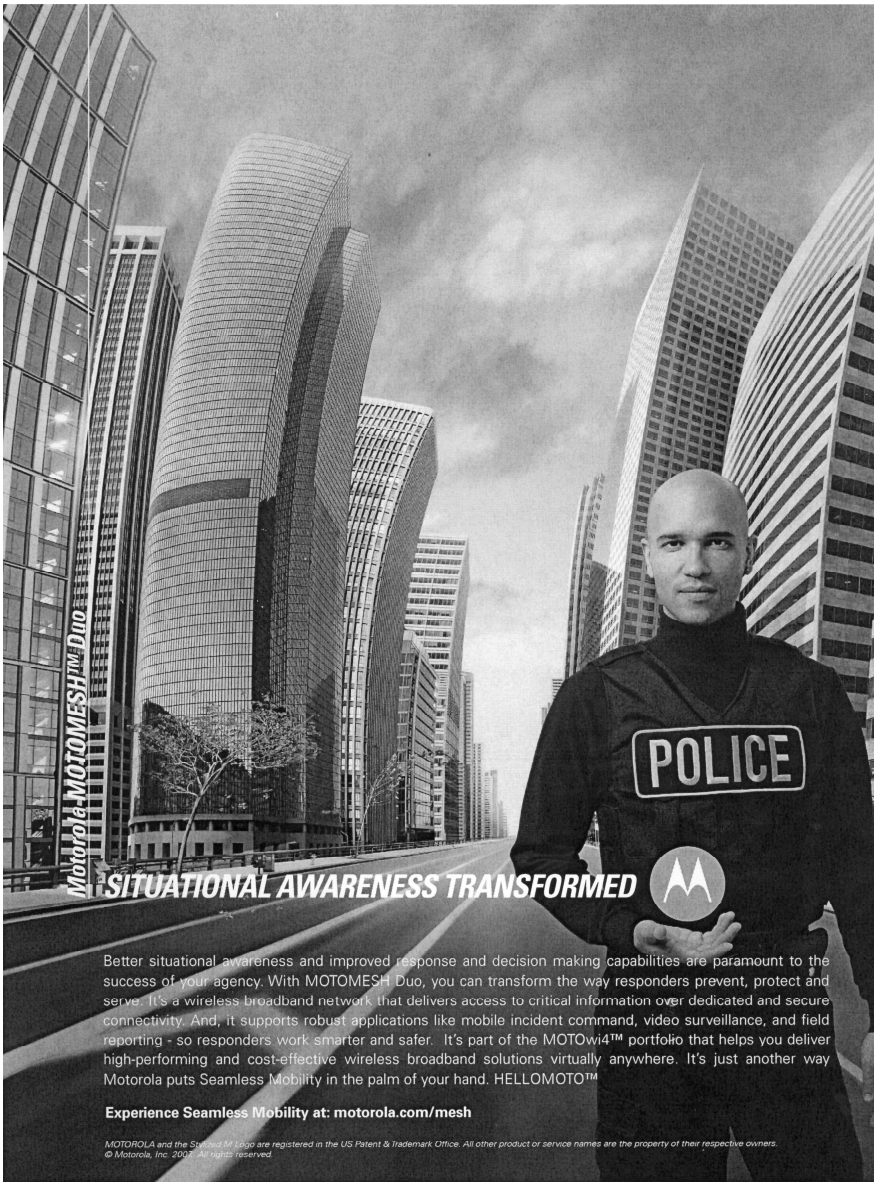
A ZRÍNYI MIKLÓS NEMZETVÉDELMI EGYETEM KIADVÁNYA

Kommunikáció 2007
Communications 2007

8



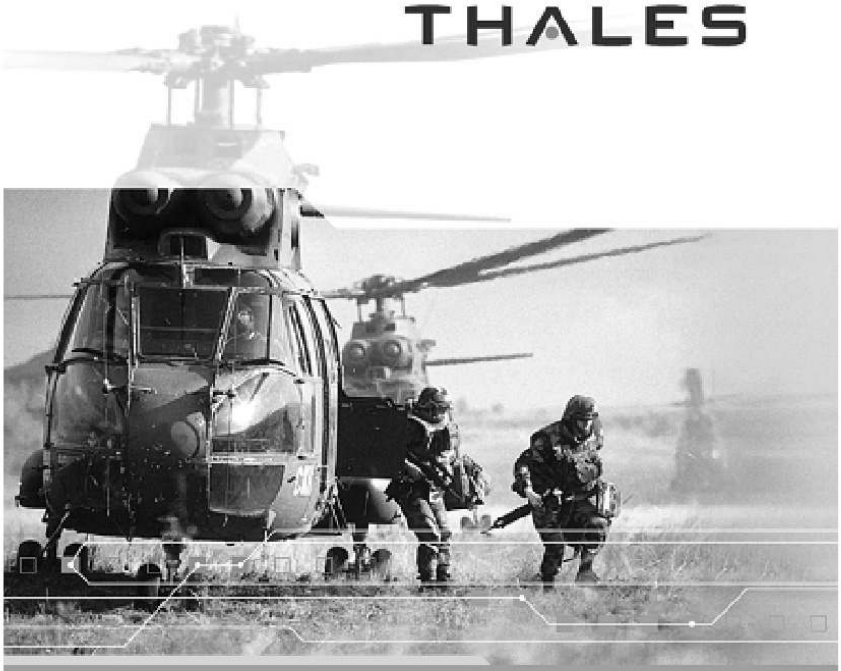
SITUATIONAL AWARENESS TRANSFORMED

Better situational awareness and improved response and decision making capabilities are paramount to the success of your agency. With MOTOMESH Duo, you can transform the way responders prevent, protect and serve. It's a wireless broadband network that delivers access to critical information over dedicated and secure connectivity. And, it supports robust applications like mobile incident command, video surveillance, and field reporting - so responders work smarter and safer. It's part of the MOTOwi4™ portfolio that helps you deliver high-performing and cost-effective wireless broadband solutions virtually anywhere. It's just another way Motorola puts Seamless Mobility in the palm of your hand. HELLOMOTO™

Experience Seamless Mobility at: motorola.com/mesh

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. 2007. All rights reserved.

THALES



Your partner for Land Systems

Securing your future

Zrínyi Miklós Nemzetvédelmi Egyetem
Budapest, 2007. október 16.

A tudományos kiadványt lektorálták:
Dr. habil. Sándor Miklós nyá. ezredes, egy. docens
Dr. habil. Rajnai Zoltán mk. alezredes, egy. docens
Dr. Fekete Károly mk. alezredes, egy. docens
Dr. Pándi Erik r. alezredes, egy. docens

