat a katasztrófahelyzetek gyors és hatékony kezeléséhez.

A rövid szöveges üzenet (SMS) lehetőséget biztosít nagy tömegek egyidejű gyors informálására, amellyel például mozgósítás, vagy lakossági tájékoztatás hatékonyan megoldható.

A GPRS161 csomagkapcsolt adatátviteli szolgáltatással küldhetünk a GPS162- szel nyert pontos pozícióadatokat163, vagy számítógépek között adatfájlokat, dokumentumokat stb. mozgathatunk, vagy hozzáférhetünk központi adatbázisok tartalmaihoz164.

Amennyiben a készülék rendelkezik a szükséges műszaki paraméterekkel, a beépített digitális fényképezőgéppel készített képek MMS165-ben azonnal továbbíthatók például az illetékes elöljárók, vagy szakértők (pl.: tűzszerészek) felé a gyors helyzetértékelés elősegítése érdekében.

A harmadik generációs hálózatok biztosítják mozgóképek valósidejű továbbítását, ami szintén a katasztrófa következtében kialakult állapot értékelésében segíthet a helyszíntől távoli szakemberek, továbbá a vezető beosztású személyek részére biztosítja a videokonferencia lehetőségét. Természetesen az UMTS166 technológia szélessávú adatkommunikációs lehetőséget is nyújt a felhasználók számára, ami lehetővé teszi az INTERNET-es tartalmakhoz, vagy a fent említett adatbázisokhoz való gyors hozzáférést.



3. ábra: SECTRA NSK 200 Secure Phone

[161] General Packet Radio Service – csomagkapcsolt adatátviteli protokoll mobil alkalmazásokhoz

[162] Global Positioning System – globális műholdas helymeghatározó rendszer

[163] Akár lakott területeken, akár azoktól távol bekövetkező katasztrófák esetén fontos lehet a mentés mielőbbi megkezdéséhez

[164] Személyi adatok terroristák körözéséhez; meteorológiai, geológiai, vízügyi adatok a szükséges felszerelések meghatározásához stb.

[165] Multimedia Message Service – multimédiás üzenetküldési szolgáltatás

[166] Universal Mobile Telecommunications System – univerzális mobil telekommunikációs rendszer

Gyakran szükség lehet az információk titkosított továbbítására, amire a jelenlegi hálózati technológia nem kínál kielégítő megoldást. Létezik azonban a Kongsberg cégcsoportnak egy olyan mobiltelefonja, amely megfelel a szigorú NATO kriptográfiai előírásoknak és biztosítja a lehallgathatatlan hang- és adatátvitelt a szabványos mobilhálózatokon. Az ilyen NSK 200-as telefonról[167] (3. ábra) kezdeményezett hívás csak azonos típusú készülékkel dekódolható…

Végezetül nézzünk egy fiktív példát (a Londoni terrortámadás analógiájára):

Budapest egyik bevásárlóközpontja előtti parkolóban, majd 2 perc elteltével 700 m-rel odébb egy metróállomás peronján nagy erejű pokolgép robban. Az első detonációt követően a helyszínre érkező járőrpáros miután felmérte a helyzetet, rádión, vagy annak „hibája" esetén mobiltelefonon értesíti az elöljáró parancsnokot, vagy az eljárási szabályokban rögzítet illetékes parancsnokot, aki meghatározza számára a feladatokat. Az elöljáró értesíti az intézkedésre kijelölt rendőri szerveket, mentőszolgálatokat, a tűzoltóságot, a nemzetbiztonsági szakszolgálatokat, a tűzszerészeket stb. Időközben bekövetkezik a második detonáció, amit az első helyszín felé úton lévő tűzoltóautó személyzete észlel és jelenti parancsnokának. Az tájékoztatja a rendőrség illetékes parancsnokát, aki gyors helyzetértékelést követően utasítja a mobilszolgáltatókat az elsőbbségi hozzáférés vezérlési program aktiválására, meghatározva az érintett körzeteket. A lekapcsolást megelőzően az üzemeltető SMS-t küld a körzetben tartózkodóknak és a rendszer összes előfizetőjének a foganatosított intézkedésekről és a javasolt magatartásról. (Ezzel jelentősen csökkenthetők a lakosság azon pánikreakciói, melyeket az információhiány okoz.) Ezt követően a fennálló összeköttetések megszakadnak és az „átlagos felhasználók" a körzetből induló, valamint az ide irányuló híváskezdeményezés esetén foglaltsági jelzést hallanak, míg a mentésben résztvevők minden szolgáltatáshoz „korlátlanul" hozzáférhetnek. Így a terroristák nem tudnak mobiltelefonos távirányítással újabb pokolgépeket robbantani a mentőalakulatok közelében. (Amennyiben fennáll a veszély, hogy esetleg más körzeteket is támadás fenyeget, a korlátozást például a Miniszterelnöki Hivatalt vezető miniszter, a rendőrség javaslatára kiterjesztheti a Főváros teljes területére.) A két vezeték nélküli távközlési rendszer együttesen ki tudja szolgálni a kommunikációs igényeket mindaddig, amíg az EDR üzemében zavarok nem lépnek fel. Ekkor ugrásszerűen megnő a mobilforgalom, amit a rendelkezésre álló kapacitások még a tartalék áramkörök aktiválásával sem tudnak folyamatosan kielégíteni. A „híradás" további biztosításának érdekében az illetékes parancsnok utasítására a kérdéses körzetekben a szolgáltatók ügyeletes karbantartó egységei tartalék bázisállomásokat telepítenek.

A forgalom jelentős részét ugyan a hangátvitel teszi ki, azonban a hálózatok számos kiegészítő szolgáltatást biztosítanak a krízis kezelése során, melyek hasznosítására számos lehetőség kínálkozik:

- A számos halálos áldozat fényképét MMS–ben továbbítják a náluk talált papírokból nyert személyi adatokkal együtt a központi adatbázisba, ezzel meggyorsítva azonosításukat, a családok tájékoztatását és a későbbi adminisztrációt…

[167] Ilyen eszközökkel rendelkezik már a holland, és német haderő.

- A sebesültek osztályozása és ellátása lassan halad, mert a kialakult kaotikus forgalmi helyzetben a mentőalakulatok csak lassan tudják megközelíteni a helyszíneket, annak ellenére, hogy a körzeteket biztosító járőrök folyamatosan irányítják az érkező járműveket. A helyszínen tartózkodó elsősegélynyújtók és mentőápolók a súlyos, speciális sérülésekről (pl.: égési és csonkolásos sérülések) fényképeket küldenek az ügyeletes kórházaknak és specialistáknak, akik az információk birtokában előre tervezhetik a beavatkozásokat és a szükséges kezeléseket, ezzel jelentősen növelve a túlélés esélyeit…
- Az egyik helyszínt átvizsgáló tűzszerész egy gyanús csomagot talál a bevásárlóközpont bejárata mellet, majd a terület biztosítását követően megkezdi annak vizsgálatát. A csomagban talált szerkezet azonban számára még ismeretlen, ezért fotókat készít róla és elküldi azokat tapasztaltabb kollegáiknak, akik nemzetközi adatbázisokban és az Interneten próbálnak a feltételezett pokolgépről adatokat fellelni…
- Időközben a családtagjaikért, ismerőseikért aggódók a helyszínek közelében próbálnak információkhoz jutni a felállított mobil tájékoztatási központokban elérhető, folyamatosan bővülő adatbázisokból. (sebesültek és az őket fogadó egészségügyi intézmények, elhunytak stb.)…

Néhány óra elteltével a hatóságoknak sikerül a helyzet normalizálása, helyreáll a közrend és a közlekedés, a sérültek többségéhez időben eljutott a megfelelő orvosi segítség, így az idő múlásával nem nő tovább a halálos áldozatok száma. Elhárították az egységes digitális rádiórendszerben keletkezett üzemzavart, elbontják a tartalék mobil bázisállomásokat. A hatóságok döntése alapján inaktiválják az elsőbbségi hozzáférés-vezérlési programot, visszaáll a normál üzemállapot, minden előfizető azonos prioritással telefonálhat.

A mobiltársaságok a szerződésekben foglaltak szerint „kiállítják a számlát” a korlátozás miatt keletkezett kár, és a készenléti szervek által generált forgalom alapján.

A fenti, talán kissé erőltetettnek tűnő eset bemutatásával szerettem volna szemléltetni a mobiltelefon hálózatokban rejlő technikai lehetőségeket. (A jelenlegi biztonsági környezetben sajnos semmilyen lehetőséget nem lehet kizárni, még akkor sem, ha annak valószínűsége minimális.)

Cikkemmel szerettem volna felkelteni a figyelmet ez iránt a különleges kommunikációs platform iránt, ami nagyban segítheti a természeti katasztrófák, ipari balesetek, terrorcselekmények következtében kialakuló krízishelyzet megelőzése, illetve kezelése során az érintett hatóságok, szervezetek, szakemberek együttműködését.

A rendszer esetleges bevezetéséhez azonban mind jogi, mind technológiai területen számtalan feladat vár megoldásra. Például:

- Fel kell mérni a készenléti szervek igényeit a rendszer bevezetését illetően.
- Hatástanulmányokat szükséges készíteni a döntések előkészítésére.
- Egyeztetéseket kell folytatni a szolgáltatók és a kormányzat felelős szervei között.
- Meg kell alkotni a rendszer alkalmazásának jogszabályi hátterét (döntési szintek, felelősségi körök).

- A szolgáltatókat kötelezni kell a rendszer bevezetésének technikai és technológiai hátterének biztosítására, mobilizálható tartalékok kiállítására168, cselekvési tervek kidolgozására.
- Meg kell határozni a szolgáltatás igénybevételének ellentételezését.
- Meg kell határozni azokat a szervezeteket és személyeket, akik jogosultak magasabb prioritású készülékek használatára.
- Az érintett szerveket el kell látni a különböző szintű szolgáltatások igénybevételére alkalmas készülékekkel (alapkészülékek, „titkosított" készülékek, multimédiás készülékek)169.
- Tesztrendszer kialakítása.
- Lakossági tájékoztatási rendszer kidolgozása.

## Felhasznált irodalom:


[14] PÁNDI Erik: A magyar kormányzati távközlés egységesítésének hatása a rendvédelmi-, katonai-, és közigazgatási kommunikációs rendszerek megszervezésére és irányítására (Doktori értekezés tervezet) - Budapest, 2005

[15] FEKETE Károly: A Magyar Köztársaság kommunikációs infrastruktúrája (Egyetemi jegyzet) – Budapest, 2004

[16] DÉRFÖLDI László, Pintér István (Szerk.): A Honvédelmi felkészülésre, Nemzetbiztonságra, Polgári Védelemre, Katasztrófavédelemre, Titokvédelemre vonatkozó és a NATO tagságból adódó fontosabb Jogszabályok - Hírközlési Felügyelet, Budapest, 2003

[17] NÉMETH András, Dr. habil Sándor Miklós: A katasztrófavédelmi kommunikáció jogi szabályozása Magyarországon – Kommunikáció 2004

[18] András NÉMETH, András Somos: Emergency Communications Systems in the United Kingdom, AARMS Vol. 4, No. 2, 2005

[19] Borough of Barking and Dagenham, Emergency Plan-Communications, Appendix 3, September 2004.

[20] Wireless Week-UK Networks On New Year's: Too Loaded, Jan 10,2000

[21] Continuity Central, How Effective Is Mobile Telephony in a Crisis, Dec 3,2004

[22] Walsall Metropolitan Borough Council, Emergency Plan 2004

[23] London Emergency Services Liaison Panel, Major Incident, Procedure Manual, Sixth Edition-July 2004, Communications Systems

[24] NHS Information Authority, ACCess OverLoadControl for Cellular Radio Systems, Jan 05, 2003

[25] 2003. évi C. törvény az elektronikus hírközlésről

[26] 131/2003 (VIII. 22.) kormányrendelet a nemzetgazdaság védelmi felkészítése és mozgósítása feladatai végrehajtásának szabályozásáról

[27] 100/2004 (IV. 27.) kormányrendelet az elektronikus hírközlés veszélyhelyzeti és minősített időszaki felkészítésének rendszeréről, az államigazgatási szervek feladatairól, működésük feltételeinek biztosításáról

[28] IHM rendelet-tervezet a védelmi feladatokban résztvevő elektronikus hírközlési, illetve postai szolgáltatók kijelöléséről és felkészülési feladataik meghatározásáról

[29] 27/2004 (X.6.) IHM rendelet az informatikai és elektronikus hírközlési, továbbá a postai ágazat ügyeleti rendszerének létrehozásáról, működtetéséről, hatásköréről, valamint a kijelölt szolgáltatók bejelentési és kapcsolattartási kötelezettségeiről


[168] A mobil hálózat infrastruktúrájának esetleges sérülése esetén, rövid időn belül megtörténjen a szolgáltatás helyreállítására.

[169] Közbeszerzési eljárások lefolytatása.

**NÉMETH András, Dr. OSVÁTH Zoltán**

# MÚLT –JELEN – JÖVŐ… AVAGY VILLAMOS- KONTRA „HADMÉRNÖK” A HÍRADÓTISZT-KÉPZÉSBEN

Németh András okleveles mérnök hadnagy – Dr. Osváth Zoltán alezredes

A Berlini Fal leomlása, a Varsói Szerződés felbomlása és a Szovjetunió szét-hullása a kétpólusú világrend végét jelentette. A geopolitikai és biztonsági környezet jelentős változása új kihívások elé állították az egyesülés útjára lépő Európa, így Magyarország fegyveres erőit is. A túlideologizált ellenségkép szertefoszlásával feleslegessé váltak a hidegháború időszakát jellemző tömeghadseregek, így lehetőség nyílt a mennyiségi paraméterek rovására egy minőségi átalakítási folyamat beindítására... (Természetesen a modernizálás sebessége nagyban függ az adott ország gazdasági erejétől.) Az új kihívásoknak való megfelelés minden szinten új képzési struktúrák kialakítását tette szükségessé.

## A magyar műszaki tisztképzés múltja [1]

Az Osztrák-Magyar Monarchia idejében a tisztképzés a bécsi mérnök iskolában folyt, melyet később katonai intézménynek nyilvánítottak, majd 1788-ban Hadmérnök Akadémiává alakítottak. (Az intézet falai között végzett Bolyai János is 1823-ban) Az 1872. évi XVI. törvénycikk elrendelte a Magyar Királyi Honvéd Ludovika Akadémia felállítását a bécsi császári és királyi Terézia Akadémia mintájára, a közös hadsereg hadmérnöki és műszaki tisztképzése azonban továbbra is az osztrák tanintézetekben folyt. A növendékek (majd 1903-tól az akadémikusok) nevelése 19. életévüktől kezdődött és 3, majd 4 éven keresztül tartott. A felvettek fele polgári, másik fele katonai középiskolából került ki. Tanulmányaik befejezése után az itt végzett tisztek vagy a magyar királyi honvédségnél, vagy a közös hadseregben szolgáltak. A műszaki tiszteket a mödlingi Műszaki Katonai Akadémián képezték, míg a felsőbb Hadmérnöki Tanfolyamot 1905-1907-ig a vezérkari képzést adó Hadiiskolába tagolták.

Az I. világháborút lezáró békeszerződés csak egy tisztképző főiskolát engedélyezett, melynek következtében a honvédség minden fegyvernemére vonatkozó szakképzést a Ludovika vette át. Az erősen korlátozott létszámú hadseregben először alakultak meg a magyar királyi műszaki csapatok, így 1918-ban megkezdődhetett a magyar nyelvű műszaki tisztképzés. A híradótisztek képzése ebben az időben ennek keretében folyt. A Ludovika Akadémia 1922-ben főiskolai rangot kapott, így megváltoztak a jelentkezés feltételei is. Az intézménybe való bekerülés feltétele „4 polgári”, vagy gimnáziumi érettségi és a felvételi vizsga sikeres teljesítése volt. (A katonaiskolából felvételi nélkül, a polgári életből felvételivel, ill. egyéves „karpaszományos szolgálat” után kezdhették meg az akadémikusok tanulmányaikat.)

1931. október 1-évl a főiskola hűvösvölgyi bázisán megalakult a Ludovika Akadémia II. Főcsoport. Az átszervezéssel kivált és három szakon (műszakiak, híradók, folyamőrök) folytatódott a műszaki tisztképzés. (A híradó képzésben részesülő akadémikusok az elméleti időszak alatt tanult anyagot kora tavasztól kezdve, a pénteki kiképzési napokon gyakorolták.)

Mindhárom műszaki évfolyam a nyári gyakorlati időszakra Esztergomba került kihelyezésre július 1-tõl augusztus 14-ig.

Az 1938. szeptemberében tartott bledi konferencia megadta Magyarország fegyverkezési egyenjogúságát, ami a honvédség jelentős fejlesztésével járt. A megnövekedett haderő tiszti feltöltése érdekében a képzés három éves lett és eltörölték a csapatgyakorlatot.

A gyorsított képzésre történő áttérés két avatást tett lehetővé. 1939. január 15-én 56 fő (8 híradó), augusztus 20-án 47 fő (7 híradó) tett esküt. 1940-es évek elején a Ludovika II. Főcsoport kettévált, és a repülőtisztek képzése a Kassán felállított Magyar Királyi Vitéz Nagybányai Horthy Miklós Honvéd-repülő Akadémián170, míg műszaki, híradó, folyamőr tisztek képzése a Magyar Királyi Bolyai János Honvéd Műszaki Akadémián folyt. Itt 1940 és 1944 között 324 hadnagyot, köztük 114 híradót171 avattak fel az 1940 május 5-én átadott Bolyai csapatzászló árnyékában. A II. világháborúban a képzési idő lerövidült, így 1943-ban két év, 1944-ben egy év két hónap volt. (Az akadémikusokat tanulmányi eredményeik alapján félévenként értékelték és rangsorolták, aminek nagy szerepe volt az első tiszti beosztásba való helyezéskor).

A párizsi békeszerződés a szárazföldi haderőnél 65000, a légierőnél 5000 főben maximálta a hadsereg létszámát, így a második világháború után az alapfokú tisztképzés két évig szünetelt.

A vezetés felismerte a hatalom megszerzéséért folyó harcban a hadsereg kulcsfontosságú szerepét, ezért igyekezett a Horthy- hadsereg tisztikarát fokozatosan lecserélni. Először nevelő-, majd gazdásztiszti tanfolyamokat szerveztek, majd a hivatásos tiszti alap- és továbbképzés problémáinak megoldására 1947. október 1-én megnyitotta kapuit a Honvéd Kossuth Akadémia és a Honvéd Hadbiztos Akadémia, a vezérkari tisztek képzésére pedig létrehozták a Honvéd Hadi Akadémiát. A fegyvernemi tiszti iskolák hálózatát172 1949-ben kezdték kiépíteni, melynek keretében létrejött többek között október 1.-én a Zalka Máté Híradó Tiszti Iskola Budapesten. 1957. februárjában a Kossuth Lajos Tüzér és Tüzér Technikus Tiszti Iskola jogutódjaként Budapesten megalakult az Egyesített Tiszti Iskola, melynek sajátossága volt, hogy a tanszékeket fegyvernemi tagozatokba173 sorolták, és csak kisebb részük működött

170 1942-tõl a Horthy István Honvéd-repülő Akadémia

171 1940. júl. 04. -11 fő, 1941. aug. 20. - 6 fő, 1942. jún. 18. -5 fő, 1942. dec. 06. -10 fő, 1943. aug. 20. -22 fő, 1944. aug. 20. -19 fő, 1944. nov. 15. -41 fő

172 Bem Légvédelmi Tüzér Tiszti Iskola (1949. 10. 0l. Budapest), Dózsa Lövész Tiszti Iskola (1949. 10. 0l. Pécs), Kilián György Repülő Hajózó Tiszti Iskola (1949. 10. 01. Szolnok), Kossuth Tüzér Tiszti Iskola (1949. 10. 01. Budapest), Petőfi Politikai Tiszti Iskola (1949. 10. 0l. Budapest), Rákosi Páncélos Tiszti Iskola (1949. 10. 01. Tata), Táncsics Műszaki Tiszti Iskola (1949. 10. 01. Szentendre), Vasvári Repülő Műszaki Iskola (1949. 10. 01. Budaörs), Zalka Máté Híradó Tiszti Iskola (1949. 10. 01. Budapest), Ságvári Hadtáp Tiszti Iskola (1949. 10. 01. Budapest), Sporttiszti Iskola (1950. 10. 15. Budapest), Gépkocsi és Traktor Tiszti Iskola (1950. 05. 01. Budapest), Egészségügyi Tiszti Iskola (1950. 10. 15. Budapest), Tolmács Tiszti Tanfolyam (1950. 11. 01. Budapest), Gábor Áron Tüzér Technikus Tiszti Iskola (1951. 09. 15. Budapest), Térképész Tiszti Iskola (1951. Budapest)

173 lövész-, páncélos-, (majd a kettő összevonásával összfegyvernemi-), tüzér-, híradó-, műszaki-, hadtáp-, társadalomtudományi tagozat

önállóan174. A parancsnoki képzést biztosító tanszékek mellett 16 olyan tanszék is működött az iskola fennállásának közel 11 éve alatt, amelyeknek a műszaki tisztek képzése volt a feladata. A Híradótagozatot a Vezetékes Technikai- és a Rádiótechnikai Tanszékek alkották. Az Egyesített Tiszti Iskolán a tanulási időt kezdetben 2, illetve 3 évben határozták meg, majd 1963-ban bevezették a 4 éves képzést, és az azonos katonai követelményekkel együtt egy második polgári szakmát is el kellett sajátítaniuk a növendékeknek. (1964. szeptemberében avattak először olyan tiszteket, akik már katonai és szaktechnikusi diplomát is kaptak.) A növendékeket kezdetben növendéki ezredbe sorolták, majd a 1964/65-ös tanév kezdetétől szakáguk szerint külön-külön századokba osztva a tagozatparancsnokságok alá rendelték. A tiszti szakaszparancsnoki rendszer megszűnt, feladatkörük egy részét a tagozatok tanárai vették át.

1967-ben a Népköztársaság Elnöki Tanács 13. törvényerejű rendelete a Magyar Néphadsereg tiszti iskoláit katonai főiskolákká nyilvánította, így az Egyesített Tiszti Iskola jogutódjaként létrejött (a három katonai főiskola egyikeként) a Zalka Máté Katonai Műszakin Főiskola. A képzésben fontos változások következtek be azzal, hogy az alapfokú tisztképzést főiskolai rangra emelték, s a tananyag tartalmát az azonos profilú más főiskolákéhoz igazították. Az oktatói állományban növekedett az egyetemet végzettek száma, míg a létrejött 3 katonai főiskolán175 a hallgatói létszám közel megduplázódott.

A 4 éves képzés a maga 4536 tanórájával a tisztképzés beágyazódását jelentette az állami felsőoktatásba. Növelték a felvételi követelményeket, fokozott jelentőséget tulajdonítottak előképzettség szintjének, az egyéni adottságoknak és rátermettségnek, melynek következtében fokozódott a pálya iránti érdeklődés, így a felvételi eljárás folyamán a túljelentkezés mértéke megadta az intézménynek a kiválasztás lehetőségét. A felvételi eljárás követte a polgári felvétel rendjét, azonban a pályaalkalmasság szempontjából fontos fizikai és pszichikai alkalmasságot is mérték. A hallgatók végzéskor két diplomát176 kaptak, amely lehetett többek között híradó parancsnoki, vagy híradó rádiótechnikusi. Az elsajátított tananyag 10 %-át társadalomtudományi, 28 %-át az általános katonai felkészítés, 22 %-át az alap-és szakalapozó képzés, 40 %-át fegyvernemi szakkiképzés tette ki, míg a tanórák 45 %-a az elméleti, 55 %-a a gyakorlati jellegű felkészítést szolgálta. A hallgatók által készített szakdolgozatok színvonala a polgári főiskolákon készítettekkel azonos volt. Az államvizsga bizottságokba megjelentek a polgári szakemberek is, így a valós tudás megítélése biztosítottabb volt. 1971-től a növendék megszólítást a hallgató váltotta fel. Az oktatás 5 hónapos sorkatonai képzés után kezdődött, és végzéskor (1969. augusztus 20-tól) már a hadnaggyá, főhadnaggyá avatott hallgatók, egyesített polgári és katonai végzettséget igazolódó diplomát kaptak. A főiskolán 1967-1973 között a 14 szakon 1061 főt avattak.

174 Általános katonai-, Testnevelési tanszék

175 Kossuth Lajos Katonai Főiskola, a Zalka Máté Katonai Műszaki Főiskola és a Killián György Repülő Műszaki Főiskola

176 csapatvédelmi tüzér, csapatvédelmi rakétatüzér, honi légvédelmi rakétás, híradó parancsnoki, híradó rádiótechnikus, vegyivédelmi, hadtáp, harcjármű-üzembentartó, gépjármű-üzembentartó, rádiólokátoros (rádiótechnikai), tüzér és fegyverzettechnikus (általános fegyverzeti üzembentartó), katonai pénzügyi

(Ebben az időszakban a művelődési miniszter már csak felügyeleti jogkört gyakorolt az oktatási intézmények felett, azaz nem kiadta a tantervet, hanem csak annak tartalmát határozta meg, illetve kinevezte az államvizsga-bizottság elnökét.)

Az 1973-1981 közötti időszakban az alapfokú tisztképzés megerősítése, a létszám biztosítása és a főiskolára való jobb felkészítés jegyében megindult a katonai kollégiumok177 hálózatának kiépítése, valamint a Katonai Előkészítő Tanfolyam (KET) beindítása, amelyet érettségivel nem rendelkező, a tiszti pályát választó fiataloknak szerveztek Szolnokon 6 hónapos időtartamban.

A főiskolai képzés augusztus 1-jével kezdődött 5 hónapos csapatkiképzéssel (Debrecenben és Egerben), amely lehetőséget biztosított a beiskolázási elgondolás esetleges megváltoztatására, még a tényleges tanulmányok megkezdése előtt. Az 1973-ban megkezdett hadseregfejlesztési koncepció tervszerű, arányos minőségi fejlődést, a képzés gyakorlatiasabbá és hatékonyabbá tételét tűzte ki célul. A 70-es évek elején a polgári életben gyakorlatilag befejeződött a felsőfokú technikumok műszaki főiskolákká fejlesztése, amelyek ezután üzemmérnöki képesítést adtak. 1973-tól kezdve a 4 éves képzés végén a katonai intézmények is üzemmérnöki (a képzési szaktól függően üzembentartói, üzemeltetői, vagy üzemgazdászi, parancsnoki szakon pedig nevelőtanári) diplomát adtak, azaz az eddigi vezetőképzés mellé másik végzettség is párosult.

A korábban végzett tisztek részére lehetővé tették, hogy kiegészítő tanfolyamok elvégzése és különbözeti vizsga letétle után õk is megszerezhessék az üzemmérnöki, ill. üzemgazdászi végzettséget. A képzés ebben az időszakban 12 szakon, ezen belül 25 ágazaton folyt.

A csapatkiképzés idejét 5 hónapról először 2, majd 1979-tõl 1 hónapra csökkentették. Oktatási intézményeink ekkorra jutottak el oda, hogy a megfelelő hatékonyságot biztosító képzési bázisokkal is rendelkeztek. A tanári kar felkészültsége látványosan fejlődött, előtérbe kerültek az egyetemei és a pedagógiai továbbképzések.

Tantervi célként határozták meg a vezetői ismeretek alkalmazására való készséget, a pedagógiai tudást és a szakmai felkészültséget. Katonai szempontból alapvető követelmény volt, hogy a végzett tiszt legyen képes az első tiszti (és eggyel magasabb) beosztás ellátására.

1979-tõl a főiskolán tanító katonai és polgári tanárok részére is elérhetőek a felsőoktatásban megszokott címek és rangok. Előírták a tanári státusokra a követelményeket és bevezették a tiszti beosztásokra a tanszékvezető, tanszékvezető-helyettes, főtanár, tanár és oktató; a tanárokra a főiskolai tanár, docens, adjunktus és tanársegéd megnevezéseket. Az 1973-1981 közötti időszak alatt a főiskolán 1491 tiszt szerzett diplomát.

A 80-as évek elejére ismét szükségessé vált a tisztképzés tartalmának jelentős megváltoztatása, mert a korábbi rendszer szerint kibocsátott tisztek teljesítőképessége, általános felkészültsége, megszerzett tudása egyre kevésbé elégítette ki a hadsereg általános fejlődéséből, és ezzel összefüggésben a tiszttel szemben támasztott magasabb követelményekből adódó csapatigényeket. Az 1981. őszétől továbbfejlesztett képzési rendszerben első évfolyamon - mindhárom főiskolán fegyvernemtől és képzési szaktól függetlenül - egységes, általános katonai és természettudományi alapfelkészítést vezet-

[177] Eger 1974/1975; Nyíregyháza, Tata 1978/1979

tek be azzal a céllal, hogy megfelelően megalapozott, "konvertálható" ismereteket biztosítson a hallgatók számára fegyvernem-, illetve szakválasztás elősegítésének érdekében.

1981-tõl folytatódott a középiskolai kollégiumok hálózatának építése178 is, míg a Katonai Előkészítő Tanfolyam létszámát 50-rõl 80-ra növelték. (A katonai felsővezetés elképzelése szerint 1990-re ez a rendszer biztosította volna a főiskolai hallgatók 80-90 %-át.)

A főiskolai képzésben is jelentős változások történtek a hallgatók terhelésének csökkentése érdekében. Jelentősen csökkentették a tantárgyi átfedéseket, valamint a képzési cél szempontjából feleslegesnek ítélt tananyagokat szüntettek meg. Ezzel nem csak a tantárgyak, hanem a számonkérések és a vizsgák számát is sikerült csökkenteni.

Az alapfokú tisztképzés általános irányítását az 1984. április 1-jén alakult Tanintézeti Csoportfőnökség vette át, majd bevezették az integrált képzési rendszert, melynek keretében a képzési időt 3 évre csökkentették. (Ez volt a mérnöktiszt képzés mélypontja!) A főiskolai képzés számra négy feladatot határoztak meg, miszerint a leendő tiszteket ki kell képezni politikai vezetővé, harcvezetővé/harcbiztosítóvá, kiképzővé, a napi élet irányítójává. A tantervet négy időszakra tagolták:

- időszak I. félév - egy hónap sorkatonai alapkiképzés, továbbiakban minden szakon egységes képzés, oktatás.
- időszak II. félév - alapozás.
- időszak III-VI. félév - fegyvernemi alapozás.
- időszak V-VI. félév - szakképzés, két hónapos csapatszolgálattal.

1990. szeptember 29-én a Zalka Máté Katonai Műszaki Főiskola a „Bolyai János Katonai Műszaki Főiskola” nevet vette fel a magyar királyi Bolyai János Honvéd Műszaki Akadémia jogutódjaként.

A főiskola a Honvédelmi, illetve a Felsőoktatási törvény szellemében működő katonai felsőoktatási intézmény, melynek alaprendeltetése: a Magyar Honvédség és Határőrség részére olyan tisztek képzése, akik a Magyar Köztársaság Alkotmányára tett fogadalmuk alapján, a nemzet ügye iránt elkötelezett, az ország kormányához lojális, hazájukat szerető, mély hivatástudattal és szilárd erkölcsi tartással bíró, kiegyensúlyozott életvitelű, értelmiségi szakemberek. A képzés újra a négyéves rendszerben folyt 13 szakon és 22 ágazaton.

(A híradástechnikához sorolható katonai szakok a légvédelmi, a lokátortechnikai, elektronikai harc, híradó és rádiófelderítő.)

Híradó szakon a vezetés legalapvetőbb elemének, a híradás megszervezésének, létesítésének elveit, a híradó eszközök üzemeltetésének gyakorlatát sajátították el a leendő tisztek. Nagytávolságú összeköttetéseket létesítettek és híradó berendezéseket javítottak.

A tisztképzés mellett a főiskolán egyes szakokon, így híradó szakon is tiszthelyettes képzés és tartalékos parancsnoki képzés is folyt.

A főiskolai oktatás egy hónapos alapkiképzéssel kezdődött. Ezt követően a képzési idő 8 szemeszterből állt. Az egyes félévek vizsgákkal zárultak, majd a 8. félév végén, sikeres záróvizsga letétele után kerültek a hallgatók avatásra.

[178] Szeged, Győr, Balassagyarmat, Zalaegerszeg, Pécs, Székesfehérvár

A képzés fő célkitűzése, hogy a kibocsátott tisztek jó műszaki felkészítést kapjanak, tudásuk feleljen meg az európai felsőoktatás színvonalának, legyenek képesek tudásuk birtokában tekintélyt kivívni beosztottaik előtt. A szakmai felkészítés mellett ismerjék meg hadtörténelmünket, nemzeti és katonai hagyományainkat, tudjanak azokkal azonosulni és azok szellemében élni. A leendő tisztekkel szemben társadalmi elvárás a nyelvtudás és a jó fizikai állapot.

A képzés tananyaga 4 főbb tantárgycsoportot képzett:

- - általános értelmiségi felkészítés tantárgyai (21 %)
- - szakmai törzsanyag tantárgyai (28 %)
- - differenciált szakmai tananyag tantárgyai (22 %)
- - katonai tananyag tantárgyai (29 %).

A hallgatók a gyakorlatias felkészítés érdekében a képzési időszak alatt összesen 20-29 hét időtartamban vettek részt csapat-, illetve üzemi gyakorlaton.

A képzés folyamán a hallgatók szakonként - 4600 tanórában - eltérő tantárgyakat és minden szakon kötelező tantárgyakat tanultak. Minden szakon kötelező alaptantárgyak: filozófia, politikaelmélet, közgazdaságtan, szociológia, idegen nyelv és a testnevelés.

Minden szakon kötelező alapozó tantárgyak: általános katonai ismeretek, hadtörténelem, pszichológia, katonai pedagógia, általános és hadijog ismeretek, vezetéselmélet, katonai etika.

1993-ban 144 főt avattunk tisztté, akik közül 9 fő főhadnagyi előléptetésben részesült. 1994-ben a 4 éves képzésre történő áttérés miatt tisztavatásra nem került sor. 1995-ben 123 fő került felavatásra. (1994-től lányok is tanulhatnak a főiskolán.)

1996. szeptember 1.-től a Bolyai János Katonai Műszaki Főiskola kivált a Magyar Honvédség kötelékéből, szakmailag önálló, önkormányzattal rendelkező, részben önálló gazdálkodást végző jogi személyként folytatta további tevékenységét. Feladatait a katonai felsőoktatási intézmények részére biztosított autonómia szellemében, a vonatkozó jogszabályok keretei között, a Honvédelmi Miniszter közvetlen felügyelete alatt látta el.

A Bolyai János Katonai Műszaki Főiskola a katonai felsőoktatás első lépcsőfokán működő, négy éves alapképzést és nevelést folytató, bentlakásos, több képzési profilú főiskola, amely alapító és társult tagja volt a Budapesti Politechnikumnak. Biztosította és máig biztosítja a Magyar Honvédség és a Belügyminisztérium részére a mérnök, és a közgazdász tisztek folyamatos utánpótlását. Működését a Felsőoktatási Törvény és a Honvédelmi Törvény harmonikus alkalmazása határozza meg.

A sikeres felvételi után a hallgatók 1 hónapos katonai alapkiképzésben részesülnek. A főiskolai karon korszerű katonai, haditechnikai tananyag mellett a humán területeken (pszichológiai és pedagógiai) és hadtörténelem, haditechnika története területén is magasak a követelmények.

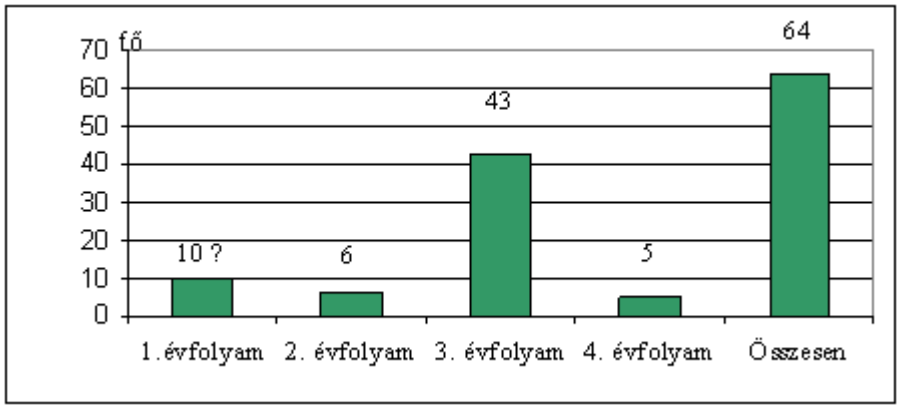
2000. január 01.-től, a Zrínyi Miklós Nemzetvédelmi Egyetemmel történő egyesüléstől, a főiskola a ZMNE Bolyai János Katonai Műszaki Főiskolai Karaként, majd 2004. szeptember 01.-től Bolyai János Katonai Műszaki Karaként működik tovább.

## A híradótiszt-képzés jelene

A 2005-ös év, mint a 2004/2005 és 2005/2006-os tanévek metszete, számos változást hozott a mérnök és így a híradótiszt-képzés területén. Augusztus 20-án ava-

tásra került az utolsó, tanulmányait a „hagyományos” rendszerben folytató évfolyam 4 híradó hadnagya (2 ösztöndíjas, 1 kettős jogállású, 1 határőr), akik polgári villamosmérnöki diplomájukat is átvehették. (Ezen felül 2 ösztöndíjas hallgató a nyelvvizsga kritérium teljesítésének hiányában elesett a hivatásos tiszti pályától, villamosmérnöki diplomájukat azonban a nyelvvizsga bizonyítvány bemutatása után utólag átvehetik.)

Jelenleg mind a 4 évfolyam kreditrendszerű képzésben vesz részt, azaz 2006. augusztus 20.-án kerülhetnek avatásra az első, ebben a rendszerben végzett tisztek, akik a követelményrendszer teljesítése esetén átvehetik villamosmérnöki diplomájukat is. A helyzet azonban koránt sem ilyen rózsás… A végzős híradók (1071) jelenleg mindössze öten vannak és közülük mindössze egy fő rendelkezik középfokú „C” típusú nyelvvizsgával, míg többen vannak olyanok, akik az előző szemeszterek tárgyai közül egyet vagy többet nem tudtak teljesíteni. Ennek következtében kérdéses, hogy hány új hadnaggyal bővülhet a híradó szolgálat állománya. (Öröm az ürömben, hogy a testnevelés szigorlatot a tancsoport sikeresen abszolválta) A Magyar Honvédségben jelenleg számos híradótiszti beosztás betöltetlen, ami elsősorban a mögöttünk álló időszak folyamatos átszervezéseiből, létszámleépítésekből fakad. A másik - a fenti folyamatokat hátrányosan érintő - tényező, a közoktatási képzési rendszer évek óta tartó „reformja”, melynek következtében a felsőoktatásba, így a Bolyai Karra bekerülők tudásszintje, felkészültsége, évről évre csökken, ráadásul fizikai állapotuk is romlik. Mivel Egyetemünknek alapvető rendeltetése a Magyar Honvédség tiszti utánpótlásának minőségi biztosítása (megfelelő katonai, szakmai, fizikai, nyelvi és vezetői felkészültség), a lemorzsolódás a négyéves képzési idő alatt jelentős mértékűvé vált a képzés színvonalának szintentartása mellett. A hallgatói állomány felkészültségének gyengüléséhez hozzájárul továbbá a honvédségben évek óta tartó bizonytalanság, ami a katonai felsőoktatást sem hagyja érintetlenül. A fiatal tisztjelöltek motiváltsága jelentősen csökkent annak következtében, hogy a katonai pálya már rég nem nyújtja azt a biztonságot a szervezet tagjai számára mint korábban, és ami az intézménybe való jelentkezésükkor még fontos szerepet játszott. Az életpálya modell megszűnt, helyét a „felfelé vagy kifelé” elv vette át. Ez egy katonai szervezetbe szocializálódott ember számára nem nyújt megfelelő perspektívát… (Éppen ennek következtében a hallgatók szemléletében hangsúlyeltolódás tapasztalható a polgári (mérnök) diploma megszerzése iránti igény irányába, a hivatásos tiszti státusszal szemben.)



[1]

1. ábra: A nappali alapképzésben résztvevő híradó hallgatók évfolyamonkénti megoszlása

A jelenlegi helyzet vizsgálatához nézzük meg a tanszékünkön tanuló híradó hallgatók (nappali, alap) évfolyamonkénti megoszlását a 2005/2006 –os tanév 1. félévében. (1. ábra)

A 3. évfolyam kiugróan magas létszáma a Honvédség „folyamatos" átalakítására vezethető vissza, melynek egész fegyvernemek és szakcsapatok estek áldozatul. 2003- ban 10 fő került híradó szakra beiskolázásra. Ez a szám, sorozatos szakváltási kérelmek következtében az első év folyamán először 18 főre ugrott, majd az önkéntes leszerelések következtében 11 főre csökkent. Második év elején egy leszerelés és egy szakváltás következtében a létszám nem változott. Második félévben a HM visszavonta megrendelését az évfolyamon párhuzamosan tanuló RT179, REF180, és EHC181 szakos tisztjelöltekre, melynek következtében helyzetük bizonytalanná vált. Hosszas egyeztetések után az a döntés született, hogy ezek a hallgatók 3. évfolyamon híradóként folytathatják tanulmányaikat, így ma két tancsoportban 43-an tanulnak tanszékünkön, és esélyesek a villamosmérnöki diploma megszerzésére. (Így valószínűleg 2007-ben megszűnhet az ágazat tiszthiánya, sőt…)

2. évolyamon az eredetileg felvett 10 fő helyett, a tanulmányi elégtelenség miatti leszereléseket követően ma már csak 6 -an tanulnak. Jelen állapot szerint átmenetileg ők az utolsók, akik végzéskor a villamosmérnöki diplomát is átvehetik.

Végezetül ejtsünk szót az 1. évfolyamosokról, akik jelenleg katonai alapozáson vesznek részt Szentendrén az új „hadmérnök" szak tantervének megfelelően…

### Ki, vagy mi is az a „hadmérnök"[182]?

A „hadmérnök" szak indítását két független tényező együttes hatása tette „szükségessé". (Ez jelentős visszalépést jelent az évtizedeken keresztül formálódó magas színvonalú mérnökképzés történetében.)

[179] Radartechnikai
[180] Rádióelektronikai Felderítő
[181] Elektronikai Harc
[182] Had- és Biztonságtechnikai Mérnök Szak

- A Magyar Honvédség létszáma a rendszerváltás óta drasztikusan csökkent. Helyőrségek, fegyvernemek, szakcsapatok, alakulatok tömegei szűntek meg. A folyamatos leépülés következményeként a tisztek aránya a teljes állományon belül jelentősen megnőtt. A személyi összetétel torzulásában jelentős szerepet játszott a sorkatonaság megszűnése, illetve az hogy a tiszti kar létszáma lényegesen lassabban csökkent a többi állománykategóriához képest. A folyamat megállítására csak az elmúlt években történtek lépések, melynek következében a fent említetett arány ismét 20% alá csökkent. Ezen lépések következtében a tiszti, és ezen belül a mérnöktiszti beosztások száma (a Magyar Honvédség mérnöktiszti utánpótlás igénye) lényegesen csökkent, a humánerőforrás gazdálkodás hosszú távú tervezése (4 év) nehézkessé vált. (A tiszti létszámigények a fegyvernemek és szakcsapatok részéről csak 1-2 évre előre határozhatók meg.) Ezen anomália megoldására alapította az egyetem a „hadmérnök" szakot, melynek sikeres akkreditációját követően idén beindulhatott az első ilyen jellegű képzés.
- Az új képzési struktúrát úgy kellett kialakítani, hogy az illeszkedjen az Európai Unió felsőoktatási rendszerének reformjába (Bolognai folyamat), amely a háromszintű lineáris képzés (BSc, MSc, PhD) megvalósítását tűzte ki célul. Bár a „hadmérnök" szak a fenti kritériumot teljesíti, ezért nagy árat kell fizetni…

A „hadmérnök" se nem villamosmérnök, se nem gépészmérnök, se nem közlekedésmérnök, se nem vegyészmérnök, se nem építőmérnök, se nem műszaki informatikai mérnők, se nem biztonságtechnikai mérnök, így a korábbi gyakorlattal ellentétben, a polgári életben is elismert diplomát nem kap. A felsorolt szakok diplomái azonban nem csak nevükben jelentenek többet, mint a „hadmérnöki" diploma…

Az új rendszerű képzésre való áttérés úgynevezett „kompromisszumok árán" valósulhatott meg, melynek következtében a szakmai vonal drasztikusan gyengült a korábbiakhoz képest:

- - Az új képzés bevezetésének alapvető indoka az állandóan változó honvédelmi politika által gerjesztett humánerőforrás-gazdálkodási problémák enyhítése volt, így az új struktúrában jelentősen csökken differenciáltság az egyes szakirányok között. Ennek következtében éppen azon speciális ismeretanyagok aránya csökken jelentősen a tanagyagban, amire az egyes szakcsapatoknak szakszolgálatoknak a legnagyobb szüksége lenne… (Nem biztos, hogy a hadseregnek „univerzális mérnök tisztekre van szüksége…)
- - A probléma ugyanakkor nem a speciális tantárgyak szintjén jelentkezik először, hanem már a természettudományos és mérnöki alapozás során, hiszen például egy híradó-, fegyverzettechnikai-, vegyivédelmi-, vagy műszaki tisztnek („szakmérnökök") eltérő tananyagra van szüksége (mennyiségi és minőségi különbségek!!!) későbbi tanulmányainak megalapozásához matematikából (vektoranalízis, mátrixelmélet stb.), fizikából (elektronika, optika, mechanika, statika stb.), kémiából (szerves, szervetlen), vagy akár számítástechnikából.
- - Bár sokan azt feltételezik, hogy a katonai jelleg erősödött (a szakmai rovására), ez csak részben lehet így. A katonai és szakmai képzés időben történő, ilyen mértékű kettéválasztásával a 4. év végére jelentősen leromlik a katonai oldal hatékonysága is, hiszen a jelenlegi alapkiképzés (amit a magas színvonal ellenére elvettek az Egyetemtől) legfeljebb az éppen bevonulóknak (1. évf.) jelenthet többle-

tet, míg a másodévfolyamosok parancsnoki tevékenységének gyakoroltatása jelentős csorbát szenved.

(Ezeket a problémákat elsősorban azok veszik észre, akik folyamatosan részt vesznek a képzésben, tisztában vannak a hallgatók, oktatók, és a rendszer nehézségeivel…)

## Ki a megrendelő?

A megrendelő általánosságban a Magyar Honvédség. A kérdés arra vonatkozik, hogy a szervezeten belül ki dönti el, mire is van szükség?

A HM Humánpolitikai Főosztály álláspontja szerint a „hadmérnök"-képzésnek kell biztosítania a szükséges mérnöktiszti utánpótlást.

A HM HVK Katonai Tervező Főcsoportfőnökség, mint a végzetteket beosztásba helyező, illetve alkalmazó szakmai főnökség (Híradó Osztály) továbbra is villamosmérnökökkel kívánja megoldani azt.

Így már érthető a kérdés, amire a válasz véleményem szerint egyértelmű: a magrendelő az, aki a végzett tisztek tudását hasznosítani kívánja annak érdekében, hogy a Magyar Honvédség maradéktalanul meg tudjon felelni hazai és nemzetközi követelményeknek, a politikai, társadalmi, és szakmai elvárásoknak, és feladatait maximális eredményességgel hajtsa végre.

## Összegzés

A „hadmérnök"-képzés visszalépést jelent az eddigi gyakorlathoz képest, és legfeljebb csekély mértékben felelhet meg a Karral szemben támasztott szakmai elvárásoknak, nem kompatibilis egyetlen más képzéssel sem. Ha a megrendelő felé a kibocsátandó tisztek eddigi szakmai felkészültségét biztosítani szeretnénk, azt a végzést követően csak számos különböző „továbbképző" tanfolyammal tudjuk biztosítani, ami jelentős többletterhelést jelent az oktatói állománynak, többletkiadást a megrendelőnek.

Amennyiben az egyetlen figyelembeveendő szempont az volt, hogy megkönnyítsük a beosztásba helyezést, a minisztérium humán erőforrás gazdálkodását, ez kétségtelenül sikerült. Sőt ezzel a struktúrával elérhető a leendő mérnöktisztek Honvédség iránti kötődésének (kiszolgáltatottságának) erősítése is, hiszen a „hadmérnök" diplomát a hadseregen kívül sehol nem fogadják el... Ez azért jelent problémát, mert a Hivatásos Katona már nem életpálya, nem „nyugdíjas állás". Az új szakon végzettek jelentős hátrányba kerülhetnek a munkaerőpiacon, egy-egy újabb „átszervezést" követően. Amennyiben a honvédség fenntartja eddigi humánpolitikai elgondolását, miszerint a rendszerből kikerülők át, ill. továbbképzését, a civil munkaerőpiacra történő beilleszkedését biztosítani kell, el kell gondolkodni, hogy anyagilag nyertünk-e annyit a „hadmérnök"-képzéssel, mint amennyit a későbbiekben elveszthetünk a folyamatos át és továbbképzésekkel.

## Alternatíva?

A cikk születésekor még nem lehet tudni, hogy a MAB183 elfogadja-e a beadott szakindítási (köztük a villamosmérnöki) kérelmeket. Ez a döntés azonban jelentős hatással lesz a mérnök-, elsősorban a híradótiszt-képzés jövőjére. Pozitív döntés

[183] Magyar Akkreditációs Bizottság

esetén a 2006/2007-es tanévben a Karon folytatódhat villamosmérnök-híradótisztek képzése, míg az elutasítás jelentős problémákat okozhat az utánpótlás biztosításában. Ebben az esetben ugyanis a 74-éves múlttal rendelkező híradótiszt-képzés eltűnhet az ZMNE repertoárjából, amennyiben a szakmai elöljáróság ragaszkodik a villamosmérnökökhöz, és azokat a polgári felsőoktatásból (BME) rendeli meg. Ez a megoldás azonban újabb kérdéseket vet fel:

- A villamosmérnök nem csak Magyarországon, hanem az egész világon hiányszakma (azaz folyamatosan több betöltetlen állás van, mint szabad kapacitás)
- A villamosmérnökök óriási, sehol máshol meg nem szerezhető szellemi kapacitást képviselnek („mérnöki gondolkodásmód" ~ logika, problémamegoldó képesség…)
- Az előző két pontból következik, hogy a villamosmérnöki tudás árfolyama rendkívül magas a munkaerőpiacon, ami felveti a kérdést, hogy milyen feltételekkel, milyen anyagi ellentételezéssel, juttatásokkal lehet egy polgári felsőoktatási intézményben szocializálódott, például a BME által kiállított diplomával rendelkező szakembert rávenni arra, hogy egy olyan szigorú szabályok szerint működő szervezet „parancsuralmi" rendszerébe lépjen, mint a Magyar Honvédség. Megoldást jelenthetne a jelenleg kifutóban lévő ösztöndíj rendszer, aminek lényege, hogy polgári felsőoktatási intézményekben tanuló másod/ harmadéves hallgatókkal ösztöndíjszerződést köttetnek, ezzel lekötve őket a munkaerő piacon (a szerződésben rögzített időtartamra). A jelenlegi tiszti fizetések mellett, figyelembe véve a szakmai, ill. rendfokozati előmenetel erősen korlátozott lehetőségeit, összevetve a honvédség által elvárt ellenszolgáltatásokkal („…életem árán is megvédem!"), finoman szólva is kétséges a „küldetés" kimenetele. (A bizonytalanságot az jelenti, hogy öt vagy tízévente találnak egyetlen olyan villamosmérnököt, aki hajlandó lenne pusztán hazaszeretetből lemenni Hódmezővásárhelyre híradó szakaszparancsnoknak a féléves katonai alapkiképzést és a több hónapos szakkiképzést követően. Valószínűleg a szerződést korábban aláírók diplomával a zsebükben inkább a szerződésbontást választják.)

### Megoldás?

A Kar és így a Híradó Tanszék a folyamatos leépítések ellenére még mindig alkalmas a differenciált „szakmérnök" képzés feladatainak ellátására, ami elsősorban az egyetem és a kar vezetésének, a magasan kvalifikált, tapasztalt, a tiszti pályát és a tanítást hivatásnak tekintő oktatói állománynak és a szakmai főnökségeknek köszönhető. Így a BSc mérnök szakok akkreditálása esetén a megrendelő szakmai elöljáróságok maguk dönthetik (dönthetnék) el, hogy leendő tisztjeik „hadmérnök" vagy „szakmérnök" (esetünkben villamosmérnök) képzésben vegyenek részt…

### Megoldás!!!

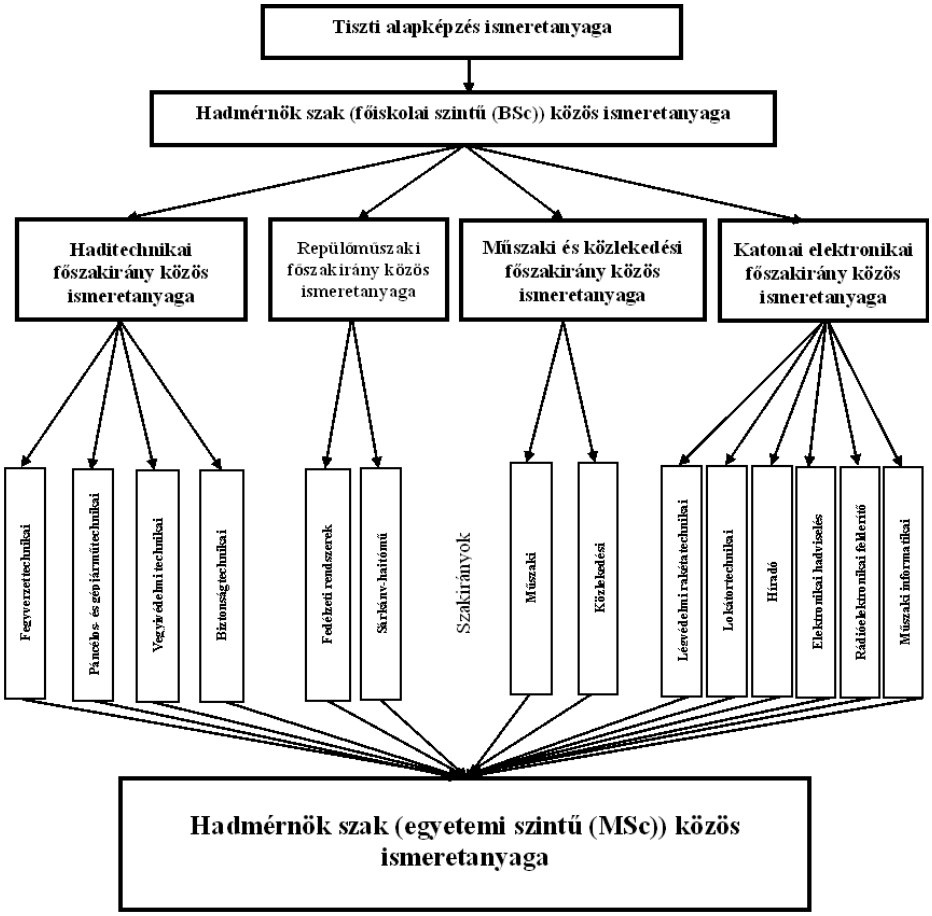
A cikk leadása előtt a Híradó Osztály engedve a nyomásnak, a szakmai érvek ellenére hozzájárult a híradó hallgatók „hadmérnök" szakon történő képzéséhez…

### Felhasznált irodalom:

[30] www.bjkmf.hu
[31] JAKUS János: Magyar Honvédség – a rendszerváltástól napjainkig - Új honvédségi szemle LIX. Évfolyam 2005/7.

[32] Dr. KOCZKA Ferenc: Változó honvédség, átalakuló mérnöktiszt-képzés – Kommunikáció 2003
[33] Dr. habil SÁNDOR Miklós: Új kihívásokra –új válaszok?! – Kommunikáció 2003
[34] RÉVÉSZ Gyula - Dr. habil SÁNDOR Miklós: A híradó képzés az átalakítás tükrében – Kommunikáció 2004
[35] A honvédelem négy éve 1998-2002
[36] NAGYNÉ Jakab Sára – GÁL Anna: Helyzetkép a magyar és katonai felsőoktatás átalakításáról - Új honvédségi szemle LIX. Évfolyam 2005/8.
[37] a zmne bjkmfk főigazgatójának jelentése a kar 2001/2002. tanévben végzett munkájáról
[38] a zmne bjkmfk főigazgatójának jelentése a kar 2002/2003. tanévben végzett munkájáról
[39] a zmne bjkmfk főigazgatójának jelentése a kar 2003/2004. tanévben végzett munkájáról

**Melléklet:**




A had- és biztonságtechnikai mérnök szak képzési szerkezete [3]

**Dr. PÁNDI Erik**

# A KORMÁNYZATI KOMMUNIKÁCIÓT KISZOLGÁLÓ RENDSZEREK LEHETSÉGES INTEGRÁCIÓJA[184]

A szakterületet érintő korábbi vizsgálódásaim alapján a magyar kormányzati távközlés fejlődési szakaszait a következőképpen határoztam meg:

- I. 1967. október 19-től 1989. december 31-ig terjedő időszak:

  a Magyar Forradalmi Munkás-Paraszt Kormány 3343/1967. sz. határozatának kiadása és a távközlésért is felelős egységes Magyar Posta fennállása közötti időszak;
- II. 1990. január 1-jétől 2004. január 8-ig terjedő időszak:

  a Magyar Távközlési Vállalat, a Magyar Műsorszóró Vállalat (majd a koncessziós távközlési szervezetek) megalakulása és az Elektronikus Kormányzati Gerinchálózat (EKG) jogszerű működésbe lépése közötti időszak;
- III. 2004. január 9-től terjedő időszak:

  az EKG jogszerű működésbe lépése az 5/2004. (I.9.) Korm. rendelettel kihirdetett EKG Hálózat Használati Szabályzat és Informatikai Biztonsági Szabályzat hatályba lépésétől.

A jelzett időszakban a kormányzati távközlés nem volt egységes. A kormányzat fogalmát a közigazgatás felé szélesítve úgy értelmezhető, hogy a kormányzati távközlés mai fő összetevői a következő rendszerek:

- Elektronikus Kormányzati Gerinchálózat (EKG);
- a kiépülő Egységes Digitális Rádiótávközlő Rendszer (EDR);
- Egységes Belügyi Digitális Hálózat (EBDH);
- MH Hálózata;
- Közháló.

Korábban jellemezve ezek mindegyikét, feltárva mind a hazai, mind a nemzetközi (NATO, EU) kapcsolódási pontokat, helyénvalónak és időszerűnek látszik feltenni a következő két kérdést:

1. Szükség van-e egységesítésre a kormányzati távközlést megvalósító (kiszolgáló) kommunikációs rendszerek körében?

2. Miként lehetséges megoldani az egységesítést?

Az eddigi vizsgálatok alapján kialakított álláspontom szerint minden felmerült körülmény azt igazolja, hogy célkitűzésként megfogalmazható az integráció, vagyis a kormányzati kommunikációs rendszer egységességének kialakítása, mivel jelenleg a kormányzati távközlés technológiai, jogi és megfelelőnek tekinthető gazdasági környezete egyrészt elősegítheti az integrációt, másrészt ki is kényszerítheti azt.

[184] Pándi Erik r. alezredes: BM Távközlési Szolgálat főosztályvezető-helyettes. A szerző a ZMNE Katonai Kommunikációs Rendszerszervező Tanszék (jelenleg: Híradó Tanszék) által rendezett korábbi nemzetközi szakmai tudományos konferenciákon (2003-ban és 2004-ben) a kormányzati távközlés korabeli (1967-1989) és napjainkban fennálló (1990-2004) helyzetéről már adott elemzést

## 1. Az integráció szükségessége

Az integráció szükségességének vizsgálatánál kiindulópontként rögzíteni kell, hogy hazánkban a kormányzati igényeket kiszolgáló elkülönült rendszerek működésének és fenntartásának mély hagyományai vannak, amelyek kezdetei a múlt század ’40-es éveihez vezethetők vissza. A saját rendszerek tekintetében természetesen az irányítás kérdése a döntő, mivel a kormányzati és ágazati szereplők csak akkor tekintenek magukénak egy rendszert, ha a vele kapcsolatos folyamatok alakulására jelentős és érdemi befolyásuk lehet, ahogyan azt általában az irányítással kapcsolatosan Dr. Mráz István185 meg is fogalmazza: „Az irányítás célját legáltalánosabban a […] jogszerű működésnek átfogó és teljes körű biztosítása, továbbá a működéshez szükséges feltételekről való gondoskodás adja. Az irányítás lényege tehát az […] akaratérvényesítés a […] működés fölött.” [1].

A kormányzati távközlést önálló kommunikációs rendszer sem az 1967-1989, sem az 1990-2004 közötti időszakban nem szolgálta ki. Az igényeket a különböző államigazgatási szervek rendszerei és a hazai kommunikációs rendszerek egyéb szegmensei elégítették ki. 1989-ig ezek az egyéb szegmensek is állami irányítás alatt álltak, azonban 2004-re fokozatosan a hírközlési szektor piaci szereplőivé alakultak át. Kormányzati részről 1989-ben döntő többségében csak a belügyi és honvédelmi ágazat szervei vettek részt a megvalósulásában, azonban 2004-ig ez a szám fokozatosan emelkedett, így tehát újabb megválaszolandó kérdésként merülnek fel a hálózatok bővülésének, mint jelenségnek az okai.

A bővülés egyik okát részben a konvergenciában kell keresni. Technikai szempontból hazánkban 1989-ig jellemzően a távbeszélő, fax és géptávíró szolgáltatások jelentették a kommunikáció alapját, mivel a távközlő hálózatok technikai megoldásai e szolgáltatásfajtákat nyújtották. Az 1990-től fokozatosan megnyíló technológiai lehetőségek elsőként a hagyományos távközlő rendszereket modernizálták, miközben megjelentek a különböző számítástechnikai és informatikai rendszerek és azokat összekötő – az első időkben még – elkülönülő hálózatok. Az informatika térhódítása révén a hagyományos kommunikációs szolgáltatások köre is bővült186 és elsősorban a piaci szereplők körében kezdődött meg olyan – a két ágazatra épülő adatkommunikáció mindazon termékeit és szolgáltatásait magukba foglaló – intelligens kommunikációs rendszerek kialakítása, amelyek elsősorban a személyek és szervezetek közötti kapcsolattartás és együttműködés, valamint az információkhoz való távoli és gyors hozzáférés lehetőségét támogatják.

A kormányzat indirekt úton, már a kezdetektől elősegítette a bővülést, hiszen az Informatikai Tárcaközi Bizottság 1991-ben történt megalakulásával prioritást kapott a kormányzati információs rendszerek modernizációja, a közigazgatás informatikai fejlesztése. Ezzel párhuzamosan az államigazgatásban is megkezdődött az egyedi szervezeti igényeket kielégítő informatikai hálózati struktúrák kialakítása. Az elmúlt évtized második felében – a konvergenciára alapozva kidolgozott információs társadalom elméletek és nemzetközi trendek alapján – hazánkban is egyre nagyobb hangsúlyt kap az elektronikus kormányzat, mint hatékonyabb hatalomgyakorlási és államigazga-

185 Dr. Mráz István vezérőrnagy a publikáció közlésének időszakában a HM HVK Hadműveleti és Kiképzési Csoportfőnökség csoportfőnöke volt

186 e-mail, ftp, telnet, stb.

tási forma, amelynek középpontjában a szolgáltató állam koncepciója áll. A szolgáltató állam elektronikus ügyintézés187 formájában is lehetővé kívánja tenni a közszolgáltatások igénybevételét, ezért a közigazgatás szereplőivel szemben is – uniós csatlakozásunk óta fokozottabban – egyre hangsúlyosabb kormányzati elvárás, hogy tevékenységük során alkalmazzák a korszerű elektronikus informatikai és kommunikációs eljárásokat. Nagykiterjedésű hagyományos, saját irányításban levő távközlő rendszerekkel csak a honvédelmi és belügyi ágazat rendelkezett és rendelkezik. A többi ágazat – az alapinfrastruktúra hiánya miatt – informatikai rendszerei működtetéséhez szükséges hálózatai elemek (összeköttetések) biztosítását saját technikai erőforrásokra alapozni nem tudta, ezért az elmúlt évtizedben fokozatosan jelentek meg a sajátos ágazati célokat szolgáló, egymástól elkülönülő – a hírközlési szolgáltatók által bérbe adott összeköttetésekre épülő – informatikai hálózatok.

A bővülési folyamatok irányait és azok – nem minden esetben kedvező – hatásait a kormányzat is viszonylag korán, az elmúlt évtized elején már érzékelte, azonban az a közvetlen beavatkozó- és manőverező-képessége, amely az állami vállalatok irányítása terén 1990 előtt megvolt – a szabályozási környezet átalakulásával – teljesen elveszett. Ez egyúttal azt is jelentette, hogy a kormányzati távközlés területén az erős koordináció révén 1990-ig összetartott kvázi önállónak is tekinthető hálózat legfontosabb elemének188 folyamataiba az újonnan kialakuló piaci környezetben már csak kizárólag hatósági szervezetrendszere révén, sokkal szabályozottabb és ugyanakkor korlátozottabb módon, gazdasági alapon tud beavatkozni. Az közvetlen irányítás alól kikerült közcélú189 szegmens pótlására, a még saját irányításban levő rendszerekre alapozva190 a kormányzat a ’90-es évek második harmadától több koncepciót dolgozott ki, de különböző okok miatt egyik terv (EKZH, KTR és KODNET) sem került megvalósításra. Az elkülönülő informatikai hálózatok elterjedési folyamatának eszkalálódása így visszavezethető a megfelelő alternatíva hiányára is. A hálózatok számának és kiterjedtségének bővülése egyúttal azt is jelenti, hogy az irányítás rendszere is egyre tagoltabbá válik, ami természetesen nem segíti elő a központi elképzelések gyors és hatékony megvalósítását.

Az 1998-ban megjelent hírközléspolitikában az informatikai hálózatok bővülése, a párhuzamosságok és az irányítás felismert problémájának helyes megoldása stratégiai feladatként került megfogalmazásra. A kormányhatározat a központosítás mellett, a párhuzamok ellen lép fel. Az egyes célkitűzések sikeres megvalósulásának hiányára utal, hogy néhány évvel később a 1077/2004. (VII.22.) Korm. határozat191 megbízta a „…Miniszterelnöki Hivatalt vezető minisztert, hogy az Elektronikus Kormányzat Központ útján vizsgálja felül a kormányzaton belül jelenleg használt zártcélú (és különcélú) hálózatok technikai megoldásait, megvalósításuk hatékonyságát, és tegyen

187 amelyre példa a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény, vagy az elektronikus közigazgatási ügyintézésről és a kapcsolódó szolgáltatásokról szóló 184/2004. (VI.3.) Korm. rendelet is

188 a Magyar Posta hálózatai

189 az egykori távközlési törvény terminológiája szerint

190 elsősorban a BM-re és HM-re, amely az EKZH koncepciókban meg is jelenik

191 amelyet az egységes digitális rádiótávközlő rendszer (EDR) kialakításával, valamint az EDR szolgáltatás vásárlásával kapcsolatos feladatokról szóló 1053/2005. (V.26.) Korm. határozat 16. pontja hatálytalanít

javaslatot ezek ésszerűsítésének felgyorsítására az elkészült Elektronikus Kormányzati Gerinchálózatra támaszkodva, összhangban az EDR készenléti rendszereivel;" [2]. A Miniszterelnöki Hivatal által készített és 2005 elején összegzett felmérés eredménye alapján a zártcélú távközlő hálózatokon túlmenően – az államigazgatási szervek által más-más technikai és gazdasági konstrukcióban fenntartott – mintegy 30 (!) különböző szolgáltatási és technológiai színvonalon álló, de országos kiterjedésű hálózat került regisztrálásra.

A távközlési törvény felhatalmazása alapján a zártcélú távközlő hálózatok működését és egyéb fontos kérdéseit szabályozó kormányrendelet teremtett olyan jogi környezetet, amely lényegében véve sikerrel tette lehetővé a kormányzati és államigazgatási igényeket kiszolgáló kommunikációs rendszerek fenntartói számára az első és második időszak közötti átmenet lehetőségét, valamint jelenleg is biztosítja a jogszerű és stabil működési feltételeket. Ugyanakkor a jogszabályban meghatározott hálózatgazdák és a felügyeletükben létesíthető önálló hálózatok – viszonylag magas – száma nincs összhangban a párhuzamok megszüntetésével, a központosítással, valamint a hatékonyság és ésszerűség növelésével, mint kormányzati stratégiai követelményekkel.

A nyilvánvaló jogszabályi lehetőség folytán tehát az önálló zártcélú hálózatok irányítása a centralizációs elképzelésekkel szemben továbbra is megosztott maradt,[192] így ezt a jelenséget a kormányzat a koordinációs folyamatok hatékonyságának fokozásával kísérli meg ellensúlyozni.[193] A hatékonyság növelése elsősorban abban nyilvánult meg, hogy a Miniszterelnöki Hivatal szervezetében kialakításra került egy „szakmai centrum",[194] amelynek működése a 148/2002. (VII.1.) Korm. rendelettel tovább erősödött. A jogszabály a szaktárca feladatköréből a kormányzati informatikáért való felelősséget a MeH miniszter hatáskörébe utalta. A centrum működése ellenére az önálló rendszerek fenntartásának hagyománya nem tűnt el, hiszen sem – a távközlési törvényt felváltó – hírközlési törvény, sem az azt követő elektronikus hírközlési törvény nem kísérli meg megváltoztatni, illetve megszüntetni a „zártcélú hálózatok" jogi kategóriát. Ez egyértelműen azt jelenti, hogy a kormányzat továbbra sem kíván lemondani a kormányzati távközlést kiszolgáló saját rendszerek folyamatai feletti irányítás lehetőségéről.

Visszatérve az önálló kommunikációs hálózatok számarányai növekedésének jogosságára, le kell szögezni, hogy az ágazati szervek szemszögéből a bővítések végrehajtása teljes mértékben szükségszerű és ennél fogva indokolt volt, hiszen az elektronikus kormányzás megvalósításával kapcsolatos elvárások mellett a kormányzatok a zártcélú hálózatgazdáknak 2004. január 8-ig nem kínáltak gyakorlati alternatívát az informatikai rendszerek – közcélú szolgáltatások igénybevétele nélkül történő – összekapcsolási problematikájára.

---

[192] mivel az adott zártcélú kommunikációs rendszert felügyelő hálózatgazda köteles biztosítani a működési feltételeket, ez azt is jelenti egyúttal, hogy jogot formálhat a fenntartás és fejlesztés kérdéseinek a sajátos szervezeti érdekek mentén történő rendezésére

[193] az irányítási problémák koordinációs tevékenységgel való fokozásának megoldása ugyanakkor a központi kormányzat számára egy kedvező lehetőség arra is, hogy a forráshiányos finanszírozásból eredő problémák rendezési kényszerét a szaktárcákhoz delegálja

[194] 2000-ben: Informatikai Kormánybiztosság; 2002-ben: Kormányzati Informatikai és Társadalmi Kapcsolatok Hivatala, 2004-től: Elektronikuskormányzat-központ

Az EKG működése új szakaszt nyitott a kormányzati távközlés történetében, mert lezárt egy olyan korszakot, amelynek alapvető jellemzője volt, hogy a terület irányításában fajsúlyos szerepet – a központi kormányzat koordinatív tevékenysége mellett – a zártcélú távközlő hálózatok gazdái töltöttek be. A központi szinten működő szakmai centrum (jelenleg: EKK) befolyását egyrészt adminisztratív eszközökkel erősíti,195 másrészt saját hálózat kialakításával és irányításával biztosítja a szükséges műszaki feltételeket, vagyis megoldási alternatívát kínál a párhuzamosságok tényleges felszámolásának végrehajtására. Némileg ellentmondásosnak tűnhet, de az új szakasz kialakulását elsősorban a konvergencia segítette elő, hiszen a mindenfajta híranyagtípus továbbítására képes intelligens kommunikációs rendszerek megjelenése napjainkra már feleslegessé teszi a távközlő és informatikai rendszerek (és szolgáltatások) fizikai és funkcionális megkülönböztetését, tehát a különállás fenntartását. Az 1990-2004 közötti szakaszt tehát akár az akkumulálódás időszakaként is jellemezhetjük, mivel napjainkra kialakult a lehetősége annak, hogy ismét visszatérjünk az 1989-ben kvázi önállóként jellemezhető, kevés szereplővel és erős kormányzati irányítás alatt állóként, a kor elvárásaihoz igazodó szolgáltatás-nyújtási képességekkel jellemzett, de magasabb technológiai színvonalon álló struktúrához.

A konvergencia és hatásai természetesen befolyásolják a két legnagyobb zártcélú távközlő hálózattal rendelkező ágazat műszaki-technikai átalakítási folyamatait is, amelyek a saját rendszeren belüli informatikai és távközlő alrendszerek technológiai integrációját tűzték ki végső célul. E mellett a belügyi ágazat megfogalmazta és rögzíti az ágazati zártcélú távközlő hálózaton belül jelenleg fennálló szervezeti megosztottság felszámolásának szükségességét és elvét is, kijelentve,196 hogy: „…a belügyi szervek távközlési ellátásával kapcsolatos műszaki-technikai és anyagi-pénzügyi tevékenységeket költséghatékonyan, centralizáltan kell megszervezni…” [3], ami a katonai zártcélú távközlő hálózat esetében egyáltalán nem vet fel problémákat, mivel az irányítás és vezetés197 rendje itt mindig is erősen centralizált volt.

A fejlődéstörténet új, harmadik szakaszában a legfőbb és tényleges kihívást az elektronikus kormányzás megvalósítása jelenti. A hírközléspolitika stratégiai célul tűzte ki, hogy 2004-ig, az egyetemes szolgáltatási kötelezettség keretében az ország lakosságának minden rétege számára biztosítani kell a 64 kbit/s adatátviteli sebességű, Internethez történő hozzáférés technikai lehetőségét.198 A célkitűzés, illetve a közcélú

[195] a témakört érintő közösségi programokban való részvétel; jóváhagyási, illetve egyetértési jog az ágazatok és így a zártcélú távközlő hálózatok fejlesztéseit érintően; a zártcélú távközlő hálózatok többsége esetén a gerincirányú szakaszok viszonylatában megjelenő belépési és szerződéskötési kényszer

[196] a telekommunikációs eszközökkel történő ellátás rendjéről, valamint a távközlési és informatikai szolgáltatások igénybevételének szabályairól szóló 19/2004. (BK 14.) BM utasítás 33. pontja

[197] az irányítás és a vezetés közti alapvető különbséget az igazgatástudomány abban hangsúlyozza, hogy az irányítást végző személy az irányított szervezeten kívül – a hierarchikus kapcsolatból eredendően fölötte – áll, addig a vezető az adott szervezet csúcsán, mindenképpen azon belül helyezkedik el. A vezető a szervezet részeként gyakorol hatást annak helyzetére és tevékenységére

[198] ami lényegében 2004-re csak eltérő formában valósult meg, mivel az elektronikus hírközlésről szóló 2003. évi C. törvény 117. § a) pontja alapján a helyhez kötött előfizetői hozzáfé-

szolgáltatóknál már megvalósult technikai feltételek előrevetítik, hogy a lakosság egyre szélesebb köre válik képessé a kijelölt kormányzati adatbázisokhoz való hozzáférésre. A lakosság ezirányú képességeire, valamint az ehhez szervesen kapcsolható elektronikus ügyintézéshez szükséges és nélkülözhetetlen – egységes elvekre épülő – új kommunikációs megoldások, valamint a hitelesség biztosítására199 kell tehát elsődlegesen felkészülni. A jövőben a kormányzati távközlést kiszolgáló kommunikációs rendszernek már nem csak a korábban tisztázott fogalom szerinti kör kommunikációs igényeit, hanem a lakosság részéről jelentkező és fokozódó igények kielégítését is szolgálnia kell.

Másodsorban, további megoldandó probléma a vizsgált kommunikációs rendszerek azon hiányosságai, amelyek nem teszik lehetővé, hogy az államigazgatás helyi szervei rendszerbe történő integrálása közvetlenül állami infrastruktúrán keresztül oldódjon meg. Ez teszi szükségessé a Közháló program működtetését és kiterjesztését a helyi szervek körében.

Harmadsorban, ki kell használni az intelligens kommunikációs rendszereknek azon képességét, amely lehetővé teszi mindenféle híranyag továbbítását és a kormányzati távközlés hatókörében, egységesen, országos szintre kell kiterjeszteni a hagyományos kommunikációs szolgáltatásokat.

A fejezet elején feltett első kérdésre, miszerint: Szükség van-e egységesítésre a kormányzati távközlést megvalósító (kiszolgáló) kommunikációs rendszerek körében? – a válasz eddigi vizsgálataim és elemzésem alapján egyértelműen csak igenlő lehet. Az integrációt alátámasztó érvek, elősegítő lehetőségek és körülmények:

- a kormányzati munka minőségét jelentősen befolyásolhatja a kormányzati távközlést kiszolgáló kommunikációs rendszerek helyes megszervezése és irányítása. A vizsgált időszakokban – elsősorban a II. szakaszra vonatkozóan – a törvényi változások ellenére a zártcélú távközlő hálózat, mint kategória továbbra is hatályos, tehát a hálózatok jogszerűen funkcionálnak jelenleg is. A saját rendszerek hagyományait is figyelembe véve, a mindenkori kormányzat tehát nem mond le irányítási lehetőségeiről, így tehát nem célja a zártcélú hálózatok megszűntetése, de a hatályos ágazati stratégia alapján a párhuzamok megszüntetése, a központosítás, valamint a hatékonyság és ésszerűség növelése igen, amelynek végrehajtására saját hatáskörben is lehetősége van alsóbb fokú jogszabály módosítása révén;
- a hatékonyabb központi irányítás céljából szakmai centrum jött létre. Adminisztratív úton megkezdődött a zártcélú hálózatok részleges integrációja. A szakmai centrum a kormányzati kommunikáció területét érintő közösségi programokban egykapus rendszerben képviseli az országot, illetve indirekt módon a zártcélú hálózatok fejlesztését képes befolyásolni egyetértési, illetve jóváhagyási jogának gyakorlásával;
- hazánkban lezajlott egy technológiai szemléletváltás és mind a közcélú, mind a rendészeti és katonai zártcélú rendszerek tekintetében megindult az integrált kommunikációs rendszerek kiépítése. A zártcélú hálózatok átalakítását elősegítheti a tényleges verseny hírközlési piacon történő megindulása is. A rendészeti és katonai távközlő hálózatok tekintetében – a fejlesztések eredményeképpen – erős

résí ponton keresztül történő legalább 9,6 kbit/s sebességű, 1/10.000 bit hibaarányú Internet hozzáférés már egyetemes szolgáltatásnak minősül

[199] PKI – kormányzati elektronikus aláírás rendszer

belső centrális működés, illetve annak elérése irányába ható folyamatok figyelhetők meg;

- az elektronikus kormányzás és az elektronikus ügyintézés bevezetése révén fel kell készülni a lakosság szélesebb körben történő kiszolgálására, amely egységes elvekre kell, hogy támaszkodjon.

## 2. Megvalósítási irányok

Az előző fejezetben megfogalmazott válasz alapján a másodikként feltett kérdés, azaz Miként lehetséges megoldani az egységesítést? – megválaszolása előtt célszerű – a kommunikációs rendszer első fejezetben rögzített definícióját is szem előtt tartva – röviden áttekinteni és kitűzni a megvalósítás lehetséges irányait.

Ehhez kapcsolódóan, a rendszerek fejlesztésével és átalakításával összefüggésben Dr. Szücs Ervin200 általánosságban úgy vélekedik, hogy a rendszerszemléletű gondolkodás: „…nem csak (nem is elsősorban) a meglevő rendszerek részekre (végső soron elemekre) bontásához, az elemek rendszerezéséhez, a rendszer belső és külső kapcsolatainak feltárásához, a sokféle vizsgálati szempont (tudományközi együttműködés) lehetőségeinek és szükségességének felismeréséhez szükséges, hanem ahhoz, hogy meglevő elemekből az új igényeknek megfelelő és a környezettel összhangban levő rendszereket tudjunk összeállítani. […] A meglevő rendszerek működtetése – valamilyen meghatározott szempont szerint – optimális üzemviszonyok között szükségessé teszi egyes részek megújítását, esetleges cseréjét. […] A társadalom fejlődése miatt nemcsak a rendszer működésével szembeni követelményértékek, hanem még a – már többször említett – biztonsági tartomány is változik. A „változatlan" technikai rendszer általában – a környezet szakadatlan változása miatt – elavul, használhatatlanná válik, tehát: relative visszafejlődik. […] A rendszerelemzés következtetései – mindezek miatt – nem egyszeriek, örökérvényűek, hanem olyanok, amelyeket időszakonként felülvizsgálni, a környezeti feltételek változása és a rendszer egyes részeinek (erkölcsi és anyagi) kopása miatt módosítani kell. Ez pedig annyit jelent, hogy még a meglevő rendszerek működtetése is szükségessé teszi az állandó megújítást, a részek cseréjét, a használati mód fejlesztését, illetve új rendszerek létrehozását." [4]

Fentieket alapul véve, megítélésem szerint a kormányzati távközlés egységesítése folyamán a megvalósítás – elméleti alapvetésem szerint – történhetne új rendszer kialakításával, a részrendszerek teljes összevonásával, a részrendszerek részleges összevonásával, vagy ezek célszerű kombinációjának alkalmazásával.

### 2.1. Új rendszer kialakítása

Az értekezés által vizsgált időszakot áttekintve, a kormányzati távközlés teljes vertikumát átfogó és kiszolgáló új rendszer kiépítésére soha nem került sor. Ennek egyik okát egyértelműen hazánk gazdasági helyzetében kell keresni, hiszen mind az első, mind a második fejlődési szakaszban technikai és szervezési tervek, valamint kormány-előterjesztések is készültek a rendszerek részleges (kormányhíradás), illetve teljes (EKZH, KTR, illetve KODNET és TETRA) átalakítására. Ezek lényegében a szükséges financiális erőforrások hiányában maradtak megvalósítatlanul. Második okként említhető, hogy – az egységes rendszer hiányában – az elsősorban sajátos szer-

[200] Dr. Szücs Ervin nyugalmazott egyetemi tanár, 1996-ig az Eötvös Loránd Tudományegyetem Természettudományi Kar Általános Technika Tanszékének volt a vezetője

vezeti érdekek alapján külön-külön létesített és folyamatosan fejlesztett kommunikációs hálózatok műszaki-technikai paraméterei és szolgáltatásnyújtási képességei egyszerre soha nem süllyedtek olyan minőségi színvonal alá, amely már komolyan hátráltatta, illetve lehetetlenné tette az egyes államigazgatási szervek alaptevékenységét, és ezáltal indokolttá tette volna egy teljesen új, komplex rendszer kialakítását.

Figyelembe véve, hogy az előző alfejezetekben megvizsgált rendszerek technikai mutatóikat tekintve napjainkban is korszerűnek tekinthetők, így nem látom sem indokát, sem reális lehetőségét annak, hogy egy nagyobb volumenű[201] beruházással új, egységes kormányzati kommunikációs rendszer jöjjön létre az országban.

Összességében tehát a megvalósítás ezen iránya hazánkban jelenleg nem tekinthető alternatívának, bár a megoldás alkalmazása hosszútávon egyértelmű, tiszta technikai és szervezeti viszonyokat eredményezne.

### 2.2. A rendszerek teljes összevonása

A kommunikációs rendszer definícióját figyelembe véve, a teljes összevonás annyit jelent, hogy a rendszert alkotó elemek mindegyike egy államigazgatási szerv[202] irányítása alá kerül, vagyis ez a szerv gondoskodik a továbbiakban a jogszerű működés átfogó és teljes körű biztosításáról, valamint a működéshez szükséges feltételek megteremtéséről. Az összevonás során az alábbi elemek válnak érintetté:

- a technikai rendszerek;
- az irányításért, üzemvitelért és fenntartásért felelős személyek és szervezetek;
- a különböző szervek és rendszerek közötti információátvitel biztosítására létrehozott szervezetek;
- a szervezési intézkedések együttese.

Az előzőekben rögzítettem, hogy az egységesítés során az EKG, (várhatóan az EDR is), az EBDH, valamint a Közháló tulajdonságaik, jellemzőik és helyzetük folytán alapját képezhetik a megvalósításnak, míg az MH Hálózatát speciális vonásai miatt csak részlegesen javasolt az egységesítési folyamatba bevonni. A megvalósítást ténylegesen elősegítheti az EKG-EBDH, az EBDH-Közháló, valamint az EKG-Közháló összekapcsolására vonatkozó konkrét műszaki-technikai együttműködési szándék is. [5] A teljes összevonás azonban alapvetően az MH Hálózata miatt válik kétségessé, hiszen a Kormány védelmi igazgatási feladatai mindenképpen megkövetelik a katonai kommunikációs rendszerek egyes – főként technikai – elemeinek bevonását a kormányzati távközlés megvalósulásába. E követelményt meghaladóan az MH Hálózata elemei többségének (pl.: az üzemvitelért és fenntartásért felelős személyek és katonai szervezetek, a különböző szervek és rendszerek közötti információátvitel biztosítására létrehozott katonai szervezetek) integrációja a polgári és rendészeti igazgatás rendszerébe jelentős szakmai érdekérelemmel járna.

Természetesen, amennyiben a védelmi igazgatás fenntartása és működtetése nem lenne az ország egyik stratégiai érdeke,[203] úgy a teljes összevonás végső célként megfogalmazható lenne az EKG, az EBDH, a Közháló és az EDR rendszerek tekintetében.

---

[201] nézőpontom szerint ennek nagyságrendje több tízmilliárd forint lenne

[202] e szervnek nézőpontom szerint mindenképpen az állami hierarchia csúcsán levő központi államigazgatási szervnek (minisztériumnak, főhatóságnak) kell lennie

[203] amelyet lényegében a Magyar Köztársaság biztonság- és védelempolitikájának alapelveiről szóló 94/1998. (XII.29.) OGY határozat rögzít

Figyelembe véve azonban fentieket, rövidtávon szintén nem lehet jó alternatíva a megvalósítás ezen útjának kiválasztása.

### 2.3. Részleges összevonás, virtuális önállóság

A részleges összevonás alkalmazását alapvetően akkor tartom jó megoldásnak, amikor az egyes kommunikációs rendszerek alkotó elemeinek egy részét valamilyen oknál fogva nem lehet, vagy nem célszerű összevonni.[204] A részleges összevonás során tehát mérlegelni kell, hogy az egyes elemek integrációja, illetve önállósága milyen mértékben segíti elő vagy hátráltatja az egységes kommunikációs rendszerrel szemben támasztott elvárások megvalósulását, a vele szemben támasztott követelmények teljesülését. A rendszer összevonásra nem kerülő elemei számára a módszer előnye abban jelentkezik, hogy virtuális önállóságuk továbbra is biztosítható marad. Mindezt annak érdekben, hogy az egyes szervek speciális feladataiból fakadó olyan egyedi kommunikációs szükségletek is kielégíthetők legyenek, amelyeket az egységes rendszer használatával nem, vagy csak aránytalanul nagy ráfordítással lehet megvalósítani. Előző gondolatokat a magyar kormányzati távközlés egységesítésének kérdéskörére vetítve a következő helyzetet kell figyelembe venni:

- 2004-től a gyakorlatban is megkezdődött a zártcélú kommunikációs rendszerek EKG-val párhuzamos hálózati szakaszainak megszüntetése, vagyis egyes technikai alrendszerek integrációja;
- az egyes zártcélú távközlő rendszerek egymás közötti együttműködése – a vonatkozó jogszabály szerint – csak az EKG-n keresztül valósulhat meg;
- megvalósul az EKG-EBDH-Közháló rendszerek közötti műszaki-technikai együttműködés;
- az MH Hálózatának integrációja csak részlegesen javasolt;
- kialakítás előtt áll az EDR.[205]

A megállapítások alapján kijelenthető, hogy a technikai rendszerek szintjén megfigyelhető egyrészt egy részleges integráció, másrészt egy szorosabb együttműködés felé irányuló folyamat. A kommunikációs rendszer definíciójából levezetett további rendszerelemek szintjén jelenleg tényleges összevonásról nem beszélhetünk.[206] Az EDR tervezése során – a vonatkozó kormányhatározat[207] alapján – figyelembe kell venni, illetve fel kell használni a zártcélú kommunikációs rendszerek egyes technikai alrendszereit, így kimondható, hogy a technikai rendszerek közötti együttműködés szélesedése várható a közeljövőben.

---

[204] ezek lehetnek olyan műszaki-technikai problémák, amelyek ténylegesen megakadályozzák a hálózatok összekapcsolását, illetőleg olyan szervezeti problémák, amelyek szintén – általában azonban csak időlegesen – teszik lehetetlenné a teljes integrációt

[205] az EDR szolgáltatás vásárlásával kapcsolatosan a Központi Szolgáltatási Főigazgatóság által kiírt közbeszerzési pályázatra három ajánlat érkezett be (MVM Rt.-SAAB Rt. konzorcium, Antenna Hungária Rt.-Siemens Rt. konzorcium, T-Mobile Rt.-T-Com Rt. konzorcium). Az ajánlatok bontása 2005. augusztus 15-én 09.00-kor történt meg

[206] némileg elvonatkoztatva elmondható, hogy az EKG-hoz csatlakozásra kötelezettek esetében a szervezési intézkedések, és ebből adódóan az irányításért, üzemvitelért és fenntartásért felelős személyek és szervezetek szintjén van együttműködés, hiszen az 5/2004. (I.9.) Korm. rendelettel kiadott EKG használati és üzemeltetési szabályzat szerint az EKG és az egyes zártcélú hálózattal rendelkező szervek között szerződéses kapcsolat alakult ki 2004-ben

[207] 1053/2005. (V.26.) Korm. határozat

Összességében, tekintettel az integráció irányába ható folyamatokra, valamint az MH Hálózatának helyzetére úgy ítélem meg, hogy a módszer eredményes alkalmazása érdekében meg határozni az összevonásra kerülő, illetve a virtuálisan együttműködő rendszerelmeket és azok körét.

Figyelembe véve fentieket, a részleges összevonás és virtuális önállóság alternatívája a megvalósítás egyik útja lehet.

### 2.4. Kombinált alkalmazás

Kombinált alkalmazás alatt az előző két alfejezetben ismertetett megoldások – időtényezőtől függő – egymásra épülő, vegyes felhasználását értem. Álláspontom szerint a részleges összevonás ideiglenes célként is szóba jöhet abban az esetben, amikor a végcélként megfogalmazott teljes integráció előnye és haszna – előre láthatóan ugyan – biztosított, azonban az egyes rendszerelemek adott időszakbeli azonnali és teljeskörű összevonása különböző okoknál fogva nem járható, de bizonyos ráfordításokkal[208] (átalakításokkal, fejlesztésekkel) az azonos kategóriába tartozó rendszerelemek felkészíthetők az integrációra, majd ez ténylegesen meg is valósítható. Az eljárás természetesen irreverzibilis, vagyis bármelyik irányból kezdeményezett átalakítás során átmenetet képezhet a teljes, illetve a részleges összevonás (és megfordított) állapota között, azonban nézőpontom szerint a módszert nem elsősorban a dezintegrációs folyamatok elősegítésére kell felhasználni. Az alkalmazás fő funkciójaként tehát megfogalmazható, hogy a módszernek olyan, a gyakorlatban is felhasználható tervet kell tudni megfogalmaznia, amely az – ideiglenesen – virtuálisan önálló rendszerelmek teljes és optimális összevonására ajánlást adhat.

Áttekintve az előző alfejezetben tett megállapításokat is, nézőpontom szerint megfontolás tárgyává lehet tenni az összevonás kombinált alkalmazásának módszerét, mivel – hosszútávon – végcélként definiálható a kormányzati távközlésben jelenleg részt vevő kommunikációs rendszerek teljes körű integrációja.

Összességében, arra a kérdésre „Miként lehetséges megoldani az egységesítést?” – válaszolni a következőképpen lehet: a fennálló objektív helyzet okán az egységes magyar kormányzati távközlés rendszerét első lépcsőben a résztvevő és korábban meghatározott kommunikációs rendszerek egyes elemeinek teljes egységesítésével, majd a virtuálisan önállóként fennmaradt elemek további teljes összevonásával lehet megvalósítani.

## 3. A megvalósítás egy lehetséges módja

Megítélésem szerint, a kormányzati távközlés egységesítését a kombinált módszer alapján lehet megvalósítani, tehát végcélként megfogalmazható a rendszerek teljes – két vagy több lépésben történő – összevonása. Az integráció eredményeképpen – hosszabb távon – csak egy olyan egységesített kommunikációs rendszer megvalósulása lehet, amely egyrészt biztosítja a kormányzati szervek közötti, a nemzeti és közösségi kormányzat közötti, valamint a nemzeti kormányzat és a társadalom egyéb szereplői közötti információáramlást.

[208] elsősorban a ráfordítás financiális és szervezési jellegű, de egyes esetekben a megvalósítás az időtényezőktől is erősen függhet

### 3.1. Az integráció első lépcsője

Az első lépcsőben olyan állapot elérésére való törekvés a cél, amely során – elsősorban – a kormányzati távközlés korábban meghatározott fő összetevői körében – az egyes alrendszerek tekintetében – megtörténik a részleges összevonás és létrejön egy egységesnek tekinthető rendszer. A részleges integráció nem terjedne ki az MH Hálózatára, hiszen – többek közt – az egységesítési szempontból a legnagyobb bizonytalansági tényezőt jelenleg is ez a rendszer jelenti, amely lényegében egy hosszabb időtávú – az észak-atlanti szövetség által még kidolgozás alatt álló fejlesztési koncepció alapján történő[209] – átalakítási eljárás megvalósítása előtt áll. Az egységesítési lépések gyakorlatilag már megindultak, mivel a kombinált módszer egyik alapját összességében az 5/2004. (I.9.) Korm. rendelettel kiadott EKG Hálózat Használati Szabályzat teremtette meg, amely révén az egyes zártcélú rendszerek EKG-ba történő integrálódása megkezdődött, vagyis ez azt jelenti, hogy az egyes kommunikációs hálózatok technikai alrendszerei tekintetében a közös technikai infrastruktúra kialakítása folyamatban van.

A második alapot az EKG-EBDH, az EBDH-Közháló, valamint az EKG-Közháló között kialakuló műszaki-technikai együttműködés biztosítja. Ezek a folyamatok tehát lényegében véve a részleges összevonás kategóriájába tartoznak.

A harmadik fontos pillér az egységes digitális rádiótávközlő rendszer létrehozásával és működtetésével kapcsolatos feladatokkal megbízott kormánybiztos feladat- és hatásköréről szóló 98/2005. (V.26.) Korm. rendelet, amely a – még kialakítás előtt álló – EDR tekintetében a zártcélú hálózatgazda funkciót a MeH miniszter hatáskörébe[210] utalja.

A vonatkozó rendeletben[211] rögzített szabályozási megoldás jelenleg nem teszi lehetővé a teljes összevonás irányába történő elmozdulást, vagyis csak egy részleges összevonást, mivel adminisztratív előírásokkal továbbra is biztosítja az egyes zártcélú hálózatok önállóságát. Annak érdekében, hogy a jövőben – a koordinatív jellegű irányítási modell felváltásával – átalakítható legyen a széttagolt irányítás évek óta megfigyelhető és jelenlevő problematikája, első lépésként az irányításért, üzemvitelért és fenntartásért felelős szervezetek központosított struktúráját kell kialakítani,[212] ami természetesen a jelenlegi szabályozási alapelvek részleges átalakításával jár. Lényegében, az integráció első lépcsőjében meg kell teremteni annak lehetőségét, hogy az EKG (EDR), az EBDH, a Közháló, valamint az EKG gerinchálózatához csatlakozásra kötelezett szervek irányításért[213] felelős szervei egy szervezeti egységben – egy hálózatgazda felügyelete alatt – összevonásra kerüljenek. Kezdetben ennek egyszerű egy-

[209] hálózatközpontú hadviselés (NCW). Ennek lényege NATO Hálózat Nyújtotta Képesség (NNEC) néven került elfogadásra

[210] az EDR-rel kapcsolatos feladatok végrehajtását ténylegesen Pesti István kormánybiztos irányítja

[211] 5/2004. (I.9.) Korm. rendelet

[212] az egységes, integrált rendszer mibenléte és definíciója az 1.1. alfejezetben került meghatározásra

[213] gyakorlatilag ez azt jelenti, hogy a zártcélú távközlő hálózatok gazdáinak feladatrendszerét ellátó szervezetek egy egységes minisztérium, illetve főhatóság szervezetén belül összevonásra kerülnek. Az integráció szakmai végrehajtására a Miniszterelnöki Hivatal, vagy Informatikai és Hírközlési Minisztérium szervezeti keretében látok lehetőséget

máshoz rendelés keretén belül kell megvalósulnia, majd ezt követően át kell tekinteni az azonos feladat-ellátási funkcióból adódó párhuzamokat és megszüntetni a felesleges vezetési és irányítási szinteket.

Ugyanekkor a különböző szervek és rendszerek közötti információátvitel biztosítására létrehozott ágazati szervezeteknek is be kell tagozódniuk az integrált vezetési rendszerbe. Ez a lépés összességében azt jelenti, hogy a folyamat megvalósításával párhuzamosan át kell alakítani az integrációra tervezett zártcélú kommunikációs rendszerek jogi, irányítási, felügyeleti és finanszírozási státuszát, vagyis a jelenleg hatályos jogszabályt[214] módosítani kell. Az egységesített hálózat a meglevő kormányzati humán, távközlési és informatikai erőforrások felhasználásával, bővítésével, a vonatkozó műszaki előírások, szabványok, és hatósági eljárási rend megtartásával üzemeltethető. Az egységesített rendszer kiterjedésénél a következőket kell alapul venni:

- a vezetékes alrendszeren az adatátviteli szolgáltatásnak ki kell terjednie a fővárosra, a megyeszékhelyeken telepített csomópontokon keresztül a dekoncentrált szervekre, néhány, az országvédelem szempontjából fontos létesítményre, valamint a helyi önkormányzatokra és fontosabb közigazgatási intézményekre;
- a vezetékes alrendszeren – a fenti viszonylatokat tekintve – ki kell terjeszteni a hagyományos távbeszélő szolgáltatásokat;
- ráépülve az összevonásra kerülő infrastruktúrára – elsősorban a készenléti szervek részére – a rádiós alrendszernek (EDR) országos lefedést kell biztosítania.

Az egységesülő rendszerrel szemben támasztható követelmények az alábbiak szerint fogalmazható meg:

- alkosson egységes egészet a kormányzat békeidejű és minősített időszaki kommunikációs feladatainak megoldására;
- integrált rendszerben biztosítsa a távközlési és informatikai szolgáltatásokat a kor által megkívánt, a hazai és nemzetközi viszonyok között reálisan elérhető műszaki színvonalon;
- a mobilitás és a biztonság növelése érdekében vezetékes és rádiótávközlési összeköttetéseket biztosítson;
- tegye lehetővé a külön meghatározott vezetőállomány számára az összeköttetések elsőbbséggel történő használatát;
- biztosítsa az integrált hálózat fokozott biztonságát, információvédelemmel való differenciált ellátását;
- létesítsen biztonságos távközlési és informatikai kapcsolatot a minősített időszaki létesítményekből a kitelepült egyéb vezető-, illetve a helyükön maradó államigazgatási szervekkel, valamint a helyi vezetési pontokkal;
- a hálózatban biztosítani kell az arra jogosult szervezetek részére valamennyi információfajta valós idejű és kiértékelhető hozzáférését, a jogszabályok alapján meghatározott eljárási rendet is figyelembe véve;
- előző ponton túlmenően törekedni kell arra, hogy a rendszer képessé váljon az állampolgár és az állam közötti kommunikációra, azaz a meghatározott körű információfajták szabadon álljanak rendelkezésre az állampolgárok számára;
- a hálózat fokozatos megvalósításában kapjon prioritást az adatátviteli igények kielégítése mind a vezetékes, mind a rádiótávközlésben. A területi megvalósítás-

[214] 50/1998. (III.27.) Korm. rendelet

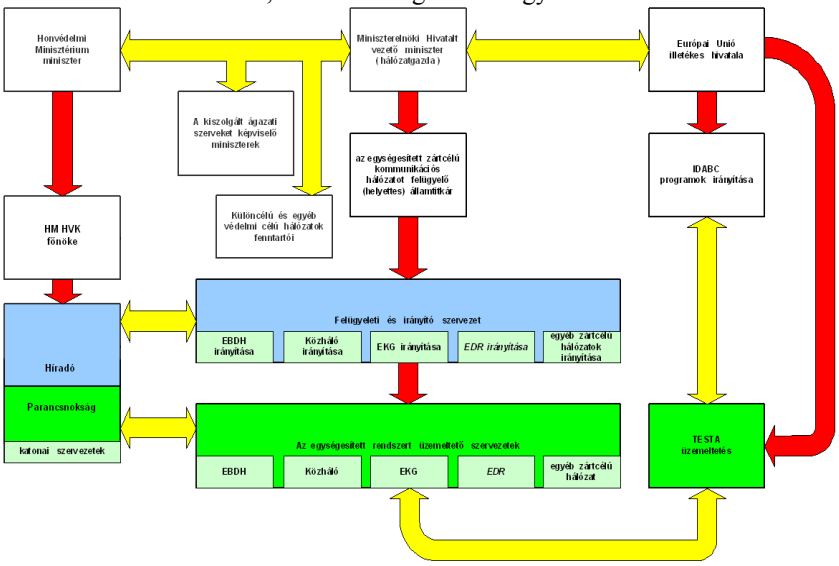
ban pedig a fővárosi (béke és minősített időszaki) követelmények kielégítésére kell az elsődleges hangsúlyt helyezni;

- a rendszer műszaki felügyeletét, irányítását, a szolgáltatásokhoz való hozzáférés menedzselését, valamint a működtetés feltételeinek biztosítását központilag kell megoldani, különös tekintettel a minősített időszaki követelményekre;
- a kommunikációs rendszerek egységesítése során – biztonsági, védelmi, gazdasági és speciális szolgáltatási szempontból – a kormányzat e célra létrehozott szervezete által működtetett, alapvetően a kincstár tulajdonát képező infrastruktúrára épülő hálózat kialakítása célszerű, mert a biztonsági követelményeket felelősséggel csak ez garantálhatja.

Az így kialakítandó rendszerben az MH Hálózata (irányítói és működtetői számára) és a részlegesen egységesített kormányzati távközlő rendszer közötti együttműködési kötelezettséget továbbra is fenn kell tartani. Az első lépcső végére az államigazgatást kiszolgáló kommunikációs rendszerek körében a következő szervezési struktúrát lenne célszerű elérni:

zártcélú kommunikációs hálózat:

- miniszter vagy főhatóság vezetője, mint zártcélú kommunikációs hálózat gazdájának felügyelete alatt az egységesített kormányzati kommunikációs rendszer;
- a Honvédelmi Miniszter, mint hálózatgazda felügyelete alatt az MH Hálózata.




1. ábra: az integráció első lépése során kialakítandó irányítási és szervezési modell

Az elkülönülő (zártcélú) kormányzati távközlő hálózat működtetése nem nélkülözheti a felelős szerv (hálózatgazda) kijelölését. Tekintettel arra, hogy a kormányzati hálózat több államigazgatási és egyéb szerv ellátását is biztosítja, célszerű a felelősség és a jogkör megosztott megfogalmazása oly módon, hogy a rendszer felügyeletét a Miniszterelnöki Hivatalt vezető miniszter lássa el, egyetértésben a hálózatgazda jogkö-

röket az összevonásig gyakorló miniszterekkel.215 Az egységesítés kombinált módszerének alkalmazása során az első lépcsőben létrejövő irányítási és szervezési modellt az alábbi 1. sz. ábra szemlélteti:

Az ábra alapján megállapítható, hogy az integráció első lépcsőjében az MH Hálózata kivételével a zártcélú távközlő hálózatok, a kiépítésre kerülő EDR, valamint a Közháló jelenlegi irányítási és felügyeleti szervei, virtuális függetlenségüket megtartva – adminisztratív úton – integrálásra kerülnek az őket irányító hálózatgazda hivatalába. Az üzemvitelért felelős szervezetek a hálózatgazda hivatalának háttérintézményeként működő szervekként kerülnek egy egységbe összevonásra oly módon,216 hogy a korábbi ágazati alá-fölérendeltségi viszonyok az irányítás és végrehajtás terén még fennmaradnak.

Az MH Hálózatának gazdája, illetve az üzemeltetéssel megbízott szervek a jogszabályokban meghatározott – más zártcélú hálózatgazdával történő – együttműködési kötelezettség rendje szerint vesz részt a kormányzati távközlés megvalósításában. Az egységesített kommunikációs rendszer szolgáltatásaival, technológiai továbbfejlesztésével kapcsolatos igények visszacsatolása és megjelenítése érdekében a kiszolgált területek miniszterei, valamint az egyéb külön- és védelmi célú hálózatok fenntartói együttműködnek a két zártcélú hálózatgazdával.

Az alkalmazott megoldás révén megkezdhetővé válik a közösségi ajánlások teljesítésével, a fejlesztéssel, valamint a működéssel kapcsolatos szervezési elgondolások, koncepciók és intézkedések egységesítése.

### 3.2. Az összevonás továbbfejlesztése

Miután az integráció megkezdésével a főbb szervezeti keretek már felvázolásra kerülnek, ezért az összevonás továbbfejlesztésének második szakaszában át kell tekinteni a hálózatgazda hivatalában – virtuálisan működőnek tekinthető – felügyeleti és irányító szervek struktúráját és megkezdeni azok funkcionális átalakítását, illetve célszerű kombinációban történő szervezeti összevonását. Figyelemmel arra, hogy az EKG-EBDH, EKG-Közháló, valamint EBDH-Közháló rendszerek szorosabb technikai együttműködésének műszaki akadálya nincs, ezért az összevonás második lépcsőjében a hálózatokkal kapcsolatos felügyeleti és irányítási tevékenység összekapcsolható. Jellemzően e modell válik alkalmazhatóvá azon zártcélú távközlő hálózatoknál is, ahol a gerincirányú összeköttetések az EKG infrastruktúrája útján kerül biztosításra.

Az EDR-nek, mint kiépítés előtt álló rendszernek üzembeállításakor, jellemzően a rendészeti és egyéb mozgószolgálati szervek speciális igényeinek kielégítését kell elsősorban biztosítania úgy, hogy infrastruktúrájának egy része majd épüljön rá a jelenlegi államigazgatási hálózatokra. Tekintettel arra, hogy a kiszolgálni kívánt kör szűkebb, továbbá arra, hogy e területen hazai irányítási és működtetési tapasztalat – a helyzet adottságánál fogva – még nem alakulhatott ki, ezért az egységesített kommu-

215 informatikai és hírközlési miniszter, belügyminiszter, pénzügyminiszter, legfőbb ügyész, igazságügy-miniszter

216 az üzemvitelért felelős szervezeti egységek jogi státusza eldöntendő kérdés, mivel jelenleg e területen vegyes kép tárul a vizsgálódó elé. A közigazgatási besorolású szervtől az állami többségi tulajdonú gazdasági társaságon át a közhasznú társaságig több fajta szervezet vesz részt az üzemvitelben

nikációs rendszer rádiós alrendszerének felügyeletét és irányítását nem célszerű más alrendszerek hasonló területeivel összevonni, integrálni.

Fentiek figyelembe vételével – a felügyelet és irányítás síkjában történő összevonást követően – a szakterületek struktúrája a következők szerint módosulhat:

- hálózatgazda miniszter;
- felügyelő (helyettes) államtitkár;
- telekommunikációs és informatikai rendszerek irányítása;
- EDR rendszer irányítása.

A második lépcsőben az egységesített kommunikációs rendszert – virtuális önállóságuk megtartása mellett – üzemeltető szervek összevonását kell megvalósítani, hiszen az előző alfejezetben követelményként is megfogalmazásra került azon elvárás, miszerint a rendszer műszaki felügyeletét, irányítását, a szolgáltatásokhoz való hozzáférés menedzselését, valamint a működtetés feltételeinek biztosítását központilag kell megoldani, különös tekintettel a minősített időszakokra. Az üzemvitelért és fenntartásért felelős személyek és szervezetek, valamint a különböző szervek és rendszerek közötti információátvitel biztosítására létrehozott szervezetek célszerű kombinációban történő összevonása komplex – némileg bonyolult – kérdéskör. Az integrációval összefüggésben a következő legfőbb kérdéseket kell áttekinteni:

- az üzemeltetés és fenntartás szervezetei működtetésének konstrukciója, vagyis a szervek besorolása;
- egyes szervezetek, vagy integrált fenntartó és üzemeltető szervek kialakítása;
- a szervezetek célszerű struktúrájának kialakítása.

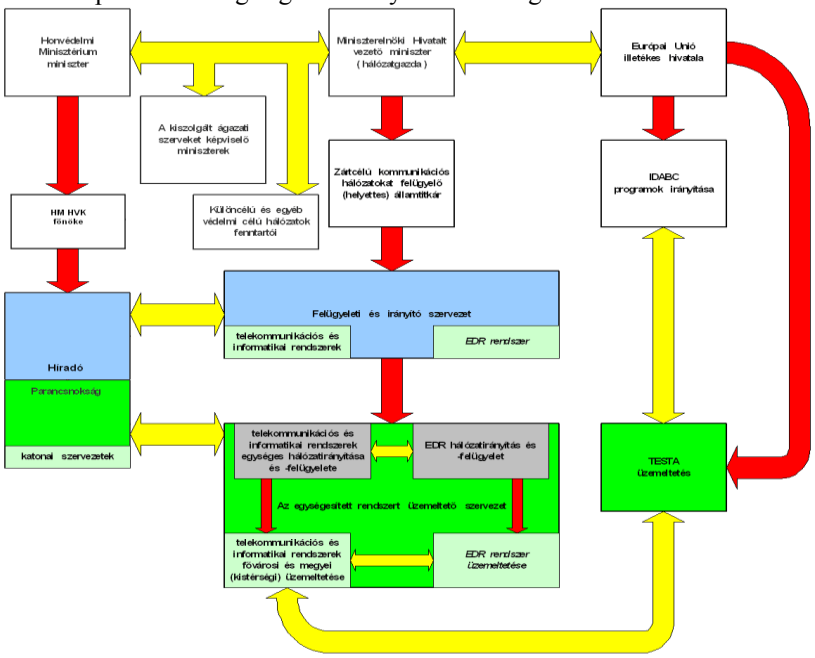
A kérdéseket megválaszolva, szintén az előző fejezetben került meghatározásra, hogy a kommunikációs rendszerek egységesítése során – biztonsági, védelmi, gazdasági és speciális szolgáltatási szempontból – a kormányzat e célra létrehozott szervezete által működtetett, alapvetően a kincstár tulajdonát képező infrastruktúrára épülő hálózat kialakítása célszerű, mert a biztonsági követelményeket felelősséggel csak ez garantálhatja. Az egységesített kormányzati rendszer szempontjából tehát továbbra is fontos az állami tulajdonhányad kérdése, amely egyrészt az infrastruktúrára, illetve a működést biztosító szervezetek tulajdonformájára terjed ki. A tulajdonhányad alapvetően meghatározza a működtetés további költségeinek alakulását is. Nézőpontom szerint a tulajdonhányad a kormányzati rendszer önállóságának alaptétele is, hiszen stratégiai kérdésekben – a közcélú szolgáltatóktól való – függetlenség jelentősen befolyásolhatja a központi akarat megvalósulását. Ezt tekintve alapul, minimális követelményként fogalmazható meg, hogy az üzemeltetés és fenntartás egyes szervezeteinél – nem vizsgálva részletesen a gazdasági aspektusokat – az állami tulajdon részaránya haladja meg a 90 %-ot, vagyis a közösségi normák szerint feleljenek meg az állami tulajdonú társaságként történő besorolás kritériumának. Természetesen ennél szigorúbb követelmény is támasztható, példaként az, hogy ezek a szervezetek képezzék részét az államigazgatásnak, vagyis működjenek a hálózatgazda hivatalának központi vagy területi szerveiként.

A második felvetéssel összefüggésben, tekintettel arra, hogy az EDR-rel kapcsolatosan egyrészt még hiányoznak a hazai üzemeltetési tapasztalatok, másrészt a az elmúlt években kiadott vonatkozó határozatok szerint vásárlás útján – egyszolgáltatós modellben – valósul meg a szolgáltatások biztosítása, ezért nem javaslom az integráció második lépcsőjében sem a teljesen integrált üzemeltetést és fenntartást megvalósítani.

Célszerűnek mutatkozik, ha a felügyelet és irányítás rendszeréhez igazodóan legalább a következő két különálló üzemeltetési és fenntartási szakterület alakul ki:

- telekommunikációs és informatikai rendszerek üzemvitele és fenntartása;
- EDR rendszerek üzemvitele és fenntartása.

A telekommunikációs és informatikai rendszerek tekintetében támaszkodni szükséges az EKG, EBDH, Közháló és a jelenlegi egyéb zártcélú hálózatok üzemeltetési és fenntartói szervezeteire,[217] amely felhasználásával ki kell alakítani – illetőleg egységesíteni – az összevont kommunikációs rendszer központi hálózatfelügyeleti és -irányítási szervezetét. A szervezetek célszerű struktúrájának kialakításakor elsősorban azt a tényt kell figyelembe venni, hogy az egységesített kommunikációs rendszer kiterjedtségét tekintve országos lesz. Jelenlegi technikai alkotóelemei a elsősorban a megyei közigazgatási határokhoz igazodnak, amelyeket – a jövőt illetően – a megyei rendszerre alapozó kistérség-régió viszonylathoz kell igazítani.




2. ábra: az egységesített rendszer irányításának egy lehetséges változata

A második lépcsőben a szervezeti struktúrákat – elsősorban a telekommunikációs és informatikai rendszerek tekintetében – tehát úgy kell kialakítani, hogy az üzemvitel és fenntartás alsófokú szervezete legalább megyei szinten legyen jelen, amelyet a további lépések során – az üzemviteli tapasztalatok figyelembe vétele alapján – kiterjeszthetővé kell tenni a kistérségek irányába is. A megyei szint alatti helyi szintek (kistérségek) rendszerbe való integrálása fontos feladatot jelent a jövőben, mivel a jelenlegi zártcélú kommunikációs rendszerek tekintetében gyenge pontot jelent annak az adatátviteli képességnek a hiánya, amely egyelőre nem teszi lehetővé a helyi szintű

[217] amelyek közül az EBDH-t fenntartók köre tekinthető a legnagyobbnak. Elsősorban kiterjedtsége folytán területi szervek is részt vesznek munkájában

közigazgatási szervek állami infrastruktúra felhasználásával való integrációját. Ennek elmaradása gyakorlatilag azt jelenti, hogy a kormányzati távközlést megvalósító kommunikációs rendszer nem tekinthető – a korábbi definícióban meghatározottaknak megfelelően – teljesnek. A második lépcsőben tehát az első szakaszban adminisztratív úton összevont kommunikációs rendszerelemek további célszerű integrációját kell végrehajtani. Az elemek összevonása összességében véve a kormányzati tevékenység javulásához vezethet a különböző nemzeti és közösségi kormányszervek, a lakosság és egyéb társadalmi szervek közötti információáramlás hatékonyabb megvalósulása révén. Az egységesített kormányzati rendszer és környezetének jövőbeni kapcsolatának egy lehetséges változatát a 2. ábra szemlélteti.

Megállapítható, hogy az összevonás második lépcsőjében a jelenlegi különállás sok tekintetben megszüntethető. Az irányítás és végrehajtás egy lehetséges változata került feltüntetésre az ábrán, vagyis az értekezés korábbi alfejezetében rögzítettek alapján az EDR-t üzemeltető, mint – egy legalább – állami többségi tulajdonú szervezetként került jelölésre. Az MH Hálózatának integrációja továbbra sem következik be, a kormányzati távközlés megvalósulásában továbbra is a vonatkozó jogszabályok szerint előírt együttműködés keretén belül vesz részt.

Az összevonás második lépcsőt követő továbbfejlesztése az MH Hálózat részleges vagy teljes integrációja lenne, azonban hazánk észak-atlanti szövetségi tagságából eredő – korábban már rögzített – problémák miatt a megvalósítás üteme jelenleg nem látható.

## 4. Összegzés, következtetések

A kormányzati távközlés helyzete a harmadik időszak elején218 olyan stádiumba jutott, amely előrevetítheti egy egységesített kormányzati kommunikációs rendszer tényleges megszervezését. A kialakult – és a jelenleg előre meg nem határozható ideig fennálló – körülmények elvi síkon jó alapot szolgáltatnak arra, hogy a hírközléspolitikában még 1998-ban, a kormányzati rendszerrel összefüggésben megfogalmazott elgondolások – az erre irányuló kedvező döntés és akarat esetén – belátható időn belül teljesüljenek.

A fejlődéstörténet második szakasza végén, a kormányzati szervezeti struktúrán – a Miniszterelnöki Hivatalon – belül létrejött szakmai centrum és az EKG működése véleményem szerint új, harmadik szakaszt nyitott a kormányzati távközlés történetében, hiszen megteremtette a lehetőségét annak, hogy lezárjon egy olyan korszakot, amelyben a központi kormányzat helyett a zártcélú távközlő hálózatok gazdái töltenek be fajsúlyos szerepet a terület összességének irányításában, folyamatainak alakításában. Természetesen a korábban kialakult helyzetért az ágazati hálózatgazdák csak részben tehetők felelőssé, hiszen a globalizáció és a konvergencia hatásaként megjelenő és velük szemben újonnan támasztott – az államigazgatási tevékenységek elektronizálása és informatizálására irányuló – modernizációs követelmények teljesítéséhez a központi kormányzat kezdetben nem tudott infrastrukturális alternatívát felkínálni. A kezdeményezés lehetőségének átvételét egyértelműen elősegítette a jogi szabályozás megengedő jellege is, ami az önálló rendszerek további fenntarthatóságához és üzemeltethetőségéhez kedvező feltételeket biztosít mind a mai napig.

[218] 2004. január 8-át követően

Hazánk Európai Unióhoz történt csatlakozása az eddigiektől eltérő kihívásokat jelent a kormányzati távközlés területén, hiszen a közösség célja, hogy a tagállamokban megteremtse az egységes páneurópai elektronikus kormányzati szolgáltatások körét, amely során az interoperabilitás követelményét nem csak az egyes országok rendszereinek összekapcsolása, együttes működtetésének biztosítása vonatkozásában kell alkalmazni, hanem a nemzeti közigazgatási szervek által már létesített vagy az elkövetkezendőkben létrehozásra kerülő elektronikus kormányzati rendszerek tekintetében is. Tehát a kormányzat saját rendszerein az információáramlás képességét a jövőben nemcsak a kormányzati szervek részére, hanem egyre szélesedő körben a lakosság számára is meg kell teremteni.

Az elektronikus közigazgatás bevezetésével és továbbfejlesztésével összefüggő közösségi különböző programokban Magyarországot a Miniszterelnöki Hivatal egykapus rendszerben képviseli, tehát az e témakörben felmerülő EU koncepciók elsőként a kormányzat legfelső szintjén jelennek meg. Ehhez a fontos pozícióhoz csatlakozik a MeH azon műszaki-technikai képessége is, amelyet számára az EKG biztosít az adminisztratív eszközökkel is elősegített, egyre szélesedő felhasználói körrel. A nemzeti hálózatok összekapcsolásával összefüggő közösségi elgondolások gyakorlati technológiai kivitelezését szintén az EKG irányítja és végzi. Az elektronikus kormányzat hazai kialakítása tehát már nem csak nemzeti érdek, hanem egyértelműen uniós elvárás is, amelynek teljesülését – ha ahhoz közösségi pénzügyi források is felhasználásra kerültek – EU hivatalok is vizsgálják. A hírközléspolitika kombinált, a zártcélú távközlő hálózatokat is magába foglaló kommunikációs rendszer kialakítását irányozta elő. A harmadik időszakra kialakult helyzet már megteremti annak lehetőségét, hogy a jelenlegi zártcélú távközlő hálózatok számának optimalizálása úgy kerüljön végrehajtásra, hogy azok a megszervezésre kerülő egységes kormányzati kommunikációs rendszer elemeiként jelenjenek meg a jövőben. Az integráció szempontjából fontos kérdés a zártcélú távközlő hálózatok jövőbeni viszonyrendszere, mivel a jelenlegi szabályozás szerint az EKG-hoz való csatlakozási adminisztratív kötelezettség nem terjed ki sem a honvédelmi (MH Hálózata), sem a belügyi ágazatra (EBDH), illetve az EDR-re.

A rendészeti kommunikációs rendszerek keretében vizsgált EBDH alapvetően országos kiterjedésű integrált gerinchálózat, és vele kapcsolatosan kijelenthető, hogy az ágazati szervek – így a közigazgatás egy része – kommunikációjának teljes vertikumának kiszolgálását képes biztosítani. A belügyi ágazaton belül az önálló szervek és főhatóságok gyakorlatilag rendelkezhetnek különálló, zártcélú hálózatokkal, azonban a 2004-ben megindult centralizációs folyamatok a rendszerek EBDH-ba történő integrációját irányozzák elő. Az EBDH irányítására legfőképpen a széttagoltság jellemző, amellyel párhuzamosan alapvetően gyenge a központosított szabályozási tevékenység is. A centralizációval párhuzamosan gyakorlati kereteket ölt az EKG-EBDH-Közháló együttműködési programja, amely előirányozza a rendszerek 2005. II. félévében történő összekapcsolását.219 Az MH Hálózata alapvetően két önálló alrendszerből áll, amelynek integrációjára irányuló törekvések megkezdődtek, azonban azokat hátráltatja az észak-atlanti szövetségi rendszer – kommunikációs rendszerek átalakítására kiterjedő – újfajta információszervezési koncepciója. Általánosságban azonban elmondható, hogy az alrendszerek integrációs elképzeléseinek középpontjában – a NATO tagorszá-

[219] amely lényegében 2005. szeptemberében valósággá vált

gok mintájára – egy nagysebességű, minimálisan 155 Mbit/s adatátviteli sebességűre tervezett, a közcélú infrastruktúrára alapozó virtuális zártcélú kommunikációs rendszer kialakítása áll. Az MH Hálózatának irányítására alapvetően az erős centralizáltság és a normatív szabályozottság jellemző.

Az egységes kormányzati kommunikációs rendszer többlépcsős kialakításánál tehát az EKG és EBDH valós műszaki-technikai együttműködési képessége folytán tervezni lehet mindkét hálózat integrációját, amelyet a belügyi ágazaton belüli centralizáció is elősegít. Az MH Hálózata tekintetében a továbbfejlesztéssel kapcsolatos igen sok bizonytalansági tényező miatt az egységesítendő kormányzati rendszerbe – összevonás útján való – bevonását érdemes további megfontolás tárgyává tenni. Az EDR elsősorban a belügyi rendészeti szervek igényeit fogja kielégíteni, így a rendszer integrálása mindenképpen indokolt, amelyhez szervesen kapcsolódik, hogy az EDR kialakítására irányuló beruházás során a felhasználható, az állami vagyon részét képző technikai elemeket be kell vonni, ami az EBDH esetében – a rendszerelemek nagyfokú infrastrukturális integráltsága miatt – nehézen végrehajtható. A közigazgatás helyi szervei információáramlásának központi, kormányzati infrastruktúrán való biztosítása nem megoldott. Pótmegoldásként értékelhető a Közháló program alapján kiépített rendszer, amely nem minősül zártcélú távközlő hálózatnak. A Közháló lényegében véve teljes mértékben a közcélú szolgáltatókra épül, és csak az informatikai alkalmazások használatát támogatja, tehát a rendszer nem teszi lehetővé más típusú híranyag továbbítását. Az egységesség gondolatiságának szempontjából azonban e rendszer integrációja is szükségessé válik.

Az egységes kormányzati kommunikációs rendszer megszervezését tehát a harmadik időszakra kialakult szervezési és műszaki helyzet kedvezően befolyásolhatja. A rendszer kialakítását első lépcsőben mindenképpen felülről irányítva, elsőként adminisztratív szervezési eszközökkel kell megindítani, amelynek végeredménye az lehet, hogy a zártcélú távközlő hálózatok jelenlegi köre kétszereplősre csökkenhet.

Az első lépcsőben megvalósítandó szervezési folyamaton túl, az összevonás továbbfejlesztése lehet az egymáshoz rendelt irányítási és felügyeleti, valamint az üzemvitelért és fenntartásért felelős személyek, valamint a különböző szervek és rendszerek közötti információátvitel biztosítására létrehozott szervezetek célszerű integrációja. Fontos meghatározni továbbá a kormányzati rendszerben elfoglalt helyüknek, szerepüknek és státuszuknak a rögzítése is, hiszen az integrációra tervezett üzemviteli és fenntartó szervezetek egy része közigazgatási szerv, vannak állami többségi tulajdonban levő gazdálkodó szervek és a tevékenységben részt vesznek a hírközlési piaci szereplői is.

A leírtakat mérlegelve az alábbi következtetéseket vonom le:

- A kormányzati távközlés értekezésben vizsgált időszaka kettő, konkrétan behatárolható fejlődési időszakra bontható fel. A fejlődéstörtének harmadik szakasza napjainkban is tart.
- A fejlődéstörténet harmadik – jelenlegi – szakaszában adottak a körülmények ahhoz, hogy a korábbi stratégiai elképzeléseknek megfelelően megszervezésre kerüljön egy egységes kormányzati kommunikációs rendszer, amely hatékonyan elősegítheti a kormányzati munkát és szolgáltató jellegének erősítését.

- Az erős, egy hálózatgazda kezében levő központi irányítás révén biztosítható az elektronikus kormányzással kapcsolatos közösségi és nemzeti programok megvalósulása, a párhuzamos fejlesztések visszaszorítása.
- Az integráció révén optimalizálható a zártcélú távközlő hálózatok száma is, amely korábban stratégiai koncepcióként került megfogalmazásra.

Az időszakra vonatkozó főbb megállapítások az alábbiak:

Az egységes kormányzati kommunikációs rendszer megszervezését felülről irányítva, több lépcsőben kell elvégezni, amelynek során a rendszerek integrációja elsőként adminisztratív szervezési úton jön létre. Új rendszer kiépítését tervezni nem lehet, a jelenlegi összetevők célszerű egységesítését kell végrehajtani.

Az összevonás továbbfejlesztése során részletesen meg kell határozni üzemvitelért és fenntartásért felelős személyek, valamint a különböző szervek és rendszerek közötti információátvitel biztosítására létrehozott szervezetek kormányzati rendszerben elfoglalt helyét, szerepét és státuszát, majd pontosan meg kell határozni a műszaki kompatibilitás és együttműködés, illetve a virtuális hálózatok üzemeltetésének további feladatait.

## Hivatkozások:


[1] Dr. Mráz István: A haderő vezetése békétől eltérő (minősített) időszakokban, „Kommunikáció 2003." nemzetközi szakmai tudományos konferencia, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, ISBN 963 86229 6 2, 222. oldal, 2003. október 15.

[2] Az egységes digitális rádió-távközlő rendszer (EDR) szolgáltatás vásárlásáról szóló 1077/2004. (VII.22.) Korm. határozat, Magyar Közlöny, 2004/103. szám, Budapest, 9537-9539. oldal, 2004.

[3] A telekommunikációs eszközökkel történő ellátás rendjéről, valamint a távközlési és informatikai szolgáltatások igénybevételének szabályairól szóló 19/2004. (BK 14.) BM utasítás, Belügyi Közlöny, 2004/14. szám, Budapest, 1300. oldal, 2004.

[4] Dr. Szücs Ervin: Rendszer és modell I., Egységes Jegyzet (ELTE TTK), Kézirat, Tankönyvkiadó, Budapest, 99-100. oldal, 1987.

[5] IHM miniszter-MeH PÁT-BM KÁT, Feladatterv az Elektronikus Kormányzati Gerinchálózatnak (EKG), illetve a Közhálónak az Egységes Belügyi Hálózattal (EBH) történő összekapcsolására, BM Távközlési Szolgálat irattár, Budapest, Iktatási szám: 228-7/2004. ált. (63-386/1/2004.), 1-5. oldal, 2004. július 29.


## Felhasznált irodalom:


[1] A Belügyminisztérium közigazgatási és rendészeti ágazati stratégiájáról (2003-2006) szóló 8001/2003. (BK különszám) BM tájékoztató, Belügyi Közlöny, különszám, Budapest, 7-131. oldal, 2003.

[2] Az elektronikus aláíráshoz és alkalmazásaihoz kapcsolódó monitoring jelentés, GKI Gazdaságkutató Rt. – Nemzeti Hírközlési Hatóság, 2004., http://www.nhh.hu/e_alair2004gki_nhh.pdf

[3] Dr. Baja Ferenc: Reform a kormányzati informatikában, Írások az Internet és a média világáról 2002., Média Hungária Könyvek 4., Budapest, ISSN 1587-3846, 171-180. oldal, 2000.

[4] Fekete Károly: A katonai kommunikációs rendszer szabályozói környezetének változása a zártcélú hálózatok tükrében, A kommunikációs (híradás) helye és szerepe a vezetés tükrében – Országos Tudományos Konferencia Különkiadás, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 119-134. oldal, 2000.

[5] Jobbágy Szabolcs – Serge Gábor: Az Egységes Készenléti Digitális Trönkölt Rádiórendszer, TETRA és TETRAPOL jellemzői, sajátosságai „Kommunikáció 2003.” Nemzetközi szakmai tudományos konferencia, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, ISBN 963 86229 6 2, 119-131. oldal, 2003. október 15.
[6] Mikita János: A katonai infokommunikációs rendszerek fejlődésének főbb irányai, Bolyai Szemle X. évf. 1. szám, Budapest, ISSN 1416-1443, 143-152. oldal, 2001.
[7] Dr. Polyák Gábor: Az elektronikus közigazgatás néhány szabályozási kérdése, Magyar Közigazgatás LIII. évf. 7. szám, Budapest, ISSN 0865 736 X, 405-412. oldal, 2003.
[8] Dr. Verebélyi Imre: A jó kormányzás néhány jellemzője, Magyar Közigazgatás LIV. évf. 5. szám, Budapest, ISSN 0865 736 X, 298-304. oldal, 2004.

**RÉVÉSZ Gyula**

# A HÍRADÓ KIKÉPZÉS MÚLTJA, JELENE ÉS JÖVŐJE

## A katonai híradás fejlődése

A híradás fejlődése is egyidős az emberiség fejlődéstörténetével. Az ősemberek már akkor felismerték annak a tényét, hogy kommunikációra szükség van, amikor még beszélni sem tudtak. A beszéd kialakulása és az alkalmazása után a beszéd tartalmának továbbítása vált kérdésessé. A területeiket ért támadás egyre több, háborúhoz és harcokhoz vezetett, mely során a hordák közötti kapcsolattartást az adott kor alapvető technikai eszközeivel oldották meg amit, nevezhetnénk valamiféle „katonai híradás" alapjának. A katonai híradás jelzéseit leggyakrabban a tűz fénye, füstje használva továbbították, de használtak dobokat, kürtöket és zászlókat is. Ez utóbbit napjainkban is használják.

A középkorban a körülzárásos város háborúk, várháborúk a galambpostamódszer kialakulásához vezetett. Az emberek felhasználása a hír továbbítására a legősibb eredetű. A hír továbbítása a hírvivők feladata volt, akik gyalog, lovon, kocsin közlekedtek. A híradás szóbeli majd írásbeli üzenetek továbbítása volt, amelyet a kor technikai eszközeivel továbbítottak.

A híradás elsősorban és a kezdetekben katonai és később polgári célokat szolgált, arányuk és fontosságuk a kor történelmi helyzetétől függött és országonként változott. A XVII. sz. -ig alapvetően két fegyvernem volt a gyalogság és a lovasság. A műszakiak a XVIII. sz.-ban váltak önállóvá, ők végezték a két fegyvernem kiszolgálását.

A XIX. sz. technikai fejlődése következtében új eszközök jöttek létre. Távíró majd a távbeszélő eszközök fejlődése. (Chappe féle karos Távjelzők, Hughes betűtávíró, Bell-Edison telefon, Puskás Tivadar telefonközpont) A világ első vezetékes elektromos távíróját 1832-ben Siling orosz tudós találta fel és alkalmazta. 1837-ben Morse kidolgozta a még mai használatos távírójeleket. A későbbiek során a távíró jelentett a hadseregekben az elektromos híradóeszközök alkalmazásának kezdetét és innen indul meg a híradás forradalma.

Változás ált be a XIX. sz. második felében, a fejlődő nehéziparban, melynek köszönhetően egyre több új találmány született. Vasútvonalak kiépítésével a hadipar is fejlődik.

A technikai fejlődéssel új eszközök kerülnek a hadseregbe és új szakágak jelennek meg. (Vasútépítés, útépítés, gázvédelem, és a híradás).

A híradás kezdetben műszaki feladat volt. Ez a gépi háború, aminek következtében szükség van a pontos, gyors, megbízható híradásra. Fontossá vált a hadviselésben, hogy a hírváltás nagyobb távolságokban is fenntartható legyen.

A XIX.sz. végén kísérletek a drótnélküli távíró berendezések létrehozására. A rádiózás alapjait Clark Maxvell teremtette meg, majd ezeket a kísérleteket Henrich Herz a hullámterjedésekkel folytatta. A csapatok vezetésének biztosítsa területén hatalmas lépést jelentett Popov felfedezése, aki 1896-ban elsőnek a világon készítette el a rádió ősét, amely segítségével először került megvalósításra a jelek adása és vétele elektromágneses hullámok segítségével. Popov munkájának eredményeképpen a rádiózás rohamos fejlődésnek indult az egész világon. Az 1897 év elején Popov és munka-

társai rádiótávíró összeköttetés létesítetek Kronstadt és egy 640 méter távolságra lévő hajó között. 1899-ben Marconi a kisérleteket folytatva Tesla nagyfrekvenciás transzformátorát és Popov antennáját alkalmazva és Morse távírójával összekapcsolva megalkotja a rádiózást. Az 1900-as évek kezdetétől fogva a rádiótávírót összeköttetésre kezdték használni a haditengerészetben és a hadseregben. 1901-ben már tábori hordozható rádióállomásokat használtak jó eredménnyel. Az Osztrák hadsereg volt, aki először használta fel a géptávírót tábori körülmények között. 1883-ban a Császári és Királyi vasút és távíróezredet két zászlóaljjal felállították. A Lovas és gyalogos jelzőosztagok kiképzése a lajta menti Bruck-i távíróiskolában végzik. (4 hetes távjelző, leolvasó és rejtjelző)

1889. január 1-én Kornenburg-ban indul távíróiskola és Talln-ban lovassági és gyalogsági távíró tanfolyam a távírók hiányának pótlására. 1911-ben a Vasúti és Távíró Ezred szétválik. A hadsereg felismeri a rádiózás katonai jelentőségét és megindulnak a fejlesztések. 1913-ban Meissner megalkotta visszacsatolás elvét, elkészítette az első csillapítatlan rezgéseket létrehozó rezgéskeltőt. Ezzel már a távbeszélő üzemmódot is megvalósították. Az első világháborúban nagy fejlődésnek indult a rádiózás, aminek eredményeként 1920-21-ben a Szovjetunióban és az Egyesült államokban felépítették az első műsorszóró állomásokat.

A hadseregben az első világháborúban főleg szikraadók voltak, második világháborúban már tömegesen alkalmazták a rádiót a csapatok vezetésére. Például: a kurszki csatában egyetlen összfegyvernemi hadsereg 5000 rádióállomással rendelkezett. Az I. világháborúban távbeszélő és távíró szakaszok voltak majd később rádiós csoportok, önálló rádióállomások. A Távíró Ezredben rádiós század alakul. Új szakág alakul ki az ellenséges híradás lehallgatására.

A két világháború között fejlődésnek indul a híradástechnika, az eszközök nagyobb mennyiségben kerülnek a rendszerbe. A szikrát felváltotta a hordozható elektroncsöves távíró-távbeszélő üzemmódban működő berendezések. A háború kezdetére 18 rádiótípust kaptak a rádiósok, többségük magyar termék. A vezetékes technika is, fejlődött ezt is folyamatosan cserélték. A háborút a gépesítés jellemezte, a híradó eszközök, állomások szállítására is jutott gépkocsi. A híradó eszközök többségét még mindig lovakon, szekéren vagy háton szállították.

1945-től a híradó századok vezetékes technikával rendelkeztek jobban.

1946-47 között megkezdték a távírász kiképzést. Ezzel megteremtve a rádiós alegységek személyi feltételeit. 1946-ban katonai kerületparancsnokságokon is folytak híradó képzések. Az úgynevezett „Egységesített tanfolyam" keretében műszerész és tiszti tanfolyam indult. A kiképzést a Honvéd Híradó Szertár állományából végezték. Majd később a „Demokratikus átképző tanfolyamokon" is sok tiszt vett részt. 1947-ben az átszervezés során a 6. híradó század, ami a kiképzésért volt felelős bővítésre került és így megalakult az 1. Önálló Híradó Zászlóalj Pécsen és a vezetékes, rádiós századoknál folytatódtak a híradó tanfolyamok.

**Tiszt és tiszthelyettes képzés:**

1947 őszén a Honvéd Kossuth Akadémián megkezdték a híradó tisztek és tiszthelyettesek képzését. A képzés során egyaránt általános híradó képzettségre oktatták a hallgatókat. A tárgyak alapozó és elméletiek voltak. A nem híradó hallgatók részére híradó ismereteket oktattak saját fegyvernemi szakcsapatuk híradó berendezései kezelését, és rejtjelzéssel kapcsolatos feladatokat. A híradó szakmai kiképzés 1947-

48-ig a Honvéd Kossuth Akadémián folyt. 1949-ben Budapesten a Petőfi laktanyában a Híradó Kiképző Iskola bázisán jött létre a tiszti iskola és a 43. Híradó Ezred, amely a régi 101. Híradó Zászlóalj és a pécsi 1. Híradó Zászlóalj állománya. Később felvette a Zalka Máté nevet. Az iskola parancsnoksága magyar–szovjet vezetés alatt működött. Tartalékos képzés is folyt. A Honvéd Kossuth Akadémián a kiképzési idő először 2 év volt majd 1950-ben 1évre csökkentették. 1950-ben tanulmányi versenyt szerveztek a „kiváló cím" elnyeréséért. Tansegédlettel rendelkeztek és a nehézipar könyveit alkalmazták, híradó felszerelési utasítással, valamint módszertani segédlettet is rendelkeztek.

1951-ben 2 évre emelték a kiképzést és a hallgatók egy éves sorkatonák és újoncok alkották. A tiszti képzés felgyorsul és a tiszthelyettesek képzése háttérbe szorult. 1951 végén kiadtak egy intézkedést, mely szerint a hiányzó tiszthelyettesi helyek tisztesekkel töltötték fel, majd 1952-ben a leszerelő tisztesek továbbszolgálóként töltötték be. 1953-ban megjelent a „Híradó" amely a hallgatóknak adott politikai és módszertani segédletet. 1956 nyarán összevonták a Szentendrei Műszaki Tiszti Iskolával, majd ősszel a forradalom idején szünetelt a kiképzés, mert pesten védelmi feladatot láttak el. 1957-ben, kis létszámban folytatódott a kiképzés, de tavasszal beolvadt a „Egyesített Fegyvernemi Tiszti Iskola" –ba. Itt működött a híradó kiképzés a konszolidáció végéig.

1957-ben Szentendrén megalakult a Központi Tiszthelyettesképző Iskola.

### A felsőfokú tisztképzés:

1948 szeptemberétől a híradó tisztek felsőfokú képzése magasabbparancsnoki és törzstiszti tanfolyamokon vette kezdetét. 1949-től folyamatosan küldték ki a fiatalokat a Szovjetunió akadémiáira, különböző speciális tanfolyamokra. 1951 őszétől indult a Honvéd Kossuth Akadémián a híradó szaktisztek felsőfokú képesítése. Az oktatás módszertani és oktatási segédeszközök hiányában zajlott. 1953-ban színvonalának növekedését jelezte, hogy főiskolává nyilvánították. 1955-ben felvette a Zrínyi Miklós nevet. 1958-tól 4 éves képzés folyt az iskolán és 1959-ben a Magyar Népköztársaság Elnöki Tanácsa egyetemmé nyilvánította.

A felsőfokú képzés másik vonala a mérnök tisztek képzése volt. A „Honvéd Kollégium" hallgatóit a polgári egyetemeken képezték. A tisztek esti vagy levelező tagozatra járt.

### Csapatkiképzés:

A haderő fejlődésével a csapatok vezetésének rendszere is egyre bonyolultabbá vált. A vezetés nagyobb igényű követelményeit ki kellett elégíteni a híradó technikai eszközöknek, ezzel együtt újabb és újabb technikai eszközök jelentek meg. A híradó kiképzést ezekhez az új megnövekedett követelményekhez kellet igazítani. A magyar haderő fejlődése és átalakulása során a híradó kiképzés is változott. A modern magyar haderő fejlődése és átalakulása során három egymással összefüggő időszakot különböztetünk meg:

- Hadkötelezettséggel összefüggő sorkatonai szolgálatra épülő haderő;
- „vegyes" haderő, megjelennek a tisztesi beosztású önkéntesek (szerződéses katonák);
- Csak önkéntesekből álló professzionális haderő.

A csapatkiképzés színvonala a kiképzők és a technikai eszközökkel való ellátottság nagyban befolyásolta. A sorállomány kiképzése központilag kiadott utasítások és intézkedések alapján történt. Az állomány politikai, általános katonai, testnevelési és szakmai kiképzésére nagy hangsúlyt fektettek. Az 50-es évektől a csapatok a kijelölt táborokban tavasztól őszig folytatták a kiképzést. Az új technikai eszközök rendszerbeállításával a sorállomány képzését növelték. Több segédlet jelent meg mely a kiképzést segítette. A tartalékosok kiképzése a kiképző táborokban, de nagy létszám esetén híradó csapatoknál hajtották végre. 1953-ban 8260 fő kiképzését a 43. és a 32. híradó ezrednél, valamint a 2. és 4. vonalépítő zászlóaljaknál végezték. A műszerészek és az új technikai eszközök kezelőállományának kiképzését rendszerint tanfolyamokon végezték. A tanfolyamok a Híradó Szertár, a Híradó Tiszti Iskola, az Akadémia és a HM közvetlen híradó csapatoknál vezették le. A híradó tisztek kiképzésére mindenkor nagy gondot fordítottak. A minőségi követelmények, és a napi gyakorlati élet tapasztalatai határozták meg a híradó tisztek továbbképzését. Minden tiszt meghatározott témakörből készült és parancsnoki csoportokban vizsgáztatták őket. A csapatoknál csoportonként a híradó hadműveleti tisztek részére híradásszervezést, híradóterv kidolgozást írták elő. Az előforduló hiányosságokra miniszteri parancsban megszabták a törzsfőnökök és a híradó tisztek feladatait.

1952-től a szovjet tanácsadók segítségével fokozott fejlődés vette kezdetét. A szovjet hadsereg segédletként rendelkezésre bocsátotta szabályzataikat és akadémiai előírásait. A segédletek és előadások tanulmányozását parancsnoki csoportok keretében nagy intenzitással végezték. Bevezették a szovjet egyezményes jeleket, ami nagy segítséget nyújtott az elméleti anyag elsajátításához. A híradó szakterület elméleti művelése nagyon jelentős helyet kapott ebben az időszakban. 1957- ben felvetődött először a híradó gyakorló terep problémái. A rádiós kiképzés fejlesztése érdekében különböző versenyeket hirdetett a főnökség. Az egyik ilyen, pl. a Távírász verseny, mely a híradó főnökség szervezésében évenként került megrendezésre. A versenyen a legképzettebb rádiós állományú távírászok vettek részt, ahol a hangolvasás és a billentyűzés elért üteme és a hibaszázalék alapján állapították meg a helyezéseket. Később kiegészült még a berendezések ismeretével is. A Magyar Néphadsereg Híradó Szakmai Versenyét is a híradó főnökség szervezte és vezette, de a verseny helyszíne mindig más híradó zászlóalj berendezett táborában jelölték ki. Itt előre kidolgozott rádiós, vezetékes, központ- és vivőkezelő feladatokat kellett végrehajtani harcászati körülmények között.

A szakkiképzők és a kiképzési feladatok a szervezeti fejlődéssel és a technikai eszközök rendszerbe állításával összhangban fejlődtek. A híradó főnökség nagy figyelmet fordított az állomány kiképzésére, továbbképzésére, valamint a híradó csapatok kiképzésének irányítására.

### Sorkatonákra épülő haderő

A híradó katonák kiképzését – mind az alapkiképzés, mind a szakkiképzés – a saját alakulatuknál kapták meg. A sorkatonai szolgálat időtartam a haderő átalakulásával folyamatosan változott. A sorkatonai szolgálat lerövidülésével a kiképzésre is kevesebb idő lett fordítva. Általánosságban el lehet mondani, hogy ebben az időszakban a kiképzés két részre bomlik:

- Alapkiképzés: általános katonai ismeretek megszerzése;

- Szakkiképzés: két részre bontható, szakalapozó felkészítés, amely során az adott szakbeosztásra történő felkészítés történt, és a szakharcászati felkészítés, amely során más híradó eszközökkel való komplex működést gyakorolták be.

Ennek a haderőnek volt egy önkéntes jellege is, ezt tovább szolgálatnak hívták. Az adott sorállományú katona elöljárója javaslatára folytathatta katonai szolgálatát. A sorállományú idő után 2 év próbaidő következett, majd ezután hivatásos állományba került, mint tiszthelyettes.

Ezen haderőnek a legnagyobb előnye az volt, hogy az adott katona kezelői szinten elsajátította a technikáját illetve a gyakorlatok sűrűsége miatt nagyon sok gyakorlati tapasztalatra tett szert. A kiképzések ideje alatt az I időszakos katona szolgálatot nem adott , a szolgálatokat a II, III, időszakos katonák adták.

A legnagyobb hátrányát a sűrű gyakorlatok illetve a nagy létszám miatt a költségessége jelentette.

### „Vegyes" haderő – szerződéses katonai szolgálat

A haderő átalakulásával ezzel együtt csökkenésével megjelent az un. szerződéses katonai szolgálat, ami azt jelentette, hogy az önkéntessel aki vállalja a katonai szolgálatot (általában tovább szolgáló sorkatona) egy határozott idejű munkaszerződést kötöttek. A kiképzésben részt vett, de neki már munkaideje volt ugyanúgy, mint a hivatásos katonának.

A haderő átalakítása során megszüntették az alakulatoknál az alapkiképzést és a szakalapozó kiképzést erre a feladatra hozták létre a kiképzőközpontokat. Ahol már nem csak konkrétan szerződéses katonákkal foglalkoztak, hanem a katonai végzettséggel nem rendelkező önkéntes szerződéses katonák kiképzésével is.

Legnagyobb előnye, hogy magyar haderőben kezdtek megjelenni az olyan katonák akikre huzamosabb ideig lehetett számítani, erre szükség is volt mivel a sorkatonai szolgálat ideje nagyon lecsökkent.

Hátránya, hogy a technikai eszközök korszerűtlenné és elhasználódottá váltak, de a feladatukat a javítások karbantartások elvégzése után még mindig el tudták látni.

### Professzionális haderő

Csak szerződéses és hivatásos katonákra épülő haderő. A szerződéses katonák képzésénél az elsődleges szempont a célirányos kiképzés, tehát konkrétan a beosztásával kapcsolatos feladatokat maximálisan ismerje, és ezeket folyamatosan fejlessze.

Előnye, hosszú időre lehet számolni viszonylag állandó állománnyal, követelményszint növelhető, takarékosabb kiképzés, ütőképesebb.

Hátránya a kiképzést nehezíti az elavult technika, az ezekhez a technikákhoz kapcsolódó javítóanyag hiánya, kiképző helyek hiánya és a kisebb költségvetés kereteket a gyakorlati képzésnek (mobilitásnak).

A II. Világháborút követően új magyar rádiókészülékek. (R-10-től R-50-ig) A szovjet behatás érvényesül a Magyar Néphadseregben. A Varsói szerződés hatására a híradó eszközök cseréje beindul, és 1960-70 között ellátják az alakulatokat. Ezek a rádiók még a mai napig rendszerben vannak és használjuk őket. Ezek az R-130, R-111, R-123, R-140, R-137, R-107, R-159, R-1260, Troposzféra rádióállomás, Relék: R-1412, R-1406, Mikro: R-404, R-414.

A 80-as években kísérleti jelleggel műholdas híradást üzemeltettünk. A rács-rendszerű híradás gondolata már a 80-as években felvetődött, de szovjetek nem engedték mert az irány-tengely híradást alkalmazták.

Napjainkban még mindig az analóg rádiók vannak többségben, de már a rendszerváltás után megjelentek az új digitális eszközöket is. A digitális eszközök megjelenésével szükségessé vált a készülékekre történő kiképzés. (Digitális központok: HICOM 300E; Rádiók: Harris, MRR; Műholdas telefonok: Turaya, Motorola) Ezeket központi tanfolyamokon valósították meg. Ezekre a tanfolyamokra a csapatoktól iskoláztak be az állományból, de a tiszti és tiszthelyettes képzésben is oktatták.

Napjaink rohamosan fejlődő kommunikációs igényei a Magyar Honvédségnél is jelentkeztek. Az analóg kapcsolástechnika kiváltásának folyamata napjainkban is zajlik, a rendszer homogenitásáig még hosszú időnek kell eltelnie. A tervezett, a jövőben hadrendbe állítható katonai kommunikációs eszközök, hírhálózatok működése elkerülhetetlen az előzőekben említett kiválóan tréningezett katonák nélkül. Ezen állomány számára a sikeres feladat végrehajtás szempontjából legfontosabb a rendszerszemléletű gondolkodásmód, amely azt jelenti, hogy képes legyen az adott feladathoz kiválasztani a legmegfelelőbb kommunikációs rendszer felépítését, az alkalmazott módszereket, az összeköttetéseket, az alkalmazásra kerülő eszközöket. A legmodernebb technikai eszközök sem alkalmazhatók kezelőszemélyzet nélkül, tehát a kezelő állomány felkészítését is képesnek kell lennie irányítani, a megfelelő oktatási kérdéseket meghatározni, melyek alapján a tiszthelyettes állomány megtarthatja a kiképzést.

A modern távközlési hálózatok egyre bonyolultabbá válása megkívánja az üzemeltetés központosítását, ezzel egyidejűleg, olyan rendszerek beszerzését, amelyek megvalósítják ezt a központosított felügyeletet és vezérlést, az egész országot lefedő távközlési hálózaton. Ezek az eszközök elősegítik a jobb minőséget, és magas szintű szolgáltatások nyújtását. Az üzemeltetés terén költségmegtakarítást és hatékonyságot eredményez, és egységesítést a hálózaton belül.

A hivatásos állománynak el kell sajátítania az új digitális rádiók, és más híradó eszközök rendszerben történő használatát, azok beillesztését a hálózatokba, azokkal történő szervezési, tervezési munkák elvégzését.

A tiszthelyettesi állomány a kivitelezés és megvalósítás legfontosabb rétege, számukra elsőrendű feladat az eszközök teljes mértékű ismerete, alkalmazása, illetve a beosztott állomány felkészítése.

A kiképzésen megfelelő mennyiségű, minőségű szemléltető eszközöket, segédeszközöket, trenazsőröket kell alkalmazni, illetve az éles gyakorlatok számát növelni kell a kiképzési tervekben.

A műholdas összeköttetés kiemelt jelentőségű az új kommunikációs rendszerben, ez az egyetlen átviteli út, amelyet a Magyar Honvédség nem használt a régi (analóg) eszközök alkalmazása során. Mára a külszolgálatok fontos összeköttetési vonala a műholdas kapcsolat.

A jelen és a jövő új technikai vívmányai közé tartozik az előző eszköz mellett a „digitális katona” által alkalmazott eszközök, video-konferencia összeköttetések, és számos újítások, melyeket a nyugati országok hadseregei már alkalmaznak.

## Összegzés

Összegezve, a jövő katonáinak ismernie kell a számítástechnikai eszközöket, alkalmazásokat, a digitális rendszereket, magas szintű nyelvtudás birtokában kell lenniük.. A tiszt állománynak szervezői, tervezői, a tiszthelyettesi állománynak technikai és kiképzési ismeretekkel, a szerződéses legénységi állománynak pedig kezelői ismeretekkel kell rendelkeznie.

A civil szférában a kommunikációs információs hálózatok és eszközök sokkal nagyobb ütemben fejlődnek, mint a katonai téren. Ennek oka egyértelműen a sokkal nagyobb piac a civil szférában. Kevés cég foglalkozik katonai alkalmazásra szolgáló berendezésekkel. Éppen ezért, hogy a hadsereg ne maradjon le technikailag, a kereskedelmi célokra gyártott rendszereket kénytelen alkalmazni. Ez persze nem minden esetben tesz eleget a NATO-irányelveknek. Napjainkban és a jövőben is a civil informatikai és a távközlési technológiák és eszközök fejlődési irányvonala határozza meg a Magyar Honvédségben alkalmazott eszközöket is.

**TESSEDIK Tamás**

# SZOLGÁLTATÁSMENEDZSMENT EGY TÁVBESZÉLŐ SZOLGÁLTATÓ INFORMÁCIÓ BIZTONSÁGI KÖVETELMÉNYEINEK SZEMSZÖGÉBŐL

Tessedik Tamás PH.D doktorandusz
Pannon GSM Távközlési Rt., Biztonsági igazgató

## Az információ és IT biztonság kialakításának alapjai

A távbeszélő szolgáltatók feladat köreit a szokásos piaci tevékenységeik mellett léteznek további jogszabályi kötelezettségek is. Ezeket a feladatokat – részletezés nélkül - az alábbi jogszabályok írják elő:

Elektronikus Hírközlési Tv.

- A nemzetbiztonsági és rendvédelmi szervek működését és feladatrendszerét szabályozó törvények, kormány rendeletek és más utasítások és rendeletek,
- Az adatkezelést meghatározó adatvédelmi jogszabály és állásfoglalások alkalmazása,
- A katasztrófa elhárításáról szóló jogszabályok és végrehajtási rendeletek
- A szolgáltatás kimaradásával kapcsolatos intézkedési rendek és eljárási utasítások valamint a rendkívüli helyzetek re vonatkozó szolgáltatás átmeneti szüneteltetése, illetve korlátozása.

Természetesen még számos más jogszabály is meghatározó szerepet játszik a szolgáltató működésében, de azok nem részei ennek az összefoglaló munkának. Az itt tárgyalandó szolgáltatásmenedzsment témakör összetettségét az alábbi gondolatok támasztják alá:

- A vállalat mindenkori stratégiai menedzsmentje,
- Az operatív feladatok végrehajtásának menedzsmentje,
- Az információ áramlások menedzsmentje,
- Az alkalmazott szabványok és eljárások menedzsmentje.

E négy gondolat csoportot csak együtt – egy közös rendszerben – lehet kezelni.

Amikor egy vállalat stratégiai menedzsmentjéről beszélünk, akkor azt a jövőben megvalósítani kívánó feladatrendszert képzeljük, amit a külső és belső környezeti tényezők hatásai mellett reálisan megvalósítani szándékozunk. Az elmúlt évtizedek stratégiai menedzsment elvei más és más megközelítési elveken alapultak, de mindig nagy figyelmet szentelt a piaci szereplőt érő külső környezeti hatások alakulására.

Ennek megfelelően meghatározó külső tényező volt a stratégiai menedzsment kialakítására pl. a ’70-es évek második felében bekövetkezett energiaválság vagy a ’80-as évek első felében lejátszódó munkanélküliségi nyomás, illetve a ’80-as évek második felétől tömegesen megjelenő IT technika és technológia felhasználása.

E külső tényezők közé került be a legutóbbi időkben a piaci szereplők biztonságát veszélyeztető tömeges méreteket öltő terror fenyegetettségek vagy a napjainkban egymást érő katasztrófa események.

Ez utóbbi tényezőknek, a fenyegetettségnek a felismerése a korábbi időszakokban nem játszott önálló meghatározó tényezőt. Ez az új felismerés, természetesen a biztonsági célok meghatározását is illetve azok még pontosabb és közvetlenebb beintegrálását kívánta meg, ami egyben komoly kihívást indikált a stratégiai célok megvalósításában közreműködő minden egyes szervezeti egység számára is.

A stratégiai menedzsment célmeghatározásai a napi operatív feladatok végrehajtásában és a kiépített információ áramlás megvalósulásában ölt testet. Mivel a stratégiai menedzsment az operatív végrehajtással szoros szinergiát mutat, ezért ebben a dolgozatomban ez utóbbival nem szeretnék külön foglalkozni. Ugyanakkor kiemelkedő funkciója van az információáramlás jellemzőinek és szabályozottságának. Ezeket a tényezőket az alábbi szempontok szerint lehet csoportosítani:

- Az információ tartalma,
- Az áramlás iránya, gyakorisága, rendszerességének jellege,
- Az információt hordozó technikai architektúra topológiája,
- Információ és informatika biztonsági alapelvek gyakorlati megvalósulása,
- A szervezet, mint rendszer az új biztonsági kihívások és a biztonsági tudatosság értelmi belátása.

Ezek a felsorolt tényezők együttesen gyakorolnak hatást a stratégiai menedzsment megvalósításában. A XXI. Század egyik nagy kihívásának mutatkozik a nagyarányú, vagyonkárt okozó és egyben tömeges áldozattal járó természeti katasztrófák vagy az előre nehezen felderíthető terror események hatása. A polgári szférában dolgozó vállalatok, közintézmények, piaci szereplőknek van egy jelentős szegmense, melyeknek alap funkcióik mellett felelős közreműködést vállalnak a nemzetbiztonsági, rendvédelmi, nemzetvédelmi és katasztrófa védelmi főhatóságok feladatainak ellátásában. A továbbiakban ezen intézmények közül kizárólag a távbeszélő szolgáltatók biztonsági feladat ellátásainak egy szegmenséről, az információ biztonsági tudatosság felépítésének szervezési metódusával foglalkozom.

Függetlenül attól, hogy az említett közreműködők az információáramlás zavartalan vagy tudatosan szabályozott, illetve korlátozott áramlásával találkozunk a telekommunikációs biztonság szempontjából, nagy hangsúlyt kell fektetni a szervezett és szigorúan és következetesen kontrollált prevenciónak. A prevenciós elvek gyakorlati alkalmazására több könyvtárnyi irodalom is a rendelkezésünkre állhat.

A prevenció rendszerét az alábbiak szerint csoportosíthatjuk:

- Dokumentált elvek;
  - Jogszabályok, rendeletek, kormány szintű határozatok és utasítások,
  - A közreműködő piaci szereplő speciális együttműködési leírásainak dokumentációi,
  - A stratégiai üzleti szereplők egymás közötti megállapodások dokumentációs rendszere (Az erre vonatkozó lehetőségekről és korlátokról külön jogszabály intézkedik.),
  - A stratégiai szereplő belső működését meghatározó szabályozó elvei és azok dokumentációi,
  - Az alkalmazott szabványok vagy szabvány rendszerek.
- Fizikai elvek
  - Adat és információ tárolás fizikai védelmi elvei (Ebbe természetesen bele tartoznak az objektum, az adatkezelési rendszabályok fizikai tárolási rendje),

- Az információ vagy adatátadás fizikai védelmi elvei (Ebbe a kategóriába tartoznak a hozzáférési topológia vertikális és időbeli horizontális fizikai védelmi megvalósításai, valamint a kommunikációk folyamatos nyilvántartási rendjeinek kialakítása is.),
- A telekommunikációs eszközök karbantartása, folyamatos üzemeltetésének biztosítása, kiesések helyre állítása és az ismételt folyamatos üzembe állítás fizikai biztosítása,

Azzal együtt, hogy ezeket a pontokat valamilyen rendezési elv alapján rendszerbe igyekeztem foglalni, könnyen felfedezhető, hogy a két nagy gondolati csoportnak van közös kezelési felülete. Ezeket a közös rendezési elveket találjuk a legkülönbözőbb minőség biztosítási szabványokban, melyeknek egy külön csoportját képezik az IT biztonsági szabványok. A szabvány ebben a funkciójában nem helyettesíti a dokumentált elvekben, a fentiekben részletezésre került összefoglaltakat. Erre konkrét példa az adatkezelés kategóriája.

Az adatkezelés adatvédelmi kategória, amely meghatározza az adatok gyűjtését, tárolását, feldolgozását, betekinthetőségét, módosítását, továbbítását, valamint törlését és megsemmisítését. Az adatkezelés során az ügyfelek adatait kezelik a szolgáltatók, amelyek lehetnek szerződésben rögzítettek vagy a számlázáshoz kötődő forgalmi típusú adathalmaz. Az adatvédelem számos alapelveiből – a dolgozat szempontjából – csak hármat emelnék ki:

- az adatminőséget, tárolhatósági elvet
- az adatbiztonságot, ez foglalkozik az adatok valódiságával
- és a célhoz kötöttséget, amely meghatározza, hogy ügyfél adatát csak konkrét esetekre, adott célból és időtartamig lehet kezelni.

Ahhoz, hogy az adatkezelő a szolgáltatás minőségének szinten tartásához vagy növeléséhez hozzá tudjon járulni, az alábbi megfontolásokat kell szem előtt tartania:

a szolgáltatás értéknövelését biztosító, információ biztonságot garantáló minőség biztosítási alrendszer meghatározása, a megfelelő szabvány kiválasztása és bevezetése, alkalmazása

az információ biztonsági kritériumok meghatározása, melyeket három csoportba lehet sorolni:

- bizalmasság, a fogyasztó részéről bizalom az adatkezelő szakmai képességeiben,
- sérthetetlenség, amiben az adatkezelő megteremti az összes feltételt az adatbiztonság garantálására,
- rendelkezésre állás, üzletviteli folytonosság biztosítása, esetleges kiesés esetén az eredeti állapot visszaállításának a garantálása.

Ahogy említettem, ezek nagyon speciális szolgáltatások melyek a nem látható kategóriákba tartoznak, ugyanakkor hibás működésük vagy teljes működés képtelenségük teljes mértékben tönkre teheti a szolgáltató cég piaci hírnevét és elveszthetti fogyasztóinak teljes bizalmát. Mindezek mellett biztonsági feladatainak ellátásában is csorba eshet.

Visszatérve a szabvány alkalmazási elvekre, megállapítható, hogy azok funkciói és működés szabályzó elvei nem helyettesítik a dokumentációs és fizikai elveket, és nem kérdőjelezi meg azok működési alapelveit. Sokkal inkább integrálni kívánja a már meglévő rendszer lehetőségeket, a szinergia elvnek megfelelően, azonos szemlé-

letbeli koncepciók alapján. Összességében, tehát megállapítható, hogy a szabványrendszerek alkalmazásának elve szorosan korrelál a biztonsági tudatosság elvéhez.

Dolgozatom további részében arra térnék ki, hogy hol tart ma a hazai piaci szereplő ennek megítélésében, hogyan alakult az elmélet a gyakorlathoz képest, valamint milyen kiválasztási szempontok szerint kerültek meghatározásra az egyes szabványok és azok milyen területeken kerültek bevezetésre.

## Információ biztonsági szabványok és alkalmazási területeik

A nemzetközi irodalom számos információ biztonsági és informatikai minőség biztosítási szabványt említ. Az elmúlt évtizedek során azok a szabványok és megoldások bizonyultak életképesnek, amelyek a szervezet üzleti céljaiból és stratégiájából kerültek levezetésre, valamint az eddig többségében termékorientált szemléletet, illetve az értékelési, tanúsítási és minősítési folyamatok meghatározását egy szervezeti szintű, informatikai biztonságmenedzsment központú szemlélet váltotta fel.

A telekommunikációs szektor (első sorban mobil szektor) a minőség biztosítás bevezetésével a 90-es évek közepén kezdtek foglalkozni. Első sorban a vállalat egészére kiható minőség menedzsmentet kezdtek bevezetni és csak a későbbiekben indult meg az önálló információ biztonsági menedzsment létrehozása. Az alábbiakban összefoglalom a legfontosabb minőség biztosítási szabványokat.

- Common Criteria 2.1 (ISO 15408)

A CC alatt ismertté vált szabvány lényege, hogy egyesíti a tengeren túli TCSEC (Trusted Computer System Evaluation Criteria - Kritériumok a számítógéprendszerek megbízhatóságának kiértékeléséhez) és az európai ITSEC (Information Technology Security Evaluation Criteria – Információtechnológia Biztonsági Értékelési Kritériumok) szabványok előnyeit és igyekszik kiküszöbölni a hátrányos tényezőket. A fő jellemzői az egységesítési elv, módszertan, értékelési és auditálási folyamat.

- ITIL

Az ITIL (IT Infrastructure Library) módszertant a CCTA (Central Computing and Telecommunications Agency – Központi Számítástechnikai és Telekommunikációs Ügynökség) munkatársai fejlesztették ki jó minőségű, költség-hatékony IT szolgáltatások támogatása céljából. Az ITIL-t úgy kell elképzelni, mint egy tudásbázis könyvtárt, amely a best pracise alapon a legjobb gyakorlati megvalósításokat gyüjti és ajánlásként javasol.

- ISO/IEC 1799

A Common Criteria (ISO/IEC 15408:1999) mellett a másik nemzetközileg is elfogadott és elismert szabvány. Az információbiztonság menedzsmentjének gyakorlati kódexe. Ez a szabvány nem követelményeket ír elő, hanem – a minőségbiztosításra vonatkozó ISO 9000-es szabványokhoz hasonlóan – a teljes körű informatikai biztonság megteremtéséhez szükséges szervezési, szabályozási szempontrendszert adja meg.

- ISO

Az ISO 9000-es szabvány sorozat a szoftver fejlesztésre és karbantartására ad meg ajánlásokat. Habár önmagában a benne rejlő ajánlások nagy horderejűek , mivel azonban a szolgáltatás támogatásának csak rész feladataira ad megoldást , ezért nem tekinthető teljes körű szabványosításnak.

- COBIT

A Common Criteria és az ISO 17799 mellett az ISACA (Information Systems Audit and Control Association – Nemzetközi Informatikai Auditorok Egyesülete) által

kidolgozott COBIT (Control Objectives for Information and Related Technology) a harmadik olyan nemzetközi szabvány, amely alapján a szolgáltatásmenedzsmentet támogató informatikai rendszerek fejlesztését és üzemeltetését biztonságosabbá lehet tenni. A COBIT a nemzetközileg elfogadott informatikai kontroll célok olyan gyűjteménye, amely általánosan alkalmazható és elfogadott az informatikai biztonsági rendszerek területén.

A minőségbiztosítási szabvány rendszerek integrálása és a legfőbb tapasztalatok

A telekommunikációs szolgáltató cégeknek, amelynek szakadatlanul eleget kell tenniük a folyamatosan változó informatikai környezet kockázatkezelésének, a kontrollok kialakításához szükséges beruházások mérlegelésének, valamint az ügyfél bizalom megőrzésének (pl. stabil számlázó rendszer, megbízható logisztikai folyamatok, stb.)

A fentiek alapján a kiválasztási folyamat egyáltalán nem tűnik egyszerű feladatnak. Az egyes szabványok sok esetben lefedik a vállalati elvárásokat, azonban mindig lehet találni, olyan egyedi tényezőket, eseteket, amelyek kizárták az egy eszköz bevezetésének lehetőségét. Ezért az utóbbi években a stratégiai menedzsment egyre inkább a több szempontú, de még nem integrált szabványrendszer bevezetését preferálja. A szolgáltatói folyamatok esetében, az utóbbi időben a COBIT 3 szabvány látszik teret nyerni, míg az információ biztonsági elvek megvalósítására a CC szabvány ajánlásai kerülnek az előtérbe. A két meghatározó minőség biztosítási rendszer mellett további – rész feladatok lefedésére alkalmas – minőség biztosítási rendszereket is bevezetésre kerülhetnek. Ezeknek a funkciói elsősorban az ügyfelek bizalmának megőrzésére kerültek bevezetésre. Ezek közé tartoznak az auditált számlázó rendszerek, valamint a bemutató termeket ellátó alkalmazások.

A fentiek alapján három lényeges gondolat már megállapítható, ezek pedig:

- Az új stratégiai menedzsment feltétel rendszeréből nem hiányozhatnak a biztonsági elvek, melyeknek integrált része a biztonsági stratégiai rend. Függetlenül attól, hogy a stratégiai szervet a támadott vagy aktív részvevője a veszélyelhárításnak.
- A vállalatok működési folyamatait szabályzó szabványok széles tárházában ma már egyre inkább kerülnek elő azok az ajánlások, melyek alapelvként kezelik a biztonsági követelményeket.
- A jelenlegi több szempontú szabvány ajánlások „önálló szigeteket” alkotnak, nincs meg a teljes átjárás az egyes modulok között. Ezért szükség lesz egy olyan eljárásra, amelyik biztosítja az egyes szabvány technológiák közötti szabványos átjárást. Ezt nevezhetjük a jövőben integrált vállalati biztonsági szabvány rendszernek.

**Befejezés**

Ennek a dolgozatomnak az volt a célja, hogy rámutassak, milyen összetett feladatot is jelent a szolgáltatásmenedzsment kialakításakor a minőség biztosítás megvalósítása. Számos vállalat esetében lehet tapasztalni, hogy egy bevezetett minőség biztosítási eljárás önmagában nem képes a teljes vállalati folyamatokat lefedni, ezért fordul elő – és más vállalatok estében ezt már tapasztaltam – hogy csak nagy erőltetések árán igyekeznek a minőség biztosítási és controll rendszereiket üzemeltetni. Egyre több vállalat esetében tapasztalom, hogy a szolgáltatásmenedzsmenti feladatokat tá-

mogató információ biztonsági rendszerek nem egy és kizárólagos szabvány szerint kerül kialakításra, hanem több szabványt alkalmaznak aszerint, hogy melyik felel meg a vállalat adott folyamataihoz.

Korunk biztonsági, védelmi és üzleti stratégiája sokkal szorosabb együttműködést vár el,a biztonságért közvetlenül felelő és a piaci szereplők között, mint bármikor korábban. Ez az új helyzet alapozza meg az egyes közszolgáltatóknak és piaci szereplőknek a biztonsági feladat rendszerét.

**Dr. VÁNYA László**

# FORRADALMIAN ÚJ ELJÁRÁSOK A RÁDIÓ- ÉS RÁDIÓTECHNIKAI ZAVARÁSBAN

Dr. Ványa László okl. mk. alezredes
Zrínyi Miklós Nemzetvédelmi Egyetem Informatikai tanszék
1101 Budapest, Hungária krt. 9-11.
E-mail: vanya.laszlo@zmne.hu

## Bevezetés

Az elektronikai zavarás a kommunikáció megszületését és fejlődését árnyékként követő területe a katonai tevékenységeknek. Ahogy a 20. század elején a rádióhírközlés, majd a 40-es években a radartechnika megindult hódító útjára, úgy vette kezdetét a velük vívott küzdelem is - a rádióháború -, később rádióelektronikai harc, mai terminológiánk szerint - az elektronikai hadviselés. Ebben a kétoldalú harcban általában előbb a kommunikáció és a radartechnika lépett a fejlődésben előre, majd ezt követte, mintegy válaszként a zavarási technikák fejlődése.

Jelen előadás előbb azt a fejlődési utat mutatja be, amelyet e két terület egymás mellett élve és szüntelenül fejlődve befutott, majd a jelen és a várható közeljövő kérdéseit vizsgálja.

Kiemelt figyelmet érdemel az elmúlt mintegy tíz-tizenöt év, amely során úgy tűnt, hogy a digitális kommunikációs és radartechnológia igen komoly lépéselőnyre tett szert a zavarással szemben. A helyzet kialakulásában közrejátszottak a két világrendszerben lezajlott társadalmi-politikai változások is, de világossá vált az is, hogy gyökeres szemléletbeli és technológiai szemléletváltás szükséges ahhoz, hogy a modern infokommunikációs rendszereket üzemeltető katonai és más szervezetek vezetési rendszereivel, hálózataival ismét hatékonyan fel lehessen venni a harcot.

Ebben az előadásban a figyelmet kiemelten a katonai rádiókommunikációra és radartechnikára fordítjuk, de tudni kell, hogy az elektronikai hadviselés a fizikai spektrum valamennyi más tartományában is széleskörű felderítő, zavaró és védelmi tevékenységet folytat a szembenálló fél személyi állományával és szinte valamennyi harci technikai eszközével, amelyre most nincs mód részletesen kitérni. Ahhoz, hogy jobban megérthessük a rádió és rádiótechnikai felderítés, zavarás mai problémáit és azok megoldásának lehetséges új módjait, előbb a múlt tapasztalatait kell röviden áttekintenünk.

## A kezdetektől a 2. világháborúig

A drótnélküli távíró 1896-os első bemutatóját követve csak néhány év telt el addig, amíg az akkoriban még igen nagy méretű és energia felvételű rádióállomások megjelentek a hadseregekben, elsősorban a hajókon és a stabil objektumokban. Az első rádiótávíró berendezések alkalmazásáról a feljegyzések 1904-es keltezésűek. Az 1905-ös orosz-japán háborúban az orosz flotta két hajóraja a Szuvorov és az I. Miklós vezérhajó irányítása alatt rádiótávíró berendezéseikkel navigáltak a Van-Fong-öbölben. A rádiók megjelenésével egyidőben a kezelők az ellenséges japán rádióforgalmazást is hallották, így azonnal felmerült a lehallgatás, valamint a zavarás gondolata is.

Az 1905-ös csuzimai tengeri ütközetben az aktív rádióharc is kezdetét vette, amikor is az orosz hajók fedélzeti rádió berendezéseivel megzavarták a japán flotta híradását. Ugyanakkor a történetíró feljegyzése szerint a manővereket irányító Rozsgyesztvenszkij tengernagy határozott kérése és indokai ellenére sem engedélyezte az Ural cirkáló parancsnokának, hogy korszerű rádiótávíró állomását zavarásra használja, ami valószínűleg az első, de bizonyosan nem az utolsó „szakmai vita" volt a zavarás harci alkalmazását illetően.

A rádiólehallgatás és a rádiózavarás veszélyeit a hadvezetés hamar felismerte. Komoly erőfeszítéseket tettek például a közlemények fedése, kódolása érdekében, vagyis az évezredek óta ismert és oly gyakran különböző módszerekkel folyó rejtjelzés és kódfejtés behatolt a rádiótechnikába is. A kódtáblák, kulcsok, eszközök és dokumentumok megszerzése az ügynöki felderítés kiemelt feladatává vált. A rádióháború tehát ebben az időben a lehallgatást, a zavarást és az ügynöki információszerzést foglalta magába.

A technikai fejlődés rohamléptekkel haladt. Az 1910-es évekre elkészültek az első gépjárműbe épített rádiók, majd nem sokkal később a hordozható típusok is szolgálatba álltak. Az első világháborúban már szervezetszerű híradó alegységeket, tábori hírközpontokat alkalmaztak a vezetés támogatására. A háború jellegéből adódóan a híradás előbb döntően vezetékes eszközökkel folyt, azonban a kábelek sérülései miatt a híradó alegységek a javításra kiküldött katonáik közül jóval nagyobb veszteségeket szenvedtek el, mint a többi gyalogos alegység. Ez is a rádiók elterjedése mellett szóló érv volt.

Komoly ellenérzést, sőt ú.n. „rádióiszonyt" okozott az a harci tapasztalat, hogy azok az alegységek, amelyek rádiókat használtak, rövid időn belül komoly tűzcsapásokat szenvedtek el. Ezt az tette lehetővé, hogy kifejlesztették a rádió-helymeghatározás első eszközeit, a rádiópelengátorokat, amelyekkel meglehetősen pontosan bemérték az üzemelő rádiókészülékek helyét és tüzérségi tüzet vezethettek rájuk. Az első harci repülőgépek fedélzetükön már hordoztak szikratávíró berendezéseket, előbb felderítési, tűzvezetési, majd csapásmérési feladatokban alkalmazva azokat. A bevetések hatékonyságát nagymértékben növelték a köteléken belüli, és a földi irányító pontokkal folytatott hírváltások.

Az első világháborúban a rádiólehallgatás, a pelengálás (helymeghatározás), zavarás mellett komoly szerepet kapott a fontos rádióberendezések megsemmisítésére való törekvés, amely a mai napig az ellenük vívott harc egyik fontos módszere.

Az első világháborúban szervezetszerű alegységeket nem alkalmaztak a lehallgatási, zavarási feladatokra, ezek a híradó alegységekre hárultak. A légvédelemben ez időben hírközlési, riasztási és értesítési feladatokra alkalmaztak rádiókat, a légierő repülőgépein általánosan elterjedtek voltak.

A bombázók és vadászrepülők fejlődése a harmincas években egy újabb nagy háború sötét árnyát vetette előre. A harmincas évek elején mind német, mind angol hajókon végeztek rádióhullám visszaverődési kísérleteket. Először úgy gondolták, hogy csak nagyméretű fémtárgyak detektálására alkalmas ez a módszer, vagyis elsősorban a hajók bemérésére. Nagy-Britannia hadvezetése felismerve Robert Watson-Watt rádióhullámokkal való helymeghatározási kutatásainak jelentőségét, 1935-ben döntést hozott a radarállomások megépítésére a Temze két oldalán. Az először meg-

épült öt állomás segítségével mintegy 200 km-ről lehetővé vált a 350 és 3500 m közötti magasságon repülő gépek felfedése és tevékenységük megfigyelése.

Előbb a 10 m-es hullámhosszon üzemeltek a radarok, majd a technikai fejlődésnek köszönhetően egyre magasabb frekvenciákon, amely egyre pontosabb mérést tett lehetővé. Jelentős erőfeszítéseket tettek mind a németek, mind az angolok a radarok kutatás-fejlesztése területén. Ezzel együtt aktív zavaró berendezésekkel és passzív dipólszóró eszközökkel is eredményesen kísérleteztek.

A 30-as évek közepétől a legnagyobb szovjet városok köré többlépcsős légvédelmi figyelő és jelzőőrs rendszert telepítettek, amelyeket RUSZ-1, majd RUSZ-2 rádióbemérő állomásokkal láttak el. Ezeket a fontos irányokban léggömbzárral is kiegészítették, mivel az angol radarokhoz hasonlóan ezeknek sem volt megfelelő a kismagasságú repülők felderítési valószínűsége.

## A 2. világháborútól a két világrendszer felbomlásáig

A 2. világháborúban először az angol-német összecsapások során beszélhetünk szervezett elektronikai hadviselési tevékenységről. Az angol területeken egyre több és korszerűbb rádióbemérő, lehallgató és zavaró berendezést alkalmaztak. Kiemelkedő szerepet kapott a rádióelektronikai dezinformáció, ami egyrészt hamis közlemények tartalmával, majd hamis elektronikai objektumok üzemeltetésével okozott nagyon sok esetben fejtörést a felderítésnek, illetve a hadvezetés egészének.

A rádiótechnika fejlődése úgy a szárazföldi hadműveletekben, mint a légi és tengeri csatákban egyre komolyabb befolyással bírt. A szárazföldi erőket a rövidhullámú rádiók mellett egyre több ultrarövid hullámú készülékkel is ellátták. Megoldották az úszó aknák és tengeralattjárók radaros felderítését, ami jelenős hatással volt a konvojok biztonságának növelésére. Olyan kiemelkedő események fűződnek a rádiófelderítés és a rejtjelfejtés sikereihez, mint a német flotta büszkeségének, a Bismarc csatahajónak elsüllyesztése. Mennyiségi és minőségi szempontból egyaránt nagyon jelentős előrelépés történt a harcoló feleknél, ugyanakkor nem tulajdonítottak egyformán megfelelően nagy jelentőséget az új eszközökben rejlő lehetőségeknek. Egyes hadtörténészek úgy tekintenek a radarra, mint a 2. világháború kimenetelét eldöntő egyik kulcseszközre.

A rádiótechnika mellett a robotika, az automatikus irányítás is jelentős fejlődést mutatott. A rádió parancsvezérlés, a vezetősugaras irányítás, a közelségi rádiógyújtó egyre szélesebb alkalmazást nyert. A háború évei alatt intenzív fejlesztés folyt a sajátellenség felismerő berendezések területén is, amelyek lehetővé tették, hogy a vadászgépek felismerjék a saját gépeket, a megfigyelő és rávezető pontok, pedig megkülönböztessék az ellenséges kötelékeket a sajátoktól.

A 2. világháború éveiben a szembenálló felek csak ideig-óráig birtokoltak a rádiótechnika területén jelentős műszaki előnyt, mert főleg a zsákmányolt eszközök tanulmányozásával hamar felfedték az új megoldások lényegét, másolhatták le a szükséges alkatrészeket.

A 2. világháborútól a század végéig igen sok helyi háború zajlott le. Ezek történetében egyértelmű az a tendencia, hogy egyre nagyobb mértékben támaszkodnak a hadviselő felek a rádióik, radarjaik, navigációs eszközeik, légvédelmi rendszereik elektronikai berendezéseire. Tudatossá, tervszerűvé válik ugyanakkor az ezen berendezésekkel vívott harc is. Megjelennek a kimondottan lehallgatási, rádióbemérési és rádió- és radarzavarási feladatokra kifejlesztett komplexumok a haderőnemek fegyver-

zetében. A hetvenes évekig ezek jellemzően csöves berendezések voltak és a hagyományosnak tekintett AM-FM adásmódokban üzemeltek.

A hatvanas évek elejétől mind a katonai, mind a polgári alkalmazásokban forradalmi változást hozott az elektronika és a rakétatechnika fejlődése. Ezek eredményeképpen kiemelkedő tudományággá vált az űrkutatás. A mesterséges holdak megjelenése és az űrtechnológia új eredményeinek gyakorta politikai nyomásra erőltetett alkalmazása kiterjesztette a felderítés és az elektronikai hadviselés határait.

A vezető nagyhatalmak katonai koalíciói az Egyesült Államok, illetve a Szovjetunió vezetésével óriási mennyiségű elektronikai eszközt és ezen belül nagyszámú elektronikai harceszközt fejlesztettek ki. Voltak ezek között univerzálisabbnak számító, széles frekvenciasávban áthangoltatható, pl. rádiózavaró állomások, de voltak egyes eszközök ellen kifejlesztett olyan berendezések is, mint például az orosz R-388 navigációs zavaró berendezés, amelyet speciálisan a TACAN közelnavigációs rendszer repülőfedélzeti berendezésének lefogására használtak.

A fejlesztési és harci alkalmazási filozófiák sokban hasonlítottak, de sokban különböztek is. Az amerikai fejlesztések a hadászati elképzeléseknek megfelelően igen nagy hangsúlyt fektettek a repülőgépek fedélzetére helyezett zavaró berendezésekre, amíg a szárazföldi csapatok fegyverzetében viszonylag kevesebb földi állomást alkalmaztak. A felderítési és elektronikai zavarási feladatokat a NATO országok többsége integrált felderítő és elektronikai hadviselési alegységekben hajtotta végre, amíg a Varsói Szerződés országaiban a rendszerváltásig szervezetileg és technikailag mereven elkülönült, pl. a rádiófelderítés és a rádióelektronikai harc. Ez rendkívül sok együttműködési és alkalmazási hátránnyal járt, de ez a rend alakult ki.

A második világháború utáni legnagyobb helyi háborúk, a koreai, a vietnami, az arab-izraeli háborúk, majd az Öböl-háborúk történetét jelentős mértékben befolyásolta a rádióelektronikai harc fejlettségi szintje, az újabb eszközök és harceljárások megjelenése, kipróbálása. Kiemelkedő területté vált a légierő és a légvédelem összecsapása, amelyben egyik fél sem nélkülözhette a rádióelektronikai harc eszközeinek intenzív alkalmazását. A manőverek, földi és légicsapások előtt intenzív felderítő, megtévesztő, dezinformációs tevékenységet folytattak a felek. A csapásokban résztvevő repülőgépeket intenzív aktív és passzív zavarokkal oltalmazták a légvédelmi felderítő, rávezető és tűzeszközöktől. Kifejlesztették a földi rádiólokációs berendezésekre indított önirányítású rakétákat (ARM, HARM, SHRIKE, stb.) A sikerek általában csak rövid ideig tartottak, mert hamarosan minden esetben megjelentek a válaszlépések. Rendszabályok, majd pl. konkrét zavaró berendezések óvták a légvédelmi rendszert az önrávezetésű rakéták ellen.

Bebizonyosodott, hogy a csapatok és technikai berendezések, komplexumok életképességének megőrzésében rendkívüli jelentősége van a manőverező képességnek, az alkalmazás utáni, illetve a felderítő berepülések utáni azonnali áttelepülésnek. A földi rádióelektronikai harc komplexumok is mobil, viszonylag gyorsan telepíthető, bontható egységekből kezdték felállítani. Minden hadműveletet intenzív rádiófelderítési, lehallgatási és dezinformációs tevékenység is kísért. A csapások elsősorban a szembenálló ellenség állami, felsővezetői, csapatvezetési és fegyverirányítási rendszerei ellen irányultak. A haderőnemek, fegyvernemek erőfeszítéseit egyre precízebben kellett összehangolni, tudományos alapokra helyezve a tevékenységet, a rádióháború fokozatosan a komplex információs háború egyik pillérévé vált.

A berendezések technikai színvonala követte az adott kor élenjáró műszaki színvonalát, bár az egyre gyorsuló technológiai fejlődés mellett az amortizáció is egyre gyorsult. A nagy, nehéz, csöves berendezéseket a félvezetős berendezések új generációja követte, amelyek már nem csak a méret, tömeg és energia-felvétel terén hoztak minőségileg újat, hanem erre az időszakra esett a számítástechnika alapjainak lerakása is. A tranzisztoros generáció a csöves töredékéig tartotta magát, mert szinte elsöpörte őket az olyan berendezések tömege, amelyek már processzorokkal dolgoztak, programozhatóak voltak, távvezérelhetőek, számítógéppel vezéreltek voltak.

Erre a folyamatra jó például szolgálhat a magyar RH rádiófelderítő és zavaró rendszerek fejlődése. A Varsói Szerződés hadseregeiben alapvetően orosz fejlesztésű, majd később licensz alapján gyártott felderítő, iránymérő, zavarvezénylő és zavaró állomásokat használtak. Minden funkcióra külön állomás szolgált, külön telepített nagyméretű antennarendszerekkel. A teljes komplexum telepítése igen hosszú időt vett igénybe, különösen az iránymérő és a zavaró antennáké. A manőverező képességet úgy javították, hogy ezek az állomások dupla antennarendszerrel rendelkeztek és amikor az új telepítési helyen telepítették az antennákat, csak akkor települtek át a műszeres gépkocsik. A teljes rendszer belső híradása komoly vezetékes és rádiórelés összeköttetés kiépítését igényelte, mivel a rövidhullámú komplexum a hadsereg teljes sávjában széttelepülve működött.

A fejlesztések során előbb a felderítő munkahelyeket váltották le a tranzisztoros vevőkészülékek. Az iránymérő alrendszerbe hazai fejlesztésű forgókeretes iránymérők kerültek, de a nagyteljesítményű zavaró állomások leváltására viszonylag hosszú időt kellett várni. A számítógépes vezérlési, adatfeldolgozási és adatbázis kezelési lehetőségek egyre szélesebb körű elterjedésével világossá vált, hogy a többgenerációs, hibrid technológiájú eszközök együttalkalmazása nem célszerű, technikailag nem lehetséges és az átépítésük gazdaságtalan is lenne, tehát egy teljesen új komplexum kifejlesztése szükséges.

Az új automatizált zavaró rendszer megőrizte a harc megvívásának hagyományait, a sok éve változatlan harcászati elveket. Ezek szerint a hadsereg sávjában mintegy 20-24 felderítő, lehallgató munkahely, 4x4 zavaróállomásból álló zavaró csoport szükséges, amely kW-os teljesítményű zavaró adókkal rendelkezik. A telepítési távolságot a hagyományoknak megfelelően, a fő erőkifejtés irányában, a peremvonaltól 5-8 km-re határozták meg. Az új rendszer kétségtelenül a kor egyik legmodernebb fejlesztése volt. Valamennyi zavaróállomás számítógéppel vezérelt felderítő vevőt, KF panoráma analizátort, automatikus rádió iránymérő állomást és 1 kW teljesítményű, digitális hangolású teljesen félvezetős adórendszert tartalmazott. A kor számítástechnikai színvonalának megfelelő beépített algoritmusok, adatátviteli, adatbázis kezelési és megjelenítési funkciók lehetővé tették, hogy a rendszer a felderített forgalmi adatok alapján előre leprogramozott frekvenciákon, többféle zavarási filozófiának megfelelően, akár emberi beavatkozás nélkül is aktív harci munkát folytasson az ellenség rövidhullámú rádióforgalmi rendszerei ellen.

A rendszerváltáskor elkezdődött haderőcsökkentés derékba törte a teljes rendszer kiépítését. A haditechnikai fejlesztések, beépítések lelassultak, majd teljesen le is álltak, így teljes kiépítésében csak egy zavaró csoport, valamint a hozzá tartozó magasabb vezetési szintek készülhettek el. A rendszer gyenge láncszeme a források hiánya miatt kényszerűségből beépített analóg rádiórelé berendezés volt. Filozófiáját tekintve

a legkorszerűbb, automatizált zavaró rendszer volt, azaz lehetett volna, ha a rádiótechnika fejlődése túl nem lép az analóg üzemmódokat alkalmazó rendszereken és meg nem jelennek ebben az időben a frekvenciaugratásos, illetve az adaptív rádiókészülékek a híradó rendszerekben. Be kell látnunk, hogy az új, digitális adásmódokkal szemben a legcsodálatosabb algoritmusokkal működő, magas szinten automatizált, de végeredményében továbbra is analóg eszközök teljes mértékben tehetetlenek, tehát az ilyen rendszerek fejlesztése a 90-es évekre teljesen értelmetlenné vált.

Az ilyen, hagyományosnak nevezhető harceszközök, valamint ezek harci alkalmazása komoly aggályokra adott azért okot. A zavaróállomások a maguk kW-os teljesítményével megfelelő áttelepülési gyakoriság nélkül hamarosan bemérhetők és pusztíthatók. Nem véletlenül fejlesztettek ki páncélosba épített URH zavaróállomást, amely megállásból, vagy menet közben is képes volt feladatot végrehajtani. A zavaróállomások a saját harcrendben települve a leggondosabb frekvenciaegyeztetés és beépített saját rendszerek zavarását kizáró algoritmusaik ellenére is komoly rádiózavarokat okoztak a saját erőknek. Az állomások üzemeltethetőségüknél és pl. az antennarendszerük telepítéséhez szükséges minimális létszámnál fogva, jelentős személyi állományt igényeltek, vagyis komoly logisztikai támogatást. Az alkalmazott híradó eszközök sajátos üzemeltetési jellemzőikkel hamar felfedték a rendszer teljes kiépítését, ami komoly kérdéseket vetett fel a túlélőképességüket illetően.

Ezeket a gondokat egy merőben új filozófiájú eszköz sok tekintetben orvosolta és ez nem volt más, mint az egyszeri felhasználású zavaró berendezések csoportja. Ezeket a megvalósított és rendszeresített eszközöket kivitelüktől függően repülőgépre, vagy helikopterre függesztett konténerből dobták le az ellenséges harcálláspontok, hírközpontok körzetében, illetve tüzérségi ágyútarackkal lőtték át. Becsapódásuk után egy inerciakapcsoló hozta működésbe őket és az áramforrásuk kimerüléséig, mintegy 0,5-1 óra időtartamig néhány W-os teljesítményű, szélessávú rádiózavart hoztak létre maguk körül. A nyolcvanas évek technikai színvonalán több ország is gyártott, illetve exportált ilyen eszközöket, de lényegében mind hasonló volt, sok alkalmazásbeli előny mellett sok hátrányt is hordoztak. Előnyük volt, hogy nem igényeltek kezelőállományt, csak az előkészítéshez kellett személyzet. Működésük teljes egészében az ellenséges területre korlátozódott, nem okoztak a saját csapatoknak nemkívánatos interferenciákat. Méretüknél fogva nehezen felkutathatóak és kiiktathatóak voltak. Üzemelésük automatikus volt, kezelést nem igényelt.

Ezen előnyök mellett egy sor hátrány is felsorolható. Működési idejük igen korlátos volta miatt a harc legkritikusabb idejére koncentrálódott az alkalmazásuk, azonban a repülőeszközről való kijuttatás ebben az időszakban a legkockázatosabb. Az üzembelépés valószínűsége nagyban függött a becsapódás körülményeitől, mivel az ejtőernyőnél fogva fákon fennakadó példányok nem kapcsoltak be, a talajba be nem fúródottak pedig eldőltek, így a földön fekvő antenna hatásfoka nagymértékben romlott. Az áramforrás korlátozott, rövid ideig működött, a bekapcsolást késleltetni, illetve távvezérelni nem lehetett. A zavarjel 8-10 MHz széles frekvenciasávban egyenletesen oszlott el, a zavarjel koncentrálására, illetve manővereztetésére nem volt mód. A keskenysávú URH rádiócsatornákra igen kis fajlagos zavarjelsűrűség jutott. A valós elektronikai környezettől teljesen függetlenül működtek, annak változásaira nem reagáltak. Gyárilag beállított alsávokban kerültek készletezésre, ezért a felhasználásuk egyenetlenné vált, mivel a rádióhíradás zöme néhány alsávra koncentrálódott, vagyis a fogyás

ezekben jóval nagyobb volt. A bevetésükről semmilyen objektív információ nem jutott vissza a parancsnokhoz, mert sem a becsapódás pontos helye nem volt ismert, sem a bekapcsolódás ténye. A zavarás valódi hatására a zavarásra tervezett forgalmi rendszerek viselkedésének megfigyeléséből lehetett következtetést levonni. További hátránynak tekinthető, hogy ezen eszközök ára meglehetősen magas volt.

Műszaki modernizálásukra az ezredfordulóra rendkívül sok reálisan megvalósítható lehetőség lett volna, azonban a digitális hírközlés térnyerése, a kiterjesztett spektrumú rádióadásmódok elterjedése miatt erre ebben a formában nem került sor.

A korábban említett haderőcsökkentés, valamint a meglévő berendezések tartozék és javítóanyagainak felhasználása, a beszerzési források elapadása fenntartási nehézségeket okozott úgy a rádió, mint a rádiótechnikai zavaró berendezések üzemeltetői, alkalmazói számára. A haderőben megváltozott hivatalos prioritások sem kedveztek az elektronikai hadviselési csapatok fennmaradásának. Az átszervezések, létszámleépítések eredményeképpen előbb a légvédelmi rádiótechnikai zavaró zászlóalj(ak), majd a rádiófelderítő, rádiózavaró szervezetek is szinte teljesen felszámolásra kerültek.

Mindeközben beköszöntött a digitális hírközlés és rádiótechnika kora. Soha nem látott mértékben terjednek az új szélessávú, nagykapacitású átviteli rendszerek, a digitális harctéri eszközöktől a globális műholdas és személyi kommunikációt biztosító eszközökig, a helymeghatározótól, a saját-ellenség felismerő eszközökig minden megtalálható a katonáknál és civileknél egyaránt. A repülőgép fedélzeti elektronikai rendszerek nélkül lehetetlen a navigáció, a biztonságos légtérhasználat, a fel- és leszállás.

Hivatalosan deklarálva is beléptünk az információs korba, a társadalom és értelemszerűen, a hadseregek működésének is alapját képezi az információs infrastruktúrák megfelelően megbízható működése. Tehát komoly lépéselőnybe kerültek a digitális rendszerek az elektronikai hadviseléssel szemben? Egy újabb „nagy ötlet” kellene?

## A digitális korszak és a jövő

A mára kialakult helyzet szerint az analóg berendezések kora lejárt, a berendezések váltása folyamatosan halad. Az elektronikai hadviselés az információs műveletek, az információs hadviselés kulcstényezője az elméleti tanulmányok és elvek szerint, azonban a gyakorlati megvalósulás komoly technikai nehézségekbe ütközik. A leselejtezett, hadrendből kivont berendezéseken, rendszereken nem kell keseregni, mert azok gyári új állapotban sem lennének alkalmasak a mai korszerű viszonyok között semmire. A megoldás azonban nem a felszámolás, hanem a meglévő technikai kultúra továbbfejlesztése, a meglévő szakemberek továbbképzése és új berendezések kifejlesztése. Az elektronikai hadviselés „szolgáltatásaira” a jövő katonai vezetőjének is óriási szüksége lenne. A felderítési adatok nagy része innen származik, a különböző eseményekhez kötődő riasztásokat az elektronikai támogató tevékenységnek kell(ene) szolgáltatnia, a szembenálló fél hírközlési, felderítési, fegyverirányítási eszközeit fénysebességgel az elektronikai ellentevékenység hivatott megtéveszteni, lefogni, vagy akár pusztítani.

Történik ezen a területen valami? Annak ellenére, hogy általános meggyőződés szerint ez egy roppant drága terület, mégis jól érzékelhető, hogy nem csak a nagyhatalmak tesznek erőfeszítéseket a fent vázolt gondok megoldása érdekében. Példaképpen megemlítem, hogy a számítógép hálózati hadviselés (Cyber Warfare), a számítógép hálózati támadás és védelem (Computer Network Attack and Defense) egyre gaz-

dagodó elméleti és gyakorlati eszköztára a hadviselésnek úgy háborúban, mint békében. Ehhez pedig nem kellene nagyhatalmi anyagi kondíciók.

Az irányított energiájú fegyverek katonai kísérletei és a kutatási projektekben megfogalmazott célkitűzések azt bizonyítják, hogy a sebészi pontosságú, kiválasztott objektumokra mért csapások már nem a katonát akarják elpusztítani, nem a polgári lakosságot akarják terrorizálni, hanem csak a szükséges és elégséges mértékben kívánják a szembenálló fél vezetését megbénítani.

Ha megvizsgáljuk, hogy a jelen előadásban vizsgált rádió és rádiótechnikai zavarás területén történik-e valami jelentős változás, akkor azt kell mondanunk, hogy igen, felismerhető „a nagy ötlet". A haditechnikai kutatás-fejlesztés a hadszíntéri rádió és rádiótechnikai zavarás új eljárásának kidolgozása és kipróbálása fázisában van. A fentebb leírtakból egyértelműen látható, hogy a kódolt digitális hírközlésből valós időben már nem kaphatunk információkat, a közlemények tartalmának lehallgatásáról a hangsúly elsősorban a rádiótechnikai felderítéshez hasonló helymeghatározásra, paraméteranalízisre és az üzemi jellemzők meghatározása felé tolódott el.

A frekvenciaugratásos berendezések adási szekvenciájának megfejtése lehetetlen, így a tetszőlegesen hosszú idejű minta sem képezheti alapját egy frekvenciában célzott szinkron zavarótevékenységnek. A rövid idejű kisugárzások vétele és a vevőkészülékek válaszzavarokkal való lefogása bizonyos ugrási sebesség felett a saját harcrendből futási idő korlátok miatt nem valósítható meg, ezért a zavaró berendezéseket az ellenség mélységébe kell kijuttatni.

A vett kisugárzások saját-ellenség analízise alapesetben eldönthető akár úgy is, hogy amely rádiókisugárzást az ellenséges területen azonosítunk, az ellenséges, vagyis megfelelő időszakban zavarandó. Alapvetően ezen szempontok képezik az alapját az új zavaró rendszernek, az amerikai Wolfpack rendszernek.

Ebben megtalálhatók azok az előnyök, amelyeket az egyszeri felhasználású zavaró berendezések hordoztak, azonban a 21. századi technológiák által biztosított lehetőségekkel kibővítve. A Darpa által kifejlesztett alapokon a Raytheon, majd a BAE Systems kezdte meg a rendszer fejlesztését és építését. Lényege, hogy az ellenséges területre miniatűr felderítő-zavaró eszközök sokaságát szórják le, amelyek egymással hálózatba kapcsolódnak. A forradalmian új filozófia szerint a területen csoportokba szerveződő egységek a meghatározott program szerint felderítést, helymeghatározást, célazonosítást végeznek, információkat továbbítanak a honi területen lévő központi állomás felé, és megfelelő döntések parancsok alapján célzott, manőverező zavarokat képesek előállítani a megfelelő forgalmi rendszerek, vagy radar berendezések ellen.

A fejlesztési projekt központi elemei: a nagyhatásfokú szubrezonáns antennák fejlesztése, a hálózati irányítóprogram kifejlesztése, amely optimálisan osztja el a jelfelderítési (SIGINT), helymeghatározási, kommunikációs és zavarási feladatok között az erőforrásokat, olyan algoritmusok kifejlesztése, amely lehetővé teszi a gyors jelfelderítést, analizálást, azonosítást és az optimális zavarstruktúra, valamint zavaró erőforrás allokációt.

Az ötös csoportokban tevékenykedő „farkasok" egyike a vezető állomás, amely veszi a többiek jelentését, és továbbítja az „AirWolf", a légi farkas számára, amely egy pilóta nélküli repülőgép. A kisugárzó eszközök helyét GPS segítségével mintegy 10 m-es pontossággal képesek meghatározni, amely elégséges pontosságú célmegjelölést

ad például a tűzzel való pusztításhoz. Az egyes modulok saját napelemes töltő berendezéssel rendelkeznek, az aktív energiamenedzsment jóval hosszabb élettartamot biztosít, mint a valamikor használt egyszeri felhasználású zavaró adók telepei. Kivitelét tekintve az egyes modulok 2,5 kg tömegűek, 15 cm átmérőjű, hengerek. Becslések szerint a hálózatos működéshez és a hatékony zavaráshoz néhány db/km2 szükséges. A működés várható időtartama átlagosan 2 hónap. Egy egység bekerülési költsége jelenleg mintegy 10.000 USD.

## Befejezés

Komoly feladatok állnak előttünk. Az információs műveletek elmélete alapvető pillérként támaszkodik az elektronikai hadviselésre. Ha kihagyunk elemeket, megbomlik az egyensúly, kulcsfontosságú képességeket fogunk veszíteni. A felderítés, a NATO feladatokra felajánlott erők ISTAR képességei, a hálózatos hadviselés alapjainak kidolgozása nem kevés kutatói és elméleti kidolgozó munkát igényel az elektronikai hadviselési szakemberektől. A jövőben beszerzésre kerülő modern fegyverzet rendszerbeállítása, a Gripen üzemeltetése, objektumok elektronikai védelme és sok más terület elképzelhetetlen összehangolt tervező-szervező és oktatói munka nélkül. A világ pedig halad, csak rajtunk áll, hogy haladunk-e velük, vagy nem akarunk tudomást venni a haladásról.

## Felhasznált irodalom


[1] Bokor: Rádióelektronikai harc korunk háborúiban, Zrínyi Katonai Kiadó, Budapest, 1989.

[2] Haig-Várhegyi: Hadviselés az információs hadszíntéren. Zrínyi Kiadó, 2005, ISBN 963-327-391-9.

[3] Ványa: Felderítő és elektronikai hadviselési eszközök típusváltása az amerikai haderőben. In: Haditechnika 2000/2. 12.─17. p. HM HTI Budapest, 2000.

[4] Ványa: Az elektronikai hadviselés aktuális kérdései a 21. században. - A korszerű szórt spektrumú harcászati-hadműveleti rádiók felderítési és helymeghatározási problémái az elektronikai harc csapatoknál. In: Bolyai Szemle 2000. IX. évf. 1. szám. 113.─128. p. Budapest, 2000. ISSN 1416 1443.

[5] Ványa: Az elektronikai hadviselés aktuális kérdései a 21. században II. A korszerű, szórt spektrumú harcászati-hadműveleti rádiók elektronikai zavarásának kérdései. In: Bolyai Szemle 2001. X. évf. 2. szám. 55.─64. p. Budapest, 2001. ISSN 1416 1443.

[6] Ványa: Új technikai kihívások az elektronikai ellentevékenységi rendszerekben. In: Nemzetvédelmi Egyetemi Közlemények 3. évfolyam 1. szám. 81.-99. p. Budapest, 1999. ISSN 1417 7323.

[7] Ványa: Unmanned Air Vehicles – Commander's Eyes and Arms in the Information Age. In.: The Challenge of Next Millennium on Hungarian Aeronautical Sciences. eR-GROUP, 91.─100 p. Budapest, 1999. ISBN 963 03 7803 5

[8] Ványa: Electronic Attack - Tactics and Technics. In: Hadtudományi tájékoztató 1999/7. A ZMNE és a HVK TSZO kiadványa. 107.─122 p. Budapest, 1999.

**Dr. VASS Sándor**

# AZ INFOKOMMUNIKÁCIÓS BERENDEZÉSEK BIZTONSÁGOS ÜZEMELTETÉSÉNEK NÉHÁNY AKTUÁLIS KÉRDÉSE

## Bevezetés

Az elektronikus berendezések gyors fejlődése egyre bonyolultabb és tökéletesebb rendszerek megépítését tette lehetővé, melyekkel mind szélesebb körben lehet sokkal magasabb szinten kielégíteni a felhasználói igényeket. Az utóbbi évtizedben robbanásszerű fejlődésnek indultak az infokommunikációs eszközök és rendszerek különösen a hírközlés, az informatika és az elektronikus média területén. Ugyanakkor az infokommunikációs rendszerek egyes elemeit nem lehet elkülönülten kezelni mivel a különféle beavatkozások, zavarok minden esetben hatással vannak a rendszer egészére.

Az infokommunikációs eszközök, rendszerek gyors fejlődése a jövőben is markánsan átalakítja életünket, hatékonyabbá teszi a napi munkavégzést, lerövidíti a szükséges munkaidőt és szervesen beépül mindennapjainkba. Szinte már el sem tudnánk képzelni az életünket például fax, számítógép vagy mobiltelefon nélkül. Sok feladat nélkülük nehezebbé, vagy esetleg megoldhatatlanná válna, mivel az ipar és a gazdasági élet egyre nagyobb mértékben függ az elektronikus adatfeldolgozástól. A korszerű hadseregekben is tömegesen alkalmaznak olyan infokommunikációs eszközöket, amelyek létfontosságúak a felderítő rendszerekben, a csapatok vezetésében és a fegyverek irányításában.

Mindezen előnyök mellett azonban az érzékeny elektronikus elemekből épülő infokommunikációs eszközök és rendszerek üzembiztonság és megbízhatóság szempontjából új veszélyeztetéseket is teremtettek.

Villamos elven működő berendezéseivel az ember villamos, mágneses és elektromágneses erőtereket hoz létre, szándékosan, mint a rádió- és TV-adások vagy a mobiltelefon-hálózat esetében, vagy mellékhatásként, mint a távvezetékek, transzformátorok, villamos motorok üzemeltetésénél. Az egymástól függetlenül létrehozott erőterek befolyásolják a villamos elven működő berendezéseink működését, zavarok, rejtélyes hibák forrásai lehetnek.

Az érzékeny elektronikai berendezések, infokommunikációs rendszerek üzemeltetésénél nem szabad figyelmen kívül hagyni a természetes zavarforrások hatásait sem, tehát például a villámcsapások hatásaival is számolnunk kell. Az emberek régóta tudják, hogy a közvetlen villámcsapások komoly károkat, tüzet, robbanást okozhatnak. A villamos vezetékekbe csapó villám okozta túlfeszültség, vagy a közelben lecsapó villám által az áramkörökben indukált túlfeszültség a villámcsapás helyétől távolabb is roncsolhatja az elektronikus eszközöket.

Ez a villamos hálózatokkal átszőtt világ a növekvő információátvitelével együtt a zavarokra és működéséhez szükséges adatátviteli, illetve távközlési hálózatok meghibásodásaira, üzemkieséseire igen érzékeny. Hosszabb ideig tartó meghibásodásuk akár katasztrófahelyzetet is előidézhet, ezért szükséges megvizsgálni, hogy az

infokommunikációs eszközöket, rendszereket, hogyan tudjuk megvédeni a különféle természetes és mesterséges elektromágneses zavaroktól.

## 1. Az infokommunikációs rendszerek elektromágneses kompatibilitásának biztosítása

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

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

Az elektronikus készülékek, rendszerek zavarjelenségeinek vizsgálata alapján alapvetően négyfajta oka van a zavarok kialakulásának:

- rádiófrekvenciás zavarás, amely oka valamilyen rádióadó vagy parazitakisugárzás jelenléte (pl. URH rádiók, szikrák, ívek stb.);
- külső vagy belső eredetű elektromágneses impulzusok megjelenése a hálózatokon, amelyek az eszközök tönkremenetelét okozhatják (például közeli villám, kapcsolás az elosztóban stb.);
- az ipari frekvenciás rendszerek és eszközök önmagukra és a gyengeáramú rendszerekre és eszközökre gyakorolt zavaró hatása (pl. a transzformátor mágneses tere, feszültségcsökkenés, felharmonikus termelés, „brumm” jelenléte stb.);
- az elektrosztatikus feltöltődés nyomán megjelenő kisülés elektronikus eszközöket tehet tönkre illetve tűz- és robbanásveszélyt okozhat.[1]

A zavarok terjedése alapvetően vezetett vagy sugárzott módon történhet.

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

- galvanikus csatolás, ahol a zavaró hatások az áramkörök közös (ohmos) elemein keresztül jönnek létre. A zavaró jellemző az áram;
- kapacitív csatolás, ahol a zavaró hatások a váltakozó villamos terek útján kerülnek a zavaró áramkörből a berendezés zavart részébe. A zavaró jellemző a feszültség;
- induktív csatolás, ahol a zavaró hatások egy zavarforrás váltakozó mágneses tere által indukált feszültségként keletkeznek a zavart elszenvedő vevőben. Okuk a zavarforrás áramának változása.[2]

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

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

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

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

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

A gyakorlatban azonban sokszor előfordulnak olyan rövid idejű elektromágneses impulzus hatások is, melyek az elektromágneses kompatibilitás szabványban megengedett határértékeket messze meghaladják és a berendezéseket az elektromágneses kompatibilitás feltételek teljesítése ellenére tönkreteszik. Ilyen elektromágneses hatások lehetnek a különböző zárlati jellegű védelmi működéskor fellépő kapcsolási túlfeszültségek, valamint a közvetlen-, vagy közeli és távoli villámcsapások (Lighting Electromagnetic Pulse - LEMP).