Szerkesztette:
Dr. Fekete Károly mk. alezredes, egy. docens

Anyanyelvi lektor:
Fregan Beatrix

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

ISBN 978-963-7060-31-1

TARTALOMJEGYZÉK

BEVEZETŐ 14
SZABÓ András 16
HÁLÓZATI INCIDENS REAGÁLÓ KÉPESSÉG KIALAKÍTÁSA A MAGYAR HONVÉDSÉG ELEKTRONIKUS ADATKEZELŐ RENDSZERÉBEN 16
Gyula RÉVÉSZ 24
THE SIGNAL BATTALION OF THE HOME DEFENCE FORCES 43RD JÓZSEF NAGYSÁNDOR SIGNAL AND COMMAND SUPPORT REGIMENT 24
Levente DUDÁS, Péter KOVÁCS, Rudolf SELLER 28
PHASE CONTROLLED LINEAR TRANSMITTER ANTENNA SYSTEM 28
NÉMETH András 44
MOBILTELEFON HÁLÓZATOK ALKALMAZHATÓSÁGA A LAKOSSÁGI RIASZTÁS ÉS TÁJÉKOZTATÁS RENDSZERÉBEN 44
HÓKA Miklós 54
AZ ÖSSZHADERŐNEMI HARCÁSZATI RÁDIÓRENDSZER FEJLESZTÉSE 54
KASSAI Károly 66
AZ ELEKTRONIKUS ADATKEZELÉSSEL KAPCSOLATOS KOCKÁZATOK KEZELÉSÉNEK EGYES KÉRDÉSEI 66
RAJNAI Zoltán, KERTI András 72
AZ INFORMÁCIÓVÉDELMI SZAKÁLLOMÁNY TOVÁBBKÉPZÉSI RENDSZERE 72
Erik Pándi 78
MODERNISATION PROCESS OF PUBLIC ADMINISTRATION SERVICES 78
NÉMETH András 86
SZOLGÁLTATÁSALAPÚ MŰHOLDAS HÍRKÖZLÉS VESZÉLYHELYZETI FELHASZNÁLÁSI LEHETŐSÉGEI 86
Andras KERTI, Dr. Zoltan RAJNAI 104
INTERNETTERRORISME 104
Farkas Tibor 108
A BLACKBERRY RENDSZER 108
MEDVECZKI Zoltán 115
AZ ORRLÉGZÉS MÉRÉSI MÓDSZEREI 115

Dobák Imre 131
COMMUNICATIONS-GEOGRAPHY - SHORT OVERVIEW OF THE SITUATION OF THE PUBLIC SAFETY COMMUNICATIONS NETWORKS IN THE CENTRAL-EASTERN EUROPEAN COUNTRIES 131
Tibor FARKAS 139
INFORMATIC NETWORK MANAGEMENT IN THE HUNGARIAN DEFENCE FORCES 139
Erika Kucsera Magyarné 145
NEW POSSIBILITIES OF WIRELESS TRENDS IN THE AREA OF MOBILE INFOCOMMUNICATION AND MANAGEMENT 145
NÉMETH András 153
TÁVLATI MŰHOLDAS MEGOLDÁSOK A KATASZTRÓFAVÉDELMI KOMMUNIKÁCIÓ TERÜLETÉN 153
Zoltán MEDVECZKI 161
METHODOLOGICAL MEASUREMENT OF NASAL AIRWAY 161
PÁNDI Balázs 179
A TÁBORI ALAPHÍRHÁLÓZAT ERŐFORRÁSAINAK MODELLEZÉSE 179
TAKÁCS Péter 187
A WIFI HÁLÓZATOK ESETLEGES KATONAI FELHASZNÁLÁSÁNAK LEHETŐSÉGEI 187
Sebestyén Attila 203
CSÖKKENTHETŐ-E A „SUPERUSER”-EL KAPCSOLATOS BIZTONSÁGI KOCKÁZAT? 203
RÉVÉSZ Gyula 213
MISSZIÓS HÍRADÓ FELKÉSZÍTÉS SOKSZÍNŰSÉGE 213
Erik PÁNDI, Attila TAKÁCS 219
UNION SUPERVISION OF THE REGULATORY SYSTEM OF ELECTRONIC INFORMATION 219
CZAP László, ZÖMBIK László 227
ADAPTÍV, ELOSZTOTT DÖNTÉSHOZÁS KÜSZÖBKRIPTOGRÁFIÁVAL 227
Erik PÁNDI, Balázs PÁNDI 235
STRUCTURAL CHANGES AMONG DOMESTIC CLOSED-PURPOSE NETWORKS 235
Peter TAKÁCS 243
POSSIBLE WIRELESS NETWOKS ON THE BATTLEFIELD 243
Attila BLEIER, Zoltán RAJNAI 247
OPTIMIZATION OF A TRANSMISSION NETWORK 247

József MÁTÉ 269
STATUS OF IMPLEMENTATION OF THE MONITORING AND PUBLIC WARNING 269
Beatrix FREGAN 279
CERTAINS ACTEURS DU NOUVEL ENVIRONNEMENT MONDIAL 279
KOZÁK Piroska 284
FÉSÜLETLEN GONDOLATOK A FŐISKOLAI KÉPZÉS ÜRÜGYÉN 284
SCI-Network Távközlési és Hálózatintegrációs zRt. 294
CERAGON PONT PONT ÖSSZEKÖTTETÉSEK - NAGYSEBESSÉGŰ IP ÉS INFORMÁCIÓ VÉDELEM A LEVEGŐBEN 294
KOPINT DATORG 300
CÉGISMERTETŐ 300
Alcatel-Lucent 314
WIMAX & ARMY MOBILE INFRASTRUCTURE 314
ANTÓK Péter 328
HÁZIG VEZETETT FÉNY 328
KOPINT DATORG 346
PROFESSZIONÁLIS SZOLGÁLTATÁSOK A KR-EN 346
CZIROK Ferenc 356
TESTRESZABÁS 356
Gabor EGRI 376
INTEGRATION OF THE SCHENGEN INFORMATION SYSTEM IN HUNGARY 376
FERCOM Kommunikációs Kft. 390
MOTOMESH SOLO ÁTTEKINTÉS 390
Hungaro DigiTel Kft. 404
MŰHOLDAS MEGOLDÁSOK AZ ÁLLAMI SZERVEK TÁVKÖZLÉSI IGÉNYEINEK KISZOLGÁLÁSÁRA 404
MÁTÉ József 414
A KATASZTRÓFAVÉDELEM 2007. ÉVI FŐ PROJEKTJEI 414
MÉSZÁROS Árpád 428
TÁVKÖZLÉSI NEHÉZSÉGEKRŐL A MADÁRINFLUENZA ÜRÜGYÉN 428
SEBESTYÉN Attila 440
CSÖKKENTHETŐ-E A SZUPERUSEREKKEL KAPCSOLATOS BIZTONSÁGI KOCKÁZAT? 440

SÍK Zoltán Nándor 444
AZ INFORMÁCIÓS HADVISELÉS ÉS A KRITIKUS INFRASTRUKTÚRÁK VÉDELME 444
TESSEDIK Tamás 458
VESZÉLYHELYZETI KOMMUNIKÁCIÓ 458
SPRINGEL János 464
DIGITÁLIS ALÁÍRÁS ÉS HITELES ARCHIVÁLÁS EGYES KÉRDÉSEI 464

A nemzetközi szakmai tudományos konferencia kommunikációs partnere:

A tudományos konferencia támogatói:

	Alcatel-Lucent Hungary Ltd.
	THALES COMMUNICATIONS
	Fercom Kommunikációs Kft.
	Magyar Villamos Művek ZRt.
	Hungaro DigiTel Kft.
	Határőrség Országos Parancsnoksága
	KOPINT-DATORG Infokommunikációs ZRt.
	Országos Katasztrófavédelmi Főigazgatóság
	SCI-Network Távközlési és Hálózatintegrációs zRt.
	SIEMENS ZRt.

A rovidfilmek felolvasása a hátoldalon 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.: (00-1) 353 1027 Fax.: (00-1) 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. Maradi István, T-Mobile Rt. Dr. Pap László, Budapesti Műszaki és Gazdaságtudományi Egyetem
Főtitkár	Horváth Pál, Actel Kft.
Főtitkár-helyettesek	Ágoston György Dr. Kántor Csaba, Magyar Telekom Rt. Dr. Tormási György, Antenna Hungária Rt.
További Intéző-bizottsági tagok	Dr. Cinkler Tibor, Budapesti Műszaki és Gazdaságtudományi Egyetem Bölcskei Imre, Magyar Telekom Rt. Duró Imre, HUNSAT Rt. Dr. Kolláth Gábor, Ericsson Magyarország Kft. Marchhart Pál, Vodafone Rt. Vágujhelyi Ferenc, SzilCom Kft.
Ellenőrző bizottsági elnök	Halmi Gábor, Műszaki és Természettudományi Egyesületek Szövetsége
Ellenőrző bizottsági tagok	Kubinyi Imre, Edusys Rt. Dr. Szecsődi Istvánné, EMITEL Rt.
Etikai bizottság elnök	Dr. Gosztony Géza, Pázmány Péter Katolikus Egyetem
Etikai bizottsági tagok	Csikász István 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. Bárányné Dr. Sülle Gabriella, T-Mobile Rt. Dr. Géher Károly, Budapesti Műszaki és Gazdaságtudományi Egyetem Fáy András, Nokia Magyarország Kft. Dr. Halász Edit, Budapesti Műszaki és Gazdaságtudományi Egyetem Halász Miklós, Hungarotel Rt. Hazay István, HUNSAT Rt. Dr. Henk Tamás, Budapesti Műszaki és Gazdaságtudományi Egyetem Dr. Horváth László, Puskás Tivadar Távközlési Technikum Jambrik Mihály, Informatikai és Hírközlési Minisztérium Dr. Lajtha György 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

A NEMZETKÖZI KONFERENCIA HÁTTÉR INFORMÁCIÓI

A konferencia fővédnöke:
Mikita János mk. altábornagy, MH Honvédvezérkar vezérkar főnök helyettes

A konferencia védnökei:
Prof. Dr. Szabó János dandártábornok, ZMNE rektor
Horváth Ferenc dandártábornok, MH Támogató Dandár parancsnok

A konferencia kommunikációs partnere:
T-Systems

A konferencia támogatói:
ALCATEL-LUCENT Hungary Kft.
Thales Communications
Magyar Villamos Művek ZRt.
FERCOM Kommunikációs Kft.
Határőrség Országos Parancsnoksága
KOPINT-DATORG Infokommunikációs ZRt.
Országos Katasztrófavédelmi Parancsnokság
SCI-Network Távközlési és Hálózatintegrációs ZRt.
Hungaro DigiTel Kft.
SIEMENS ZRt.

A konferencia rendezői:
Zrínyi Miklós Nemzetvédelmi Egyetem Híradó Tanszék
Hírközlési és Informatikai Tudományos Egyesület ZMNE Egyetemi Csoport

A szervező bizottság elnöke:
Dr. habil. Rajnai Zoltán mk. alezredes

A szervező bizottság titkára:
Dr. Fekete Károly mk. alezredes

A szervező bizottság tagjai:
Dr. habil. Sándor Miklós ezredes
Dr. Pándi Erik r. alezredes
Dr. Hóka Miklós alezredes
Szöllősi Sándor okl. mk. őrnagy

BEVEZETŐ

Ön a Kommunikáció 2007. (Communications 2007) tudományos kiadvány könyv változatát olvassa.

A Zrínyi Miklós Nemzetvédelmi Egyetem Híradó Tanszéke által szervezett rendezvény idén nyolcadik alkalommal kerül megrendezésre, amelylyel egyik nem titkolt szándékunkat és célunkat szeretnénk elérni, nevezetesen azt, hogy a honvédelmi, rendvédelmi, nemzetbiztonsági, illetőleg közigazgatási ágazat – *vagyis lényegében az állami szféra* – és a magánszektor képviselői számára ismételten olyan konzultációs lehetőséget biztosítsunk, amely kölcsönösen elősegítheti a távközlési, telekommunikációs, valamint információ-technológiai infrastruktúrák magas szintű alkalmazásának további elterjesztését és a korszerű elektronikus szolgáltatások mindennapjainkba való bevezetését.

A Magyar Információs Társadalom Stratégia felvázolja (vizionálja) az eMagyarország tudatos megvalósítását, amelyben az állami szektor szereplőinek kiemelt felelőssége van, hiszen hazánknak a tudásalapú társadalmi modell kialakításában vállalt elkötelezettsége Európai Uniós csatlakozásunkkal erősödött. Tisztában vagyunk ugyanakkor azzal, hogy e kitüntetett szerep betöltéséhez elengedhetetlen a magánszektor tudásbázisának alkotó módon történő felhasználása, ami egyúttal alapja lehet a helyes gyakorlatok kifejlesztésének és alkalmazásának is.

A konferencián elhangzó előadások, illetőleg a kiadványban bemutatásra kerülő publikációk reményeink szerint – *e tárgykörben* – elősegítik az állami- és a magánszektor közötti sikeres interakciót, amelynek elmélyítését jelen könyvünk mellett a kiadvány elektronikus változatának – *bár korlátozott példányszámban történő* – terjesztésével is szolgálni kívánjuk.

A szervező bizottság

SZABÓ András

HÁLÓZATI INCIDENS REAGÁLÓ KÉPESSÉG KIALAKÍTÁSA A MAGYAR HONVÉDSÉG ELEKTRONIKUS ADATKEZELŐ RENDSZERÉBEN

2006.01.17, Kedd - Forrás: MTI
Őrizetbe vettek egy spanyol hackert, mert az interneten behatolt az amerikai haditengerészet nukleáris meghajtású tengeralattjárók karbantartását végző műhelyének egyik számítógépébe[1].

2007. március 1, Csütörtök - Forrás: MTI
Egy görög sorkatona a hadsereg háború esetére kidolgozott mozgósítási terveiről szóló titkos dokumentációkat töltötte fel egy internetes fájlmegosztó honlapra[2].

2007. június 7, Csütörtök - Forrás: MTI
Andrus Ansip észt kormányfő a Kremlt vádolja az észt intézmények ellen végrehajtott kibertámadások okán[3].

Biztonsági incidensek száma világszerte

Mai nap	850 222
Előző 7 nap	392 025 141
Összesen:	18,068,375,310

Megtámadott IP-k száma

Mai nap	65,271
Előző 7 nap	11,169,677
Összesen:	465,885,880

1.ábra. A Symantec DeepSight Analizátorának mérése[4]

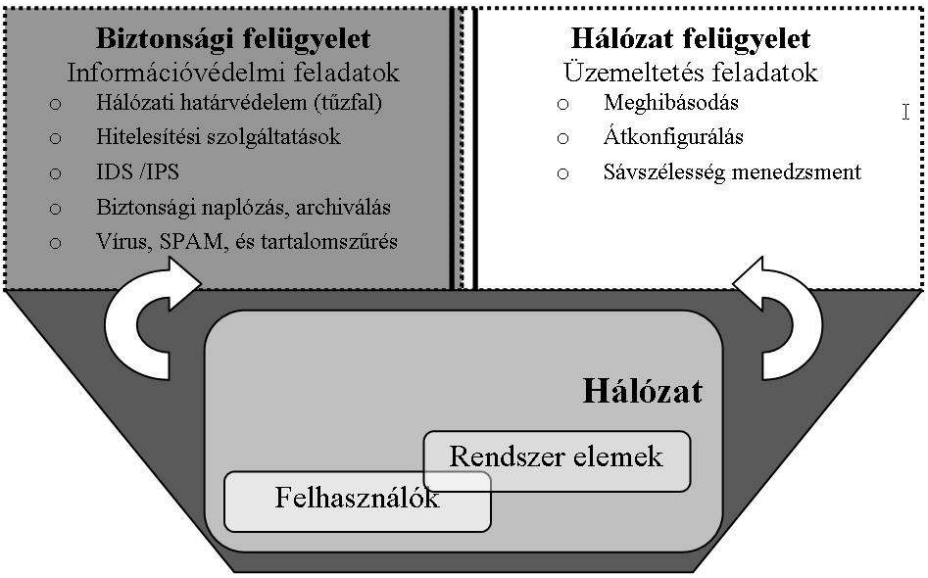
A fenti példák bizonyítják, hogy az informatikai és a távközlési infrastruktúra a bűnözés új formái előtt nyitja meg az utat. A számítógépes bűnözés (EU terminológiában Cybercrime) jellemzője, hogy a számítógép segítségével elkövetett bűncselekmény nyomai nem kézzelfoghatóak, továbbá, hogy a földrajzi határok nem korlátozzák.