Az elektronikus berendezések csak akkor üzemelnek biztonságosan, és a törvényi előírások szerint csak akkor hozhatók kereskedelmi forgalomba, ha az elektromágneses zavarás és zavartatás „Az elektromágneses összeférhetőség” MSZ EN 61000 szabványsorozat követelményeinek is megfelelnek, és azt a termék gyártója illetve forgalmazója vizsgálati jegyzőkönyvekkel igazolja.

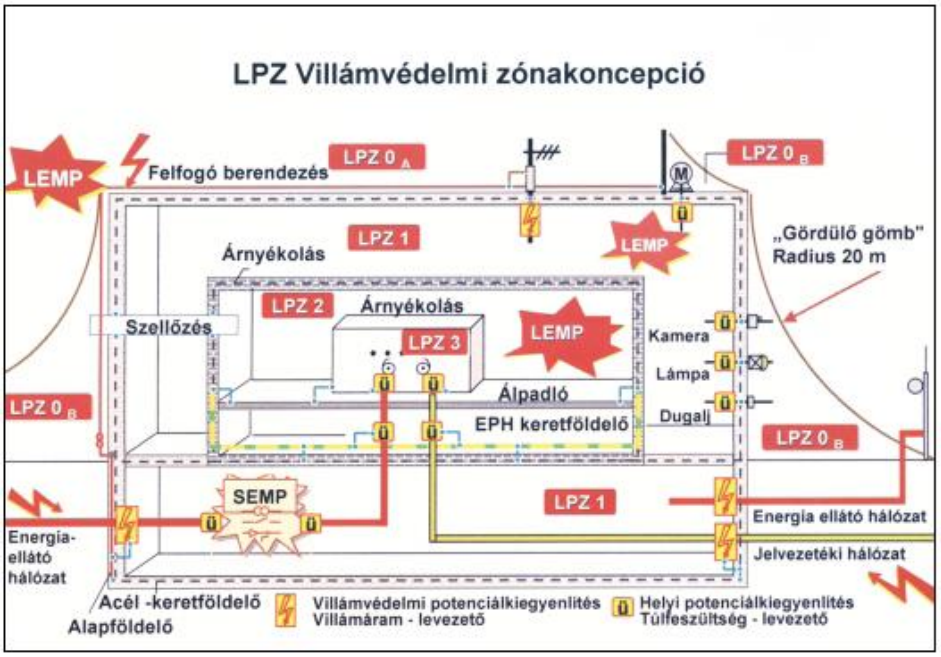
## 2. Elektromágneses kompatibilitás orientált elektromágneses villámimpulzus és túlfeszültség elleni védelem módszerei, eszközei

Mivel az infokommunikációs eszközök és rendszerek üzemeltetéséhez nélkülözhetetlen a villamos energia folyamatos felhasználása, ezért fontos a villamos energia elosztó hálózatok és a fogyasztói rendszerek villám- és túlfeszültség-védelme. Az elektronikus készülékek növekvő száma és az elektronikus áramkörök fokozott túlfeszültség érzékenysége ugyanis olyan növelt védőhatású túlfeszültség-védelmet igényel, amely mind a villámcsapás, mind a kapcsolások és zárlati események által keltett túlfeszültségek károsító hatásait biztonsággal kivédi, és a fellépő túlfeszültség csúcsértékeket az elektromágneses kompatibilitás szabványokban előírt határértékeknél alacsonyabb értékek alá korlátozza.

Az utóbbi évtizedek tapasztalatai igazolták, hogy - csak egy hagyományos külső villámvédelemmel („villámhárítóval”) védett épületen belül - az ott üzemelő túlfeszültségekre érzékeny elektronikus berendezések és rendszerek a másodlagos villámhatások következtében gyakran meghibásodnak, illetve tönkremennek. Ennek kivédésére az MSZ 274 „Villámvédelem” szabvány követelményrendszere módosult és befogadta az MSZ IEC 1312-1 „Az elektromágneses villámimpulzus elleni védelem. Általános alapelvek.” és az MSZ IEC 61000 „Elektromágneses összeférhetőség” szabványok követelményrendszerét is. Az MSZ 447 szabvány pedig lehetővé tette és befogadta a méretlen fővezeték belépési pontján a villámáram levezetők beépítését,

mert az áramszolgáltató és a fogyasztó közös érdeke a szabványoknak megfelelő, biztonságot nyújtó túlfeszültség-védelem létesítése.[3]

Az új magyar és nemzetközi MSZ IEC 1312-1 szabvány a túlfeszültség-védelmi potenciálkiegyenlítést, és egy védelmi zónakoncepciót vezetett be. Az épületek és építmények villámvédelmi zónákra (Lighting Protecting Zone - LPZ) osztásával a nagykiterjedésű adatátviteli hálózatok esetében is a túlfeszültség - védelmi készülékek differenciált, de ugyanakkor az adott hálózatra illesztett teljes körű túlfeszültség-védelme valósítható meg. Ezáltal a jelvezetékekre is a lehető legnagyobb mértékű üzembiztonság érhető el. Ez a védelmi koncepció az új rendszerek létesítése vagy a meglévő rendszerek átépítése és korszerűsítése esetén is biztos megoldást kínál. A 1. sz. ábrán a villámvédelmi zónakoncepció felépítése látható.[4]




1. sz. ábra Villámvédelmi zónakoncepció

A statisztikai adatok igazolták, hogy az üzemzavarok okai között egyre nagyobb hányadban fordulnak elő villám- és túlfeszültségek által okozott hálózatkiesések. Gyakorlati tapasztalatok igazolták azt is, hogy ha a hálózatkiesést villámcsapás okozza, és nincs megfelelő villám- és túlfeszültség-védelem az épületen felszerelve, akkor a villámcsapás következtében nem csak a túlfeszültség-érzékeny fogyasztói berendezések mennek tönkre, hanem egyidejűleg a szükségáramforrások is meghibásodnak, és a teljes fogyasztói hálózaton a szünetmentes tápegységek ellenére tartós üzemzavar és hálózatkiesés lép fel, tetemes elektronika villámkárok is keletkeznek.[5]

Csak olyan villámvédelem képes megvédeni az épületen belül üzemelő elektronikus berendezéseket az elektromágneses impulzus hatásokkal szemben, amely közvetlen villámcsapás esetén is az elektromágneses kompatibilitás szabványban előírt határértékek alá korlátozza az elektronikákra jutó túlfeszültségeket.

## 2.1. Villámimpulzus kialakulása és hatása

A villámkisülés zivatarfelhőkben keletkezik. A zivatarfelhők fő méretei több kilométeresek is lehetnek. Az erős függőleges légáramlás következtében a felhők belsejében pozitív és negatív töltésű felhőtömegek keletkeznek. Ezek között, illetve a felhő és a Föld között fellépő elektromos kisülés a villám. A villám ívcsatorna átmérője csak néhány centiméter, de az ívkisülés fényereje 1 millió darab 100 Wattos izzólámpa fényének felel meg. A kialakuló nagy energiájú villamos ívkisülés körül, amely rövid ideig (legfeljebb a másodperc ezredrészéig) létezik, az ívben folyó nagy áramok hatására erős elektromágneses erőtér is keletkezik.

Magyarországon 1998 óta működik villámfigyelő rendszer. A SAFIR a Kárpát-medence jelentős részét lefedve, mintegy 200 000 négyzetkilométernyi területet tart állandó megfigyelés alatt. A SAFIR rendszerrel közel 2 km-es pontossággal lehet megadni a felhőkből a földre lecsapott villámok helyét. Évente átlagosan 28-33 zivataros nap van Magyarországon. A zivatarok közel 95 százaléka a nyári félévre esik, az év legzivatarosabb hónapja a június. 2004-ben összesen 30 220 villám csapott le, ezek közül 10 849 júniusban. A Magyar Biztosítók Szövetségének adatai szerint 2004-ben Magyarországon 31 500 alkalommal jelentettek be villámcsapás kárt, és a biztosítók 1,7 milliárd forintot fizettek ki. Azonban ez az összeg valószínűleg még mindig nagyságrendekkel kisebb a tényleges károknál, mivel az APC (American Power Conversion) tavaly készült felmérése arra mutat rá, hogy a hazai háztartások 53 százaléka észlelt áramellátási problémát, és ezek a háztartások 17 százalékánál villámcsapásokra vezethetők vissza.[6]

### 2.1.1.Villámok hatásai és következményei

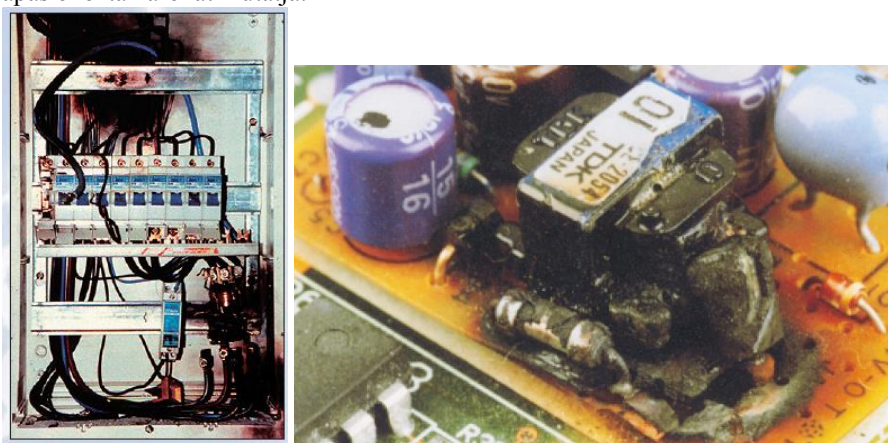
Az épület villámhárítóját ért közvetlen villámcsapás esetén, a villámáram fele az épület földelőn, másik fele pedig a villámsújtotta épületet és a távoli földpotenciálú pontokat összekötő áram utakon folyik el, vagyis a legkedvezőtlenebb esetben a villámáram másik fele teljes egészében az energiaellátó hálózaton át folyik a transzformátor felé. A szabvány szerinti I. védelmi szinthez tartozó villámimpulzus csúcsértéke 200 kA (10/350) (MSZ IEC 1312-1).[5]

A Magyarországon üzemelő villámfigyelő és -mérő rendszer eddigi, 60 000 villámcsapásra vonatkozó mérési eredményeit értékelve az állapítható meg, hogy néhány %-ot kivéve a villámimpulzusok csúcsértékei nem haladják meg a 100 kA-t sem, és az impulzusok töltése és energiatartalma is a szabványos csúcsértéknél többnyire kisebb. Ez azt jelenti, hogy a szabványkövetelmény betartásakor biztonsági tartalék áll rendelkezésünkre.

A villámáram által átjárt vezetők nyomvonala körül a villámimpulzus mágneses erőteret hoz létre, amely az elektromágneses környezetével kölcsönhatásba lép. Ez a magyarázata annak, hogy az egymáshoz közel elrendezett villámáram vezetők között az áramirányoktól függően olyan erőhatások lépnek fel, amelyek a vezetők rögzítéseit széttéphetik és a vezetőket vagy összeszorítják, vagy egymástól eltávolítják.

A külső villámvédelem hibásan elrendezett áramvezetőin a dinamikus erőhatások a nem megfelelő szilárdságú villámvédelmi tartókat, kötéspontokat, rögzítéseket megrongálják, és azt követően a villámimpulzus fajlagos energiája a már nagy átmeneti ellenállású szakaszt és annak környezetét szétrobbantja. Ezért fontos, hogy külső villámvédelem minden esetben csak a megfelelően minősített H és L jelű villámvédelmi szerelvényekből készüljön.

Amikor villámcsapás éri a villámhárítót, az nagy áramot vezet le a földbe. Ettől a szakszerűen tervezett és kivitelezett villámhárító, illetve a védett épület valóban nem károsodik. Fontos azonban tudnunk: a villámhárító közvetlen összeköttetésben van az épület elektromos hálózatával (másképp nem tudná feladatát ellátni)! Ez, sajnos, azt is jelenti, hogy a villám áramának egy része behatol majd az elektromos hálózatba, és ez az érzékeny berendezéseket tönkreteszi, rosszabb (és szerencsére ritkább) esetben elektromos zárlatot, esetleg tüzet okoz. Ilyenkor nem közvetlenül a villám, hanem annak másodlagos hatása okoz kárt, veszélyhelyzetet. A 2. sz. ábra a villámcsapás okozta károkat mutatja.



2. sz. ábra. Villámcsapás okozta károk

Az elektronikus berendezéseinkre nem csak a közvetlen villámcsapás az egyetlen veszélyforrás. Az is ismert tény, hogy a villámcsapás köré rajzolható veszélyzóna sugara több mint 1,5 km, az így kialakult másodlagos villámhatás következtében az elektromágnesesen indukált és a vezetékeken vezetett túlfeszültségek nem csak hatnak az elektromos berendezésekre, hanem tönkre is tehetik azokat.

### 2.1.2. A túlfeszültségek hatásai és következményei

Az elektromos berendezéseket meghatározott feszültség- és áramerősségértékekre méretezik. A biztonságos működést a névleges értéket néhány százalékkal meghaladó feszültség nem veszélyezteti, de ha tovább növeljük a feszültséget, a berendezés egyre nagyobb feszültségen egyre rövidebb ideig marad üzemképes. A névleges feszültség 5-8-szorosánál ez az idő már kevesebb, mint a másodperc ezredrésze! A villámcsapások másodlagos hatásaként létrejövő túlfeszültségek időtartama legfeljebb egy ezredmásodperc, de csúcsértéke több ezer volt lehet, ami általában a berendezés működőképességének megszűnéséhez vezet. Ennek oka az elektromos berendezések belsejében lévő szigetelések átütése. A túlfeszültség-levezető alkalmazásával az a célunk, hogy a túlfeszültségek csúcsértékét olyan mértékben csökkentsük, hogy azt berendezésünk ebben a rövid időtartományban képes legyen elviselni (a szigetelések ne üthessenek át). A szabványok ezt a legfeljebb kb. egy ezredmásodpercig megengedhető feszültséget erősáramú, 230 V-on üzemelő berendezésekre 1500 V-ban határozzák meg. Természetesen kisebb feszültségen üzemelő berendezések esetében a

megengedhető túlfeszültségérték is kisebb: megközelítőleg a névleges feszültség 5-szörösével lehet számolni.[7]

A kis energiatartalmú, viszonylag lomha felfutású és kis amplitúdójú túlfeszültségek általában csak múló zavarjelként terhelik a villamos rendszereket. A nagyobb impulzusok azonban már súlyosabb következményekkel járnak.

Tűz- és robbanásveszélyes gázok illetve anyagok jelenlétében előfordulhat, hogy a levegő túlfeszültség okozta igénybevétel meghaladja annak villamos szilárdságát, és bekövetkezik az átütés. Ennek során a kialakuló nagy hőmérsékletű ívcsatorna - szerencsétlen esetben - képes belobbantani a közeget, tüzet vagy robbanást okozva.

Minden villamos készülék, eszköz vezető és szigetelő anyagokból épül fel, s általában addig üzemképes, míg szigetelései épek. Ha a készülék kapcsain megjelenő túlfeszültség okozta igénybevétel nagyobb az adott szigetelés villamos teherbíró képességénél, bekövetkezik az átütés, s a berendezés tönkremegy, s sok esetben ki is gyullad.

A kisfeszültségű hálózatokon nagy tömegben előforduló elektronikus készülékek rendkívül érzékenyek a túlfeszültségekre: a rendkívül vékony félvezető átmenetek ugyanis már igen kis energiával roncsolhatók. Ez a magyarázata, hogy sok esetben semmi látványos nyoma nincs a túlfeszültségnek, csak az elektronika megy tönkre, ugyanakkor számos esetben a viszonylag kicsi, de többször is ismétlődő túlfeszültség igénybevétel az alkatrész élettartamának rövidülését eredményezheti.

## 2.2. A villámcsapás hatásai elleni védelem módszerei

A hatékony villámvédelmi rendszer főbb elemei a következők lehetnek:

A külső villámvédelem az MSZ 274 „Villámvédelem” szabvány előírásainak megfelelően kiépítve a villámot felfogja, és gyújtóhatás mentes, biztonságos áramúton levezeti a földbe. A külső villámvédelem azonban nem tudja megvédeni az épületben lévő túlfeszültség érzékeny villamos és elektronikus berendezéseket a villám másodlagos romboló hatásaival szemben.

A belső villámvédelem az MSZ 274 és MSZ IEC 1312 - 1 szabványok előírásainak megfelelő kiépítve megvédi a túlfeszültség érzékeny elektronikus berendezéseket a villámcsapáskor fellépő másodlagos villámhatásokkal és a gyakori kapcsolási túlfeszültségekkel szemben. Hatásosan véd mind az épületet ért közvetlen villámcsapáskor, mind az épület környezetében bekövetkezett közeli villámcsapáskor is, továbbá véd akkor is, ha a villámcsapás a kis, vagy középfeszültségű energia elosztó hálózaton átvezetett áramimpulzusként akar behatolni az épületbe.

A túlfeszültség-védelem az épületen belül létesített többlépcsős védelem, melyet a védendő berendezések tápellátó és jelvezeték nyomvonalain és bemenetén kell beépíteni. A túlfeszültség - védelem hatásos védelmet nyújt a különböző kapcsolási túlfeszültségekkel szemben is. Az elektromágneses kompatibilitás követelményeknek megfelelő túlfeszültség - védelem a többlépcsős védelem utolsó tagja. Az elektromágneses kompatibilitás szabványokban (MSZ EN 61 000) meghatározott feszültség határértékek alá korlátozza a feszültségeket, és amelyet mindig közvetlenül a védendő berendezés bemenetein kell beépíteni.

Fentiekből látható, hogy a szabványos védőkészülékek fokozatai egyre csökkenő, egyre alacsonyabb határértékek alá korlátozzák a túlfeszültségeket. Ahhoz, hogy egy valóban megbízható jó túlfeszültségvédelmet építhessünk fel, a tervezésnél az összes tényezőt figyelembe kell venni. Csak finomvédelem beépítése nem elegendő,

mert a finomvédelmi készülékek csak az előző fokozatokon áthatolt maradék impulzusok levezetésére, és az elektromágneses kompatibilitás határértékek alá korlátozására képesek.

A külső villámvédelem mellett olyan belső villám- és túlfeszültség-védelmet is létesíteni kell, amelyik közvetlen villámcsapás esetében is megvédi a fogyasztói berendezéseket és a villamos energiaellátás sem esik ki. A szünetmentes áramforrásokat is minden üzemállapotban mind a bemenetükön, mind a kimenetükön legalább C osztályú túlfeszültség-levezetőkkel kell védeni.

A védelem kialakításának egyik lényeges szempontjaként figyelembe kell vennünk, hogy a túlfeszültség milyen módon hatolhat be a ház belső terébe és az ott elhelyezett elektromos berendezésekbe.

A vezetett és sugárzott terjedési mód mindig egyszerre van jelen, de a vezetve, illetve sugározva terjedő túlfeszültségek nagysága és aránya számos körülmény függvénye. Mennyiségi becslést nehéz adni, mert a sugárzott túlfeszültségek nagysága döntően függ a berendezéshez csatlakozó fémes vezetők geometriájától. Elfogadva azonban a szakirodalomban fellelhető adatokat, még a néhány száz méter távolságban lecsapó villám hatására is kV nagyságrendű sugárzott túlfeszültségek ébredhetnek, amit nem hagyhatunk figyelmen kívül.

## 2.3. Túlfeszültség-védelem területei és fokozatai

A túlfeszültség-védelem elve rendkívül egyszerű: vagy nem szabad megengednünk, hogy a túlfeszültség impulzus bejusson villamos rendszereinkbe, vagy ha bejutott már, akkor olyan értékűre kell csökkenteni, hogy készülékeink, eszközeink károsodás nélkül viseljék el jelenlétét.

Túlfeszültségek elleni hatékony védelmet csak a szabványos, összehangolt, teljes körű, hézagmentes és bevizsgált háromlépcsős villám- és túlfeszültség-védelem biztosíthat. Ez természetesen érvényes az összes jelvezetéki és adatátviteli hálózatra is, (pl. kábeltelevízió, TV és rádió antenna, telefon, Fax, Internet, Ethernet, riasztók stb.) mivel az infokommunikációs eszközök, rendszerek villamos energiát is igényelnek, az adatátviteli hálózat túlfeszültség - védelmét az energia-elosztó hálózattal együtt, azzal összehangoltan kell megoldani.

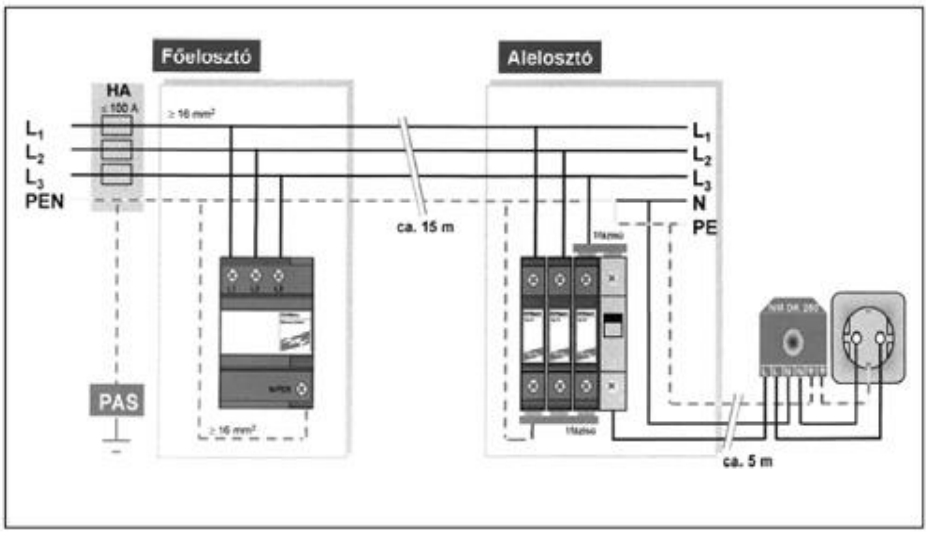
Az adatátviteli rendszereknél az árnyékolatlan kábelből kialakított strukturált hálózat veszélyeztetettebb, mint az árnyékolt, aminél viszont még egy fokkal jobban védett a földelhető fémharisnyával is körülvett rézkábel. Az üvegszálat nem kell védeni, mert az érzéketlen az elektromágneses tér változására. Az árnyékolás nélküli rézkábel viszont minden elektromágneses zajt felvesz. A kisebb zavarok, áthallások ellen viszonylag jó védettséget nyújt az, ahogyan sodorják a réz érpárokat, de éppen a villám olyan nagy változást idéz elő a környező tér mágnesességében, hogy az már óhatatlanul feszültséget generálhat benne. Ez a néhány voltos üzemi feszültségnél jóval nagyobb, s így előfordulhat, hogy tönkretesz valamit az aktív hálózat berendezésekben, vagy a munkaállomásokban.

A túlfeszültség-védelemnél a három fokozatú védelemre azért van szükség, mert villámcsapás esetén a behatoló teljes impulzusenergiát az első és második fokozat nélkül a harmadik, D osztályú finomvédelmi készülékek egyedül nem képesek levezetni, túlterhelődnének, a védendő berendezésekkel együtt tönkremennek, esetleg szétrobbannak és további károkat is okozhatnak. Ugyanakkor csak az első két védelmi fokozat (B és C) beépítése szintén nem elegendő, mert a második C osztályú védelem

feszültséghatárolási szintje még nem nyújt megfelelő védelmet az elektronika tápegységek számára. A 3. sz. ábra egy példát mutat a kisfeszültségű energia-elosztó hálózatok villám- és túlfeszültség védelmére.[5]

Az MSZ IEC 1312-1 szabvány alapján, amely a védelem alapelveit fogalmazza meg, különbséget kell tennünk a vezetett, illetve a sugárzott túlfeszültségek elleni védekezés eszközei között:

- • a vezetett zavarok elleni védekezés eszközei a túlfeszültség-levezetők.
- • a sugárzott zavarok elleni védekezés eszköze az elektromágneses árnyékolás.[8]




3. sz. ábra. Kisfeszültségű energia-elosztó hálózatok villám- és túlfeszültségvédelme

### 2.3.1. A vezetett zavarok elleni védekezés eszközei

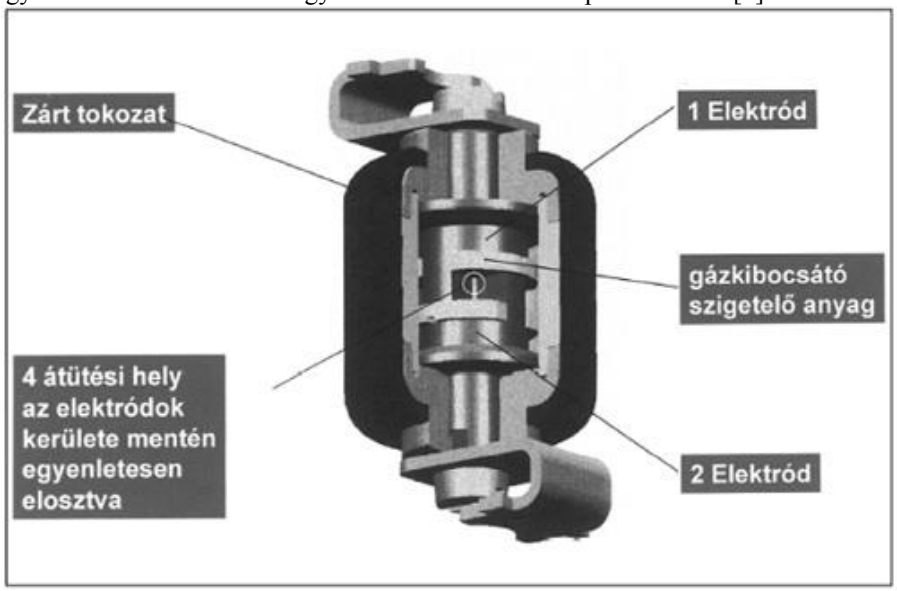
Célunk, hogy a túlfeszültségek csúcsértékét annyira csökkentsük, hogy berendezésünk megtartsa üzemképességét. A túlfeszültség-levezetők közös jellemzője, hogy (jelentős) feszültségemelkedés hatására rövidzár-szerű, majd a feszültség csökkenésével ismét szakadás-szerű állapotba kerülnek, mintha egy kapcsolót gyorsan zárnánk-nyitnánk. Ennek hatására a levezetővel párhuzamosan kapcsolt védett fogyasztó bemenetét a feszültség emelkedésekor rövidre zártuk, így az nem kap majd feszültséget. A feszültség csökkenésével a levezető nyit, a rövidzár megszűnik, és a fogyasztó ismét a normális feszültséget kapja. Ne feledjük, hogy a zárás-nyitás a másodperc kevesebb, mint ezredrésze alatt lezajlik.

A túlfeszültség-levezetők működési elvüket tekintve alapvetően két csoportba sorolhatók:

- szikraköz elvén működő típusok;
- változtatható ellenállás (varisztor) elvén működő típusok.

A szikraközök alaptípusának felépítése és működése egyszerű. Két elektróda között szigetelőrétegként levegő helyezkedik el. Alaphelyzetben az elektródák között a szigetelőréteg miatt nem folyhat áram, ezért ez az állapot a kapcsoló nyitott helyzetének felel meg. Ha az elektródák közötti feszültséget emeljük, akkor elérjük azt a fe-

szültséget, amelyen bekövetkezik az átütés, és elektromos ív alakul ki. Az ív nagyon kis ellenállású elektromos összekötésnek tekinthető, ezért ez az állapot a kapcsoló zárt helyzetének felel meg. Az átütési feszültséget az elektródák távolsága határozza meg: úgy állítják be, hogy az átütés hamarabb következzen be a szikraközben, mint a védett fogyasztóban. A 4. sz. ábrán egy korszerű szikraköz felépítése látható.[5]




4. sz. ábra. DEHNblock nyomásvezérelt, zárt kúszószikraköz

A varisztoros túlfeszültség-levezetőket alapvetően a C osztályú védelemnél alkalmazzák, így a 320V feletti feszültség felett a varisztor vezet, és eldisszipálja a túlfeszültséget.

A hagyományos (tehát elektronikus gyújtással nem rendelkező) szikraközök és a varisztoros túlfeszültség-levezetők kombinált kapcsolása nem teljesíti a nagy levezető-képességet, az alacsony védelmi szintet és a gyors megszólalást.

Az új túlfeszültség-védelmi aktív energiavezérléssel (Active Energy Control - AEC) az elektronikus vezérlésű szikraközök és középvédelmi varisztorok párhuzamos kapcsolását valósíthatjuk meg. Az elektronikus vezérlésű szikraközök gyújtóelektronikája egy gáztöltésű szikraközt tartalmaz, mely önmagában nem biztosítja a gyors megszólalást, ezt továbbra is a varisztor garantálja számunkra. A kis homlokmeredekségű impulzusok esetén (ez esetben a leválasztó tagon eső feszültség nem lenne elegendő a szikraköz begyújtásához) az elektronikus gyújtás a rá jellemző megszólalási feszültség elérésekor (0,9/1,5 kV) minden esetben biztosan előgyújtja a főelektródákat és megtörténik a levezetés. Ezzel a védelmi kapcsolás érzéketlenné vált a feszültségemelkedés meredekségére, mely a régi kialakításoknál a kritikus hibákat okozott.[9]

### 2.3.2. A sugárzott zavarok elleni védekezés eszközei

A kapacitív és induktív csatolás esetében a védekezés módja a megfelelő árnyékolás alkalmazása és a rendszerek vezetékeinek, valamint a villámhárító levezetőinek átgondolt, megfelelő geometriájú elhelyezése.

Elektromágneses hullámok elleni árnyékolás módszerei lehetnek:

- abszorbeáló;
- reflektáló.[10]

Az abszorbeáló árnyékolási módszernél rádiófrekvenciás energiát elnyelő anyagokat alkalmaznak, ahol az energia elnyelés nagyságától és a frekvenciasávtól függően a vastagság a 60 cm-t is elérheti. Az árnyékolt területen átlátszó, üvegezett felületek nem megengedhetők. Ezt az árnyékolási módszert általában laboratóriumoknál alkalmazzák.

A reflektáló árnyékolási módszernél a védendő teret rádiófrekvenciásan reflektáló anyagokkal vonják be, oly módon, hogy a bevonat folyamatos legyen. Az árnyékolás elválasztja a külső teret a védendő belső tértől, a jel a reflektáló rétegen csak erősen csillapítva (50-120 dB) juthat át.

Nagy előnye ennek az eljárásnak, hogy lényegesen olcsóbb, mint az abszorbeáló módszer, sokkal kevesebb a helyigénye, és fényáteresztő üveg felületek is megengedhetők. A reflektáló módszer előnyös tulajdonságai miatt szinte kivétel nélkül ezt a megoldást alkalmazzák a rádiófrekvenciás árnyékolásban.

Az elektromágneses árnyékolás a megvalósítást tekintve lehet pontszerű vagy területi. Pontszerű árnyékolás esetén az árnyékolás egy szűk területre, pl. egy alkatrészre korlátozódik, a területi árnyékolás pedig egy bizonyos területen elhelyezett összes elektronikai berendezés árnyékolását biztosítja.

Az elektromágneses árnyékolás megvalósításánál az oldalfalakon kívül nagy figyelmet kell fordítani a nyílászárók árnyékolására is, illetve biztosítani kell, a védet térbe csatlakozó vezetékek (áramellátás, számítógépes hálózat stb.) elektromágneses szűrését.

## Összegzés

Az infokommunikációs eszközök, rendszerek gyors fejlődése teljesen átalakította, illetve beépült mindennapi életünkbe. Ugyanakkor nem szabad figyelmen kívül hagynunk, hogy ezen eszközök, rendszerek nagyon érzékenyek a különböző elektromágneses zavarokra és alapvetően villamos energia felhasználásával működnek. Ugyan az érzékeny elektronikai eszközök zavarmentes működését az elektromágneses kompatibilitás szabványiban előírt paraméterek szigorú betartásával megfelelően biztosítható, de nem szabad elfeledkezni a természetes zavarforrások hatásairól sem.

Ezért a villámcsapások közvetlen és másodlagos hatása miatt kialakuló túlfeszültségek ellen is megfelelően védenünk kell az érzékeny elektronikai eszközeinket, rendszereinket, oly módon, hogy a fellépő túlfeszültség csúcsértékeket az elektromágneses kompatibilitás szabványokban előírt határértékeknél alacsonyabb érték alá szorítjuk. Ennek szabványosítási vonzataként hazánkban „A villámvédelem” szabvány követelményrendszerét is módosítni kellett úgy, hogy már megjelent a szabványban „Az elektromágneses villámimpulzus elleni védelem” módszere is.

Mindezek alapján megállapítható, hogy hazánkban a gyakori villámimpulzusok ellenére a módosított szabványok követelményeinek is megfelelő több fokozatú villám és túlfeszültség-védelemmel biztosítható az infokommunikációs eszközök zavartalan folyamatos működése.

## Felhasznált irodalom


[1] Mi is az az elektromágneses zavarvédelem? http://www.vgf.hu/villany/index.php?action=viewfull&ID=53

[2] Vass Sándor: A Magyar Honvédségben az elektronikai harc - ezen belül az elektronikai védelem - számítógépekkel biztosított tervezése, különös tekintettel az elektromágneses kompatibilitás kérdéseire. Kandidátusi értekezés, Zrínyi Miklós Katonai Akadémia, Budapest, 1995.

[3] Villám- és túlfeszültség-védelem az MSZ 274, MSZ IEC 1312-1 és az MSZ 447 módosításai szerint: http://www.dehn.hu/

[4] Adatátviteli hálózatok védelme: http://www.dehn.hu/

[5] EMC villámvédelem és túlfeszültség-védelem V. rész: http://epa.oszk.hu/00000/00025/00001/feher.html

[6] „Villám-háború" - júniusban csap le a legtöbb villám: http://www.terminal.hu/newsread.php?id=15201506052615

[7] Hogyan védekezzünk a villámok ellen? http://www.vgf.hu/villany/index.php?action=viewfull&ID=20

[8] Túlfeszültség – védelem: http://www.vgf.hu/villany/index.php?action=viewfull&ID=85

[9] Túlfeszültség-védelmi eszközök régen és most. A védelmi technológiák fejlődése: II. rész: AEC - Aktív Energiavezérlés, az új technológia: http://www.vgf.hu/villany/biztonsagtech.php?action=viewfull&ID=115

[10] Dr. Vass Sándor - Dr. Balajti István: Elektronikai védelem, Budapest, ZMNE, J-1435, 2000.

# II. FEJEZET


ÉS ÖNNEK MI
MINDENHEZ
KELL ÉRTENIE?
Ön a telefon-specialista. És az adathálózati szakértő. Sőt, a pénzügyi guru. Elvárják, hogy mindenhez értsen. Gondoljuk csak végig: amennyiben a hang, az adat és a video egyetlen, egységes és biztonságos hálózaton utazik, a dolgok lényegesen leegyszerűsödnek. Nem kell telephelyenként eltérő alközponti rendszereket üzemeltetnie, mindent egy helyről felügyelhet, miközben pénzt és időt takarít meg. A felhasználók számára pedig az alkalmazások széles skálája válik elérhetővé. Egy hálózat. Egy megoldás.
KOMMUNIKÁCIÓ, MÁSKÉPP. CISCO IP KOMMUNIKÁCIÓ.
További információért kérjük látogasson el a www.cisco.com/hu/iptel weboldalra, vagy hívja a 06-80-017941-es telefonszámot.
CISCO SYSTEMS
THIS IS THE POWER OF THE NETWORK. NOW.

**Károly FEKETE**

# THE MULTI-NATIONAL MISSIONS AND THE NETWORK ENABLED CAPABILITY

*This Paper was supported by the János Bolyai research Scholarship of the Hungarian Academy of Sciences*

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

## Abstract

*This Paper shows a short description of the recent broadband NATO Network Enabled Capability with regard to main aims and to evolution of platform of military operations in multi-national missions. The paper shows how we can connect a deeply separated military communications network primarily and via the different kind of gateways. At the end of the paper we can see the elements of the application concept of C3IS in multinational-mission.*

## Introduction

NATO Network Enabled Capability (NNEC) is no less than embodiment of an information age transformation of the military. NNEC has the chance to utilise and growing up the war-fighting capabilities by orders of its scale. By the side of increased potential of NNEC we can make a remark into the direction of demand of the full access of all available information. From point of view of the NNEC we have a lot of particular areas from autonomous systems to safety critical systems, from interference techniques to vulnerability analysis, from human computer interaction to expert systems and from team dynamics & psychology to soft system analysis (Fig. 1). All this assessments we may see with regard to physical, information and cognitive level of NNEC.

The main aims of NNEC are:

- Information sharing improve the quality of information (access, anytime, anywhere, anyspeed) and shared situational awareness;
- Robustly networked military force improves information sharing;
- Shared situational awareness enables cooperation and self-synchronisation;
- Significant increase mission effectiveness.

Whenever the digital army system is implemented around the globe, the digital army system must be a highly modular system. This system can enables the military to implement the digital army concept under an overall master plan. Considering these

facts the NNEC shall give the opportune answers between of the well known traditional and evolving battle-space trends such as:

- Information superiority;
- Missions of low profiles;
- Reconnaissance missions;
- High weapon lethality;
- Asymmetry of Conflicts;
- Precision engagement;
- Suddenly appeared terrorism activity;
- Peace Keeping Missions.

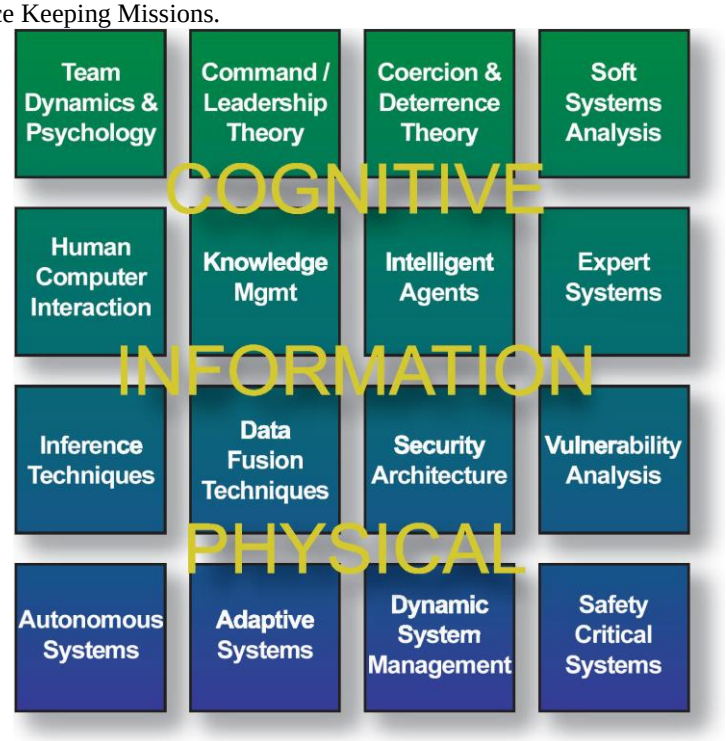



Fig. 1. The three layers of the components of the NNEC

Another important aspect is the evolution of the scenario of the military operations. Analysing the Fig. 2., we can see the three phase of the attitude to the missions.

The first aspect is the platform centric operations, where the observing process, decision and the act are separated from one another. The second one is the using of the integrated systems, where the parts of the military operations are connected to each other and have a repercussive effect on the flow-time process. The last but most sophisticated kind of the military operation is the network centric method, which is a multi-centralised and multi-sourced form. This operation has a strictly parallel behaviour in the time.

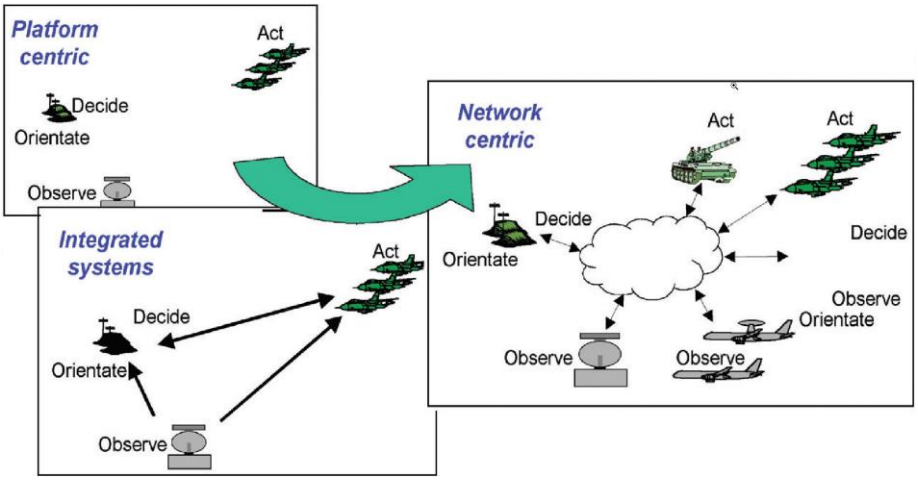



Fig. 2. The evolution of the platforms of the military operations

The next gravity of questions is the continuity of operation in time and across different operational scenarios because a snapshot view of the battlefield situation is not enough. In a multinational missions the command, control, communications and information system ($C^3IS$) should provide continues and integrative situation awareness of the missions. The $C^3IS$ is required to operate in diverse missions situations. It should continue to work in times of peace, training, peace keeping, low intensity conflict, multinational mission and comprehensive war. Consequently the needs in front of NNEC are:

- Support of all kind of operational processes;
- The finest and secure working of communications infrastructure across the entire three dimensional battlefields.

The $C^3IS$ in multi-national mission must be designed to connect the ground forces, air force and navy and streamlined information exchange between them. This kind of connectivity can be achieved through the:

- Strategic connection. The relevant information between military services is sent to each others using dedicated connections. This means, in this situation we have a freedom in designing and maintaining of tactical communications network;
- Direct connection. This type of connectivity supposes the highest level of interoperability Type 6 (Fig. 3.). The condition of effective interoperability is using compatible communications hardware, networking protocols and C3IS applications. The main drawback of this solution is the need for strong cooperation between communications services.
- Multi-national connection. It is the main type of the multi-national interconnection between units of different nations operating under the same mission framework, i.e. NATO. It is means that the military units belong to own tactical network. The digital strategical-tactical gateway (DSTG) and the STANAG 4206 gateway interconnect different units from different nations. This solution enables to design and maintain every systems independently from other nations in multinational-mission (Fig. 4.).

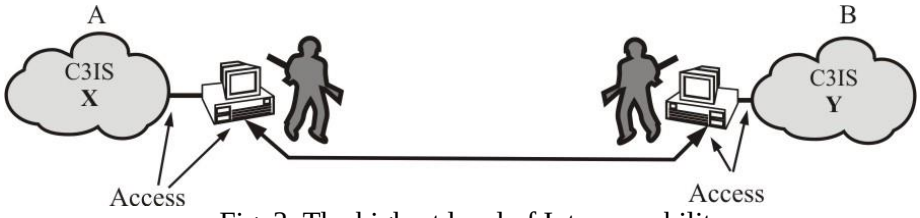


Fig. 3. The highest level of Interoperability

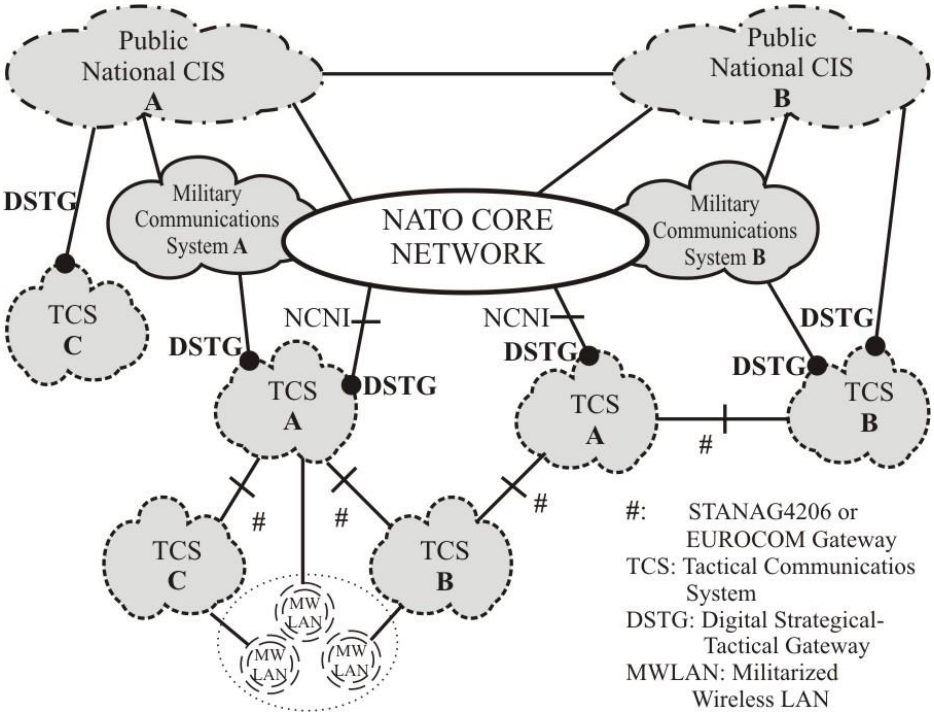


Fig. 4. The configuration of multi-national connections

In this scenario the application concept of C3IS of multinational-mission may consists:

- Vertical and horizontal integration principal;
- Interconnectivity (jointness of operation, interoperability, legacy system incorporation, sensor integration);
- Commander centric principal;
- Flexibility;
- Seamless operations.

## References


[11] Dr. Szép József: A NATO új kezdeményezése a hálózat nyújtotta képesség, Kommunikáció 2004 nemzetközi szakmai tudományos konferencia különkiadványa, Budapest, 2004. szeptember 15., pp. 289-303, ISBN 963 86441 5 X

[12] IEEE 802.16* and WiMAX, Broadband access for evereyone, White Paper Broadband Wireless Access, Intel Corporation, 2003.

[13] www.wimaxforum.org

[14] www.ieee802.org/16

[15] Dr. Barry Sowerbutts: Network Enabled Capability, Roke Manor Research Limited, Hampshire SO51 OZN UK, NBU/BS/0303/0287.1, www.roke.co.uk

[16] David Ferbrache: Network Enabled Capability: concepts and delivery, Journal of Defence Science, Vol. 8., No. 3., September 2003, pp. 104-107.

[17] David S. Alberts, Richard E. Hayes: Power to the Edge – Command … Control … in the Information Age, DoD Command and Control Research Program, Library of Congress Cataloging-in-Publication Data, June 2003, ISBN 1-893723-13-5

[18] STANAG 5048: The minimum scale of connectivity for communications and information systems (CIS) for NATO Land Forces, Edition 5 (Final Draft).

**Károly FEKETE**

# TOWARDS A NEW GENERATION OF WLAN IN MILITARY COMMUNICATIONS

*This Paper was supported by the János Bolyai research Scholarship of the Hungarian Academy of Sciences*

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

## Abstract

*The NATO Network Enabled Capability concept shows the need of reliable communications even in multi-user environment. This paper give a short analyse of the TDM based N-ISDN versus a packet-switched based protocols defined by ITU-T and IEEE 802.11a-n. The analyse shows that we may give some useful results with Markov process flow graph in both situations, but the final results of the flow process of the transmissions is a bit different.*

## Introduction

The nowadays working legacy technologies in the not too highly advanced military communications systems as the time-division multiplexing modulation (TDM) methods are assimilated into the MCN (Military Communications Networks). Not considering this fact, new fast and massive mobile data and video transmission applications in military environment serves as the basic for building block for implementing the NATO Network Enabled Capability (NNEC) concept.

The MSCS network consist a number of nodes interconnected by standard 2048 kbit/s PCM links. Some of them connected to another by n x 2 Mbit/s (n=2,3,4 or 8) PCM links. The physical mediums of interconnection are microwave, coaxial cable and a small part of them optical fibre and satellite links.

The topology of MSCS is either ring, or a meshed or a combination of the two ones with special regard to customer requirements. If necessary, analogue trunks associated with a dedicated data link for channel signalling may be used as a substitute for the PCM links, without loosing any of the networking capabilities of the MSCS. One of the operative features of the ISDN part of the MSCS provides for the ISDN a self-protective mechanism against such blocking factors as heavy traffic ( Table 1. and Fig.1. ). Networks using distributed adaptive routing procedures can dynamically sense changes in their external environment by exchanging information between nodes.

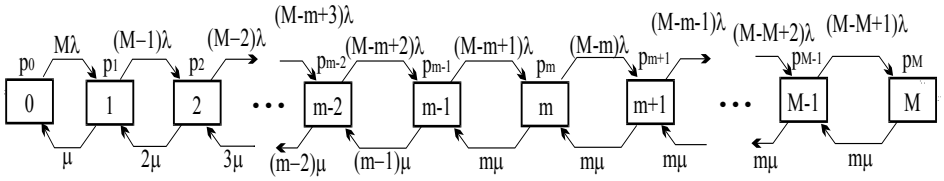



Fig. 1. Markov process flow graph for the N-ISDN, M military subscriber, group access, TDM

Table 1. Probability of queuing (Pq) and average traffic demand (N), (Ψ=0,8; N-ISDN; PRA; M = military subscriber number).

| **M** | 40 | 50 | 60 | 70 | 80 | 90 | 100 |
|---|---|---|---|---|---|---|---|
| **Pq** | 8*10-5 | 0,002 | 0,26 | 0,76 | 0,98 | 1 | 1 |
| **N** | 17,7 | 22,2 | 27 | 33,5 | 42,5 | 52 | 62,5 |

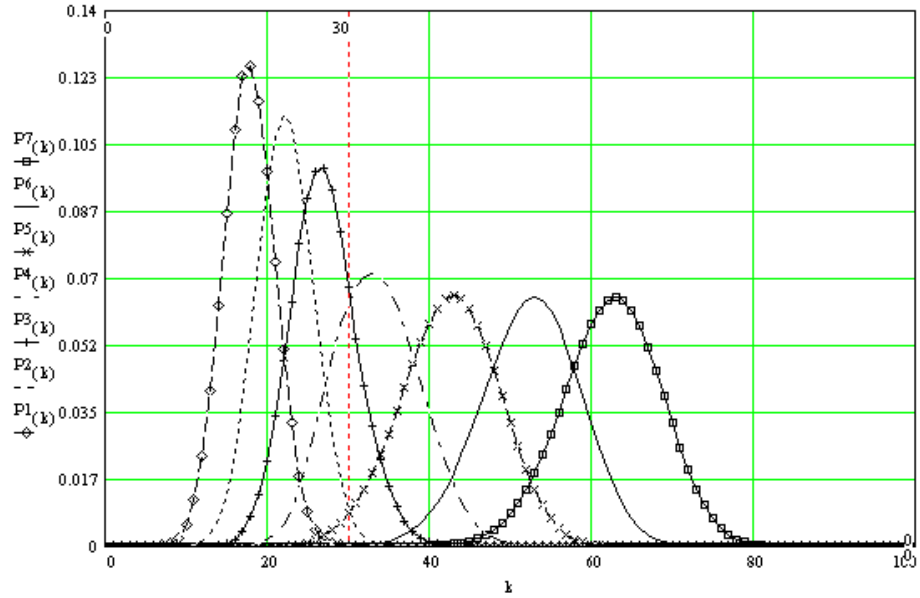



Fig. 2. Probability of queuing220 (Pq) and average traffic demand (N), (Ψ=0,8; N-ISDN; PRA; M = military subscriber number).

Differentiate two parts of the possible value of **k,** the probability of **k.** status is

**1.** in the case of $0 \le k \le m-1$:

$$p_k = p_0 \prod_{i=0}^{k-1} \frac{(M-i)\lambda}{(i+1)\mu}, \text{ and } p_k = p_0 \left(\frac{\lambda}{\mu}\right)^k \prod_{i=0}^{k-1} \frac{(M-i)}{(i+1)} \qquad (1.1).$$

[220] The simulation made with MathCad Professional V 7.0.

$$p_k = p_0 \left(\frac{\lambda}{\mu}\right)^k \binom{M}{k} \qquad (1.2).$$

**2.** in the case of $m \le k \le M$, with special regard to the probability of the $0 \le k \le m-1$:

$$p_k = p_0 \prod_{i=0}^{m-1} \frac{(M-i)\lambda}{(i+1)\mu} \prod_{i=m}^{k-1} \frac{(M-i)\lambda}{m\mu}, \qquad (1.3), \text{ and}$$

$$p_k = p_0 \left(\frac{\lambda}{\mu}\right)^k \prod_{i=0}^{m-1} \frac{(M-i)}{(i+1)} \prod_{i=m}^{k-1} \frac{(M-i)}{m} \qquad (1.4), \text{ and}$$

$$p_k = p_0 \left(\frac{\lambda}{\mu}\right)^k \binom{M}{k} \cdot m^{m-k} \cdot \frac{k!}{m!} \qquad (1.5).$$

Since in the expressions of the $\mathbf{p_k}$ (1.2 & 1.5) we can found $\mathbf{p_0}$, that is why we easily may determine value of the $\mathbf{p_0}$:

$$p_0 + \sum_{k=1}^{M} p_k = 1 \qquad (1.6), \text{ and from this:}$$

$$1 = p_0 + \sum_{k=1}^{m-1} p_0 \cdot \left(\frac{\lambda}{\mu}\right)^k \cdot \binom{M}{k} + \sum_{k=m}^{M} p_0 \cdot \left(\frac{\lambda}{\mu}\right)^k \cdot \binom{M}{k} \cdot m^{m-k} \cdot \frac{k!}{m!} \qquad (1.7).$$

The final result of the probability of 0 condition of the ISDN Primer Rate Access (p0) is the next relation:

$$p_0 = \frac{1}{\sum_{k=0}^{m-1} \left(\frac{\lambda}{\mu}\right)^k \cdot \binom{M}{k} + \sum_{k=m}^{M} \left(\frac{\lambda}{\mu}\right)^k \cdot \binom{M}{k} \cdot m^{m-k} \cdot \frac{k!}{m!}} \qquad (1.8).$$

Utilizing the last expression (1.8) the distribution of probability of queuing of military subscribers at N-ISDN PRA we can see in the Fig. 3.

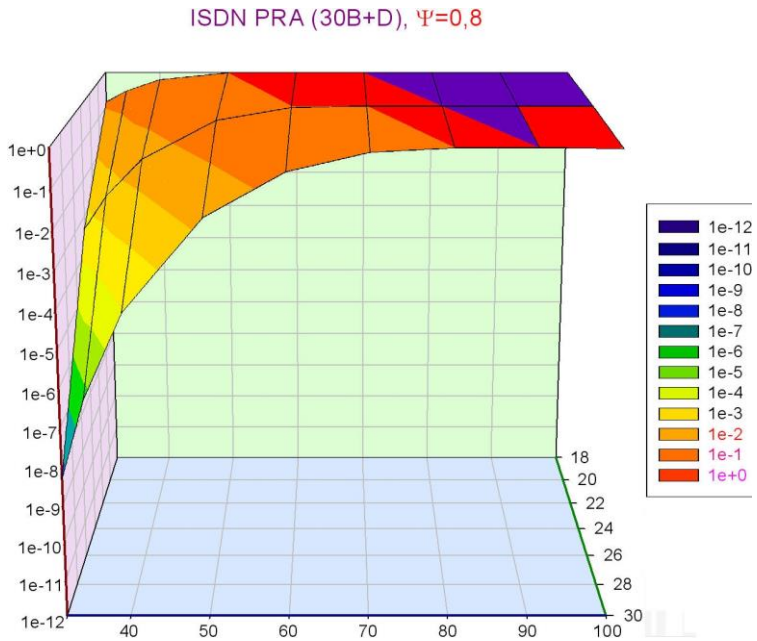



Fig. 3. Distribution of probability of queuing of military subscribers[221]

The analysis of the traffic flow in the packet-switching environment is a quite different problem. The most popular wireless LAN protocol (IEEE 802.11b) working with packet fragmentation. That is why we must introduce in the military TCP/IP based WLAN the Analytical Model for the packet transmission time (Ψ).

The Ψ is the time required to successfully transmit a TCP/IP packet with a message duration $T_m$. Considering the IEEE 802.11a-n standards, these messages may be either a single packet or as a sequence of $N_f$ small packets. At this time a message, which is fragmented into $N_f$ packets require:

$$T_m N_f^{-1} \quad (1.9).$$

The packet-switching transmission has two important characteristics:

- the good point of this kind of transmission is a lower packet collision likelihood because of the shorter transmission time;
- the bad point of the packet-switching method is the need of the additive transmission overhead.

The quality of the packet-switching transmission we may evaluate by assessing the expected transmission time E[Ψ].

Important emphasize that fact the IEEE 802.11a-n based protocol designed not only in peer to peer but in the ad-hoc mode. In this environment the factor influencing the probability of collision, p is defined as the event when an IEEE 802.11a-n packet[222] requires retransmission due to the presence of another IEEE 802.11a-n interface. This kind of distribution is a $K_j$ type and we can use a Markov process to evaluate the

[221] The final result represented by Sigmaplot V.7.0 graphing software.

[222] Or fragment of packets

number of collisions (Fig. 3.). $K_j$ is associated with transmitting the *j*th packet (or fragment).

The packet transmission time is:

$\Psi = N_f(T_m N_f^{-1} + T_{0S}) + (T_m N_f^{-1} + T_{0F})K + T_{b0}(K)$ (1.10),

where $T_{0S}$ is the successful packet fragment overhead transmission time, and the $T_{0F}$ is the failed packet fragment overhead transmission time.

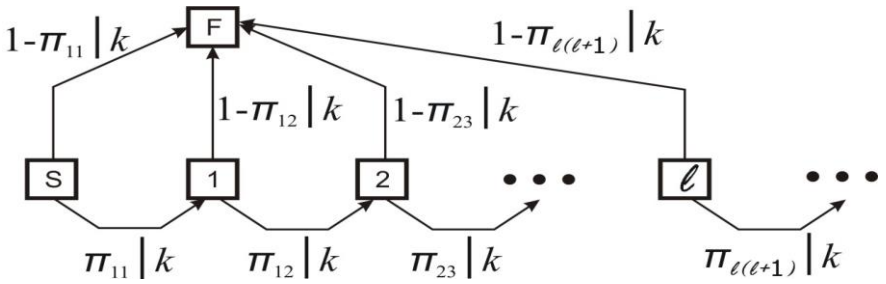



Fig. 4. Markov process flow graph for the general model of Kj

In the Markov process flow graph S and F represent the initial packet transmission and successful fragment transmission states, and 1, 2, 3, … *l*-1, *l*, *l*+1 are the retransmission states. The state transition probabilities is $\pi_{l(l+1)} \mid k$.

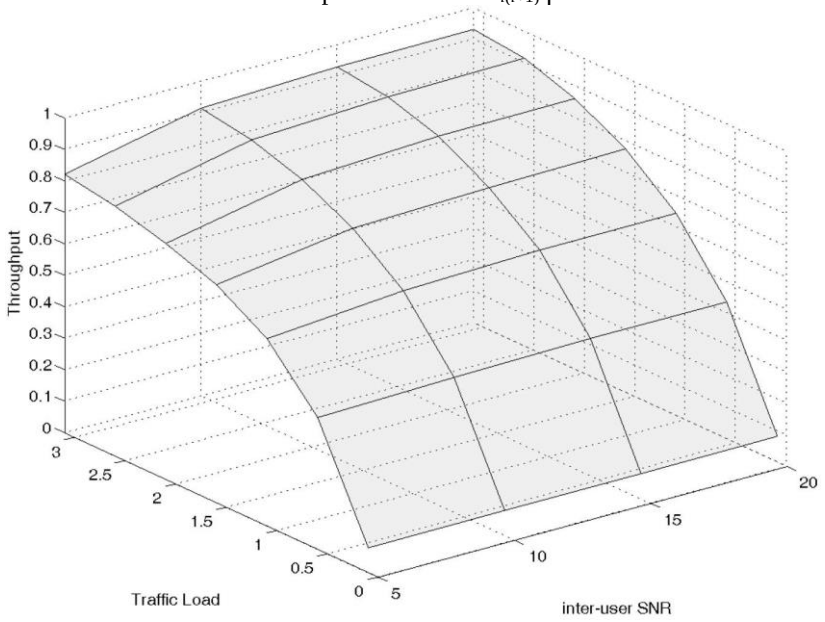


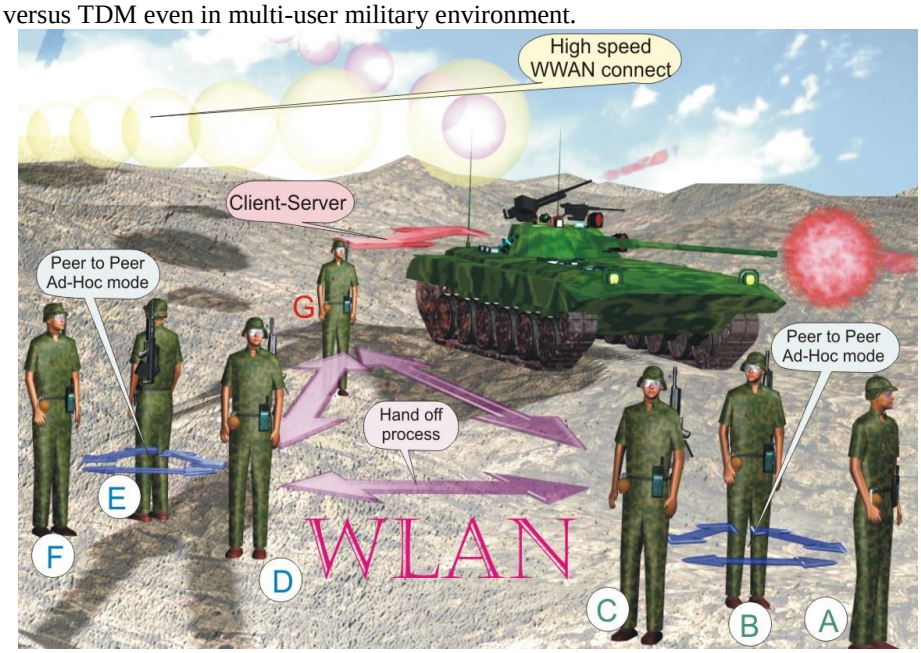

Fig. 5. Throughput versus traffic load and inter-user SNR (v=3m/s, R=12 Mbps)

Considering these facts, the IEEE 802.11a-n based protocol seems as a slotted-ALOHA system, which allows user transmit in an uncoordinated fashion every time they have a packet to transmit. But for the pure slotted-ALOHA the highest throughput

is 1/e. At the end of the examination in the environment of the flat fading channel with the transmission rate R=12 Mbps we can see the throughput of the IEEE 802.11a-n based protocol in the Fig. 5.

## Conclusions:

Considering the fast and massive mobile data and video transmission demand, the wireless TCP/IP based transmissions come to the front in the military applications. The analysis of the TDM based N-ISDN and a packet based 802.11 WLAN shows that, the queuing models are different. The packet switched protocol has some benefit versus TDM even in multi-user military environment.




## References


[1] Fekete Károly: A keskenysávú ISDN primerhozzáférésének vizsgálata katonai alkalmazási környezetben, Nemzetvédelmi Egyetemi Közlemények, 2001/4. szám, 144-157. oldal, ISSN 1417-7323, 2001.

[2] Karoly Fekete: Hungarian Military Strategic Communications System -in mirror of Advanced Military Technology, Korszerű Katonai Technológiák a XXI. században – Az új felderítő elektronikai hadviselési rendszerek koncepciói, Nemzetközi Konferencia, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2000. május 17-18.

[3] Fekete Károly: A Magyar Honvédség állandó telepítésű kommunikációs rendszere továbbfejlesztésének technikai lehetőségei, Doktori (PhD) értekezés, Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, 2003.

[4] Proposal for Non-Collaborative 802.11 MAC Mechanisms for Enhancing Coexistence: Adaptive fragmentation, IEEE 802.11b Coexistence Testing Data, Ieee 802.15-01/083, 2001.

[5] Ivan Howitt, Fahed Awad: Optimizing IEEE 802.11b Packet Fragmentation in Collocated Bluetooth Interface, IEEE Transactions on Communications, pp. 936-938, June 2005, Vol. 53, Number 6, ISSN 0090-6778.
[6] Rui Lin, Athina P. Petropulu: A New Wireless Network Medium Access Protocol Based On Cooperation, IEEE Transactions on Signal Processing, pp. 1-27, December 13, 2004.
[7] Robert Hoskins: Military Spec, Multi-mode 802.11 WLAN Solutions for Indoor, Outdoor & Harsh Environments, (BW)(MD-3E-TECHNOLOGIES), www.bbwexchange.com/publications/newswires/page546-809891.asp, 2005.
[8] Peter Rysavy: Secure Wireless Networking Using SSL VPNs, RYSAWA Research, http://rysavy.com, 1-551-386-7475.
[9] Roy Mark: IPv6 Transition Crucial to Military, http://www.internetnews.com/infra/print.php/3287191, December 9, 2003.
[10] Dilip Advani: 802.11g – The Need for Speed, Airmagnet, www.airmagnet.com, 2004.
[11] David Essex: Eight developments will shape how agencies balance the need for security againts the push mobility, GCN Staff, Antrim, N.H., Wireless 2006: Gaining momentum, Vol. 24. No. 21, aug. 01. 2005.
[12] Karoly Fekete: Network Enabled Capability with regard to WLAN, „Robot Warfare" Nemzetközi Tudományos Konferencia, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2004. november 24.

**Károly FEKETE**

# SECURE BASED WIRELESS IP PROTOCOLS WITH REGARD TO CLOSED NETWORKS

*This Paper was supported by the János Bolyai research Scholarship of the Hungarian Academy of Sciences*

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

## Abstract

*The recent industrial WLAN solutions suggest the deep discussion of security problems in military communications environment. This paper analyses the real vulnerable security platforms provided by most common commercial off the shelf (COTS) WLAN technologies. In this article we can found not only the problems connected to the possible attacks of several layers of the WLANs but the paper trying out to give some suitable solutions and practical improvements.*

## Introduction

Security is the principal topic of the peace time and the critical missions in military operations from Department of Defense to any unit or formation. The moving toward in communications and networking technology have enabled new possibilities in mobile military applications. But as in the overwhelming majority of the cases the physical medium of mobile communications is the atmosphere (air), so this "opened door" increasing vulnerability of communications networks and risks in security.

The most attractive characteristics of the mobile communications are the ability to call up information and communicate at any time, in any place. These points of view are so considerable that the disadvantages of mobile communications thrust into the background, even the security risks are real.

The stunning success of "wireless Ethernet" based on the standard IEEE 802.11a-n made it widely known not only to the civilian but even particularly to the military communications applications.

The IEEE 802.11a-n standards recommend the optimal communications distances from 10 to 3-400 meters (with special hardware upgrades to 1000 meters in military applications) and to 256 mobile users simultaneously. The IEEE 802.11a-n standards (IEEE 802.11a, b, or g) describe how data is transmitted from each user to other user at the physical level (Physical layer of OSI-ISO).

As we mentioned the data transmitting through the air so everybody can access to the information of the physical level, but the IEEE 802.11a-n standard consist layers

above this physical layer. That is why we can not prevent hackers from detecting our RF signal of WLAN.

The IEEE 802.11b devices working with Complementary Code Keying (CCK) modulation and operate in the 2.4 GHz band (Industrial Scientific Medical – ISM). The IEEE 802.11a is uses the Orthogonal Frequency Division Multiplexing (OFDM) technology and operate in the 5 GHz band (Unlicensed National Information Infrastructure –UNII). IEEE 802.11g WLAN devices operate at ISM band and use OFDM modulation with supporting Barker Code and CCK modulation for backward compatibility with IEEE 802.11b standard.

The IEEE 802.11g has the Extended Rate Physical (ERP) layer. Every packet is made of preamble, header information and the payload for the serviceable information. The short preamble (96 μsec) is optional and the longer preamble (120 μsec) is mandatory at the IEEE 802.11b, but both types supported by IEEE 802.11g. That is why the wireless LAN is easy to find, and top of all WLAN network must transmit Beacon frames with adequate network parameters.

It is suppose from attackers to have high-gain antennas. For example the working IEEE 802.11a-n network parameters are available for anybody with an IEEE 802.11a-n card. The solutions for this access problem are quite different. In military environment strong user authentication should be deployed and networks should place access points outside of security perimeter devices (firewalls, routers). If the radius of the WLAN applications is known, the wireless network operators may adjust the minimal required signal level and in extreme situations a WLAN could be confined to an electromagnetically shielded place (for example at HQ).

The second problem about the security of WLAN is the applications of the "Rogue" access points. This is the kind of extravagant behaviour of military users. They can run to the nearest computer store to buy a WLAN access point, and connect to the military WLAN without any authorization from central military officers or security administrators.

This type of users actions hold great security risks because a no-name WLAN hardware (routers, switches, access points) do not have any security features enabled. Good method for discovery of unauthorized networks is use a good high-gain antenna and finds it (before the attackers exploit them). This is the regular site audits and it should be conducted as frequently as possible. The other prevention method is may be the using the products and WLAN set of well known manufacturers.

The next focus point about the secure based wireless protocols is the unauthorized use of service even in multi-national environment. This type of problem connected with not activated Wired Equivalent Privacy (WEP), which is the security protocol for IEEE 802.11b wireless networks. In this situation almost all of the military access points running with default configuration or are put in service with only minimal modifications.

The possible answer for this practice is to prevent unauthorized users from accessing the military WLAN. Any Virtual Private Network (VPN) solution presumes the strong physical defense and protection of traffic at the time of transmission across the air. The well controlled cryptographically protected authentication is a good way for support of privileged access and for takes care of user identity. The other important

procedure at this point is the rigorously followed authentication and authorization policies.

The responsible military officer for the design and audit for strong authentication must be ensured that the strong authentication mechanism is in use, so the site audits are an indispensable element of WLAN security.

Accordance to the IEEE 802.11a-n standards the WLANs have limited transmission capacity. IEEE 802.11b based networks have the 11 Mbps maximum throughput and IEEE 802.11a and IEEE 802.11g have a bit rates up to 54 Mbps.

Considering the fact of the size of the MAC-layer's overhead, the average throughput about the half of the theoretical limited data transfer speed. That is why the service and performance constraints in military wireless LANs exist. The IEEE 802.11a-n employs Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) protocol, which is allows the WLAN device that is transmitting data exclusive transmitting rights.

Consequently no other wireless LAN device will transmit at the time and will begin information transmission only when the air is free. The IEEE 802.11a-n MAC is designed to allow multiple networks to share the same space and RF channel.

This limitation is a good way to attackers to launch a denial of service (DOS) type attack on the limited resources. Attackers can send a massive and oppressive traffic – even with method of sending a high powered "white noise" transmission - on the same radio channel so the military WLANs can simply overload.

The best prevention from this malicious attacks is the monitoring the military wireless network to report on signal quality and WLAN's health at the military deployment. The software developers must implicate several built-in alarm services for detecting malicious floods of unauthenticated control of MAC frames.

The higher OSI-ISO level attack is the most sophisticated tools in the hands of the attackers. The Secured Socket Layer (SSL) and Internet Protocol Security (IPSec) are both encryptions used to create VPNs. These protocols often use public – and private key encryption algorithm (for example: Rivest – Shamir – Addleman –RSA).

IPSec works at Network layer (Layer 3) of OSI-ISO interconnection model and secures everything in the network. IPSec uses two-way authentication using Data Encryption Standard (DES), which is a symmetric cipher defined in Federal Information Processing (FIPS) Standard Number 46 in 1977.

The experience of the latest years shows that the hackers ready to work long and hard to break encryptions. Once the hacker gains access to the WLAN (and it is only a matter of time), it can serve as a base for attacks on other military communications systems.

The solution over the higher level attacks is the next. The responsible military signal officer must place the WLAN access point logically inside the area defended with a strong, proven access control technology (firewall). For all practical purposes the IT manager must apply the latest security protocols described in IEEE 802.11i for delivering strong security on a wireless network, because of the IEEE 802.11i may be implemented regardless the type of IEEE 802.11a-n.

Instead of the Wired Equivalency Privacy (WEP) where the authentication is 1-sided, the encryption is a weak implementation of RC-4 (Rivest-Cipher algorithm 4) and uses static keys, the responsible officer can use WIFI protected access (WPA) type

2, which is based on the new IEEE 802.11i[223] wireless security standard. The WPA type 2 includes Advanced encryption standard (AES) and use a 128-bit encryption technique.

The authentication form of WPA is 2-sided provided by IEEE 802.1x and the security of the WEP is very strong but must properly managed. WPA uses the Temporal Key Integrity Protocol (TKIP) with a 48-bit Initialization Vector (IV) with automatic changes of keys after a specific number of packets instead of the 24-bit IV of WEP. The IEEE 802.11i with WPA type 2 is use a Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). CCMP utilizes 128-bit keys (Table 1.), with a 48-bit initialization vector (IV) for replay detection and the Cipher Block Chaining Message Authentication Code (CBC-MAC) component of CCMP provides data integrity and authentication.

Table 1. Comparison of several encryption protocols of IEEE 802.11a-n WLAN

| **Name of security protocol** | **WEP** | **WPA** | **802-11i with WPA type2** |
|---|---|---|---|
| **Encryption protocol** | WEP | TKIP | CCMP |
| **Cipher** | RC4 | RC4 | AES |
| | 40 or 128 bit | 128 bit | 128 bit |
| | 24 bit IV | 48 bit IV | 48 bit IV |

## Conclusions

The paper shows that the choosing a good security strategy in the WLAN-s is only a half the battle because every security strategy carries with it certain vulnerabilities.

Effective administration of an IEEE 802.11a-n WLAN requires military network professionals to maintain the full control over the WLAN operating in the military environment.

The main tasks of the responsible military officers with regard to support of the security of WLANs are:

- Randomly timed security audits to track WLAN devices;
- Performing ongoing the military WLAN hardwires;
- Proper choosing and applying the latest encryption protocols and security enhancements;
- Performing systematic security testing of the WLAN;
- Discovering and monitoring wireless technology for new threats and vulnerabilities.

[223] WPA is the standard proposed by WI-FI Alliance and the 802.11i is the standard delivered by IEEE, and is the official standard to replace WEP.

## References


[13] Wade Williamson: Wireless Security in the Government Environment, Airmagnet, www.airmagnet.com , pp. 27., 2004.

[14] George Ou: New generation of hacking tools puts many more Wireless LAN at risk, http://216.239.59.104, pp. 6, December 16, 2004.

[15] Wade Williamson: Best practices for securing your enterprise WLAN, Airmagnet, www.airmagnet.com , pp. 29., 2005.

[16] Dilip Advani: 802.11g – The need for Speed, Airmagnet, www.airmagnet.com , pp. 17, 2004.

[17] Matthew Gast: The top seven security problems for 802.11 Wireless, Airmagnet, www.airmagnet.com , pp. 18, 2004.

**Gyula MIKÓ, András MAGYAR**

# C-BAND ADAPTIVE RADIO DIRECTION FINDING SYSTEM

Hardware Description and Measurement Results
Gyula Mikó (miko@mht.bme.hu)
András Magyar (magyar@mht.bme.hu)
Supervisor: Rudolf Seller (seller@mht.bme.hu)

Department of Broadband Infocommunications and Electromagnetic Theory, Budapest University of Technology and Economics,
Műegyetem rkp. 3-9.,H-1111, Budapest, Hungary

## Abstract

A recently developed re-configurable 16-channel radio direction finder antenna array is presented with measurement results. The array has 16 I-Q channels and it is capable of measuring the direction of radio sources radiating at 4500MHz in 2D. First, few words are said about adaptive radio direction estimation in general, then the structure of the system is explained. Following this, usage aspects, such as calibration, sampling, EM environment and array structure, effecting measurement results are discussed.

## 1. Introduction

Today the spectrum of adaptive antenna applications is wide-spread, regarding both

military and civilian fields. Antenna arrays are utilized in RADAR and SONAR techniques, they offer significant capacity growth in 3G mobile telecommunication systems and are present on many other fields too. The main applications of antenna arrays are: direction-finding, beam-forming and angular filtering. In the case of direction finding so called adaptive algorithms were developed to increase the performance of the measurement. These techniques can be investigated with our 16-channel antenna system .

## 2. Direction estimation theory

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

First we specify an n-element antenna structure, then we measure the nxn correlation matrix R of the structure.

$$\hat{R} = \frac{1}{M}\sum_{i=1}^{M} Z_i * Z_i^{H}$$

The estimated correlation matrix is: , where Zi contains the i-th measured complex field strength values of the antenna elements, M times measured.

$R = E\{ \hat{R} \}$

Then, we calculate the estimated far-field power distribution by a function with scanning vector S and the estimated correlation matrix $\hat{R}$ , depending on the estimation method. The elements of S depend on the presumed angle of incidence and the geometrical structure of the antenna array .

The non-adaptive Fourier-method, also called Bartlett-method, only uses the simple Fourier-relation mentioned above to estimate the far-field EM power distribution, however, adaptive methods go further in signal processing utilizing different techniques to achieve better performance of the estimation. That is, lower sidelobe-level and sharper main lobes. We particularly focused on the method of Capon and on the MEM method.

The importance of sinusoidal signals from the aspect of data processing is that they can easily be converted into In-phase, and Quadratic components (I-Q) using a reference signal, thereby, creating complex numbers of these signals for further processing is easy.

## 3. Hardware description

In this chapter a brief overview of our measuring system is presented. In figure 3.1. the system block diagram can be seen.

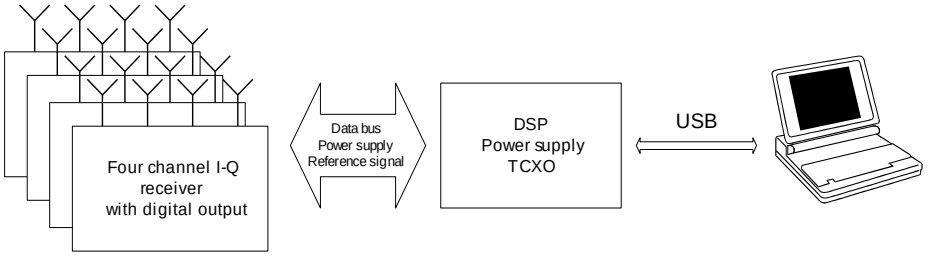



Figure 3.1.: System block diagram

Our measurement system contains three major parts. The four receiver blocks, the DSP unit and the measuring software running on a laptop computer.

The four receiver units with overall 16 input channels operate at 4.5GHz center frequency, after double conversion baseband I-Q signals are sampled and converted to 12bit data. The DSP can provide sampling numbers the powers of 2 (1, 2, 4,…,256). The receiver antennas are circular-polarized microstrip patch antennas. Those antennas are directional elements so we placed them at 2/3 wavelength. This distance gives us about 90 degrees grating-lobe free angular measuring interval in both dimensions. It is also an advantage of this situation that in those directions where grating-lobes are significant the sensor antennas have less sensitivity. The antennas are circular-polarized because our target has a linear-polarized radiator and it can have any position while it moves in azimuth or elevation plane. The receivers are independent, therefore, synchronization is needed and realized by an external frequency reference. The most important issue is to take the samples of the receiver signals simultaneously. Like taking a photo we must capture the amplitude and phase of the signals at the aperture of the antenna array at the same time instance. The proper timing is made by the digital signal processor module. The captured digital samples are fed into the DSP. Our DSP is a 320 MIPS dual-core processor which makes the sampling timing, data shaping and it can also calculate the correlation matrix. The power supply and the

frequency reference are also placed in the DSP unit. The computed correlation matrix is sent to a signal processing software via USB connection. This high speed interface can achieve up to 8Mb/s data speed which is enough to transfer the unprocessed data of the 32 digital channels for more flexibility when DSP processing is bypassed and more signal processing functions are made by the computer software. That software runs under LabVIEW environment and it does the compensation of the array, the direction estimation and it also has a simulation module.

In figure 3.2. the photograph of the measuring hardware can be seen.

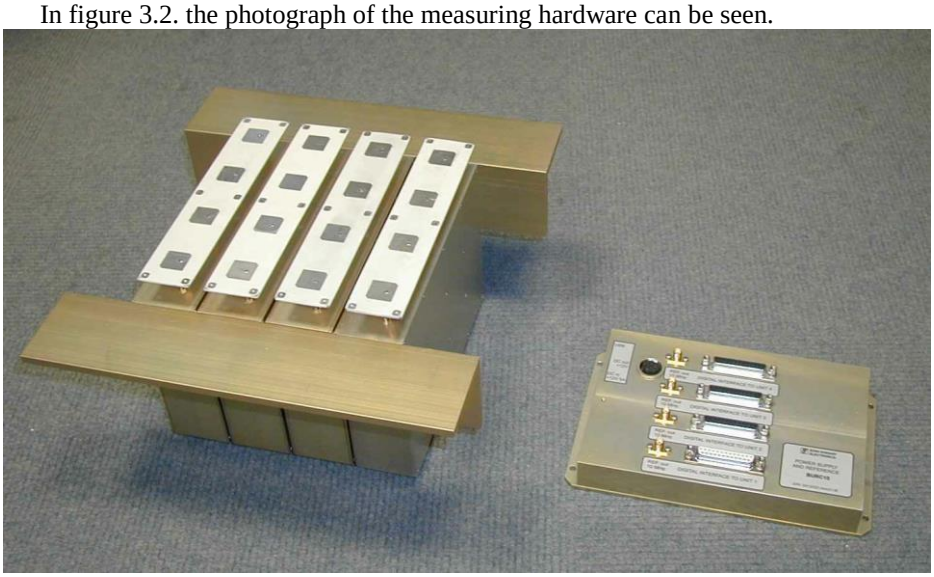


Figure 3.2.: Photograph of the hardware

### 3.1. Phase and amplitude errors of I-Q channels, calibration and compensation

In the following section we try to show the importance and method of basic array calibration and compensation for an improved accuracy of the direction estimation.

Such a receiver system like ours which contains multiple numbers of downconverters the matching of these receivers is a critical issue. The improper phase and amplitude alignment of the outputs causes severe degradation of the efficiency and accuracy of direction estimation algorithms. In case of some tens degrees phase and several decibels amplitude mismatch can cause a practically useless result. In figure 3.3. the spatial spectrum of an uncompensated system with only one signal source at zero degrees in both dimensions is shown on the left. To maintain a good performance of direction estimation methods we need phase matching below one degree and amplitude equalization below one decibel. The problem is that such a multi-receiver system can not be produced with such a tight tolerance at a high frequency of 4.5GHz. The used semiconductors, PCBs, discreet devices have larger tolerance in their parameters and even if we carefully select pieces with very close parameters, it is not guaranteed that the parameters of the complete receivers will also be close to each other. The dependency of the receiver parameters of the environmental variables is also an important matter. The most influential is the temperature and moisture, these

environmental parameters have strong effect on the system performance. The matching of the receiver hardware against manufacturing variance, temperature dependency, component aging needs special design techniques, careful production and component selection which in overall is a very expensive process. Another technique, which is worthy for consideration, is the software compensation. In this process the hardware is untouched, we can use this method theoretically in case of large amplitude and phase mismatch, practically for several tens degrees of phase and several decibels of amplitude errors can be handled easily and have great effect on array performance.

In this process we calibrate the array with a known signal and we determine the difference between the expected and the real response of the system, finally we correct the output signals with the inverse of the difference.

The calibration can be automatic, supported by built-in hardware and can be semi-automatic. Automatic process needs also precise matched hardware so we chose the semi-automatic way. In that case we inject a known signal into the receivers, practically an equal amplitude and phase excitation at each receiver input. That could be done by direct feeding the receivers without antennas through a power splitter network. This network can be matched better because it has a simple structure than a receiver. However, with this method we can not measure the mismatch caused by the antennas, only the receivers can be tested. Another solution is possible by generating a plane wave at the antenna array. This is a better method because we can determine the total system response easily. The problem is that we need a single path propagation signal for a proper result. Multipath propagation ruins the efficiency of this technique therefore we need to do this calibration in a special reflection-free room. This is a bad news. The good news is that we do not have to make such a calibration before every measurement, only after a change in the system or in the environmental parameters. For example if the system is built together and fixed we can calibrate it in a laboratory on different temperature and moisture levels and we can store the calibration data in files. When we obtained those data we can recall them anytime and make the software compensation. There is another interesting issue of the compensation. Antenna elements placed near together affect each other by disturbing the electromagnetic field of the nearby sensors. This phenomenon is called mutual coupling. Typically the magnitude of the coupling is below -15dB, in some cases it is about -30dB. Maybe it seems non-significant but we want to examine the effect of this mutual coupling on direction estimation and give a compensation for this case, too.

In the followings our phase compensation method is discussed. The measurements were done in a mode where the digital unit gives the estimated correlation matrix $\hat{R}$, to the LabVIEW software for further processing. Due to the non-equal phase shifting and amplification of the I-Q channels this matrix is not calibration-error free. To obtain the calibration-error free matrix $\hat{R}$, as mentioned above, software compensation was necessary to measure radio direction with the appropriate accuracy . If the k-th measured vector is:

zk’ = [ (r01+r1k)ej(φ 01+φ 1k) … (r0i+ rik)ej(φ 0i+φ ik)… (r0n+ rnk)ej(φ 0n+φ nk) ],

where r0i is the static amplitude error and φ0i is the static phase error of channel i, and

rik and φik are the actual amplitudes and phases of the incoming EM wave,

then:

Rk’ = [(r0i+ rik)ej(φ 0i+φ ik) (r0j+ rjk)e-j(φ 0j+φ jk)]i,j and

$$\hat{R}' = \frac{1}{M}\sum_{k=1}^{M} z'_k * z'^{H}_k = \frac{1}{M}\sum_{k=1}^{M} R'_k$$

If

zk = [ r1kejφ 1k … rikejφ ik… rnkejφ nk ], then

$$\hat{R} = \frac{1}{M}\sum_{k=1}^{M} z_k * z_k^{H} = \frac{1}{M}\sum_{k=1}^{M} R_k$$

Rk = [rikejφ ik rjke-jφ jk]i,j and .

Since the system has minor amplitude errors, those could be neglected.

These yield the following compensation matrix:

F = [ e-j(φ 0i-φ 0j) ]i,j , which must be element-by-element multiplied with the measured matrix $\hat{R}$’ to obtain the calibration-error free matrix $\hat{R}$ .

Matrix F is obtained by measuring with one single source placed at the desired 0° elevation and azimuth angles and element-by-element dividing it with the absolute value matrix of itself. In figure 3.3. the measurement results of a source placed at 0° elevation (Theta) and azimuth (Phi) angle, measured with the 4x4 array, calculated with the Bartlett-method are shown. The software-compensated case is shown on the right, compared to the uncompensated case on the left, in the same scenario. Notice the importance of phase compensation of I-Q channels on figures.

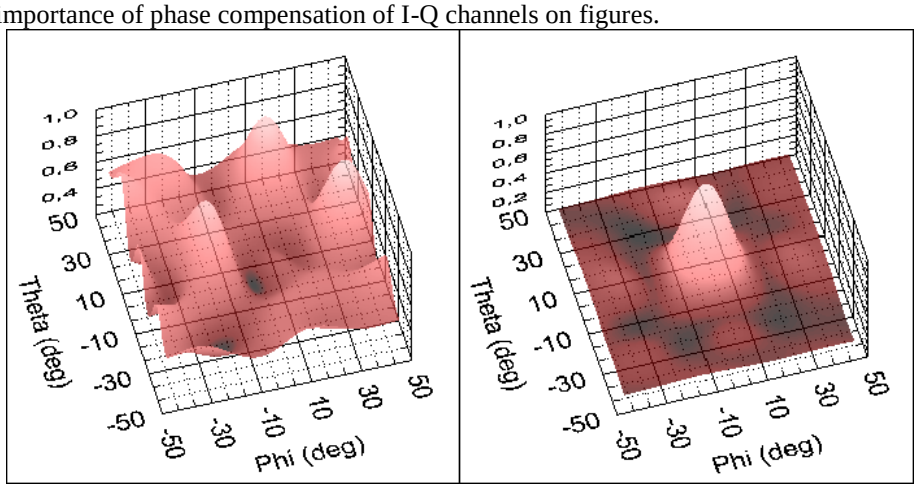



Figure 3.3.

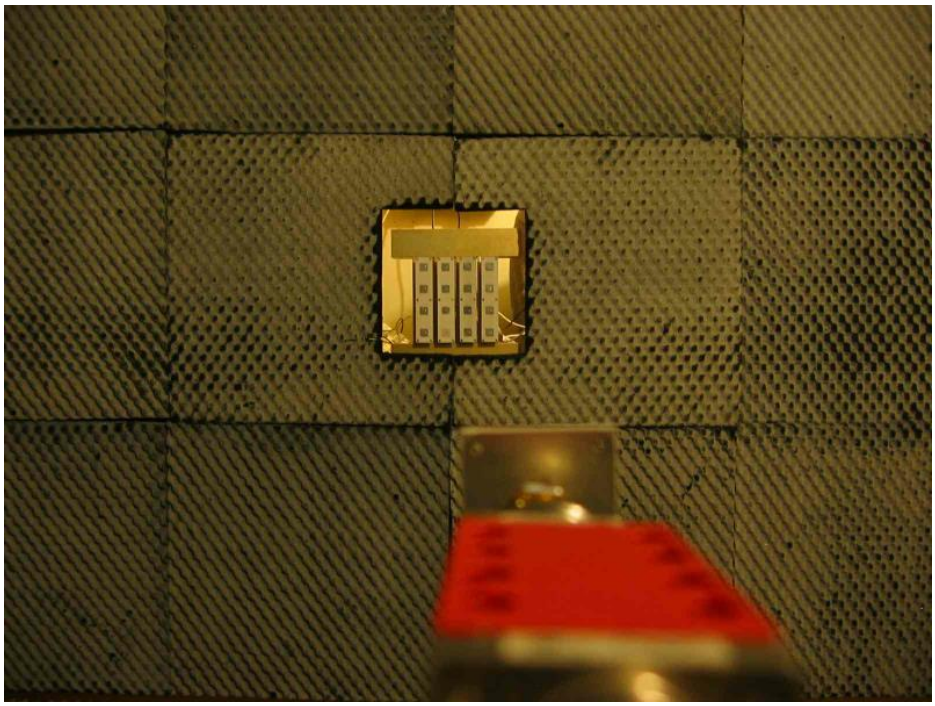


Figure 3.4.: Measurement

**4. Measurement results**

In the following section measurement results are presented, obtained by using our 4,5GHz 16-channel I-Q receiver system. Our measurements were conducted in a specially designed shielded room, equipped with energy absorbers. The scenario can be seen above in Figure 4. We applied the maximum applicable received amplitude by using the appropriate attenuators at the source in order to maximize the Signal-to-Noise-Ratio. The upper limit of the amplitude was set by the I-Q channels, higher amplitudes would have caused signal distortions. The sampling time was 1 ms. The measurement results show the relative estimated angular power distributions, where Theta is the elevation angle and Phi is the azimuth angle in a spherical coordinate system.

**4.1. Sampling dependency**

Adaptive algorithms desire multiple sampling, in order to work efficiently. As the number of samples taken increases, the scattering of the measured estimated correlation matrix $\hat{R}$ decreases. The less scattering causes the better efficiency of adaptive direction estimation algorithms .

To demonstrate the above, measurement results for a 4x4 antenna array arrangement are presented below in Figures 4.1. and 4.2., where the measured relative power distributions of a source placed at 0° azimuth and elevation angle are shown. In Figure 4.1. calculated with the non-adaptive Bartlett-method and in Figure 4.2. with

the adaptive Capon-method, first, measured with 4 samples (on the left), then with 256 samples (on the right).

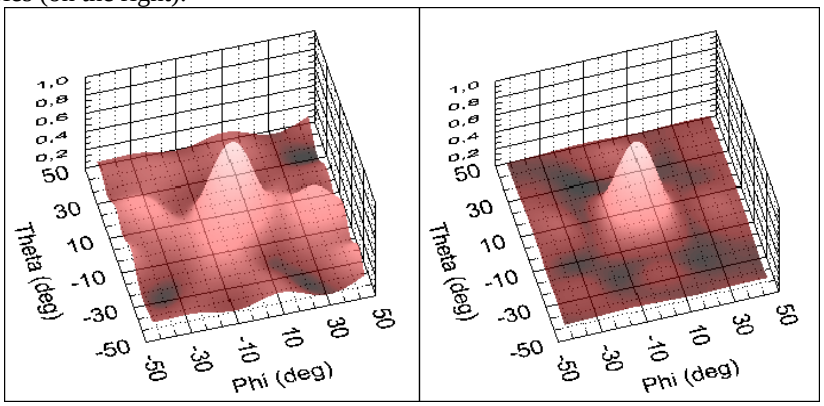



Figure 4.1.: Results, calculated with the Bartlett-method

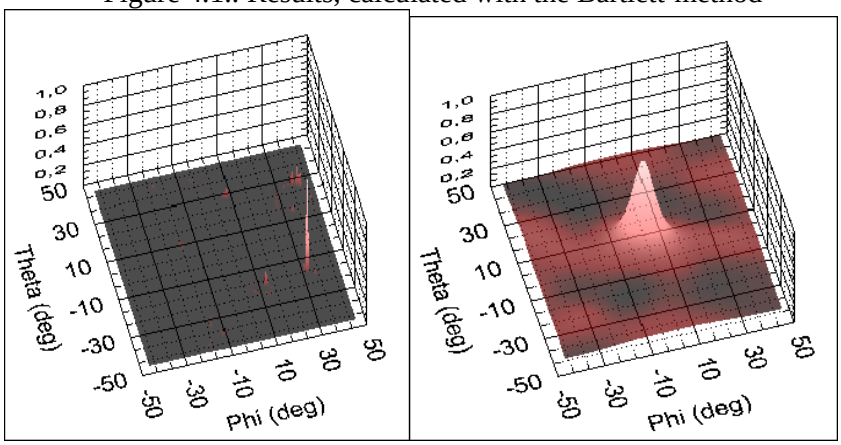



Figure 4.2.: Results, calculated with the Capon-method

We can see that if we do not provide a high number of sampling the adaptive Capon-method crashes, and so does MEM and LP, while the Bartlett-method, even if distorted, still provides usable results. We got the first usable results with Capon sampling 32 times and with the MEM sampling 128 times. As a result, during our further measurements we used the maximum achievable 256 sampling number.

### 4.2. The effect of multiple correlated sources on direction estimation

Two signals are called fully correlated or coherent when those are delayed and scaled versions of each other. If two or more such fully or partially coherent signals arrive at the antenna array the performance of the adaptive direction estimation methods is severely reduced. In that case the correlation matrix might be ill conditioned and can not be inverted, which is a great problem for example in the case of the Capon-method, which uses the inverted correlation matrix. This phenomenon occurs for example in the case of multipath propagation. Additive white noise coming

from thermal noise and high bandwidth of the target signal reduces the effect of coherency. There are several methods to cancel the effects of multiple correlated incident sources, two of them are introduced here.

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

Spatial averaging: this method divides the antenna array into multiple, overlapping sub-arrays with equal element-number. Due to the less sensor elements in one sub-array the maximal number of signal sources distinguishable by the system is decreased, we lose degrees of freedom, whereas, this method does not cause stationary measurement errors. In Figure 4.3. and 4.4. two sub-array structures can be seen .

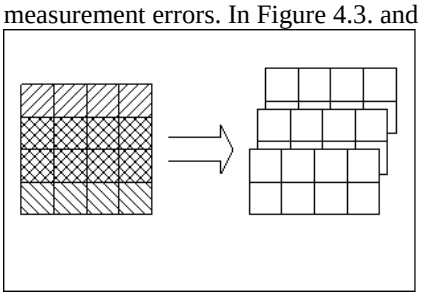


Figure 4.3.: Sub-array arrangement

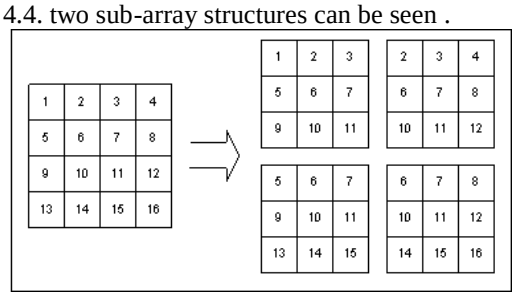



Figure 4.4.: Sub-array arrangement

Generally, it can be said that the number of separable sources in one dimension, azimuth or elevation, depends on the number antenna elements in one row. The structure in Figure 4.3. can handle more targets and gives better resolution in the azimuth plane and worse in the elevation plane. Figure 4.4. shows a uniformly good arrangement for both planes. The resultant correlation matrix, from which we calculate the final results, in this case, is the average of the correlation matrices of the sub-arrays.

The correlation matrix of the k-th sub-array, where xk is the vector of the signals of the sub-array elements:

$$R_k = E[\underline{x}_k \underline{x}_k{}^H] .$$

The estimation of matrix $R_k$ ,calculated from M pieces of samples:

$$\hat{R}_k = \frac{1}{M}\sum_{m=1}^{M} x_{km} x_{km}{}^* .$$

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

$$\hat{R} = \frac{1}{K}\sum_{k=1}^{K} w_k \hat{R}_k .$$

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

Even though the shielded room we took the measurements in had energy absorbers, there were still reflections present of our radio source, which caused the crash of the adaptive algorithms we used (Capon, MEM and LP). Therefore, we had to implement the above described spatial averaging algorithms to cancel the effects of multiple coherent incident signals.

In the following figures we can see the results for a source placed at -20° elevation and azimuth angle, calculated with the Bartlett-method (on the left) and the Capon-method (on the right). In Figure 4.5. the results calculated without spatial averaging and in Figure 4.6. the results using the redundancy averaging method can be seen.

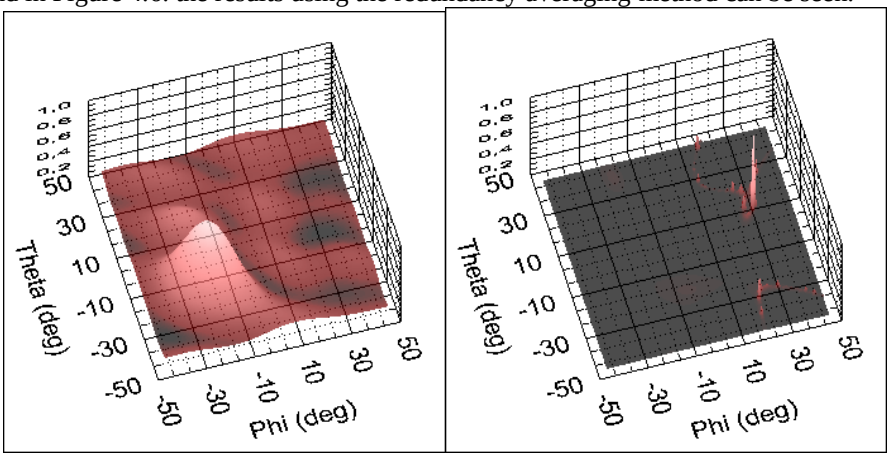



Figure 4.5.: Bartlett and Capon without redundancy averaging

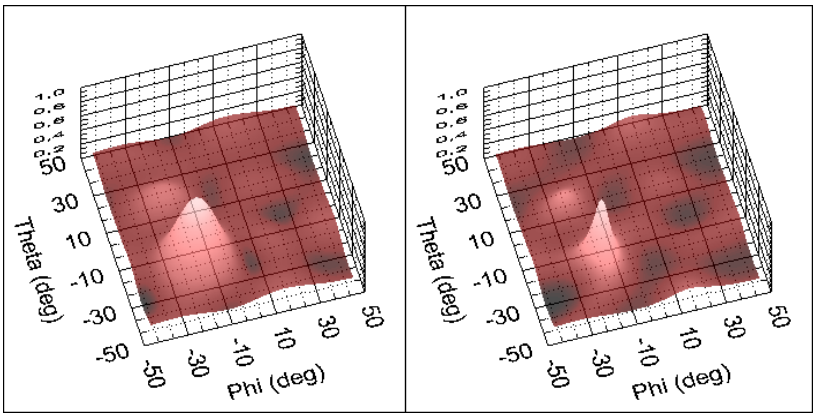



Figure 4.6.: Bartlett and Capon with redundancy averaging

In the first case, the Bartlett-method measured the angular position of the source correctly at ±1° accuracy, however, the adaptive Capon-method crashed.

In the second case, both methods worked, however, as expected, the measured angular position of the source shifted with 3° in azimuth towards the origin, while in elevation the shift was less than 1° .

However, in most of the cases total redundancy averaging was effective, in some cases averaging only the main diagonal of matrix $\hat{R}$ proved effective. An example for that can be seen below in Figure 4.7., where the angular position of a source at -30° elevation and 30° azimuth angles is estimated. First, calculated with the Bartlett-method, then with the Capon-method, averaging all diagonals of matrix R, and finally averaging only the main diagonal.

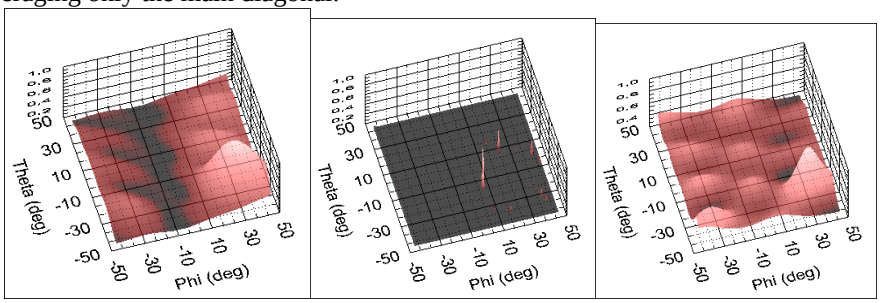



Figure 4.7.

Utilizing correlation canceling algorithms combined could lead to more effective direction estimation when multiple coherent sources are present.

### 4.3. The effect of the antenna array arrangement on the measurements

#### 4.3.1. Horizontally wide structure

We have also conducted measurements with antenna arrays other than a uniformly shaped 4x4 array. Here we present the measurement results of a source located at 30° in elevation and

-15° in azimuth, measured with a horizontally wide 2x4 array structure .

In Figure 4.8. the measurement results with the Bartlett-method, with the Capon-method and with the MEM method can be seen, in case of the last two using single diagonal averaging.

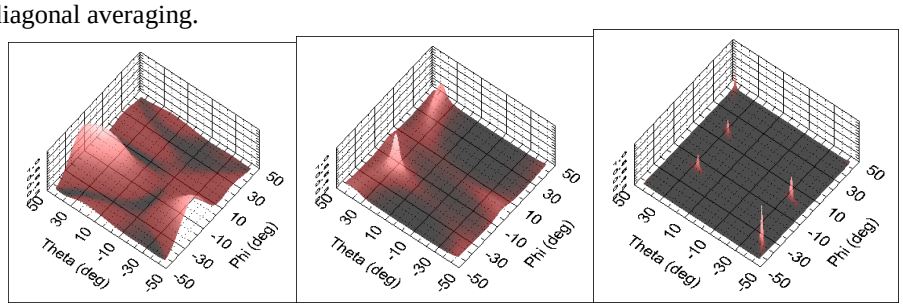



Figure 4.8.

The Bartlett-method estimated 35° in elevation and -13° in azimuth. The Capon-method estimated 27° in elevation and -18° in azimuth, the shift due to the averaging. MEM estimated a peak close to the real position of the source at 26° in elevation and -

16° in azimuth, the shift due also to the averaging, whereas, the highest peak this method estimated was not near the real position of the source. This is a property of the MEM method, which makes it hard to be utilized alone or as the main direction estimation algorithm in a system. Combined with the Bartlett-method the direction estimation can become quite effective .

### 4.3.2. Rare element structures

Rare element arrays are arrays that have the same frame as full arrays, with the difference that not all antenna elements are present in the antenna matrix. A special class of these arrays is called MRA (Minimum Redundancy Arrangement) arrays. The benefit of these arrays is that due to the same frame they have with full arrays, they possess approximately the same main lobe width as full arrays. The drawback of these arrays is that due to the absence of some elements the PSL of the structure will decrease. In the case of adaptive algorithms this degradation does not appear intensively.

Figure 4.10. shows the measurement results, calculated with different direction estimation methods for the structure shown in Figure 4.9., where the switches switched up represent the antennae that are present during the measurement. The down-switched ones represent the inactive ones. The source was located at 0° azimuth and elevation angle.

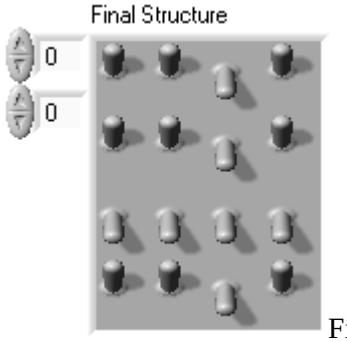



Figure 4.9.

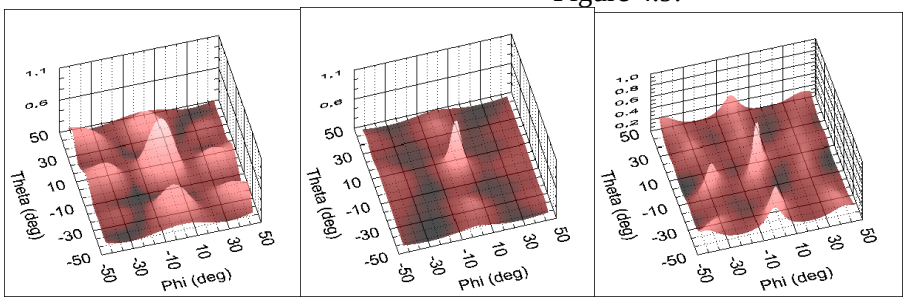



Figure 4.10.: Measurement results of the rare element structure, calculated with the Bartlett-, with the Capon- and with the MEM-method

It can be seen as the sidelobes rise measured with the Bartlett-method, compared to the results shown in Figure 4.1. that are calculated with 256 sampling. The omitted elements slightly change the sidelobe-structure of the results measured with the

Capon-method. The results measured with the MEM method show the same characteristics as in the case of the full 4x4 array.

## 5. Open field measurements

Open field measurements were also conducted in order to measure the angular position of a SLAR antenna, carried by a helicopter. The system was equipped with a camera as well, which followed the helicopter according to the angular information the antenna sytem provided. Photos of the measurement can be seen below.



Figure 5.1.: Open field measurement

The console-mounted container of the helicopter contained the SLAR hardware electronics as well as the signal source our system was tracking. In the picture at the lower left corner of figure 5.1 the direction measurement system can be seen. After a calibration procedure the helicopter took-off and the measurement started. The helicopter made several manoeuvre above the airfield and beyond that. Its tangential velocity and its distance varied over a large range. The azimuth and elevation angle of the helicopter was measured and very good results were obtained. Measurement results were checked by an optical azimuth and elevation measuring binocular with digital readout. The accuracy of the measurement depended on the velocity and distance of the target. When it was near and moved quickly the time delay of the signal processing and field sampling of the antenna system caused relative high uncertainty and quasi-stationarity problems. This uncertainty was in the range of the optical direction measurement accuracy, it was about 3 degrees plus-minus in average. The results were obtained by the Bartlett method. When the helicopter moved farther its displacement in angular dimension was lower, better results were obtained. In this case

an accuracy of 1 degree plus-minus was achieved. The effective detection radius of the measurement was about 30 kilometers. In that case the signal of the target suffered heavy fading and the average signal-to-noise ratio was about 6dB after averaging 128 samples.

## 6. Conclusion

We have created a radio direction measurement antenna system of a 16 channel, configurable I-Q receiver unit and its data processing units, which is capable of estimating radio directions at 4500MHz, utilizing adaptive direction estimation algorithms. We have conducted several measurements, which justified the previous simulation results. We have observed several aspects of radio direction estimation, regarding the effects of sampling, the coherency of multiple incident EM waves and the structure of the antenna array on the performance of different direction estimation techniques .

We implemented redundancy averaging algorithms to improve the performance and reliability of adaptive direction estimation algorithms in case of multiple coherent EM waves incident on the antenna array. It proved efficient in the case of adaptive algorithms we used (Capon, MEM and LP), the conventional Fourier-method was not sensitive to the coherency of multiple incident EM waves. We have investigated the matter of compensation techniques. The importance of software compensation was indicated.

We are planning to implement the technique of Spatial Averaging, used to decrease the negative effect of multiple correlated sources on direction estimation also, and prove the efficiency of it in real measuring scenarios. The practical question about this algorithm is: what is the optimal weighing (wk) of sub-array matrices in a given measurement scenario and exists or not a globally optimal combination for all cases? We will make observations in this matter. Other methods, based on time-domain signal processing are also to be investigated. We wish to thank for the cooperation to Bonn Hungary Electronics Ltd. and Technology Agency of the Hungarian Defence Ministry.

## References

[1] Alfonso Farina: Antenna-Based Signal Processing Techniques for Radar Systems, Artech House, Norwood, 1992.

[2] John Litva, Titus Kwok-Yeung Lo: Digital beamforming in wireless communications, Artech House Publishers, 1996.

[3] Darel A. Linebarger, Don H. Johnson: The Effect of Spatial Averaging on Spatial Correlation Matrices in the Presence of Coherent Signals, IEEE Transactions on Acoustics, Speech and Signal Processing. Vol. 38. No. 5. May, 1990.

[4] A. Manikas: Evaluation of Superresolution Array-Techniques as applied to Coherent Sources, International Journal of Electronics: 22nd September 1997.

**Sándor MUNK**

# INTEROPERABILITY INFRASTRUCTURE IN MILITARY INFOCOMMUNICATION SYSTEMS

## A possible extension of the interpretation of communication

Communication in the broader sense is transmission, receipt, or exchange of information, values, behavioral, or mental patterns224, according to the most accepted interpretation information transfer according to agreed conventions225, and in a narrower sense conveyance of information of any kind from one person or place to another except by direct unassisted conversation or correspondence226. In communication context information is the intelligence and knowledge capable of being represented in forms suitable for communication, storage, or processing227. Representation is possible by signs, symbols, pictures or sounds.

Information transmitted during communication is first of all facts, ideas, or instructions, that are exchanged between the parties mainly, but not exclusively during and to support collaboration, and cooperation. According to the parties in communication human, biological, social, and technical communication. In the following we will discuss only questions of human communication, especially assisted with technical, namely communication systems.

In the process of communication the sender itself or with the help of the appropriate device (terminal) transforms the information in the usual or agreed way into the format (representation) accepted by the communication system. The communication system – with intermediary transformations if necessary – transmits this representation to the receiver, who itself or with the help of the appropriate device (terminal) transforms it back to the original format, and then exploits, interprets, and build into its knowledge. Information can be transmitted using beacons, flag-signals, semaphore-signals, Morse signals, telephones, telex-, fax-, radio-devices, videoconference systems, or data-transmission devices.

As it can be seen from we said previously, communication systems in essence transmit not information (facts, ideas, instructions, etc.), but representations carrying information. Among others these can be traditional information representations, such as voice, speech, text, picture, and different data-like representations. Previously different representation were transmitted by special devices (terminals) and special networks (telephone, telex, etc.) connecting these devices. In our days special user devices have remained, but transport systems have become into integrated services networks.

---

[224] Pedagogical Lexicon (Pedagógiai lexikon), p 260.

[225] AAP-31(A), NATO Glossary of Communication and Information Terms and Definitions. – communication.

[226] AAP-31(A), NATO Glossary of Communication and Information Terms and Definitions. – communications.

[227] AAP-31(A), NATO Glossary of Communication and Information Terms and Definitions. – information [1].

Due to the integration of transport systems, during transmission the number of transformations between different information representations – done transparently for parties involved in communication – has increased. A sheet of paper with text on it is transformed into a digital (raster) picture in a fax device; afterwards this picture is transformed into an audio-frequency signal sequence by a modem. Transport network transforms these signals into digital format (bit sequence), and transmits it as data packages, and on the other side of the transmission link the transformations are also done in opposite direction.

In the last decades of the XX. Century, in addition to the technical devices assisted direct communication, previously almost exclusively between people, indirect information-, and data transmission – between persons, and IT systems, and between IT systems – has appeared, and continuously received an ever-growing importance. In IT systems information is handled (stored, created, and processed) in the form of appropriate internal representations. After all data transmission, or exchange between IT systems is indirectly also an information transmission between people (realized with intermediate storage of information), since data handled by IT systems represents, stands for information of primary user community of these systems.

So basic purpose of communication is the transmission of information representation – independently of its contents, the information carried – taken over on an appropriate communication end-point (terminal, interface), to an other designated communication end-point within user defined time limits, with given reliability, protection, and with well-defined quality of service (QoS) parameters, and there to put it in the original form at the receiver's disposal.

ꕥ

Changes in, and extension of user requirements, development, continuously growing application of information technology, infocommunication, and the consequences of the wide application more and more require the reconsideration of the concept, content, and tasks of communication, and the extension of its interpretation. In consequence of extended interpretation, functions earlier implemented by users of communication systems, or by their systems, devices are transferred to communication systems, and from the point of view of users become infrastructure services.

Extension of concept, content of communication is strongly connected to the concept, and interpretation of information. Among many definitions of information a definition related to human consciousness, recognition, and understanding and based on the concept of meaning plays significant role. According to this approach human knowledge is a reflection, mental representation of the world, the environment in the human mind, and information is a reflection, mental representation of a particular aspect of the world, a piece of knowledge in the human mind. In other words information is knowledge concerning objects, such as facts, events, things, processes or ideas including concepts, that within a certain context has a particular meaning.228

So communication can be interpreted not only as transmission of representations carrying information, but as a reliable, protected, assured quality transmission of information content, meaning. In this case a communication system

[228] AAP-31(A), NATO Glossary of Communication and Information Terms and Definitions. – information [2].

has to transmit the information representation received from the sender not by all means in an unaltered, identical format, but in such a format, that after interpreted by the receiver results in the same – or at least similar enough to successful cooperation – information as the sender wanted to transmit.

This extended interpretation makes the meaning-preserving transformations of the information representations transmitted part of the communication process, task of the communication system. Such transformations are needed, or could be needed, if there are differences between communicating parties in external representations of the same "information", the mental representations about the same piece of the environment. In case of such differences, heterogeneities every actor naturally wants to send its information, and receive information of other actors in its usual, used, known format.

Questions of meaning-preserving transformations between different interpretations, representations during information transfer, information exchange belong to research field of information interoperability, and interoperability of IT systems. Up to the present discussion of these questions, development and implementation of content-oriented, semantical interoperability solutions were practically beyond of interest of communication. However in our days extension of functions of communication systems, and networks come to the front in other areas too.

So called intelligent, or application oriented networks[229] increase the role of infrastructure in the support of communication in broader sense, and collaboration. In possession of a detailed, content-oriented knowledge of information to transmit, infocommunication infrastructure, the network can play an active role in the implementation of applications, and services. In addition to extended support of applications intelligent networks can more efficiently implement the required quality, prioritized transmission, and protection of information, or the monitoring of information traffic.

From user point of view benefits of extended interpretation of communication, and extensions of functions and capabilities of infocommunication infrastructure can not be questioned. The new capabilities could do unnecessary, that communicating parties, and their IT systems, and devices should have to adapt to actual possibilities of the communication system, and to the specific characteristics of their partners. Instead the infocommunication infrastructure should adapt, adjust itself to communicating parties, and should hide – to the possible degree – the specific characteristics of the communication system, and partners from them.

An infocommunication system including interoperability functions could make possible, that one actor describes a length in miles (feet, etc.), and an other receives it in meters; one actor gives a date according to Mohammedan (Jewish, Chinese, etc.) calendar, and the other receives it as a Gregorian date; one actor gives the position of a bridge in World Geodetic System 84 (Gauss-Krueger, etc.) coordinate system, and the other receives it in UTM system; one actor sends an aerial picture in GIF (TIF, BMP, etc.) format, and the other receives it in JPG format; one actor sends a

[229] Intelligent Networking (Intelligent Information Network), Application-Oriented Networking (Application Aware Network).

formatized message in an ADatP-3 type MTF format, and the other receives it in XML format; or even one actor sends a text in Hungarian, and the other receives it in English. In order to realize these transformations infocommunication systems need to have information about the communicating parties, and information transmitted between them. These pieces of metainformation describe the environment, context that is used in and necessary for the appropriate interpretation of information (messages).

In case of traditional communication systems lack of information interoperability functions did not raise problems first of all because differences between points of view, interpretations, representations of communicating parties were solved by actors themselves, by people with appropriate knowledge. They were who made the necessary transformations during preparation, and receipt of information between their internal representation, and the intermediary representation used in transmission. However for this there were necessary information activities that essentially do not belong to information exchange and realization of these activities requires special knowledge, additional time, and involves possibility of errors.

Significance, and at the same time, necessity of new infrastructural interoperability functions especially increases in consequence of the wide spread of "communication", data exchange between IT systems, and devices. In case of this type of communication there is no, or is only a very limited possibility to realize the transformations between different points of view, representations, contexts, without human knowledge and participation. In consequence of this now interoperability functions are built in the given systems. Due to the extension of the volume of information exchange, and connections among systems, more and more identical, or similar interoperability subfunctionality is realized, and used in a lot of systems. The essence of different infrastructures is exactly the centralized, widely accessible implementation of basic functions, services used by a lot of users, that increases the accessibility, efficiency, economy of these functions, and services, helps their continuous extension, and development, and makes unnecessary their individual implementation.

Finally the necessity of the growing role of interoperability functions, and in consequence their infrastructural implementation is can be explained by the ever growing application of infocommunication services; appearance of worldwide networks connecting a lot of persons, and devices; extension of volume of connections between people, systems, and devices; and as a consequence the growth in the heterogeneity of parties involved in information exchange, in communication. This is because information exchange between heterogeneous actors requires a wider and wider application of interoperability solutions.

## Interoperability infrastructure and its characteristics

Basic components of communication process models used during theoretical analysis and practical implementation are communicating actors, and information handled by and flowing between them. Actors can be individual persons, organizational units, organizations, organizational systems, or mission-oriented operational elements (groupings). Information can exist in human mind, and in the form of traditional or IT representations.

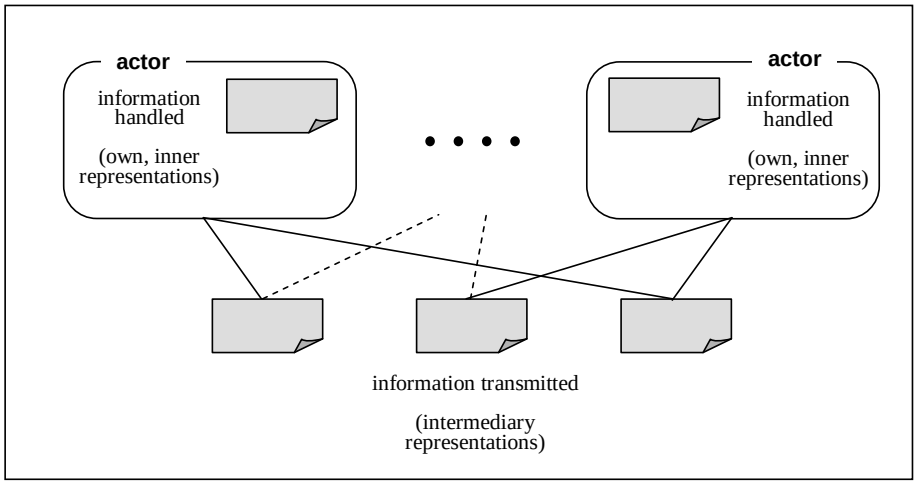



Figure 1: Model of communication from information point of view

Questions of information interoperability have significance during communication only if there are differences between communicating parties in concepts, information representations, or interpretations used. Since in case of actors "homogeneous" from information point of view intermediary representation used during communication obviously will the common representation used by all participants, in other words "all talk on the same, their mother language".

In a, from information point of view, heterogeneous environment for successful communication it is necessary to make transformations between different "points of view", different information of individual actors. So in this case basic components of a model of communication include descriptions of information handled by particular actors, and descriptions of intermediary representations (systems of concepts, ontologies, contexts, etc.), and necessary meaning-preserving transformations between individual representations.

Model of communication extended with interoperability components can be divided into the actors involved, and the infocommunication environment ensuring interoperable information transmission, information exchange. Information handled by actors, their inner representations, descriptions, transformations between inner, and intermediary representations, and IT systems, devices that handle, and process information belong to individual actors. Infocommunication environment contains intermediary representations used during transmission of information (information exchange), their descriptions, necessary transformations between different representations used during transmission, devices (systems) implementing these transformations, and communication system that transmits intermediary representations.

Individual actors are linked to the infocommunication environment at different connection points. These connection points can provide different services, different actors can be reached through them, and well-defined intermediary representations can be used. In accordance with this a given actor – depending on the content of communication, so depending on intermediary representation used, and

depending on the actors involved in communication – can connect to the infocommunication environment at different connection points.

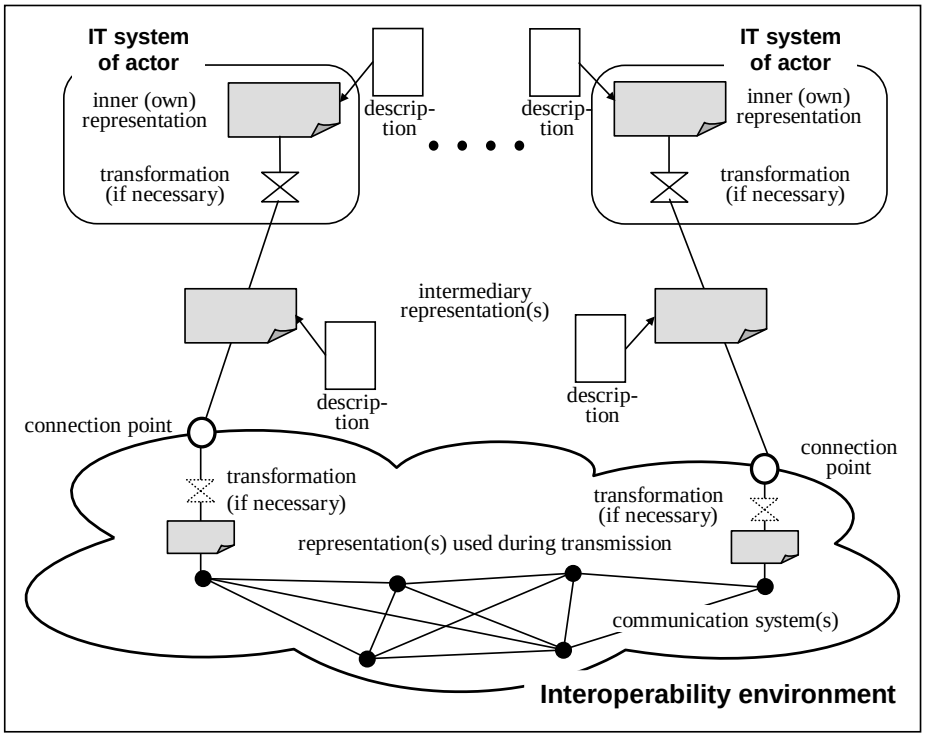



Figure 2: Model of communication extended with interoperability components

An interoperability component is such a (software and/or hardware) functional component of an IT system that purpose is to ensure the conditions of meaning-preserving information exchange between/among heterogeneous interpretation environments (contexts). Its main task is to transform an – elementary, or complex – information representation connected to a given interpretation environment into an other information representation linked to an other interpretation environment with total, or maximum possible preservation of meaning.

Different interoperability components can be classified according to the level of the implemented functionality, and to the type of the transformation. The task of the highest level interoperability components is meaning-preserving transformation of largest autonomous units (messages, documents, questions, answers, etc.) of information transmission, information exchange between actors of infosphere that have different interpretation rules (contexts). The task of the lowest (elementary) level interoperability components is transformation of a given representation of a single elementary information to an other representation with identical, or similar enough meaning. Concept of elementary information obviously can be interpreted differently in case of sensual and abstract information, and in regarding the latter in case of data

like in narrower sense, textual, or other document-like symbolic information. Finally the task of intermediate level interoperability components is the meaning-preserving transformation of often used complex information, information sets between different interpretation environments.

According to type of transformation format-oriented, or syntactical, and content-oriented, or semantical transformations can be differentiated, although the delimitation in some cases is not so unambiguous. In case of syntactical transformations basically there are no conceptual, and content-oriented differences between information carried by the two representations, the heterogeneity appears only in the format used. While semantical transformations are necessary when information carried by the two representations belong to different conceptual systems, interpretation environments.

Transformation of information representations between two different interpretation environments, contexts is usually a multilevel process containing several subtasks. Lower level(s) of transformation contain(s) syntactical transformation(s), while the upper level is the semantical transformation. So realization of transformation process can be partitioned into subtasks, that may be implemented by different interoperability components, "specialized" for a given interoperability task. Apart from simplest cases in the process of transformation usually different inner representations of the given component are used.

Different types of interoperability solutions, transformation require different expertise, different kinds of knowledge components. Creation of syntactical level representations, and implementation of syntactical level transformations require IT-specific, especially IT development knowledge. Data, and data structure formats used in particular IT systems are determined by the capabilities provided by available system software (compilers, database systems, etc.), by the specialties of information handled, and by efficiency requirements. These do not belong directly to the range of interest of IT systems' user community. Their implementation details should not be known by users, they have only content-oriented, and efficiency requirements.

On the other hand selection of semantical level representations, and definition of necessary transformations between them is almost fully a user's competence. Semantical representations mainly depend on user requirements, traditions, efficiency expectations of the given application area. Realization of transformation between semantical representations of identical, or similar information requires also application field knowledge. One part of semantical transformations is independent of particular application areas, and widely used in practice. Such are for example transformations between units of measurements, coordinate-, or calendar systems.

In practice those interoperability functions, components should be implemented at infrastructural level, as a communication system service, that are used by several communicating parties, and that implement well-defined, algorithmically stable transformations. First of all most of syntactical transformations, and the widely used semantical transformations mentioned below belong to this category.

ꕥ

Information interoperability infrastructure – belonging to an infocommunication system, and built on top of a traditional communication system – is a widely available unified system of personnel, devices and services that's purpose is

to ensure information exchange based on common understanding, between cooperating partners. Basic components of interoperability infrastructure are functional components that implement interoperable transformations.

Components of interoperability infrastructure were previously implemented as parts of IT systems, and applications, then they were separated as autonomous middleware components. Purpose of middleware applications is exactly the support of cooperation, information exchange between, integration of heterogeneous IT systems. In consequence these applications, application components are closer to infrastructural, mainly to communication services, than to supported IT systems, applications.

From the point of view of communication system, interoperability infrastructure is such a value-adder service layer, that works built on top of traditional communication service layers. Basic purpose of communication systems, networks instead of traditional information transmission nowadays is more and more support of integrated functioning of a given organization, community of cooperation as a unified entity. These systems, networks connect particular officials, and organizational units, and they should do this independently of the fact that "what language" the individual actors "speak", what representations they use during information exchange.

Implementation of interoperability infrastructure will probably according to service oriented architecture widely spreading nowadays. In this architecture different components implementing interoperable transformations appear as autonomous servi-ce-providers that can be used to build a complex transformation. This kind of implementation, in case of missing interoperability subfunctionality, makes possible to extend the infrastructure with application-side interoperability components, even to provide this functionality to other applications, and later to build into the infrastructure. All this ensures dynamic, application-requirement oriented extension of infrastructural services. At the same time service oriented architecture requires implementation of service-advertisement, -registering, -seeking, and task decomposition/subtask planning functionalities that should also be part of the interoperability infrastructure.

Several components of an interoperability infrastructure are already available in form of independent applications, operation system functions, or functions of system development, and run-time platforms230, only conditions of their wider availability should be ensured by placing their services at users' disposal in form of infrastructural services. Components providing interoperability services can be operated in linking nodes of the communication system (routers, gateways, switches, etc.), in autonomous infrastructural servers, or in application systems at their operation system, or middleware layers.

**Summary**

According to traditional understanding of communication it is built not on transmission of information, but on transmission of representations carrying information. So basic purpose of communication is the transmission of information

[230] For example document conversion (still and motion image conversion, audio conversion, textual document conversion, etc.) utilities, character set conversion functions, elementary data (e.g. numeric data) transformation functions.

representation – independently of its contents – taken over on an appropriate communication end-point, to an other designated communication end-point according to user requirements, and there to put it in the original form at the receiver's disposal.

Changes in, and extension of user requirements, development, continuously growing application of information technology, infocommunication, and the consequences of the wide application more and more require the reconsideration of the concept, content, and tasks of communication, and the extension of its interpretation. Communication can be interpreted as a reliable, protected, assured quality transmission of information content, meaning. In this case a communication system has to transmit the information representation received from the sender not by all means in an unaltered, identical format, but in such a format, that after interpreted by the receiver results in the same – or at least similar enough to successful cooperation – information as the sender wanted to transmit.

In consequence of extended interpretation, functions earlier implemented by users of communication systems, or by their systems, devices are transferred to communication systems, and from the point of view of users become infrastructure services. This makes the meaning-preserving transformations of the information representations transmitted part of the communication process, task of the communication system, that belongs to the research field of information interoperability, and interoperability of IT systems.

Significance, and at the same time, necessity of new infrastructural interoperability functions especially increases in consequence of the wide spread of "communication", data exchange between IT systems, and devices. Necessity of the growing role of interoperability functions, and in consequence their infrastructural implementation is can be explained by the ever growing application of infocommunication services, appearance of worldwide networks connecting a lot of persons, and devices.

Model of communication extended with interoperability components can be divided into the actors involved, and the infocommunication environment ensuring interoperable information transmission, information exchange. Information handled by actors, their inner representations, descriptions, transformations between inner, and intermediary representations, and IT systems, devices that handle, and process information belong to individual actors. Infocommunication environment contains intermediary representations used during transmission of information (information exchange), their descriptions, necessary transformations between different representations used during transmission, devices (systems) implementing these transformations, and communication system that transmits intermediary representations.

An interoperability component is such a (software and/or hardware) functional component that purpose is to ensure the conditions of meaning-preserving information exchange between/among heterogeneous interpretation environments (contexts). Its main task is to transform an – elementary, or complex – information representation connected to a given interpretation environment into an other information representation linked to an other interpretation environment with total, or maximum possible preservation of meaning. Transformation of information representations between two different interpretation environments, contexts is usually

a multilevel process containing several subtasks. Lower level(s) of transformation contain(s) syntactical transformation(s), while the upper level is the semantical transformation.

Information interoperability infrastructure – belonging to an infocommunication system, and built on top of a traditional communication system – is a widely available unified system of personnel, devices and services that's purpose is to ensure information exchange based on common understanding, between cooperating partners. Basic components of interoperability infrastructure are functional components that implement interoperable transformations. From the point of view of communication system, interoperability infrastructure is such a value-adder service layer, that works built on top of traditional communication service layers. Several components of an interoperability infrastructure are already available in different forms, only conditions of their wider availability should be ensured by placing their services at users' disposal in form of infrastructural services.

## References

[1] AAP-31(A), NATO Glossary of Communication and Information Systems Terms and Definitions. – NATO C3 Agency, 1998.

[2] Pedagógiai lexikon. I-III. kötet. – Keraban Könyvkiadó, Budapest, 1997.

**Erik PÁNDI**

# UNIFICATION OF THE HUNGARIAN GOVERNMENTAL COMMUNICATIONS SYSTEMS[231]

## 1. Description of the academic question

The technological convergence in the fields of telecommunication and information technology is the product of recent development of human civilization, the technical achievements, beneficiary effects and negative results affect our everyday life, while our communication habits are changing from the youngest generation to the oldest. For hundreds of years, government is one of the most specific elements of state existence, at the same time it is integrated into the society, in this way it is affected by the various achievements of the development of civilization, its activity is influence just like the single members of the society are affected. Due to the accelerated development of the electronic world, communications systems and information technology, governments are facing a new challenge, since the methods of exchanging data are so wide ranging, that the increase in the speed and volume of accessing information resulted a communication "boom".

The pushing force consists of multinational telecommunication and information technology companies operating in the global market and through the products bought it also contains the private- and civil sector, that is the individual persons all over the world; as through the developed communication and data processing systems, means and processes these can enforce indirectly the modernization of governmental activities, its changing into a supplier type one, taking into consideration, that the governments of the individual states became potential economic competitors. In the circumstances of the strict competition for the provision of abundance it is essential that the national government authorities improve their own communication facilities and the communication with the society, through which prosperity could be assisted.

A key to the development of abilities is a well organised and controlled government communication system, which is set up according to different the different practices and traditions by countries. Entering the European Union means at the same time, that Hungary has to co-operate in the programs aiming the improvement of the communication facilities of administration too, for which the field and statues of government telecommunication have to be surveyed and elaborated scholarly Hungarian governmental telecommunication has traditions coming from the middle of the last century, however, there are only a few publications in this topic, which are available – especially before 1990. The exact mapping of development processes and its operational mechanism, furthermore developing the effects on the environment are quite difficult for the lack of resource documents, there are still a lot of unknown gaps in its history. Practically, the topic can be considered "terra incognita", that is entirely

[231] Ltc. Erik Pándi, depute head of general department of Telecommunications Service of the MoI (and PhD-student of Telecommunications Department at Zrínyi Miklós National Defence University). This paper presents summary of author's PhD-dissertation

undeveloped, therefore the execution of the first survey was a very interesting academic and professional task.

## 2. Project aims

1. to process horizontally the history of Hungarian governmental communication, to determine and describe the main phases of development;
2. to analyse and evaluate the communication systems and capabilities of the organisations participating in the governmental communication process during the individual phases. To present a complex view of the legal, technical environment and the development tendencies in a certain period.
3. finally, to study in a nutshell the possibility and necessity of the integration of governmental communication, to give theoretic basis, organizational and control recommendation for the setting up of an integrated communication system.

## 3. Subject, scope, method and basis of research

1. Subjects of my research:
- Features, progress of the development phases;
- Legal environment determining the communication infrastructure of Hungary, its effect on governmental telecommunication;
- Features of the closed-purpose, mainly army and government communication systems and that of the systems connected to them;
- The necessity, methodology of integration.

2. Topics out of the scope of my research:
- Detailed analysis of the factors and technical features of the communication systems studied;
- Actual economic influence of integration, its human resources demands;

3. Fields of research upon working out the project:
- Legal requirements determining governmental communication;
- Improvement trend of public and closed-purpose communication systems;
- The effect of convergence on the improvements of communication and information systems;
- Conditions, alternatives of the development of a uniform system.

4. The method of project elaboration:
- I have studied and processed the available archive materials and the related academic studies, candidate, PhD and university doctorate essays;
- I have analysed and systematized the legal background of public and closedpurpose communication systems connected to government telecommunication;
- When studying the history of improvement I have deduced partial facts concerning the composition and features of government telecommunication systems of the certain periods;
- Based on the digested facts, partial conclusion and the discovered relations I have specified the development stages of government telecommunication, I have also confirmed the necessity of integration and gave theoretic recommendation for the method of setting up a uniform system.

5. Main base of research:

- Archive documents available in the Archives of the Ministry of the Interior, in the archives of the Telecommunication Service of the Ministry of the Interior;
- Regulations, doctorate, PhD and university studies, research books, publications, articles found in the academic, information and document library of Zrínyi Miklós National Defence University;
- Descriptions, regulations received from the Ministry of Defence, GS Communication and Information Group Directorate (Army Planning Main Group Directorate), the Ministry of the Interior, the Hungarian Police Headquarters and the National Border-Guards Headquarters;
- Materials of international and national professional conference lectures organised by Zrínyi Miklós National Defence University;
- International (EU, NATO) and national electronic data bases, electronic archives (CD-s, floppy discs);
- Academic publications available on Internet

## 4. Summary of the examinations executed

1. Governmental Decree No. 3343/1967. was the first document, which prescribed the development of a system supplying governmental communication demands. The system set up actually has only partly served the governmental communication function between August 1967 and 31 December 1989 (Phase I), as the safety requirements system used consequently in connection with „governmental communication" has continuously impeded the extension of those using communication services. In spite of the fact, that before 1990 the imports in Hungary were under strict control and limitation concerning modern Western technologies, both the army and provost communication systems furthermore the communication networks of the Hungarian Post underwent various communication network quality development progresses, due to the state safety limits beside low capacity government communication system, systems under the control of other organisations took also part in the technical actualization of governmental communication, in addition to the defence, home affairs, traffic and post portfolio.
2. This combined, multi-party solution was mainly explained by limited infrastructural facilities, however, it did not curtail the interests in governmental communication, as these remained enforceable for the dominance of state property and centralised state control practice given. In addition to the application of this method, between 1967 and 1989 each Government in duty considered important, that the development and control of technical and organisational structures serving state communication demands were handled by the government.
3. On the basis of the above it can be stated, that between 1967 and 1989 government telecommunication was not served by individual government communication system in Hungary. The demands of governmental organisations were supplied by the communication systems of various state administration and state authorities jointly, beside strong state co-ordination, where this model could be also considered an individual government system.
4. In the second phase, between 1 January 1990 – 8 January 2004 the Government still not dropped the possibility of controlling government telecommunication,

therefore the systems ensuring government communication were intended to be kept. The new legal regulation made possible increasing the number of closedpurpose telecommunication networks, thus individual development progresses could be started, taking into consideration sector interests. There were more organisations taking part in the realisation of government telecommunication on the state side than before, to which effort public companies also joined. Due to the changes in the economic structure, major part of the Hungarian communication infrastructure was privatised, resulting that the possibility of executing interests connected to government telecommunication was pushed into the background due to the marked conditions not liberalised, which fact was not compensated by the independence of state infrastructure ensured by legal regulations either.

5. The development concepts for the "replacement" of privatised participants were not realised because of the expected significant cost effects, however, the approach changed from the middle of the decade, as centralisation was aimed to impede prolific individual systems, on the other hand not only state infrastructure was intended to be used during the integration.
6. Electronic governance and the servicing state concept in the fields of government telecommunication intensified centralisation efforts and a professional central authority was also set up in the Prime Minister's Office. By the end of the second phase two large suppliers' centres the Electronics Governmental Main Network (EKG) and the Integrated Digital Trunked Radio-system (EDR) were established beside the existing closed-purpose networks.
7. It can be accounted for the definite effect of convergence, that during the organisation of its services the EKG emphasized remote and quick accessing of information, while the connection and co-operation (traditional telecommunication) between persons and organisations was only the second point of view.
8. Between 1 January 1990 and 8 January 2004 government telecommunication was still not supplied by an individually organised communication in Hungary. Demands were supplied by the communication systems of various state administration organisations and by the participants of the telecommunications market under liberalisation, beside state supervision and strengthening coordination state activity. Main feature of the period is that the entire Hungarian communication infrastructure undergoes modernisation, in parallel with which there is centralisation progress in the fields of government telecommunication.
9. The third phase in the development of governmental communication (from 9 January 2004) is still in progress. In the third (present) phase of the history of development the conditions are given for the setting up of an integrated governmental communication system according to the earlier strategic ideas, which would effectively assist governmental work and strengthen its service feature.
10. The realisation of common and national programs, the suppression of parallel development efforts can be ensured through strong central control in the hands of one network manager. The number of closed-purpose telecommunication

networks can be also optimised through integration, which was earlier described as a strategic concept.

11. The organisation of the integrated government communication systems shall be executed as controlled from the top, in more stages, during which the integration of systems will be executed at first in an administrative, organisational way. The setting up of a new system cannot be planned, rational integration of the existing components shall be executed instead. Upon the development of integration the position in the governmental system of the persons in charge for operation and maintenance, furthermore the governmental position, status of organisations established for ensuring information exchange between the different organisations and systems have to be specified in detail, and then further tasks concerning technical compatibility and co-operation, and of the operation of virtual networks shall be exactly specified.

## 5. Conclusions

In the essay I have tried to prepare the academic analysis of a topic, concerning which there are only a few resources to research both in quantity and quality, and which seems to be entirely undeveloped at present. The only points of reference were legal codes and external regulations.

In my essay I have analysed the earlier and the present status of Hungarian government telecommunication in three chapters. After giving the basic definitions to the topic I have described the organisations taking part in governmental telecommunication between August 1967 – 31 December 1989, I have introduced the main characteristics of their systems and the connection between them. I have established the lack of an integrated system, in parallel I have also presented the wide possibilities of governmental control of that period.

In Chapter Two, analysing the period between 1 January 1990 and 8 January 2004 I have reviewed and analysed the general effects of convergence on telecommunication and information technology, coming to conclusions concerning the expectable direction of national development. Taking into consideration the basic changes in legal circumstances and the effects of convergence I have examined in progress the complex organisational and technological development features of market characters participating in government telecommunication, which I extended to the relevant closed-purpose telecommunication networks as well.

I have discovered and elaborated for this period those concepts, which could be connected to the development of government telecommunication. At the same time I specified and described those main procedures, which basically impeded or could assist the setting up of the integrated system. I have certified, that at the end of the examined period the influence of the technological progress could assist the development of an integrated system also preferred by the Government.

In Chapter Three I have specified the phases of development. Based on the confirmed integration processes I have developed and introduced the applied organisational and controlling routines of the communication systems presently relevant to government telecommunication, and the technological platforms. Based on Chapter Two I have specified the common expectations and programs for the setting up of electronic government due to our entering the Union. Confirming the necessity of the development of an integrated government communication system, furthermore

the existence of beneficial legal-technical surrounding assisting integration, I have determined a possible legal base for the realisation, and recommended theoretic organisational and controlling routine in connection with the integrated communication system.

## 6. Recent academic achievements

1. I was the first to elaborate – applying academic methods – the history, determinant progress and participants of Hungarian governmental telecommunication between 1967-2004. Based on wide range analysis I have defined, that the history of Hungarian government telecommunication can be basically split into three separate phases;
2. I have confirmed, that based on the present closed-purpose telecommunication systems, by optimising the number of them a rational integration of communication systems participating in government telecommunication can be achieved and through this the integrated government communication system can be effectively established. I have recommended a form for the realisation of integration. I have elaborated the multistage solution of integration, in which I have fixed, that the integrated government communication system shall be set up centralised, basically controlled from the top; at first with administrative organisational procedures, later through the expedient combinations of the elements of the communication systems;
3. A part of my observations and my results published based on the academic elaboration of the project was integrated into the regulation system of the Ministry of the Interior.

## 7. Recommendation for further use of the essay

1. Literature for further studies in this topic;
2. For the undergoing centralisation efforts in the communication systems of the home affairs sector;
3. Using the study as recommended literature in the basic education of special studies at Zrínyi Miklós National Defence University.

**Zoltán RAJNAI, Beatrix FREGAN**

# NOUVELLES STRATEGIES DE TECHNOLOGIES ET ART DE LA GUERRE

Les technologies nouvelles sont susceptibles d'apporter un avantage décisif dans les conflits, mais en même temps, elles sont susceptibles d'être mises en défaut par des conditions d'environnement complètement inattendues, où le facteur humain tient un rôle essentiel.

## Les senseurs

C'est un domaine transverse et très vaste. La plupart des senseurs sont de nature électromagnétique, avec les radars mais aussi les senseurs optroniques, qui travaillent dans des gammes de fréquence très différentes (la lumière, l'infrarouge) et que l'on trouvera dans à peu près tous les systèmes qui seront évoqués par les intervenants. Il en existe d'autres, comme les vibrations, les senseurs biologiques, chimiques, etc. On voudrait donner rapidement quelques exemples de ruptures technologiques, de produits différents et de fonctions nouvelles que l'on peut réaliser à l'aide de technologies nouvelles. Un premier exemple est donné au niveau des composants. On évoquait tout à l'heure la détection infrarouge, qui a le mérite de permettre de voir la nuit, d'être passif, non détectable, et les détecteurs futurs non refroidis permettront d'abaisser les coûts, d'utiliser de façon plus autonome et d'augmenter la robustesse.

Un autre exemple concerne les capteurs qui permettent, en utilisant des principes nouveaux, d'avoir des informations nouvelles. C'est le cas notamment des sonars de la détection sous-marine. Le sonar mesure le bruit selon une variation de pression dans le milieu, mais si au lieu de mesurer la variation de pression, on mesure la variation de vitesse, on a des informations supplémentaires, comme par exemple la direction de la source. Il existe d'autres innovations de rupture, poussées par les technologies, qui sont des capacités accrues de systèmes de senseurs existants.

On peut signaler deux exemples. Dans la détection infrarouge, le fait de faire de l'hyperspectral, c'est-à-dire d'observer dans des bandes très différentes permet de rendre le leurrage beaucoup plus difficile. C'est de l'antifurtivité. Le fait également d'avoir des radars qui travaillent dans des bandes de fréquence extrêmement larges permettra d'avoir une polyvalence, puisqu'il faut une fréquence particulière pour être très précis, et d'autres types de fréquence pour détecter et reconnaître les éléments.

Cela permet également d'être plus difficilement brouillable. Sans doute le plus ambitieux, concerne les changements dans l'architecture d'ensemble des senseurs, qui sont souvent associés aux méthodes nouvelles de traitement du signal. On peut indiquer l'antenne active, prolongement du balayage électronique, qui permet d'associer à la fois une grande efficacité et une polyvalence. Ainsi, le même radar peut remplir les différentes fonctions évoquées (veille, alerte, renseignement et détection, poursuite) au service d'une armée. On peut citer également les systèmes de traitement des radars, comme les radars à ouverture synthétique, qui remplacent la taille de l'antenne par des mesures à des moments différents, et qui permettent d'atteindre des résolutions d'images radar, en particulier dans l'espace, dont il sera question. C'est

une véritable révolution si l'image radar commence à donner des informations analogues à celles de l'optique, en tout temps. Dans certains radars, l'émission et la réception ne sont pas au même endroit. Il s'agit parfois de deux endroits différents (bistatique), et parfois le radar est réparti, par exemple tout au long d'un produit, voire d'un avion. Cela permet d'augmenter l'efficacité et d'être parfois plus discret. En effet, s'il y a une émission d'un côté et une réception de l'autre, on peut détecter l'émission mais pas la réception.

La conclusion de tout cela est que dans le domaine des senseurs, les ruptures se font réellement par des avancées technologiques, mais surtout en croisant des technologies différentes, en fusionnant des données, chaque nouveauté apportant un élément qui n'est pas complet en lui-même. On obtient des avantages du point de vue opérationnel à travers d'une part la robustesse et l'antifurtivit(é (qui permet aux senseurs de fonctionner dans des conditions imprévues et également lorsque quelqu'un cherche à brouiller en face) et, d'autre part, la polyvalence (qui permet à un même senseur grâce à ses utilités différentes d'être intégré plus qu'auparavant dans le système).

## Rappel sur les missions des drones

Dans les derniers conflits évoqués les drones sont un atout majeur dans la conduite des opérations aéroterrestres. Ils sont d'une mise en œuvre rapide adaptable à la mission, tout terrain, essentiellement pour les drones tactiques, qui nécessitent d'être au contact de l'action, tout temps, capables pour certains de s'insérer dans le trafic aérien. Ils sont utilisés pour différents contextes d'emploi, tant dans la maîtrise de la violence, dans l'opération de déploiement dans les Balkans, que pour les surveillances des points chauds, les zones tampon, l'observation de mouvement des populations, l'acquisition de renseignements et la couverture des unités engagées. Mais ce sont également des actions de contexte de coercition, du type "Iraki Freedom", comme l'ont bien illustré les Américains sur différents aspects (surveillance, reconnaissance, attaque, illumination), des fonctions de "target-kill", la destruction physique de la cible, par Hellfire sur Predator, ou des actions de neutralisation par brouillage de l'adversaire. Cela est encore plus du domaine de l'entraînement et de l'exploration technologique que de la réalité, bien qu'en France il existe un système de brouillage embarqué sur les drones. Enfin, cela sert également au soutien dans les flux logistiques, dans l'optimisation des convois lors des opérations qui sont absolument nécessaires. Comme cela a été rappelé ce matin, la nature du conflit dans lequel ce nouvel outil est employé est très variée (conflits symétriques, dissymétriques ou asymétriques).

En ce qui concerne le contexte d'emploi, il s'agit d'un économiseur d'effectifs en espace fortement lacunaire et pour la coercition, c'est un multiplicateur d'effets en espace souvent lacunaire. L'aspect lacunaire du déploiement est un leitmotiv au cours des dernières opérations menées tant dans les Balkans qu'en Irak et en Afghanistan.

## L'apport présent des systèmes de drones

Le système Sperwer a été acquis très rapidement par les forces canadiennes (le Canada n'a pas de code des marchés publics), pour combler une lacune capacitaire. Les Canadiens prenaient la direction de l'Isaf, à Kaboul. Ils ont annoncé un appel

d'offres le 25 juin et ont sélectionné le système de drones le 1er août. Les systèmes concurrents étaient américains, français et israéliens. C'est le système Sperwer qui a été retenu. Les opérationnels tant de mise en œuvre que de maintenance sont arrivés vers la mi-août, et dès le début du mois de novembre ils étaient en opération sur le terrain. Les moyens de boucher des lacunes capacitaires existent. Ils sont partis avec un seul système, assez peu de moyens, et ils le mettent en œuvre à partir du camp Julien qui est très proche de Kaboul et qui est un endroit assez clos et difficile pour la mise en œuvre. L'utilisation quotidienne est de un à trois vols et les missions se font principalement de nuit. La notion de tout temps, jour et nuit, est donc cruciale.

Les types de missions qui sont conduites sont la surveillance de sites militaires, civils, et la surveillance de l'aéroport de Kaboul. Il faut savoir que les Canadiens survolent des zones urbanisées, ce qui nécessite une certaine fiabilité et des moyens embarqués comme IFF, liaison avec le contrôle aérien local, en temps réel.

L'insertion dans la troisième dimension est donc nécessaire. Ils font également du monitoring en temps réel des troupes au sol, les opérateurs de la station au sol sont en liaison directe avec la compagnie d'infanterie qui intervient sur un site à Kaboul et un dialogue est établi en permanence avec un guidage au plus proche des forces sur le terrain. Ils sont également utilisés dans des missions de police, dans des interventions de démantèlement de trafic de drogue, et d'arrestations. Il convient de savoir qu'à Kaboul, le contexte d'emploi est assez difficile. La surveillance ne peut être pratiquement qu'aérienne car tous les bâtiments sont clos, avec des systèmes de cours qui communiquent entre elles par des murs de deux à trois mètres. Il est donc nécessaire de travailler de nuit, car l'adversaire travaille de nuit, et en survol, puisque le théâtre opérationnel ne se prête pas à une observation depuis le sol, sans compter que l'observation doit être discrète.

L'exploitation du renseignement se fait de différentes façons, avec une « dissémination » de vidéos en temps réel à travers des réseaux locaux vers le QG de Brigade situé dans un autre camp que celui de déploiement des drones, et vers l'aéroport de Kaboul, qui est un autre centre de collecte de renseignements. Des images sont également diffusées vers l'U.S. Air Force et le quartier général de l'OTAN, au travers de standards OTAN. La collecte du renseignement est assurée par l'U.S. Air Force sur place. Les conditions de la mise en œuvre locale sont très difficiles : mille huit cents mètres d'altitude, conditions jusqu'à ISA +35, avec des amplitudes de température très élevées. La mise en œuvre se fait depuis un espace très confiné, dans le camp et la récupération dans le camp, avec un espace ouvert à tous vents et une foule qui se précipite à chaque récupération. On a pu voir un avion qui bougeait dans tous les sens dans la caméra embarquée car des enfants piétinaient l'avion et s'en servaient comme le « baron Munchausen » avec son boulet voici quelques siècles. L'environnement montagneux, avec du vent, des turbulences, de forts masquages pour les transmissions, tout cela demande des transmissions robustes avec des capacités de navigation en mode silence pour les aéronefs si nécessaire, en cas de rupture de la liaison.

Le même système que les Canadiens à quelques évolutions fonctionnelles près, ou interfaçage de C4I un peu différente. Le système est multimissions, optimisé pour la désignation d'objectifs pour l'artillerie. On atteint des capacités grâce au système de navigation inertielle, à l'optronique moderne et à la capacité de

transmission en temps réel, avec une désignation d'objectifs qui est bien meilleure que cinquante mètres pour l'artillerie ou pour le ciblage de l'armée de l'air et la reconnaissance. La mise en œuvre tactique se fait depuis une catapulte automatique ; la récupération par parachute, ce qui est le cas de la majorité des systèmes européens, qu'ils soient français ou non. Le système est interopérable, au sens français ou OTAN. Il existe un standard OTAN pour les transmissions de données, avec 80 km extensibles jusqu'à 200 km selon le choix des clients, et des interfaçages multiples.

Il convient de souligner que l'environnement d'interopérabilité pour le système des drones est assez fluctuant. Le STANAG 4586 définit l'interopérabilité des drones qui n'est pas tout à fait ratifiée et laisse la porte ouverte à beaucoup de travail entre les opérationnels et les industriels. Pour l'illustration de l'interopérabilité française, on peut signaler les trois niveaux (stratégique, opératif et tactique). Le système de drones n'est pas une fin en soi et il doit forcément être interfacé avec le monde extérieur. Le système français est directement interfacé en direct avec SICF (système de C4I au niveau plutôt opératif mis en œuvre par les hauts niveaux brigades et divisions), interfacé avec Atlas pour la désignation des objectifs de l'artillerie, interfacé avec SAIM (des images ou du renseignement pour les dossiers d'objectifs pour les forces armées air et aéronavales), et interfacé actuellement via SICF à MARTHA (la coordination 3D). A terme, cela se fera par la liaison en direct pour déclarer le système de drone dans son environnement. Les informations sont possibles également avec les forces alliées via les passerelles MIP, standard OTAN, comme le font quotidiennement les Canadiens.

L'environnement est donc assez complexe, et l'on peut imaginer la difficulté au niveau de l'OTAN.

### Les enjeux futurs

Le grand enjeu, étant donné les finances limitées actuellement en Europe, est de mutualiser et de créer une base européenne de technologie. Cette base serait tirée par deux systèmes qui sont les drones tactiques et les drones mâles. On peut citer quelques chiffres illustrant les difficultés à maintenir cette base en Europe. On évalue le marché annuel à 1,8 milliard pour les drones, dont 600 millions seulement hors USA par an (1,2 milliard pour les USA). Le marché européen représente 600 millions. On risque donc de rencontrer des difficultés pour maintenir la base technologique si les tendances actuelles sont maintenues. De plus, on constate un hiatus dans le système actuel entre les drones tactiques et les drones mâles, les premiers ayant une bonne base opérationnelle qui existe, avec des technologies éprouvées, alors que les mâles se cherchent encore et sont davantage en devenir.

Pour conclure, les futurs enjeux pour les drones tactiques ou les drones au sens large concernent l'élargissement du catalogue des missions, la permanence d'acquisition, d'objectifs ou de renseignement, à travers de nouvelles charges utiles, qui sont l'enjeu principal. Il s'agit également de pouvoir dialoguer directement avec les forces, à l'aide de systèmes de transmission qui diffuseraient l'information directement aux troupes au contact ou permettant des multidrones par station au sol actuellement afin de résoudre les problèmes d'encombrement spectral. Un autre enjeu important concerne l'insertion dans la circulation aérienne. Les technologies restent à développer. L'appontage sur bâtiment reste également un enjeu technologique pour les drones maritimes. On ne sait toujours pas faire apponter un drone sur un navire et les

technologies restent dans ce domaine expérimentales. Enfin, on peut citer la réduction du temps de traitement de l'information de l'observation au tireur. L'enjeu est la pérennité, avec l'utilisation de ces technologies qui sont pour la plupart COTS, donc civiles, et de plus en plus, il est nécessaire de concevoir des architectures tolérantes à l'héritage et à l'encapsulage. Le développement en spirale tel que l'envisagent les Etats-Unis est un enjeu important pour maintenir la capacité drone dans les forces armées.

Notre enjeu est de ne pas oublier qu'il y a toujours l'homme dans la boucle. Le vocable américain UAV est dans ce sens très mal choisi: Unmanned, car ils sont téléopérés et les hommes sont toujours dans la boucle.

**Zoltán RAJNAI, László TREMBECZKY**

# LE CIMENT DES ARMEES: LA COHESION

Malgré toutes les innovations techniques, la révolution conceptuelle des stratégies, l'élément majeur et central de l'outil de défense reste l'homme. Les notions de temps réel, de concept "zéro mort", de menace diffuse et permanente viennent stimuler un monde mouvant où l'électronique est devenue reine. Mais la technique n'est que l'outil favorisant l'action et affirmant la volonté de l'homme, qui est et reste au cœur de tout. La suspension de la conscription et son corollaire, la professionnalisation, constituent une véritable révolution culturelle pour le militaire français : membre d'une société de consommation avide d'individualisme et de prospérité, il se cherche aujourd'hui une nouvelle identité professionnelle tout en revendiquant légitimement l'amélioration de sa condition ainsi qu'une réelle reconnaissance de la nation.

Dans le même temps et dans un contexte budgétaire contraint, les armées s'attachent à ce qui est leur finalité ultime : l'efficacité opérationnelle. Pour y parvenir, elles connaissent l'importance primordiale de ce que l'on appelle communément "la cohésion", qui, à elle seule, peut parfois expliquer un succès ou un échec.

Tenter de définir cette notion, puis appréhender les effets de la professionnalisation et l'état d'esprit actuel des militaires, peut permettre d'en percevoir les ressorts et d'oser quelques pistes de réflexion pour améliorer les conditions d'émergence de "la cohésion".

## De l'esprit de corps à la cohésion

Il est de coutume de fondre en un même amalgame la cohésion, "l'esprit de corps", voire par extension, lorsque l'on évoque la perception de la chose militaire, "l'esprit de défense". Cet amalgame est naturel tant il semble difficile de définir la portée et les contours de ces différentes notions. Les deux premières ne sont d'ailleurs pas l'apanage du monde militaire. Certaines firmes tentent d'accroître leur compétitivité en créant une véritable culture d'entreprise. De grandes écoles favorisent le développement d'un caractère spécifique d'appartenance, d'une identité collective qui nourrit le besoin de reconnaissance et répond à un désir profond d'identification et de fierté. C'est le terrain propice à une forme de solidarité que rejoint en ce sens "l'esprit de corps": la solidarité professionnelle, l'un des liens sociaux les plus puissants.

La cohésion apparaît pourtant comme une notion encore plus complexe, assortie d'une plus forte connotation affective. Bon nombre d'analystes se sont penchés sur ce phénomène qui semble devoir se cantonner au groupe, au collectif de premier niveau où s'exerce le contact humain direct. Résultat des liens et relations humaines qui s'y nouent, la cohésion constitue le ciment du moral, élément essentiel dans un environnement difficile voire hostile. Elle favorise la perception d'une dynamique au sein du groupe, et se fonde sur deux principaux besoins: celui de camaraderie, de complicité; et celui de reconnaissance par les autres au sein du groupe.

Un vécu commun difficile semble indispensable à l'éclosion de la cohésion. Plus il aura été fort, plus elle sera prononcée. Pour autant, cette condition préalable ne

semble pas suffisante. La nature de l'activité professionnelle, sa durée quotidienne, son intensité, l'organisation de l'entité, son environnement, le type d'autorité qui s'y exerce, la présence ou non de danger, restent des facteurs essentiels. La recette de la cohésion est largement plus complexe qu'il n'y paraît…

### Et l'homme dans tout ça ?

La clef de la cohésion reste l'homme. De son attitude, de la perception de son environnement professionnel, mais aussi social, dépend le développement de la cohésion…

Or, la place du militaire dans la société est intimement liée à son statut. Celui-ci énonce le principe selon lequel le militaire jouit des mêmes droits que l'ensemble des autres citoyens. Il en exclut cependant l'exercice des droits politiques et en limite celui de la citoyenneté, constituant de fait leur spécificité. Une majorité de militaires apprécient cette distinction statutaire qu'ils interprètent comme un particularisme prouvant leur neutralité collective et l'abnégation propre à l'exercice de leur métier. Mais la collectivité militaire reste très attentive à la prise en compte réelle de ses inquiétudes et de ses conditions de vie. Car le militaire, malgré la spécificité de son métier, ne vit pas différemment de la majorité de la populatopn. Il ressent et vit de manière individuelle et familiale les soubresauts de la crise économique, le chômage, la morosité générale… Il exerce son métier dans une institution en pleine révolution culturelle.

### La professionnalisation des armées

Le manque d'égalité du service militaire, son coût, les évolutions politiques, sociales, économiques et scientifiques, combinées à la nouvelle dimension multipolaire du monde, imposaient l'option de la professionnalisation des armées et la suspension de la conscription. Pressentie, ce fut tout de même une véritable révolution… Ses effets ont porté sur l'organisation de l'institution elle-même mais aussi sur l'identitaire. Ainsi, le remplacement des appelés du contingent par des militaires professionnels a provoqué un "brassage social" fort différent de celui connu jusqu'alors. L'institution militaire s'est apparentée à l'entreprise et a adopté ses pratiques de gestion. De plus, y "faire carrière" est devenu un parcours d'obstacles permanent, et les phénomènes de civilianisation et de féminisation y ont complexifié les relations humaines. Enfin, dans une institution où la stabilité était jusqu'alors un véritable fondement, la population militaire a découvert la précarité de l'emploi… Signe des temps, évolution des mentalités, la professionnalisation n'a fait que renforcer la présence des civils et des femmes dans les armées et majoritairement dans les unités de soutien… Les premiers constituent souvent la mémoire collective et devraient donc favoriser la cohésion. Néanmoins, s'ils revendiquent une meilleure considération au sein de l'institution militaire, certains sont peu enclins à s'impliquer dans la vie collective. A leur corps défendant, une grande majorité des militaires montre à leur égard une certaine méfiance qu'engendre la présence des organisations syndicales. Les militaires féminins sont, quant à eux, légitimement soucieux de réussir harmonieusement leur vie professionnelle et privée. Combinant efficacement emploi, vie de couple et de mère de famille, ils n'accordent généralement que peu d'intérêt aux activités de cohésion hors des horaires habituels de travail où d'autres contraintes les

réclament. De plus, l'ambiance générale de ces unités de soutien souffre parfois de congés de maternité trop concomitants.

L'organisation interne y remédie généralement, non sans quelques difficultés, mais chaque absence prolongée entame le processus de cohésion. En fait, la perte de repères déstabilise, les certitudes s'envolent et les interrogations sur le devenir engendrent une réaction épidermique d'agressivité ou de repli sur soi qui ne favorise pas la cohésion. De surcroît, les militaires craignent surtout une banalisation de leur métier…

### Le besoin de considération des militaires.

Les militaires continuent à souffrir d'un manque de considération et d'un sentiment d'injustice. A leurs yeux, en effet, peu d'autres corps de la fonction publique auraient su assurer leurs missions et dans un même temps vivre une telle révolution organisationnelle et identitaire. Le sentiment d'être corvéable à merci, d'appartenir au seul ministère où des réformes sont possibles… et où le budget sert de variable d'ajustement reste d'actualité. Même les récentes mesures de rattrapage semblent aux militaires aujourd'hui parcellaires et d'une logique très catégorielle, donc inéquitable. La nation n'est plus aussi concernée par son armée et cette situation n'incite guère, au sein de cette dernière, au développement d'une véritable cohésion qui ne soit pas exclusivement revendicatrice à l'instar d'autres institutions.

### Mais comment développer la cohésion des armées ?

Il n'y a pas de véritable recette… Chacune de nos armées est dotée d'une structure différente, et doit doser, adapter et faire évoluer ce subtil mélange d'"ingrédients" qui favorisent l'émergence de cette notion. Sur une base aérienne sont stationnées des unités aériennes et des unités de soutien. Les premières sont constituées de groupes relativement restreints d'hommes et de femmes destinés à servir un système d'armes et à répondre à des missions bien définies. La richesse d'un passé émaillé de faits d'armes glorieux, de grandes figures et de traditions, favorise le sentiment de fierté d'appartenance du personnel, toutes spécialités confondues, à ces entités prestigieuses qui les emploient.

### Les activités conviviales pour cimenter la cohésion.

Traditionnellement, dans les unités, les "repas de cohésion" constituaient l'activité conviviale par excellence, ainsi que les bars typiques de certains escadrons les lieux d'échanges et de détente hors des heures de service. Bien loin des mythes négatifs d'excès peu glorieux, les jeunes engagés ne les considèrent pas comme facteurs de cohésion… et désertent les lieux de convivialité. Le rapprochement des militaires, accompagnés de leurs familles, participe au sentiment d'appartenance et tous se déclarent à l'issue réellement conquis après une première réaction épidermique de contrainte ressentie.

En réalité, repas, pots, lotos et autres activités ludiques et familiales ne créent pas la cohésion ; ils la renforcent, la scellent, s'ils s'appuient sur des relations internes déjà existantes. En ce sens, ils sont utiles au développement de cette notion.

**Gyula RÉVÉSZ**

# INFORMATION OPERATION IN THE "INFORMATION AGE"

In the early1980s, the manner in which the public and private sectors conduct business and provide wide range of services to the public has changed. Since then millions of computers and numerous local area networks worldwide have been connected through a global network of networks. Internet use has grown rapidly in the last few years. Today, the Internet can be accessed from anywhere and anytime. With the continuous improvements, it became possible that certain services can be provided through the worldwide network system. All around the world it has become more and more widespread to use Internet for governmental use.

In the so-called "Information Age" institutions, groups and individuals depend on computers to a great extent. It is no longer necessary for the intruders with malicious intent to have direct physical access to a computer in order to copy, destroy or manipulate data. People can use a variety of techniques and software tools to exploit a targeted system once they gain unauthorized access. To protect the network, protective measures are needed. They address physical attacks on critical systems and data; however, they have been or are in the process of being revised and updated to deal with the new class of computer-based threats defined as Information Operations (IO).

## Information Operations

The concept of IO has been affected by and comes from that of "Information Warfare" (IW). IW can be defined as „the physical and computer-based operations used by military forces in time of conflict and near-conflict to compromise the access to and viability of information received by the decision-makers of an enemy, while at the same time protecting their own information and information systems."232 The term IO is used to denote the use of IW tools and techniques. The critical sectors of a certain country can be identified: transportation; oil and gas; water; emergency services; continuity of government services; banking and finance; electrical power; and telecommunications.

IO is the outgrowth of military doctrine that focused on the use of electronic warfare measures to the capabilities of adversaries on the battlefield. These techniques can be effectively used against not only the military but the civilian networks, systems as well.

However, most discussions relating to the use of computer-based tools and techniques in the context of IO have come to focus on information assurance and the protection of computer-based systems and networks from an intrusion or attack.

## The Threat

IO can be used to disrupt, destroy or manipulate information systems from anywhere in the world using hardware and software without significant financial investment. The potential threats to the critical infrastructure include:

[232] Report # 2001/11, Information Operations, May 6, 2002, CANADIAN SECURITY INTELLIGENCE SERVICE

- the disruption of components of the national infrastructure;
- the exploitation of information;
- the manipulation of information for political, economic, or military purposes; and
- the destruction of information or infrastructure components.

Disruption, delay of the operation of, or damaging, a targeted computer system could have significant negative impacts on social, political and economic activities and thereby it is possible to seriously influence national security. Although security measures are being created to protect these infrastructures, the development of attack tools to circumvent these protective measures is ongoing and these attack mechanisms have become freely available through the Internet.233 The number of intrusions into computer-based systems is on the rise and the tools used to exploit existing vulnerabilities are growing in sophistication and simplicity. Although only a small number of system intrusions are reported, indications are that the level of reported incidents and vulnerabilities is doubling annually.

The threat of unauthorized intrusions into computer systems and networks increases as the network extends. Besides, physical attacks like cutting power cables or destroying the hardware upon which the information infrastructure depends are the equivalent of physical denial of service (DoS) attacks234. The latter form of attack prevents authorized users from gaining access to information systems and data. Any of these hostile actors can attack vulnerable infrastructure points using physical means and/or software.

The increasing reliance of states on computer networks makes critical infrastructures attractive targets for attack and exploitation, and many countries have embarked on programs to develop IO doctrines and technologies. An American Congressional report identified that certain countries (Russia, China, India and Cuba) had prepared for cyberwar and were developing IO capabilities; in addition to it, rogue states have some IO capabilities as well. Even though many countries have or are developing IO capabilities, only few of them have the means to fully integrate various IO tools into a comprehensive attack that would totally disrupt the country's infrastructure.

### Data and system security

The development of IO tools and techniques keeps pace with the rate of technological improvement in the fields of the communications and computer industries. The ability to communicate and connect to networks worldwide almost instantaneously has created both advantages and disadvantages.

Due to the intrusions into their systems and loss of sensitive information, government departments and businesses have attempted to introduce security measures to protect both systems and data. Unfortunately, these security packages can be effectively used for a short period only. The more persons, businesses and government departments become dependent on computer-based communications, the more complex the configuration of interacting computer networks and operating systems becomes and creates several vulnerabilities. Natural forces (like storms), the normal development of new hardware and software, and IO tools could pressure these

[233] Information Warfare: Hype or Reality by E. Anders Eriksson

[234] Information Superiority: What is it? How to achieve it?, Walter P. Fairbanks, June 1999

vulnerabilities and cause failures entailing a profound effect, both short- and long-term, on the operation of government and the private sector.

To summarize briefly, I intended to give you a general picture of the current situation concerning Information Operations. This area is under continuous monitoring and development. The more developed the information technology is, the more sophisticated methods are used to gain access into private, business or closed networks. The more sophisticated the intrusion attempts are, the more money and energy is needed in order to successfully counter them.

**Roland VIDA, Attila VIDÁCS**

# A SURVEY ON ENERGY EFFICIENT COMMUNICATION SCHEMES IN WIRELESS SENSOR NETWORKS

Rolland Vida, Attila Vidács
Budapest University of Technology and Economics
Department of Telecommunications and Media Informatics
Magyar tudósok krt.2, 1117 Budapest, Hungary
{vida, vidacs@tmit.bme.hu}

**Abstract:**

Wireless sensor networks entered recently into the spotlight of industry and academia, both because of the large number of possible application scenarios and the wide range of related open questions still to be answered through robust and efficient communication solutions. As sensors have small batteries that are usually impossible or impractical to recharge, one of the most important issues related to these networks is their energy efficiency. In this paper we propose a short survey of the mostly used energy-sparing strategies for such environments: clustering, energy-efficient routing, integration of mobile devices, or optimized sleep scheduling solutions.

## I. Introduction

Wireless sensor networks (WSN) became recently one of the hottest topics both for the industry and the networking research community. This is due, on the one hand, to the ever-widening range of attractive applications (e.g., disaster and environmental monitoring, wildlife habitat monitoring, intrusion detection, security surveillance) sensor networks can be used for. On the other hand, sensor networks are self-organizing ad-hoc systems where optimized energy consumption is of paramount importance; therefore, relaying information between sensors and a sink node, possibly over multiple wireless hops, in an energy-efficient manner is a challenging task that preoccupies many researchers.

Taking into account the importance of energy-efficient operation, several different communication solutions were proposed recently for sensor networks. On the one hand, clustering methods are useful as the burden of reporting is concentrated only to a reduced set of so-called cluster heads. On the other hand, communication energy can also be reduced by integrating mobile sink nodes that move close to the reporting sensors in a random, predictable, controlled, or adaptive manner. Traditional routing solutions in wired or even wireless networks were developed to optimize metrics such as delay or packet loss. However, in the case of wireless sensor networks routing paths have to be chosen in such a way so as to minimize and balance energy consumption among the communicating sensors. Finally, the monitored regions are usually covered redundantly by sensors, in which case it is essential to provide optimal sleep scheduling solutions so as to minimize redundant reporting while maintaining high coverage ratios. This paper presents a short survey on existing solutions that build on the above ideas.

The rest of this paper is organized as follows. First we present some basic characteristics of a wireless sensor network, such as the specificities of the composing

sensors, their communication patterns and reporting models. Then in Section III we describe briefly some of the most known energy-sparing solutions used for wireless sensors networks: clustering techniques, energy-efficient routing mechanisms, the benefits of integrating mobile devices and sleep scheduling solutions. Finally, Section IV concludes this paper.

## II. Characteristics of a Sensor Network

Sensor networks consist of a usually large number of tiny, low cost devices, with a consequently low storage and computational capacity, and a limited energy supply. It is usually considered impossible or impractical (from a technical or economical point of view) to recharge their batteries; thus, they should be managed in such a way to ensure the unattended operation of the network they are part of, for a long enough time period (e.g., several months).

The lifetime of a sensor network can be defined in several ways. Some applications can tolerate a loss of a large number of nodes, while in others loosing a single sensor violates the functionality of the whole network. In the latter case, the network lifetime can be defined as the time until the first node depletes its battery, while for robust applications the network can be considered to be alive till a given percentage of the sensors has enough energy to operate, or till a given percentage of the region is covered by alive sensors. Even if numerous methods were proposed to recharge sensor batteries (e.g., by deriving mechanical, chemical, or solar energy from the surrounding environment) [28] the unavoidable increase in size, weight, or price for these sensors might make the solutions unattractive. Therefore, in this study we do not address rechargeable devices.

Sensors have sensing, processing and transmitting capabilities. The main goal of their operation is to monitor a given area, gather information, and forward it to one or several sink nodes (often also called base stations). A sensor can send data either directly to the sink (single-hop), or through intermediate sensors that act as relay nodes (multi-hop operation).

Information gathering in sensor networks can follow different patterns, depending mostly on the specific needs of the applications. In a time-driven scenario all sensors send data periodically to the sink. As opposed to this, in the event-driven case sensors start communicating with the sink only if sensing an event, i.e., a situation that is worth reporting according to the requirements of the application. Finally, in a query-driven scenario a sensor transmits its data only if the sink asks for it. Most of the research papers in the area address the time-driven scenario, and provide energy-efficient solutions for homogeneous networks, with sensors having constant and equal amounts of data to send in all parts of the covered region. However, there are a large number of applications (e.g., intrusion detection, seismic activity monitoring, or animal movement tracking) where an event-driven approach is more appropriate.

## III. Techniques to Reduce Energy Consumption

One of the most important features of a WSN is its energy-efficiency, as in most of the cases sensors dispose of small batteries that are impossible or impractical to change or recharge. In such conditions it is of paramount importance to develop dedicated communication solutions that handle sensor data gathering in an energy-sparing manner, prolonging thus the lifetime of the network.

With the current technology, communicating one bit over a wireless medium, even at short ranges, consumes several orders of magnitude more energy than processing that bit; this tendency is foreseen not to change in the near future [7]. There are some straightforward ways to decrease the energy used for communication: reducing the amount of data that is transmitted, reducing the number of reporting sensors and/or shortening the communication range. In the following we present different solutions that build on these ideas.

### III.1. Clustering solutions

The amount of data to be transmitted can be reduced by dividing the network into small clusters, a cluster head being responsible for aggregating and relaying to the sink the information gathered from the sensors of its clusters [18,37].

One of the most cited clustering approaches is LEACH (Low-Energy Adaptive Clustering Hierarchy), a self-organizing, adaptive protocol where the nodes organize themselves into clusters, with one node acting as the cluster head (CH) [12]. It is assumed that the sink node is fixed and located far from the sensors.

The operation of LEACH is broken up into rounds, where each round begins with a set-up phase, when the clusters are organized, followed by a steady-state phase, when data transfers to the sink node occur. In the set-up phase, sensors elect themselves to be cluster heads with a certain probability. The optimal number of clusters to have in the system depends on several parameters, such as the network topology and the relative costs of computation vs. communication. Once elected, the CH nodes broadcast their status to the other sensors in the network. Each sensor node determines to which cluster it wants to belong by choosing the cluster head that requires the minimum communication energy. (Typically this will be the cluster head closest to the sensor.) Once all nodes are organized into clusters, each cluster head creates a TDMA (Time Division Multiple Access) schedule for the nodes in its cluster. This allows the radio components of each non-CH node to be turned off at all times except during its transmit time. The TDMA scheduling solves intra-cluster communication interference, but overhearing from neighboring clusters affects communication. To solve this problem, in each cluster different spreading codes are used, chosen by each CH randomly. However, within a single cluster all nodes use the same code, together with the TDMA scheduling.

On the other hand, in the steady phase LEACH assumes that all sensors are sensing the environment at a fixed rate, and thus, always have data to send. Data is gathered and aggregated by the cluster heads, and forwarded to the far away sink node. Being a cluster head drains the battery of that node. In order to spread this energy usage over multiple nodes, the CH role is randomly rotated among the sensors. At the beginning of each round, sensors re-evaluate their decision about being a CH node, or not; each node makes its decision independently of the other nodes in the network. Once the new CHs are obtained, the cluster borders are re-shaped; each non-CH sensors decides which new CH to join.

There are several papers that propose improvements of the basic LEACH algorithm. In [11] authors introduce an energy factor in the cluster head election process; a candidate that has more residual energy has a higher probability to become cluster head, equilibrating thus energy consumption among the nodes. In [21] nodes form a chain and send data only to the neighboring node on the chain. The cluster

head role is assumed in turns along this chain; the data collected on the chain is aggregated by the CH and sent to the sink. In ASCENT [4] nodes probe the surrounding environment and look for neighboring cluster heads; based on the received feedback, they take local decisions whether or not to switch in CH mode. Finally in HEED [38] authors propose a hybrid, distributed clustering approach, where CH nodes are elected based on their residual energy level and secondary parameters such as node proximity to its neighbors or node degree.

### III.2. Mobility Solutions

Sensors consume energy for sensing the field, for digitizing and processing the data, but the most penalizing task is by far the transmission of the information [25]. In the most commonly accepted power attenuation model [27], signal power falls as $1/d^{\alpha}$, where d is the distance from the transmitter antenna and $\alpha$ is the attenuation exponent, a constant dependent on the wireless transmission environment, with values typically between 2 and 5. Therefore, assuming that all receivers have the same power threshold for signal detection, typically normalized to one, the energy required to support communication between two nodes located at a distance d one from the other is $d^{\alpha}$. In such conditions it is straightforward to assert that by minimizing the distance between a sensor and a sink node we can efficiently reduce power consumption, both for single- and multi-hop communications (reducing the length of the multi-hop path results in fewer and/or shorter hops, i.e., less energy is needed to relay data to the sink).

There is a recent trend to explore mobility as a way of enhancing the networking capabilities of wireless systems. Besides increasing the capacity of ad-hoc wireless networks [10], it was also recognized that mobility can be used to support energy efficient operation of sensor networks; by introducing the mobility of either the sensors or the sink node(s), the communication distance can be reduced. There are some approaches that rely on sensor mobility, not for energy-efficiency but mostly for coverage problems. As an example, in [35] sensors are mobile only at the deployment phase, to eliminate coverage holes discovered through the use of Voronoi diagrams, while in [3] sensors dynamically react to environmental changes and move towards areas where events occur frequently. Mobile sensors are also considered in [31] to provide an extension of a stationary sensor network. However, using mobile sink nodes to get near the reporting sensors is a more common solution.

The approaches based on sink mobility can be classified in three categories: random, predictable and controlled mobility. In [30] randomly moving mobile agents, called Data MULEs (Mobile Ubiquitous LAN Extension) are used to collect data in sparsely populated sensor networks. A similar approach, but for dense networks, is used by SENMA (SEnsor Networks with Mobile Agents) [32]; a mobile agent is randomly flying above the sensor field and gathers data from sensors that are triggered based on the estimated fading state of their communication with the agent. Authors of [14] use a random walk model for a mobile relay to theoretically derive parameters such as delay and data delivery ratio. Finally, randomly moving sink nodes are also assumed in the SEAD (Scalable Energy-efficient Asynchronous Dissemination) protocol [19], but in a scenario where there is a single sensor to transmit data to all these mobile sinks; the goal of the protocol is to build and maintain an energy-efficient multicast dissemination tree that covers all the interested nodes.

A predictable movement of the sink is also proposed in several papers. In [5] the observer (i.e., the sink) moves along a predefined path, and pulls data from the sensors when it arrives close to them. In [22] the predefined path is the periphery of the covered circular region itself; it should be noted that the authors assume here multi-hop communication between the sensors and the sink, as opposed to the previous approaches where the sensors have waited for the best moment to send their report directly to the sink.

There are also solutions based on controlled mobility. In AIMMS (Autonomous Intelligent Mobile Micro-server) [16,17] a mobile micro-server moves across the network, along a specific trail, to route data from the deeply embedded nodes; its mobility is controlled in the sense that it spends extra time (e.g., it stops or slows down) in areas where there is a large amount of data to send, or where the channel capacity requires so. Controlled mobile nodes are used for message ferrying also in [39]; these nodes provide non-random proactive routes in highly-partitioned wireless ad-hoc networks.

An attempt to determine specific sink movements for energy optimization is presented in [8]. The authors argue that multi-hop communication results in the sensors neighboring the sink being depleted at a fast pace. Therefore, they propose to employ multiple sink nodes that periodically change their locations, and present an ILP (Integer Linear Programming) model to obtain the optimal positions of these sinks. A linear programming solution to determine the movement of the sink and its sojourn time in different points of the network is given in [34] as well. Both the sensors and the sink are placed on a bi-dimensional grid. The sink moves along the grid, sojourns times in the specific grid points being calculated so as to maximize the network lifetime.

A solution that is significantly different from all the above is presented in [33]. Authors define an adaptive strategy for sink mobility in an event-driven scenario, so as to continuously move the sink towards an optimal position as far as energy-consumption is concerned, taking into account the current events in the network. Most of the previous solutions addressed time-driven scenarios. In such cases all the sensors measure and send data periodically to the sink. Therefore, moving the sink node has mainly a load-balancing role: in case of multi-hop communication it would spare near-by nodes that relay packets from all the others, while in case of single-hop communication it would spare far-away nodes that have to spend much energy to reach the sink. As opposed to these, in an event-driven scenario the adaptive mobility of the sink could result in energy-saving benefits that reach far-beyond simple load balancing. If not all the sensors are active at a given moment, only those that sensed a specific event, it might worth moving the sink towards those nodes.

There are other approaches as well in the literature that addressed the problem of optimal sink placement. In [2] the authors assume a time-driven scenario, and solve the problem of placing n sink nodes so as to optimize energy-consumption. A similar issue is raised in [23]: an algorithm is proposed to find the optimal location of multiple sinks in sparse networks of aggregator points that report directly to these sinks.

### III.3. Energy-efficient Routing Schemes

As we stated earlier, an efficient data gathering solution should aim at minimizing the distance sensors are communicating to, while trying to inform their corresponding

sink nodes. A straightforward solution to do so is relying on multi-hop communication: instead of communicating directly with a possibly distant sink node, data is relayed hop-by-hop by the intermediate sensor nodes. Such an approach, coupled with dedicated energy-aware routing techniques might result in a more balanced energy-consumption among the network nodes.

Traditional routing algorithms in wired and even wireless environments focused on optimized data transmission in terms of delay and packet loss. However, the specific requirements of wireless sensor networks make these traditional solutions often inadequate. Therefore, new approaches were proposed to handle data forwarding in sensor networks, building on energy conserving routing techniques, i.e., finding optimal routes in terms of consumed power, and balancing the energy consumption among all nodes [6,9,15,29,40].

However, while multi-hop routing spares the energy of distant sensors, it increases the load on those located near the sink node. Moreover, complicated routing algorithms, in an error-prone wireless environment including low-capacity sensors might not yet be profitable and reliable enough for application and service providers; the majority of the deployed, real-world sensor networks we are aware of are based on single hop communication.

### III.4. Other Optimization Techniques

Besides the above described solutions, there are several other proposals targeting the energy efficiency of wireless sensor networks. Some approaches build on topology control schemes, i.e., deploying sensor and sink nodes in an efficient way or reshaping the topology through dynamic power control of the participating sensors [20,24,26,36].

Another solutions build on the monitored regions being usually covered redundantly by sensors; in such a case it is essential to provide optimal sleep scheduling solutions so as to minimize redundant reporting while maintaining high coverage ratios [41,42].

## IV. Conclusions

Energy efficiency is of paramount importance in wireless sensor networks, as sensors have usually limited energy supply that should be spared so as to maximize the lifetime of the network. This paper proposed a short survey of the most known solutions developed to support an energy efficient operation for WSNs. We presented several clustering solutions, energy efficient routing mechanisms, and approaches building on sink and sensor mobility.

## References


[1] A. Behzad and I. Rubin, "Impact of Power Control on the Performance of Ad Hoc Wireless Networks," in *Proceedings of IEEE INFOCOM'05*, Miami, FL, USA, Mar. 2005.

[2] A. Bogdanov, E. Maneva, and S. Riesenfeld, "Power-aware Base Station Positioning for Sensor Networks," in *Proceedings IEEE INFOCOM'04,* Hong Kong, China, Mar. 2004.

[3] Z. Butler and D. Rus, "Event-based Motion Control for Mobile Sensor Networks," *IEEE Pervasive Computing*, vol. 2, no. 4, pp. 34–42, Oct.-Nov. 2003.

[4] A. Cerpa and D. Estrin, "ASCENT: Adaptive self-configuring sensor networks topologies," in *Proceedings of IEEE INFOCOM'02*, vol. 3, New York, NY, June 2002, pp. 1278–1287.
[5] A. Chakrabarti, A. Sabharwal, and B. Aazhang, "Using predictable observer mobility for power efficient design of sensor networks," in *Proceedings of IPSN'03, Second International Workshop on Information Processing in Sensor Networks*, Palo Alto, CA, USA, Apr. 2003, pp. 129–145.
[6] J.-H. Chang and L. Tassiulas, "Energy conserving routing in wireless ad-hoc networks," in *Proceedings of IEEE INFOCOM'00*, vol. 1, Tel Aviv, Israel, Mar. 2000, pp. 22–31.
[7] L. Doherty, B. A. Warneke, B. E. Boser, and K. Pister, "Energy and performance considerations for smart dust", *International Journal of Parallel Distributed Systems and Networks*, 4(3):121-133, 2001.
[8] S. R. Gandham, M. Dawande, R. Prakash, and S. Venkatesan, "Energy efficient schemes for wireless sensor networks with multiple mobile base stations," in *Proceedings of IEEE Globecom*, vol. 22, no. 1, San Francisco, California, Dec. 2003, pp. 377–381.
[9] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, energy-efficient multipath routing in wireless sensor networks", *ACM SIGMOBILE Mobile Computing and Communications Review*, 5(4):11-25, October 2001.
[10] M. Grossglauser and D.N.C. Tse, "Mobility increases the capacity of ad-hoc wireless networks," in *Proceedings of IEEE INFOCOM'01*, Anchorage, Alaska, Apr. 2001, pp. 1360–1369.
[11] M.J.Handy, M. Haase, and D. Timmermann, "Low energy adaptive clustering hierarchy with deterministic cluster-head selection", in *Proceedings of MWCN'02,* Stockholm, Sweden, September 2002.
[12] W.R.Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks", in *Proceedings of 33rd Hawaii International Conference on System Sciences*, 2000.
[13] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: a scalable and robust communication paradigm for sensor networks," in *Proceedings of ACM Mobicom'00*, Boston, MA, 2000, pp. 56–67.
[14] S. Jain, R. C. Shah, G. Borriello, W. Brunette, and S. Roy, "Exploiting mobility for energy efficient data collection in sensor networks," in *Proceedings of WiOpt'04*, Cambridge, UK, Mar. 2004.
[15] K. Kar, M. Kodialam, T.V. Lakshman, and L. Tassiulas, "Routing for network capacity maximization in energy-constrained ad-hoc networks," in *Proceedings of IEEE INFOCOM'03*, San Francisco, CA, USA, Mar. 2003, pp. 673–681.
[16] A. Kansal, M. Rahimi, W.J. Kaiser, M.B. Srivastava, G.J. Pottie, and D. Estrin, "Controlled mobility for sustainable wireless networks," in *IEEE Sensor and Ad Hoc Communications and Networks (SECON)*, Santa Clara, CA, Oct. 2004.
[17] A. Kansal, A. Somasundara, D. Jea, M.B. Srivastava, and D. Estrin, "Intelligent fluid infrastructure for embedded networks," in *ACM MobiSys'04*, Boston, MA, USA, June 2004, pp. 111–124.
[18] V. Kawadia and P. Kumar, "Power control and clustering in ad hoc networks," in *Proceedings of. IEEE INFOCOM'03*, San Francisco, CA, USA, Apr. 2003, pp. 459–469.
[19] H. S. Kim and T. F. Abdelzaher, "Minimum-energy asynchronous dissemination to mobile sinks in wireless sensor networks," in *ACM SenSys*, Los Angeles, CA, Nov. 2003.
[20] N. Li and J.C. Hou., "Topology control in heterogeneous wireless networks: Problems and solutions," in *Proceedings of IEEE INFOCOM'04*, Hong Kong, Mar. 2004.

[21] S. Lindsey and C. Raghavendra, “Pegasis: Power efficient gathering in sensor information systems”, in *Proc. of the Aerospace Conference*, vol. 3, pp. 1125-1130, 2002.
[22] J. Luo and J.-P. Hubaux, “Joint mobility and routing for lifetime elongation in wireless sensor networks,” in *Proceedings of IEEE INFOCOM’05*, Mar. 2005.
[23] J. Pan, L. Cai, T. Hou, Y. Shi, and X. Shen, “Optimal base-station locations in two-tiered wireless sensor networks,” to appear in IEEE Transactions on Mobile Computing, 2005.
[24] J. Pan, Y. T. Hou, Y. S. Lin Cai, and S. X. Shen, “Topology control for wireless sensor networks,” in *Proceedings of ACM Mobicom’03*, San Diego, CA, USA, Sept. 2003, pp. 286–299.
[25] V. Raghunathan, C. Schurgers, S. Park, and M. Srivastava, “Energy aware wireless microsensor networks,” *IEEE Signal Processing Magazine*, vol. 19, no. 2, pp. 40–50, Mar. 2002.
[26] R. Ramanathan and R. Rosales-Hain, “Topology control of multihop wireless networks using transmit power adjustment,” in *Proceedings of IEEE INFOCOM’00*, Tel Aviv, Israel, Mar. 2000, pp. 404–413.
[27] T. S.Rappaport, Wireless Commnications: Principle and Practice. Prentice Hall, 2002.
[28] S. Roundy, D. Steingart, L. Frechette, P. Wright, and J. Rabaey, “Power sources for wireless sensor networks,” in *Proc. of EWSN 2004, 1st European Workshop Wireless Sensor Networks*, Berlin, Germany, Jan. 2004, pp. 1–17.
[29] A. Sankar and Z. Liu, “Maximum lifetime routing in wireless ad-hoc networks,” in *Proceeding of IEEE INFOCOM’04*, Hong Kong, Mar. 2004.
[30] R. C. Shah, S. Roy, S. Jain, and W. Brunette, “Data MULEs: Modeling a three-tier architecture for sparse sensor networks. In *Proc., IEEE Workshop on Sensor Network Protocols and Applications (SNPA)*, pages 30-41, Anchorage, Alaska, USA, May 2003.
[31] K. Sohrabi, J. Gao, V. Ailawadhi, and G. Pottie, “Protocols for self-organization of a wireless sensor network,” *IEEE Personal Communications*, vol. 7, no. 5, pp. 16–27, Oct. 2000.
[32] L. Tong, Q. Zhao, and S. Adireddy, “Sensor networks with mobile agents,” in *MILCOM 2003 - IEEE Military Communications Conference*, vol. 22, no. 1, Boston, MA, Oct. 2003, pp. 688–693.
[33] Z. Vincze, D. Vass, R. Vida, A. Vidacs, and A. Telcs, ”Adaptive sink mobility in event-driven multi-hop wireless sensor networks”, submitted to IEEE INFOCOM’06, Barcelona, Spain, April 2006.
[34] Z. M. Wang, S. Basagni, E. Melachrinoudis, and C. Petrioli, “Exploiting sink mobility for maximizing sensor networks lifetime,” in *Proceedings of the 38th Hawaii International Conference on System Sciences*, Big Island, Hawaii, Jan. 2005.
[35] G. Wang, G. Cao, and T. Porta, “Movement-assisted sensor deployment”, in *Proceedings of. IEEE INFOCOM’04*, Hong Kong, 2004.
[36] [R. Wattenhofer, L. Li, P. Bahl, and Y. Wang, “Distributed topology control for wireless multihop ad hoc networks,” in *Proceedings of IEEE INFOCOM’01*, Anchorage, Alaska, USA, Apr. 2001, pp. 1388–1397.
[37] O. Younis and S. Fahmy, “Distributed clustering in ad-hoc sensor networks: A hybrid, energy efficient solution,” in *Proceedings of IEEE INFOCOM’04*, Hong Kong, 2004.
[38] O. Younis and S. Fahmy. “Heed: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor network”, *IEEE Transactions on Mobile Computing*, 3(4), October 2004.
[39] W. Zhao and M. Ammar, “Message ferrying: Proactive routing in highly partitioned wireless ad hoc networks,” in *Proc. of the 9th IEEE Workshop on Future Trends in Distributed Computed Systems (FTDCS’03)*, San Juan, Puerto Rico, May 2003, pp. 308–314.

[40] G. Zussman and A. Segall, “Energy efficient routing in ad hoc disaster recovery networks,” in *Proceedings of IEEE INFOCOM'03*, San Francisco, CA, USA, Apr. 2003, pp. 405–421.
[41] Q. Cao, T. F. Abdelzaher, T. He, and J.A. Stankovic, “Towards Optimal Sleep Scheduling in Sensor Networks for Rare Event Detection”, In *The Fourth International Conference on Information Processing in Sensor Networks*, April 2005.
[42] G. Lu, N. Sadagopan, B. Krishnamachari, A. Goel, "Delay Efficient Sleep Scheduling in Wireless Sensor Networks," *IEEE INFOCOM*, Miami, FL, March 2005.

**WB Electronics**

# BATTLEFIELD MANAGEMENT SYSTEM TROP FOR BRIGADE AND BELOW – IRAQ FREEDOM MISSION EXPERIENCES

FILTROWA 63
02-056 WARSZAWA
http://wb.com.pl

In the year 2004 in Poland, new Battlefield Management System for Battalion and Below was developed by WB Electronics and introduced in to Army use in coalition forces in Iraq. Main advantage of implementing TROP BMS, selected by Polish Armed Forces, is the increase of situational awareness and survivability of Land Forces units in combat environment. TROP development effort was based on open standards and modular design, whereas particular s/w routines were attachable as requested with great flexibility allowing for easy adaptation for various platforms and structures.

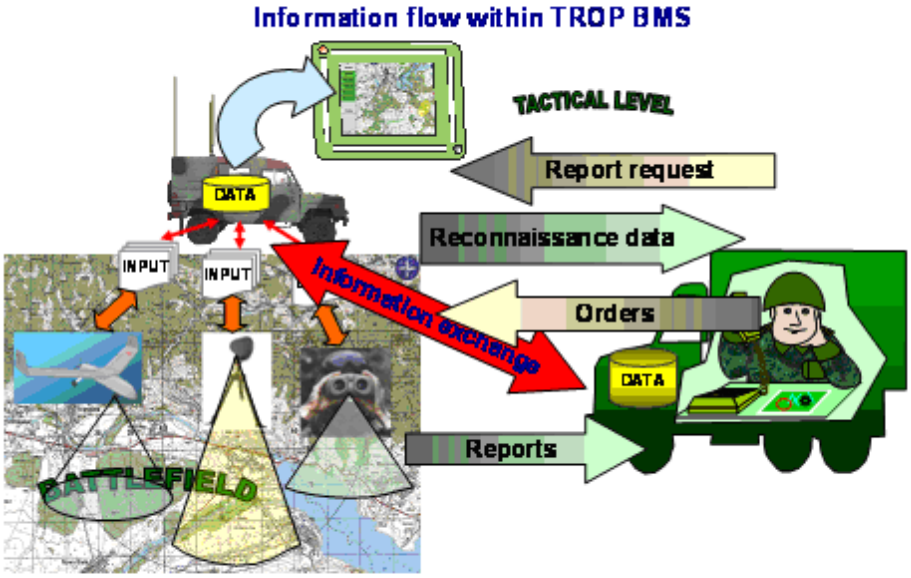



Fig. 1 Information flow within TROP BMS

Due to software modularity and openness of design, TROP BMS has required growth and upgrading potential. This can be achieved by fraction of new system cost by adding required in the future software modules to existing kernel and to installed

modules, to reflect upcoming needs to grow or upgrade caused by changes in hardware and doctrine.

Fig. 1 outlines data flow streams within TROP BMS and its position within higher echelon command structure of the Army.

TROP BMS can be easily integrated within division and army wide information structure, as all required data format information is readily available and data is transferable through defined data exchange channels. System can be also integrated within other (future) standard interfaced systems, after data interface and message exchange standards are implemented.

FONET communication system developed by WB Electronics is an integral part of company BMS development, providing robust mobile communication backbone for voice and data streams in the system. FONET input/output parameters are software defined and flexible, to accommodate various equipment and communication assets. FONET is the efficient and reliable medium of connection of sensors, measurement devices, Ethernet networks, computers, cable connections, telephone lines, transceivers and alike within particular vehicles, command posts and multiplatform military systems.

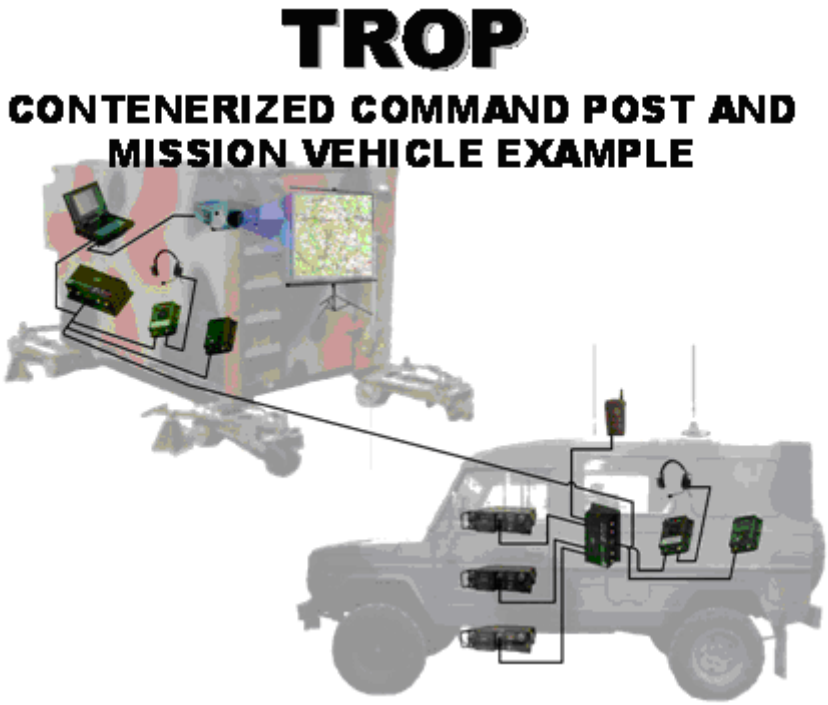



Fig. 2 Architecture of Company Command Post within Trop BMS

Due to FONET communication system modularity and ability of its interface functionality to be defined by software download, proposed system has required growth and upgrading potential. This can be achieved by fraction of new system cost by downloading required in the future software modules, to reflect upcoming needs to grow or upgrade caused by changes in hardware and doctrine. FONET central unit

Communication Server has Ethernet interface and IP addressability. System can be used for extended wide area communication networks with VoIP functionality. It is designed to be a pivotal element of modern network-centric battlefield management structures.

Connection between network elements at single platform is assured by 2 wire field cable and respective FONET communication system nodes/terminals, in larger, physically dispersed structures radio (HF, LOS) networks and other assets can be used. Communication within FONET network is digital, pulse modulated, providing required voice and data channels simultaneously within one 2 wire cable. The same cable is also used for power supply and network control purposes. In WB Electronics design, FONET intercom based network was selected to establish communication structure of proposed FCCS.

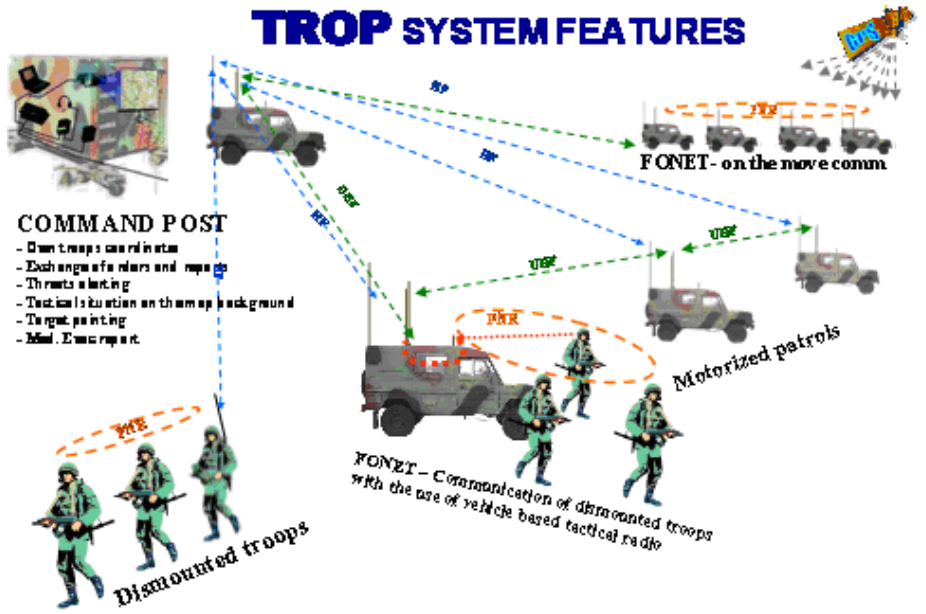



Fig. 3 TROP BMS radio networks overwiev

WB Electronics FCCS architecture is based on independent node structure (peer-to-peer) dispersed in physical battle-space with maximum of functionality available at any of nodes. Network nodes consist of respective Computer Units incorporating attached FONET communication servers. Nodes are interchangeable and redundant, and system architecture can be reorganized after minor software modification executed even in field conditions by authorized personnel. Any segment of the structure including required number of vehicles, can be operated independently for higher unit survivability and effectiveness. Respective number of radio nets (or cable/radio nets) provide communication within the structure. Lower echelon nets are subordinated to higher ones. All networks convey data streams and voice messages in common channel, with priority given to voice messages and urgent data alerts and

messages over standard combat situation update data. If redundant data transmission channels are provided, system automatically selects fastest available data channel. Application of intelligent network protocols within TROP BMS limits data transmission overhead to the minimum, in order to speed up data delivery, and reduce required radio asset count. Special attention is given to data security and data delivery robustness, to avoid errors and mismatches and resulting fatalities in artillery operation. Design error rate of used protocol is better than 10 -6 (one in a million). All mentioned measures result in exceptional stability and dependability of proposed BMS architecture.

In Polish Armed Forces Iraq mission TROP BMS was primarily used to improve situational awareness of fighting forces and increase the effectiveness of med evac and recovery measures when used during patrolling and convoy tasks in hostile environment with the presence of asymmetric threats. Large number of missions supported by TROP BMS were executed in perimeter of ca. 70 km. from home base with the application of UHF and HF radio assets (Thales PR4G and Harris 5800). Detailed combat experience based feedback material was collected and resulting conclusions have led to updates of the BMS TROP software and hardware components. Analysis of experience draws following conclusions:

- TROP BMS application increased significantly battlefield situational awareness of deployed troops
- Activities co-ordination of involved forces, especially between patrolling land forces and helicopters improved
- Recovery and Med. Evac. effectiveness improved
- HF radio asset deployment is essential, after vehicles move far beyond LOS asset reach
- Routine work – order issuing, reporting, event records etc. was made easier, leaving more time for individual command and troops initiative

General recommendation is BMS TROP feasibility for broad use in Land Forces with every vehicle to be equipped with GPS receiver, UHF and HF radio assets, the FONET intercom system and TROP computer terminal.

**Zoltán SZENTPÁL, László ZÖMBIK**

# ATTACKS AGAINST ANONYMIZER NETWORKS

Zoltán Szentpál[235] , László Zömbik[236]

Anonymizer networks are used to hide the communication of the user from local networks and to assure that the location of the user node remains unknown from remote networks. Anonymizer networks become more and more popular in the civil communication since it seems that the identity of the communicating peers remain hidden. Therefore, these networks can even be used for military or intelligence communication too237 . In this paper we show the limits of these networks as we introduce our specific attacks against the anonymity of the users of these networks.

## 1 Introduction

In a number of cases it might be important for the users to communicate securely over the Internet. Encrypting and authenticating the user's traffic does not solve all the problems, because they are not sufficient for protecting the location and identification of the user. The IP header information, which is necessary for routing, is not encrypted. Thus, looking into the packet header is the simplest attack against anonymity. To prevent it, the IP headers are masqueraded by using different methods, like Network Address Translation (NAT) or proxies, etc. However, there are other kind of attacks based on traffic analysis. Traffic analysis can be used to infer who is talking to whom over a public network, even if the packets are encrypted and the headers are masqueraded. Traffic analysis allows Internet service providers or unauthorized intermediaries to threaten the user's privacy as they can track the user's behaviour and interest. An anonymizer network distributes the user's transactions over several nodes in the Internet to reduce the risks of traffic analysis, so to try to prevent backtracing the user and its connection to destinations. There are some methods that make backtracing of the user possible even if the user encrypts, authenticates and "anonymizes" its traffic.

In chapter two, we describe two anonymizer networks. In chapter three, we introduce the theory and the implementation of our attacks. In chapter four, we show the results measured on the earlier described anonymizer networks. In chapter five, we also present measurements, based on non-TCP traffic.

## 2 Anonymizer networks

An anonymizer network usually consists of various proxy servers. A proxy server is a server that sits between a client application, such as a Web browser, and a server. It intercepts all requests to the server, changes the source IP address of the packets and then forwards the requests to the server. Proxy servers can be public or private and they can form a chain in the anonymizer network. The traffic of the user is

[235]Department of Telecommunication and Media Informatics, BUTE, Budapest

[236]Ericsson Hungary, Department of Telecommunication and Media Informatics, BUTE, Budapest

[237]The Tor network is used by the US Navy. - What The Hack conference, 2005

routed through these servers, either encrypted between each server or not (Figure 1). The source IP address of the packets is changed every time they pass through a proxy server so it is nearly impossible to determine the original source address at the end.

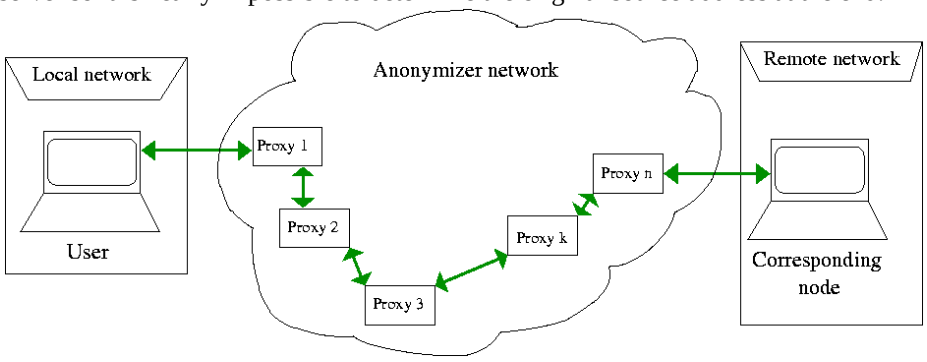



Figure 1: A typical anonymizer network.

There are a lot of client software using anonymizer networks and providing some level of anonymity to the user. Most of them support only Microsoft Windows operating systems.

The most popular networks are the following:

- Steganos Internet Anonym Pro 7 [**Hiba! A hivatkozási forrás nem található.**]
- Bypass Proxy Client [**Hiba! A hivatkozási forrás nem található.**]
- Anonymizer 2004 [**Hiba! A hivatkozási forrás nem található.**]
- GhostSurf 2005 Platinum [**Hiba! A hivatkozási forrás nem található.**]
- Tor [**Hiba! A hivatkozási forrás nem található.**]

In this paper we selected the latter two networks for analysis.

### 2.1 GhostSurf 2005 Platinum

GhostSurf 2005 Platinum is a collection of software tools that improve the user's privacy and anonymity in the Internet. It supports only the Microsoft Windows operating system and it is distributed as a closed source, non-free software238 . It uses GhostSurf's own private proxy servers which are spread over the world. This solution is on the one hand good for performance and speed (public proxies are often unstable and slow). On the other hand they are not optimal for the user's privacy, as using private proxies makes observation or even logging of the traffic of users possible for the Anonymizer Company. However, they claim that nothing is ever cached. The resistance of this anonymizer network against our attacks is discussed in section 4.1.

### 2.2 Tor

Tor is a multi-platform anonymizer toolset, supporting the most popular operating systems. It is distributed as an open source, free software under the 3-clause BSD license [**Hiba! A hivatkozási forrás nem található.**]. Tor uses a distributed, anonymous network of servers, hosted by volunteers. Data packets on the Tor network take a random pathway through these servers that cover the user's tracks so no observer at any single point can tell what the source and destination of the data is. To create a private pathway with Tor, the user's client software builds a circuit of

[238]In the measurements the free trial version of the software was used.

encrypted connections through servers on the network using onion routing (Figure 2). Each server along the way knows only the forwarding node and the next hop node. No individual server ever knows the complete path that an IP packet has taken. Tor only works for TCP streams and can be used by any application with SOCKS support. The Tor network's resistance against our attacks is discussed in section 4.2.

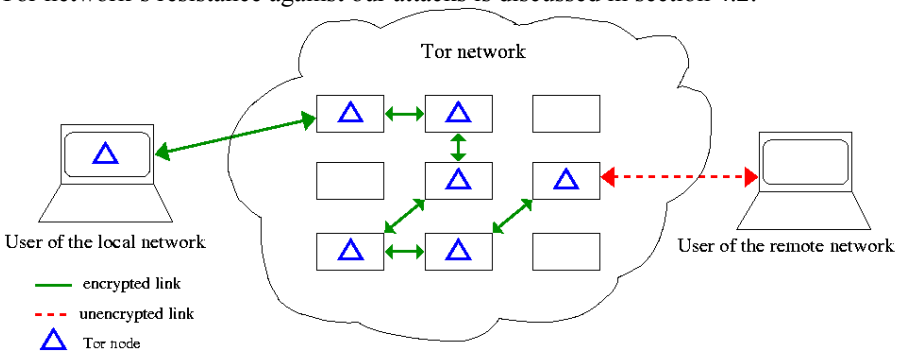


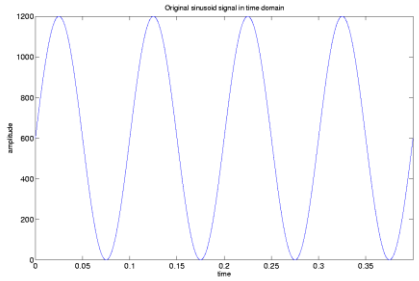

Figure 2: The Tor network.