1 http://www.mti.hu
2 http://www.mti.hu
3 http://www.mti.hu
4 Mérés időpontja: 2007. 09. 26 Forrás: https://analyzer.symantec.com/

Az illetéktelen rendszerhozzáférések, biztonsági incidensek növekvő tendenciát mutatnak, mely hatására felmerült az igény azok megakadályozását, felderítését és elemzését végző szakértő csoportok felállítására.

A NATO koncepciója, egy centralizált technikai és jogszabályi támogatás a biztonsági incidensek lokális kezeléséhez.5 A Centralizált szolgáltatások a preventív intézkedések (konferenciák, sérülékenység vizsgálatok), a felügyeleti tevékenységek (IDS/IPS6, incidenskezelő képesség), és a jogszabályi támogatás (Biztonsági házirend frissítések, nyomozási direktívák, vészhelyzeti tervek) összessége. A lokális incidenskezelést központi adatbázissal (tudástárral) támogatja.

A Magyar Honvédség decentralizált elektronikus adatkezelő hálózat hálózatvédelmének kialakításához szükséges képességek, közé tartozik a biztonsági incidensek gyanúját kivizsgáló erők és eszközök alkalmazása.



2. ábra. A Felügyelet tevékenység alapú szeparálása

A hálózatvédelem két részre osztható. Az üzemeltető, és üzemben tartó szerv feladata a biztonsági elvek, szabályok kidolgozása, technikai eszközök üzemeltetése és a felhasználók tevékenységének ellenőrzése. A felhasználók feladata pedig a kidolgozott biztonsági elvek betartása, a biztonság tudatos fenntartása.

5 Suleyman Anil Head, NCIRC Coordination Centre - NCIRC (NATO Computer Incident Response Capability) előadásanyag TF-CSIRT Meeting

6 Intrusion Detection System – behatolás jelző rendszer, Intrusion Prevention System (IPS) - behatolást megakadályozó rendszer

Biztonsági fenyegetésekkel és sebezhetőségekkel az elektronikus adatkezelő rendszerek üzemeltetésének teljes ciklusa során számolnunk kell, szükséges egy hatékonyan működő, a biztonsági incidenseket kivizsgáló és kezelő funkció kialakítása a szervezeten belül.

A kialakítás előtt (tervezés fázisában) meg kell határozni az incidenskezelő szervezet (CIRC7, CSIRT8 vagy CERT9) célját, funkcióját, továbbá gondoskodni kell a funkciók jelenlegi szervezeti struktúrába történő integrálásáról (ez alatt a hatékony szervezeten belüli információáramlást, a magas fokú együttműködő képességet értem).

A hatékony működés feltétele, hogy rendelkezésre álljon a szükséges költségvetés, személyi és technikai háttér, továbbá a munkához szükséges jogosultságok („need to know" elv).

A hálózat biztonsági funkciói nem korlátozhatják a rendelkezésre állást, az elektronikus információk időbeni felhasználását. Ezt az elvet szem előtt tartva a kialakított biztonsági funkció a vezetés szintjeinek megfelelően tagoltan helyezendő a fennálló szervezeti struktúrában.

A veszélyforrások csoportosíthatóak:

- Környezeti veszélyekre (fizikai védelem hiánya)
- Fizikai veszélyekre (eltulajdonítás, rongálás)
- Informatikai veszélyek (vírus, spyware, rootkit)
- Humán veszély (gondatlanság, elbocsátott alkalmazott, szabotázs)
- Szervezeti veszélyek (dokumentáltság hiányos, elavult szabályzók,
- rossz szervezeti kommunikáció)

A Biztonsági felügyelet elsődleges feladata, a kommunikáció bizalmasságának, sértetlenségének és a folytonos rendelkezésre állásának biztosítása10. Képes továbbá e biztonsági funkciókat akadályozó tevékenységek felderítésére, detektálásra, ellentevékenység folytatására.

Figyelembe véve a CIRC tevékenységét (a különböző csatornákon, adathordozókon beáramló, nagy mennyiségű információ elemzése), a hierarchizált kialakítás lehetővé teszi az erőforrások hatékony kihasználását. Hiszen egy centralizált elemző funkció esetén a rendszerinformációk (.log file-ok, hibaüzenetek) túlterhelnék a hálózat átviteli és tároló kapacitá-

7 A NATO terminológiában: Computer Incident Response Capability (CIRC)

8 A www.cert.org terminológiájában: Computer Security Incident Response Team (CSIRT)

9 Az U.S. DARPA terminológiában: Computer Emergency Response Team (CERT) kialakítása 1988 Novemberében kezdődött.

10 CIA követelmények: Confidentiality, Integrity, Availability

sát. A rendszer tárhely kapacitását feleslegesen terhelő információk szűrésével ugyancsak tehermentesíthető a rendszer.

Nem elég naplózni, fontos a naplók havi rendszerességgel történő elemzése, esetleg automatikus riasztási rendszer kialakítása, mely az első lépcsőfok az IDS11 felé.

A napló file-ok archiválása a későbbi elemzések, tendenciák kiértékelése és bizonyítékszolgáltatás céljából végzendő.

A különböző szintű incidenselemző, -értékelő és reagáló (CERT, CIRC) csoportok hatáskörüknek megfelelően dolgoznak, és csak a hatáskörükön túl mutató feladatokat, továbbá a tevékenységüket összefoglaló jelentéseket (koordinációs céllal) adják tovább az elöljáró szervnek.

A CIRC feladatai közé tartozik, a biztonsági tanácsadó, incidens reagáló tevékenység a szervezet hálózatán belül, és kívül (távoli felhasználó, Web portál).

Ennek folytán egyfajta analizáló, értékelő csoportot is ki kell alakítani, mely feladata az újonnan felfedezett sérülékenységek felmérése, rendszerezése, elhárítása.

A CIRC képesség több szinten hierarchizált szervezeti és technikai egységek összessége. Ezért fontos a megfelelő kapcsolati rendszer, az információ gyors, megbízható áramlása a szervezeten belül (jelentési rend) és a szervezeten kívülre (Nemzeti CERC, NATO CIRC, EU hálózat biztonsági szervezetek, ISP12-k).

A hálózat kiépítése, üzemeltetése és fejlesztése során az alábbi feladatokat látja el a biztonsági felügyelet (CIRC egysége).