## 3 The theory of attacks

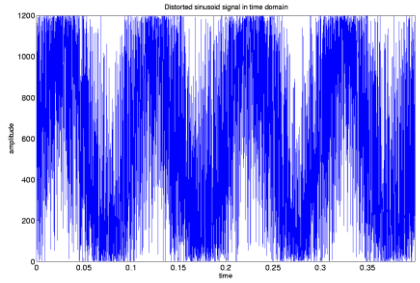
In this section we show the background of our method that makes traffic analysis and therefore backtracing of the user possible in spite of using any kind of anonymizer network.

The Fourier transform of a sinusoid signal has a peak at the frequency of the sinusoid signal in frequency domain. This fact makes the identification of the sinusoid signal easy in frequency domain, even if the signal is significantly distorted.

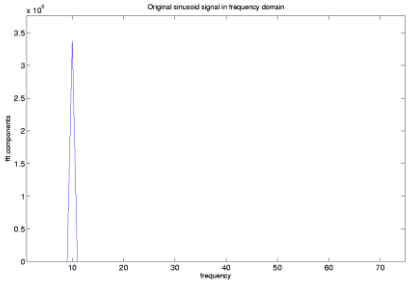
As an example let's have the original signal: 600 □□sin(2□□□□10 □□t) + 600. The distorted signal is the original signal with an additive white noise (Figure 3). It can be seen in the figures that it is much easier to determine the similarity between the original and distorted signals in frequency domain than in time domain. The distorted signal hardly looks like the same as the original signal in time domain, but its power spectrum has a peak at 10 Hz as well as the original signal's power spectrum.



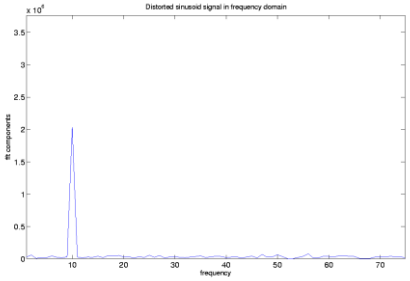

(a) Original sinusoid signal in time domain.




(b) Distorted sinusoid signal in time domain.




(c) Original sinusoid signal in frequency domain.




(d) Distorted sinusoid signal in frequency domain.

Figure 3: Sinusoid signals in time and frequency domain.

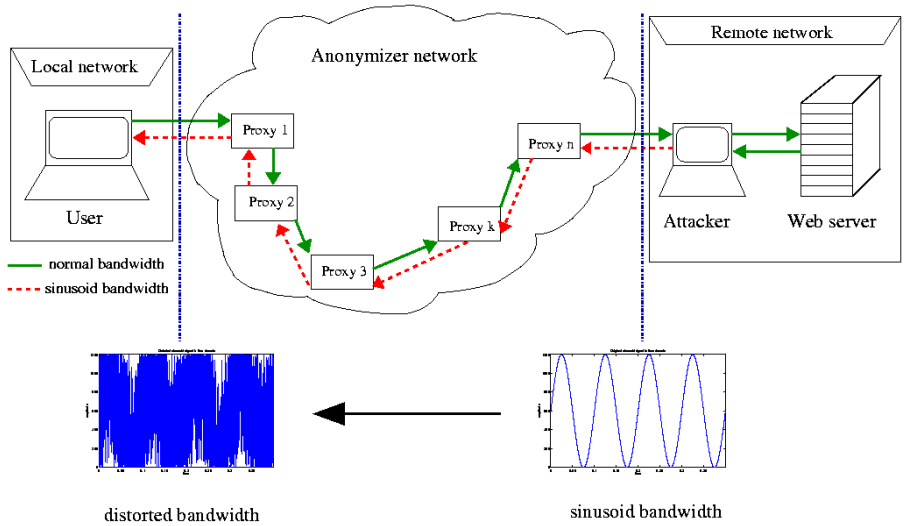



Figure 4: The principle of the attack.

This fact can be used to backtrace the user who communicates through an anonymous network without knowing its real IP address. What we can make ”sinusoid” easily in case of TCP traffic is the bandwidth of the traffic that goes to the user. So we need for example an intermediate router that sends out the packets in a way that the bandwidth of the packets form a sinusoid signal in time domain. Let us suppose that the user wants to download a file from a server. In the network where the server is, the attacker distorts the traffic, so that the bandwidth of the traffic will arrive altered to the user (Figure 4). With this method the attacker can find out where the packets from the server are going, even if the user anonymizes its traffic.

### 3.1 The implementation of the attacks

As it can be seen in Figure 4, in order to successfully launch the attacks we need to access the traffic at both ends of the anonymizer network: at the server side and in the local network of the user. Then we compare the two traffic in frequency domain and analyze the results. If they match then we got the location of the user. If not, then we have to observe different local networks until the power spectrum of the local traffic matches the power spectrum of the server side traffic.

Figure 5 shows our implementation of the server-side hosts. To minimize hardware requirements the Xen virtualization technology [**Hiba! A hivatkozási forrás nem található.**] was used to emulate a network and hosts on one physical computer. All of the host were running the Debian GNU/Linux [**Hiba! A hivatkozási forrás nem található.**] operating system. The host that actually did bandwidth shaping was the router host, running NTMF. NTMF stands for Network Traffic Manipulation Framework [**Hiba! A hivatkozási forrás nem található.**], which is a protocol testing framework. NTMF allows low-level access to the packets transmitted by the linux kernel, thus making it possible to shape the bandwidth of the outgoing traffic. The physical host (”domain 0”) and the web server were in different networks, they communicated with each other through the router host. The router host forwarded the traffic to the web server, so there was no bandwidth manipulation in the direction

”eth0” to ”eth1”. However, in the other direction the interarrival time was modified, so that the bandwidth followed a sinusoid signal in time domain.

The bandwidth-time function had the following form: A + C □□sin((2□□□□□□□□f □□n). The values are:

- A is the DC component of the bandwidth in Kbyte/s.
- C is the amplitude of the sinus in Kbyte/s.
- 1/N is the time quantum.
- f is the frequency of the signal in Hz.
- n/N is the elapsed time in seconds since the last packet was sent out.

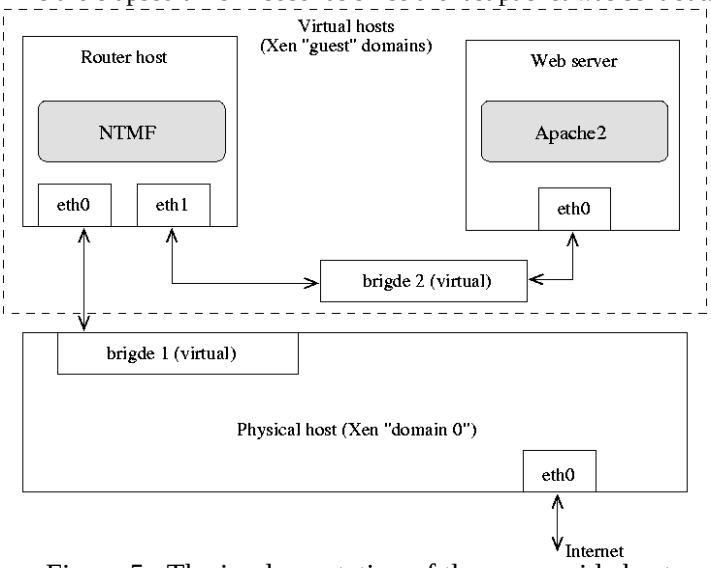
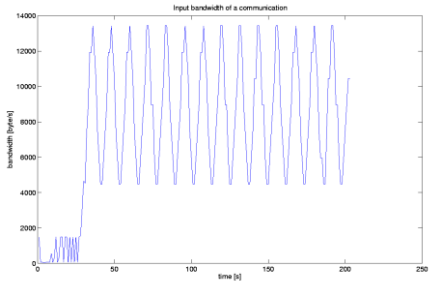



Figure 5: The implementation of the server-side hosts.

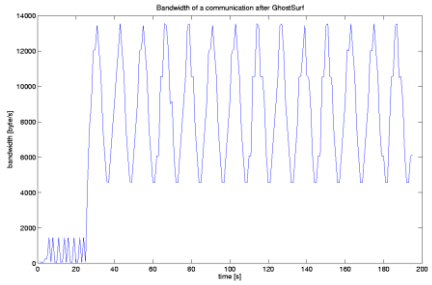
## 4 Identified communication

In both anonymizer networks the Microsoft Windows XP client software was tested, the packets were dumped with Ethereal [**Hiba! A hivatkozási forrás nem található.**] on the client side and with Tcpdump [**Hiba! A hivatkozási forrás nem található.**] on the server side. The Awk [**Hiba! A hivatkozási forrás nem található.**] text-processing programming language was used for manipulating the text files of the captured traffic. The results were calculated and displayed with Matlab [**Hiba! A hivatkozási forrás nem található.**].

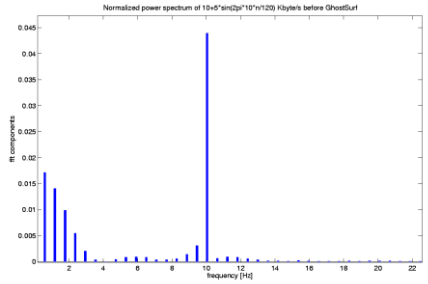
## 4.1 GhostSurf 2005 Platinum



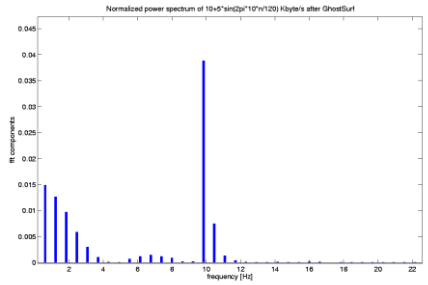

(a) Input bandwidth.




(b) Bandwidth after GhostSurf.




(c) Power spectrum of the input bandwidth.

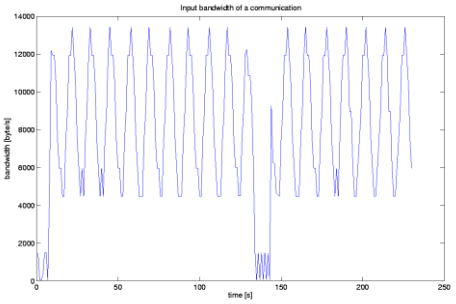



(d) Power spectrum of the bandwidth after GhostSurf.

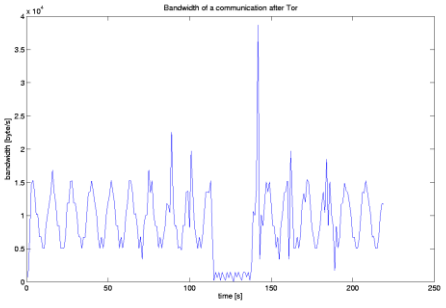
Figure 6: GhostSurf 2005 Platinum: 10 [Kbyte/s] + 5 [Kbyte/s] $\cdot\sin((2\pi/120) \cdot 10 \cdot n)$ in time and frequency domain.

Figure 6 shows the input of anonymizer networks, a 10 Hz sinusoid signal of the bandwidth: 10 [Kbyte/s] + 5 [Kbyte/s] $\sin((2\pi/120) \cdot 10 \cdot n)$ in time domain and its power spectrum in frequency domain; and the bandwidth of an unknown output traffic of the GhostSurf network in time domain and its power spectrum in frequency domain. It can be seen that the power spectrum of the input traffic matches quite well to the power spectrum of the unknown traffic originating from the anonymizer network. This means, that this anonymizer network only slightly modifies the bandwidth of the traffic so its sinusoid character is kept. That is, the anonymity of the user can be revealed.

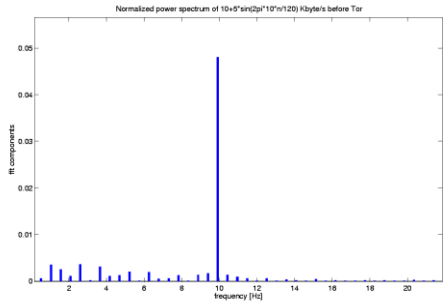
### 4.2 Tor



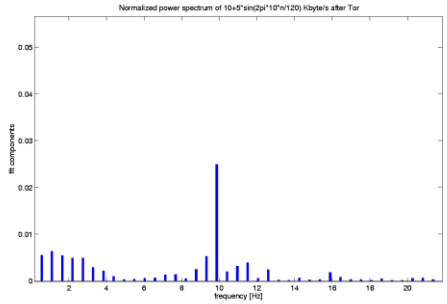

(a) Input bandwidth.




(b) Bandwidth after Tor.

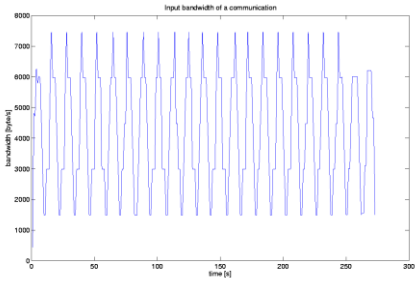



(c) Power spectrum of the input bandwidth.

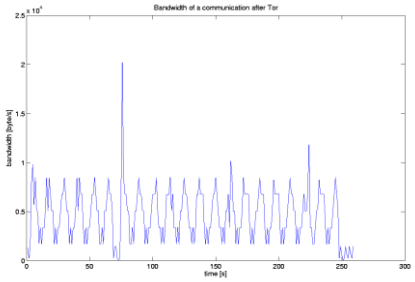



(d) Power spectrum of the bandwidth after Tor.

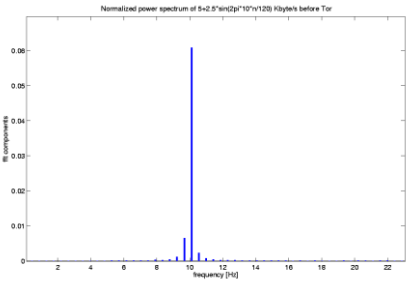
Figure 7: Tor: 10 [Kbyte/s] + 5 [Kbyte/s] ·sin((2π/120) · 10 · n) in time and frequency domain.



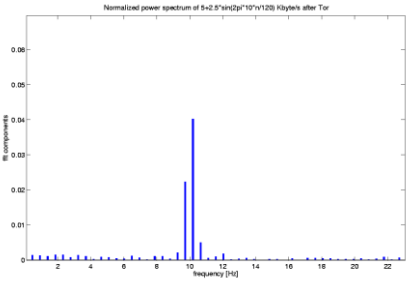

(a) Input bandwidth.




(b) Bandwidth after Tor.




(c) Power spectrum of the input bandwidth.




(d) Power spectrum of the bandwidth after Tor.

Figure 8: Tor: 5 [Kbyte/s] + 2.5 [Kbyte/s] ·sin((2π/120) · 10 · n) in time and frequency domain.

In the Tor network two measurements were made. Figure 7 shows the following input signal: 10 [Kbyte/s] + 5 [Kbyte/s] sin((2π/120) · 10 · n) and an output signal of Tor in time domain and their power spectrums in frequency domain. Figure 8 shows different input and distorted traffic: 5 [Kbyte/s] + 2.5 [Kbyte/s] □sin((2□□□□□□□□□□10 □□n) in time domain and their power spectrums in frequency domain. The frequency of both signals is 10 Hz. In spite of the fact that the Tor network modifies the sinusoid bandwidth quite a lot, the power spectrum of the original bandwidth is still recognizable. This means that even the Tor network doesn't protect its users from these type of attacks.

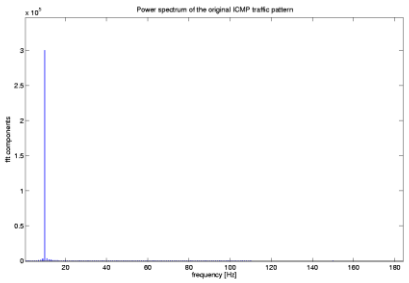
## 5 Traffic patterns for non TCP-based communication

Anonymizer networks are mostly used to hide mail and web traffic, that is, they use the TCP protocol. In this section we show some results when the ICMP and the connection-less UDP protocols are used instead of the TCP protocol. These measurements are different from the above described. Since the anonymizer networks support only TCP streams, no anonymizer network was used in these measurements. However, NATs hide the originators of non-TCP traffic, thus we can apply our methods. Since NATs similarly distort the traffic as an IP router, the delay or loss of the packets produced by the routers in the Internet gave similar results. The other difference from the TCP-based measurements is, that not the bandwidth of the traffic was sinusoid. First, some trace traffic patterns were created in both ICMP and UDP cases. The packet sizes in the patterns followed a 10 Hz sinus signal. Then, these traffic patterns were sent from a local network node to a DSL node: either with ping (ICMP case) or with jtg [**Hiba! A hivatkozási forrás nem található.**] (UDP case). The traffic was captured with tcpdump at both ends, awk was used for manipulating the text files of the captured traffic. The results were calculated and displayed with Matlab.

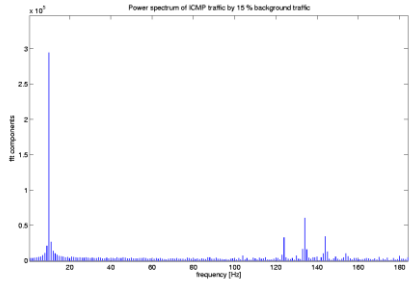
### 5.1 ICMP

Figure 9 shows the power spectrum of the original traffic pattern and the received traffic patterns at the receiver side. A traffic pattern of constant packet sizes produced the ICMP background traffic, where the amount of packets influenced the rate. 15 % background traffic was used in the first case and 400 % in the second case. This means, that in the second case four times more packets originated from the background traffic pattern, than from the original traffic pattern out of all captured packets.

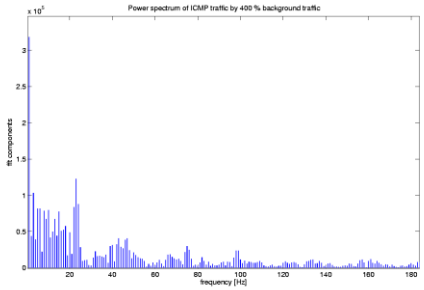
In the case of 15 % background traffic the results are convincing: the 10 Hz component can be identified easily. This means that the user can be backtraced perfectly. In the second case the power spectrum of the received traffic is spread, so it is hard to identify that the received pattern originates from the 10 Hz traffic pattern. That is, by such an amount of ICMP background traffic the user can not be backtraced certainly.




(a) Power spectrum of the original ICMP traffic pattern.




(b) Power spectrum of ICMP traffic by 15% background traffic.



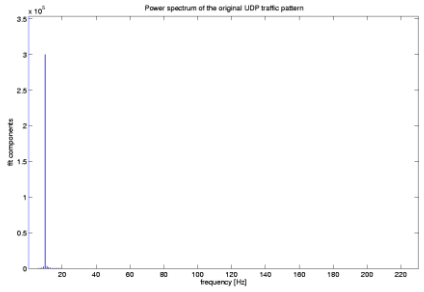

(c) Power spectrum of ICMP traffic by 400% background traffic.

Figure 9: Power spectrums of ICMP traffic.

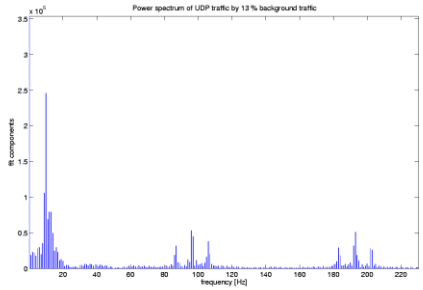
### 5.2 UDP

Figure 10 shows the power spectrum of the original traffic pattern and the received traffic patterns at the receiver side. 13 % UDP background traffic was used in the first case and 200 % in the second case.

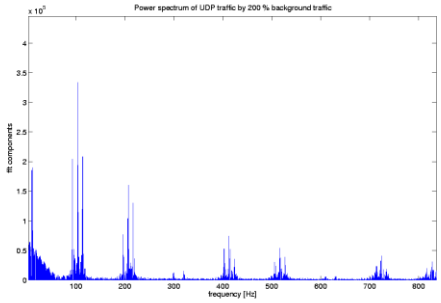
In the case of 13 % background traffic the 10 Hz component can be identified easily, despite the lower energy periodic harmonics at around 90, 190 Hz. This means again that the user can be backtraced. In the second case the power spectrum of the received traffic has some very large energy periodic harmonics so it is hard to identify that the received pattern originates from the 10 Hz traffic pattern. That is, by such an amount of UDP background traffic the user can not be backtraced certainly.



(a) Power spectrum of the original UDP traffic pattern.




(b) Power spectrum of UDP traffic by 13% background traffic.




(c) Power spectrum of UDP traffic by 200% background traffic.

Figure 10: Power spectrums of UDP traffic.

## Conclusion

In this paper a method was introduced, that uses the TCP protocol to backtrace the user of an anonymizer network. Furthermore, we presented a method that uses either the ICMP or the UDP protocol to identify the user. The first method gave quite similar and usable results in all measurements, while the second method depended much on the networking circumstances (for example the amount of background traffic). Apart from this, both methods effectively make the victim traceable, therefore the anonymity is not entirely assured in these networks.

## References


[1] Steganos Internet Anonym Pro 7, http://www.steganos.com
[2] Bypass Proxy Client, http://www.bypass.cc
[3] Anonymizer 2004, http://www.anonymizer.com
[4] GhostSurf 2005 Platinum, http://www.tenebril.com
[5] The Tor Anonymizer Network, http://tor.eff.org
[6] A 3-clause BSD-style license, http://www.gnu.org/licenses/info/BSD_3Clause.html
[7] The Xen virtual machine monitor, http://www.cl.cam.ac.uk/Research/SRG/netos/xen
[8] Debian - The Universal Operating System, http://www.debian.org
[9] Real-time Network Traffic Manipulation Framework for Protocol Testing, MSc Thesis, Balázs Lécz, Budapest, 2005, http://ntmf.sourceforge.net
[10] Ethereal Network Protocol Analyzer, http://www.ethereal.com
[11] Tcpdump, http://www.tcpdump.org

[12] The Awk text-processing programming language, http://www.gnu.org/software/gawk/gawk.html
[13] MATLAB - The Language of Technical Computing, http://www.mathworks.com
[14] J. Manner ”Jugi’s Traffic Generator”, http://www.cs.helsinki.fi/u/jmanner/software/jtg



Az **Ericsson Microwave Systems AB** az Ericsson meghatározó vállalata a védelmi elektronika és a mikrohullámú távközlés területén.

Az **Ericsson Microwave Systems AB** a harctéri információs fölényt biztosító, NATO-kompatibilis, részekből felépíthető, rugalmas hálózatok tervezője és gyártója.

A vállalat portfóliójában megtalálható a többfunkciós, többsugaras korszerű radartechnológia a légierő, a légvédelem, a szárazföldi erők és a tüzérség részére, továbbá UHF relék, érzékelők, különböző stratégiai hálózati környezetben működő védett harcászati hírközlő és informatikai rendszerek.

Megoldásaink egyik meghatározó eleme, hogy korszerű javító és támogató szolgáltatásokat kínálunk a nagy költségigényű tartalék alkatrészek raktározása helyett.

**További információ:**
Gauland János
Igazgató, kormányzati kapcsolatok
Ericsson Magyarország
1037 Budapest, Laborc utca 1.
Telefon: 437-7813
E-mail: Janos.Gauland@ericsson.com

ERICSSON
TAKING YOU FORWARD

**Ericsson Magyarország**
1037 Budapest, Laborc utca 1.
Telefon: 437-7100
Fax: 437-7467
E-mail: valaszolunk@ericsson.com
www.ericsson.com/hu

# III. FEJEZET

## A NEMZETKÖZI TUDOMÁNYOS SZAKMAI KONFERENCIA HÁTTÉR INFORMÁCIÓI

*A konferencia fővédnöke:*

- Mikita János mk. altábornagy, HM Honvéd Vezérkar vezérkari főnök helyettes

*A konferencia védnökei:*

- Prof. Dr. Szabó Miklós akadémikus, ZMNE rektor
- Horváth Ferenc dandártábornok, MH Híradó és Informatikai Parancsnokság parancsnok

*A konferencia kommunikációs partnere:*

- Magyar Telekom Részvénytársaság

*A konferencia támogatói:*

- SIEMENS Rt.
- Kapsch Telecom Kft.
- FERCOM Kommunikációs Kft.
- Thales Communications
- CISCO Systems Magyarország Kft.
- ERICSSON Magyarország Kft.
- WB Electronics

*A konferencia rendezői:*

- Zrínyi Miklós Nemzetvédelmi Egyetem Híradó Tanszék
- Honvéd Vezérkar Katonai Tervező Főcsoportfőnökség
- 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. Lehel György ezredes
- Dr. Rajnai Zoltán mk. alezredes
- Szöllősi Sándor okl. mk. őrnagy
- Kis Lajos mk. százados

**ALCATEL**

# END TO END NETWORK-CENTRIC SERVICES, THE NEEDED "BIG PICTURE" APPROACH TO DEFENSE NETWORKING



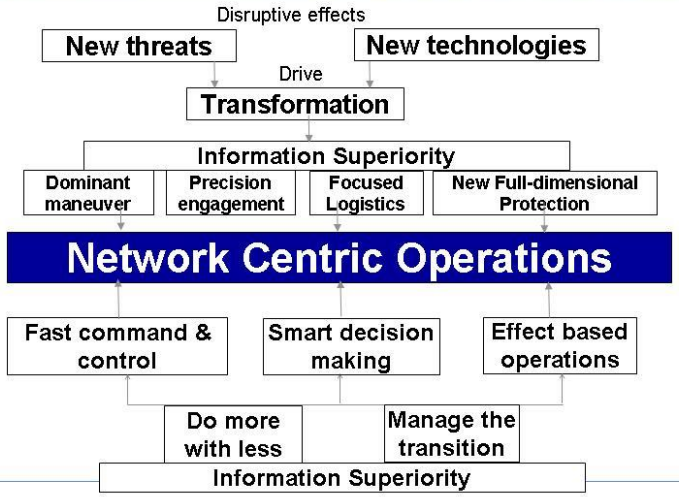




- The needs: Network Centric Operations
- An architecture framework for common services
- Case studies: NCO-aligned projects


All rights reserved © 2005, Alcatel

## Delivering Security in a changing world: Network Centric Operations

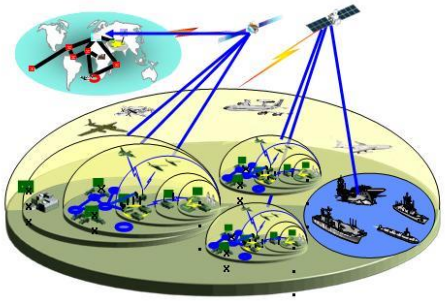


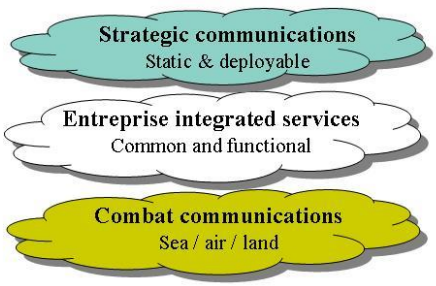


All rights reserved © 2005, Alcatel

## Network Centric Operations drives a convergence of communication and IT services …

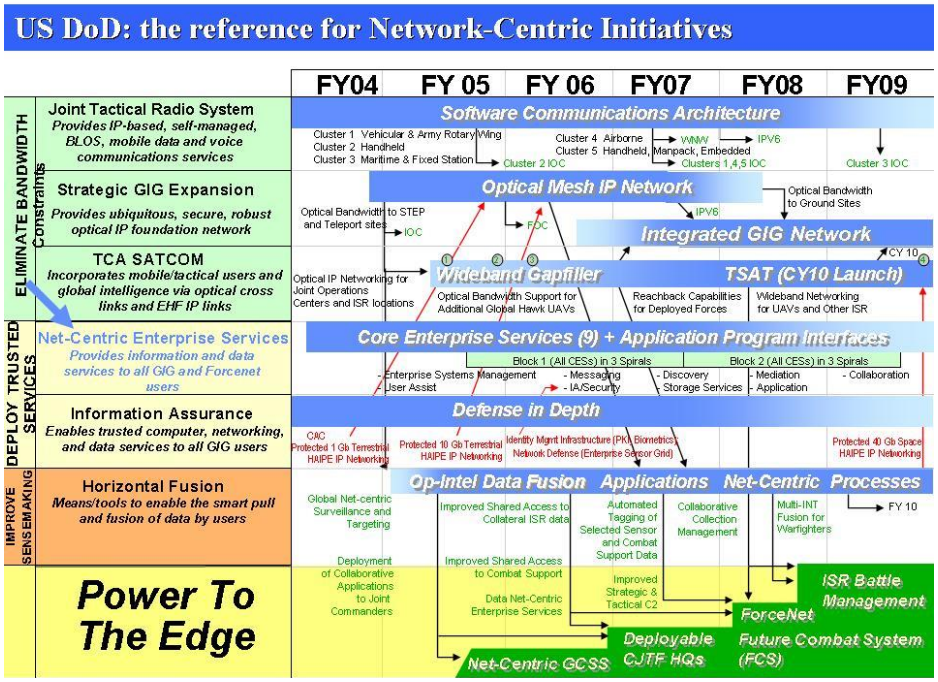
… that turns the complexity of the military world into end to end capabilities

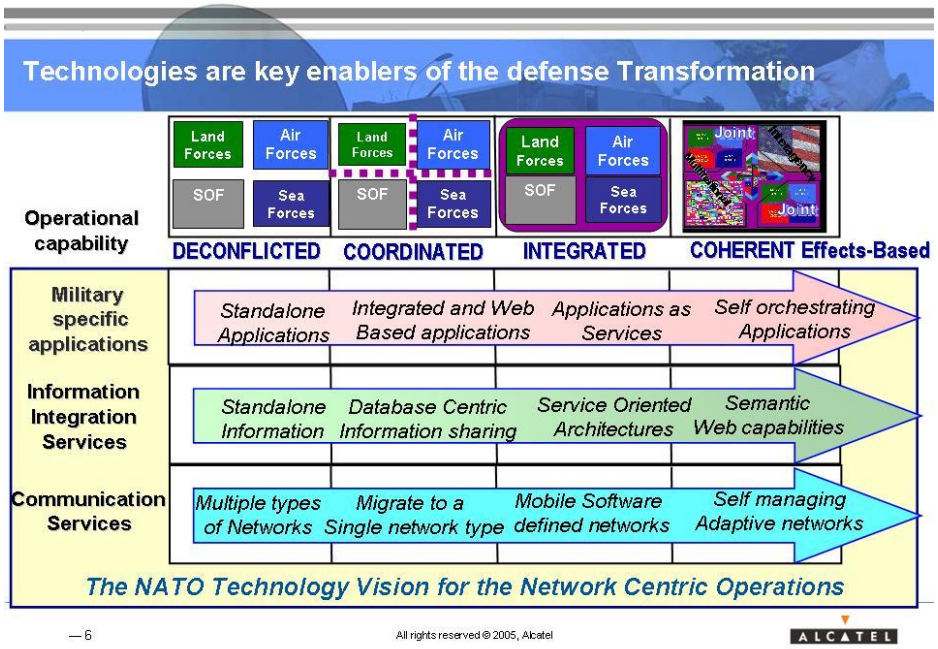






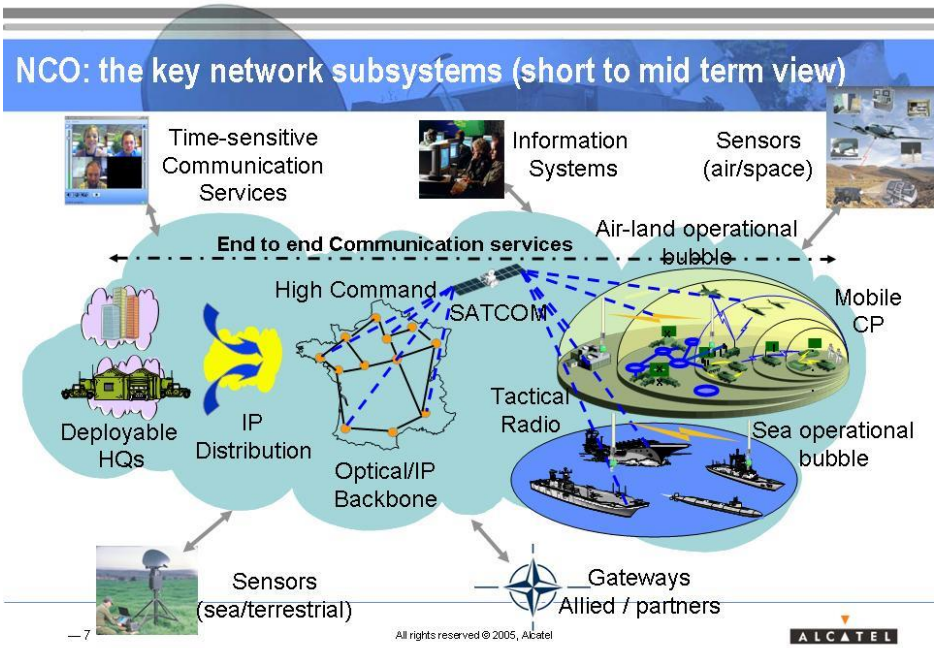
All rights reserved © 2005, Alcatel





All rights reserved © 2005, Alcatel



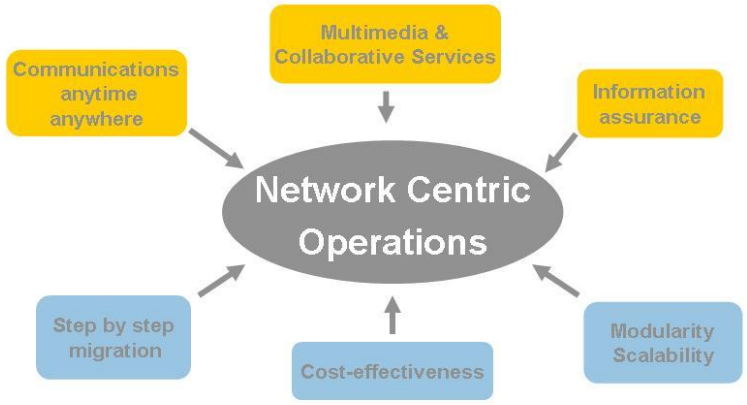




- An architecture framework for common services


All rights reserved © 2005, Alcatel

## NCO: Key drivers and success factors





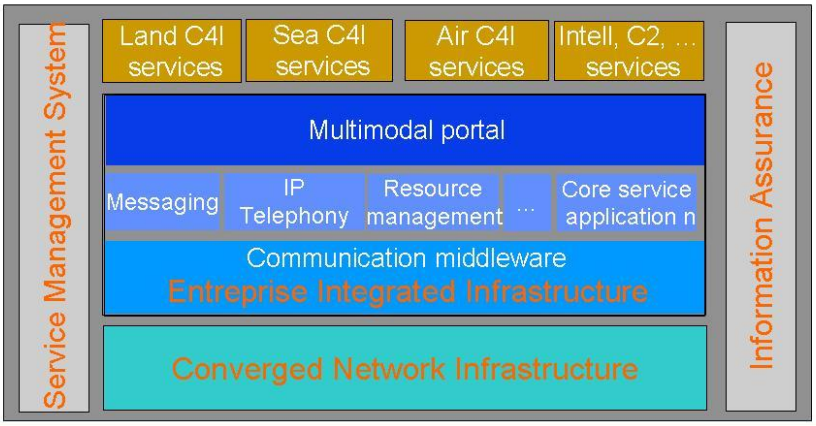
All rights reserved © 2005, Alcatel

## Objectives for an architecture for common services

- ***Automated information sharing…***
  - Fully interconnected and secured networks
  - User friendly global access to the "common" Information Systems
  - unified platforms for time-sensitive collaborative services and access to other applications & data bases
  - Compatible with field operations
  - Interoperability gateways with Allied & International organisations
- ***Towards a realistic target***
  - Migration is key from legacy IS/Telecom to common networks & services
  - National security rules & regulations must be followed
  - Operational support to be taken into account (including for OOA ops)
- ***Based on latest technologies***
  - Best of breed state of the art technologies (IP, SIP, SOAP, XML…)
  - Providing an open infrastructure for services
  - Future proof


All rights reserved © 2005, Alcatel

## The key building blocks of a conceptual architecture for unified access to common services





All rights reserved © 2005, Alcatel

## An architecture based on *Service Delivery Platforms* to unify access and management of communication services

***Application platform***

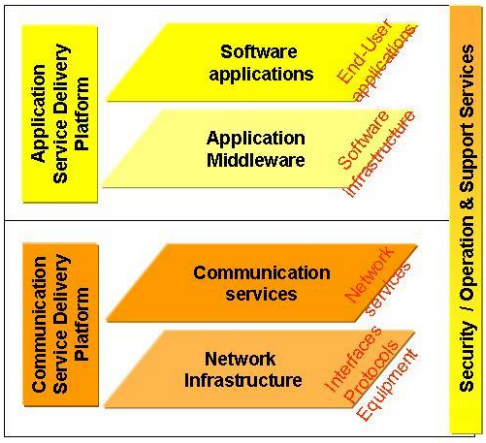
- Goal: unify access to end-user applications
- Tool: Web-oriented standardized & scalable service delivery middleware (Software infrastructure) for easy application services integration

***Communication platform***

- Goal: end to end network services converged over IP with quality of service and data integrity
- Tool: network infrastructure offering connectivity together with performance based on capacity simulation and planning

***Common functions***

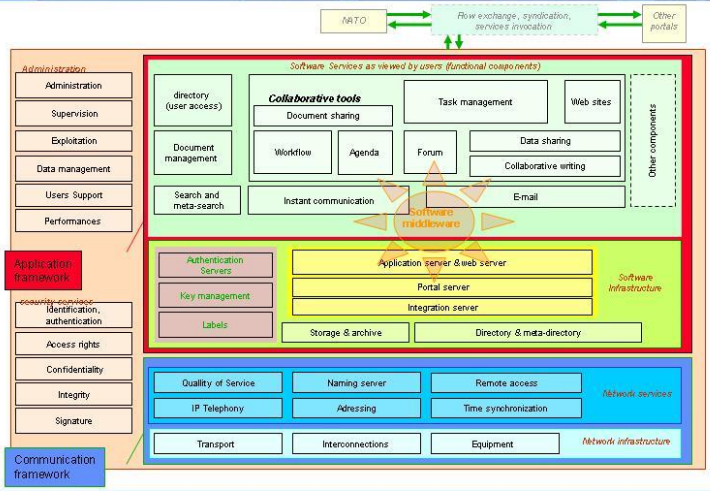
- Operation & Support Services (OSS)
- Security





All rights reserved © 2005, Alcatel

## Architectural components of the Application Service Delivery Platform

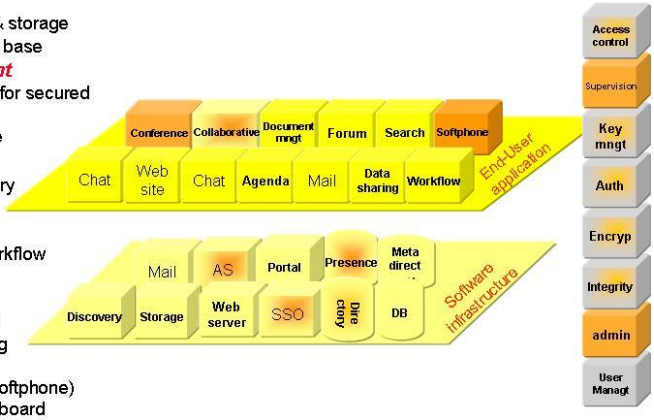




All rights reserved © 2005, Alcatel

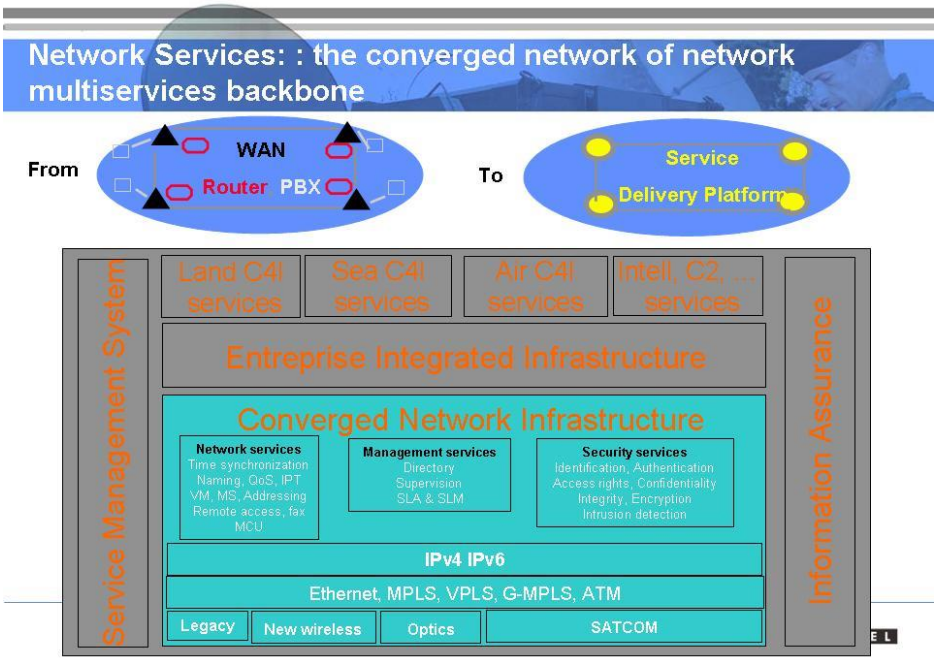
## Key sets of common services delivered by the application Service Delivery Platform

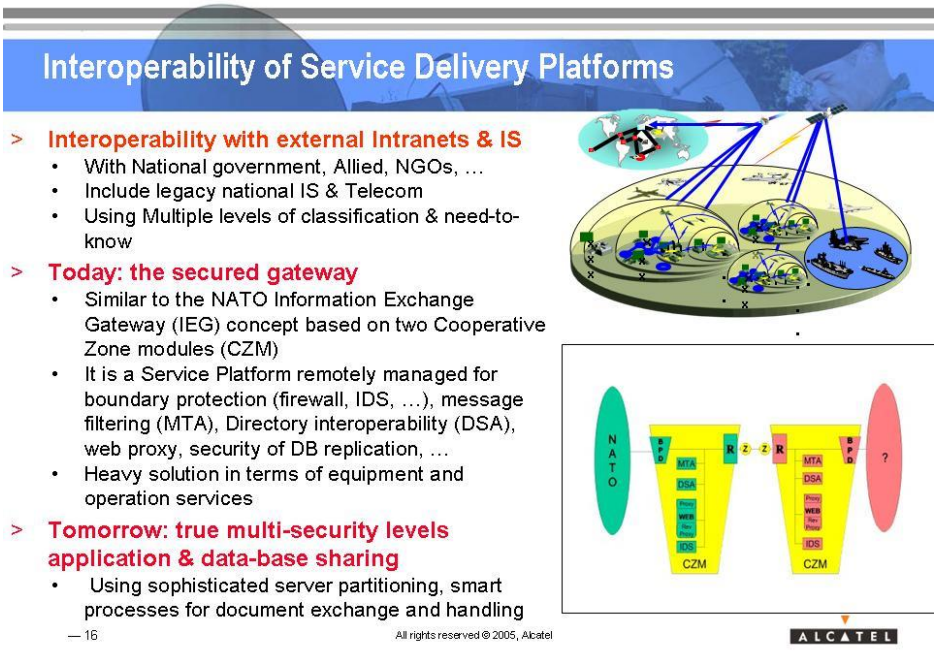
- ***Data management***
  - Smart data replication & storage
  - Secured access to Data base
- ***e-Document Management***
  - Use of labelling/tagging for secured document handling
  - Secured Search Engine
- ***Directory***
  - Unified « Meta »-directory
  - Single-Sign-On
- ***Collaborative tools***
  - Document sharing & workflow
  - e-Mail
  - Agenda
- ***Instant communications***
  - audio/video conferencing
  - Presence
  - Multi-modal terminals (softphone)
  - Forum, web chat, white-board





All rights reserved © 2005, Alcatel


Network Services: : the converged network of network multiservices backbone
From
WAN
Router PBX
To
Service
Delivery Platform
Service Management System
Land C4I services
Sea C4I services
Air C4I services
Intell, C2, … services
Entreprise Integrated Infrastructure
Converged Network Infrastructure
Network services
Time synchronization
Naming, QoS, IPT
VM, MS, Addressing
Remote access, fax
MCU
Management services
Directory
Supervision
SLA & SLM
Security services
Identification, Authentication
Access rights, Confidentiality
Integrity, Encryption
Intrusion detection
IPv4 IPv6
Ethernet, MPLS, VPLS, G-MPLS, ATM
Legacy
New wireless
Optics
SATCOM
Information Assurance


Interoperability of Service Delivery Platforms
> Interoperability with external Intranets & IS
• With National government, Allied, NGOs, …
• Include legacy national IS & Telecom
• Using Multiple levels of classification & need-to-know
> Today: the secured gateway
• Similar to the NATO Information Exchange Gateway (IEG) concept based on two Cooperative Zone modules (CZM)
• It is a Service Platform remotely managed for boundary protection (firewall, IDS, …), message filtering (MTA), Directory interoperability (DSA), web proxy, security of DB replication, …
• Heavy solution in terms of equipment and operation services
> Tomorrow: true multi-security levels application & data-base sharing
• Using sophisticated server partitioning, smart processes for document exchange and handling
NATO
MTA
DSA
IDS
R
Z
CZM
?
— 16
All rights reserved © 2005, Alcatel
ALCATEL

## Security of Service Delivery Platforms

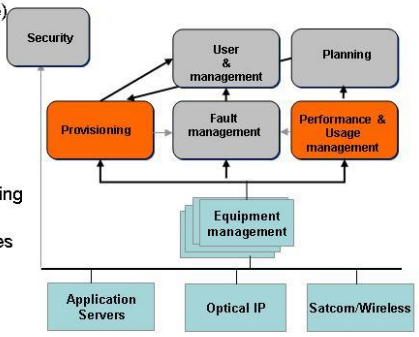
> *Comprehensive security architecture covering …*

- **National Security Agency** needed certifications
- **Network**: IPv6, QoS aware encryption, packet header compression, …
- **Application middleware**
  - Securing messages exchanges between servers with WS Reliable Messaging (WS Trust, WS Federation, SAML technologies), Securing web data exchange using HTTPS protocol, Securing access to the portal using Single-Sign-On techniques, …
- **Software applications:** document labelling, server access authentification, …
- **End-user Terminal**
  - OS, HD protection, thin client, workstation port control, biometry, smart card, PKI, ..
- **Operation & Support Services platform**: SNMP encryption, audit, authentification, …
- **Remote & nomadic access**: Web portal, VPNs, Web VPNs, …
- **Multilevel security**
  - shared "black" network, replication techniques, smart server & document partitioning and indexation


All rights reserved © 2005, Alcatel

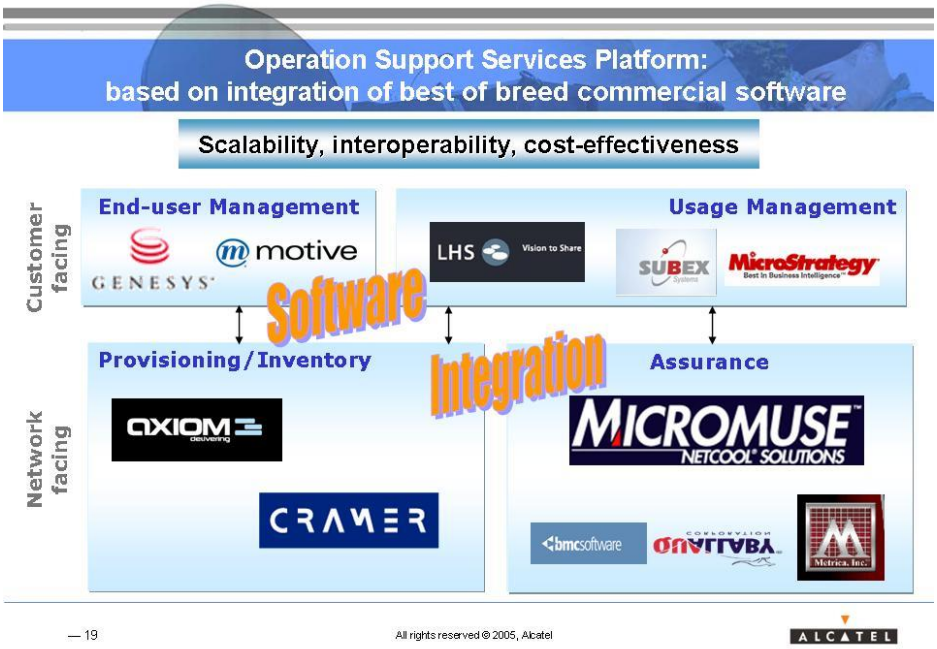
## Service Delivery Platform: operations and support services (OSS)

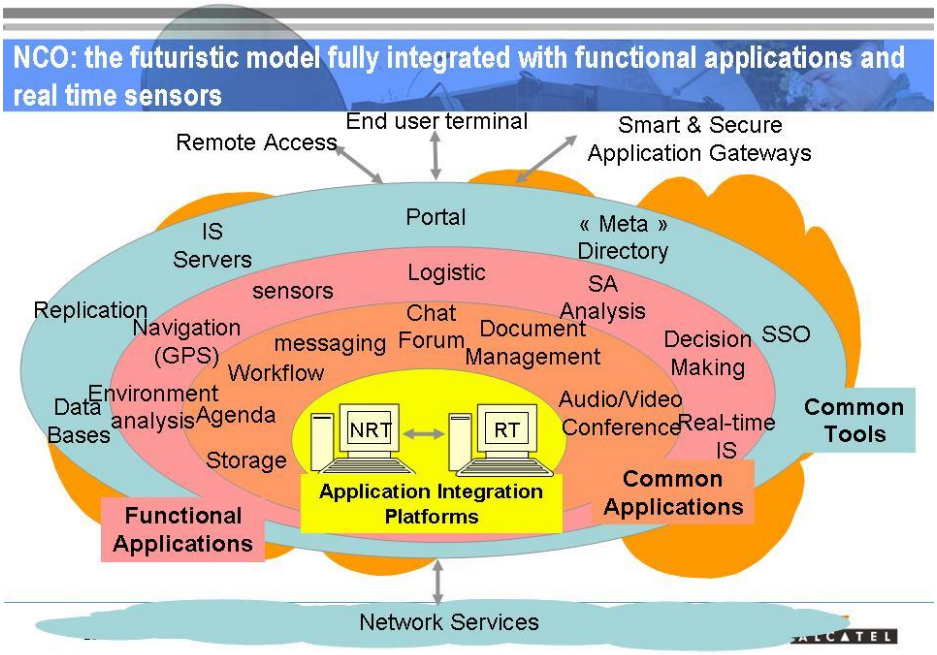
> **A comprehensive OSS platform supervising an increasing variety of objects …**
  - **Applications** (service probes, server & DB usage)
  - **Equipment** (application servers, network elements, encryption devices, …)
  - **Network** (network probes, links, flows, QoS, …)
> **… and delivering a large range of services:**
  - Configuration, Provisioning & Inventory, Fault management, Performance, Resource Planning
  - Helpdesk covering OOA operations, trouble ticketing workflow, change management, …
  - Process automation, advanced graphical interfaces
  - Security management and audit.
> **A smart OSS team organisation**
  - Right mix of **remote/central support**
  - Monitoring tuned to circumstances and specific objects
  - Right flexibility: Data collection separated from diagnosis and end-user access
  - Outsourcing to industry of carefully selected tasks





All rights reserved © 2005, Alcatel


Operation Support Services Platform:
based on integration of best of breed commercial software
Scalability, interoperability, cost-effectiveness
Customer facing
End-user Management
GENESYS
motive
Usage Management
LHS
SUBEX
MicroStrategy
Software
Integration
Network facing
Provisioning/Inventory
AXIOM
CRAMER
Assurance
MICROMUSE
NETCOOL SOLUTIONS
bmcsoftware
— 19
All rights reserved © 2005, Alcatel
ALCATEL


NCO: the futuristic model fully integrated with functional applications and real time sensors
End user terminal
Remote Access
Smart & Secure Application Gateways
Portal
« Meta » Directory
IS Servers
Logistic
SA Analysis
sensors
Replication
Navigation (GPS)
Chat Forum
Document Management
Decision Making
SSO
messaging
Workflow
Environment analysis
Data Bases
Agenda
Storage
NRT
RT
Audio/Video Conference
Real-time IS
Common Tools
Application Integration Platforms
Common Applications
Functional Applications
Network Services
ALCATEL

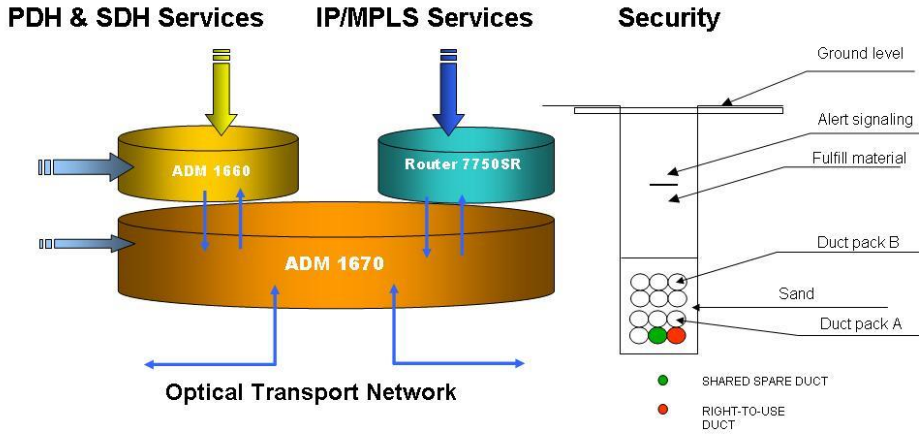
## End to end network-centric services

### Case studies: NCO-aligned projects

Italy – optical backbone
NATO – HQs deployable communications
CWID – Testing of secured wireless
Israel – e2e Service Management System


All rights reserved © 2005, Alcatel

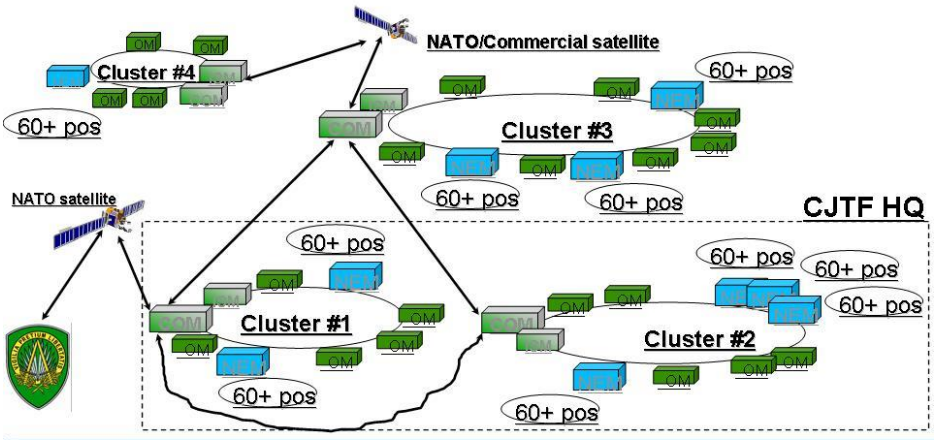
## RIFON: more flexibility in connectivity, more QoS services on IP, more security





All rights reserved © 2005, Alcatel

## Communications for deployed HQs (CJTF, …): the NATO approach





All rights reserved © 2005, Alcatel

## View of Deployable Communication Modules



NEM: Optic interface switch, router, PBX



COM shelter on Truck


All rights reserved © 2005, Alcatel

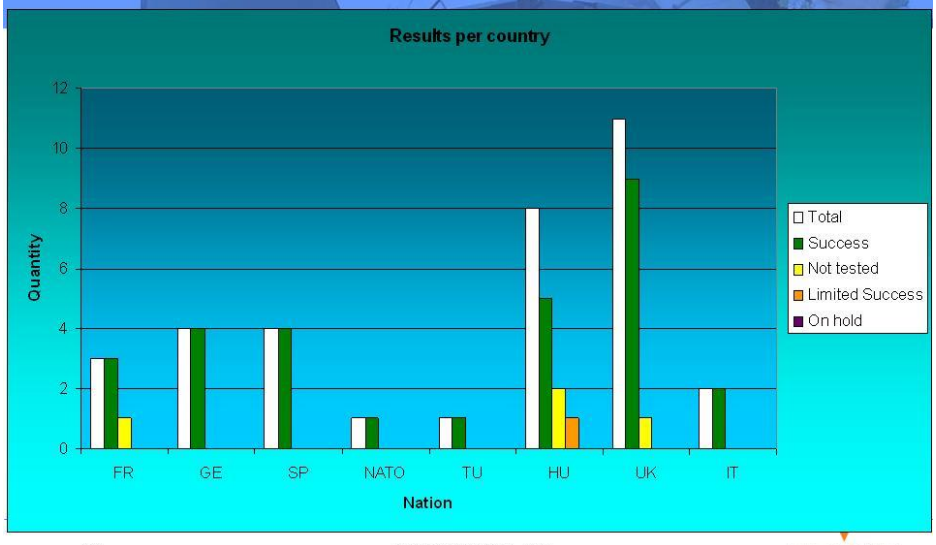
## Coalition Warrior Interoperability Demonstration (CWID)

> CWID is the U.S. Chairman of the Joint Chiefs of Staff annual event with the international community to investigate C4ISR solutions to near-term coalition interoperability challenges. The event provides opportunity for government, private industry and coalition partners to demonstrate new and emerging technologies in a simulated warfighting environment.

> Alcatel Trial: Innovative Network Enabled Capabilities (INEC)
- Validation of NATO Bi-SC AIS core and network services in the context of coalition operations and using new wireless technologies (WIP, DVB SATCOM)
- Validation of COTS based solution for delivering end to end point to multipoint information dissemination addressing four NATO CWID objectives
- 34 test cases performed in NATO SECRET environment

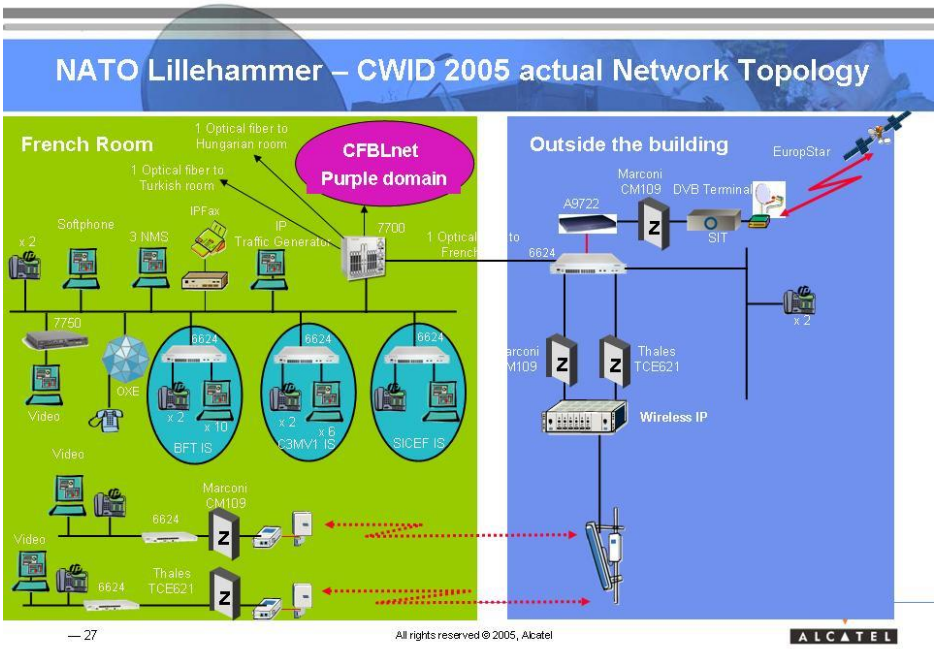

All rights reserved © 2005, Alcatel
ALCATEL

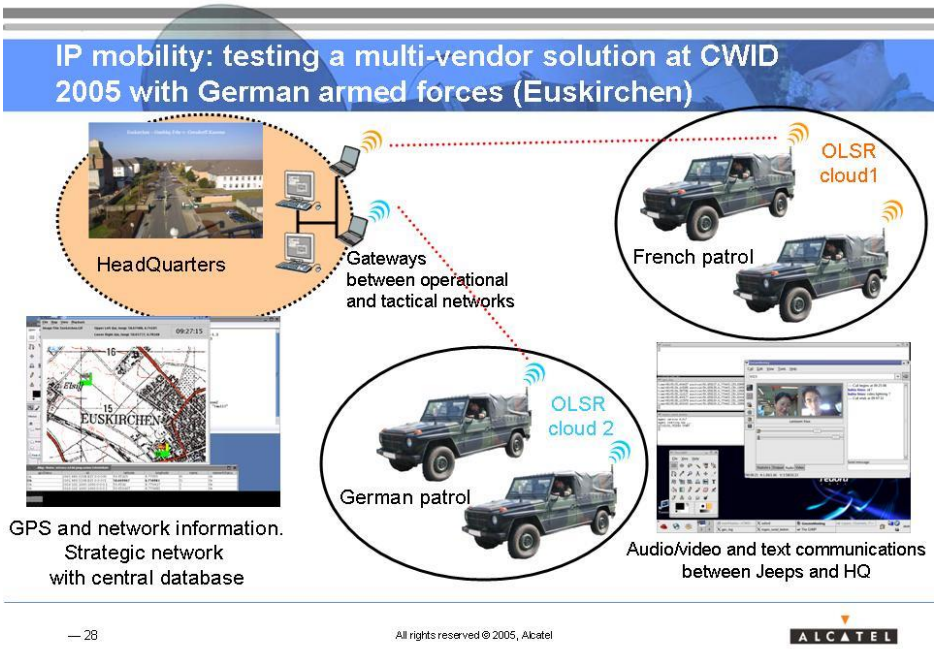
## Alcatel test cases at CWID 2005: Results per country





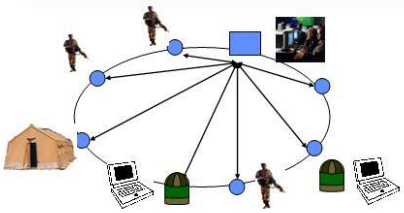
All rights reserved © 2005, Alcatel
ALCATEL


NATO Lillehammer – CWID 2005 actual Network Topology
French Room
1 Optical fiber to Hungarian room
1 Optical fiber to Turkish room
CFBLnet
Purple domain
Softphone
x 2
3 NMS
IPFax
IP Traffic Generator
7700
1 Optical
7750
6624
OXE
Video
x 2
x 10
BFT IS
x 2
x 6
C3MV1 IS
SICEF IS
Marconi CM109
Thales TCE621
Outside the building
EuropStar
Marconi CM109
DVB Terminal
A9722
SIT
6624
x 2
Thales TCE621
Wireless IP
— 27
All rights reserved © 2005, Alcatel
ALCATEL


IP mobility: testing a multi-vendor solution at CWID 2005 with German armed forces (Euskirchen)
HeadQuarters
Gateways between operational and tactical networks
OLSR cloud1
French patrol
OLSR cloud 2
German patrol
EUSKIRCHEN
GPS and network information. Strategic network with central database
Audio/video and text communications between Jeeps and HQ
— 28
All rights reserved © 2005, Alcatel
ALCATEL

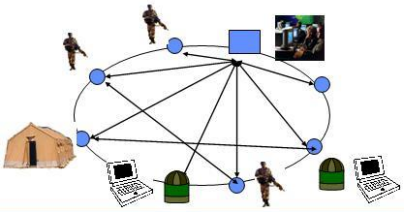
## IP enabled SATCOM: cornerstone of the Converged Multiservices Backbone

### step by step leverage of digital video broadcast technology (DVB)



Step 1: **Broadband IP Multicast broadcast** (up to 30Mb). Implemented in Syracuse III MILSATCOM as one of the 3 available communication service.

> Step 2: **fully meshed IP multicast** (1Mb) using terminals capable of DVB-RCS reception. Commercially released.

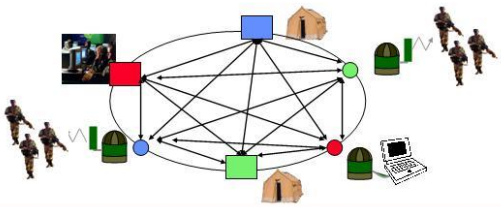



All rights reserved © 2005, Alcatel
ALCATEL

## IP enabled SATCOM: cornerstone of the Converged Multiservices Backbone

### leveraging DVB with an On-Board Processing Payload (OBP)

> Step 3: **broadband IP access network**
- Accessible by low cost terminals
- With flexible and steerable spot beam abord satellite
- With efficient DVB-RCS resource management and waveform
- Integration of IP-V6 and Ad-Hoc protocols to serve on the move communication

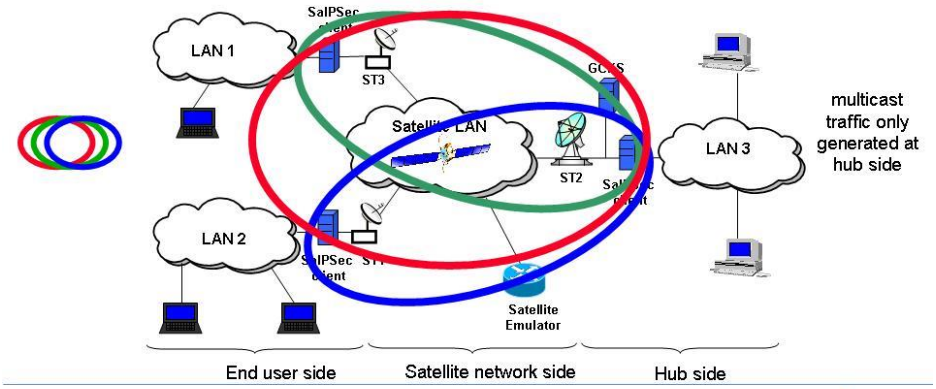



All rights reserved © 2005, Alcatel
ALCATEL

## IP enabled SATCOM: cornerstone of the Converged Multiservices Backbone

### SATIPsec: a "light" security of your SATCOM IP access network

SATIPsec: a new innovative IETF standard and an Alcatel Space patent

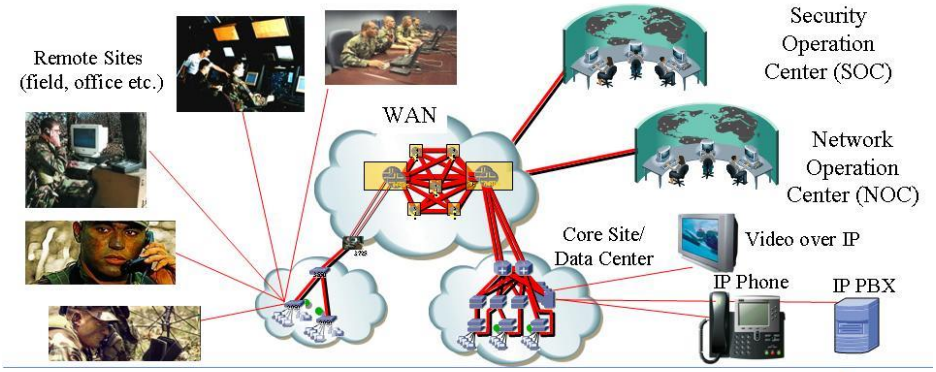




All rights reserved © 2005, Alcatel

## Israel MOD: Hoshen project – 2004/2006

> Turnkey Operations Support System (OSS) for the Strategic Communications Infrastructure that delivers end to end services over legacy, IP/MPLS, mobile networks





All rights reserved © 2005, Alcatel

## Reference: the Hoschen project

> Integrated software solution that provides end to end network and services management over a large scale multi-technology communication infrastructure comprising:
  - New generation network & services (IP/MPLS/VPN/VoIP, SDH/Optic, …)
  - Legacy networks & services (PSTN/POTS, PDH transmission, data networks, …)
  - Smart "re-use" of the existing legacy OSS
  - Tactical cellular system, tactical IP/VoIP, SATCOM (in phase 2 only)

> First contract with Ness (50%, 50%) in August 2004 ($25m)


All rights reserved © 2005, Alcatel

## Reference: Hoschen concepts

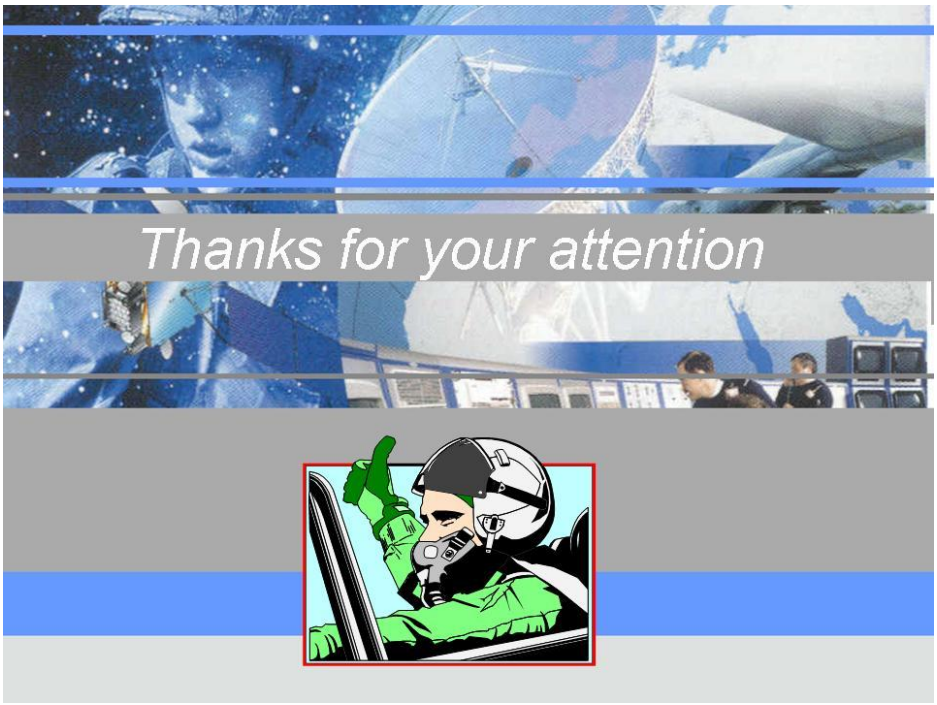
> Manager of Manager (MoM) architecture
  - The system maintains an on-line real time connection to external management systems as Element Managers, NMS, legacy OSS, other OSS, COTS products, …
  - Enables easy integration of new technologies and other OSS into the MoM suite

> Standards:
  - NGOSS, eTOMGB921, OSS/J, implementation with J2EE application server

> Security: public security concepts, COTS products, and private classified capabilities

> Capability guidelines
  - End to end view of networks, technologies,
  - Integrative tools for fulfillment and assurance processes (for resources, services, users)
  - Maximum system automation – minimum operation by the operator
  - Advanced graphical user interface
  - Pre-planned services and Activation System
  - Advanced alert system


All rights reserved © 2005, Alcatel


Thanks for your attention

# Antók Péter:

# HÍRKÖZLŐHÁLÓZAT - - HÁLÓZATBIZTONSÁG



## HÍRKÖZLŐHÁLÓZAT



**VEZETÉKES-**
**VEZETÉKNÉLKÜLI-**

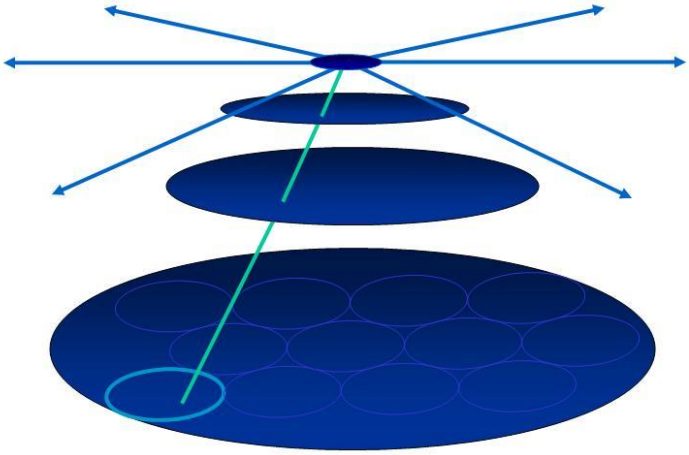
**TÁVKÖZLÉSI-**
**INFORMATIKAI-**
**KÁBELTELEVÍZIÓ-**

**NYILVÁNOS-**
**SAJÁTCÉLÚ-**
**KÜLÖNCÉLÚ-**
**ZÁRTCÉLÚ-**

**EGYÉB**

ZRINYI MIKLÓS NEMZETVÉDELMI EGYETEM * KOMMUNIKÁCIÓ 2005.

# TÖBBSÍKÚ HÁLÓZAT





# HÁLÓZATFELOSZTÁS

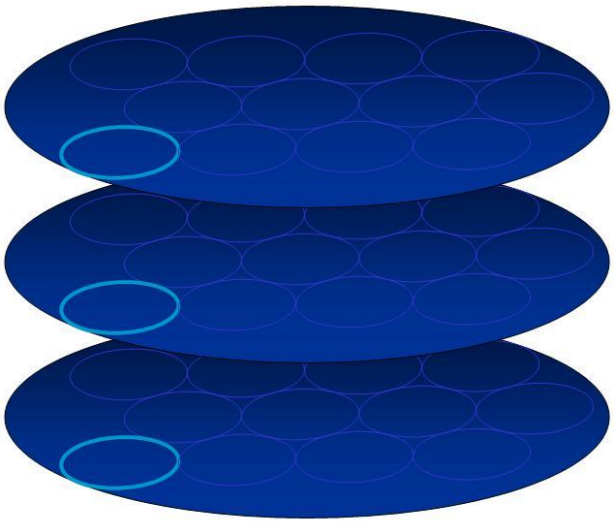
**NYILVÁNOS-**

**SAJÁTCÉLÚ-**

**KÜLÖNCÉLÚ-**

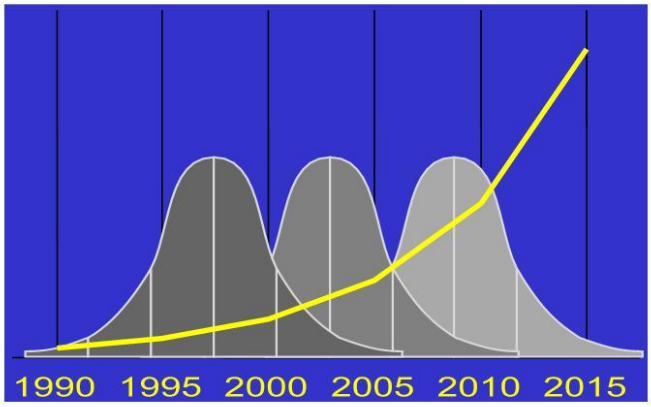
**ZÁRTCÉLÚ-**

## HÁLÓZATOK





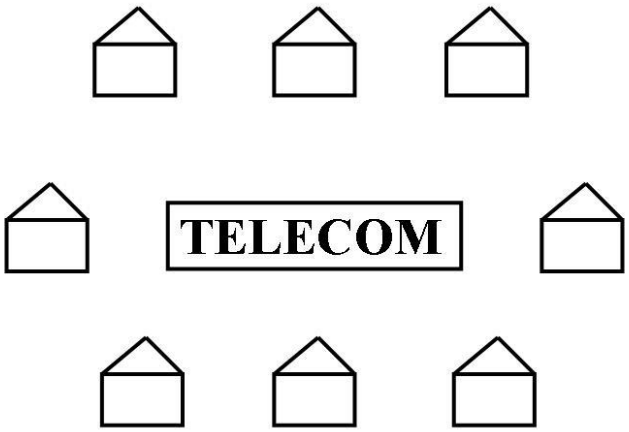
## TÖBBGENERÁCIÓS HÁLÓZAT




ZRINYI MIKLÓS NEMZETVÉDELMI EGYETEM * KOMMUNIKÁCIÓ 2005.




## EGY SZOLGÁLTATÓ

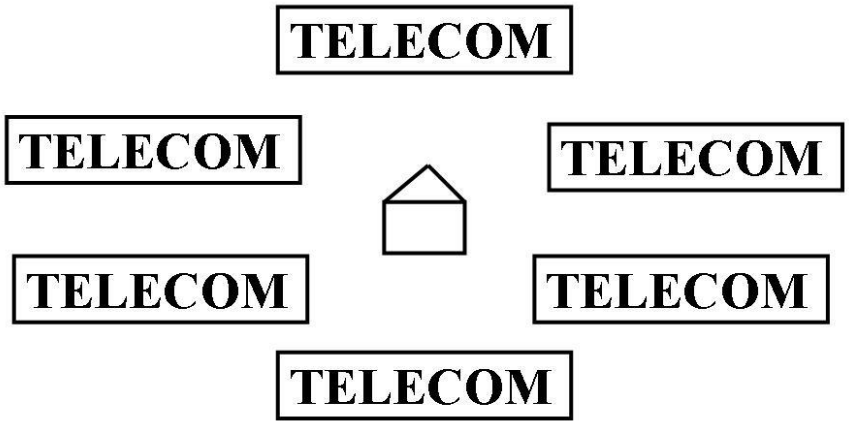




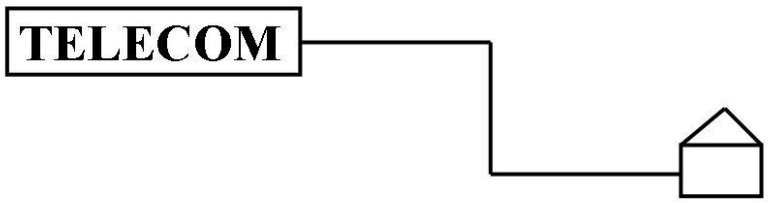




## TÖBB SZOLGÁLTATÓ



## HÁLÓZAT FELÉPÍTÉS






## HÁLÓZATBIZTONSÁG

- VÉDEKEZÉS
- ÉSZLELÉS
- KÁRENYHÍTÉS
- HELYREÁLLÍTÁS
- ÚJJÁÉPÍTÉS

# HÁLÓZATBIZTONSÁG

- Közönséges védelem: 1-3 %
- Erősített védelem: 4-6 %
- Fokozott védelem: 8-12 %
- Kiemelt védelem: 15-18 %
- Extra erős védelem: 20-25 %



# ZÁRTCÉLÚ HÁLÓZAT

**-KORMÁNYZATI**

**-BELÜGYI**

**-HONVÉDELMI**

**-NEMZETBIZTONSÁGI**

**-PÉNZÜGYI**

**-IGAZSÁGÜGYI**

**-ÜGYÉSZSÉGI**

# MSZ 17128-2:1997
# Távközlő hálózatok és távközlési szolgáltatások védettsége
Vezetékes előfizetői hálózatok védelme



## HOZZÁFÉRÉS - MSZ 17128-2:1997

**Szabad hozzáférés:** a távközlő hálózathoz vagy hálózatrészhez a hozzáférést semmilyen előírás, vagy védelmi intézkedés nem korlátozza, a nyilvánosság által szabadon hozzáférhető.

ZRINYI MIKLÓS NEMZETVÉDELMI EGYETEM * KOMMUNIKÁCIÓ 2005.

# HOZZÁFÉRÉS - MSZ 17128-2:1997

**Egyerű hozzáférés:** jogosulatlan hozzáférés távközlési berendezésekhez és szolgáltatásokhoz egyszerű eszközök segítségével (pl. csavarhúzó, bútorkulcs, tű stb.) különleges szakmai ismeretek vagy erőfeszítés nélkül.



# HOZZÁFÉRÉS - MSZ 17128-2:1997

**Nehéz hozzáférés:** jogosulatlan hozzáférés távközlési berendezésekhez és szolgáltatásokhoz erre a célra kialakított különleges eszközök segítségével (különleges szerszám, hamis kulcs stb.) különleges erőfeszítéssel és/vagy bizonyos műszaki-, szervezési ismeretekkel.

# HOZZÁFÉRÉS - MSZ 17128-2:1997

.**Különösen nehéz hozzáférés:** jogosulatlan hozzáférés távközlési berendezésekhez vagy szolgáltatásokhoz csak erre A célra kialakított különleges eszközökkel (Speciális áramkörökkel, programokkal stb.) és teljes műszaki felszereltséggel illetve szervezési ismeretekkel.



# HÁLÓZATVÉDETTSÉG

**Erősen zárt berendezés:** hálózatrész vagy távközlési berendezés, amelyhez a mechanikai védelmi intézkedések a jogosulatlan használók számára nehéz vagy különösen nehéz hozzáférést tesz lehetővé.

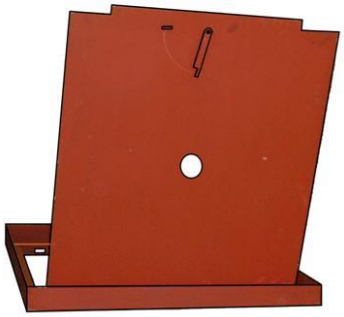
*Megjegyzés:*
*Az erősen zárt berendezés burkolata megfelelő szilárdságú és a zárszerkezet csak erre a célra kialakított, különleges eszközökkel (nem szabványos alakú szerszámmal, különleges kulccsal stb.) és/vagy erőfeszítéssel nyitható. Erősen zárt berendezést a szolgáltató olyan helyen telepít, ahol egyéb védelmi módszerek, intézkedések nem alkalmazhatók, például közterületen, szabad hozzáférésű helyiségekben.*

# SAROKHEGESZTETT LEZÁRÁS



ZRINYI MIKLÓS NEMZETVÉDELMI EGYETEM * KOMMUNIKÁCIÓ 2005.

# ZÁRHATÓ,
# BELSŐ AKNAFEDLAPOS LEZÁRÁS



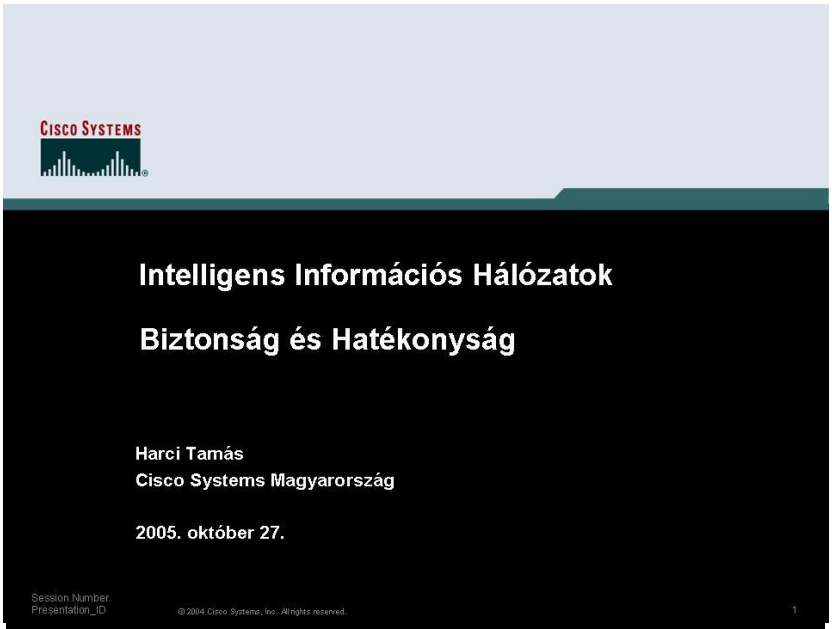
ZRINYI MIKLÓS NEMZETVÉDELMI EGYETEM * KOMMUNIKÁCIÓ 2005.

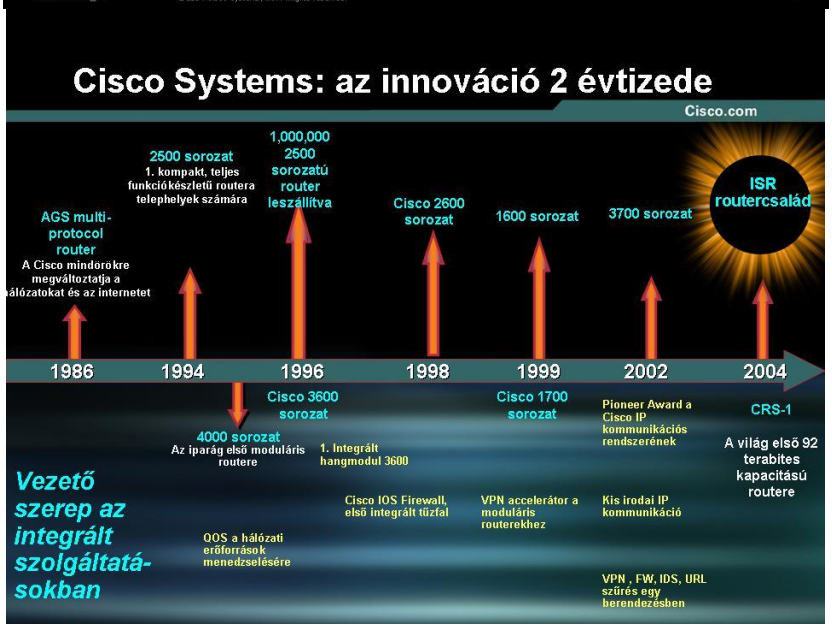
# KÖSZÖNÖM A FIGYELMÜKET

Antók Péter
Távközlési szakértő 01-1842-W-H2-V
Távközlési igazságügyi szakértő 006744
1035 Budapest, Szél utca 17.
471-1353; 30-2978-415
peter.antok@t-online.hu

**CISCO Systems Magyarország Kft.**

# INTELLIGENS INFORMÁCIÓS HÁLÓZATOK - BIZTONSÁG ÉS HATÉKONYSÁG




A Cisco technológiai jövőképe:
Intelligens Információs Hálózatok
Cisco.com
Hálózati infrastruktúra
Erőforrások, alkalmazások, szolgáltatások
Integrált alkalmazások
3
Alkalmazás-orientált hálózat és szolgáltatások
Integrált szolgáltatások
2
Virtualizált hálózati erőforrások
Integrált forgalom
1
Adat – hang – video intelligens szállítása a hálózatok rendszerein
A hálózatok és az alkalmazások összefüggései
Cisco.com
• A hálózat fogja össze az infrastruktúra elemeit
• Hatékonysági szempontból tehát a kiindulópontunk maga a hálózat
Folyamatok/Hatékonyság/IPC alkalmazáso
Hálózat
Hálózat
Middleware
Hálózat
Hálózat
Szerverek
Hálózat
Presentation_ID
© 2004 Cisco Systems, Inc. All rights reserved.
4

## Intelligens Információs hálózatok – új technológiákkal

Cisco.com

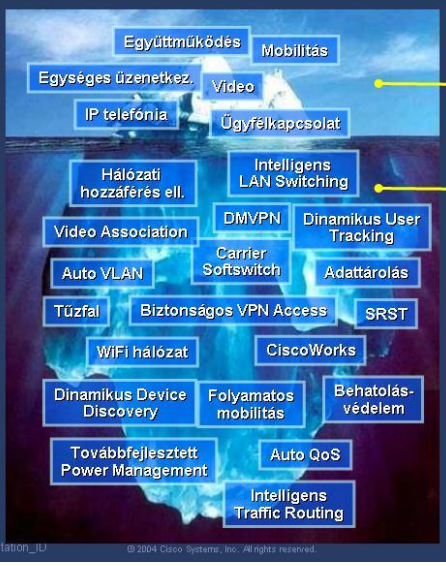
| | |
|---|---|
| IP kommunikáció | • 6,000,000 telepített készülék<br>• 25,000+ ügyfél |
| Biztonság | • Önvédő hálózat<br>• Végponttól végpontig terjedő biztonság<br>• Iparági együttműködés |
| Mobilitás | • Vezetékes és vezeték nélküli integráció<br>• Biztonságos roaming: LAN és WAN |
| Adattárolás/SAN | • Költséghatékony multiprotocol platform<br>• Adathálózati innovációk a SAN-okhoz<br>• Konszolidált SAN hálózat |
| Optika | • Multi-szerviz hálózat<br>• Költségcsökkentés és a beruházások értékvédelme<br>• Folyamatos üzletmenet / katasztrófa-elhárítás |

Presentation_ID © 2004 Cisco Systems, Inc. All rights reserved. 5

## Intelligens Információs Hálózatok

*Rendszerek. . . Végponttól végpontig.....Megbízhatóság...Egyszerűség*

Cisco.com




**Amit látunk: a jéghegy csúcsa**

**Amit nem látunk:**
***Intelligens Információs Hálózat***
***a komplexitás rejtve marad***

Presentation_ID © 2004 Cisco Systems, Inc. All rights reserved. 6


Hálózati igények a közszférában
Cisco.com
SELF-DEFENDING NETWORK
Önvédő hálózat
Adaptív védelem
HANG + ADAT + VIDEO KONVERGENCIA
MOBILITÁS
TARTALOMSZOL-GÁLTATÁS ÉS TÁROLÁS
TELJESÍTMÉNY


IP kommunikáció: kommunikáció - másképp
Cisco.com
Hagyományos telefonhálózat
Hagyományos adathálózat
Csak hang
Csak adat
Presentation_ID
© 2004 Cisco Systems, Inc. All rights reserved.
8

## IP kommunikáció: kommunikáció - másképp

Cisco.com

### Konvergens hálózat: adat + hang + video



Presentation_ID © 2004 Cisco Systems, Inc. All rights reserved. 9

## IP-alapú hálózatok:
*Középpontban a felhasználó*

Cisco.com







Presentation_ID © 2004 Cisco Systems, Inc. All rights reserved. 10

## Hálózatok a közszféra szolgálatában

Cisco.com





- Hatékonyabb szolgáltatások (lakossági, távoktatás, egészségügy)
- A biztonság erősítése (közbiztonság, adatbiztonság)
- A gazdaság fellendítése





**……IP kommunikáció, vezeték nélküli hálózatok, hálózatbiztonsági megoldások**









## A Vezeték nélküli technológia biztonságosabb környezetet eredményez Westminsterben

Cisco.com

- **Helyszín**
  Westminster London egyik legbefolyásosabb és legfontosabb kerülete
- **Cél**
  A bűnözés, vandálkodás csökkentése.
  A lakosság és a látogatók biztonságérzetének növelése.
- **Megoldás**
  Vezetéknélküli technológia. Mobil térmegfigyelő kamerák.
- **Eredmények**
  Kevesebb utcai bűnözés a CCTV lefedettség miatt
  Gyorsabb reagálás
  Segíti a terrorizmusellenes törekvéseket
  Tisztább és biztonságosabb utcák

City of Westminster


© 2004 Cisco Systems, Inc. All rights reserved.

## Katonai alkalmazások

Cisco.com





© 2004 Cisco Systems, Inc. All rights reserved.


## A haderő szerepe világszerte változik

Cisco.com

### Új feladatok:

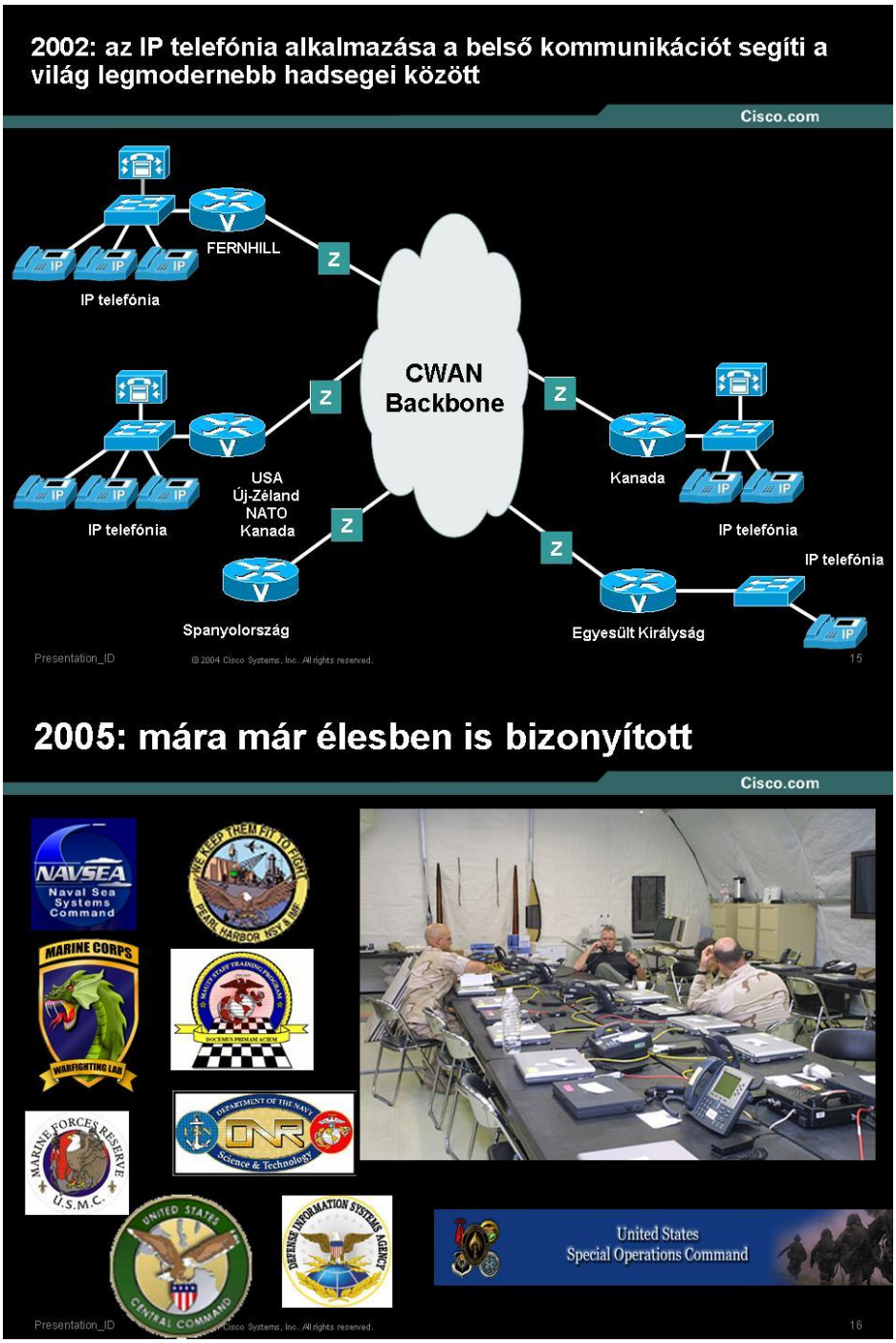
- Béketeremtő és békefenntartó missziók támogatása
- Terrorizmus elleni harc

### Új igények:

- A haderő legyen könnyebben mozgatható
- Integrált kommunikáció nem NATO országokkal
- Ad hoc hálózati megoldások
- Országon belüli feladatok
- Hálózat központú vezetési megoldások



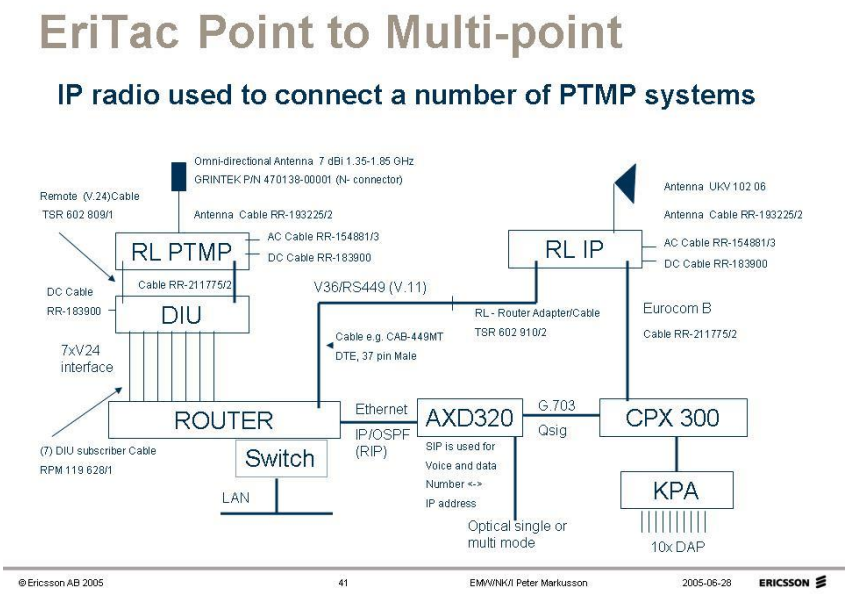

© 2004 Cisco Systems, Inc. All rights reserved.

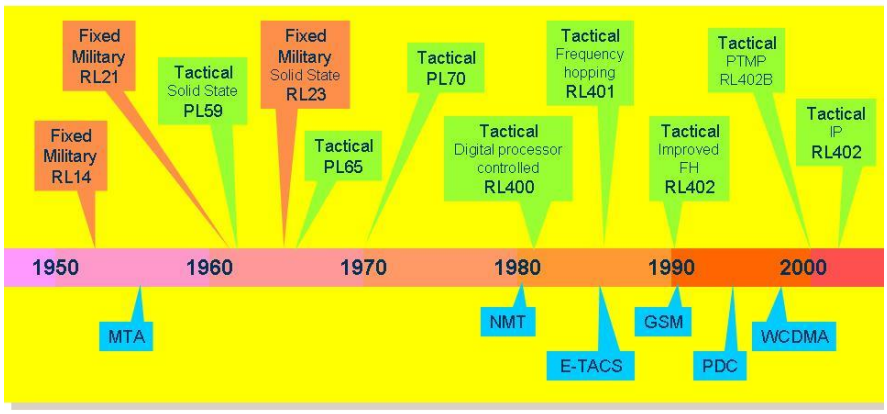

2002: az IP telefónia alkalmazása a belső kommunikációt segíti a világ legmodernebb hadsegei között
Cisco.com
FERNHILL
IP telefónia
CWAN Backbone
USA
Új-Zéland
NATO
Kanada
IP telefónia
Kanada
IP telefónia
IP telefónia
Spanyolország
Egyesült Királyság
Presentation_ID
© 2004 Cisco Systems, Inc. All rights reserved.
15
2005: mára már élesben is bizonyított
Cisco.com
NAVSEA
Naval Sea Systems Command
MARINE CORPS
WARFIGHTING LAB
MARINE FORCES RESERVE
U.S.M.C.
UNITED STATES CENTRAL COMMAND
DEFENSE INFORMATION SYSTEMS AGENCY
United States
Special Operations Command
Presentation_ID
© 2004 Cisco Systems, Inc. All rights reserved.
16


Békefenntartás Kabulban és az Iraki alkalmazások
Cisco.com
ISAF
THIS IS THE POWER OF THE NETWORK. NOW.
10 éve Magyarországon
CISCO SYSTEMS

**ERICSSON Magyarország Kft.**

## ERITAC POINT TO MULTI-POINT

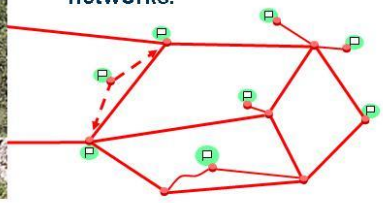


# EriTac - Tactical Area Network

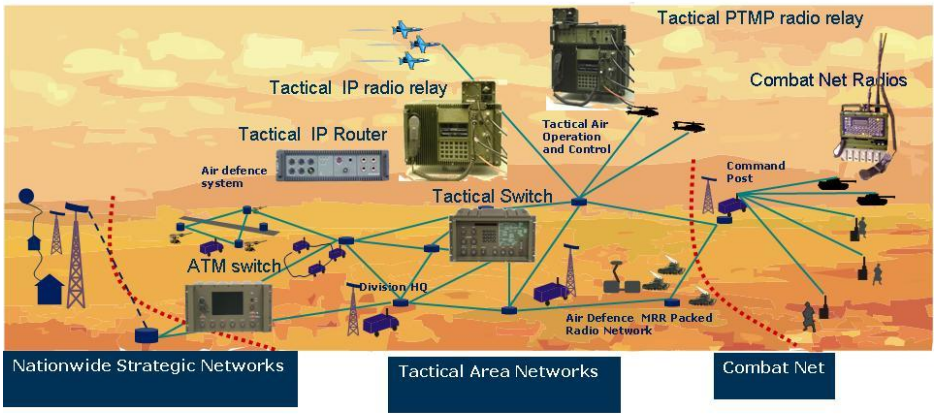


- Secure network with very strong ECCM performance thanks to adaptive frequency hopping and advanced routing.
- High mobility when installed in small cross-country vehicles.
- Voice and data communication.
- Easy to build user adapted networks.

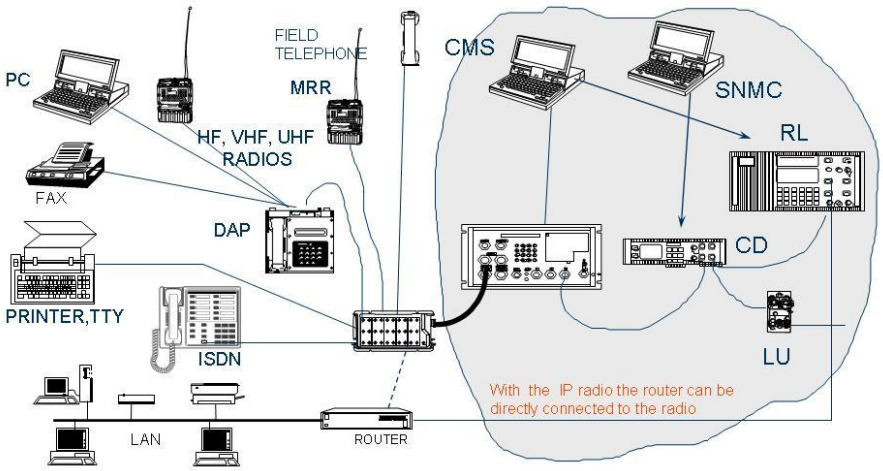




# EriTac – Theatre of operation



# EriTac – System Components






# EriTac – Radio Relay Equipment







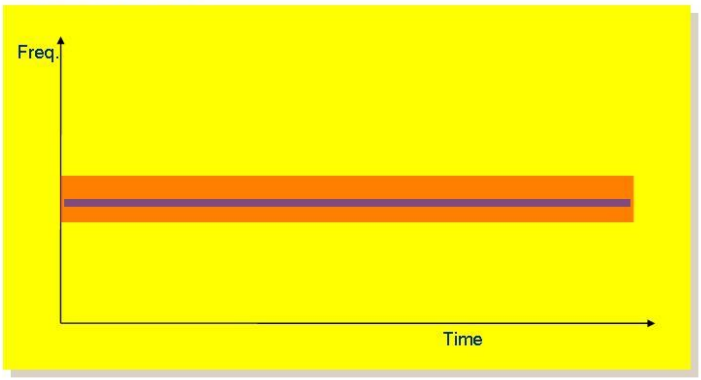



RL422A : 610- 960 MHz

RL432A : 1350 – 1850 MHz

# EriTac – Radio Relay Equipment

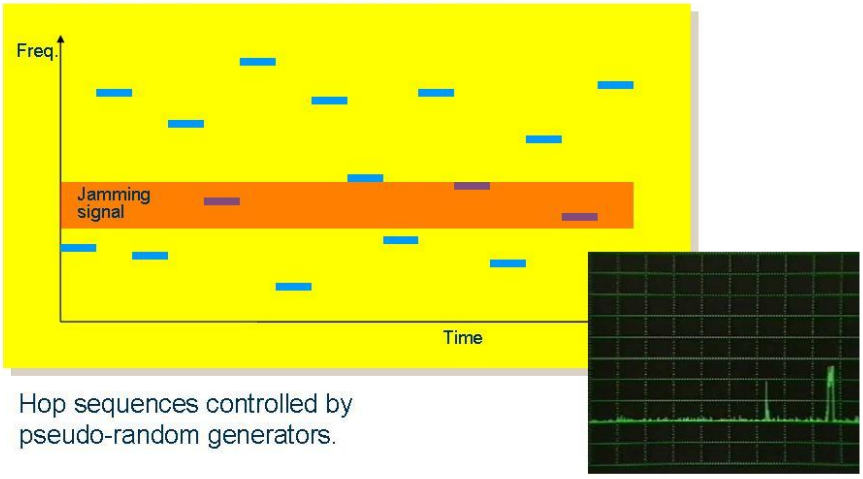
## Fix Frequency






# EriTac – Radio Relay Equipment

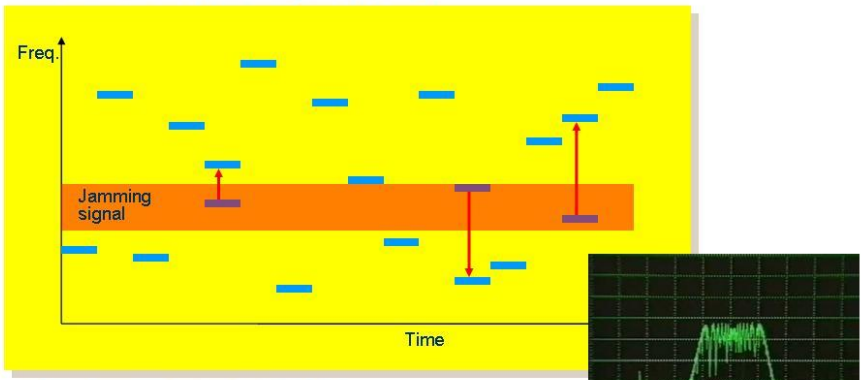
## Conventional Frequency Hopping

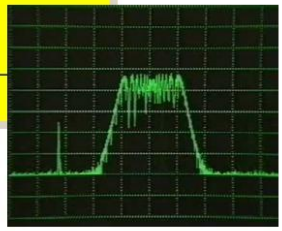



Hop sequences controlled by pseudo-random generators.