A CIRC feladatkörei

- Rendszerdokumentáció
- Kockázatelemzés (sebezhetőségek, fenyegetések valószínűségének felmérése,

Támadási fa készítése[13])

- Rendszer felülvizsgálat
- Sérülékenység teszt[14]
- Vészhelyzeti terv kidolgozása
- Biztonsági felügyeleti rendszer kialakítása (ellenőrzés, incidenskezelés)

---

11 Intrusion Detection System – behatolás jelző rendszer

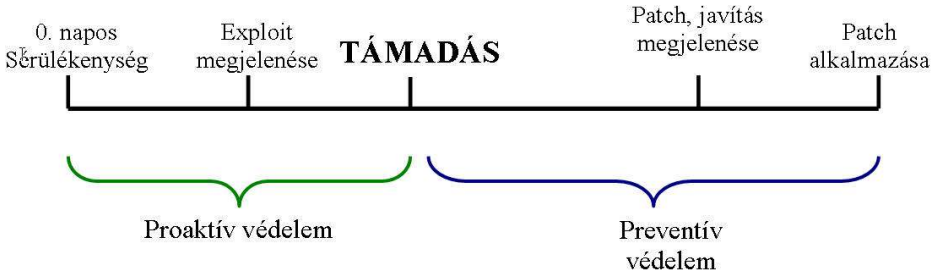
12 Internet Service Provider jelentése: Internet szolgáltató

13 Forrás: Attack Modeling for Information Security and Survivability Andrew P. Moore, Robert J. Ellison, Richard C. Linger

14 Penetration test, a számítógépes hálózat biztonságát felmérő csapat (u.n. tiger team) által végzett tevékenység

- Információvédelmi adatbázis kialakítása[15], frissítése (dokumentumtár,
- oktatóanyag tár - pl.: oktatófilmek, rövid, pontokba szedett szabályok, Howtok, hírek)
- Természeti (tűz, víz, por) és véletlenszerű károk (szoftverhiba, felhasználói mulasztás) kezelése
- Adatmentés és visszaállítás
- Bizonyítékszolgáltatás
- Maradvány elektromágnesesség problémájának kezelése[16]

A távdiagnosztikai eszközökkel végzett technikai ellenőrzés a proaktív védelem fontos lépcsőfoka, melyet a támadás megindítása után a preventív védekezés követ. Egy biztonsági rés életútját mutatja a következő ábra. A Felügyeletei szervek legfontosabb teendője, a szoftver gyártokkal való folyamatos, megbiztató kapcsolat fenntartása, a frissítések nyomon követése.



3. ábra. Egy támadás forgatókönyve

Biztonsági felügyelet technikai rendszere (Incidensdetektáló képességek)

- Azonosító mechanizmusok felügyelete (sorozatos hibás bejelentkezések kivizsgálása)
- Biztonsági naplók elemzése (tisztázatlan naplóbejegyzés esetén riasztás)
- Hálózati alkalmazások felügyelete (pl.:Portok szkennelése17)
- Tűzfalak, routerek konfigurációjának felügyelete
- IDS/IPS 18

15 Network and Information Security:Proposal for A European Policy Approach

16 Az üzemeltetésből kivont minősített adattároló (RAM, ROM, HDD), adatkezelő eszközök csak a visszamaradó információk törlése (declassification) után minősíthetőek vissza.

17 Programok: Etherreal, Fscan, nmapwin, Nmap

18 Intrusion Detection System (IDS)az aktív, és Intrusion Prevention System (IPS) a passzív védelem kialakításához.

- Hálózati behatolások ellenőrzés
- On-line frissítések

Eljárásrend biztonsági incidens gyanúja esetén

1. Riasztás
2. Elemzés (online vagy offline)
3. Incidensreagálás
4. Értékelés
5. Jelentés, bizonyítékszolgáltatás

A riasztás forrásai a biztonsági alkalmazások (operációs rendszer, tűzfal, IDS, IPS, forgalomelemző szoftverek, vírusvédelemi alkalmazások, autentikációs mechanizmusok) .log file-ai. A biztonsági incidens gyanújának személyes vagy szervezet útján történő bejelentése egy előre elkészített formanyomtatvány segítségével történik, mely tartalmazza a legfontosabb tudnivalókat, tapasztalatokat. Így az incidens jellege gyorsabban és könnyebben határolható be.

A riasztási rendnek megfelelően a szükséges szakemberek (szerver szakértő, tűzfal, switch, router szakértő, operációs rendszer szakértő, alkalmazás szakértő) bevonásával kezdődik a biztonsági incidens elemzése. Az elemzés során talált bizonyítékokból kiindulva felmérhető a sérülékenység, a támadás típusa (felhasználva a saját adatbázist, együttműködők tudásanyagát, más forrásokat[19]), az okozott kár és a kárkezelés módja.

Az elemzés történhet a hálózati eszköz leválasztásával és kiértékelésével (off-line elemzés), vagy esetenként a hálózati forgalom figyelésével (on-line elemzés).

Forgalom elemzés során figyelni kell:

- „Legnagyobb forgalmúak (kimenet)
- Legnagyobb forgalmúak (bemenet)
- Leginkább használt portok és protokollok
- Összehasonlítás ismert és valós forgalommal
- Koordináció / korreláció az igazságügyi vizsgálattal”[20]

A kiértékelés után az újonnan felfedezett sérülékenységek, hiányosságok figyelembevételével módosítani kell a hálózati konfigurációkat, frissíteni az alkalmazásokat, és adott esetben a biztonsági házirendet.

19 Sebezhetőség adatbázisok (pl.: CVE, ICAT sebezhetőség adatbázis, SECUNIA adatbázis, BUGTRAQ, vírusadatbázisok) továbbá a különböző országok CERT szervezeteinek (pl.:HUN CERT) adatbázisa

20 Forrás : Windows Forensics: A Case Study

Az elemzés módja:

Hoszt oldali elemzés

A munkaállomás hálózattól szeparált vizsgálata

- Memória, HDD elemzése
- Operációs rendszer elemzése [21]
- Szoftverek elemzése (pl.: böngésző[22] előzmények)

A munkaállomás vizsgálata hálózatra kötve

Szerver oldali elemzés:

- A hálózati forgalom on-line vagy off-line vizsgálata

Egyéb elemzés:

- optikai adathordozók elemzése
- flash memóriák elemzése
- nyomtatók elemzése

A virtuális bizonyítékok (Operációs rendszer, biztonsági alkalmazások adatai) mellett a megfelelő műveleti szervnek szükséges nyílt és titkos információgyűjtési módszerek útján a fizikális bizonyítékokat (helyszíni szemle, ujjlenyomat, külsérelmi nyomok, kihallgatások, megfigyelés) összegyűjteni, melyekkel kiegészülve hatékonyabbá válik az incidensreagálás, kárelhárítás. A hatékony munka érdekében szoros együttműködés szükséges azon szervezeti elemekkel, melyek rendelkeznek a nyílt és titkos információgyűjtés eszközeivel és módszereivel, továbbá hatáskörébe tartozik e tevékenység végrehajtása.

A reagálás alapját az előre kidolgozott Vészhelyzeti terv képezi. A CIRC tervezése során szükséges meghatározni a jelentés rendjét (mely a Need to Know elvre épül) az előjárok felé, továbbá a kapcsolattartás formáját (heti jelentés kivonatának megosztása, konferenciák, tájékoztatás sérülékenységekről, vírushíradó) az együttműködőkkel, más kormányzati, NATO és EU hálózatvédelmi szervekkel.

Számítógépes bűncselekmények kivizsgálása során rögzíteni kell az elektronikus és fizikális nyomokat, bizonyítékokat, detektálni a sebezhetőségeket, nyomon követni az információáramlást.

Ezen feladatokra hálózati forgalomelemző, adatmentő,- rögzítő szoftvereket, és különböző mérőeszközöket kell alkalmazni. Megbízható forrású és hiteles eszközök alkalmazhatók csak erre a feladatra.

Az adatok (dokumentumok, log file-ok, archivált adatok, backup-ok), szoftverek és frissítések sértetlenségét ellenőrző alkalmazások23 (hash ellenőrző alkalmazások) használata szükséges.

---

21 A .lnk file-ok az előzmények mappában mutathat egy már nem létező file-ra, vagy cserélhető lemezre. Elemzésnél link, cache, cookie, history, Temp file-ok ellenőrizendők)

22 cookie-k megjelenítése pl.: a CookieView programmal http://www.digital-detective.co.uk/

Összefoglalás

A napjainkra kialakult biztonsági fenyegetések komoly kihívások elé állítják mind a kormányzati, mind a civil szféra informatikai infrastruktúráját.

A sérülékenységek (szoftver hibák) és fenyegetettségek (vírus, spyware, rootkit) okozta károk mértéke jelentősen csökkenthető megfelelő rendszabályok életbe léptetésével.

A kor színvonalának megfelelő biztonsági felügyelet számos szegmensből áll. A nyílt (más hálózatok, Internet), valamint a lokális irányokra kiterjedő, integrált hálózatvédelmi (technikai és szabályzó) eljárásokat kell kialakítani, melynek egyik fontos eleme az incidens menedzsment. A hatékonyan működő CIRC a biztonsági intézkedések visszacsatolásaként működik.

Zárásként meg szeretném azt jegyezni, hogy amíg a biztonságot tévesen, mint technikai eszközökkel elérhető állapotként értelmezik, addig nem fogják elérni azt, hiszen a biztonság koncepcióváltást igényel. A biztonsági rendszabályok betartását nem teherként, hanem mindennapi rutinként kell megélni.

Bibliográfia:

[1] Attack Modeling for Information Security and Survivability Andrew P. Moore, Robert J. Ellison, Richard C. Linger, March 2001

[2] Cyber crime investigator's field guide Bruce Middleton 2002, CRC Press LLC

[3] http://www.securityfocus.com/infocus/1653 (Windows Forensics: A Case Study, Part One, December 31, 2002),

[4] http://www.securityfocus.com/infocus/1672 (Windows Forensics: A Case Study, Part Two, March 5, 2003) by Stephen Barish

[5] Hatósági eljáráshoz szükséges bizonyítékok gyűjtése - http://www.cert.hu/dmdocuments/Windows_forensics.pdf

[6] Incidenskezelő rendszerek (Összehasonlító elemzés) - Ficsor Péter 2005

[7] Network and Information Security:Proposal for A European Policy Approach

[8] Forrás: http://ec.europa.eu/information_society/eeurope/2002/news_library/pdf_files/netsec_en.pdf

[9] Suleyman Anil Head, NCIRC Coordination Centre - NCIRC (NATO Computer Incident Response Capability) előadásanyag TF-CSIRT Meeting

[10]

23 Pl.: integritás ellenőrző program md5sum.exe

Gyula RÉVÉSZ

THE SIGNAL BATTALION OF THE HOME DEFENCE FORCES 43RD JÓZSEF NAGYSÁNDOR SIGNAL AND COMMAND SUPPORT REGIMENT

In this paper, I intend to introduce the Signal Battalion of the Home Defence Forces 43rd József Nagysándor Signal and Command Support Regiment. By introducing this subunit, I would like to give the reader a brief overview of the predecessor organizations of the regiment, the structure of both the regiment and its Signal Battalion (SIGBAT), the present tasks the SIGBAT and its subunits face and the future plans to make the SIGBAT more effective in implementing its fundamental tasks.

I. History of the regiment

The predecessor of the Home Defence Forces 43rd József Nagysándor Signal and Command Support Regiment (HDF 43. JN SCSR), the HDF 101st Motorized Signal Regiment was established on March 15, 1949. In 1951, it was renamed to HDF 43rd Detached Signal Regiment. In 1962, the regiment was dislocated from Vác to the József Nagysándor Barrack, in Székesfehérvár. On March 15, 1991, a regimental standard was given to the regiment by the Minister of Defence.

Due to the reorganisation of the Hungarian Defence Forces, the regiment has been transformed into the HDF 43rd József Nagysándor Signal Battalion in 2000.

The predecessor of the HDF 5th Alba Regia Command Support Battalion was the 5th Army Commandant Service subordinated the 5th Army Command. It was established in the Petőfi Barrack in Budapest garrison on August 1, 1961.

In December 1963, the regiment was dislocated to the Alba Regia Barrack, in Székesfehérvár.

In 1967, the unit was renamed to HDF 5th Army Military Police and Commandant Battalion. In 1969, the unit became a regiment, the HDF 5th Army Military Police and Commandant Regiment. In 1989, the unit was renamed to Alba Regia Detached Military Police and Commandant Regiment. From November 1, 2002 till its dissolution, the unit was called HDF 5th Alba Regia Command Support Battalion.

The HDF 43rd Command Support Battalion was established by merging the HDF 43rd Signal Battalion and the HDF 5th Alba Regia Command Support Battalion by the Minister of Defence on May 28, 2004.

In the next phase of the structural reorginisation of the Hungarian Home Defence Forces of 2007, the unit was expanded. Due to the establishment of the HDF Joint Forces Command, the tasks of the HDF 43. Command Support Battalion increased, which also meant an increase in the strength of the battalion. Therefore, the HDF 43rd József Nagysándor Signal and Command Support Regiment was established by the Minister of Defence on the 1st of January 2007.

II. Mission of the regiment

The main mission of the regiment is to support the Joint Forces Command in every aspect. Additional tasks also include:

- Meeting the obligations arising from international treaties;
- Forging the subunits together, preparing the staff and the subordinate units for more effective cooperation; providing the preconditions for the subunits and sections to be capable of reaching higher operational readiness;
- The maintenance and the preservation of the equipment and the vehicles;
- Maintaining the combat readiness of the equipment and the vehicles;
- Ensuring the possibility of the mobilization of both the HDF Joint Forces Command and the subunits of the regiment;
- The peacetime and wartime command, signal, information technology and information security support of the HDF Joint Forces Command;
- Executing the necessary technical servicing tasks, and maintenance works, technical condition controls;
- Conducting reparations under the supervision of the HDF Land Forces Command; repairing on the spot with repair teams.

II. a. Structure

In the structure of the regiment six battalion-sized subunits and a one company can be found.

The executive subunits are the following:

- Signal Battalion
- Dunántúli (Transdanubian) Main Communications Center
- Alföldi (Great Plain) Main Communications Centre
- Joint Forces Information Technology Centre
- Garrision Support Command
- Logistics Battalion
- Guard Company

III. Signal Battalion

The SIGBAT was established on January 1, 2007 from the Signal Company (SIGCOY) of the HDF 43rd Command Support Battalion. With the establishment of the HDF Joint Forces Command, it has become inevitable to increase the number of the executing subunits of the regiment. New important tasks have been assigned to the regiment, which meant the imminent need to extend the range of tasks of the Signal Company.

Besides the former SIGCOY, additional subunits have been added to the SIGBAT.