# EriTac – Radio Relay Equipment

## Adaptive Frequency Hopping



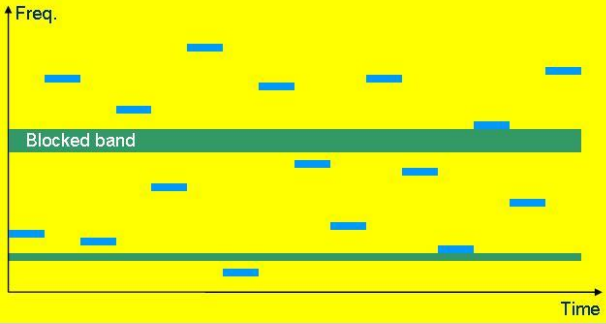
Hop sequences controlled by
pseudo-random generators
and the current jamming situation.



# EriTac – Radio Relay Equipment

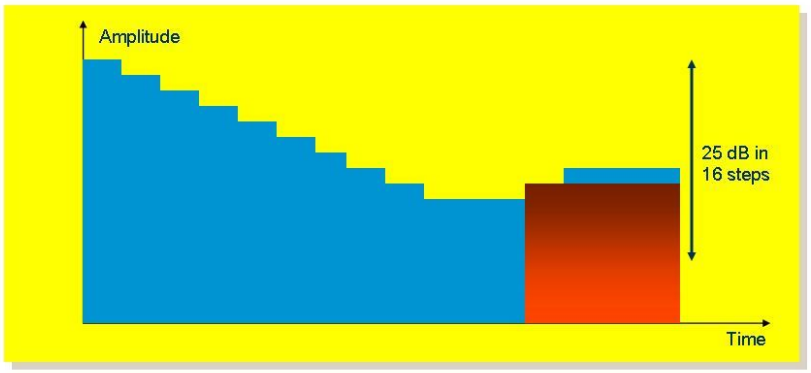
## Band spreading technique

Spreading technique Frequency hopping (FH)
Frequency management Up to 20 subbands may be excluded



# EriTac – Radio Relay Equipment

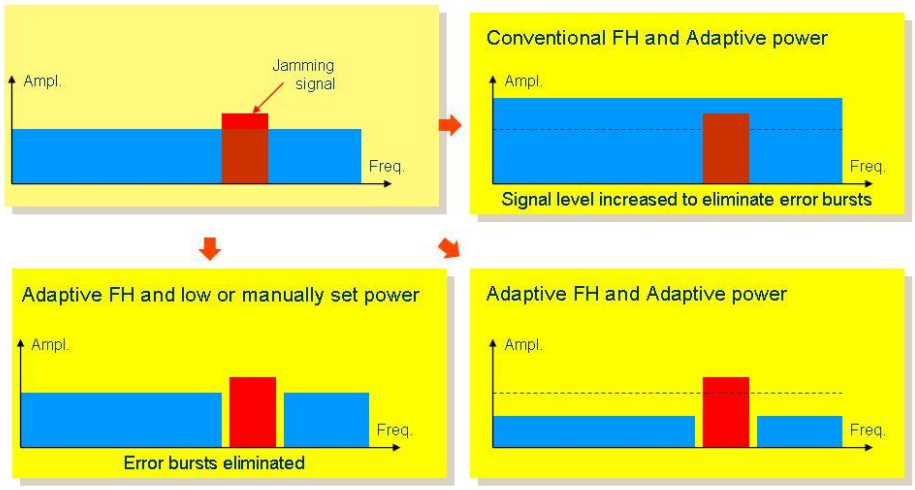
## Adaptive Output Power (LPI) Mode




LPI = Low Probability of Interception



# EriTac – Radio Relay Equipment



# EriTac – Radio Relay Equipment



Antennas



Masts



ATI



Handset



Connection Box



Loudspeaker

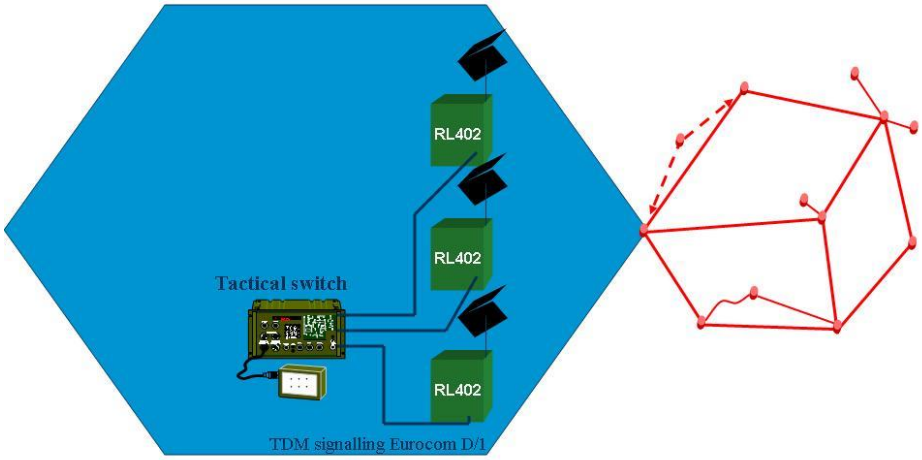


Feeder cables



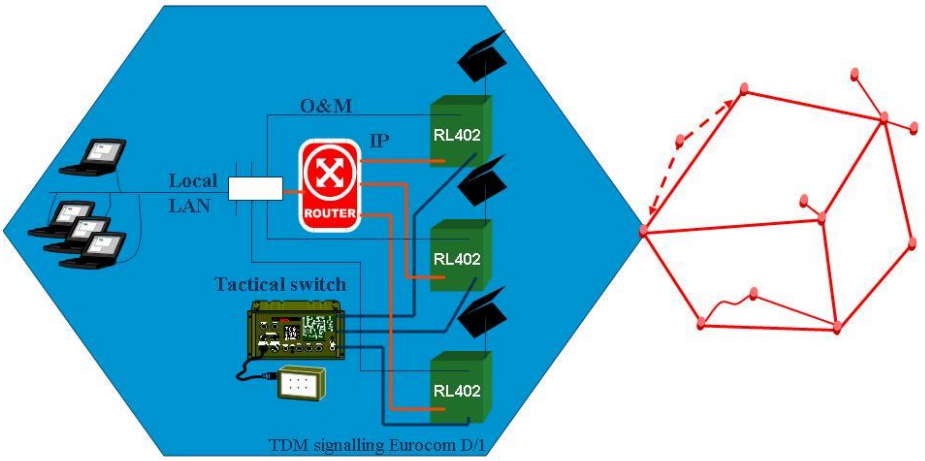
# EriTac – Radio Relay Equipment

## Traditional



# EriTac – Radio Relay Equipment

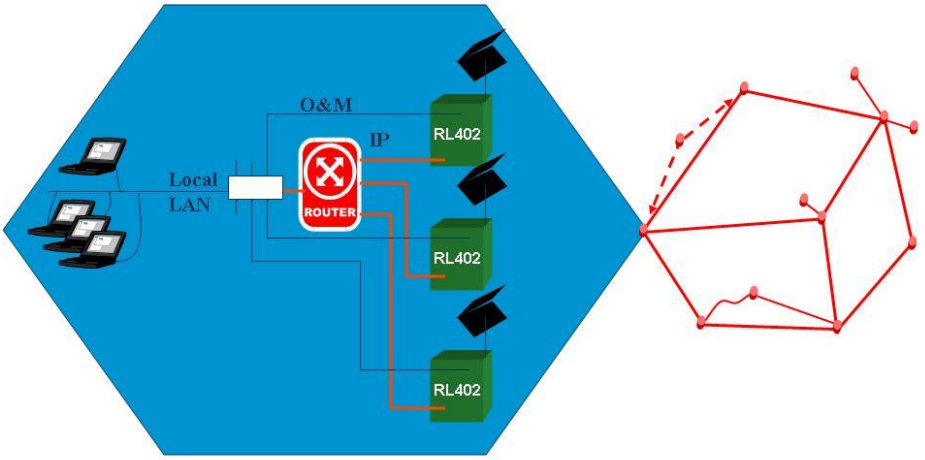
## Traditional and IP






# EriTac – Radio Relay Equipment

## IP

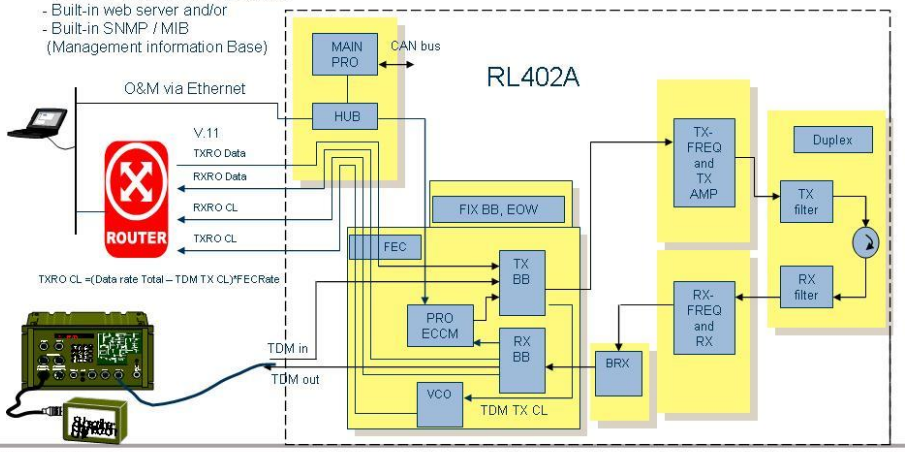


# EriTac – Radio Relay Equipment

## IP radio relay

Ethernet
- Unique IP-addresse for each radio
- Built-in web server and/or
- Built-in SNMP / MIB
(Management information Base)

Channel coding / FEC
- Implemented in FPGA – easy to upgrade (dynamically!)
- Block code chosen (Reed-Solomon) – 12,5% redundancy
- BER $10^{-3}$ is reduced to < $10^{-6}$





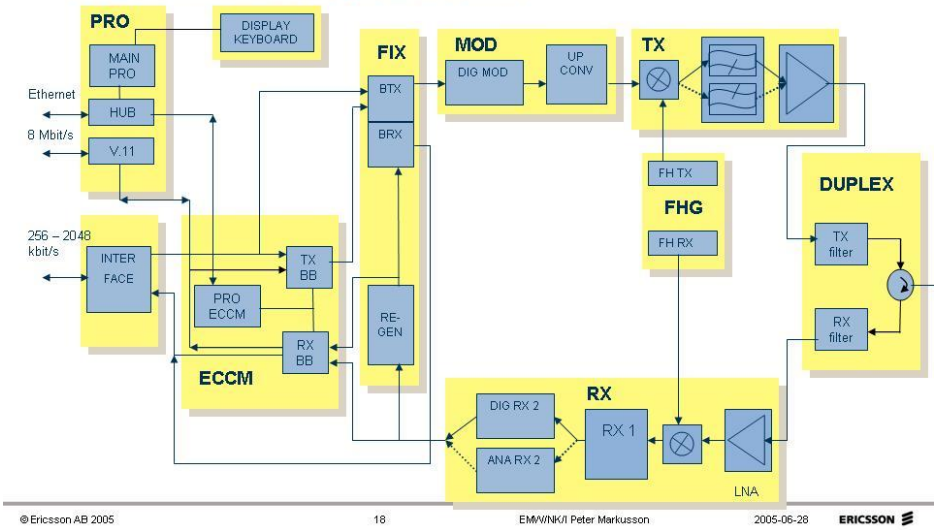

# EriTac – Radio Relay Equipment

## RL with 4 and 8 Mb/s data rate

- Linear TX and RX
- Modulation schemes: π/4-DQPSK, 16-DPSK, (in parallel with existing FSK)
- Fix frequency > 2 Mb/s
- Spectral efficiency: 3.5 MHz-filter for 4 and 8 Mb/s fix frequency (same as for 2 Mb/s FH)
- Forward Error Correction (FEC) Reed-Solomon (233,255)

# EriTac – Radio Relay Equipment

## HCLOS Radio Relay RL432A HC






# EriTac – Radio Relay Equipment

By selecting the total data rate (air rate) and the wanted data rate for the TDM (tactical switch), the data rate for the router will be automatically calculated by the radio.

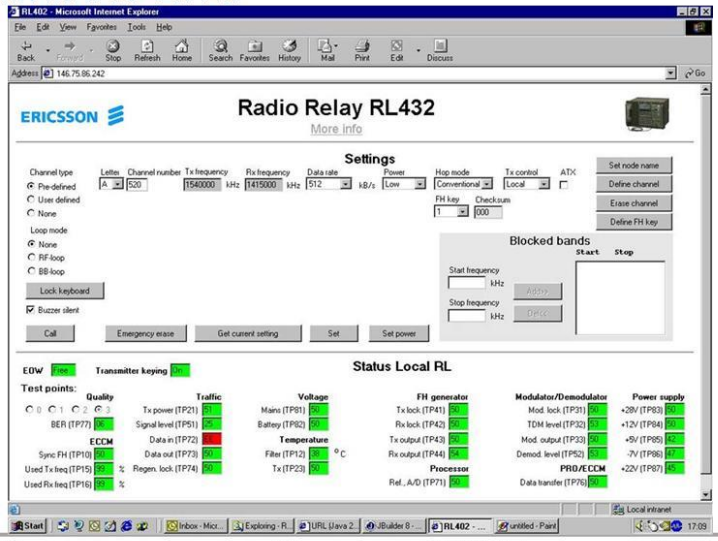
The data rate valid for the router traffic will be according to the following formula:

| Total data | TDM data | FEC | Router data |
|---|---|---|---|
| 256 kb/s | 256 kb/s | | Not used |
| 512 kb/s | 256 kb/s | off | 256 kb/s |
| 512 kb/s | 0 | off | 512 kb/s |
| 1024 kb/s | 256 kb/s | On (-12,5%) | 671 kb/s |
| 2048 kb/s | 512 kb/s | off | 1536 kb/s |
| 2048 kb/s | 512 kb/s | On (-12,5%) | 1343 kb/s |
| 2048 kb/s | 0 | off | 2048 kb/s |
| 2048 kb/s | 0 | On (-12,5%) | 1790 kb/s |
| 2048 kb/s | 2048 kb/s | | Not used |
| 4096 kb/s | 1024 kb/s | On (-12,5%) | 2686 kb/s |
| 4096 kb/s | 2048 kb/s | On (-12,5%) | 1790 kb/s |
| 8192 kb/s | 0 | On (-12,5%) | 7163 kb/s |
| 8192 kb/s | 2048 kb/s | On (-12,5%) | 5372 kb/s |

Data rate IP = (Data rate Total - Data rate TDM) * FEC rate.

# EriTac – Radio Relay Equipment

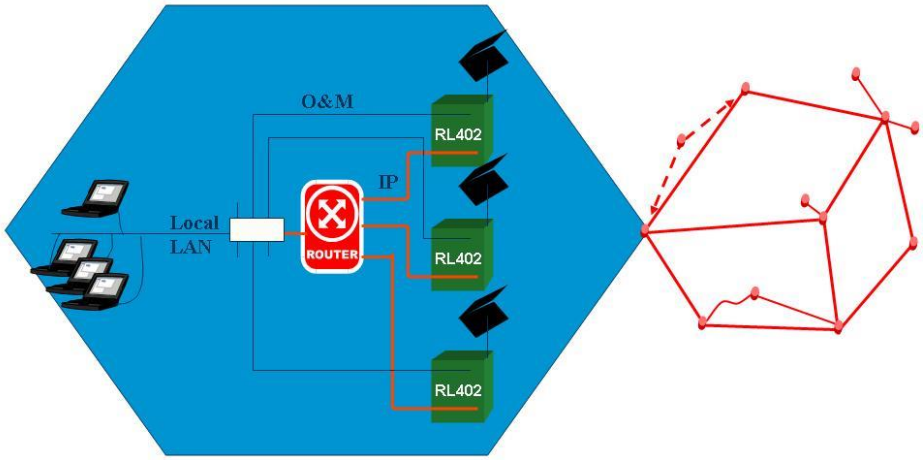
## Built in web server





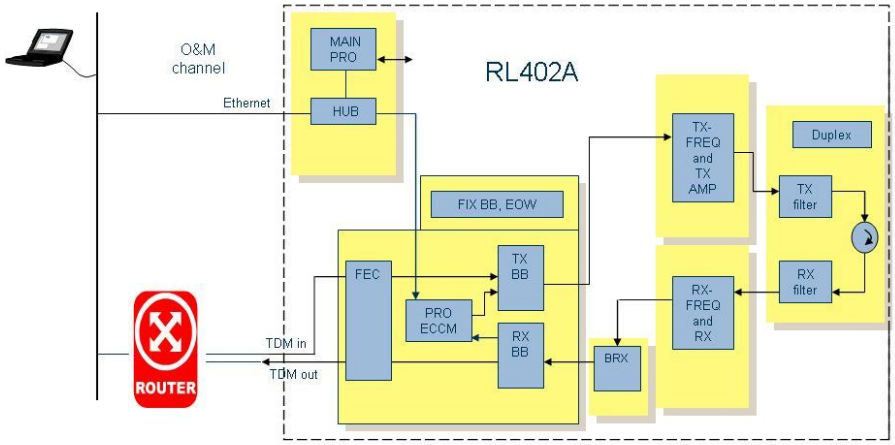

# EriTac – Radio Relay Equipment

## RL402 – IP radio relay with G.701 (E1)



# EriTac – Radio Relay Equipment

## RL402 – IP radio relay with G.701 (E1)



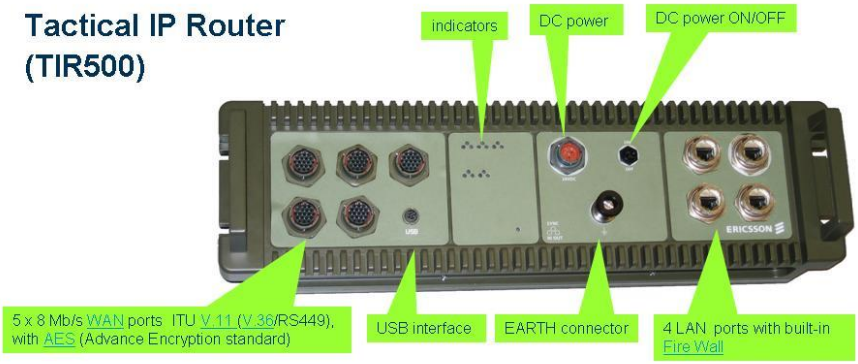



# EriTac Ruggedized Router



# EriTac Ruggedized Router

## Tactical IP Router (TIR500)



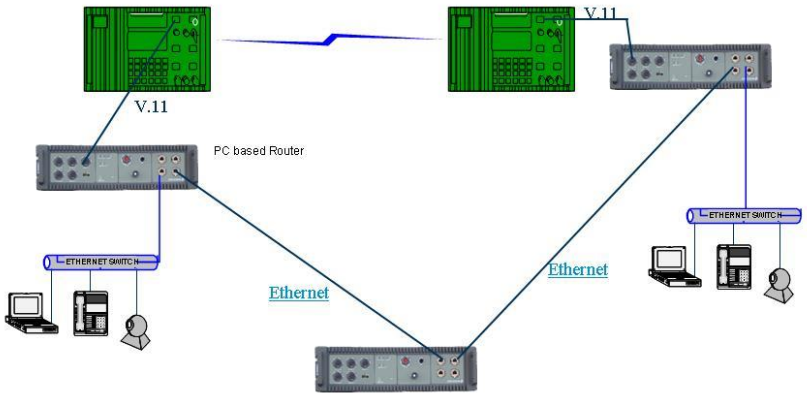

**Architecture**: PowerPC
**IP versions**: IPv4 and IPv6
**Routing Protocols**: OSPF, OSPFv3, BGP and RIP
**WAN/LAN protocols**: HDLC, PPP, Ethernet
**LAN support**: IEEE 802.3, 10/100 Base T
**Network services**: DHCP, DNS , NAT

**QoS**: DiffServ service with Class Based Queuing (CBQ) and Random Early Detection (RED)
**Security**: IPSec including 256 bits AES, VPN, Firewall password and removable crypto key
**Management**: Web based GUI, CLI and SNMPv3

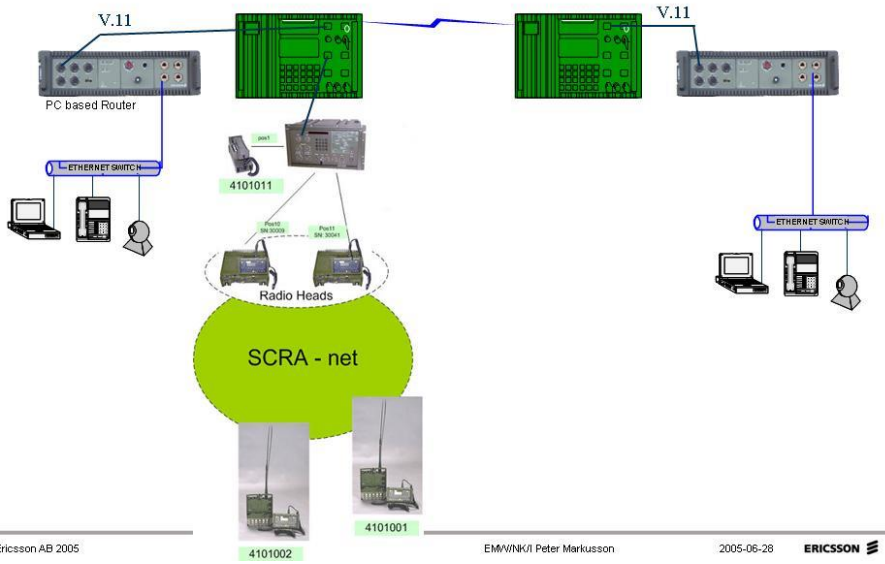


# EriTac Ruggedized Router

## Router and RL IP Demo setup



# EriTac Demo Setup






# EriTac Ruggedized Router

## Router and RL IP Demo Applications

- Battle field situation awareness: Video and sound
- VoIP: IP-Telephone (SIP Peer-to-peer, i.e. no SIP Server needed)
- Document exchange (FTP based file sharing)
- Message exchange (Email based)
- IPSec (Encryption, AES, 256 bits key)
- Dynamic Rerouting (End-to-end communication maintained through network redundancy)
- QoS (VoIP prioritized over video streaming)
- Remote O&M functionality for the router and the RL

# EriTac Bulk Encryption

## Example of Bulk Encryption Equipment

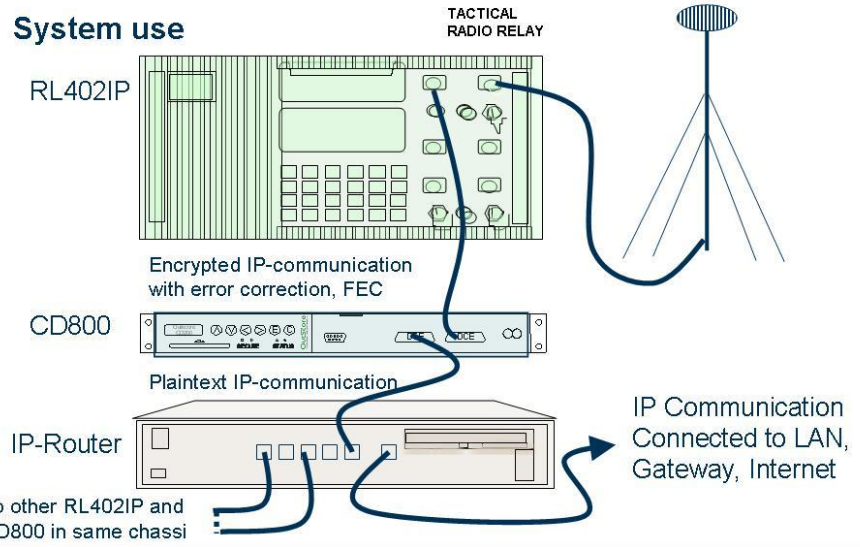



- Newest generation of bulk encryption system
- Full duplex mode of operation
- Transmission rate up to 8 Mb/s
- Smartcard key distribution
- Customized algorithm design
- No time delay
- Automatic synchronization
- Supervision
- Tamperproof
- Easy management
- Several physical interface options



# EriTac Bulk Encryption

## System use



# EriTac Portable casing "FLEX"





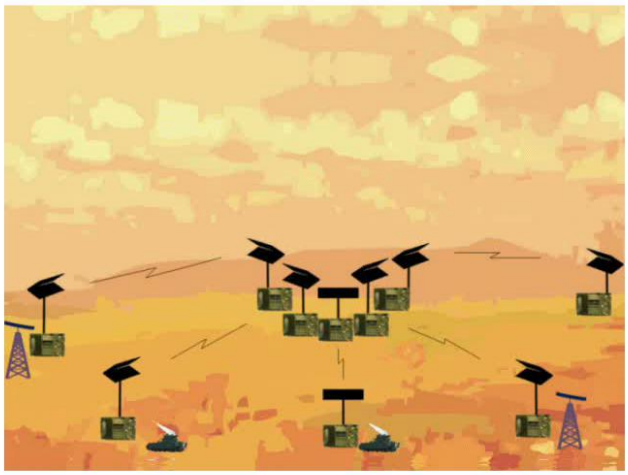
**The FLEX case**

- is a fully flexible portable casing system for 19 inch encryption and communication equipment
- will allow standard commercial equipment to be mounted in the inner frame, no requirement of ruggedized units, the case will handle this
- has sealed covers both on the front and on the back for easy operation and service access
- is fully ruggedized and EMI-proof



# EriTac Point to Multi-point

PTP for communication from a centre point to a number of outstations



# EriTac Point to Multi-point

**PTMP for communication from a centre point to a number of outstations**





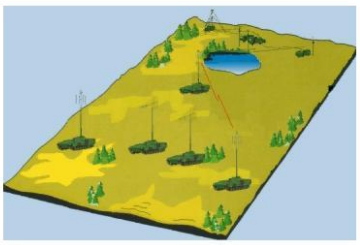
# EriTac Point to Multi-point

**The PTMP also includes full duplex EOW, selective to any outstation**



# EriTac Point to Multi-point

- True point to multi-point communication
- Full duplex data on up to 15 channels
- Data coding (FEC and interleaving)
- Robust air interface (FH)
- Fast TDMA cycle time; approx. 50 ms
  - Short delay
- RL user configurable conventional PTP mode / PTMP mode



TDMA movie



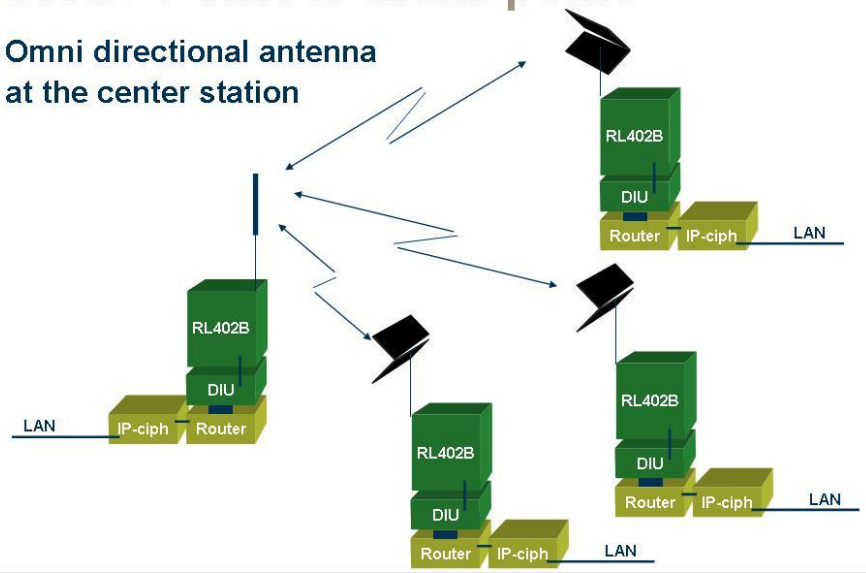
# EriTac Point to Multi-point

## Two System Components: RL402B and DIU

- DIU: A Data Interface Unit, a data multiplexer/demultiplexer with FEC and interleaving
- RL402B: The RL402A with ECCM subunit for up to 15 outstations.



# EriTac Point to Multi-point






# EriTac Point to Multi-point

- Base for the system is the ability for RL402A to maintain full bit and FH synchronization even if a high number of FH timeslots are lost.
- Individual pairs of PRGs for each Outstation makes possible:
  - independent late net entry of outstations
  - independent adaptive FH
  - independent adaptive RF power
- Switching between PTP and TDMA mode from keyboard
- Engineers Order Wire (EOW) Channel
  - full duplex
  - select any outstation from the center station
  - EOW from any outstation to the center station

# EriTac Point to Multi-point

- 256, 512, 1024 and 2048 kbit/s TDM rates
- up to 15 outstations
- user choice of 3, 7 or 15 outstation as maximum number of timeslots
- flexibility in data rate/number subscriber per outstation by using one or several timeslots

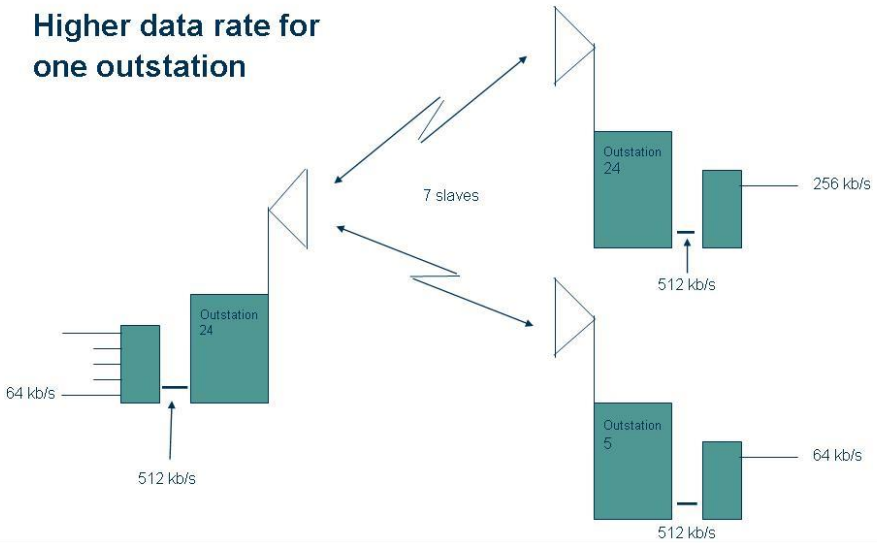
- Selectable number of outstation and data rate configuration

| Number of outstations | RL 256 kb/s | RL 512 kb/s | RL 1024 kb/s | RL 2048 kb/s |
|---|---|---|---|---|
| 3 outstations | 64 kb/s | 128 kb/s | 256 kb/s | 512 kb/s |
| 7 outstations | 32 kb/s | 64 kb/s | 128 kb/s | 256 kb/s |
| 15 outstations | 16 kb/s | 32 kb/s | 64 kb/s | 128 kb/s |



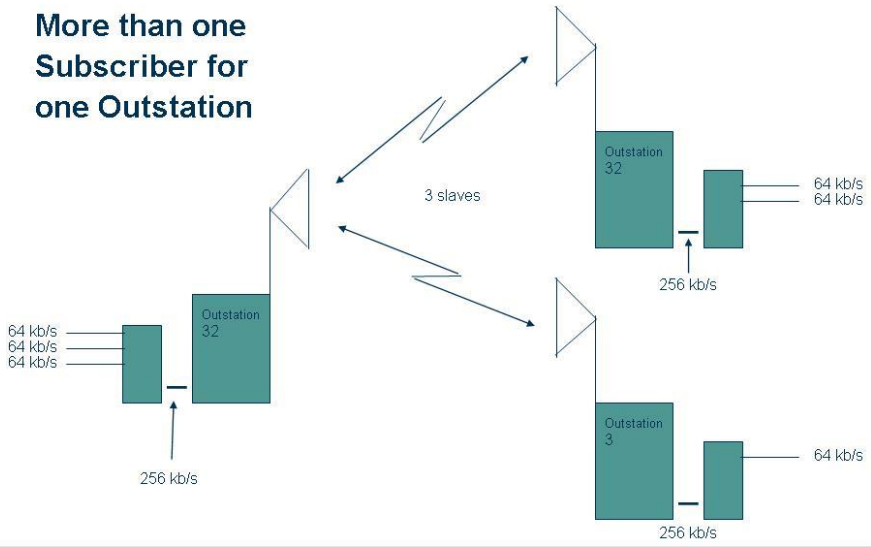
# EriTac Point to Multi-point

**Higher data rate for one outstation**



# EriTac Point to Multi-point

**More than one Subscriber for one Outstation**

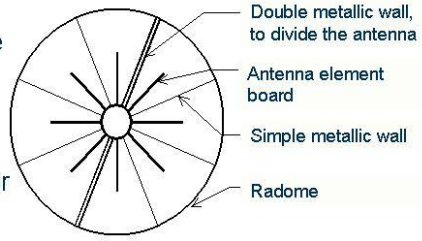





# EriTac Point to Multi-point

**Cylindrical array antenna at the center station**

- The antenna system is to be regarded as an integrated part of the whole communication system
- Cylindrical digital group antenna
  - Up to 8 adaptive lobes with for point-to-multipoint systems
  - Can be adopted for communication "on the move"




- Gain 12 -15 dBi
- 1.35-2.7 GHz
- 1100 x 350 mm
- ca 20 kg

# EriTac Switching products

## CPX 200/300 – Tactical Switch



- Combined access and transit switching functions.
- High switching capacity, 1024 time slot non-blocking switching matrix.
- Five TDM ports according to EUROCOM “A”, V11, E1 and T1.
- TDM port bitrates of 256 - 2048 kbit/s individually selectable.
- 15 position for subscribers line access, each with a free mix of bitrates 16 to 1024 kbit/s.
- ISDN access via single line or E1/T1
- Combat net radio interface
- Supported by Communication Management System (MS200)
- Full military specifications for tactical environment



# EriTac Switching products

## CPX 200/300 – Tactical Switch

**Gateways**



- STANAG 4206 Series Gateway
  - Functionality: Added 512 kbit/s on TDM.
- EUROCOM Gateway
  - Functionality: Added 512 kbit/s on TDM.
- MSE Interface
  - New HW: PRT2-card for frame synch.
  - Functionality: 256 - 2048 kbit/s on TDM, 16 kbit/s subscriber channels, A wide range of subscriber services.

# EriTac Switching products

## CPX 200/300 – Tactical Switch

**CPX300**



- New functionality (1'st release):
  - ISDN PRI connection to PABX/PTT with
    QSIG and Q.931 signaling.
    Available on all ports (through PRT4)
  - STANAG 4578 Gateway
    Available on all ports (through PRT4)
  - V.11 and G.703: 256, 512, 1024 and 2048 Kbit/s. CPX signaling.
    Available on all ports (through PRT4)
  - Connection to CPX200 and CPX250 (latest SW/HW).



# EriTac Switching products

## CPX 200/300 – Tactical Switch

**CPX300**

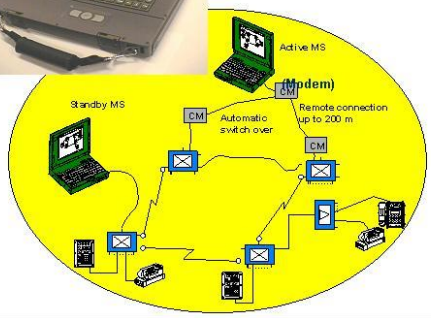


- New functionality (2'nd release):
  - MRR as SCRA connected to the CPX300.
  - Higher bit-rate (512, 1024, 2048 Kbit/s (option)) on the subscriber side
  - New routing algorithm (deterministic routing, frequently called list)
  - Meet-Me conference in DSP
  - 8 Mbit/s on port (optional)

# EriTac Switching products

## Network Management of CPX



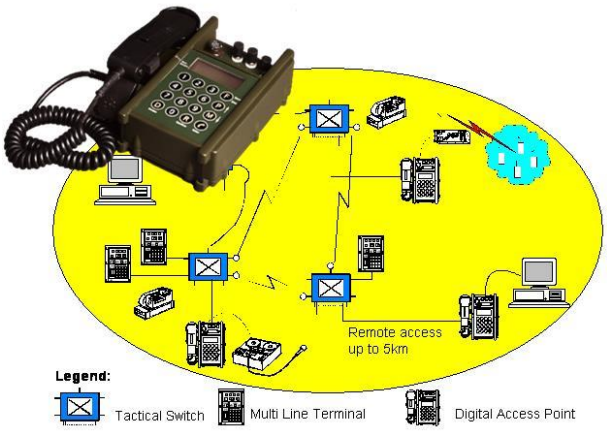



- Real-time management and control of up to 30 CPXes in a network
- Control of network elements (CPX, DMU, etc.)
- Control of subscriber profiles (number, services access, etc.)
- Off-line planning and programming of network, single elements and subscribers
- Automatically change of network control between active and standby MS200



# EriTac Switching products

## DAP220 – Digital Access Point




- Remote access to network
- Analog or Digital equipment access
- Digital telephone
- CNR interface
- Access for analog equipment
- 2-wire line interface up to 5 km (25 dB att.)
- Power feeding from network
- Self test accessible by operator

# EriTac Bulk Encryption Equipment

## CD510



- Full duplex mode of operation
- Unit **configuration with 1-5 full duplex ports:**
  - Removable trunk plug-in modules
  - Individually configurable
  - Independent bit rate
  - Independent traffic keys
  - No error propagation
- Interface
  - Eurocom
  - ITU G.703
  - V.11
- Transmission rate
  - 256 to 2048 kbps for Eurocom
  - 256 to 8448 kbps for V.11
- Fully ruggedized and EMC - proof
- Manageable from external system called SNMC



# EriTac ATM switch

## ATX300



- An ATM/Router based on AXD320
- Has extensive digital voice protocol support enables creatin of switched PBX Virtual Private Network
- Has Interchangeable physical interfaces for transmission rate from 64 kbps to 155 Mbps
- Has ATM UNI 3.1 and 4.0 that supports connection to backbone ATM services with PVC, PVP and SVC
- Supports VoIP using SIP (Session Initiation Protocol
- Has In-band and out-of-band SNMP management access

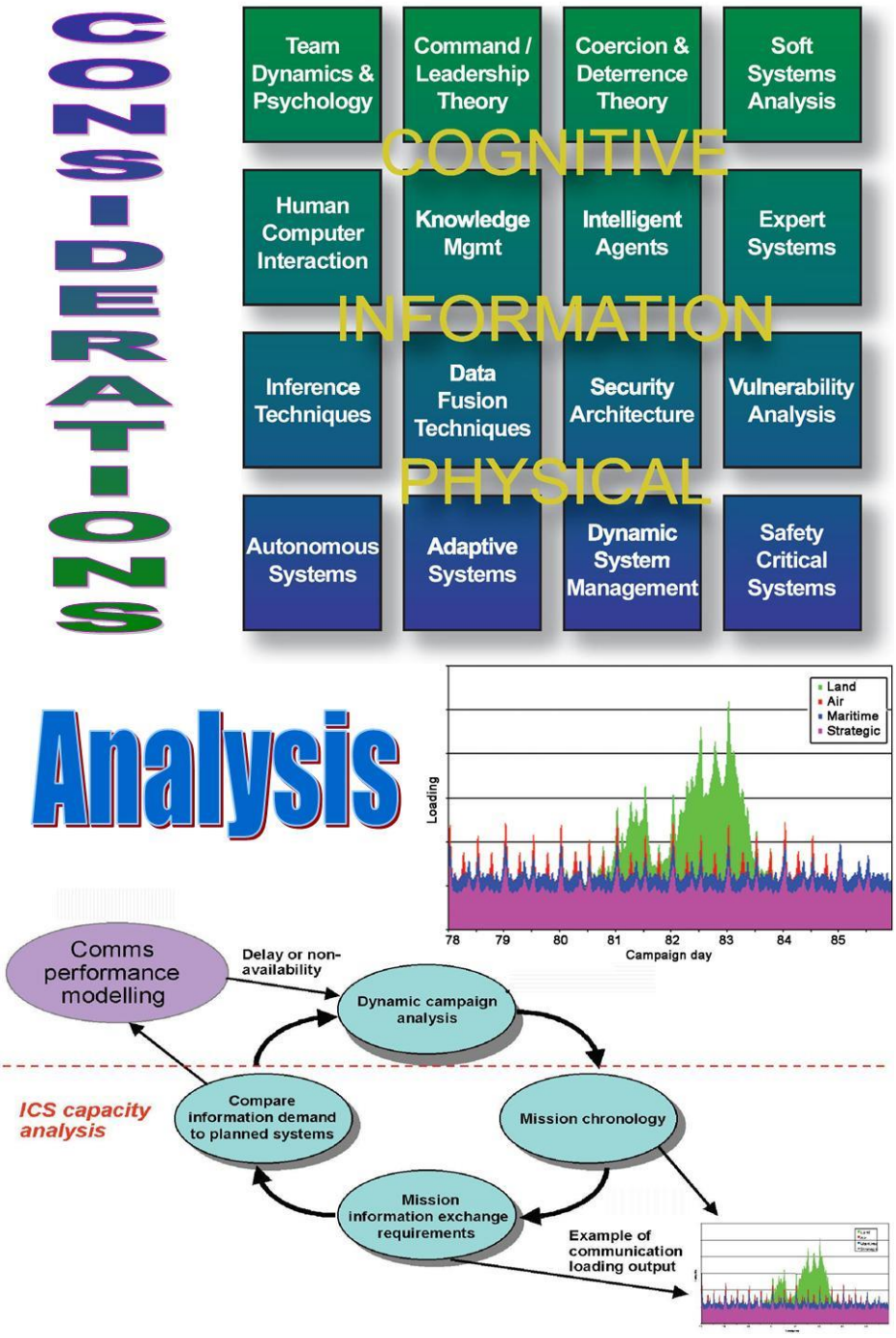

ERICSSON
TAKING YOU FORWARD

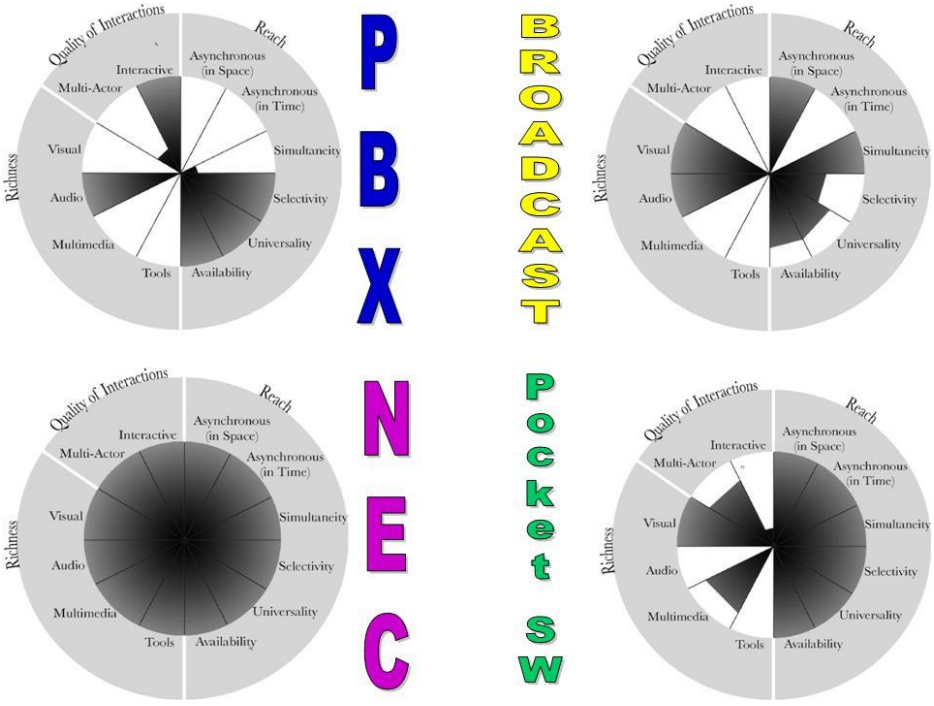
**Károly FEKETE**

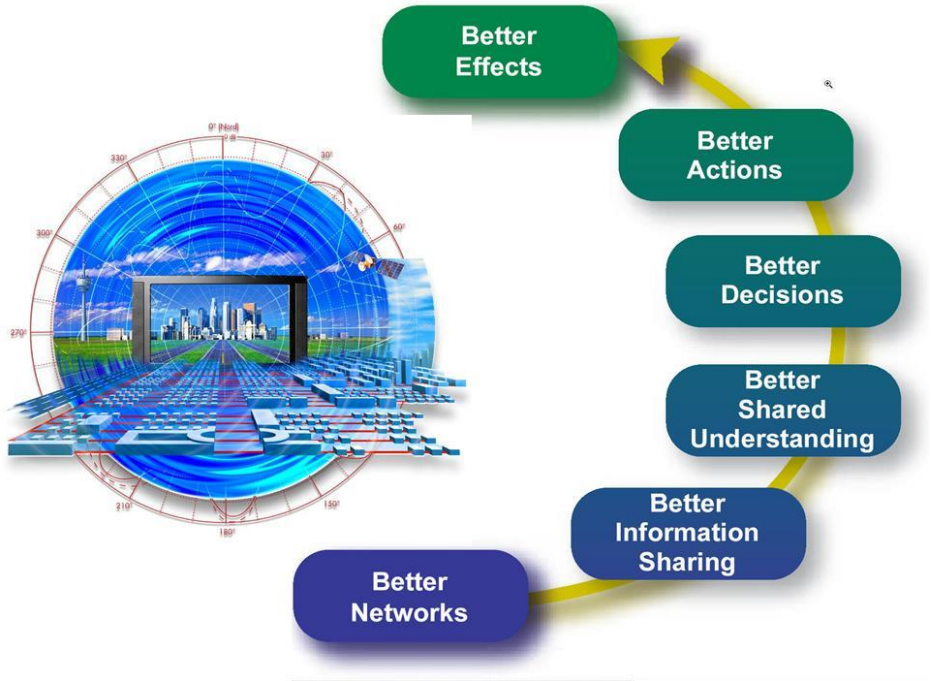
## THE BENEFITS OF HIGH PERFORMANCE WIMAX SOLUTIONS IN MULTINATIONAL MISSIONS

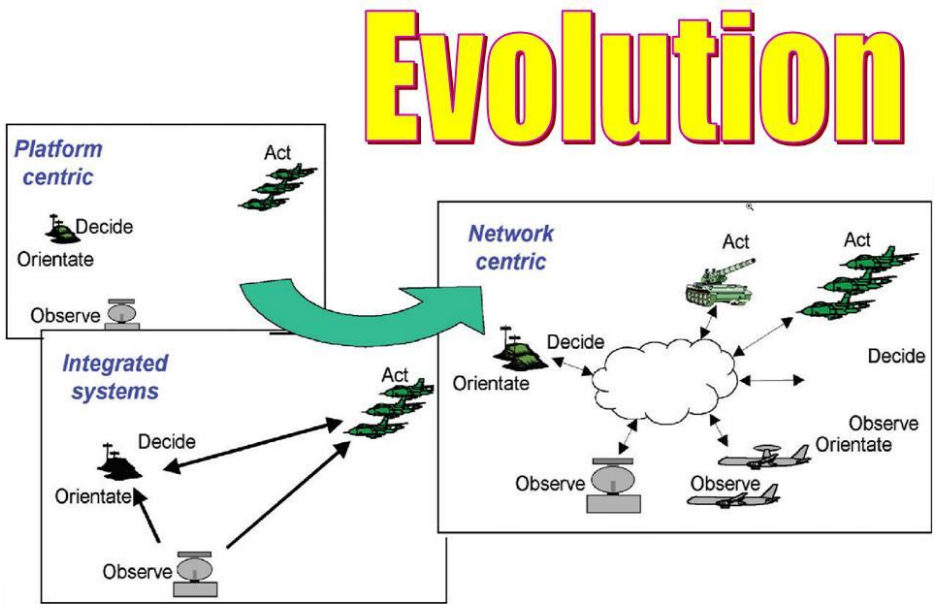






CONSIDERATIONS
Team Dynamics & Psychology
Command / Leadership Theory
Coercion & Deterrence Theory
Soft Systems Analysis
COGNITIVE
Human Computer Interaction
Knowledge Mgmt
Intelligent Agents
Expert Systems
INFORMATION
Inference Techniques
Data Fusion Techniques
Security Architecture
Vulnerability Analysis
PHYSICAL
Autonomous Systems
Adaptive Systems
Dynamic System Management
Safety Critical Systems
Analysis
Land
Air
Maritime
Strategic
Loading
78
79
80
81
82
83
84
85
Campaign day
Comms performance modelling
Delay or non-availability
Dynamic campaign analysis
ICS capacity analysis
Compare information demand to planned systems
Mission chronology
Mission information exchange requirements
Example of communication loading output

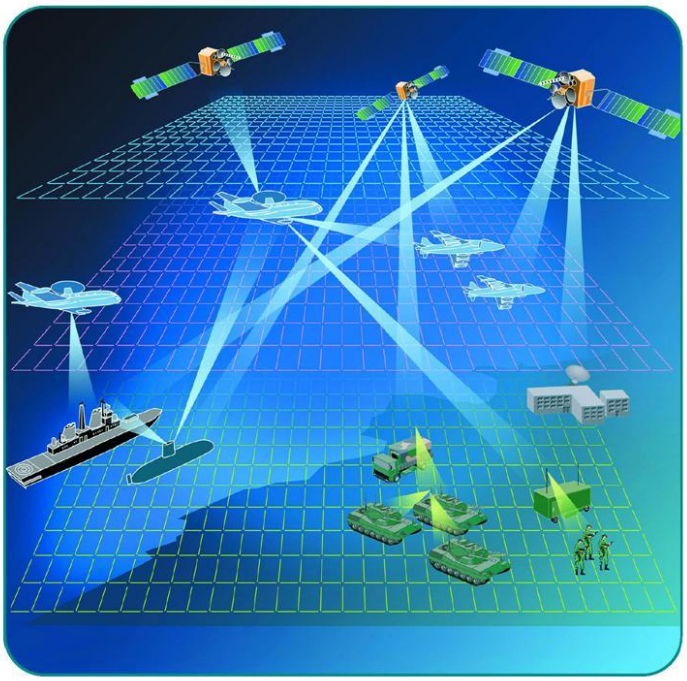

Quality of Interactions
Reach
Richness
Interactive
Asynchronous (in Space)
Multi-Actor
Asynchronous (in Time)
Visual
Simultaneity
Audio
Selectivity
Multimedia
Universality
Tools
Availability
P
B
X
N
E
C
BROADCAST
Pocket sw


Better Effects
Better Actions
Better Decisions
Better Shared Understanding
Better Information Sharing
Better Networks

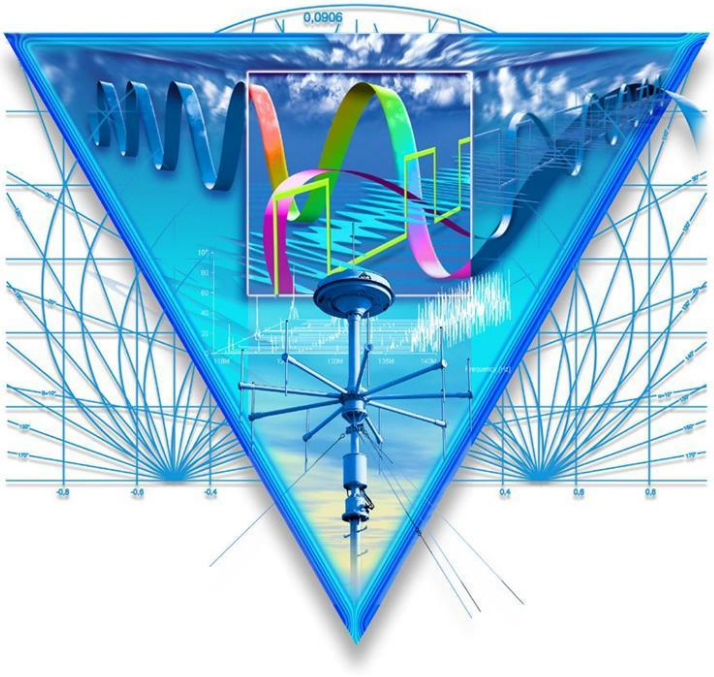

Evolution
Platform centric
Act
Decide
Orientate
Observe
Integrated systems
Act
Decide
Orientate
Observe
Network centric
Act
Act
Decide
Orientate
Decide
Observe
Orientate
Observe
Observe

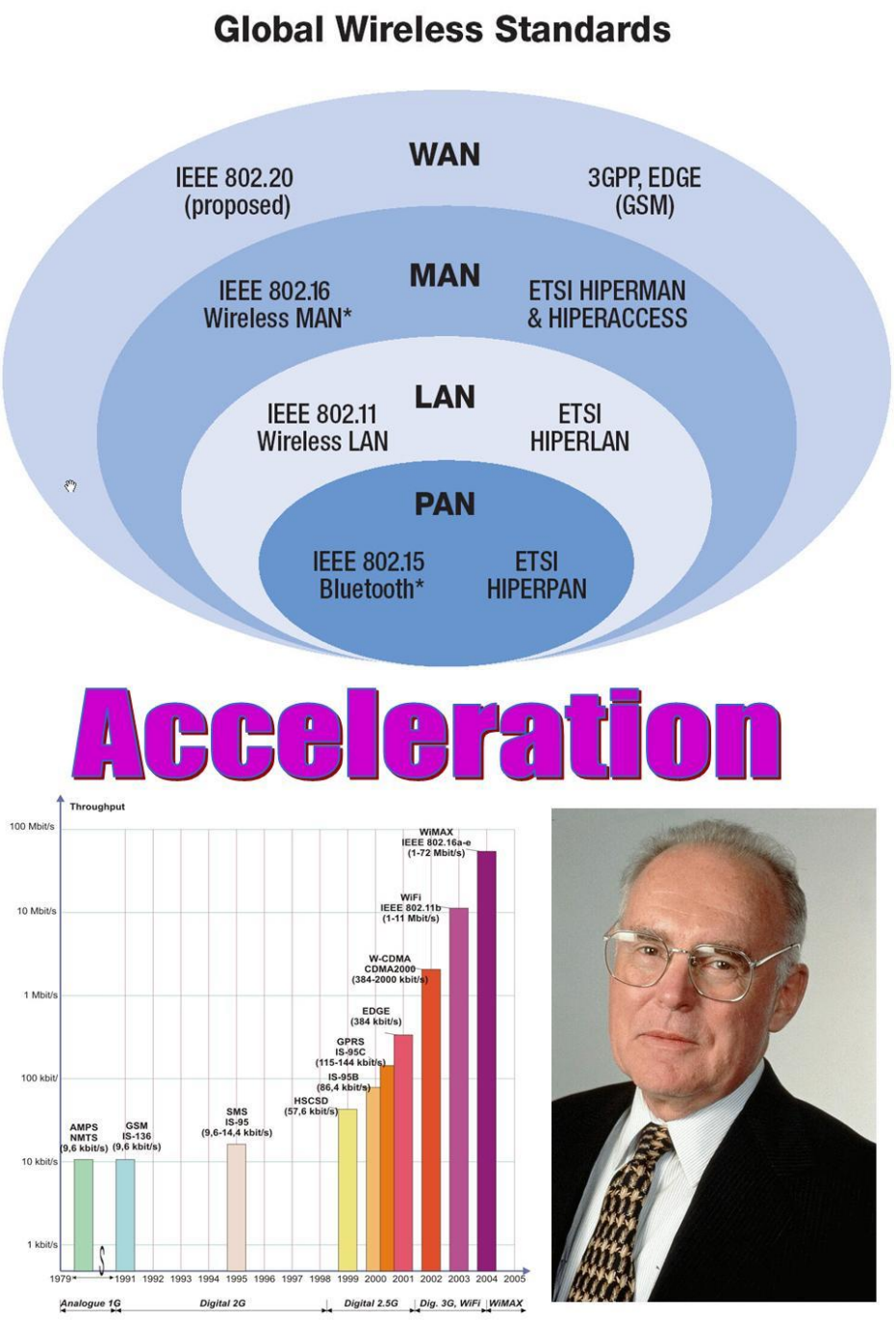

Multinational Missions
Synchronisation of actions

Enhanced infosharing



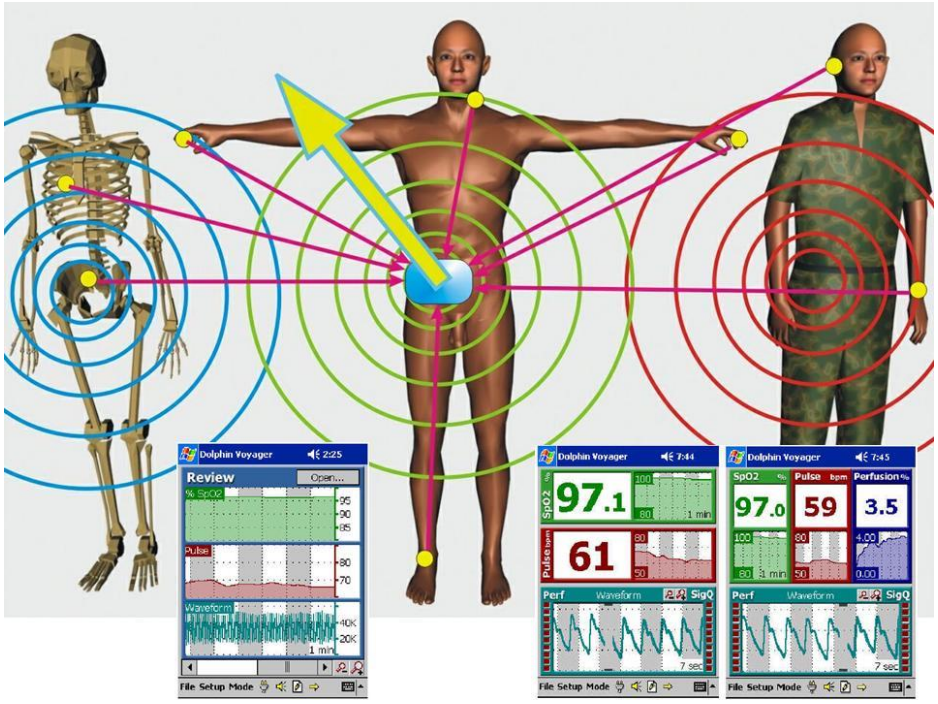
WIMAX

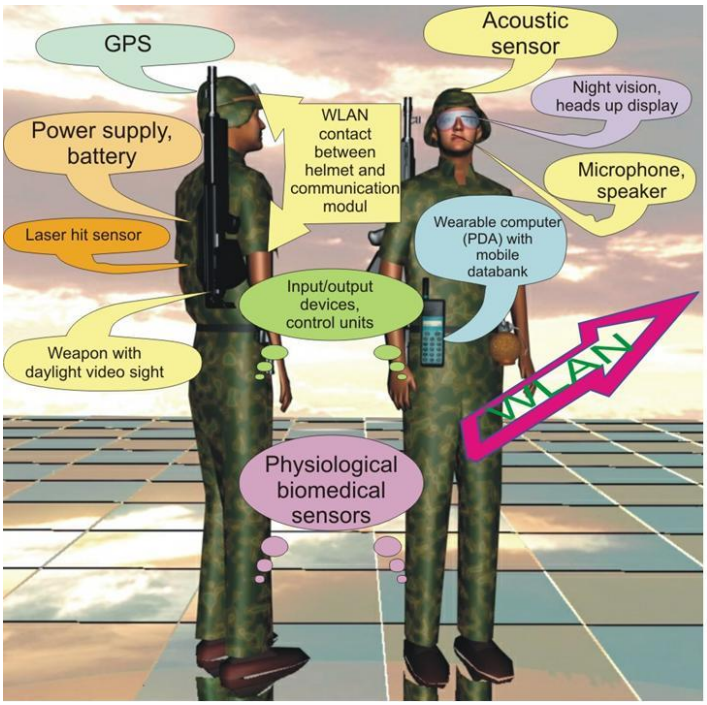



Global Wireless Standards
WAN
IEEE 802.20
(proposed)
3GPP, EDGE
(GSM)
MAN
IEEE 802.16
Wireless MAN*
ETSI HIPERMAN
& HIPERACCESS
LAN
IEEE 802.11
Wireless LAN
ETSI
HIPERLAN
PAN
IEEE 802.15
Bluetooth*
ETSI
HIPERPAN
Acceleration
Throughput
100 Mbit/s
10 Mbit/s
1 Mbit/s
100 kbit/
10 kbit/s
1 kbit/s
AMPS
NMTS
(9,6 kbit/s)
GSM
IS-136
(9,6 kbit/s)
SMS
IS-95
(9,6-14,4 kbit/s)
HSCSD
(57,6 kbit/s)
IS-95B
(86,4 kbit/s)
GPRS
IS-95C
(115-144 kbit/s)
EDGE
(384 kbit/s)
W-CDMA
CDMA2000
(384-2000 kbit/s)
WiFi
IEEE 802.11b
(1-11 Mbit/s)
WiMAX
IEEE 802.16a-e
(1-72 Mbit/s)
1979
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
Analogue 1G
Digital 2G
Digital 2.5G
Dig. 3G, WiFi
WiMAX

# Comparison of WLAN technologies (the most important)

| | IrDA | Bluetooth | IEEE 802.11a | IEEE 802.11b | IEEE 802.16a-e |
|---|---|---|---|---|---|
| **Jellemző alkalmazás** | Optikai adatátvitel elektronikus berendezések között | Vezetéknélküli, kishatótávolságú kapcsolat | Vezetéknélküli helyi számítógépes hálózat | Vezetéknélküli helyi számítógépes hálózat | Vezetéknélküli közepes távolságú szélessávú hálózat (MAN, WDSL) |
| **Technológia** | Optikai (λ=850nm) | 2,4 GHz (FHSS) | 5 GHz (OFDM) | 2,4 GHz (DSSS) | 2-11 GHz (256 FFT OFDM, OFDMA) |
| **Adatsebesség** | 115 kbit/s - 4 Mbit/s | 1 Mbit/s | 6-54 Mbit/s | 1-11 Mbit/s | 1-72 Mbit/s |
| **Max. hatótávolság** | 5 m | 10 m | 30 m | 1000 m | 50 km |
| **Topológia** | Pont-többpont (10 eszköz) | Pont-többpont (8 eszköz) | CSMA/CD (128 eszköz) | CSMA/CD (128 eszköz) | Pont-pont, pont-többpont, mobil |
| **Titkosítás** | OSI alkalmazási rétegben | Nyilvános/Titkos kulcsú hitelesítés és kódolás | WEP (40-128 bites statikus vagy továbbfejlesztett dinamikus kulcs) | WEP (40-128 bites statikus vagy továbbfejlesztett dinamikus kulcs) | Hitelesítés, adattitkosítás és rejtett kisugárzás a 802.16 protokollba beépítve |





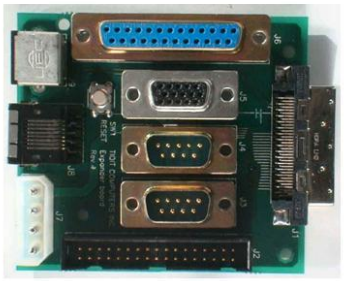

Applications

Realizations



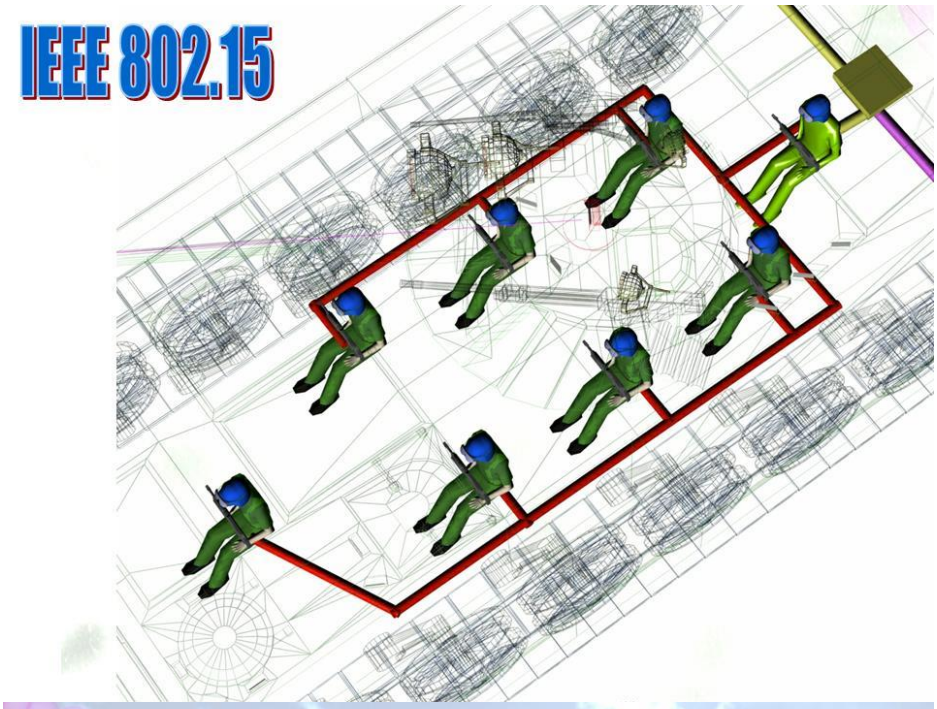

CASSIOPEIA
welcome
Windows



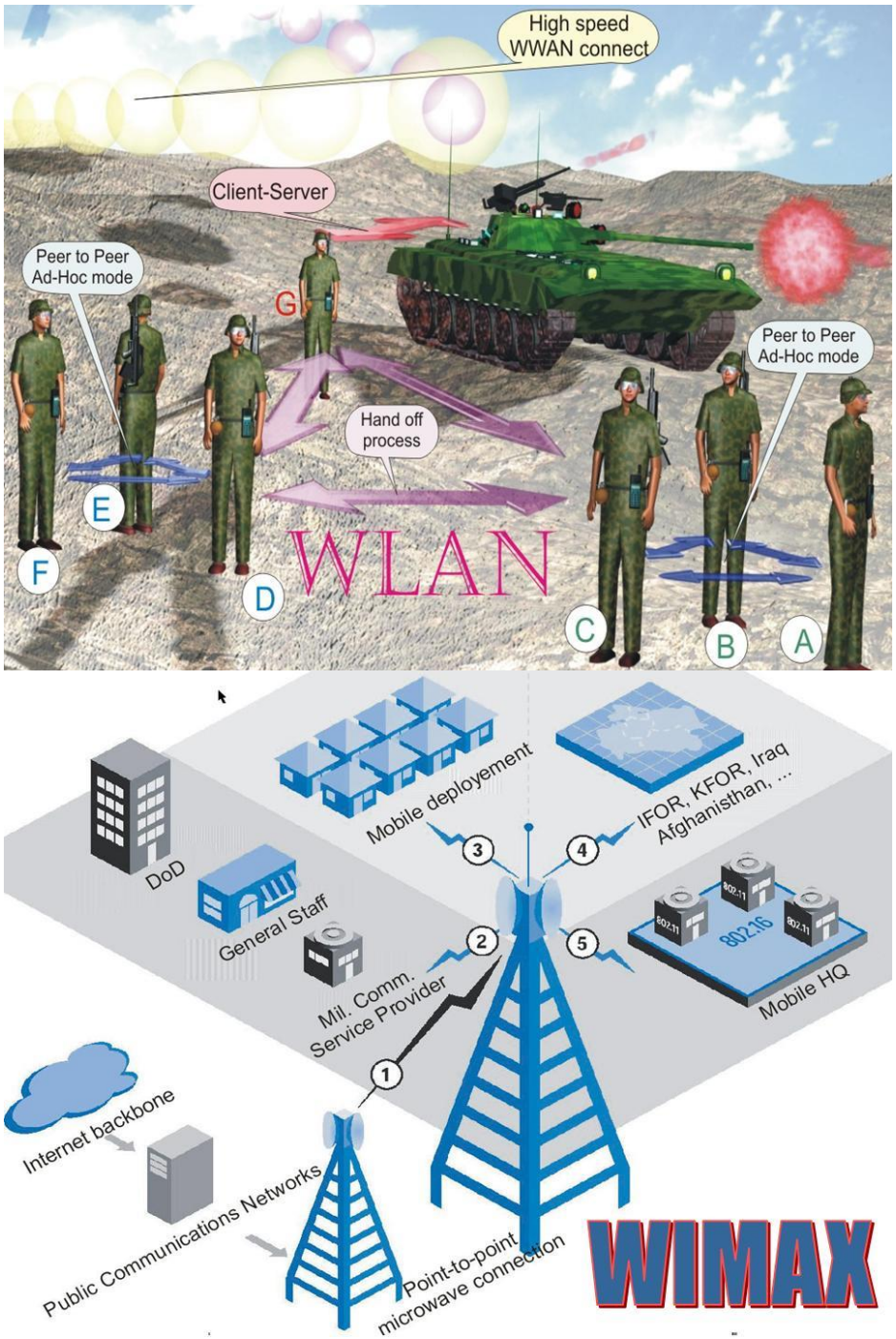





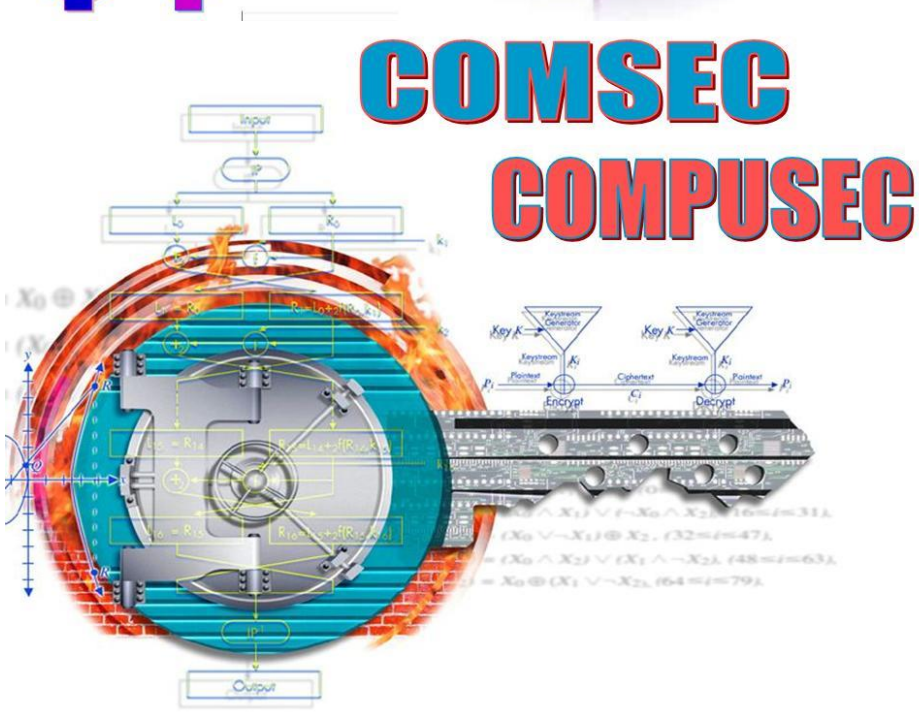




IEEE 802.15


IEEE 802.11 b-g

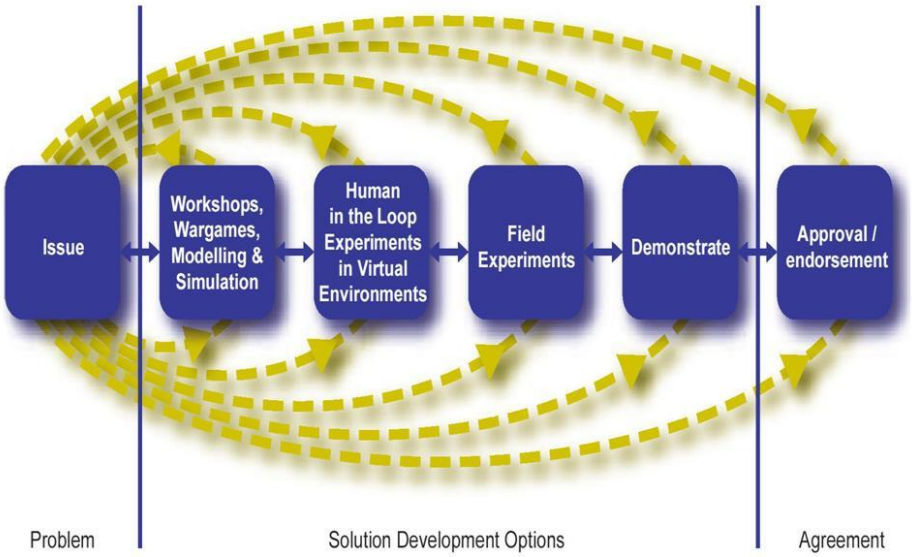

High speed
WWAN connect
Client-Server
Peer to Peer
Ad-Hoc mode
G
Hand off
process
Peer to Peer
Ad-Hoc mode
E
F
D
WLAN
C
B
A
Mobile deployement
IFOR, KFOR, Iraq
Afghanisthan, ...
3
4
DoD
General Staff
2
5
802.16
Mobile HQ
Mil. Comm.
Service Provider
1
Internet backbone
Public Communications Networks
Point-to-point
microwave connection
WIMAX


INTEROPERABILITY
COMPATIBILITY
UNO
KFOR
NATO
SFOR
STANAG 5066
KFOR


COMSEC
COMPUSEC
Input
Output
Encrypt
Decrypt




## The Experimentation Process



# References


1. Dr. Szép József: A NATO új kezdeményezése a hálózat nyújtotta képesség, Kommunikáció 2004 nemzetközi szakmai tudományos konferencia különkiadványa, Budapest, 2004. szeptember 15., pp. 289-303, ISBN 963 86441 5 X
2. IEEE 802.16* and WiMAX, Broadband access for evereyone, White Paper Broadband Wireless Access, Intel Corporation, 2003.
3. www.wimaxforum.org
4. www.ieee802.org/16
5. Dr. Barry Sowerbutts: Network Enabled Capability, Roke Manor Research Limited, Hampshire SO51 OZN UK, NBU/BS/0303/0287.1, www.roke.co.uk
6. David Ferbrache: Network Enabled Capability: concepts and delivery, Journal of Defence Science, Vol. 8., No. 3., September 2003, pp. 104-107.
7. David S. Alberts, Richard E. Hayes: Power to the Edge – Command … Control … in the Information Age, DoD Command and Control Research Program, Library of Congress Cataloging-in-Publication Data, June 2003, ISBN 1-893723-13-5




**FERCOM Kommunikációs Kft.**

## MOTOROLA VEZETÉKNÉLKÜLI ADATKOMMUNIKÁCIÓS RENDSZEREK

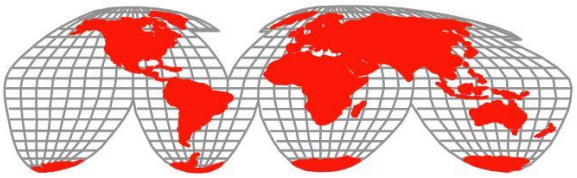
# Motorola Vezetéknélküli Adatkommunikációs Rendszerek

**Kommunikáció 2005 Konferencia,**
**Zrínyi Miklós Nemzetvédelmi Egyetem**

**Budapest, Október 26.**

Data Applications Rev Number 2.0
MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office.
All other product or service names are the property of their respective owners. © Motorola, Inc. 2005

## Motorola Inc.



- **Alapítva 1928-ban**
- **Mintegy 80 000 alkalmazott világszerte**
- **34 milliárd USD éves forgalom 2004-ben**
- **Jelenlét 160 országban**
- **Több mint 4 milliárd USD elköltve 2004-ben kutatás-fejlesztésre**

Data Applications Rev Number 2.0
MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office.
All other product or service names are the property of their respective owners. © Motorola, Inc. 2005

# Motorola Adat Alkalmazások

**Mobil Adat Eszközök**

Gépjárműbe telepített
Kézi
Hordozható laptopok
Elsősorban közbiztonsági alkalmazások





**Telepített Adat Eszközök**

– Telepített alkalmazások
– SCADA alkalmazások
– Hálózati Felügyelet rádiórendszerek számára





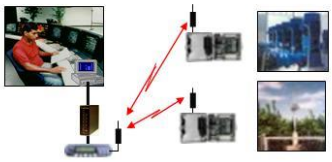

# Mobile Eszközök Katonai Alkalmazása



## Motorola - Telemetria - SCADA Üzletág

**SCADA = Supervisory Control And Data Acquisition**

**R T U = Remote Terminal Unit**



**MOSCAD = MOTOROLA SCADA**

**Üzletági Tapasztalat**

- 36 éve a SCADA piacon
- Elsősorban rádiós kommunikáció
- Több mint 8 000 felhasználó világszerte
- Katonai, vállalati és magánfelhasználók

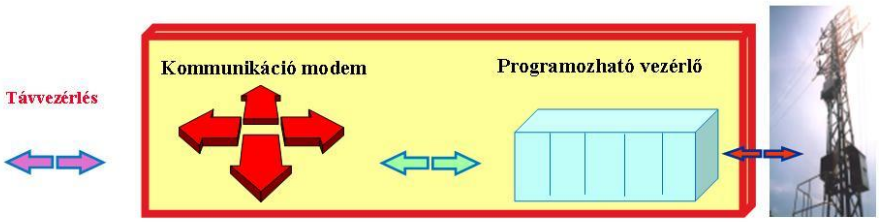


## MOSCAD RTU, aminek a kommunikáció az erőssége

**A különbség !!**

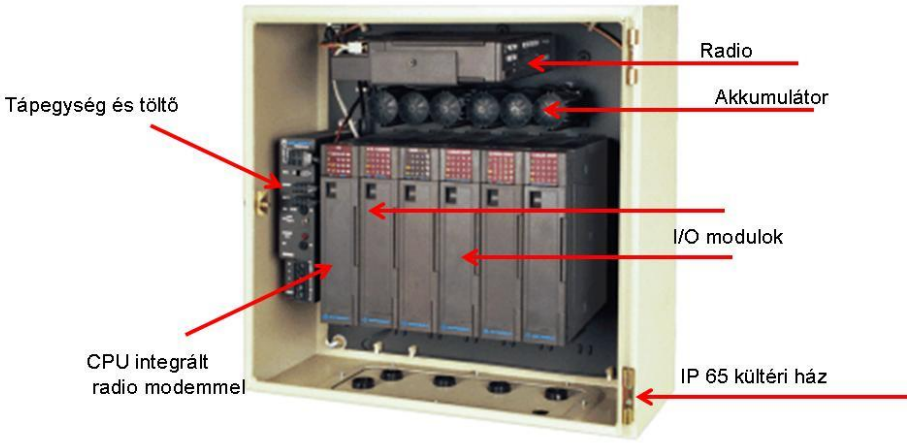
**Két funkció sikeres kombinációja :**

- **Programozható vezérlő (PLC, Programmable Logic Controller)**
- **Nagyteljesítményű kommunikációs modem**



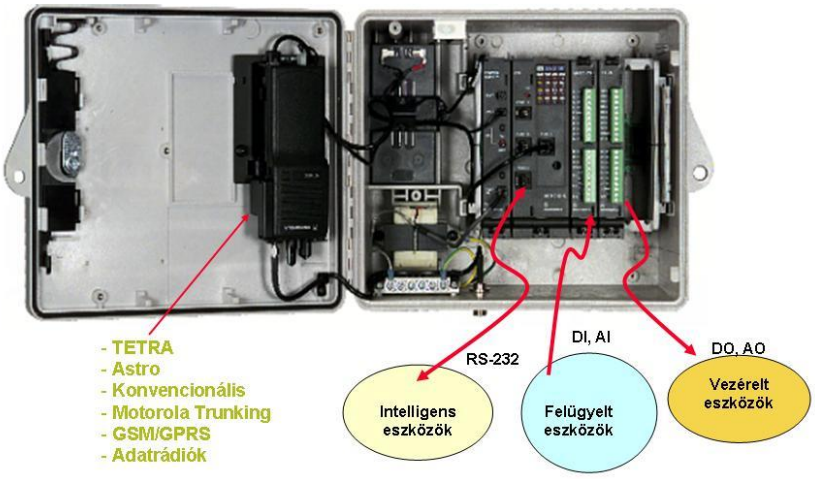

**Egy egység, kisebb helyigény, egy tápegység, egy CPU, egy programozás, kisebb áramfelvétel**

## A MOSCAD RTU

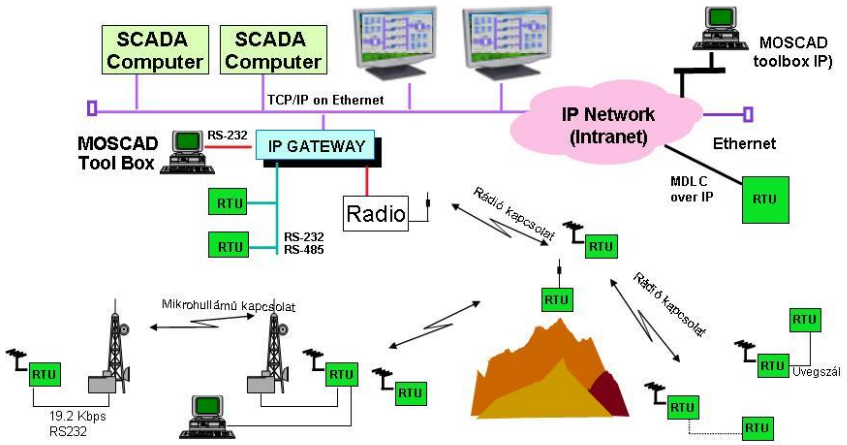





## Moscad-L Remote Terminal Unit

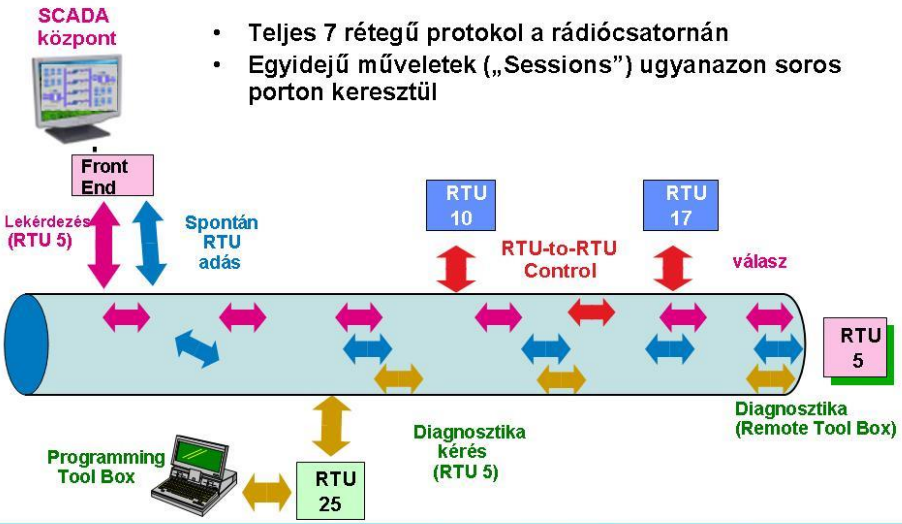


# A MOSCAD és az MDLC kommunikáció



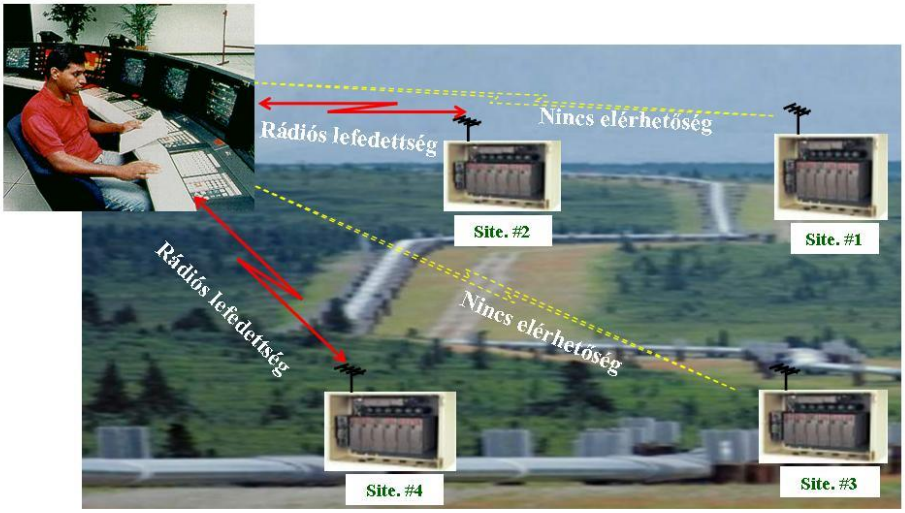



# MOSCAD MDLC kommunikáció



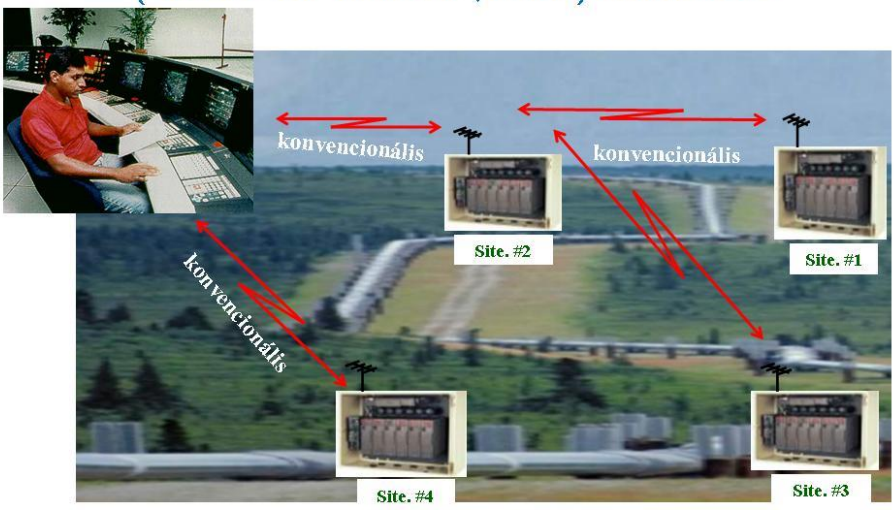

- Teljes 7 rétegű protokol a rádiócsatornán
- Egyidejű műveletek („Sessions”) ugyanazon soros porton keresztül

## MOSCAD - rádiós lefedettség növelés

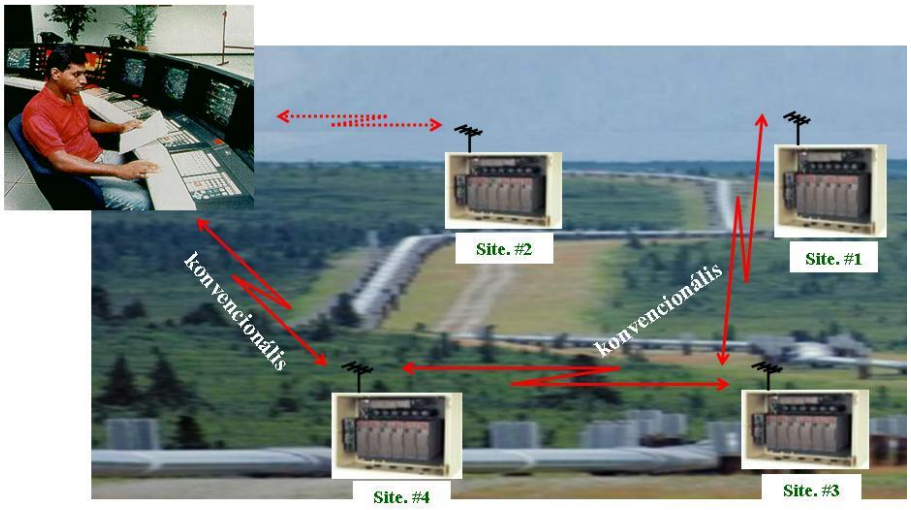





## A tárol-majd-továbbít ("Store & Forward", S&F) működés

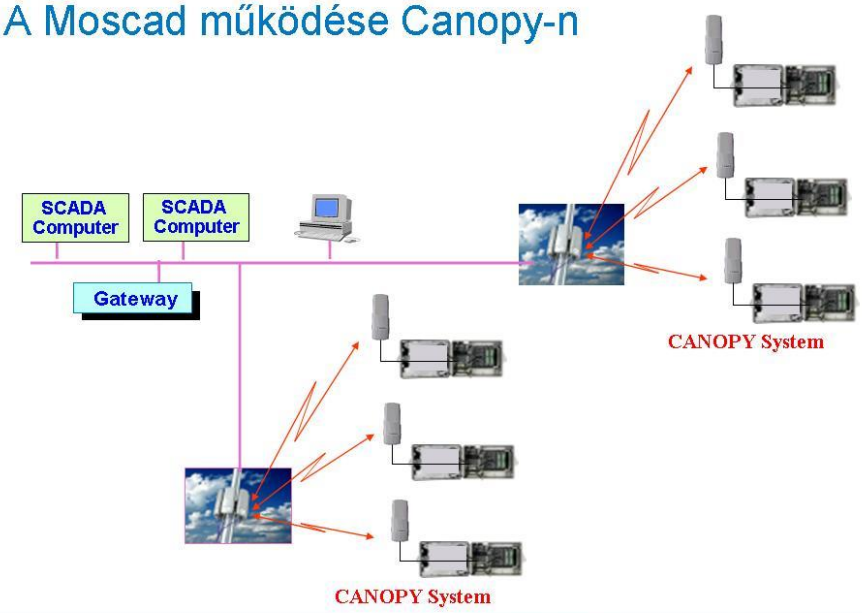


## Automatikus alternatív útvonalválasztás !

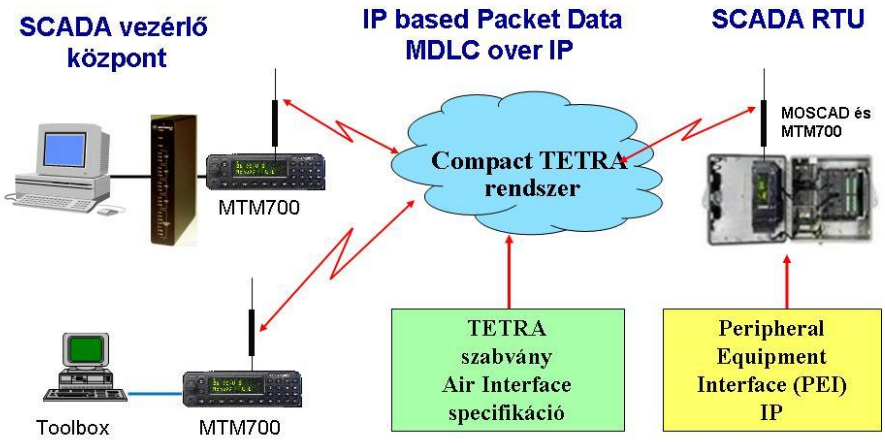





## A Moscad működése Canopy-n



# A Moscad működése TETRA rendszeren




Data Applications Rev Number 2.0
MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office.
All other product or service names are the property of their respective owners. © Motorola, Inc. 2005
Fercom
MOTOROLA

# Scada biztonsági megoldások

**Jelszó alapú azonosítás**

A belépő csak a szintjének megfelelően fér a rendszerhez

Különbséget teszünk az azonosított felhasználók között

**Igazolás**

A személy jogosultságának igazolása

Az újraküldött üzenetek érvénytelenségének biztosítása

**Titkosítás**

“Magánbeszélgetés” a SCADA egyedek között

A küldött üzenetek tartalmi megfejtésének megelőzése

Data Applications Rev Number 2.0
MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office.
All other product or service names are the property of their respective owners. © Motorola, Inc. 2005
Fercom
MOTOROLA

# MOSCAD ALKALMAZÁSOK


MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office.
All other product or service names are the property of their respective owners. © Motorola, Inc. 2005

Fercom MOTOROLA

## Aknamező kiképző rendszer



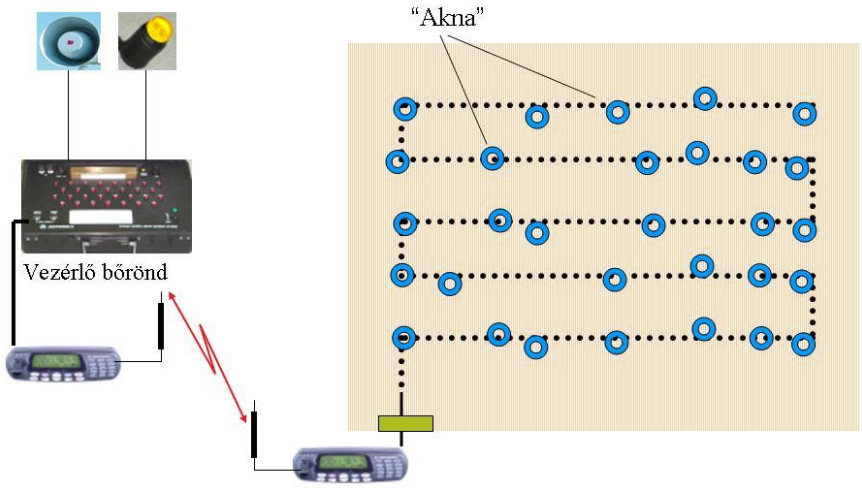





MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office.
All other product or service names are the property of their respective owners. © Motorola, Inc. 2005

Fercom MOTOROLA

## Aknamező kiképző rendszer




Data Applications Rev Number 2.0
MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office.
All other product or service names are the property of their respective owners. © Motorola, Inc. 2005

Fercom MOTOROLA

## Robot Távvezérlés



Data Applications Rev Number 2.0
MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office.
All other product or service names are the property of their respective owners. © Motorola, Inc. 2005

Fercom MOTOROLA

## Lőtéri kiképző rendszer

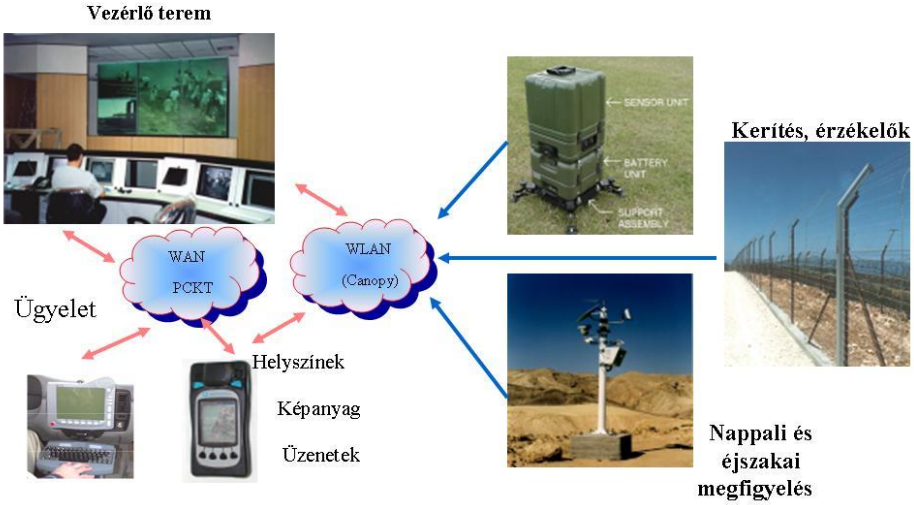




Data Applications Rev Number 2.0
MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office.
All other product or service names are the property of their respective owners. © Motorola, Inc. 2005

Fercom MOTOROLA

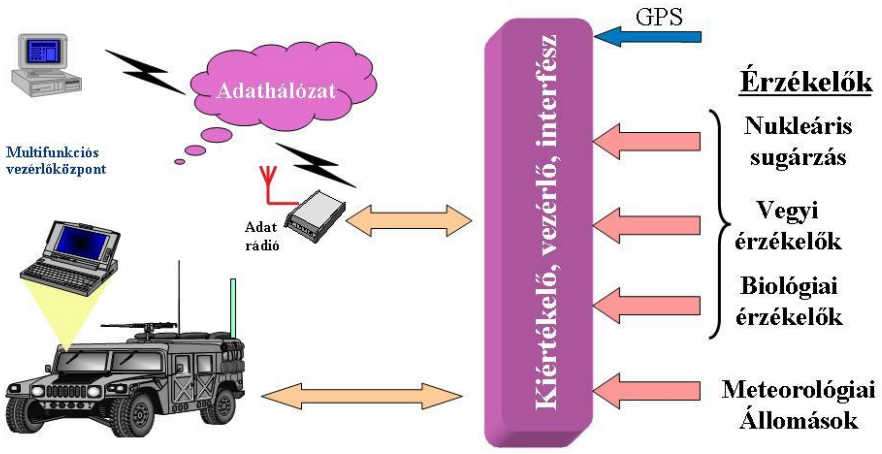
## Védett objektumok biztonsági rendszere




Data Applications Rev Number 2.0
MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office.
All other product or service names are the property of their respective owners. © Motorola, Inc. 2005

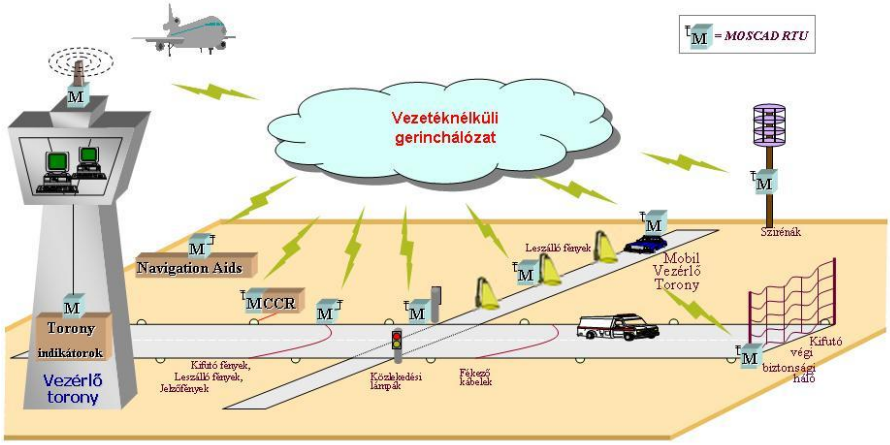
Fercom MOTOROLA

## Veszélyhelyzeti megfigyelő rendszer




Data Applications Rev Number 2.0
MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners. © Motorola, Inc. 2005
Fercom
MOTOROLA

## Repülés-vezérlő torony alkalmazás




Data Applications Rev Number 2.0
MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners. © Motorola, Inc. 2005
Fercom
MOTOROLA

## Sziréna vezérlő rendszerek







Data Applications Rev Number 2.0
MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office.
All other product or service names are the property of their respective owners. © Motorola, Inc. 2005

Fercom

MOTOROLA

Fercom

MOTOROLA
intelligence everywhere™

## Köszönjük figyelmüket !

**KAPSCH Telecom Kft.**

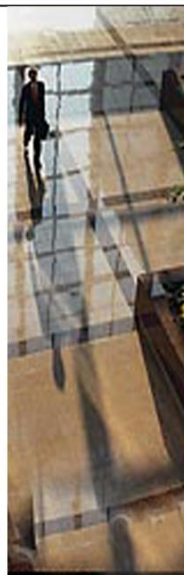
## VIDEÓ MEGFIGYELÉS EGY KICSIT MÁSKÉPPEN

NetAVIS we observe — Kapsch TeleCom Kft. | kapsch >>>

# Videó megfigyelés egy kicsit másképpen

## avagy IP-alapú videó megfigyelő rendszer a Kapsch-tól

Szabó Zoltán
*zoltan.szabo@kapsch.net*



NetAVIS we observe — Kapsch TeleCom Kft. | kapsch >>>

## Miről is lesz szó?

- IP hálózati videó megfigyelő rendszerek – miért?
- A NetAViS hálózatok általános felépítése
- A NetAViS előnyei, főbb funkciók bemutatása



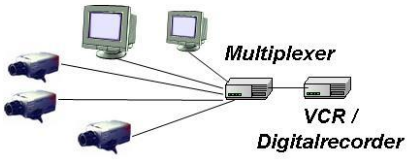
NetAVIS we observe

Kapsch TeleCom Kft. | kapsch >>>

## Hálózati videó megfigyelő rendszerek – miért?

A hagyományos CCTV rendszerek jellemzői

- **Előnyök:**
  - Kiforrott, több évtizedes technológia
- **Hátrányok:**
  - Kazettacsere
  - Távoli használat és menedzsment hiánya
  - Új szolgáltatások nem, vagy csak nehezen integrálhatók
  - Helyi, elszigetelt, centralizált rendszerek



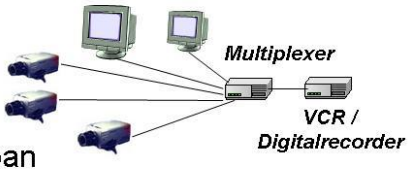

NetAVIS we observe

Kapsch TeleCom Kft. | kapsch >>>

## Hálózati videó megfigyelő rendszerek – miért?

A DVR alapú rendszerek jellemzői

- **Előnyök:**
  - Kiforrott technológia
  - Jelenleg a legelterjedtebb technológia
- **Hátrányok:**
  - Nem elég rugalmas
  - Analóg rendszerek megoldásai digitális formában
  - Új szolgáltatások nem, vagy csak nehezen integrálhatók



## Hálózati videó megfigyelő rendszerek – miért?

A PC alapú rendszerek jellemzői

- **Előnyök:**
  - Alacsonyabb ár – nem mindig
  - Rugalmasabb „upgrade”
  - Ismertség
- **Hátrányok:**
  - Hálózatos szolgáltatásai korlátozottak
  - Bővíthetősége korlátozott
  - A legkevésbé megbízható rendszer




NetAVIS we observe
Kapsch TeleCom Kft. | kapsch >>>

## Hálózati videó megfigyelő rendszerek – mert...

Hálózat (IP) alapú videó rendszerek jellemzői

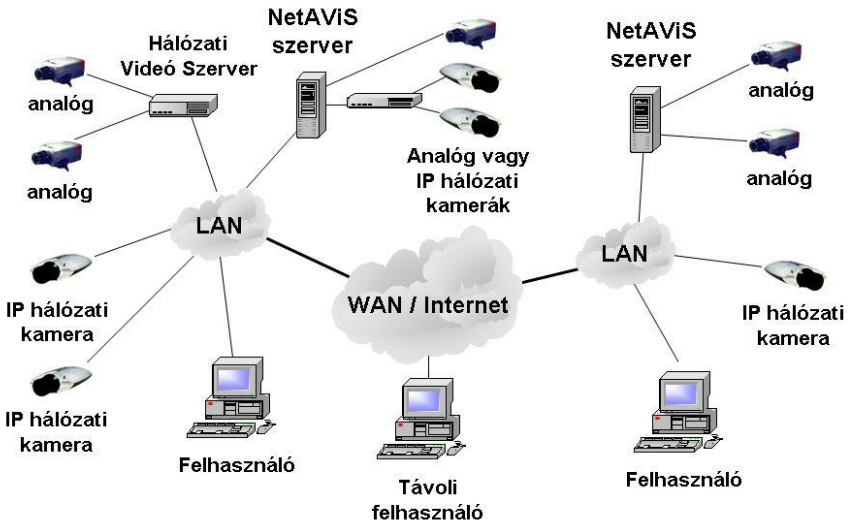
- **Előnyök:**
  - Korlátlan kameraszám egy rendszerben
  - A videó képek a világ bármely részére eljuttathatók
  - Nem helyhez kötött (pl. PDA)
  - Könnyen integrálható más rendszerekkel
  - A hagyományos rendszerek is integrálhatók
  - Könnyű új szolgáltatásokat hozzáfejleszteni
- **Hátrányok:**
  - Új technológia