III. a. Structure

The Signal Battalion is made up of the following subunits:

- battalion staff,
- 1x signal company,
- 1x information security section,
- 1x security and monitoring department,
- 1x event support section.
- The respective parts have their own well-defined responsibilities.

III. b. Battalion command staff

The battalion is lead by a small command staff. The commander, his deputy and the command sergeant major can be found in the command group. They are assisted by a small staff led by the Chief of Staff. Certain functional areas of the staff are grouped in order to make the staff work more efficient. The Personnel (S1) and Administration affairs are handled at regiment level under the direction of the chief of Personnel and Administration Department.

S4 (Logistics) is coordinated by an officer, while S3 (Operations) and S7 (Training) issues are covered by an officer and a non-commissioned officer. S3, S4, S7 affairs are under the close supervision of the Chief of Staff.

III. c. Signal Company

The signal company is responsible for the wired and wireless field communication of the Joint Forces Command. It is capable of setting up and operating four field communication centers. The company can provide the communication assets for the Main Headquarters of the HDF Joint Forces Command. Though, it is still equipped with the old Soviet analogue signal equipment, the company can provide the HDF Joint Forces Command and the regiment with secure, reliable and continuous communication service. The communications equipment the company has are the following:

- R-1406 radio relay station
- KHK-12 mobile communications centre
- R-142 radio station
- R-159 radio

Additional tasks may also include:

- organizing special signal training for the signal soldiers of other units from the Hungarian Defence Forces
- filling signal assignments in the Hungarian contingents deployed abroad

III. d. Information security section

This section's mission is to ensure the secure voice and data communication of the regiment and the HDF Joint Forces Command. The section has its own special encrypting and decrypting devices.

III. e. Security and monitoring department

This department's main mission is to monitor the and thereby ensure the communications security.

III. f. Event support section

This section is responsible for the propaganda and the audiovisual support of both the Joint Forces Command and the regiment. This section is mobile and is equipped with the latest wired and wireless equipment.

IV. Future plans

In order to keep the operational readiness high and be able to provide interoperable communication with other NATO member states digital radio system is planned to replace the currently used equipment. Besides modernizing the communications equipment, an increase in the number of the personnel of the battalion is envisaged due to the enormous workload on the signal battalion. The event section is planned to be equipped with a mobile carrier vehicle and a conference support system to enhance the capabilities of the subunit.

It is planned to increase the involvement in the preparation of the signal soldiers before deploying abroad and organize special signal basic trainings for the signal soldiers from other units.

Levente DUDÁS, Péter KOVÁCS, Rudolf SELLER

PHASE CONTROLLED LINEAR TRANSMITTER ANTENNA SYSTEM

Törölt: SMART AN

Törölt: ARRAY

Dept. of Broadband Infocommunication and Electromagnetic Theory, Budapest University of Technology and Economics, Goldmann Sq. 3, 1111 Budapest, Hungary
E-mail: *ha7wen@ha5krk.hu, kovacs.peter@mht.bme.hu, seller@mht.bme.hu*

Abstract

Our aim is to develop a microwave antenna whose radiation pattern is electronically controlled. The radiation pattern of regular antennas is determined by the Fourier-transform of the phase and amplitude distribution on the antenna aperture. This radiation pattern is mechanically fixed so its alteration is impossible. Therefore let us construct an antenna system, which contains several antenna elements. All elements are actuated by separate transmitters; let us control the amplitude and the phase of the supplying currents of the antenna elements. This way, we are able to control the radiation pattern of the antenna system. The control is computerized so that there is a possibility to change the radiation pattern several times in a second.

Törölt:

Törölt: *antenna wit cally controlled radia*

Törölt: *the*

Törölt: *by the mech*

Törölt: *the*

Törölt: *n of i*

Törölt: *t*

Törölt: *d*

Törölt: *In such*

Törölt: *ling*

Introduction

Formázott: Felsorolás és számozás

Smart antennas gain more and more space in modern wireless communication systems thanks to the very important property of spatial filtering. When all the combined TDMA-CDMA systems reach their maximum capacity, the SDMA technique can promise even higher capacities, such as in MIMO systems, where channel throughput is increased by space-time-frequency combined signal processing [2, 4]. Our goal is to develop and make scientific investigations with a digitally controlled phased-array system. It will be able to shape its direction pattern with almost totally arbitrary number of directions of main lobes or null-points without mechanics or inertia. In a two-dimensional rectangular antenna array, with 16 elements, a high degree-of-freedom exists to synthesize very sophisticated radiation patterns. In this paper our approach is presented with both hardware and software solutions.

Törölt: al

Törölt: r

Törölt: locations

Theoretical Background

Formázott: Felsorolás és számozás

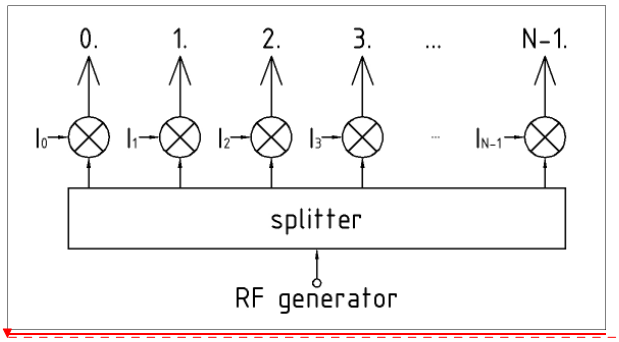
In this chapter we show the theoretical foundation of our beam former system. We omit the detailed discussion of description, analysis or synthesis methods of antenna arrays but some important relationships will be presented.

Our beamformer is a linear antenna array of microstrip patch antennas with the same direction pattern in a uniform array used only for transmission. To control the overall direction pattern of this array the excitation signal of each antenna element is controlled independently in both amplitude and phase. The resultant radiation pattern is the Fourier transform of the complex excitation current values in spatial domain and it will have rotational symmetry around the main axis of the linear antenna array. To adapt the antenna to the actual RF environment, a separate direction finder antenna is needed, wherein adaptive algorithms could be used, and this receiver equipment is able to control the transmitter. For transmission, the task is only controlling. (In our department, a direction finder receiver antenna which uses adaptive algorithms – e.g. Capon- and MEM-methods – had been developed [1, 2, 5]. Now, we do not use the receiver equipment, we control the transmitter separately.

Of course the radiation patterns of the radiator elements in the array also affect the overall radiation pattern. For the simplest description we assume that the elemental direction patterns are isotropic. Using future measurement results and/or the simulation results of the patch antennas, the controller program is able to calculate on the radiation pattern of the antenna elements. The Fourier transformation explains how can the properties of the radiation pattern be controlled by the currents feeding the antennas. For example to achieve a lower side-lobe level the weighting of the excitation amplitudes must be decreased towards the borders of the antenna array, so we apply a window-function.

To obtain the far-field radiation pattern of an equidistant linear antenna array equation (1) must be evaluated. The number of antenna elements is 16, that is why n runs between 0 and 15, k is the wavenumber, d is the distance between the antenna elements (in wavelengths), I_n is the complex value of the excitation current of the n-th antenna element [2, 3].

$$F(\vartheta) = \sum_{n=0}^{15} I_n e^{jnkd\cos\vartheta} \qquad (1)$$



Törölt: ing
Törölt: ,
Törölt: Fourier-
Törölt: ,
Törölt: element
Törölt: s
Formázott: Betűtíp
Formázott: Betűtíp
Formázott: Betűtíp
Formázott: Betűtíp
Formázott: Betűtíp
Alsó index
Formázott: Betűtíp
Törölt:

Fig. 1. Build of the linear antenna array

Contrary to conventional antennae, we can define degrees of freedom with antenna systems, which is equal to N. We are able to alter the main radiation direction, the side lobe level, null-points and the main lobe width by controlling the phase and the amplitude of the antenna elements. The realization of the antenna array is shown in Fig. 1.