NetAVIS we observe

Kapsch TeleCom Kft. | kapsch >>>

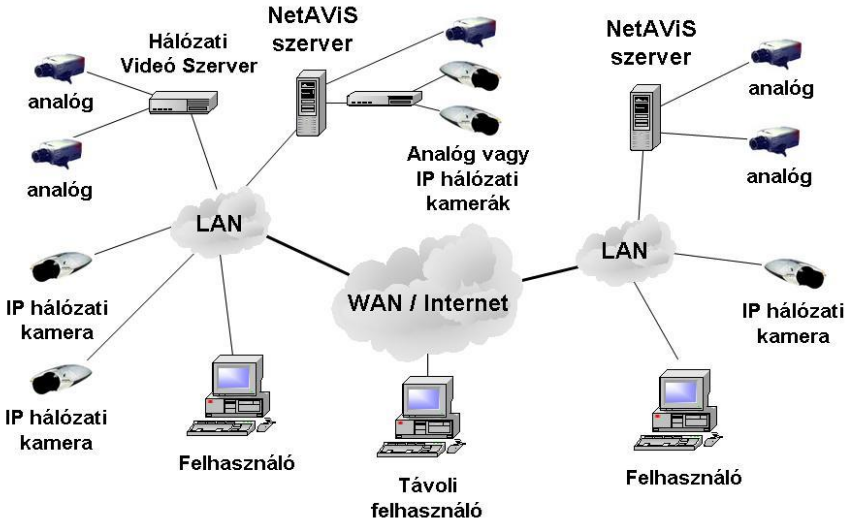
# A NetAVIS hálózatok általános felépítése

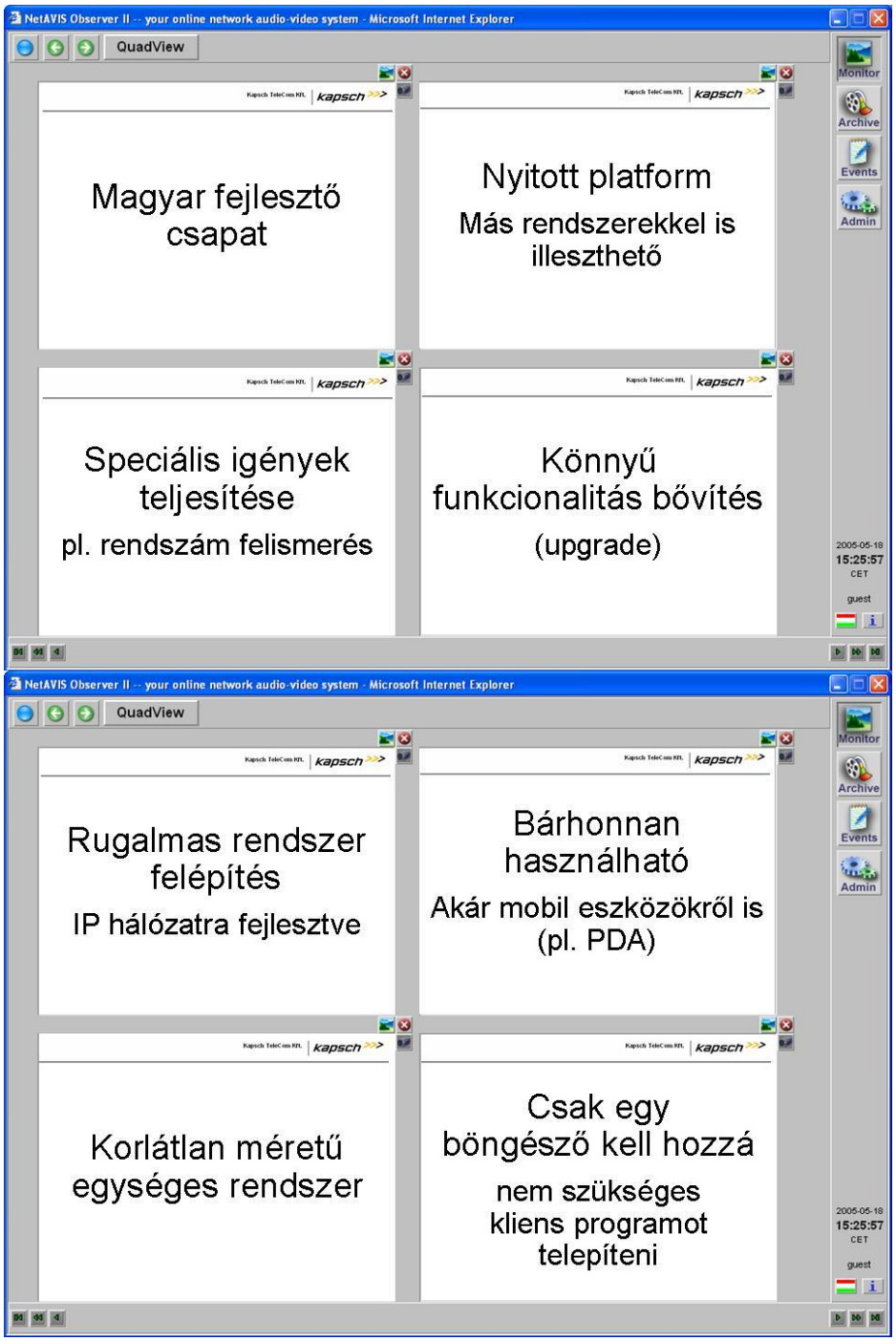


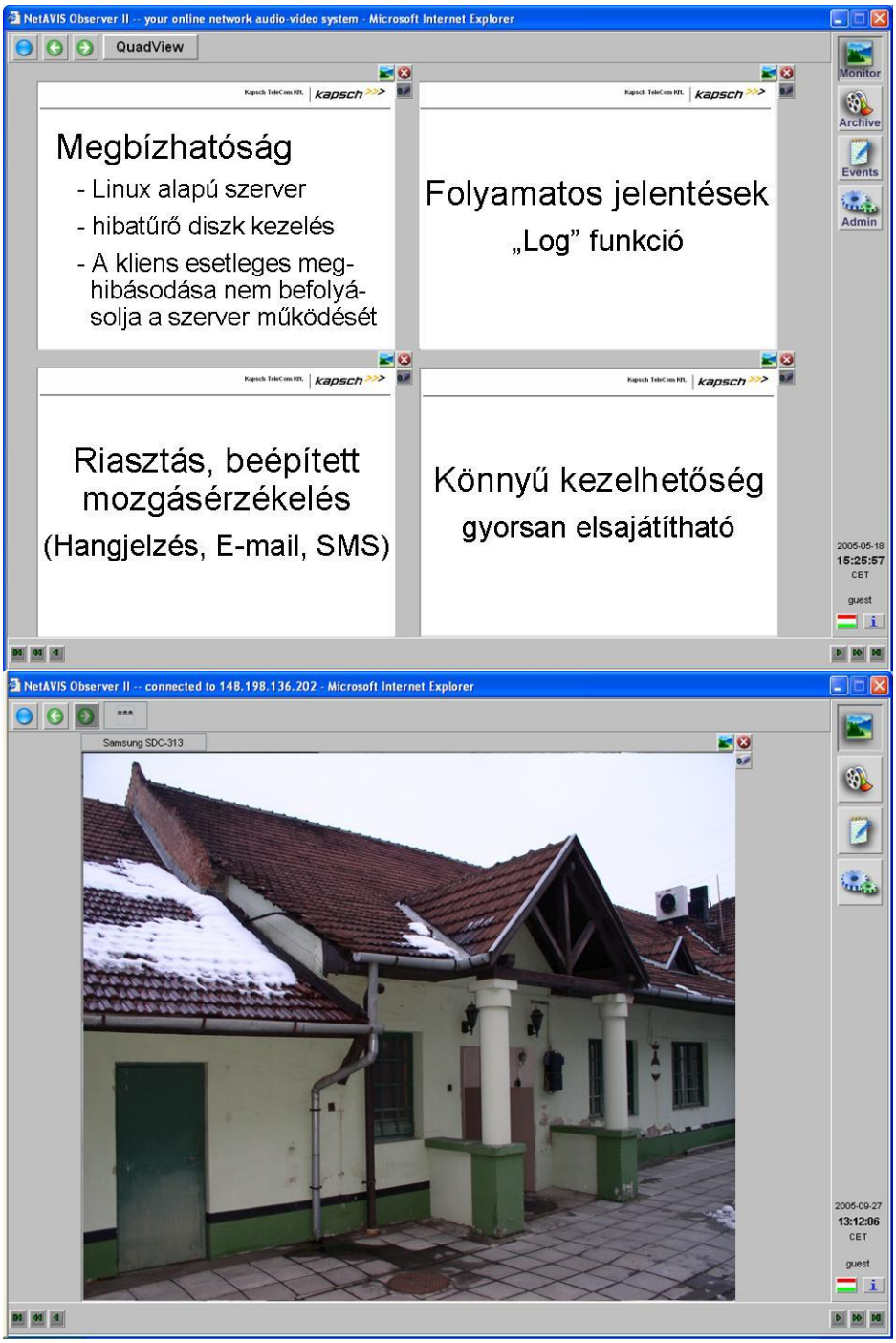

NetAVIS we observe

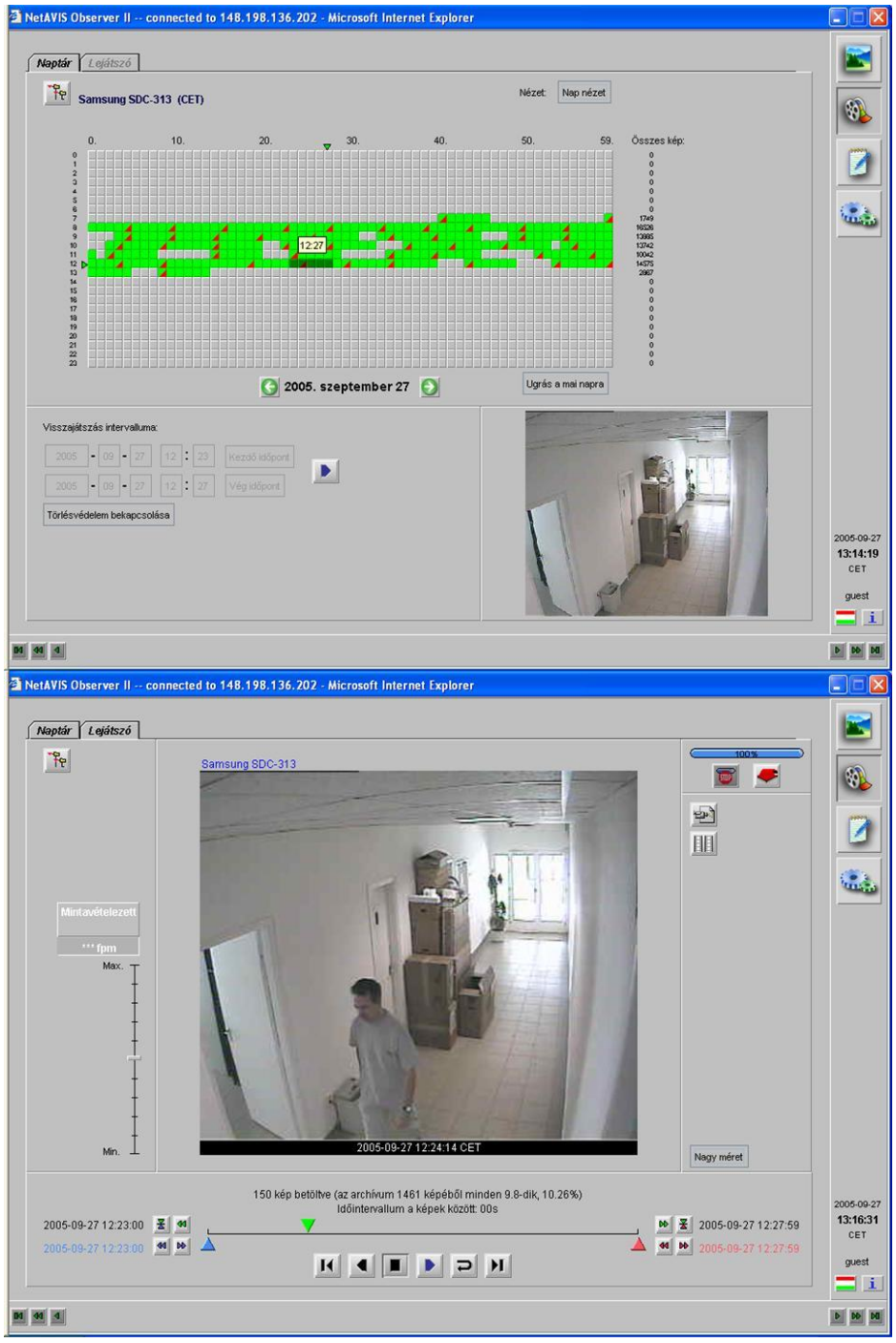
Kapsch TeleCom Kft. | kapsch >>>

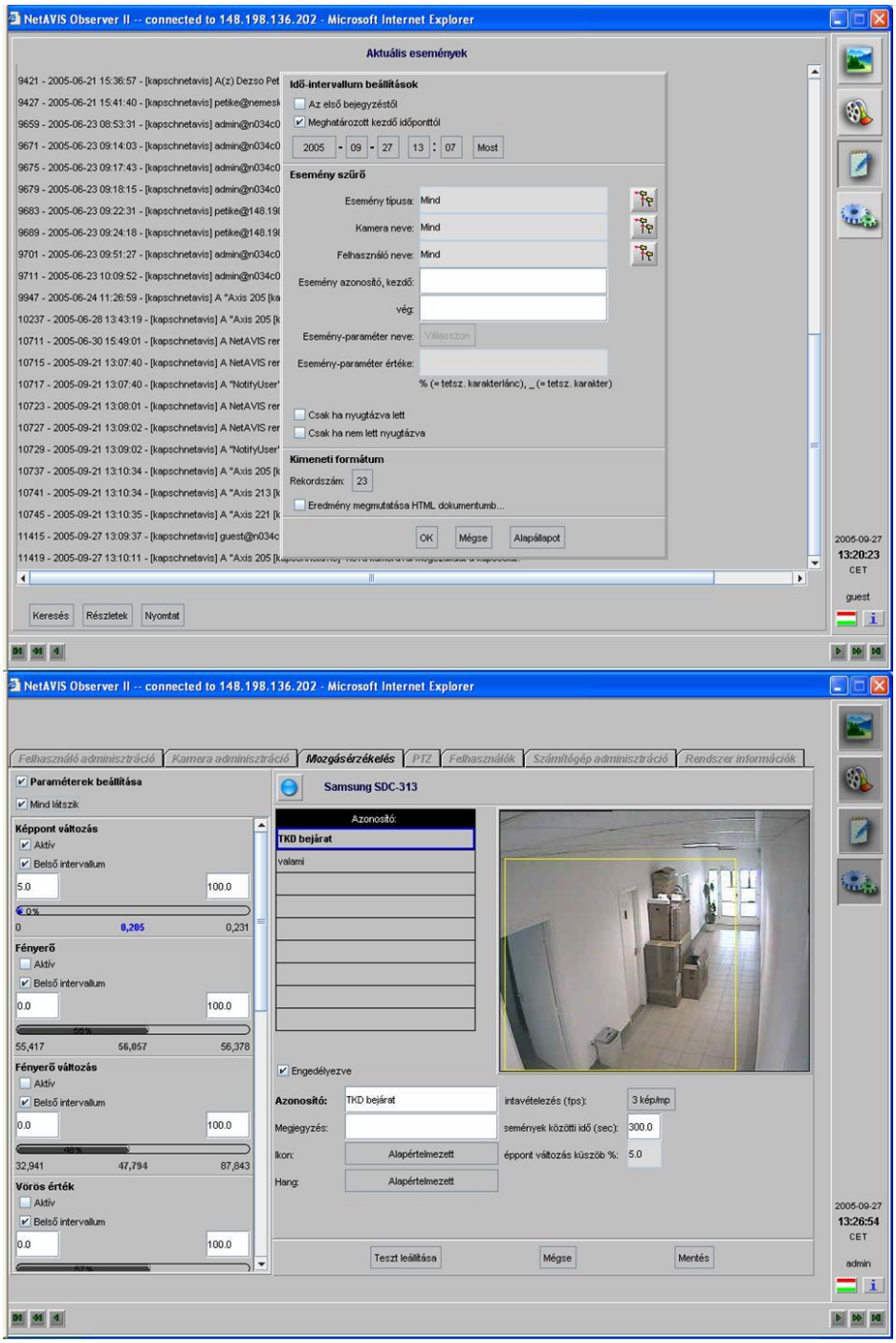
A NetAVIS hálózatok általános felépítése

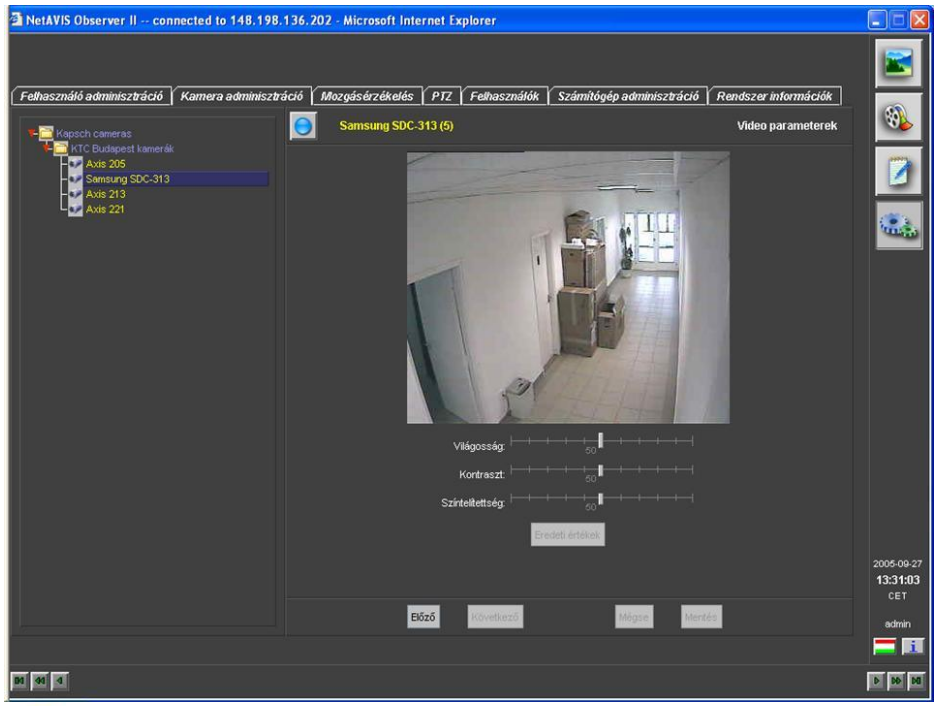



NetAVIS Observer II -- your online network audio-video system - Microsoft Internet Explorer
QuadView
Monitor
Archive
Events
Admin
Magyar fejlesztő csapat
Nyitott platform
Más rendszerekkel is illeszthető
Speciális igények teljesítése
pl. rendszám felismerés
Könnyű funkcionalitás bővítés
(upgrade)
2005-05-18
15:25:57
CET
guest
NetAVIS Observer II -- your online network audio-video system - Microsoft Internet Explorer
QuadView
Monitor
Archive
Events
Admin
Rugalmas rendszer felépítés
IP hálózatra fejlesztve
Bárhonnan használható
Akár mobil eszközökről is (pl. PDA)
Korlátlan méretű egységes rendszer
Csak egy böngésző kell hozzá
nem szükséges kliens programot telepíteni
2005-05-18
15:25:57
CET
guest


NetAVIS Observer II -- your online network audio-video system - Microsoft Internet Explorer
QuadView
Monitor
Archive
Events
Admin
Megbízhatóság
- Linux alapú szerver
- hibatűrő diszk kezelés
- A kliens esetleges meg-
hibásodása nem befolyá-
solja a szerver működését
Folyamatos jelentések
„Log" funkció
Riasztás, beépített
mozgásérzékelés
(Hangjelzés, E-mail, SMS)
Könnyű kezelhetőség
gyorsan elsajátítható
2005-05-18
15:25:57
CET
guest
NetAVIS Observer II -- connected to 148.198.136.202 - Microsoft Internet Explorer
Samsung SDC-313
2005-09-27
13:12:06
CET
guest


NetAVIS Observer II -- connected to 148.198.136.202 - Microsoft Internet Explorer
Naptár
Lejátszó
Samsung SDC-313 (CET)
Nézet:
Nap nézet
Összes kép:
12:27
2005. szeptember 27
Ugrás a mai napra
Visszajátszás intervalluma:
Kezdő időpont
Végi időpont
Törlésvédelem bekapcsolása
2005-09-27
13:14:19
CET
guest
NetAVIS Observer II -- connected to 148.198.136.202 - Microsoft Internet Explorer
Naptár
Lejátszó
Samsung SDC-313
100%
Mintavételezett
*** fpm
Max.
Min.
2005-09-27 12:24:14 CET
Nagy méret
150 kép betöltve (az archívum 1461 képéből minden 9.8-dik, 10.26%)
Időintervallum a képek között: 00s
2005-09-27 12:23:00
2005-09-27 12:27:59
2005-09-27
13:16:31
CET
guest


NetAVIS Observer II -- connected to 148.198.136.202 - Microsoft Internet Explorer
Aktuális események
Idő-intervallum beállítások
Az első bejegyzéstől
Meghatározott kezdő időponttól
Most
Esemény szűrő
Esemény típusa: Mind
Kamera neve: Mind
Felhasználó neve: Mind
Esemény azonosító, kezdő:
vég:
Esemény-paraméter neve:
Esemény-paraméter értéke:
Csak ha nyugtázva lett
Csak ha nem lett nyugtázva
Kimeneti formátum
Rekordszám: 23
Eredmény megmutatása HTML dokumentumb...
OK
Mégse
Alapállapot
Keresés
Részletek
Nyomtat
2005-09-27
13:20:23
CET
guest
NetAVIS Observer II -- connected to 148.198.136.202 - Microsoft Internet Explorer
Felhasználó adminisztráció
Kamera adminisztráció
Mozgásérzékelés
PTZ
Felhasználók
Számítógép adminisztráció
Rendszer információk
Paraméterek beállítása
Mind látszik
Samsung SDC-313
Azonosító:
TKD bejárat
valami
Képpont változás
Aktív
Belső intervallum
Fényerő
Fényerő változás
Vörös érték
Engedélyezve
Azonosító:
TKD bejárat
Megjegyzés:
Ikon:
Alapértelmezett
Hang:
Alapértelmezett
intavételezés (fps):
3 kép/mp
események közötti idő (sec):
300.0
éppont változás küszöb %:
5.0
Teszt leállítása
Mégse
Mentés
2005-09-27
13:26:54
CET
admin




NetAVIS we observe

Kapsch TeleCom Kft. | kapsch >>>

# Köszönöm @ figyelmüket!

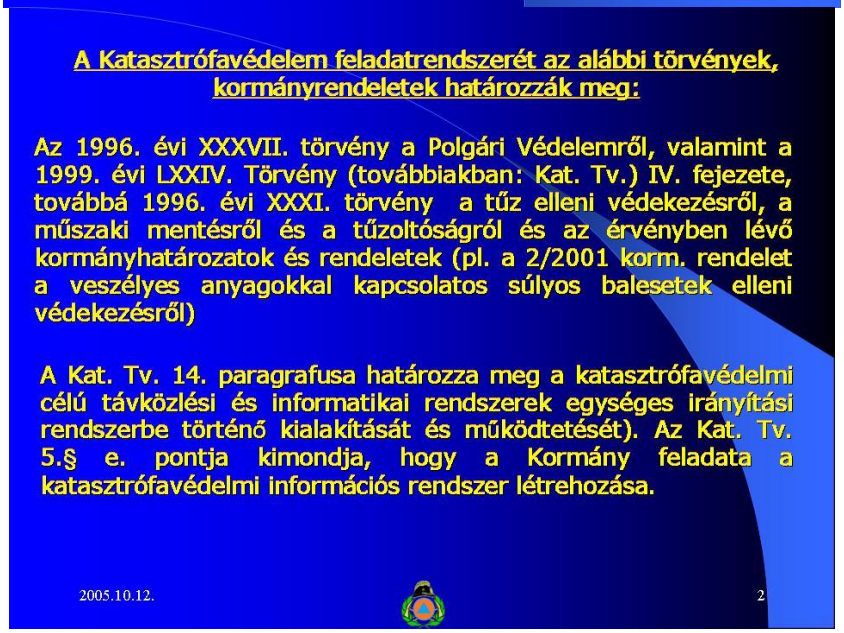
Szabó Zoltán termékmenedzser
*zoltan.szabo@kapsch.net*

***Kapsch TeleCom Kft.***

**MÁTÉ József**

# A KATASZTRÓFAVÉDELEM INFOKOMMUNIKÁCIÓS TÁMOGATOTTSÁGA



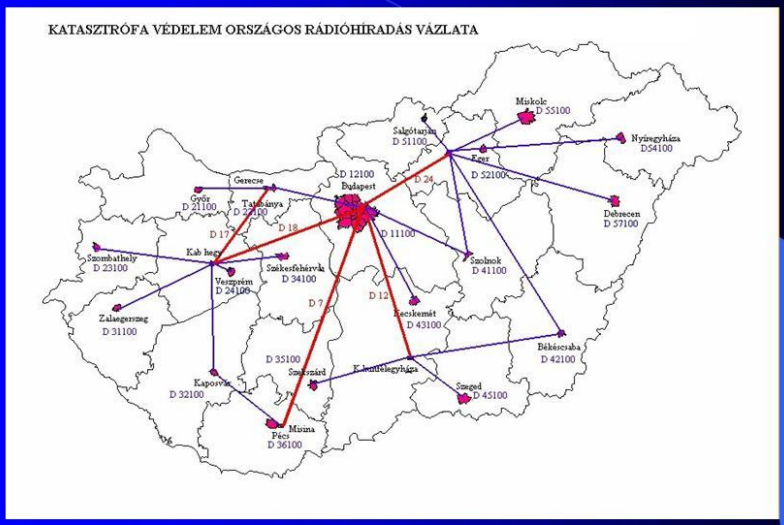



## A Katasztrófavédelem híradó és informatikai rendszerei

- Katasztrófavédelmi URH, RH rádió rendszer
- Dunai Információs Segélyhívó Rendszer
- Tiszai Információs Segélyhívó Rendszer
- Balatoni és Velence-tavi Viharjelző Rendszer
- Lakossági riasztó és tájékoztató rendszerek

2005.10.12. 3

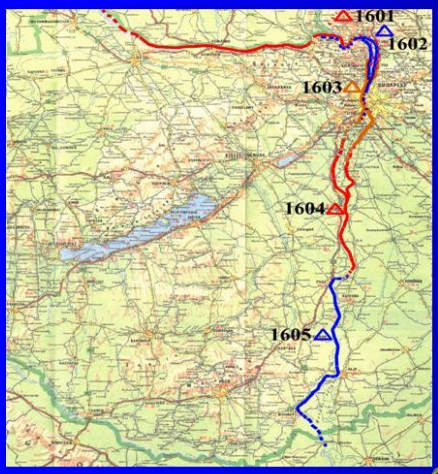
## A BM Országos Katasztrófavédelmi Főigazgatóság országos gerinchálózata




2005.10.12. 4

## A Duna magyarországi szakaszán telepített átjátszó állomások

16. Segélyhívó csatorna

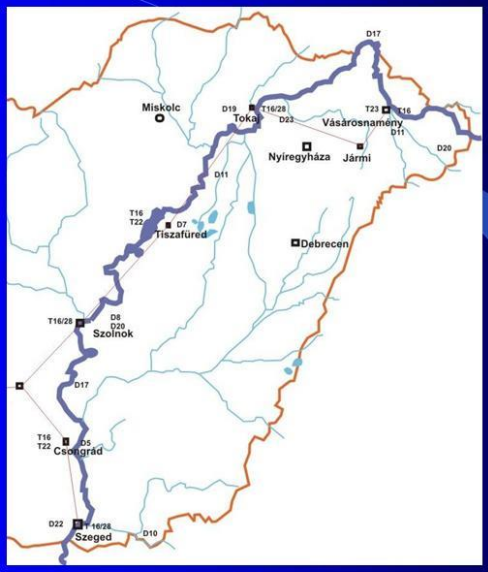



20. Információs csatorna




2005.10.12. 5

## A TISR átjátszóállomásai :




2005.10.12. 6

## A Balatoni és velencetavi viharjelző rendszer









2005.10.12.

7

## Lakossági riasztó és tájékoztató eszközök



Vasbeton oszlopra telepített motorsziréna



Mobil kivitelű tájékoztató-riasztó eszköz



Elektronikus sziréna

2005.10.12.

8

## Katasztrófavédelmi Országos Információs Rendszer (KOIR)

-Adatkapcsolatot teremt a főigazgatóság és a területi szervek helyi hálózatai munkaállomásai és a központi erőforrásokat biztosító szerverek között.

-A rendszerbe integrált többszörös hitelesítést igénylő távbehívó rendszer alkalmazásával biztosítható valamennyi területi szerv és együttműködők munkatársaival adatkapcsolat létrehozása analóg, digitális (ISDN), illetve GSM hálózatról egyaránt.

-A megvalósított infokommunikációs rendszer megfelelő hátteret biztosít a hatékony, kockázatelemzésre épülő, döntési alternatívákat adó, országos lakossági, települési adatokra épülő, osztott-egységes adatbázisú alkalmazások segítségével a helyi, regionális és országos kiterjedésű veszélyhelyzetek kezelésének informatikai támogatására.

-Jogosultság szerinti hozzáférést biztosít a katasztrófavédelem munkatársai részére a hatósági és veszélyhelyzet-kezelési szakterület által alkalmazott rendszerek adatállományához.



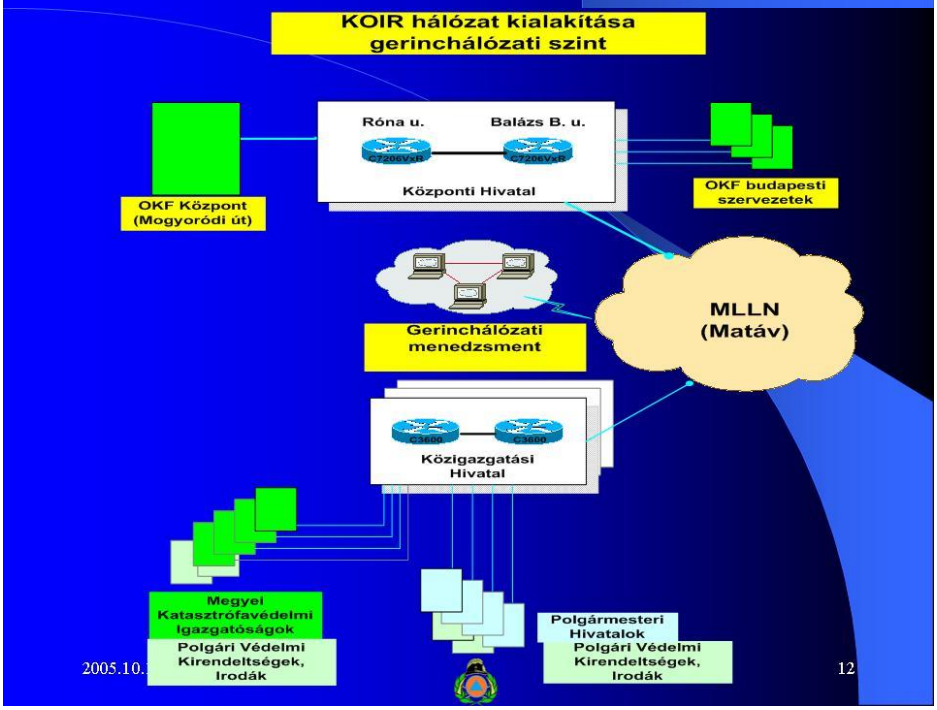
## A KOIR előnyei:

- megfelel a Belügyminisztérium hosszú távú hálózatfejlesztési koncepciójában meghatározott követelményeknek.
- biztosítja a multi-protokoll alapú adatátvitelt,
- a vonalak és a rendszer aktív elemei egy központból menedzselhetőek,
- nagy megbízhatóságú, nagy hibatűrő képességű (a rendelkezésre állás 99% fölötti),
- a hálózat virtuális magán hálózatként kezelhető,
- biztosított az adatútvonalakon a titkosított kommunikáció (3DES/IPSec),
- képes - megfelelő eszközbővítés esetén - az adat- és hangátvitel integrált megvalósítására,
- a hálózat már meglévő eszközparkjához illeszkedik, azok a rendszerbe integrálhatóak,
- a kommunikációs sávszélességet optimálisan használja ki,
- a megjelölt minimális sávszélesség (128-512kbps) rugalmasan bővíthető,
- a végpontok száma igény szerinti rugalmas növelhető,
- kialakítható a hálózati adat - és rendszer menedzsment, a napi munkavégzés hatékonyságának növelésére Intranet alapú hírcsatorna, komplex levelező-, illetve ügyviteli rendszer üzemeltethető,
- az eszközpark biztosítja továbbá a QoS (Quality of Services)-t, azaz egyfajta csomag- és csomagtípus-prioritást biztosító megoldást, a hardveres tűzfalat, a 3DES titkosítást, a VPN kliens autentikációt, a hardver elemek menedzselhetőségét, az erőforrások távoli elérését.

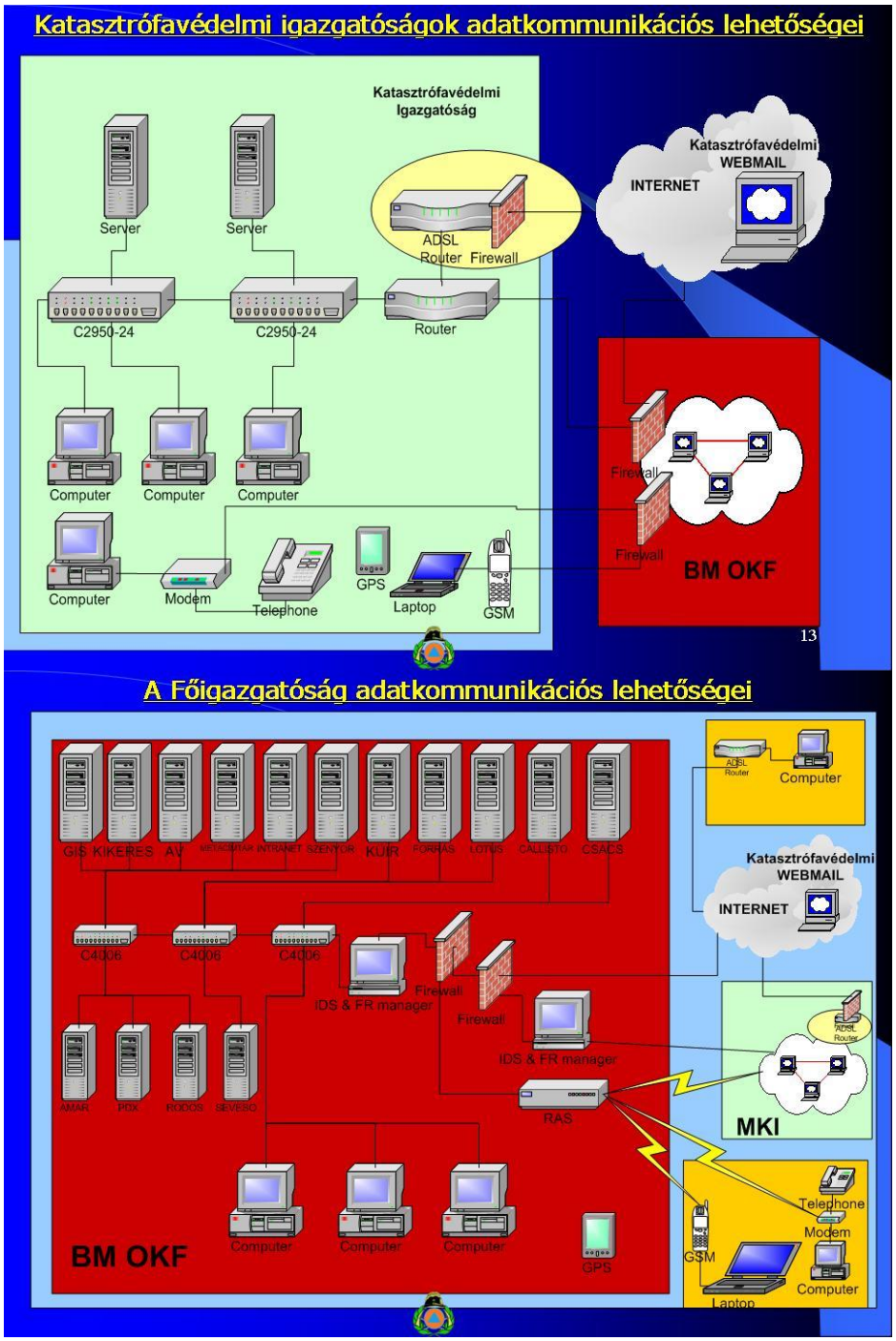
## Infokommunikációs lehetőségek:

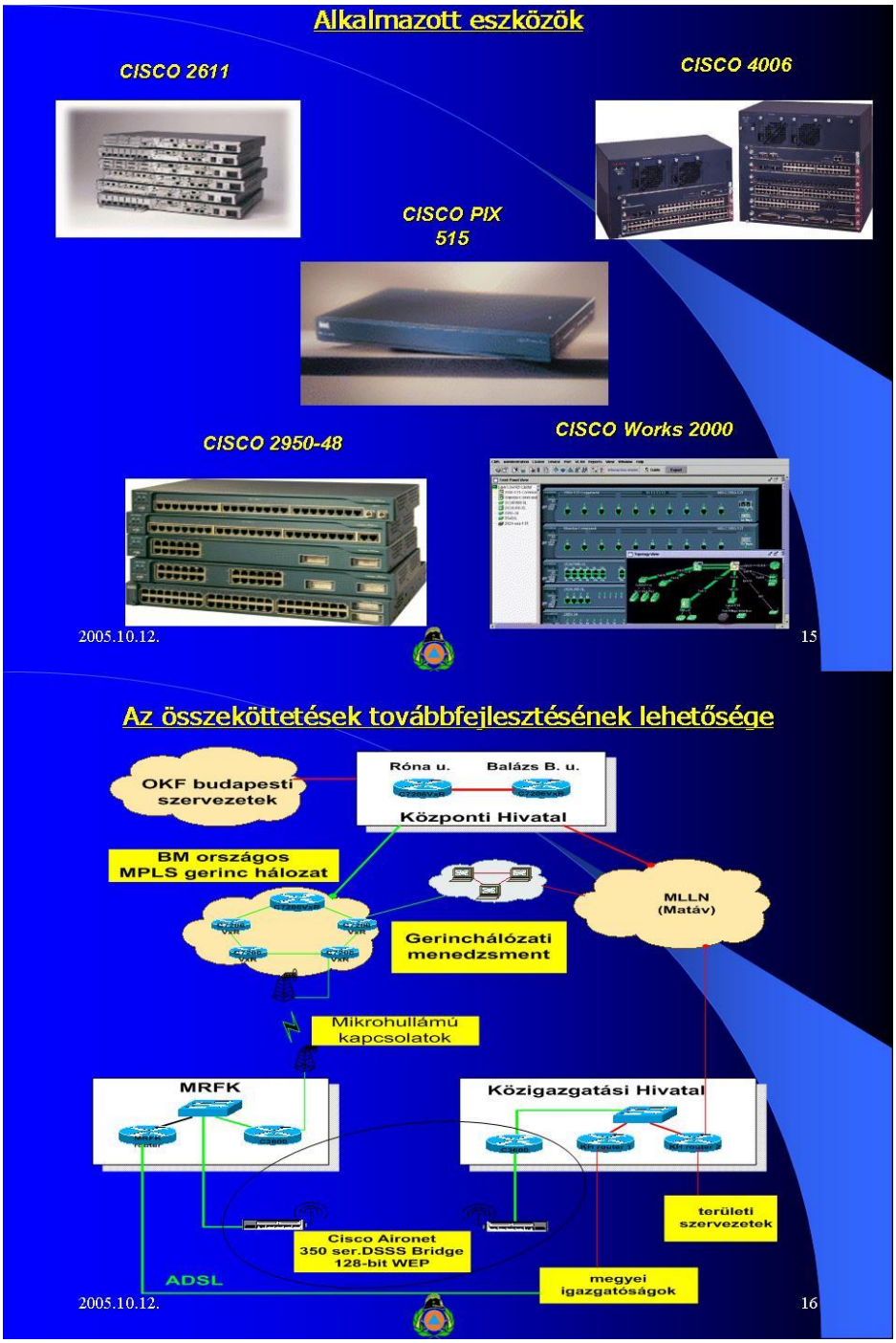
- WAN – gerinchálózati szint
- megyei igazgatóságok helyi hálózata
- főigazgatóság helyi hálózata
- főbb hálózati aktív elemek

2005.10.12. 11




2005.10. 12


Katasztrófavédelmi igazgatóságok adatkommunikációs lehetőségei
Katasztrófavédelmi Igazgatóság
Server
Server
ADSL Router
Firewall
Katasztrófavédelmi WEBMAIL
INTERNET
C2950-24
C2950-24
Router
Computer
Computer
Computer
Computer
Modem
Telephone
GPS
Laptop
GSM
Firewall
Firewall
BM OKF
13
A Főigazgatóság adatkommunikációs lehetőségei
GIS
KIKERES
AV
INTRANET
SZENTGYÖRGY
KUR
FORRAS
LOTUS
CALLISTO
CSACS
ADSL Router
Computer
Katasztrófavédelmi WEBMAIL
INTERNET
C4006
C4006
C4006
IDS & FR manager
Firewall
Firewall
IDS & FR manager
RAS
MKI
Telephone
Modem
GSM
Computer
Laptop
BM OKF
Computer
Computer
Computer
GPS


Alkalmazott eszközök
CISCO 2611
CISCO 4006
CISCO PIX 515
CISCO 2950-48
CISCO Works 2000
2005.10.12.
15
Az összeköttetések továbbfejlesztésének lehetősége
OKF budapesti szervezetek
Róna u.
Balázs B. u.
Központi Hivatal
BM országos MPLS gerinc hálozat
MLLN (Matáv)
Gerinchálózati menedzsment
Mikrohullámú kapcsolatok
MRFK
Közigazgatási Hivatal
területi szervezetek
Cisco Aironet 350 ser.DSSS Bridge 128-bit WEP
ADSL
megyei igazgatóságok
2005.10.12.
16

## Alrendszerek, kiemelt központi szolgáltatások

- Központi Ügyeleti Információs Rendszer (IP/KÜIR)
- Intranet Portál
- Katasztrófavédelmi Térinformatikai Rendszer (KATIR)
- Katasztrófavédelmi Metacímtár
- Belső Információs Honlap
- RODOS– PDX– OSJER (AMAR)
- Behatolás detektáló/Sávszélesség-menedzselő
- Lotus Notes / Callisto / KatvedMail levelező rendszerek
- Katasztrófavédelmi Internetes Honlap
- Antivírus/AntiSpam rendszer

2005.10.12. 17

## Központi Ügyeleti Információs Rendszer (IP / KÜIR) / Intranet Portál

-olyan infokommunikációs rendszer, amely széles körben felöleli a katasztrófahelyzetben, veszélyhelyzet-kezelésben érintett szervezeteket,

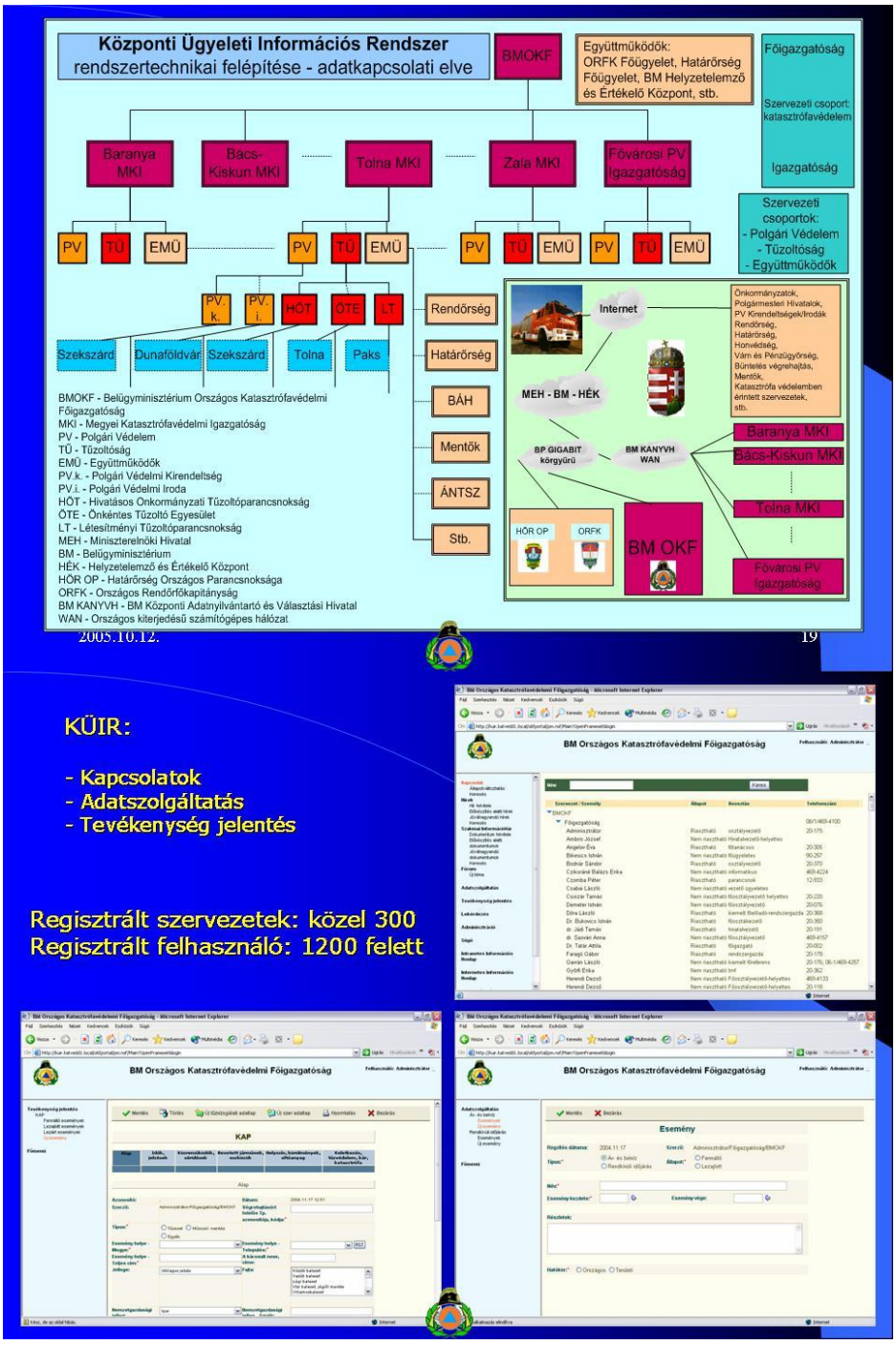
- lehetőséget teremt az elektronikus kapcsolattartásra, csoportmunkára, adatátvitelre, központi Intranet Portál szolgáltatások biztosítására (Dokumentumtár, Hírlevél, Fórum, stb.),

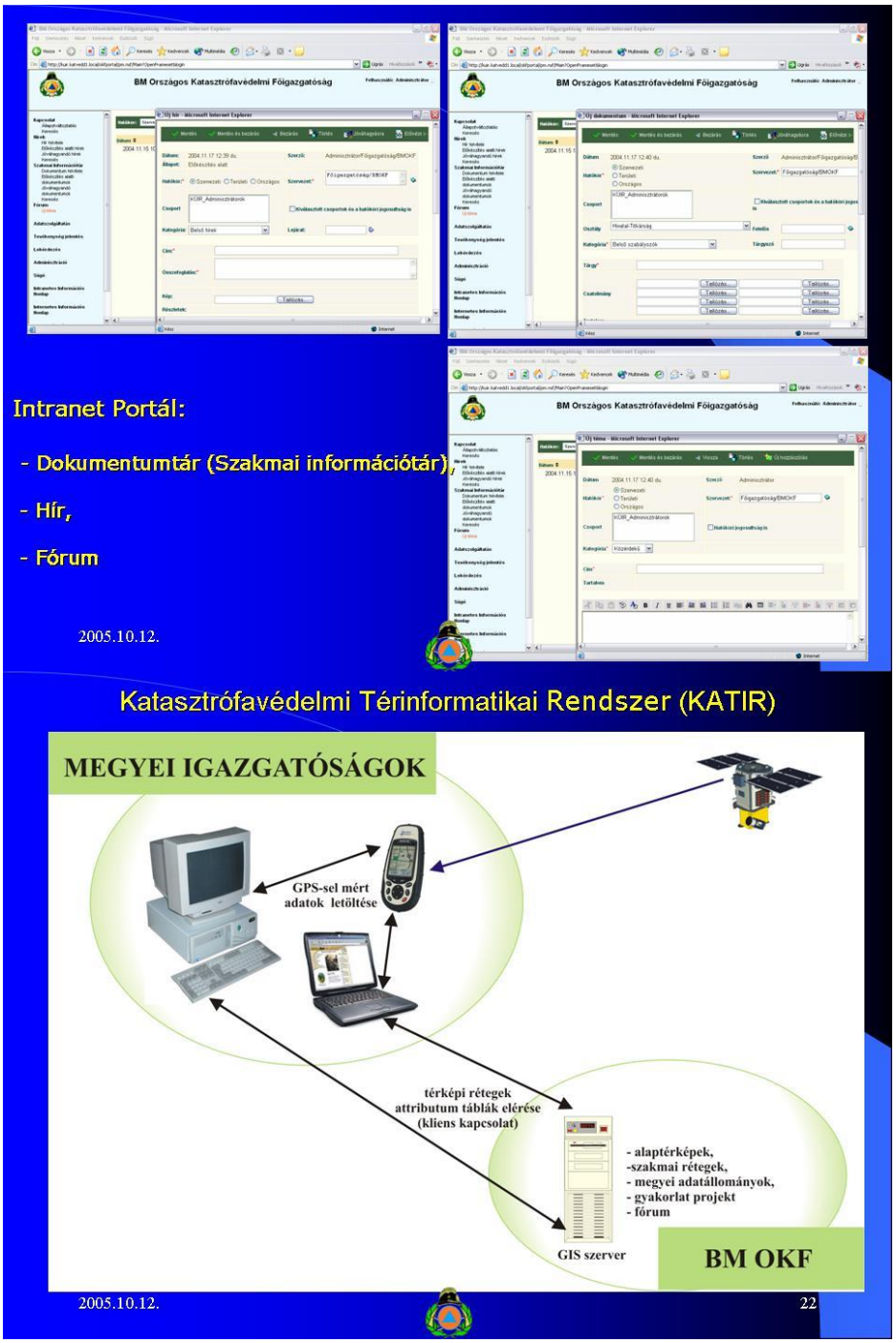
- biztosítja az űrlapalapú adatszolgáltatást:

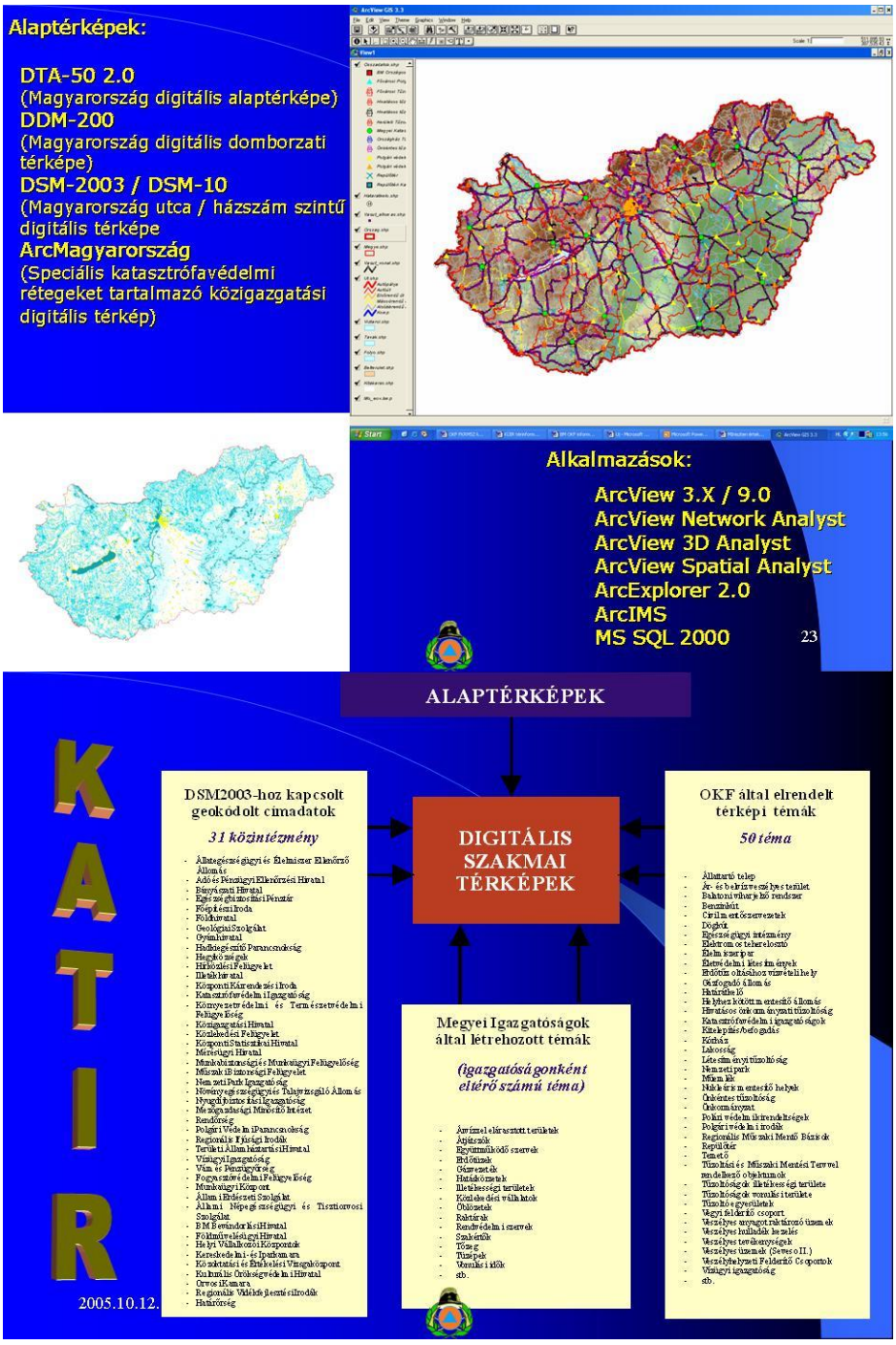
a. Létszám adatok (riasztható, nem riasztható, készenlétben, bevetésen)
b. Szerállapot nyilvántartás
c. KAP (Káreset Adatszolgáltatási Program)
d. RST (Riasztási és Segítségnyújtási Terv)
e. Rendkívüli időjárás (hóhelyzet) jelentés
f. Ár- és belvíz adatszolgáltatás

Célunk: bármely időpillanatban meghatározható legyen a kialakult katasztrófahelyzetre, illetve veszélyhelyzet-kezelésre mozgósítható személyi állomány létszáma és a technikai eszközpark összetétele, valamint adatkommunikációs együttműködés lehetőségének megteremtése valamennyi érintett (beavatkozó) szervezet között.

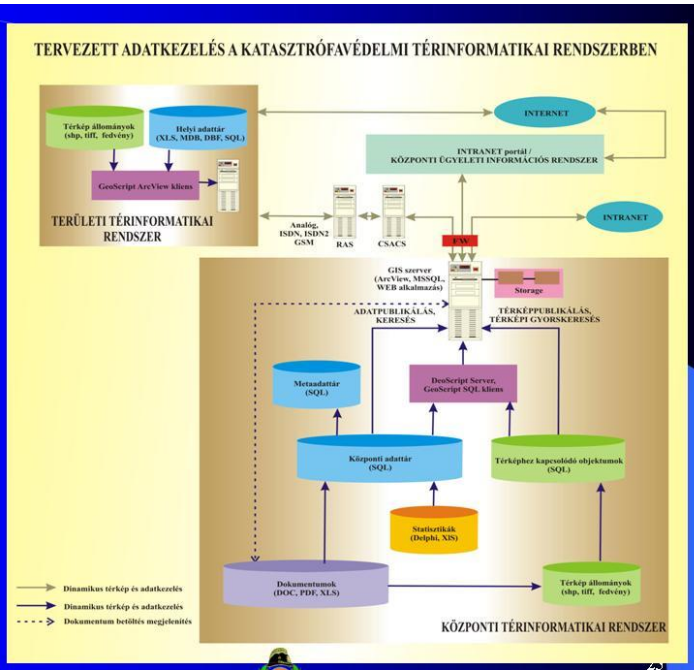
2005.10.12. 18


Központi Ügyeleti Információs Rendszer
rendszertechnikai felépítése - adatkapcsolati elve
BMOKF
Együttműködők:
ORFK Főügyelet, Határőrség
Főügyelet, BM Helyzetelemző
és Értékelő Központ, stb.
Főigazgatóság
Szervezeti csoport:
katasztrófavédelem
Igazgatóság
Baranya MKI
Bács-Kiskun MKI
Tolna MKI
Zala MKI
Fővárosi PV Igazgatóság
Szervezeti csoportok:
- Polgári Védelem
- Tűzoltóság
- Együttműködők
PV
TÜ
EMÜ
PV k.
PV i.
HÖT
ÖTE
LT
Szekszárd
Dunaföldvár
Szekszárd
Tolna
Paks
Rendőrség
Határőrség
BÁH
Mentők
ÁNTSZ
Stb.
Internet
MEH - BM - HÉK
BP GIGABIT körgyűrű
BM KANYVH WAN
Önkormányzatok, Polgármesteri Hivatalok, PV Kirendeltségek/Irodák Rendőrség, Határőrség, Honvédség, Vám és Pénzügyőrség, Büntetés végrehajtás, Mentők, Katasztrófa védelemben érintett szervezetek, stb.
Baranya MKI
Bács-Kiskun MKI
Tolna MKI
Fővárosi PV Igazgatóság
HÖR OP
ORFK
BM OKF
BMOKF - Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság
MKI - Megyei Katasztrófavédelmi Igazgatóság
PV - Polgári Védelem
TÜ - Tűzoltóság
EMÜ - Együttműködők
PV.k. - Polgári Védelmi Kirendeltség
PV.i. - Polgári Védelmi Iroda
HÖT - Hivatásos Önkormányzati Tűzoltóparancsnokság
ÖTE - Önkéntes Tűzoltó Egyesület
LT - Létesítményi Tűzoltóparancsnokság
MEH - Miniszterelnöki Hivatal
BM - Belügyminisztérium
HÉK - Helyzetelemző és Értékelő Központ
HÖR OP - Határőrség Országos Parancsnoksága
ORFK - Országos Rendőrfőkapitányság
BM KANYVH - BM Központi Adatnyilvántartó és Választási Hivatal
WAN - Országos kiterjedésű számítógépes hálózat
2005.10.12.
19
KÜIR:
- Kapcsolatok
- Adatszolgáltatás
- Tevékenység jelentés
Regisztrált szervezetek: közel 300
Regisztrált felhasználó: 1200 felett
BM Országos Katasztrófavédelmi Főigazgatóság
KAP
Esemény


BM Országos Katasztrófavédelmi Főigazgatóság
Intranet Portál:
- Dokumentumtár (Szakmai információtár),
- Hír,
- Fórum
2005.10.12.
Katasztrófavédelmi Térinformatikai Rendszer (KATIR)
MEGYEI IGAZGATÓSÁGOK
GPS-sel mért adatok letöltése
térképi rétegek attributum táblák elérése (kliens kapcsolat)
- alaptérképek,
-szakmai rétegek,
- megyei adatállományok,
- gyakorlat projekt
- fórum
GIS szerver
BM OKF
2005.10.12.
22


Alaptérképek:
DTA-50 2.0
(Magyarország digitális alaptérképe)
DDM-200
(Magyarország digitális domborzati térképe)
DSM-2003 / DSM-10
(Magyarország utca / házszám szintű digitális térképe
ArcMagyarország
(Speciális katasztrófavédelmi rétegeket tartalmazó közigazgatási digitális térkép)
Alkalmazások:
ArcView 3.X / 9.0
ArcView Network Analyst
ArcView 3D Analyst
ArcView Spatial Analyst
ArcExplorer 2.0
ArcIMS
MS SQL 2000
23
ALAPTÉRKÉPEK
KATIR
DSM2003-hoz kapcsolt geokódolt címadatok
31 közintézmény
DIGITÁLIS SZAKMAI TÉRKÉPEK
OKF által elrendelt térképi témák
50 téma
Megyei Igazgatóságok által létrehozott témák
(igazgatóságonként eltérő számú téma)
2005.10.12.

KATIR



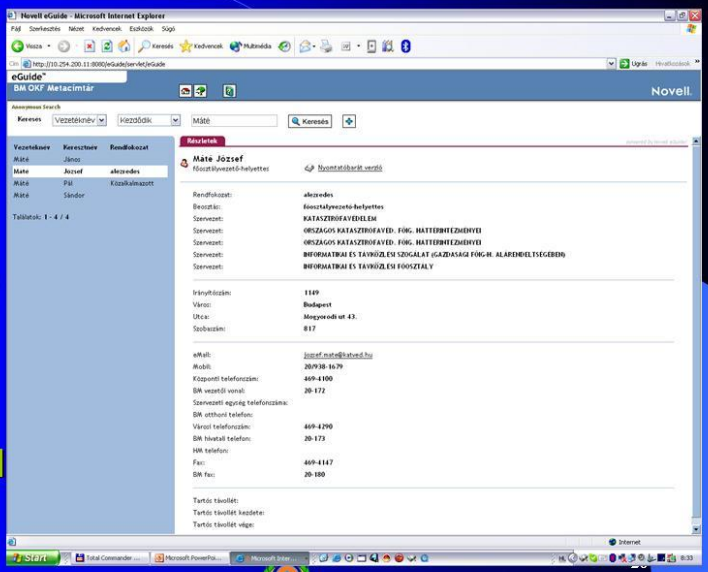

2005.10.12.

## Katasztrófavédelmi MetaCímtár

Közel 1800 fő elérhetőségi adatait tartalmazza.

A főigazgatóságon a SZENYOR személyzeti nyilvántartással került szinkronizálásra, megyei szinten a Védelmi Bizottságok tagjai is feltöltésre kerültek.

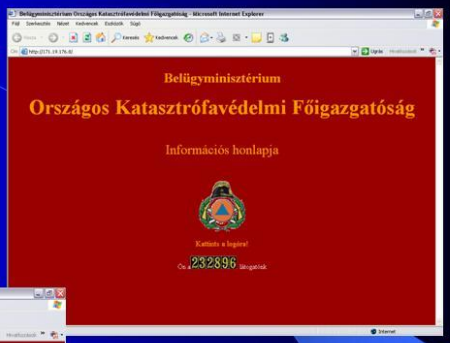
Névszerinti keresés

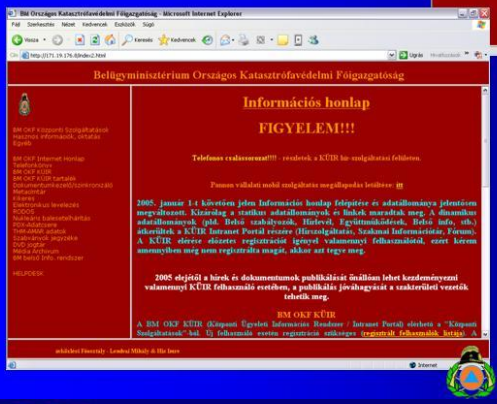



2005.10.12.

## Belső Információs Honlap

Központi szolgáltatások
Hasznos információk, oktatás,
Egyéb




A KOIR-ba kötött valamennyi munkaállomásról elérhető, az alábbi megosztásban:

Belügyi zárthálón: kb. 1200 PC

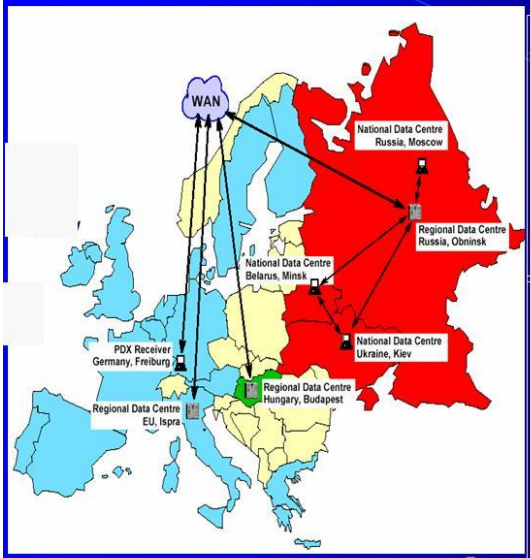
Távbehívó rendszeren: kb. 30 PC

Interneten keresztül: kb. 500 PC

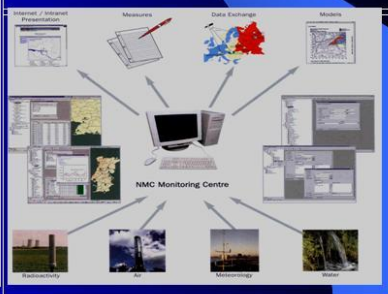
A látogatottsági számláló állása: 230000 felett, naponta 500 feletti a növekmény.

27

## PDX PROTOTYPE DATA EXCHANGE SYSTEM
/NEMZETKÖZI REGIONÁLIS RADIOLÓGIAI ADATCSERE KÖZPONT RENDSZER/




A PDX rendszer lehetőséget nyújt az európai országok számára, hogy radiológiai, meteorológiai monitoring hálózataik és radiológiai laboratóriumi rendszereik mérési adatainak cseréje, nem az egyes országok között, hanem nemzetközi regionális radiológiai adatcsere központokon keresztül (ISDN adatvonalakon) nemzetközileg egységes formátumban (EURDEP).

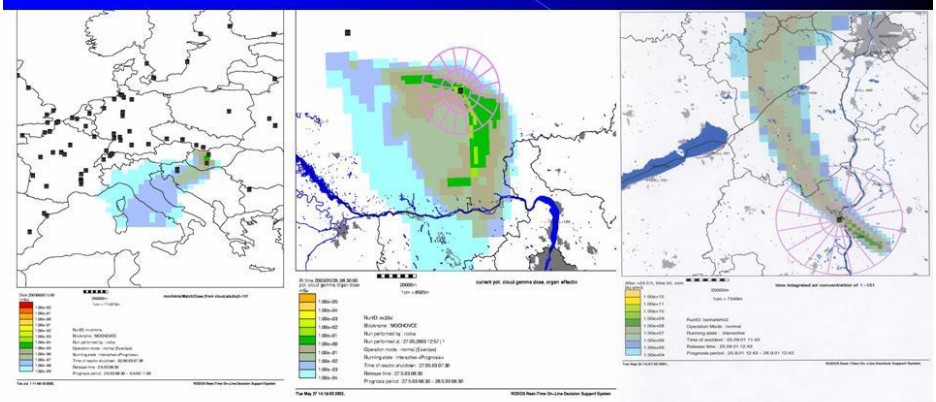



2005.10.12.

28

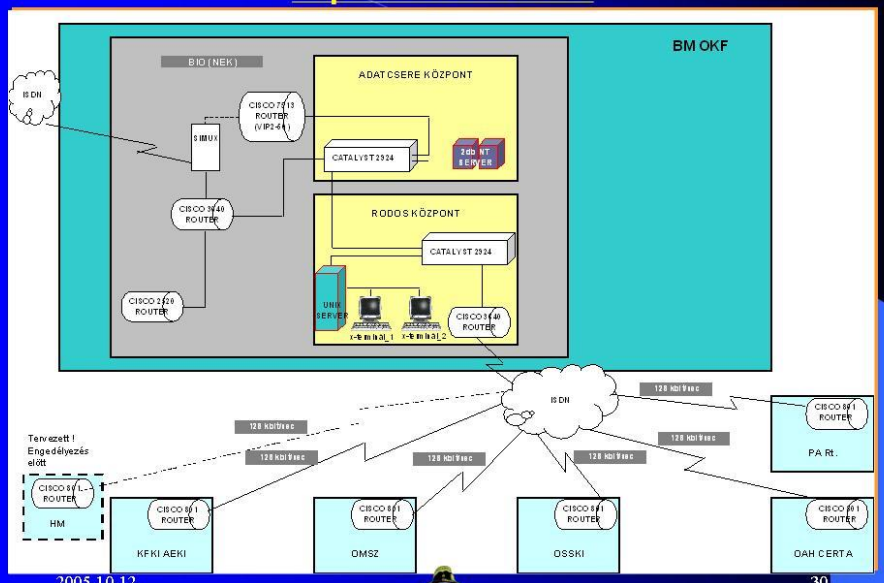
## Nemzetközi, valós-idejű, nukleáris, döntés-támogató rendszer

**RODOS** REAL-TIME, ON-LINE, DECISION SUPPORT SYSTEM

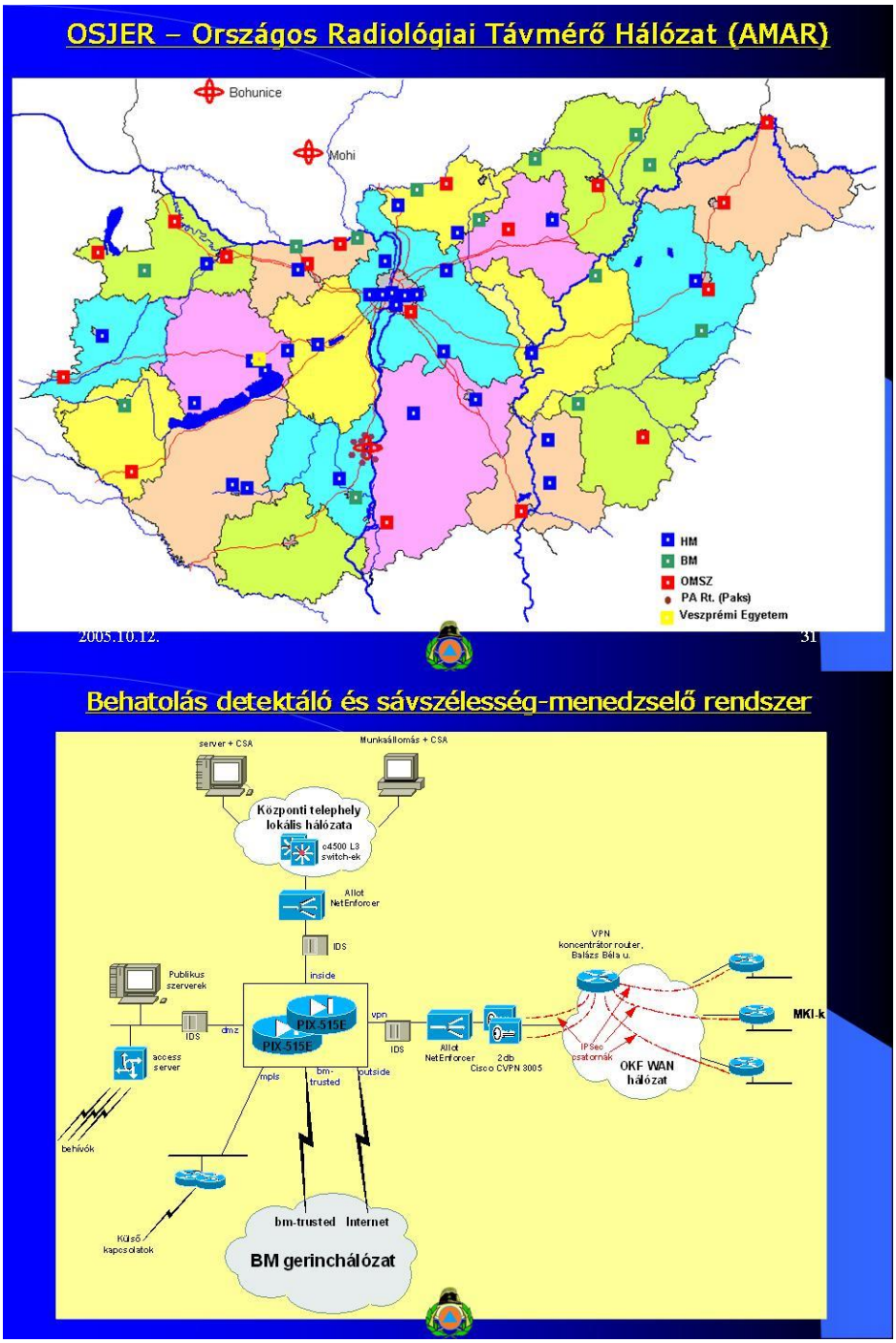


2005.10.12. 29

## A RODOS, valamint az ADATCSERE Központ kapcsolatrendszere




2005.10.12. 30


OSJER – Országos Radiológiai Távmérő Hálózat (AMAR)
Bohunice
Mohi
HM
BM
OMSZ
PA Rt. (Paks)
Veszprémi Egyetem
2005.10.12.
31
Behatolás detektáló és sávszélesség-menedzselő rendszer
server + CSA
Munkaállomás + CSA
Központi telephely lokális hálózata
c4500 L3 switch-ek
Allot NetEnforcer
IDS
inside
Publikus szerverek
PIX 515E
PIX 515E
dmz
IDS
vpn
IDS
Allot NetEnforcer
2db Cisco CVPN 3005
VPN koncentrátor router, Balázs Béla u.
IPSec csatornák
OKF WAN hálózat
MKI-k
access server
mpls
bm-trusted
outside
behívók
Külső kapcsolatok
bm-trusted
Internet
BM gerinchálózat

## Elektronikus, irányított feladat meghatározó rendszerek

Marathon – BM HÉK – BM OKF VKK munkacsoportok részére
Calliope – BM vezetői állománya részére
Callisto * – BM OKF teljes személyi állománya részére




## Elektronikus levelezés

*Katasztrófavédelmi WEBMAIL:*

*Alarmix Online:*

*Lotus Notes:*




A Katasztrófavédelmi WEBMAIL szolgáltatás adminisztrátori feladatát az ITFO végzi. Az email fiókok dedikáltan 25 MB-osak, egyébként korlátlan kapacitásúak.
A Katasztrófavédelmi WEBMAIL alkalmazása esetén a BM GOV-ostól és a LotosNotes-tól eltérően a regisztrált felhasználók akár otthonról, vagy Internet Kávézóból is elérhetik, a világ bármely pontjáról az email fiókjukat.
Az Alarmix Online vésztartalék levelezési lehetőség, az Internet kapcsolat megszakadásának esetére.
A Lotus Notes elsősorban vezetők és ügyeletek közötti elektronikus levelezést, illetve dokumentumok küldését biztosítja, valamint csoportmunka támogatási lehetőséget ad (dokumentum változtatás naplózása, kézbesítés és elolvasás visszaigazoltatása).


A katasztrófavédelem hivatalos honlapja:
http://www.katasztrofavedelem.hu
2003-ban indult, majd a 2004 és 2005-ben folyamatos fejlesztésekkel megfeleltettük a KIETB 19-es ajánlásnak.
eTrust CA Innoculate IT 6.0 víruskereső rendszer
Adminisztrátor felület
- központi vírusvédelmi rendszer
- helyi hálózaton történik a vírusadatbázis frissítés
- távmenedzselési lehetőség
2005.10.12.

## Központi valósidejű vírusvédelem



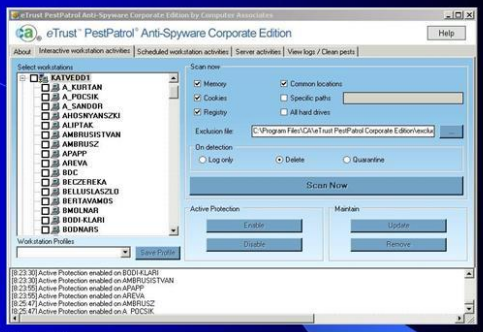

A főigazgatóságon valamennyi, a számítógépes hálózatra kötött személyi számítógépre installálásra került a CA Inoculate víruskereső.
A személyi számítógépeken futtatott vírusvédelmi kliens on-line kapcsolatban van a CA vírusvédelmi szerverrel, amely szerver automatikusan ellátja valamennyi kliensét a legújabb vírusadatbázissal, így mindig az aktuálisan legfrissebb vírusadatbázis rendelkezésre állása mellett valós-időben történik a vírusok kiszűrése.

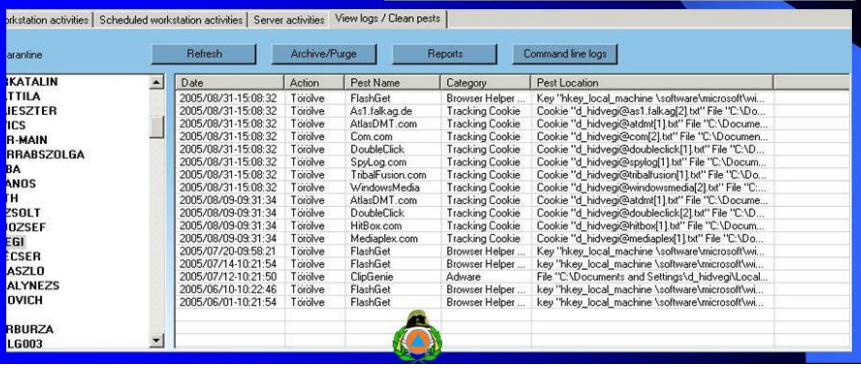
2005.10.12. 37

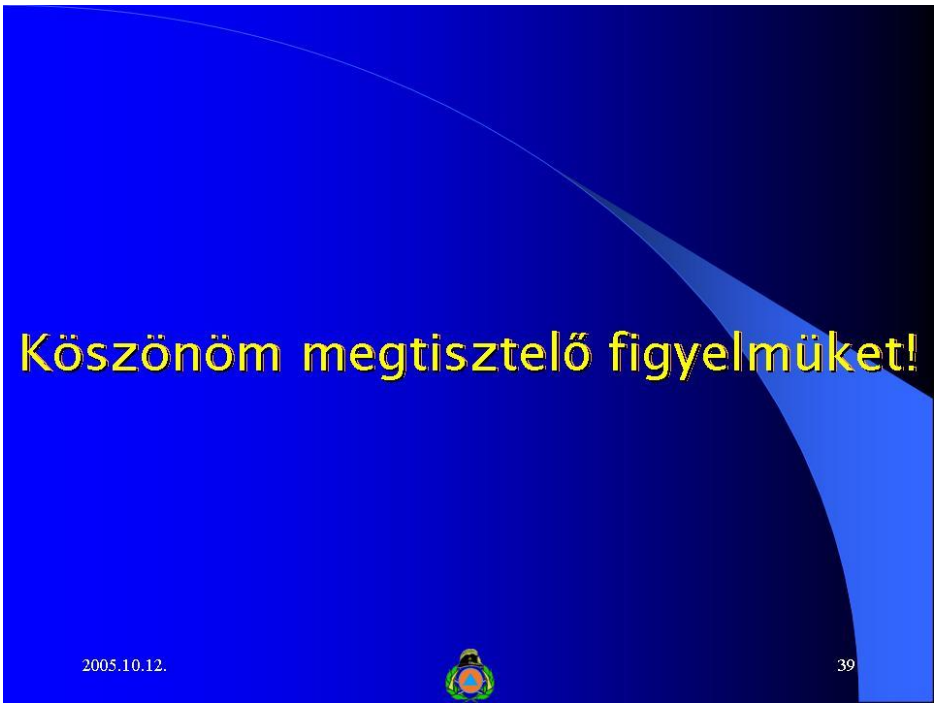
## eTrust PestPatrol AntiSpam rendszer

### Adminisztrátor felület

- központi szabályozás
- variánsok ellen „tanulási” funkció




Köszönöm megtisztelő figyelmüket!
2005.10.12.
39

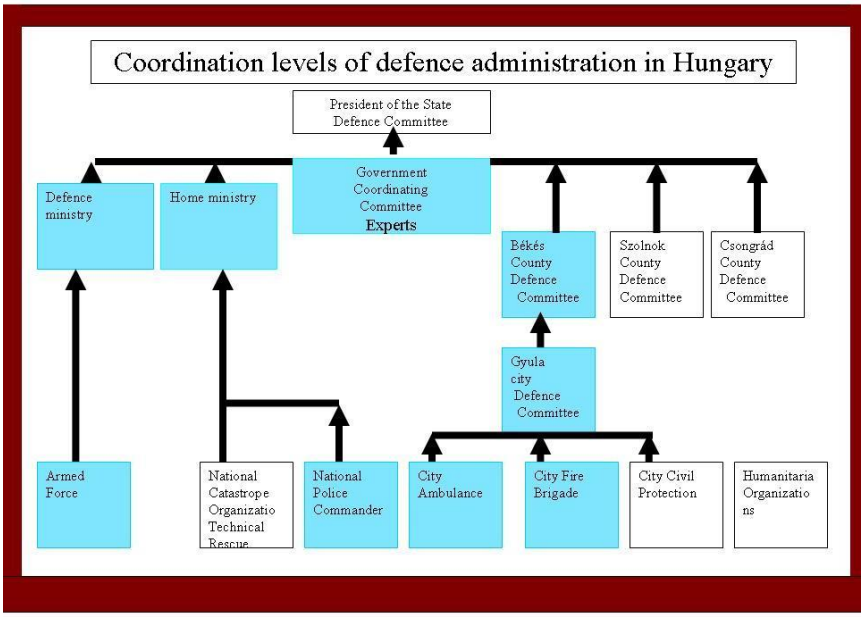
**Gyula MEZEY**

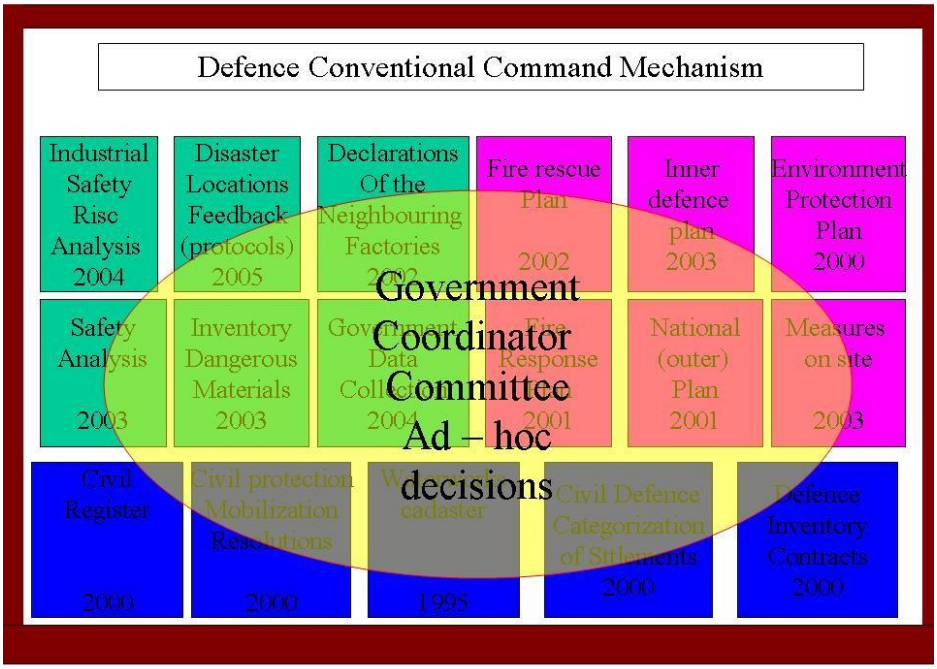
## EMERGENCY 2005 SYSTEM

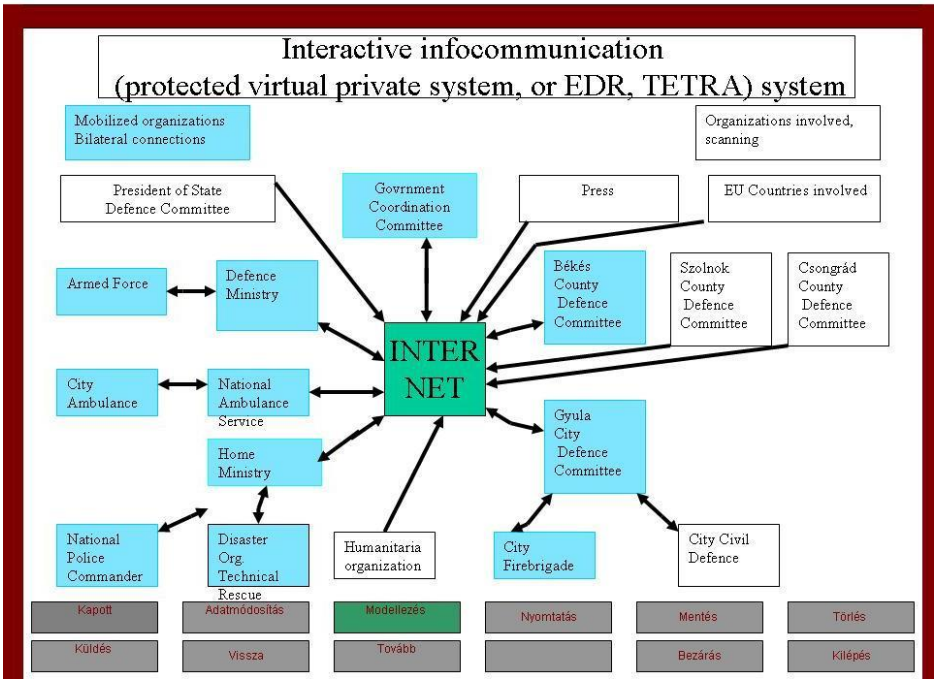
**Associate Prof. Gyula MEZEY PhD**

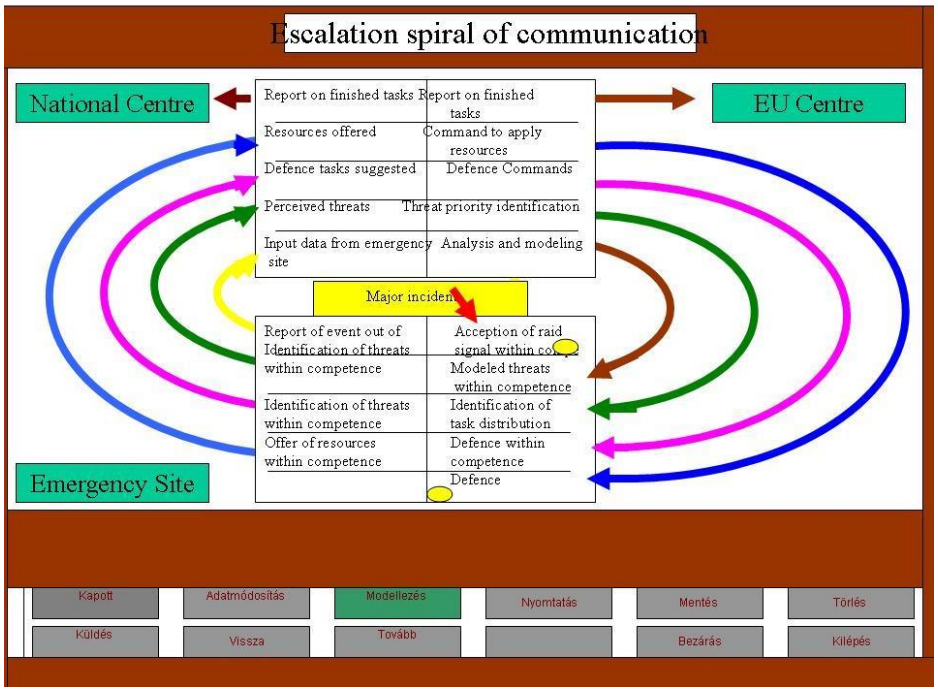
**Miklós Zrínyi National Defense University**

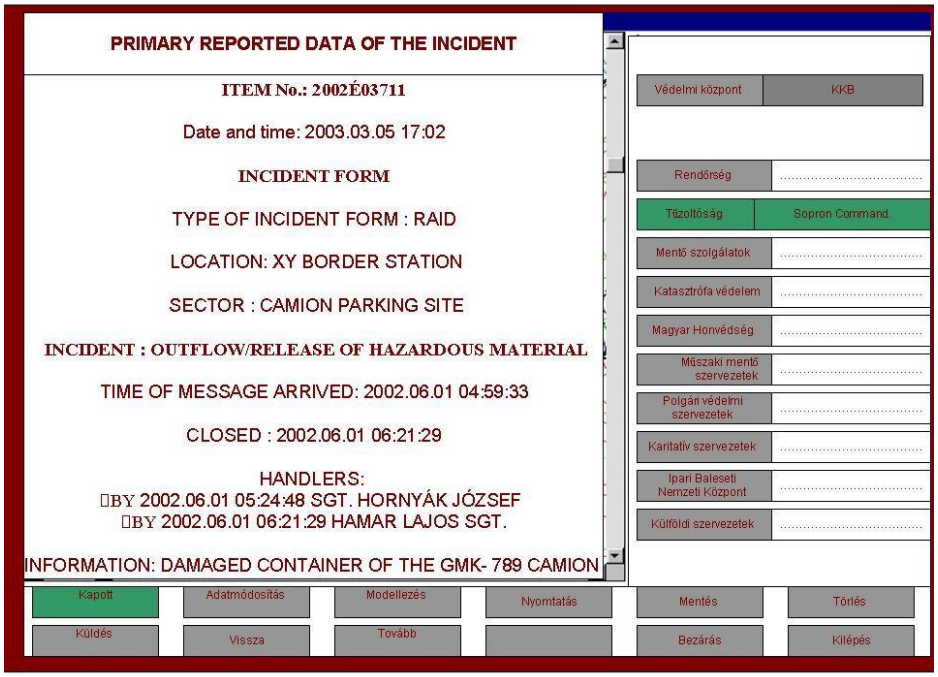


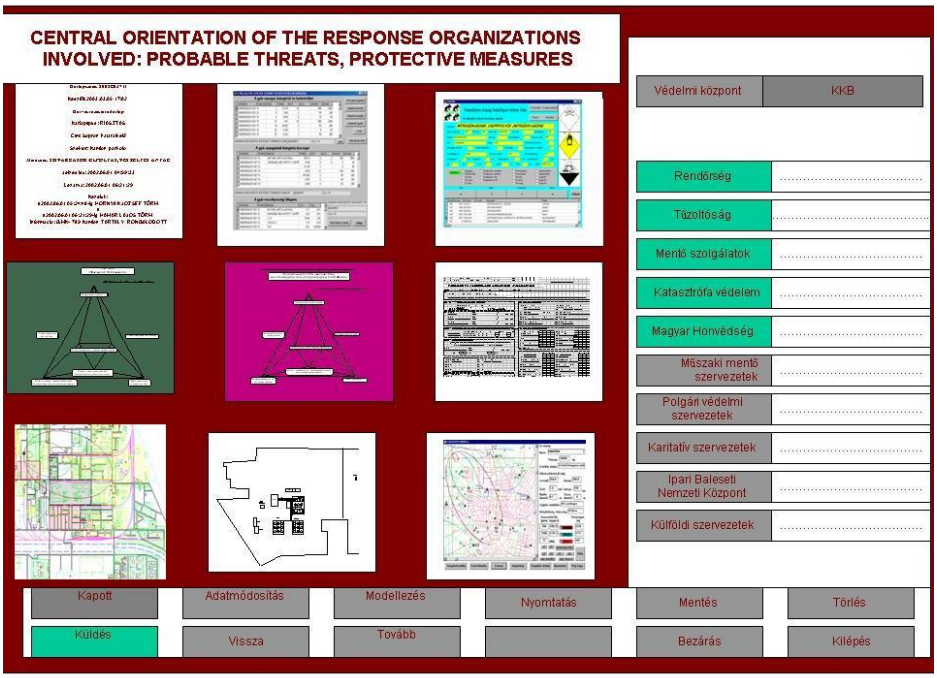



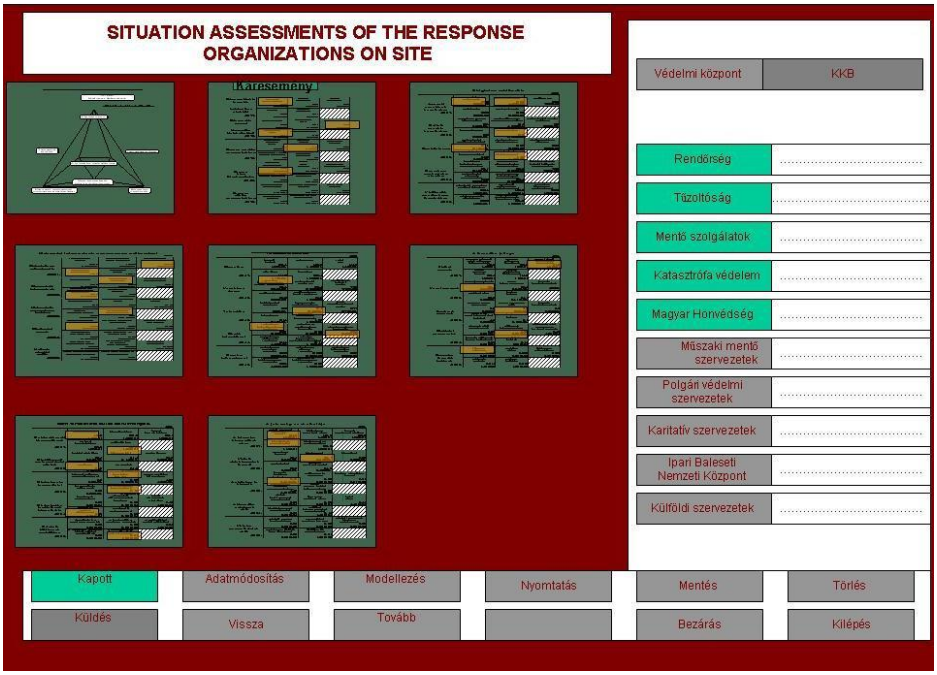

Defence Conventional Command Mechanism
Industrial Safety Risc Analysis 2004
Disaster Locations Feedback (protocols) 2005
Declarations Of the Neighbouring Factories
Fire rescue Plan 2002
Inner defence plan 2003
Environment Protection Plan 2000
Safety Analysis 2003
Inventory Dangerous Materials 2003
Data 2004
Response 2001
National (outer) Plan 2001
Measures on site 2003
Civil Register 2000
Civil protection Mobilization Resolutions 2000
cadaster 1995
Civil Defence Categorization of Stltements 2000
Defence Inventory Contracts 2000
Government Coordinator Committee
Ad – hoc decisions

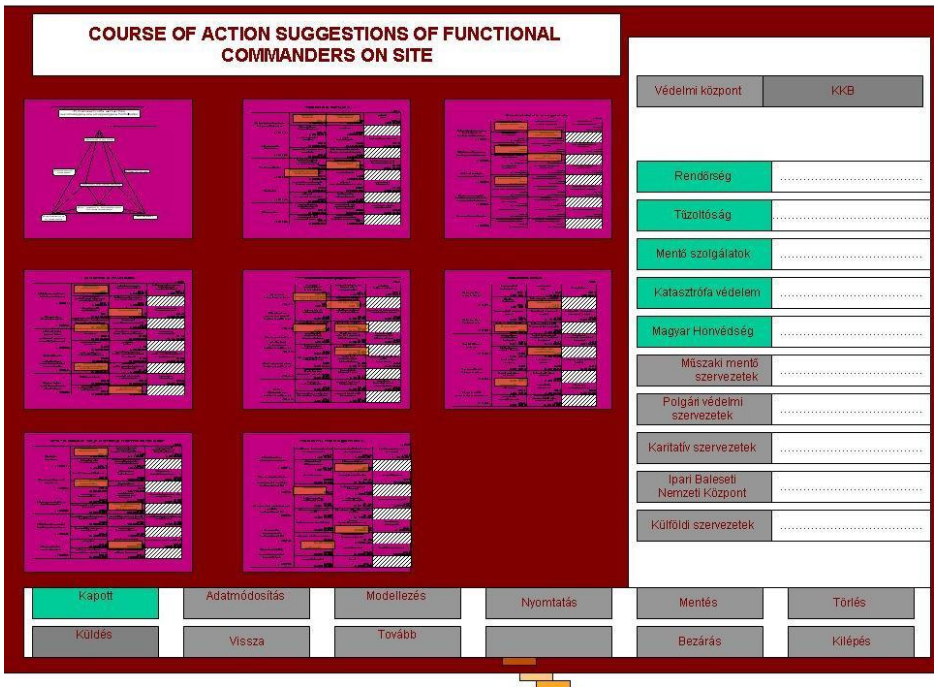

Interactive infocommunication
(protected virtual private system, or EDR, TETRA) system
Mobilized organizations Bilateral connections
Organizations involved, scanning
President of State Defence Committee
Govrnment Coordination Committee
Press
EU Countries involved
Armed Force
Defence Ministry
Békés County Defence Committee
Szolnok County Defence Committee
Csongrád County Defence Committee
INTER NET
City Ambulance
National Ambulance Service
Home Ministry
Gyula City Defence Committee
National Police Commander
Disaster Org. Technical Rescue
Humanitaria organization
City Firebrigade
City Civil Defence
Kapott
Adatmódosítás
Módellezés
Nyomtatás
Mentés
Törlés
Küldés
Vissza
Tovább
Bezárás
Kilépés

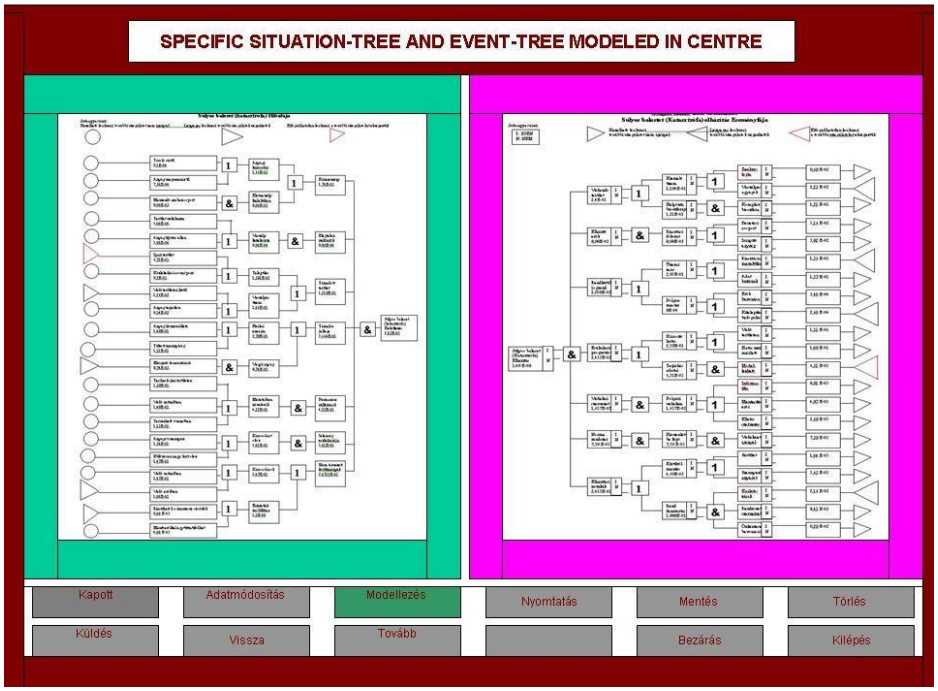

Escalation spiral of communication
National Centre
EU Centre
Emergency Site
Report on finished tasks
Report on finished tasks
Resources offered
Command to apply resources
Defence tasks suggested
Defence Commands
Perceived threats
Threat priority identification
Input data from emergency site
Analysis and modeling
Major incident
Report of event out of
Identification of threats
within competence
Acception of raid
signal within co
Modeled threats
within competence
Identification of threats
within competence
Identification of
task distribution
Offer of resources
within competence
Defence within
competence
Defence
Kapott
Adatmódosítás
Modellezés
Nyomtatás
Mentés
Törlés
Küldés
Vissza
Tovább
Bezárás
Kilépés

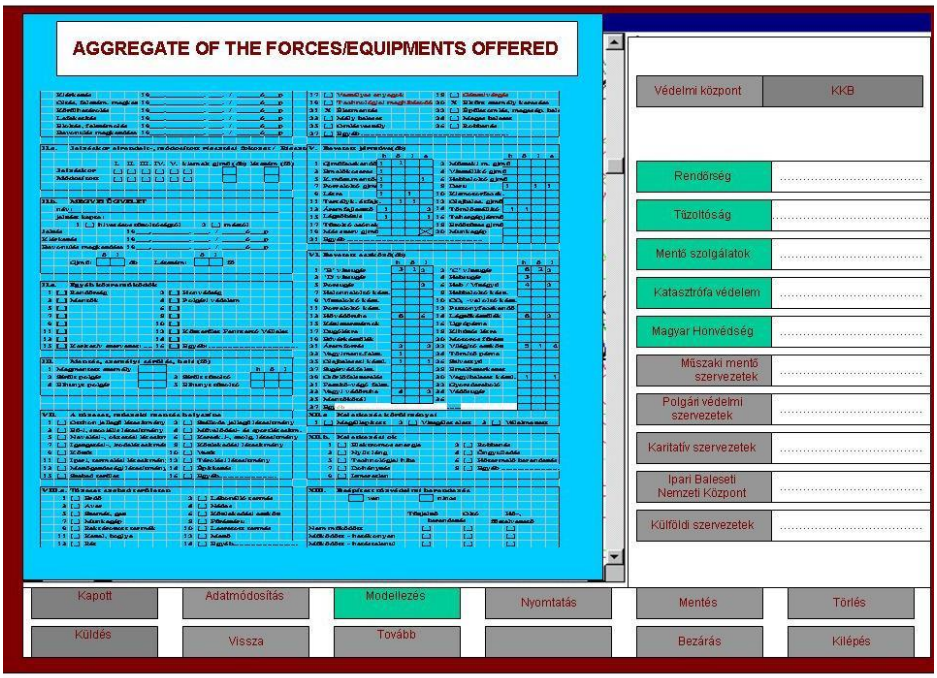

PRIMARY REPORTED DATA OF THE INCIDENT
ITEM No.: 2002É03711
Date and time: 2003.03.05 17:02
INCIDENT FORM
TYPE OF INCIDENT FORM : RAID
LOCATION: XY BORDER STATION
SECTOR : CAMION PARKING SITE
INCIDENT : OUTFLOW/RELEASE OF HAZARDOUS MATERIAL
TIME OF MESSAGE ARRIVED: 2002.06.01 04:59:33
CLOSED : 2002.06.01 06:21:29
HANDLERS:
BY 2002.06.01 05:24:48 SGT. HORNYÁK JÓZSEF
BY 2002.06.01 06:21:29 HAMAR LAJOS SGT.
INFORMATION: DAMAGED CONTAINER OF THE GMK- 789 CAMION
Védelmi központ
KKB
Rendőrség
Tűzoltóság
Sopron Command
Mentő szolgálatok
Katasztrófa védelem
Magyar Honvédség
Műszaki mentő szervezetek
Polgári védelmi szervezetek
Karitatív szervezetek
Ipari Baleseti Nemzeti Központ
Külföldi szervezetek
Kapott
Adatmódosítás
Modellezés
Nyomtatás
Mentés
Törlés
Küldés
Vissza
Tovább
Bezárás
Kilépés

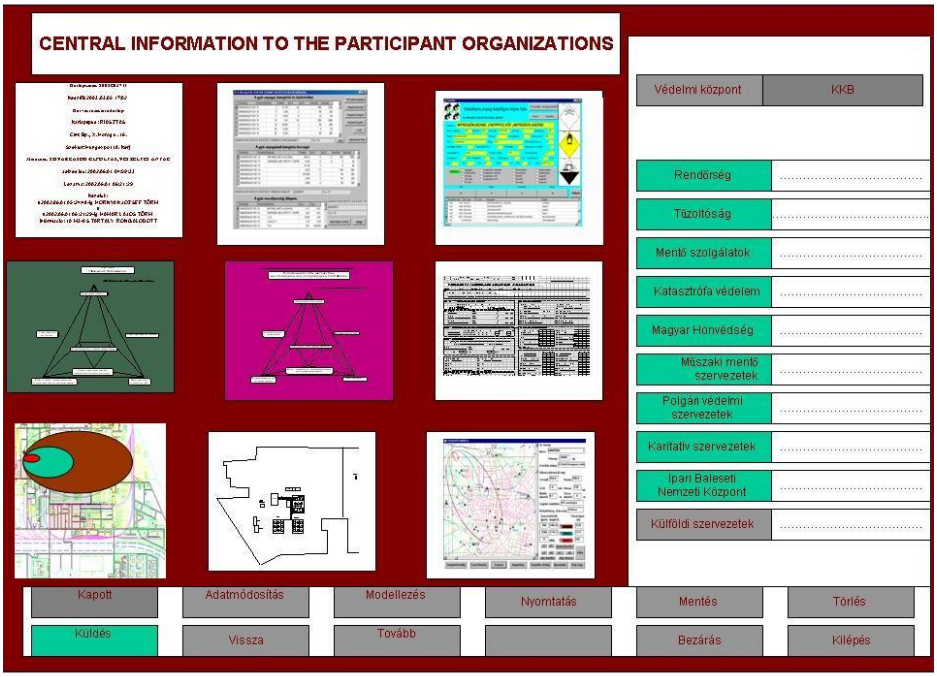

CENTRAL ORIENTATION OF THE RESPONSE ORGANIZATIONS INVOLVED: PROBABLE THREATS, PROTECTIVE MEASURES
Védelmi központ
KKB
Rendőrség
Tűzoltóság
Mentő szolgálatok
Katasztrófa védelem
Magyar Honvédség
Műszaki mentő szervezetek
Polgári védelmi szervezetek
Karitatív szervezetek
Ipari Baleseti Nemzeti Központ
Külföldi szervezetek
Kapott
Adatmódosítás
Modellezés
Nyomtatás
Mentés
Törlés
Küldés
Vissza
Tovább
Bezárás
Kilépés

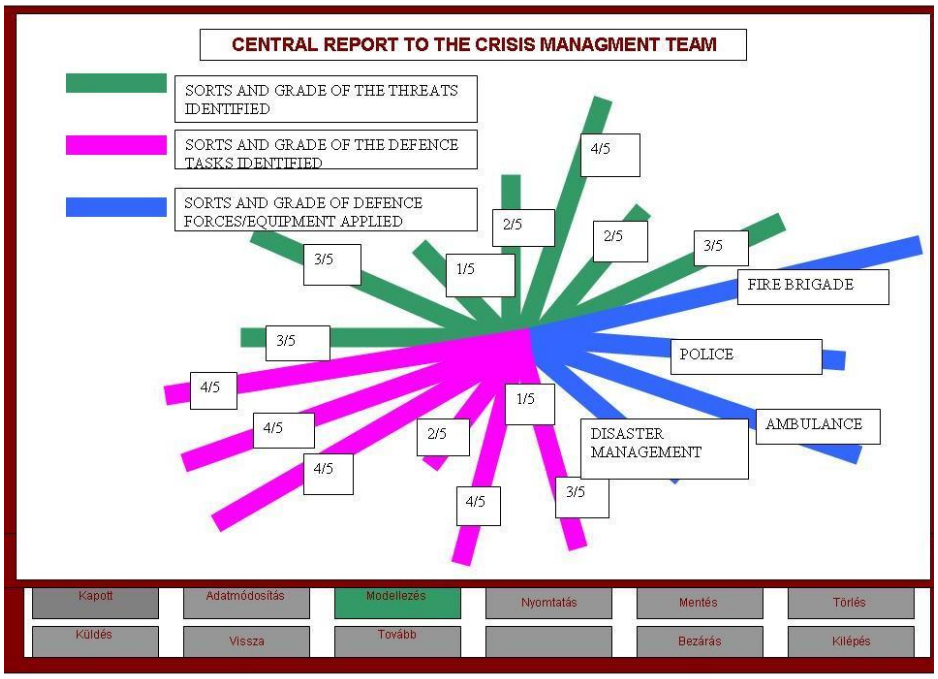

SITUATION ASSESSMENTS OF THE RESPONSE ORGANIZATIONS ON SITE
Védelmi központ
KKB
Rendőrség
Tűzoltóság
Mentő szolgálatok
Katasztrófa védelem
Magyar Honvédség
Műszaki mentő szervezetek
Polgári védelmi szervezetek
Karitatív szervezetek
Ipari Baleseti Nemzeti Központ
Külföldi szervezetek
Kapott
Adatmódosítás
Modellezés
Nyomtatás
Mentés
Törlés
Küldés
Vissza
Tovább
Bezárás
Kilépés

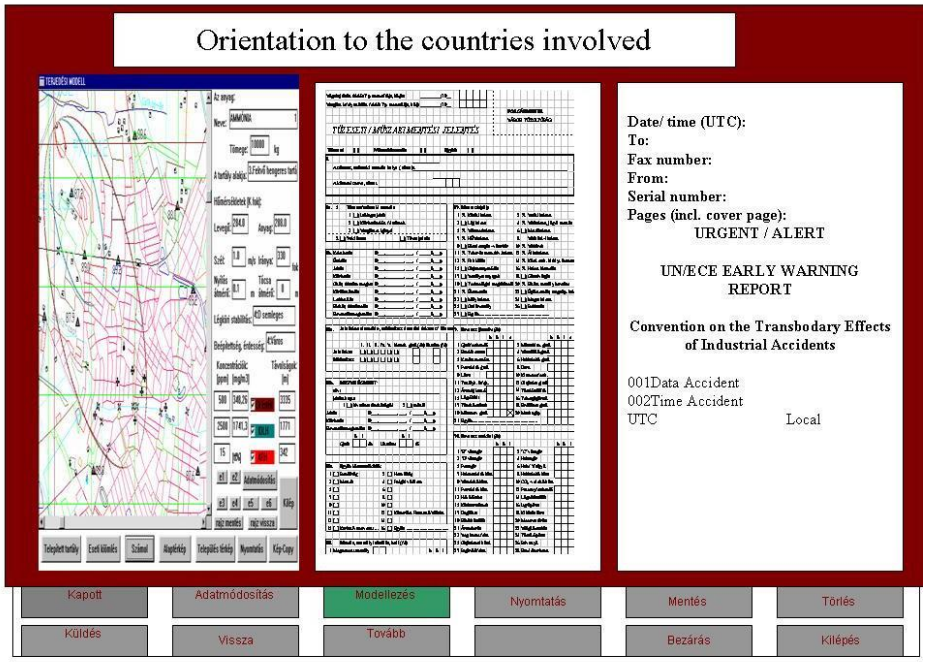

COURSE OF ACTION SUGGESTIONS OF FUNCTIONAL COMMANDERS ON SITE
Védelmi központ
KKB
Rendőrség
Tűzoltóság
Mentő szolgálatok
Katasztrófa védelem
Magyar Honvédség
Műszaki mentő szervezetek
Polgári védelmi szervezetek
Karitatív szervezetek
Ipari Baleseti Nemzeti Központ
Külföldi szervezetek
Kapott
Adatmódosítás
Modellezés
Nyomtatás
Mentés
Törlés
Küldés
Vissza
Tovább
Bezárás
Kilépés


SPECIFIC SITUATION-TREE AND EVENT-TREE MODELED IN CENTRE
Kapott
Adatmódosítás
Modellezés
Nyomtatás
Mentés
Törlés
Küldés
Vissza
Tovább
Bezárás
Kilépés


AGGREGATE OF THE FORCES/EQUIPMENTS OFFERED
Védelmi központ
KKB
Rendőrség
Tűzoltóság
Mentő szolgálatok
Katasztrófa védelem
Magyar Honvédség
Műszaki mentő szervezetek
Polgári védelmi szervezetek
Karitatív szervezetek
Ipari Baleseti Nemzeti Központ
Külföldi szervezetek
Kapott
Adatmódosítás
Modellezés
Nyomtatás
Mentés
Törlés
Küldés
Vissza
Tovább
Bezárás
Kilépés


CENTRAL INFORMATION TO THE PARTICIPANT ORGANIZATIONS
Védelmi központ
KKB
Rendőrség
Tűzoltóság
Mentő szolgálatok
Katasztrófa védelem
Magyar Honvédség
Műszaki mentő szervezetek
Polgári védelmi szervezetek
Karitatív szervezetek
Ipari Baleseti Nemzeti Központ
Külföldi szervezetek
Kapott
Adatmódosítás
Modellezés
Nyomtatás
Mentés
Törlés
Küldés
Vissza
Tovább
Bezárás
Kilépés


CENTRAL REPORT TO THE CRISIS MANAGMENT TEAM
SORTS AND GRADE OF THE THREATS IDENTIFIED
SORTS AND GRADE OF THE DEFENCE TASKS IDENTIFIED
SORTS AND GRADE OF DEFENCE FORCES/EQUIPMENT APPLIED
4/5
2/5
2/5
3/5
3/5
1/5
FIRE BRIGADE
3/5
POLICE
4/5
1/5
4/5
2/5
DISASTER MANAGEMENT
AMBULANCE
4/5
4/5
3/5
Kapott
Adatmódosítás
Modellezés
Nyomtatás
Mentés
Törlés
Küldés
Vissza
Tovább
Bezárás
Kilépés


Orientation to the countries involved
Date/ time (UTC):
To:
Fax number:
From:
Serial number:
Pages (incl. cover page):
URGENT / ALERT
UN/ECE EARLY WARNING REPORT
Convention on the Transbodary Effects of Industrial Accidents
001Data Accident
002Time Accident
UTC
Local
Kapott
Adatmódosítás
Modellezés
Nyomtatás
Mentés
Törlés
Küldés
Vissza
Tovább
Bezárás
Kilépés

# CTOS 976 Series

## Connector for Tactical Optical Systems

MAIN CHARACTERISTICS



This product offers a robust optical connection in a small size design (o.d. 38 mm) and allows for rapid deployment of high speed transmission links in harsh environnements. The specific design of the lenses garanties a large beam diameter and a low loss connection insensitive to dust and dirt. The CTOS harnesses are easy to maintain on the field with the FTOS splice kit.

## Technical description

- 2 or 4 channel Plugs and Receptacles (straight and 90°) and Tactical Harnesses and Test caps for maintenance
- Hermaphroditic interface with rapid ramp coupling
- 2 and 4 channel products are intermateable
- Large expanded beams with protective windows
- Stainless steel body with ergonomic rubber shell
- Typical Insertion Loss : 1.5 dB @ 1300 nm 50/125 fibre
  2 dB @ 1300 nm 9/125 fibre
- Typical return loss : - 45 dB @ 1300 nm HRL 9/125 fibre
- Durability : 5000 mating/unmating cycles
- Operating Temperature : -40°C, +85°C
- Vibrations : 10 to 2000Hz, 10g, 1.5 mmp/p, 3 directions
- Bumps : 4000 Bumps, 40g, 6ms, 6 directions
- Mechanical shock: 50g, ½ sinus, 3 shocks by direction, 3 axes
- Mud resistance : Mil C 83526/13
- Free drops : 26 drops 1.2m on plywood/concrete (plugs)
- Water immersion ; > 1m depth
- Salt spray : 500 hours
- Low pressure : 85 mbars 48 hours
- Termination and Maintenance FTOS tool kits available
- Tactical drums and accessories available

## Features

The Amphenol CTOS fiber optic expanded beam connector is a miniature and lighter version of the CTO connector.

The flat protective windows mounted on shock absorbers provide an easy to clean on the field surface to improve performance and protection.

## Applications

- Army, Navy and Airforce optical networks
- EMI insensitive and light tactical transmission links
- Long distance battlefield communication
- Radar deployment systems

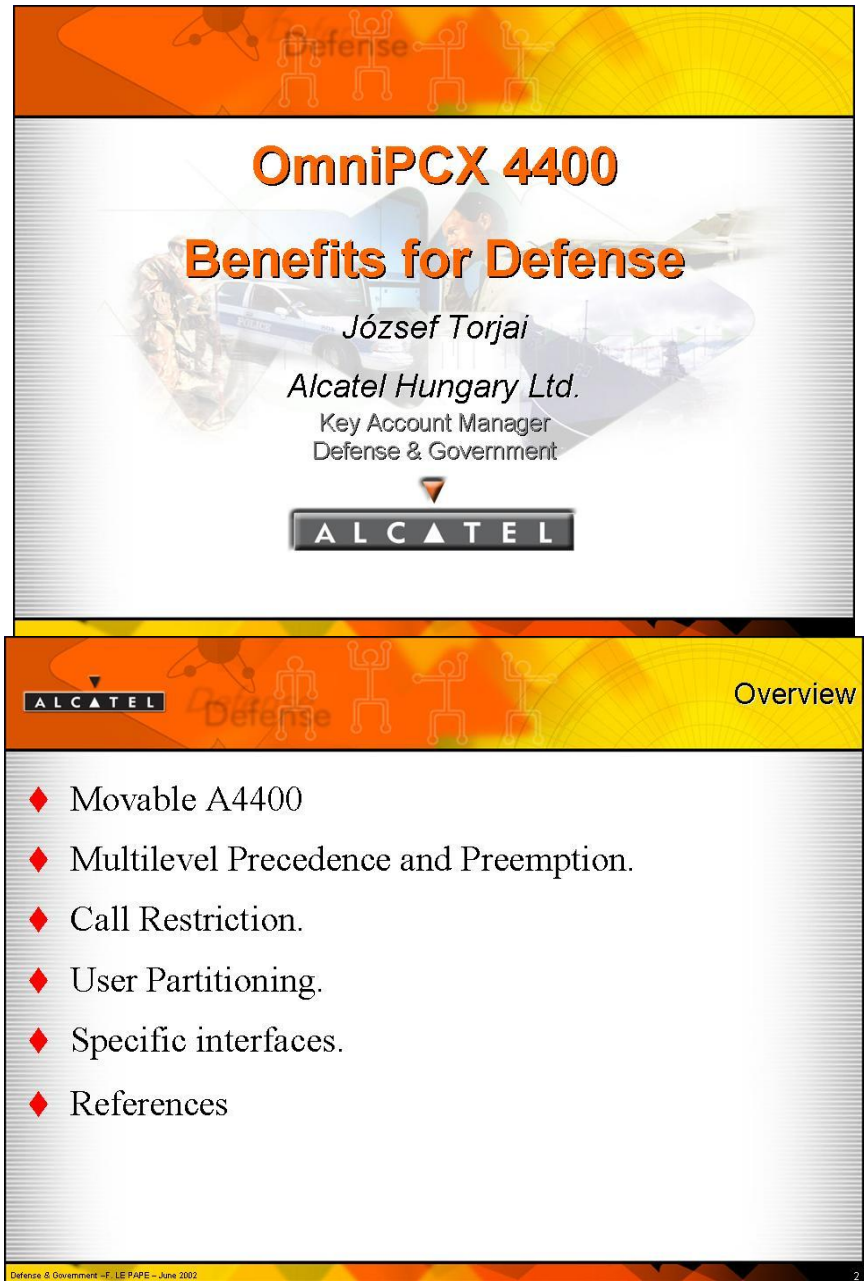
**Amphenol**

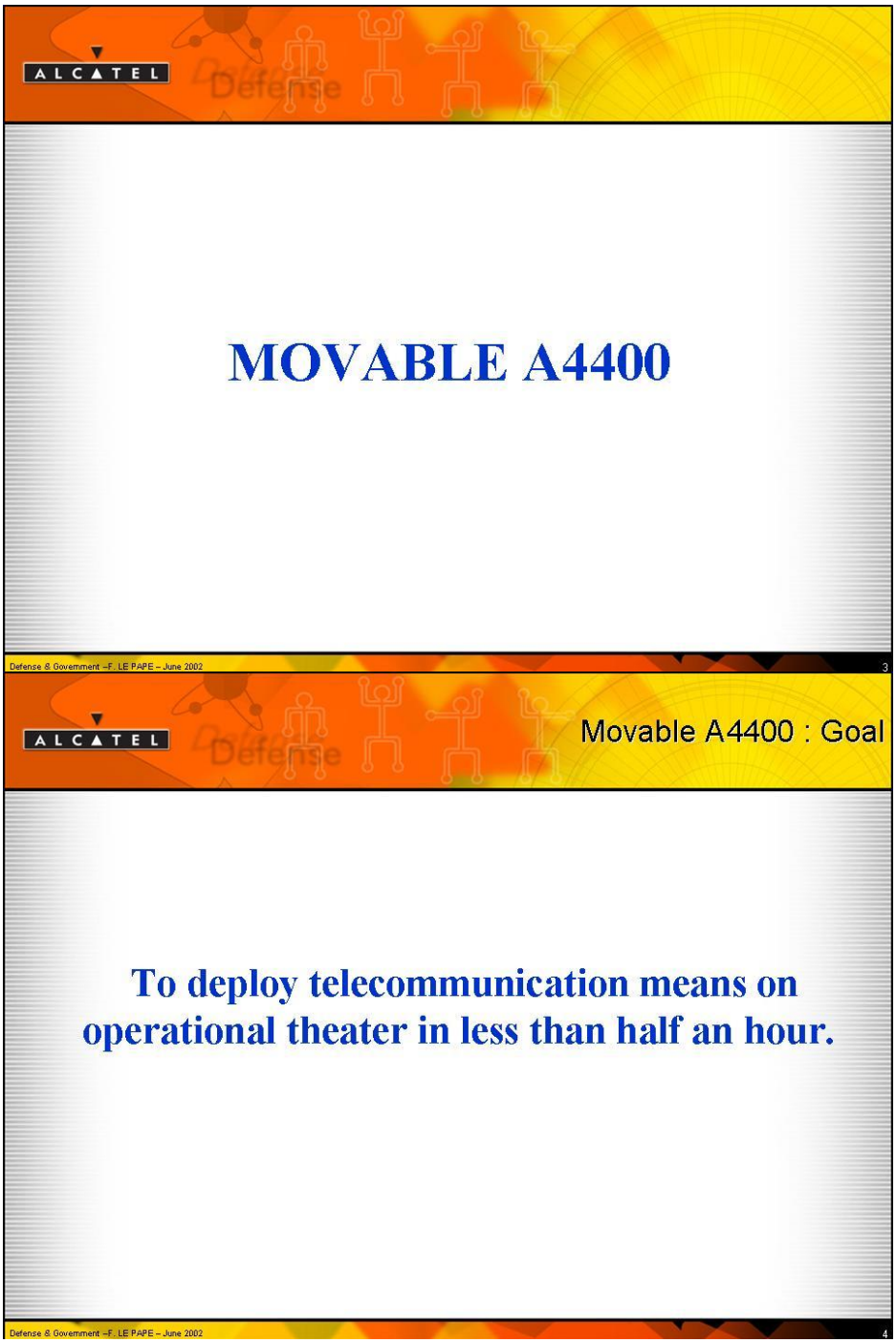
**Amphenol Socapex** Promenade de l'Arve -B.P.29 - 74311 THYEZ - FRANCE - Tel. :33 (0) 4 50 89 28 53 - Fax : 33 (0) 4 50 89 28 23

Specifications are subject to change without notice. All statements, information and data system given herein are believed to be accurate and reliable but are presented without garanty. No reproduction without agreement. E501/C. Printed in France by Amphenol Socapex.

**József TORJAI**

## OMNIPCX 4400 BENEFITS FOR DEFENSE




ALCATEL
Defense
MOVABLE A4400
Defense & Government –F. LE PAPE – June 2002
3
ALCATEL
Defense
Movable A4400 : Goal
To deploy telecommunication means on operational theater in less than half an hour.
Defense & Government –F. LE PAPE – June 2002
4

## Movable A4400: Description

- Composite material (Fiberglass and polyester resin)
- Operational temperature : -20°C +60°C
- Protection index : IP649 (with air cooling (DIN 40050 standards).
  - 6 (max) : fully protected against dusts.
  - 4 (mid) : protected against water projection from every direction.
  - 9 (max) : absorption of a shock energy of 20 joules (8 spirals shock absorbers).

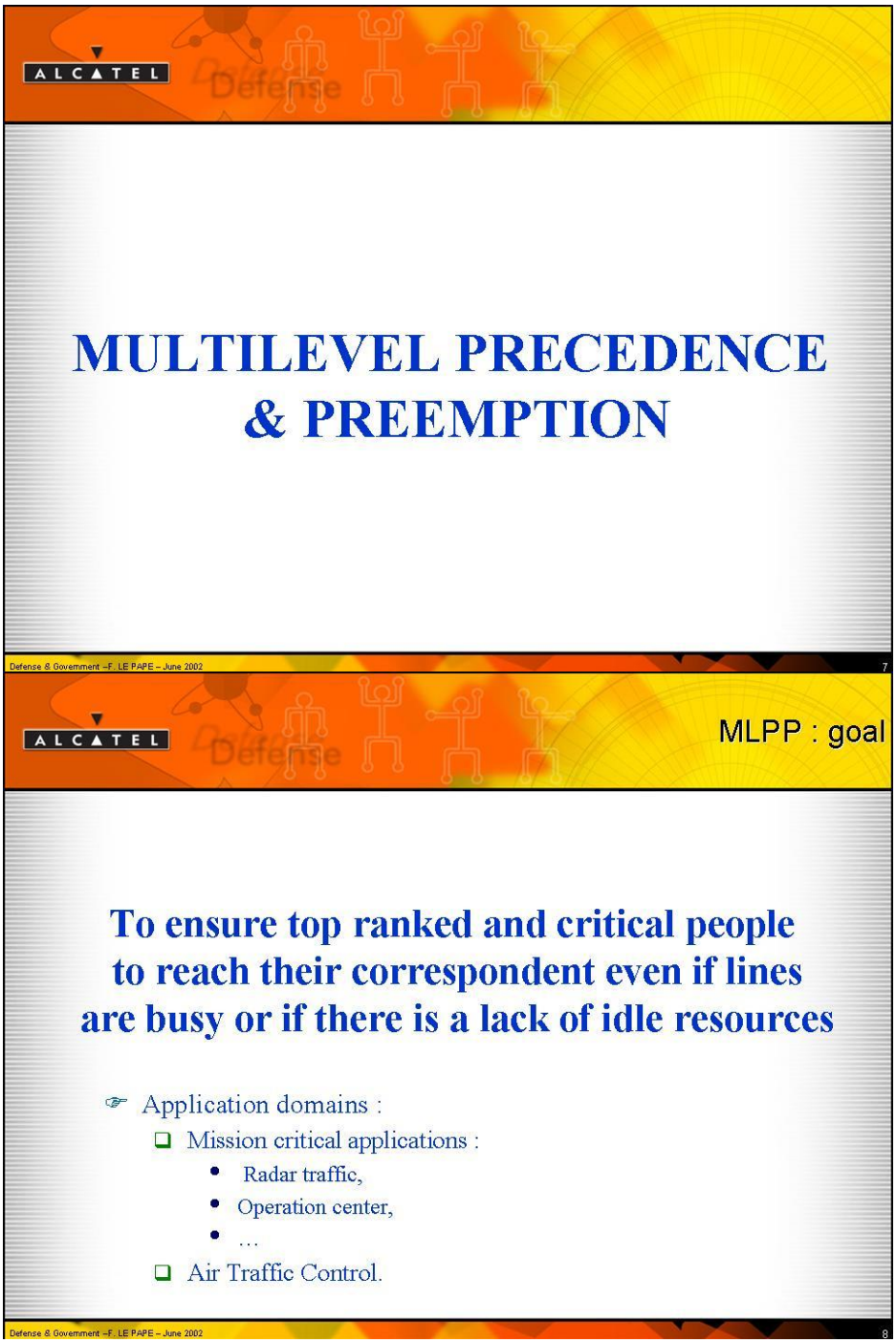




## Movable A4400: Description

- One casing for the 4400 :
  - 19 inches width, 12U height (#60 cm).
  - 14/28 position shelf (>500 users).
  - Any kind of board supported.
  - Integrated or external MDF.
  - Integrated management PC.
  - One integrated Radio Base Station for DECT.
- One casing for the power supply :
  - Rectifier & batteries.
  - 19 inches width, 6U height (depending on the battery capacity.




ALCATEL
Defense
MULTILEVEL PRECEDENCE
& PREEMPTION
Defense & Government –F. LE PAPE – June 2002
7
ALCATEL
Defense
MLPP : goal
To ensure top ranked and critical people
to reach their correspondent even if lines
are busy or if there is a lack of idle resources
Application domains :
Mission critical applications :
Radar traffic,
Operation center,
…
Air Traffic Control.
Defense & Government –F. LE PAPE – June 2002
8

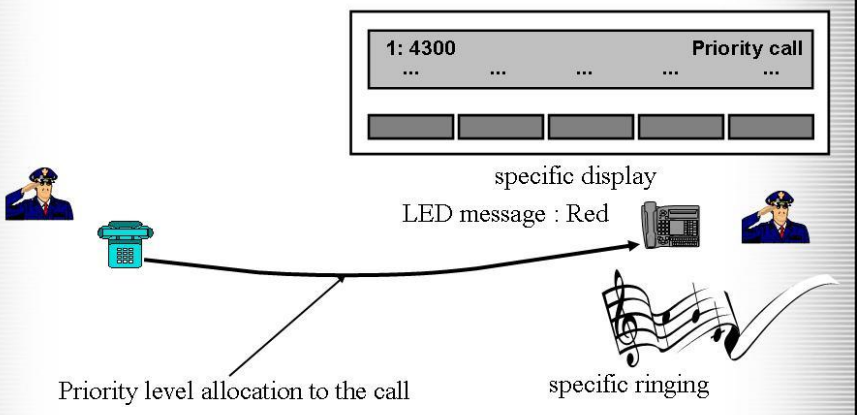
## MLPP : definitions

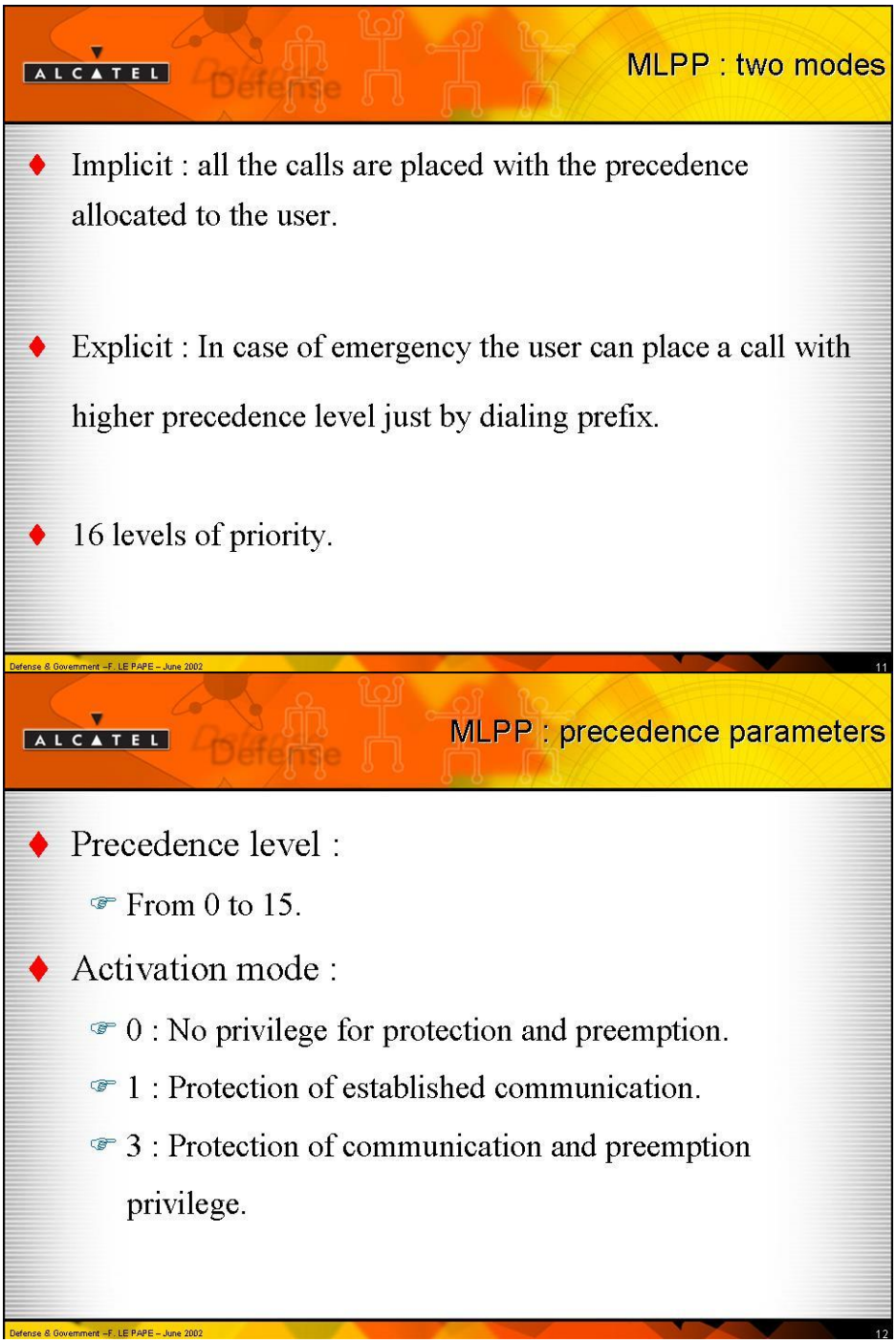
- Precedence :
  - allocation of a priority level and a specific call presentation (ringing or beep, display) to a call.
- Preemption :
  - Seizing of resources used by a lower precedence call to establish a higher precedence call in the lack of resources.
- Preemptable resources :
  - timeslots (B-channel), analog trunks, extensions.



## MLPP : Precedence

- Specific call presentation




ALCATEL
Defense
MLPP : two modes
Implicit : all the calls are placed with the precedence allocated to the user.
Explicit : In case of emergency the user can place a call with higher precedence level just by dialing prefix.
16 levels of priority.
Defense & Government –F. LE PAPE – June 2002
11
ALCATEL
Defense
MLPP : precedence parameters
Precedence level :
From 0 to 15.
Activation mode :
0 : No privilege for protection and preemption.
1 : Protection of established communication.
3 : Protection of communication and preemption privilege.
Defense & Government –F. LE PAPE – June 2002
12

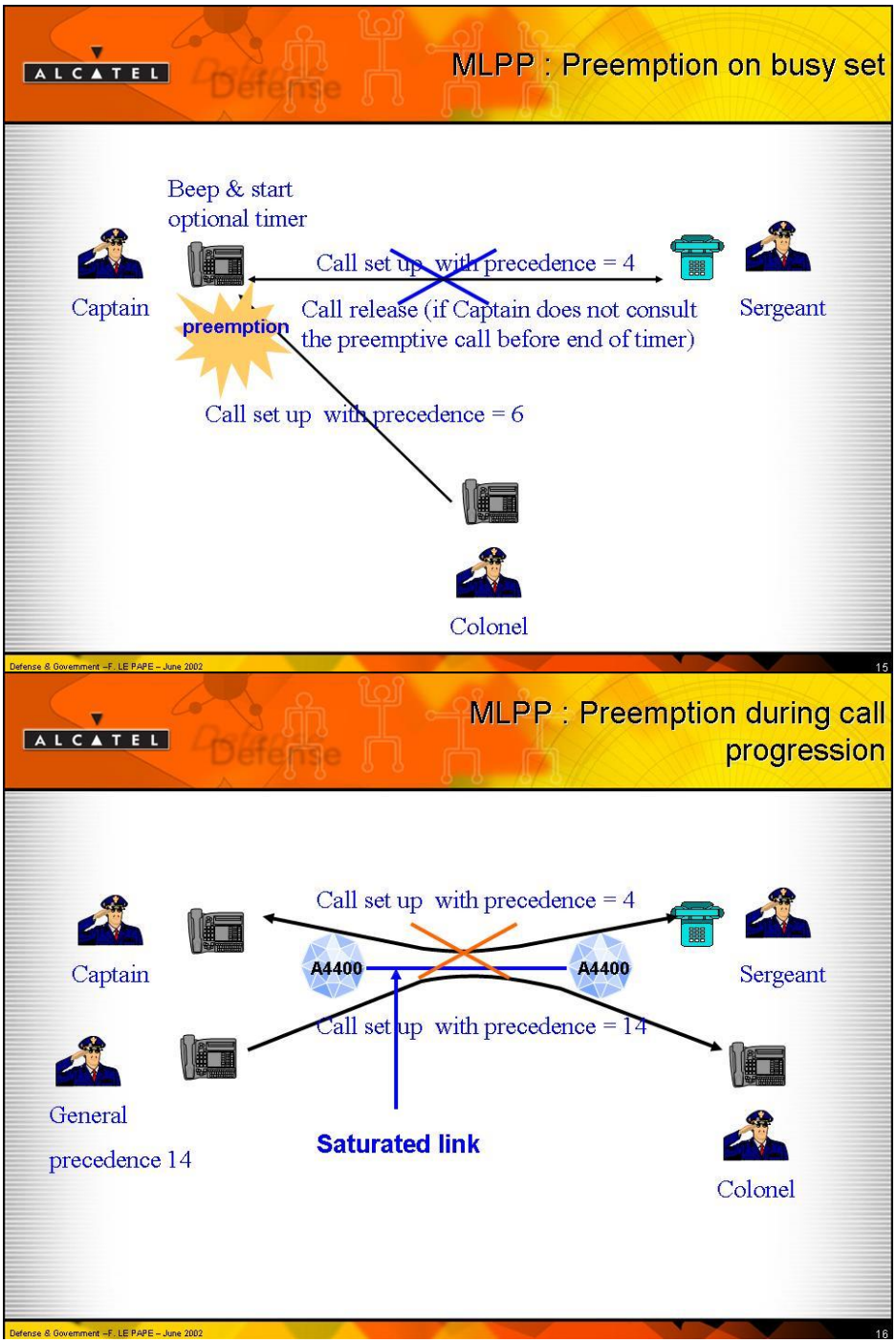
## MLPP : Preemption

- Only calls with activation mode 3 can preempt calls in the following order :
  - Calls with the activation mode 0 starting by the ones with the lowest level of precedence.
  - Calls with activation mode 1 or 3 starting by the ones with the lowest level of precedence and if the precedence level of the call to be set up is higher than the established ones.



MLPP : Preemption

- Two types of preemption :
  - Preemption on busy set.
  - Preemption during call progression.


MLPP : Preemption on busy set
Beep & start optional timer
Call set up with precedence = 4
Captain
preemption
Call release (if Captain does not consult the preemptive call before end of timer)
Sergeant
Call set up with precedence = 6
Colonel
Defense & Government –F. LE PAPE – June 2002
15
MLPP : Preemption during call progression
Call set up with precedence = 4
Captain
A4400
A4400
Sergeant
Call set up with precedence = 14
General
precedence 14
Saturated link
Colonel
Defense & Government –F. LE PAPE – June 2002
16

# CALL RESTRICTION



## Call restriction : Goal

**To gradually and temporary restrict telephone communications of non critical people from and to private or public networks**

- Main purpose :
  - Incident on nuclear power plant.
  - War.
  - Terrorist attack (11th of September).

## Call restriction : two types

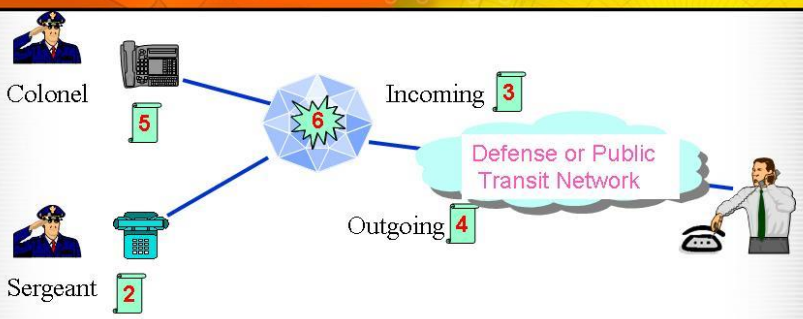
- Ivory Tower Tap mode (ITT) :
  - Established external communications are cut.
  - New external outgoing calls are forbidden, new external incoming calls are rejected.
- Minimize mode :
  - Only new external incoming / outgoing calls are forbidden.



## Call restriction : Alarm processing

- There is a “general alarm level” on the 4400 and each equipment has a “Call restriction category”.
- The cut or banning of calls are determined by comparison of :
  - The current general alarm level.
  - The call restriction category of the equipment with differentiation between incoming and outgoing call for a trunk.

## Call restriction : description



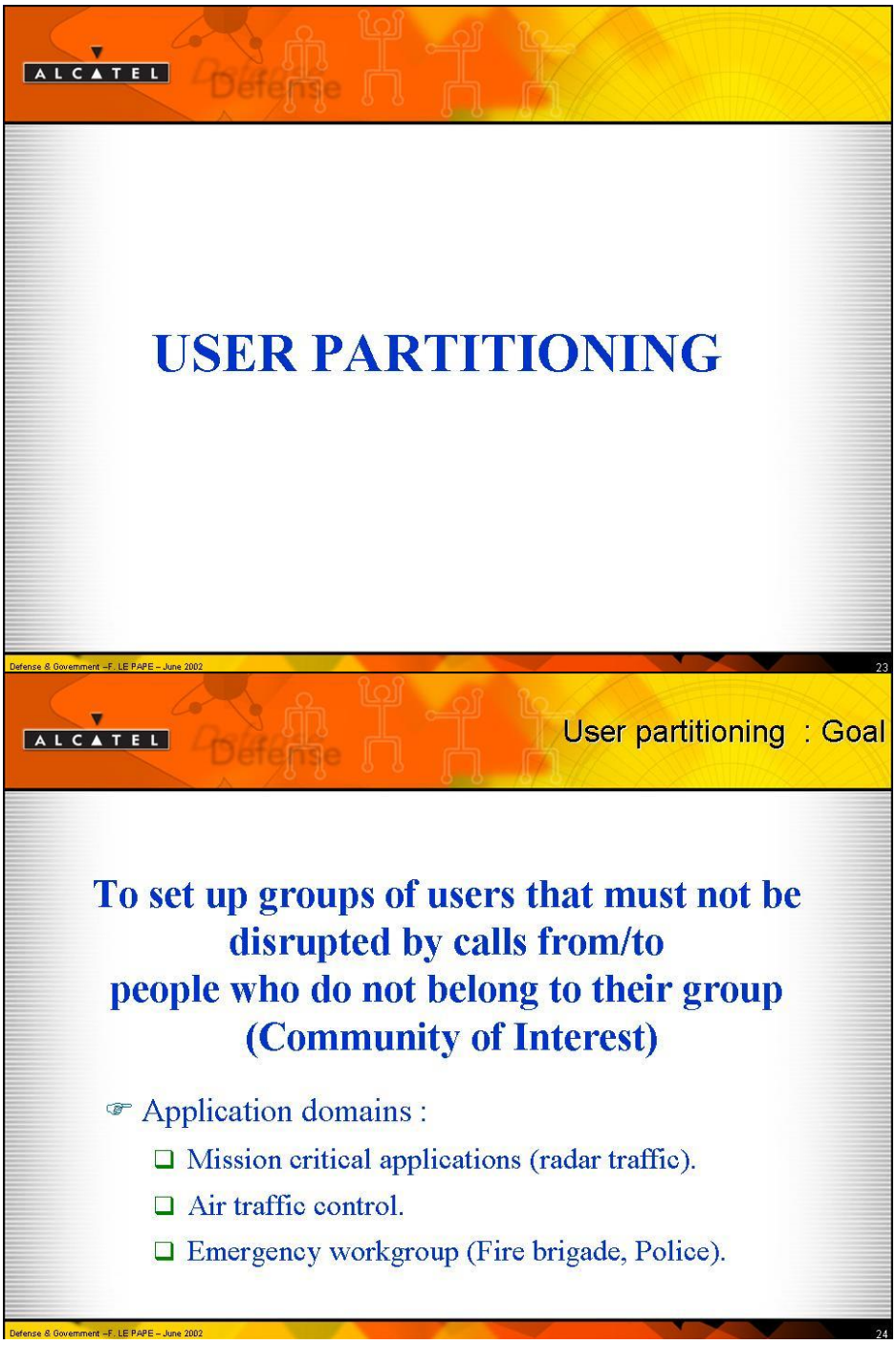

- All call restriction categories are higher than or equal to 2
  - No communication is forbidden.
- Sergeant can not receive an incoming call.
- Sergeant can not place an outgoing call.
- All outgoing and incoming calls are forbidden.

Defense & Government –F. LE PAPE – June 2002 21

## Call restriction : alarm activation

- The alarm threshold can be changed by :
  - Management.
  - An attendant.
  - An alarm set.
- Up to 10 levels of alarm can be managed.

Defense & Government –F. LE PAPE – June 2002 22


ALCATEL
Defense
USER PARTITIONING
Defense & Government –F. LE PAPE – June 2002
23
ALCATEL
Defense
User partitioning : Goal
To set up groups of users that must not be disrupted by calls from/to people who do not belong to their group (Community of Interest)
Application domains :
Mission critical applications (radar traffic).
Air traffic control.
Emergency workgroup (Fire brigade, Police).
Defense & Government –F. LE PAPE – June 2002
24

## User partitioning : two kinds

- Call category :
  - If the category of the caller and the called party are compatible the communication is set up.
  - If the category of the caller and the called party are not compatible the communication is released.
- Closed User Group :
  - Implicit :
    - Calls are placed with the CUG assigned by management.
  - Explicit.
    - Calls are placed with the CUG selected by the user.



## Closed User Group : parameters

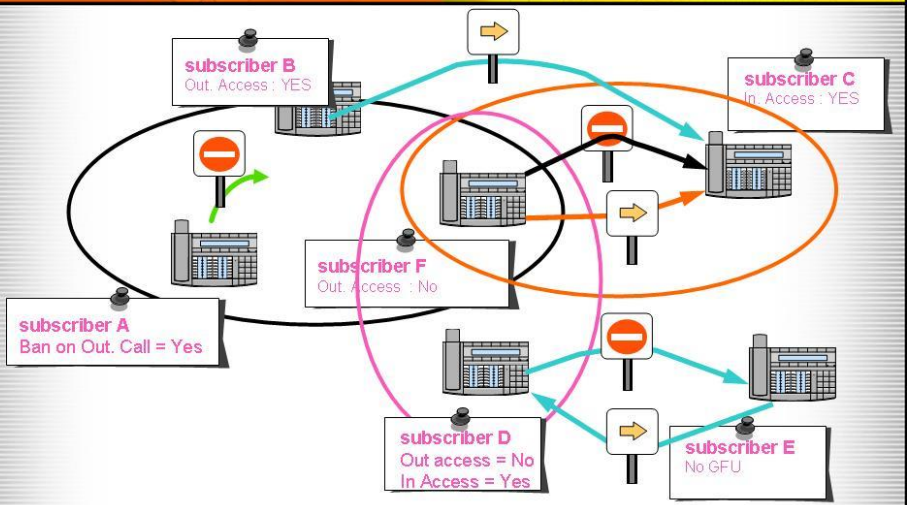
- Preferred CUG :
  - CUG by default (implicit mode) .
- Outgoing access.
  - To allow a CUG member to place calls to users who do not belong to the same CUG.
- Incoming access.
  - To allow a CUG member to receive calls from users who do not belong to the same CUG.

## Closed User Group : parameters

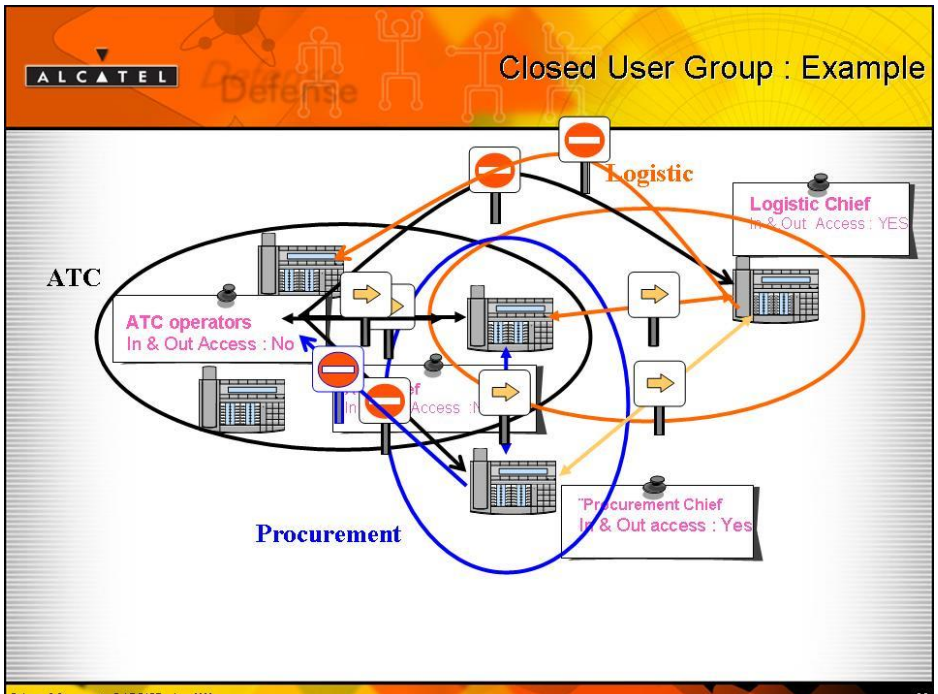
- List of authorized CUG for which the following restriction can apply :
  - Banning of outgoing call :
    - To forbid a CUG member to place call to users belonging to the same CUG.
  - Banning of incoming call :
    - To forbid a CUG member to receive call from users belonging to the same CUG.

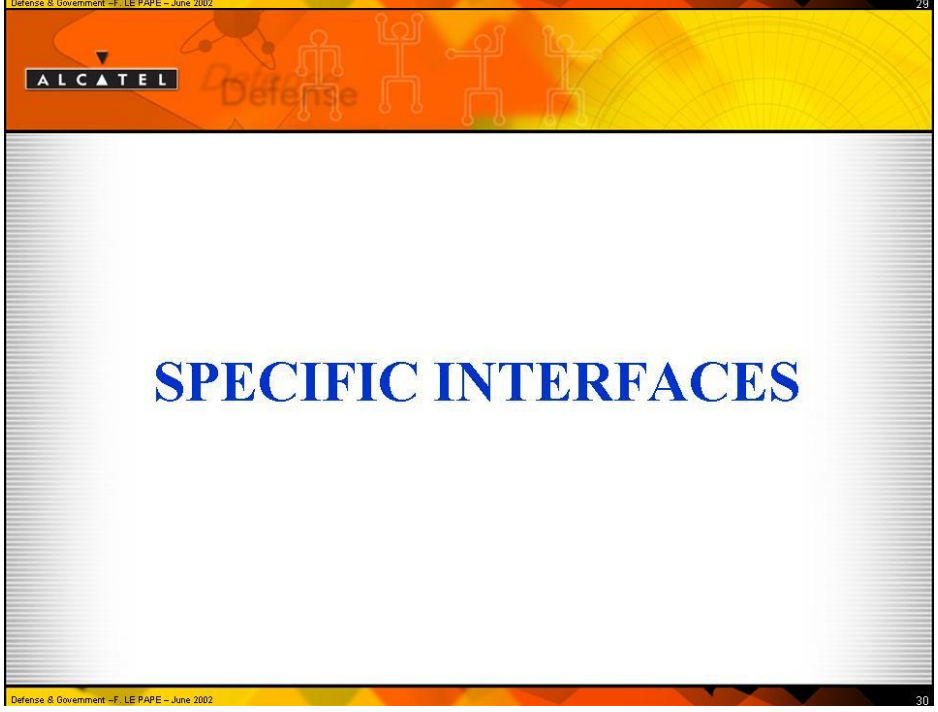
Defense & Government –F. LE PAPE – June 2002 27

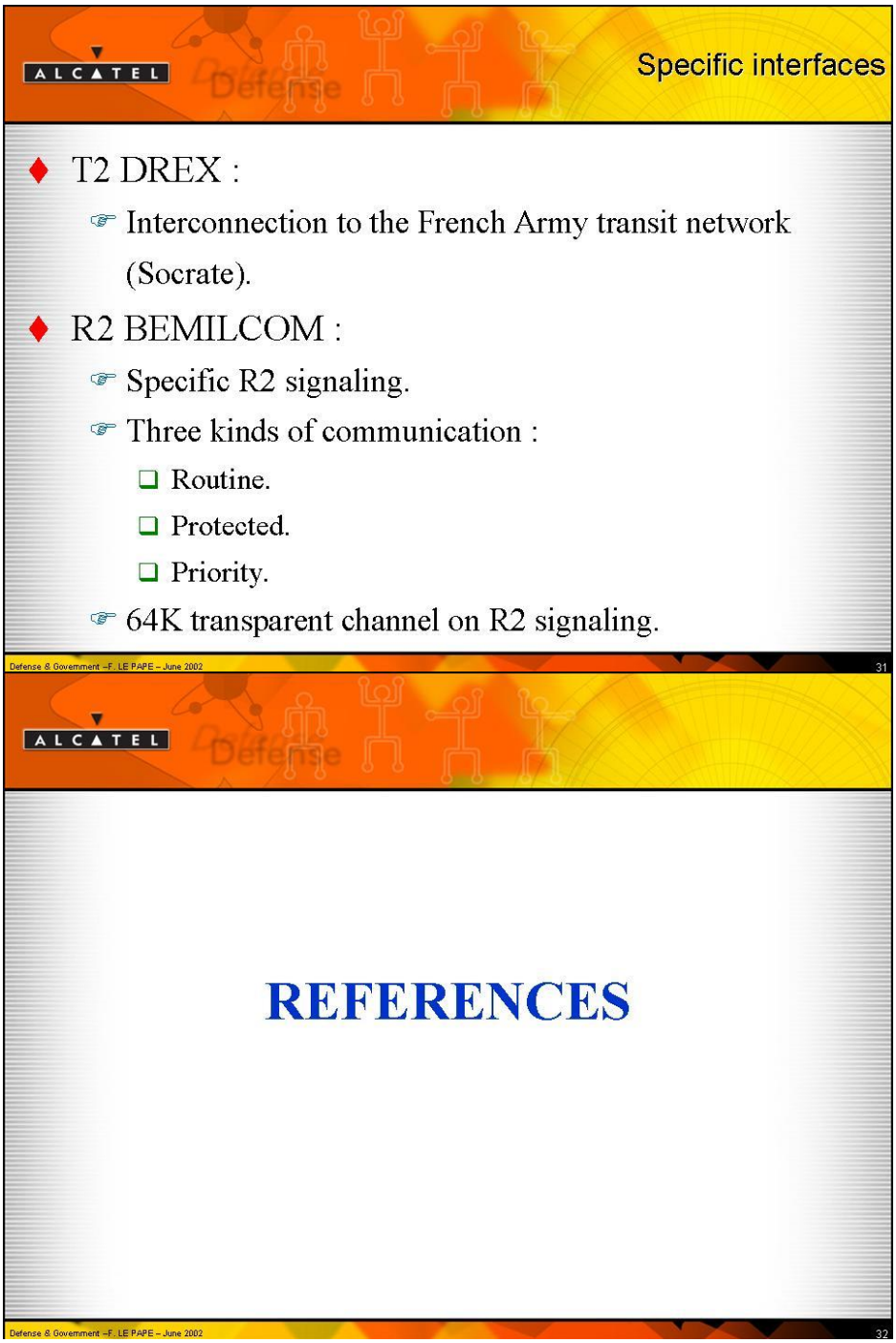
## Closed User Group : Some exercises

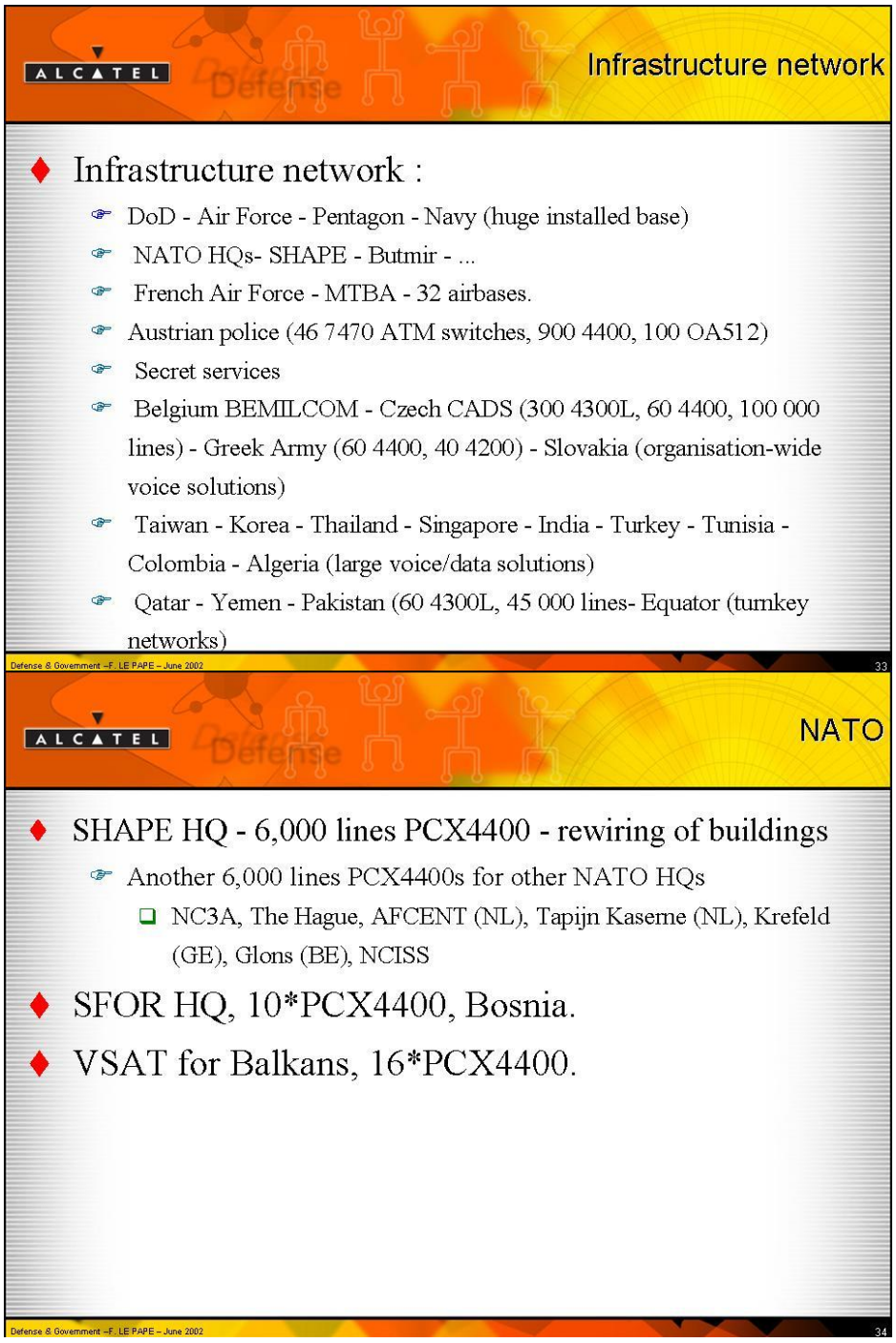



Defense & Government –F. LE PAPE – June 2002 28


ALCATEL
Closed User Group : Example
Logistic
Logistic Chief
In & Out Access : YES
ATC
ATC operators
In & Out Access : No
Procurement
Procurement Chief
In & Out access : Yes
Defense & Government –F. LE PAPE – June 2002
29


ALCATEL
SPECIFIC INTERFACES
Defense & Government –F. LE PAPE – June 2002
30

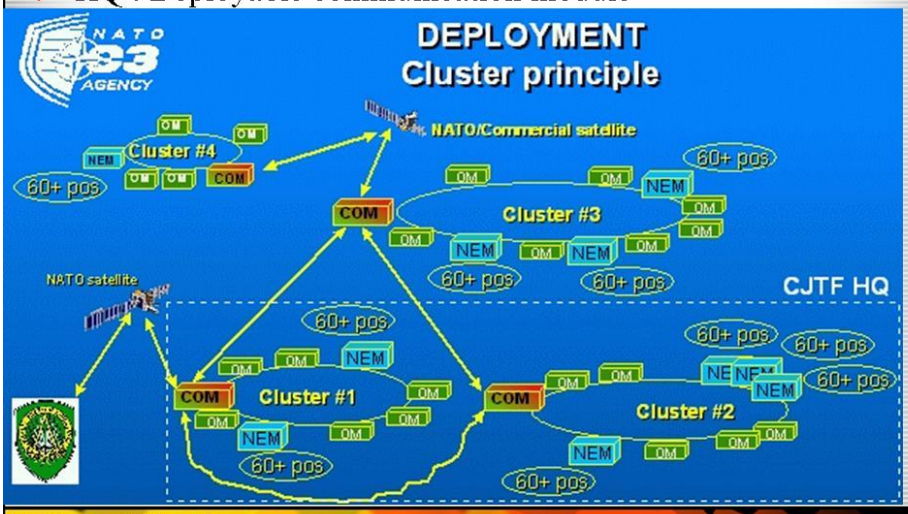

ALCATEL
Specific interfaces
T2 DREX :
Interconnection to the French Army transit network (Socrate).
R2 BEMILCOM :
Specific R2 signaling.
Three kinds of communication :
Routine.
Protected.
Priority.
64K transparent channel on R2 signaling.
Defense & Government –F. LE PAPE – June 2002
31
ALCATEL
REFERENCES
Defense & Government –F. LE PAPE – June 2002
32


ALCATEL
Defense
Infrastructure network
Infrastructure network :
DoD - Air Force - Pentagon - Navy (huge installed base)
NATO HQs- SHAPE - Butmir - ...
French Air Force - MTBA - 32 airbases.
Austrian police (46 7470 ATM switches, 900 4400, 100 OA512)
Secret services
Belgium BEMILCOM - Czech CADS (300 4300L, 60 4400, 100 000 lines) - Greek Army (60 4400, 40 4200) - Slovakia (organisation-wide voice solutions)
Taiwan - Korea - Thailand - Singapore - India - Turkey - Tunisia - Colombia - Algeria (large voice/data solutions)
Qatar - Yemen - Pakistan (60 4300L, 45 000 lines- Equator (turnkey networks)
Defense & Government –F. LE PAPE – June 2002
33
ALCATEL
Defense
NATO
SHAPE HQ - 6,000 lines PCX4400 - rewiring of buildings
Another 6,000 lines PCX4400s for other NATO HQs
NC3A, The Hague, AFCENT (NL), Tapijn Kaserne (NL), Krefeld (GE), Glons (BE), NCISS
SFOR HQ, 10*PCX4400, Bosnia.
VSAT for Balkans, 16*PCX4400.
Defense & Government –F. LE PAPE – June 2002
34

ALCATEL

## NATO NC3A UIE project

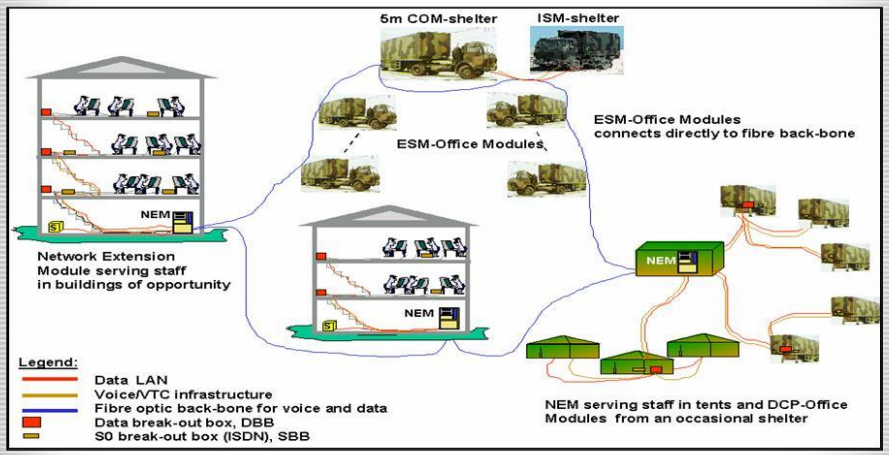
- HQ : Deployable communication module





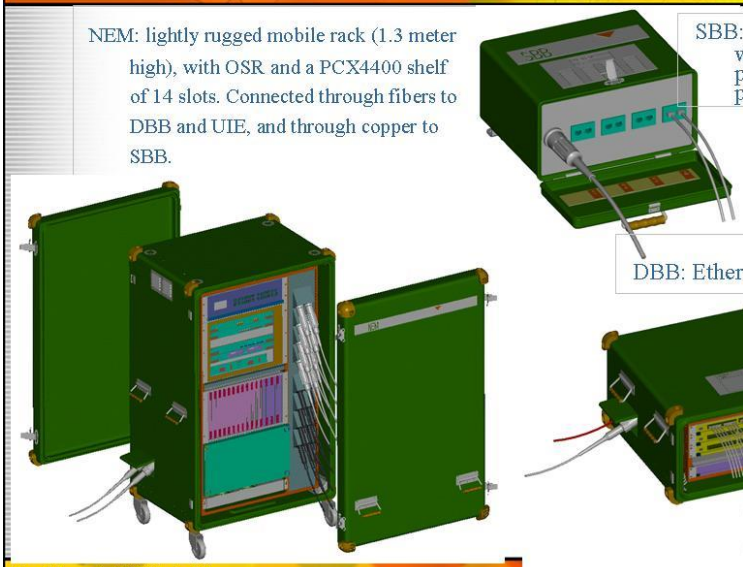

ALCATEL

## NATO : User Interface Enclosure



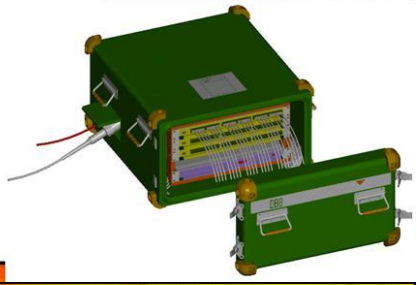
## NATO : User Interface Enclosure

NEM: lightly rugged mobile rack (1.3 meter high), with OSR and a PCX4400 shelf of 14 slots. Connected through fibers to DBB and UIE, and through copper to SBB.



SBB: 8 S0-ISDN bus, with A4094 plugware S0 powered

DBB: Ethernet stack 6024



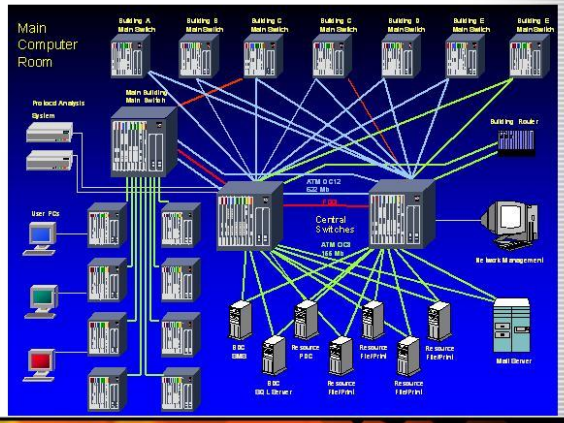


## French Air Force

- Voice/data infrastructure and air defense network
- 200 OmniPCX for 32 airbases
- System integrator Thales, deployment 1999/2003
- Approximately 65,000 users
- PCX4400 delivers ***a range of military, security, and air defense services***:
  - MLPP, Add-on conference, Broadcast, call restriction, CUG, AID
  - **Loop**, **hotlines**, **interphony**, telebriefing
  - Secure management architecture

## US : Wright Patterton Air Force base backbone : 88th comm squadron

- ATM backbone.
- 200 switches already deployed (10 000 users).






## Thank you

**T-SYSTEMS**

## AZ ELEKTRONIKUS KORMÁNYZATI GERINCHÁLÓZAT (EKG) KÍNÁLTA LEHETŐSÉGEK




### Az EKG modell



- Az EKG pályázat célkitűzései
- Az üzleti modell
- Az EKG felépítése
- Alapszolgáltatások
- Értéknövelt szolgáltatások
- Felhasználó számára kínált előnyök
- Időterv

T Systems

## Az EKG pályázat célkitűzései

- Fejlesztések: Hálózat funkcionális bővítése (újabb intézmények bekapcsolása, további központi szolgáltatások nyújtása) külső forrás bevonásával
- Költségek csökkentése (intézményközi hangforgalom EKG-ra terelése)
- Magas minőségű szolgáltatás lehetőségének megteremtése
- Kormányzati intézmények kapcsolása az EKG-hez
- Új szolgáltatások bevezetése
- Újabb intézmények bekapcsolása – jelenlegi szolgáltatások megtartása – jelentős megtakarítás
- Üzemeltetés biztonság növelése ( mission critical szint elérése) infrastruktúra szinten tartás
- Hatékonyság javítása



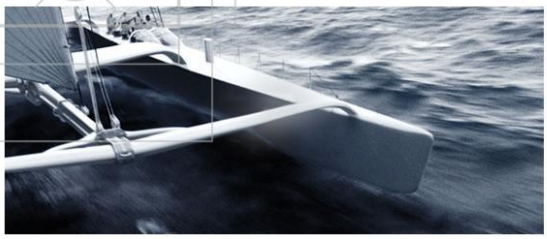
T · · Systems ·

2

## Az üzleti modell

- Magas rendelkezésre állású gerinc hálózat
- Kormányzati intézmények kapcsolása az EKG-hez
- Új szolgáltatások bevezetése
- Internet hozzáférés

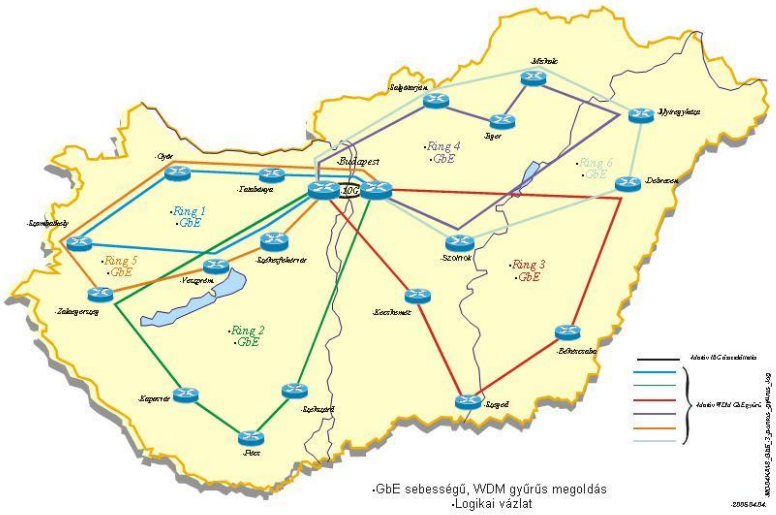




T · · Systems ·

3

## Az EKG felépítése - 1GbE gyűrűk: 100%-os rendelkezésre állás a csomópontokban

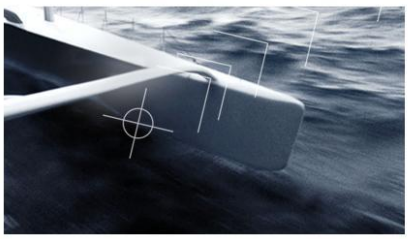





## Alapszolgáltatások

- Elektronikus Kormányzati Gerinc hálózat
  - az adatszolgáltatás a felhasználók számára ingyenes
- Adat - hang integráció, VoIP
  - egy hálózat, költség-hatékonyan
  - hangforgalom a hálózaton belül forgalomtól független díjazással
- Internet hozzáférés
  - a felhasználók számára ingyenes
- Egységes, menedzselt felhasználói hálózatok





## Emeltszintű szolgáltatások - Kommunikációs szolgáltatások



- IP telefónia
- Videó kommunikációs rendszerek
  - Videó telefónia
  - Videó konferencia rendszerek

T Systems



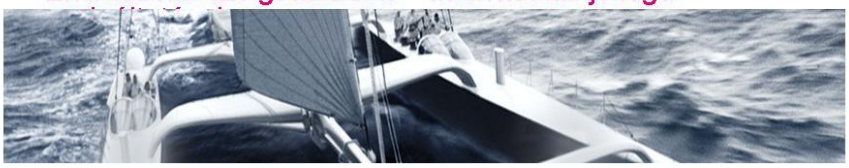
## Emeltszintű szolgáltatások - Informatikai jellegű



- **Hitelesítési szolgáltatások**
  - Fokozott biztonságú hitelesítési szolgáltatás
  - Minősített biztonságú hitelesítési szolgáltatás
  - Elektronikus aláírás csomagok:
  - Tanúsítványok – Csipkártyák
  - Aláíró és ellenőrző alkalmazások
  - Kártyaolvasók
  - Időpecsét szolgáltatás
  - Autentikációs és titkosító tanúsítványok
  - Közigazgatási „kompatibilis” Kártya és aláíró alkalmazás

T Systems

## Emeltszintű szolgáltatások - Informatikai jellegű



- **Menedzselt IT biztonsági megoldások**
  - IDS / IPS megoldások
  - DOS /DDOS védelem
  - Menedzselt tűzfalak
  - Biztonságos hozzáférés
  - VPN csatorna kialakítása
  - Vírusellenőrzés
  - Biztonsági politika kialakítása
  - IT tanácsadás

T Systems



## Emeltszintű szolgáltatások - Informatikai jellegű szolgáltatások



- Névtár szolgáltatás
- Data Center szolgáltatás
- Menedzselt LAN szolgáltatás
- Szimulációs modellezés

T Systems

## Emeltszintű szolgáltatások





- **Távmunka megoldás**
  - Távmunka csomagok
  - Autentikáció
  - Biztonsági megoldások
- **Távoktatás – esetleg ASP jelleggel is**
  - Távoktatás csomagok
  - Autentikáció
  - Biztonsági megoldások
  - Multimédia anyagok készítése
  - Oktatási környezet kialakítása
  - ASP jellegű üzemeltetés

közigazgatáson belüli előírt képzések támogatása

T Systems

10

## Emeltszintű szolgáltatások



- **Egyéb szolgáltatások**
  - Intelligens épület csomagok
  - Központi Help Desk és Ügyfélszolgálat

T Systems

11

## A HM számára kínált előnyök

- A távközlési szolgáltatások igénybevételéből eredő költségei minimum 10%-kal csökkennek
- Az EKG igénybevételével jelentős sávszélesség bővítés hajtható végre (3-5*).
- Forgalmi díj mentes telefonálási lehetőség a Kormányzati hálózaton belül. (Felhasználó valamint a Felhasználói csoporton belül)
- Felcsatlakozás - egyszeri költség nélkül a 2005. 06.30-ig jelentkezőknek
- A díjmegtakarítások emeltszintű szolgáltatások igénybevételére fordíthatók
- [illegible]

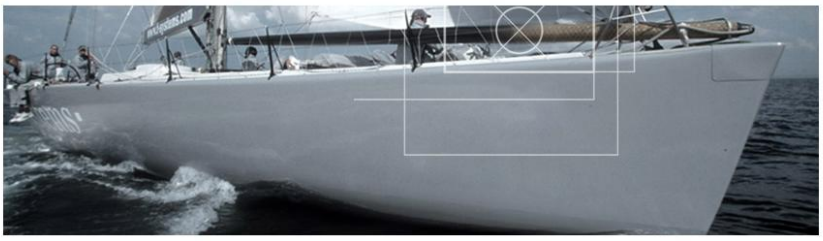


T Systems



## Időterv

| Mérföldkő | Dátum |
|---|---|
| Projekt indítása (szerződés aláírás dátuma) | 2005. ápr. 25. |
| Felcsatlakozási tárgyalások megkezdése egyes intézményekkel | 2005. jún. 13. |
| Szolgáltatás indítása | 2005. novembertől |
| Emelt szintű szolgáltatások bevezetése | 2005. novembertől ütemezetten |



T Systems


Köszönöm megtisztelő
figyelmüket!
T Systems

**WB Electronics**

## TACTICAL FIBER OPTIC COMMUNICATION

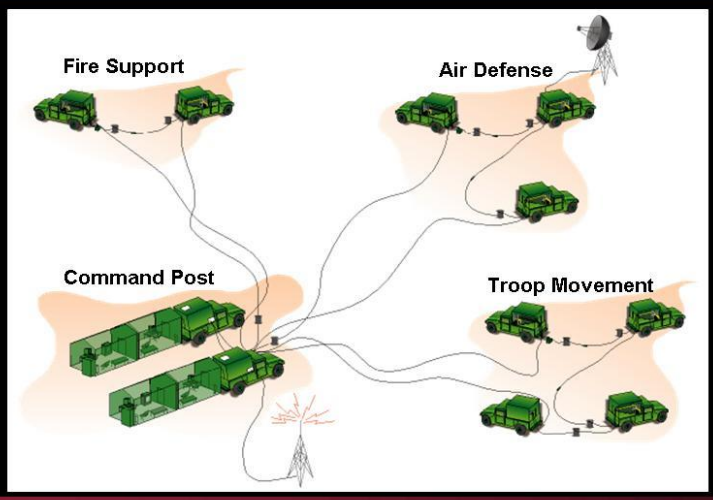




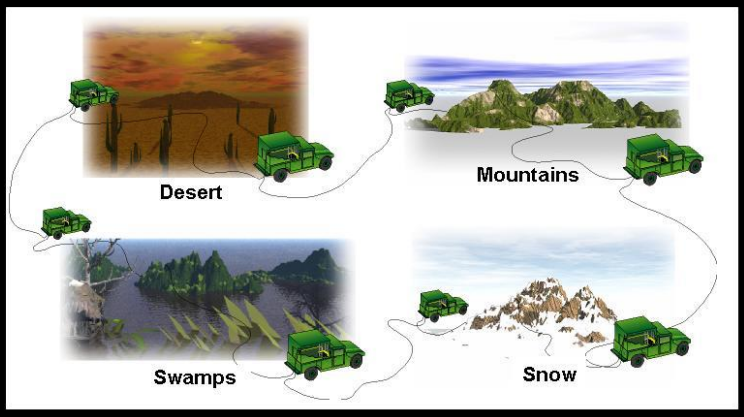

## Applications

- Dispersed Command Post
- Harsh Environments
- Down The Hill
- Disaster Relief

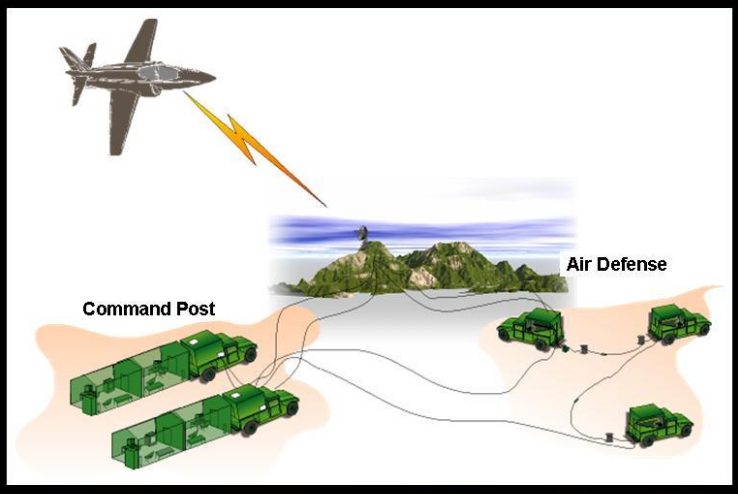
## Dispersed Command Posts



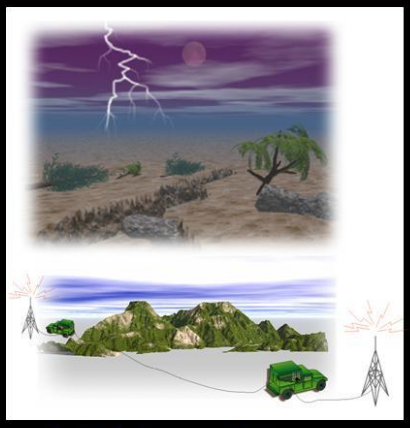
## Harsh Environments




## Down The Hill



## Disaster Relief



Rapid Deployment of Emergency Communications

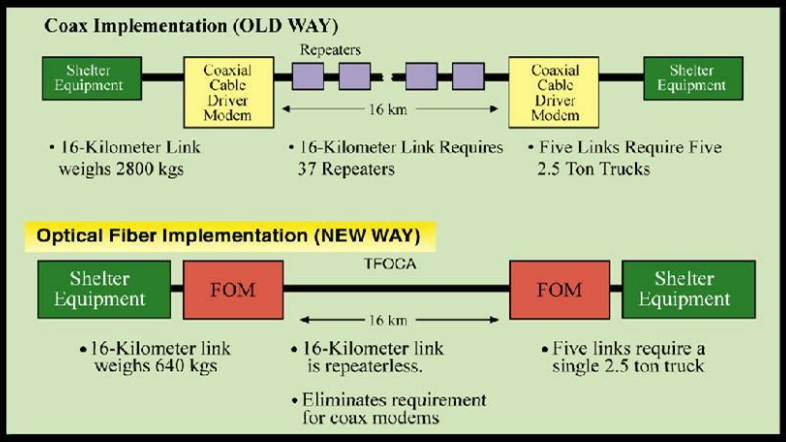
## Interconnect Tactical Communication Equipment

- Radio Terminals
- Radio Repeaters
- Tactical Switches
- Circuit Switches
- Tactical Multiplexers
- Satellite Support Radios
- TACC Shelters

## Why Fiber Optics?

- Lighter weight and smaller size for much quicker deployment
- Higher bandwidth for increased throughput
- Lower loss for long distance repeaterless communication up to 16 kilometers
- Better quality - safe from electromagnetic interference from any source
- More secure - no electromagnetic signature
- Significantly reduced maintenance

## Benefits of Optical Fiber Over Coax



## FOM Versions

**Single Channel FOM**

U.S.

Euro



Shelter or Rack Mount

**Dual FOM**

U.S.



Rack Mount or "Throw on the Ground"

**Multi Channel FOM**

Euro



Rack Mount or "Throw on the Ground"

MOOG COMPONENTS GROUP

## Single Channel FOM





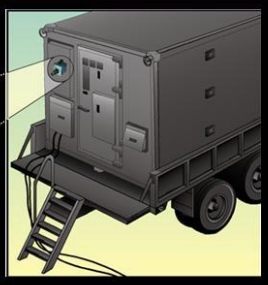


The Single Channel Fiber Optic Modem (FOM) provides an all-weather, totally transparent optical link between mobile shelter equipment and/or to remote transceiver sites for tactical communications.

MOOG COMPONENTS GROUP

## Single Channel FOM



**Physical Characteristics**

**Weight**: 3.75 lbs. (1.7 kg)

**Dimension**: 4.0" x 4.0" x 3.75"
(10.16 cm x 10.16 cm x 9.53 cm)

All of the above impact defense mobility and rapid deployment requirements.

MOOG COMPONENTS GROUP

## Single Channel FOM Configurations

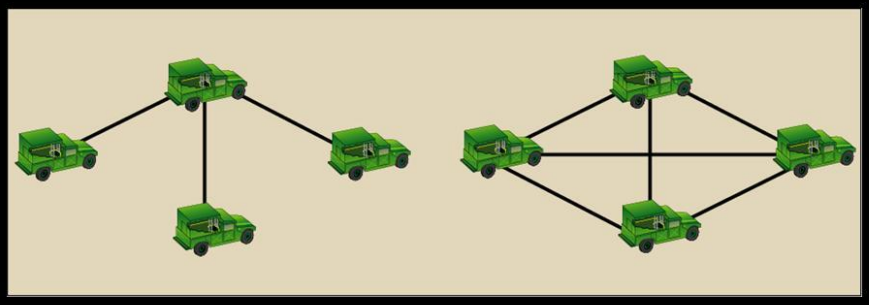
| Description | MD1272/G | EuroFOM-B/1 | EuroFOM-E3/1 | DS-3/1 |
|---|---|---|---|---|
| Power Requirement | 5 VDC | 28 VDC | 5 VDC | 5 VDC |
| Electrical Signal | Balanced NRZ Conditional Diphase | Eurocom D/1, Interface B | ITU G.703 | ANSI T1.102 |
| Optical Signal | JTC3A 9109C | Eurocom D/1, Interface $C_o$ | JTC2A 9109C | JTC2A 9109C |
| Electrical Interface | MS27468T17B35P | MS3126E14-19P | 75 Ohm BNC | 75 Ohm BNC |
| Standard Accessories | Wiring and Mounting Diagrams | Wiring and Mounting Diagrams | Power Cable, Mounting Diagrams | Power Cable, Mounting Diagrams |
| Alarms | Summary (LOS and Transmit Fault) | Summary (LOS and Transmit Fault) | Summary (LOS, BPV, EXZ) | Summary (LOS, BPV, EXZ) |
| Environmental Specifications | Mil Qualified | Designed to Meet | Designed to Meet | Designed to Meet |
| Fiber | Multimode | Multimode | Single and Multimode | Multimode |

**Operating Temperature = -35 degrees C to +52 degrees C**

**Storage Temperature = -57 degrees to +71 degrees C**

MOOG COMPONENTS GROUP

## Typical Deployment



MOOG COMPONENTS GROUP

## FOM IP/1



- -10/100 Mbps auto configuring
- IEEE 802.3 compliant
- Designed for use in harsh environments
- Fully transparent Ethernet link
- Repeater-less communications up to 2 km
- Powered from 5 VDC or optionally 28 VDC
- TFOCA I, TFOCA II and Expanded Beam tactical connector versions
- Ruggedized RJ-45 connector
- Weighs less than 1.8 Kg (4.0 lbs.)

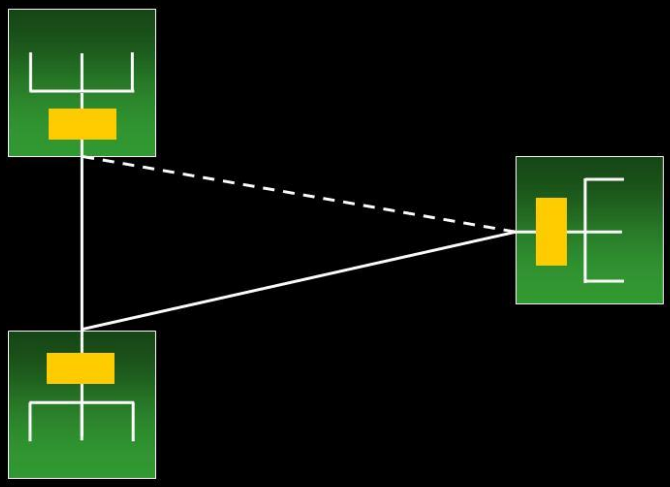
MOOG COMPONENTS GROUP

## 10/100 Mbps Configuration

| | |
|---|---|
| Power Requirement: | 5 VDC or 28 VDC |
| Electrical Signal: | IEEE802.3-2000 |
| Optical Signal: | JTC2A 91019C |
| Electrical Interface: | Shielded RJ45 |
| Standard Accessories: | Wiring and Mounting Diagrams |
| Alarms: | Discrete Status outputs provided:<br>- Optical signal speed (10-100)<br>- Electrical signal speed (10-100)<br>- Optical signal (packets) received<br>- Electrical signal speed (packets) received |
| Environmental Specifications | Designed to Meet |
| Fiber | Multimode |

MOOG COMPONENTS GROUP

## TOC LAN



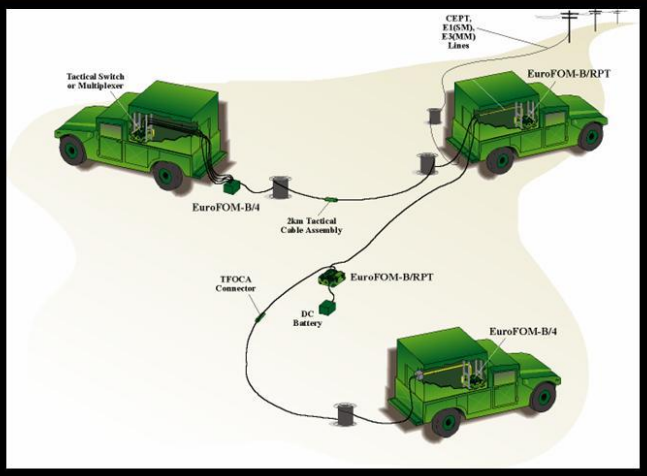
MOOG COMPONENTS GROUP

## Multi Channel FOM



MOOG COMPONENTS GROUP

## Multi Channel FOM




MOOG COMPONENTS GROUP

## Multi Channel FOM's Configurations

| Description | EuroFOM-E1/4 | EuroFOM-B/4 | EuroFOM-Drop/Add |
|---|---|---|---|
| Power Requirement | 48 VDC<br>120 VAC<br>220 VAC | 28 VDC<br>120 VAC<br>220 VAC | 28 VDC<br>120 VAC<br>220 VAC |
| Electrical Signal | CEPT E1 | Eurocom D/1,<br>Interface B | Eurocom D/1,<br>Interface B |
| Optical Signal | JTC3A 9109C | Eurocom D/1,<br>Interface $C_o$ | Eurocom D/1,<br>Interface $C_o$ |
| Electrical Interface | 120 OHM BNC and data | MS3126E14-19P | MS3126E14-19P |
| Standard Accessories | Power and Data<br>Cables, 19"<br>Rack Mount kit | Power and Data<br>Cables, 19"<br>Rack Mount kit | Power and Data<br>Cables, 19"<br>Rack Mount kit |
| Alarms | Summary (LOS and<br>Transmit Fault) | Summary (LOS and Transmit<br>Fault) | Summary (LOS and<br>Transmit Fault) |
| Environmental<br>Specifications | Designed to Meet | Designed to Meet | Designed to Meet |
| Electric Channels | Up to 4 | Up to 4 | Up to 2 |
| Fiber | Single Mode | Multi Mode | Multi Mode |

**Operating Temperature = -35 degrees C to +52 degrees C**
**Storage Temperature = - 57 degrees C to +71 degrees C**

MOOG
COMPONENTS GROUP

## Amphenol – CTOS Military Optical Connector



## Amphenol – CTOS Military Optical Connector

Main features:

- Hermafroditic
- Heavily resistant to mechanical damage
- Ambient to dirt, mud, snow etc (when mated)
- Easy to clean (if dirted when unmated)
- Ergonomical
- No maintenance or service necessary
- Available in MM i SM versions
- Standard for Polish, French, Belgian and Israelian armies
- Widely used within other NATO armies

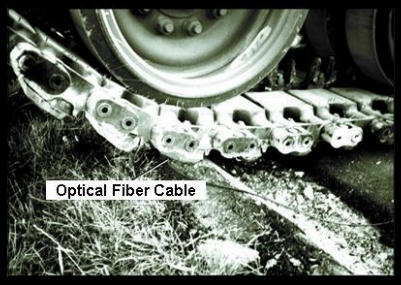
## Tactical Fiber Optic Cable Assembly

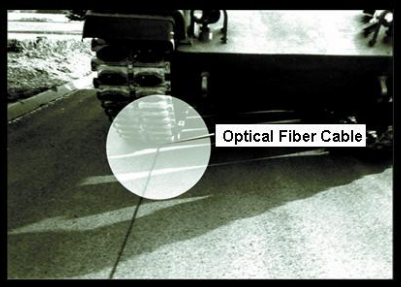


- Qualified to stringent U.S. Army Military Specifications:
  - **Temperature:**
    Operating: -46 degrees C to +71 degrees C
    Storage: -55 degrees C to +85 degrees C
  - **Tensile Load:**
    Deployment: 181 Kg
    Long Term: 51 Kg
- Light weight for rapid deployment
  1 Km (on Reel): Less than or equal to 40Kg

MOOG COMPONENTS GROUP

## Fiber Survivability

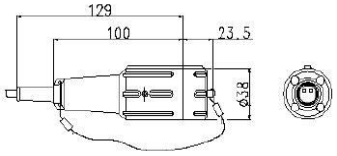


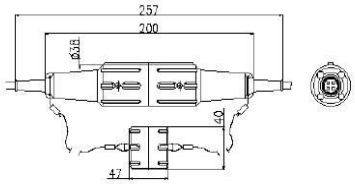
# CTOS 976 Series

## Line Drawings (dimensions in mm)

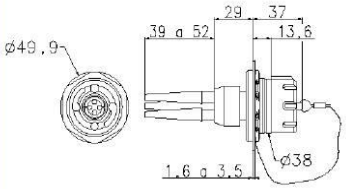
**CTOS plug with protective cap**



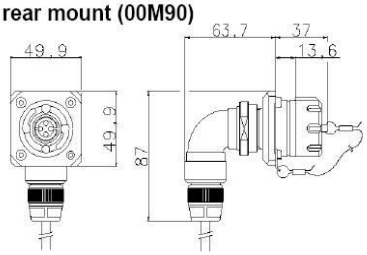

**CTOS plug to plug and caps mated**




**CTOS "jam nut" receptacle – rear mount (77P)**




**CTOS square flange receptacle with 90° Backshell for tactical cable – rear mount (00M90)**




## How to order :

CTOS – XXXX – XX – X – XX – X - XXX - XXX

CTOS : 976 series

| | |
|---|---|
| • Plug for tactical cable | : 06M |
| • Square flange receptacle for pig-tails | : 00P |
| • Jam nut receptacle for pig-tails | : 77P |
| • Flange receptacle for tactical cable | : 00M |
| • Jam nut receptacle for tactical cable | : 77M |
| • Shunt attenuating cap (4dB) | : BSA* |
| • Protective shunt attenuating cap (25dB) | : BPSA* |

* : multimode only

Straight backshell : 00
Right angle backshell : 90

Number of channels
2 channels : 2 4 channels : 4

01 : 50/125 µm
02 : 62.5/125 µm
05 : 9/125 µm singlemode

Y : Wavelength 1300 nm
Z : Wavelength 840 – 1300 nm
V : Wavelength 1550 nm
W : Wavelength 1300 – 1550 nm

All cables are tight jacket.
28 : O.D. patchcord 2.8 mm
55 : O.D. tactical 5.5 mm
230 : scindex O.D. cable 2 x 3 mm
Other cables possible.

BPF : Cap for plug
BPE : Cap for Jam Nut Receptacle
BPP : Cap for Square Flange Receptacle

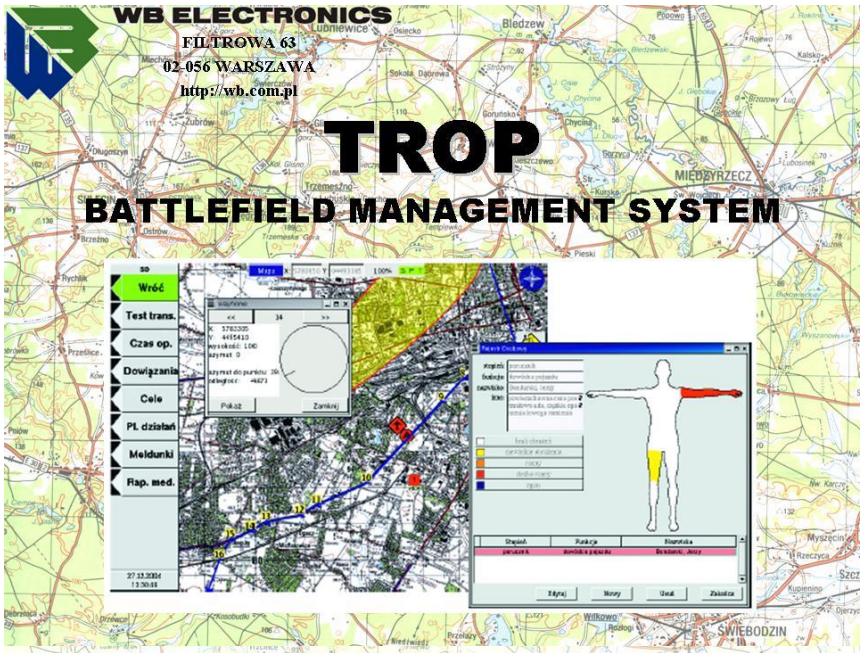
Amphenol

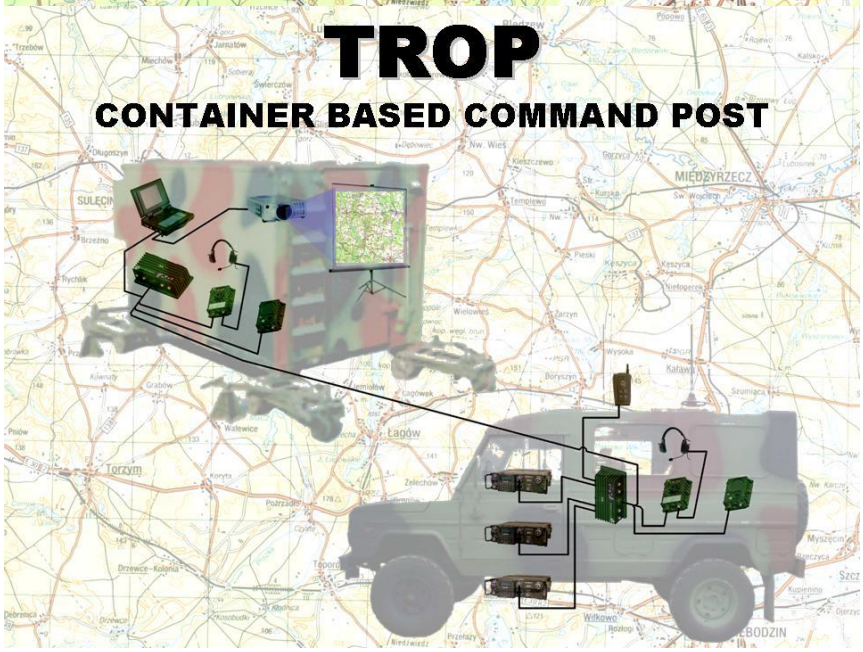
**Amphenol Socapex** Promenade de l'Arve -B.P.29 - 74311 THYEZ - FRANCE - Tel. :33 (0) 4 50 89 28 53 - Fax : 33 (0) 4 50 89 28 23

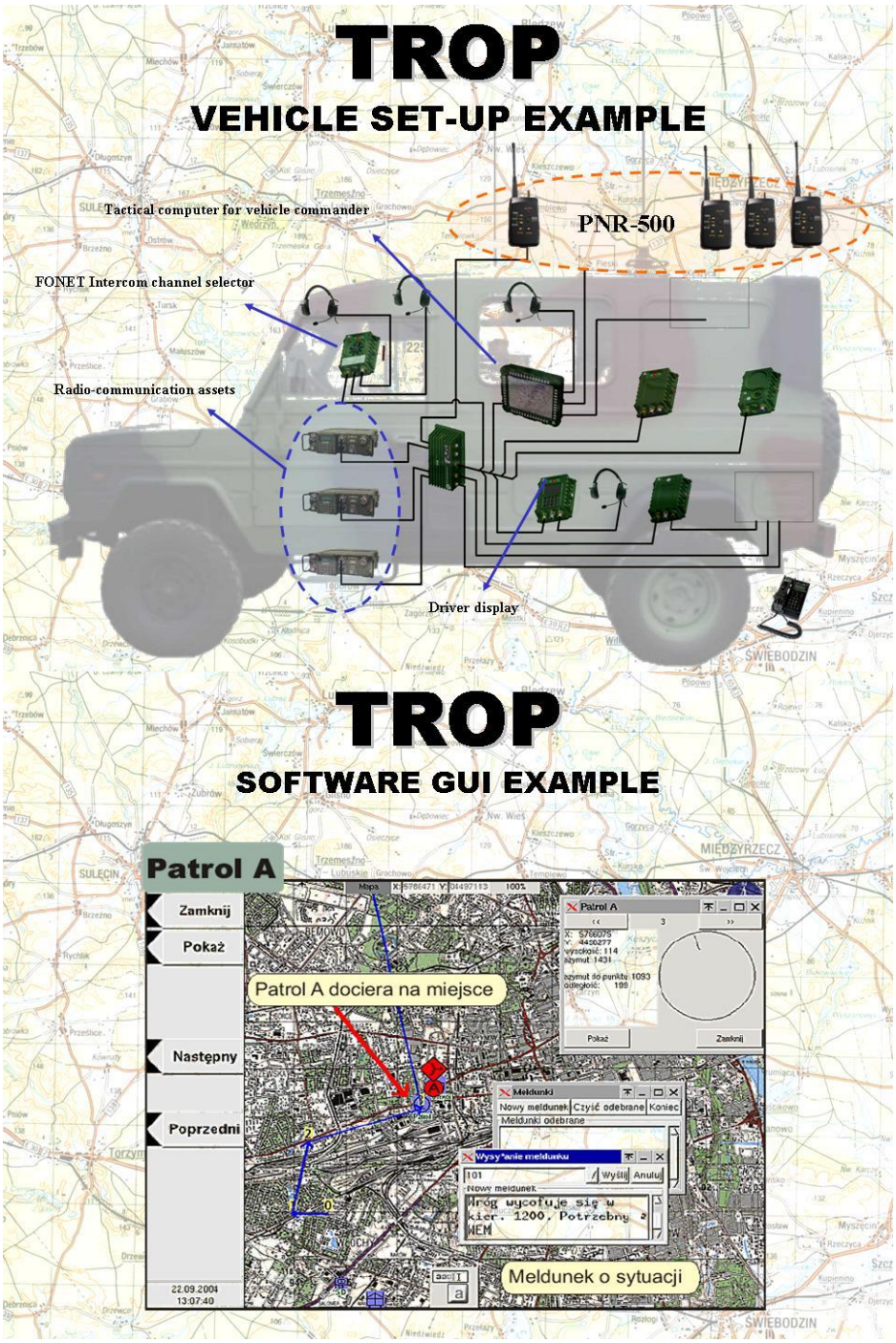
Specifications are subject to change without notice. All statements, information and data system given herein are believed to be accurate and reliable but are presented without garanty. No reproduction without agreement. E501/C . Printed in France by Amphenol Socapex.

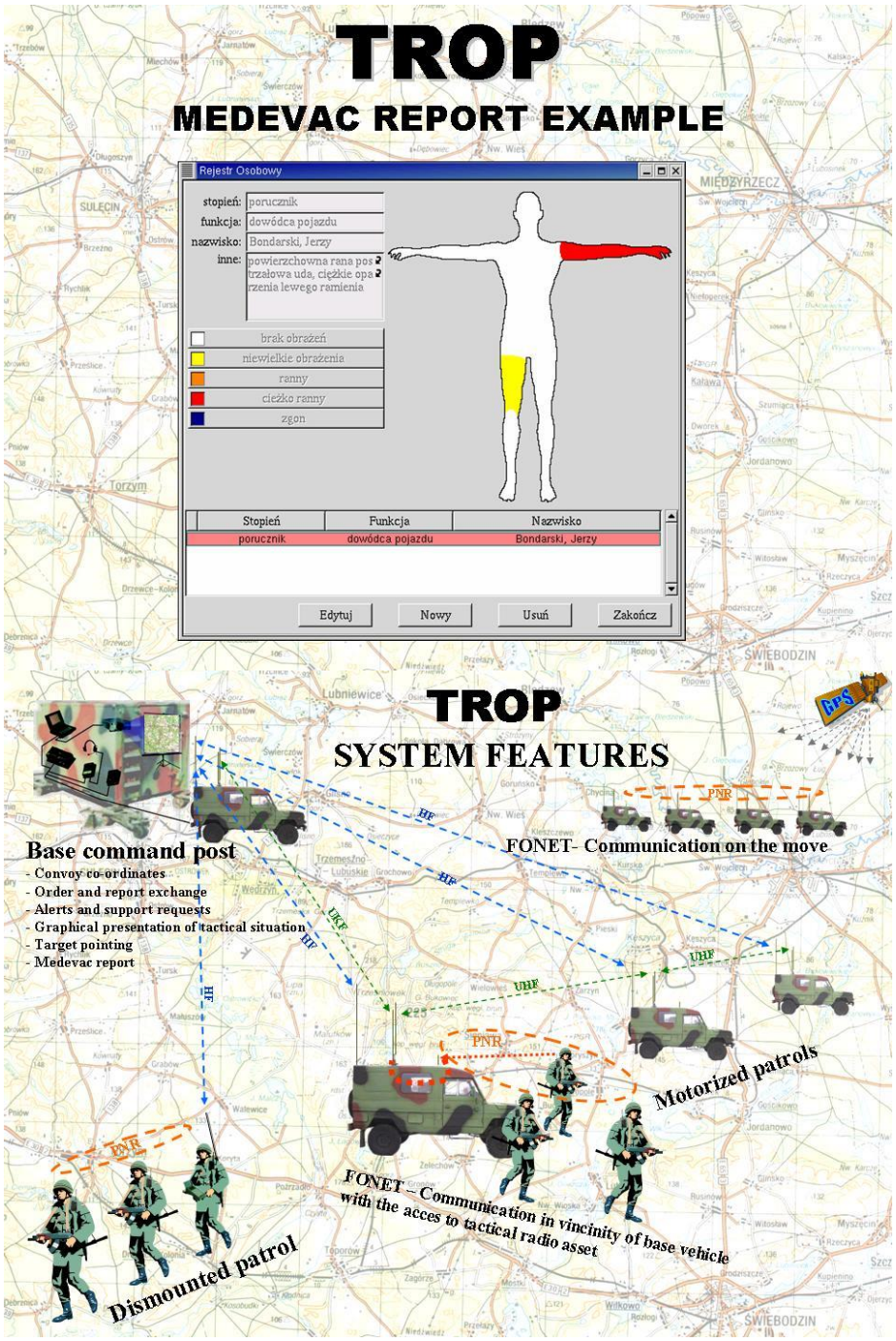
## WB Electronics

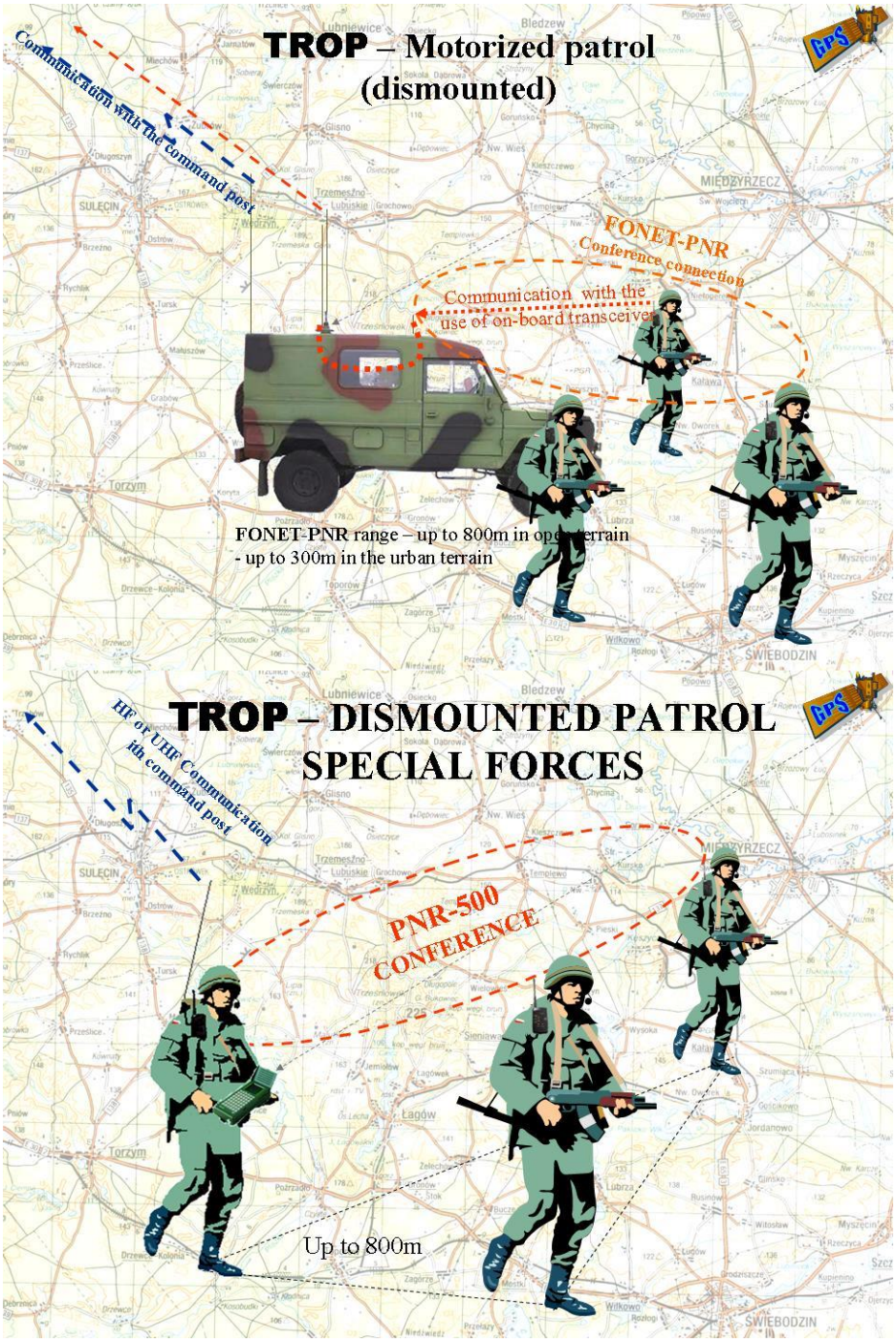
### TROP BATTLEFIELD MANAGEMENT SYSTEM




TROP
VEHICLE SET-UP EXAMPLE
Tactical computer for vehicle commander
PNR-500
FONET Intercom channel selector
Radio-communication assets
Driver display
TROP
SOFTWARE GUI EXAMPLE
Patrol A
Zamknij
Pokaż
Następny
Poprzedni
22.09.2004
13:07:40
Patrol A dociera na miejsce
Meldunek o sytuacji


TROP
MEDEVAC REPORT EXAMPLE
Rejestr Osobowy
stopień: porucznik
funkcja: dowódca pojazdu
nazwisko: Bondarski, Jerzy
inne: powierzchowna rana pos
trzałowa uda, ciężkie opa
rzenia lewego ramienia
brak obrażeń
niewielkie obrażenia
ranny
ciężko ranny
zgon
Stopień
Funkcja
Nazwisko
porucznik
dowódca pojazdu
Bondarski, Jerzy
Edytuj
Nowy
Usuń
Zakończ
TROP
SYSTEM FEATURES
Base command post
- Convoy co-ordinates
- Order and report exchange
- Alerts and support requests
- Graphical presentation of tactical situation
- Target pointing
- Medevac report
FONET- Communication on the move
Motorized patrols
FONET – Communication in vincinity of base vehicle
with the acces to tactical radio asset
Dismounted patrol
HF
UHF
PNR
CPS


TROP – Motorized patrol
(dismounted)
Communication with the command post
FONET-PNR
Conference connection
Communication with the
use of on-board transceiver
FONET-PNR range – up to 800m in open terrain
- up to 300m in the urban terrain
GPS
TROP – DISMOUNTED PATROL
SPECIAL FORCES
HF or UHF Communication
with command post
PNR-500
CONFERENCE
Up to 800m
GPS

THALES



# C4ISR
# Systems Architect

601