The complex values of the feeding currents determine the radiation pattern, but it is rotatable by the progressive phase shift (2). ϑ_{shift} is the modified direction of radiation pattern. This complex multiplication is executed by the controller software and the changed values are downloaded into the digital controller unit [2, 3, 5].

$$F(\vartheta) = \sum_{n=0}^{15} e^{jn\vartheta_{shift}} I_n e^{jnkd\cos\vartheta} \qquad (2)$$

Controller Software

Our simulation software is presently capable of evaluating the direction pattern of a linear array of uniformly spaced antennas with a maximum element number of 16. The software is written in LabView, a screenshot of it can be seen in Fig. 2. The element distance and main radiation direction are variables. The excitation amplitudes and phases are adjustable independently at every element. Some built-in radiation patterns are available for synthesis, such as binomial, triangular, equal amplitude, etc. The amplitude and phase values are displayed graphically.

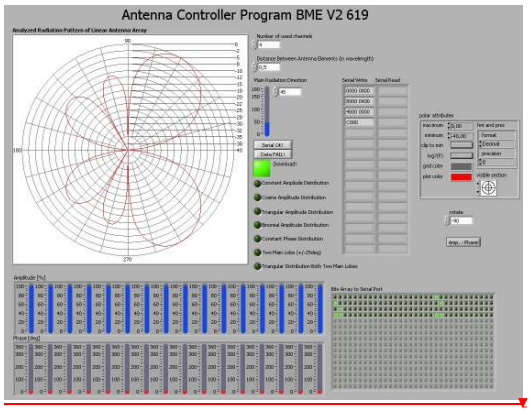


Fig. 2. Antenna array controller program

Some basic and important radiation patterns are shown in Fig. 3. Those are polar plots of radiation patterns with logarithmic scale, the axis of the antenna array is the 0..180° axis, so the first three patterns are broadside arrays and the last

Formázott: Betűsz Automatikus

Törölt: To synthesiz pattern the proper exc weighting is needed. I valued excitations arb tion patterns could be with linearly increasin phase along the array metrical radiation patt synthesizable. The ma width and side-lobe le controllable by the am

Formázott: Betűsz

Formázott: Betűsz

Formázott: Betűsz

Formázott: Betűsz

Formázott: Betűsz

Formázott: Felsorc számozás

Törölt: al

Törölt:

Törölt: interesting

Formázott: Betűsz Automatikus

one is an end-fire radiator. The first diagram shows a dual-beam pattern with two main-lobes at 72° and 108° with an element distance of half a wavelength and equal amplitudes at all the 16 elements. Number 2 shows a low side-lobe level pattern with element distance of half a wavelength and cosine amplitude distribution, 16 elements. The third diagram shows a typical equal amplitude linear array with 16 elements and element distance of half a wavelength. Figure number 4 is a cardioid pattern with 2 elements and an element distance of quarter a wavelength.

Törölt: -

Törölt: -

Törölt: T

Törölt: -

Törölt: The

Törölt: -

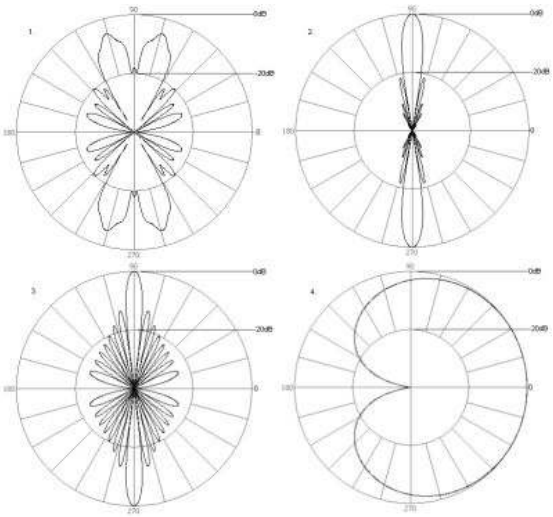


Fig. 3. Radiation patterns

We are working on the software to make it able to evaluate the radiation pattern from several input parameters, such as antenna element number, element distance, array configuration (1D linear or 2D rectangular) and main lobe number and direction. Implementation of user defined null location needs also further development. The software will be able to download the calculated excitation weighting vector into the beamformer hardware via serial port.

Hardware Description

Formázott: Felsorolás és számozás

There are many constructional aspects about the hardware design of a digital beamformer antenna array. The goal is to implement a complex multiplicative weighting on the separate transmitter channels. To achieve this we must control the amplitude and phase of the excitation signal of each antenna element. It is possible to drive more antennas with the same signal, but specific direction patterns need symmetrical excitations, for instance the dual-beam pattern in Fig. 3. For a higher level of flexibility our design is capable of driving 16 antenna elements independently. Two possible approaches exist for the implementation of the complex weighting, a “true digital” and a “quasi digital” design.

Törölt: realize

Törölt: it is for

Törölt: which

The “true digital” way does all signal manipulation with digital signal processing, producing or processing the signals at the complex baseband or at an intermediate frequency. It needs high-speed computing solutions, and for increasing element numbers and increased signal bandwidth it needs even higher speed or distributed processing. This means higher cost, but as DSPs and FPGAs develop, it will become more and more cost effective. The dynamic range of the transmitted signals is limited only by the digital calculation precision and the quality of analogue-digital converters, so it can have a very high level of dynamics. The digitally processed or produced signal then passes to the upconversion and RF amplifier stages. If the upconversion is also made digitally, only the RF amplification and the radiator element can cause unwanted radiation pattern variation by amplitude and phase errors or elemental direction pattern differences. Moreover, these effects are hard to manage because those depend on temperature and frequency.

Törölt: makes

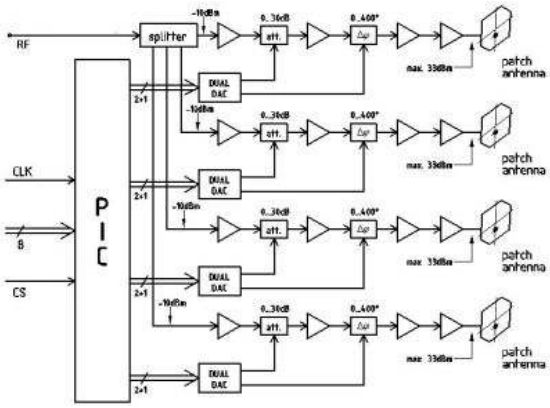


Fig. 4. Connection diagram of a four-channel transmit block

The “quasi digital” way is to make the proper amplitude and phase control directly on the upconverted RF signal by digitally controllable attenuator and phase-shifter circuits. In this way no high-speed real-time signal processing is needed until a true adaptive fading reduction or target tracking must be done. The bandwidth could be higher than in real-time baseband processing, because the carrier frequency is also high, and the control of the signal properties (amplitude, phase) is done by slowly changing signals. The common problem of the two different approaches is the calibration of the transfer functions of the transmitting channels versus temperature and frequency. That can be done by a feedback loop during operation or by storing a huge calibration database in memory and compensating the amplitude and phase errors of the RF circuits. The connection diagram of a four-channel transmitter block for 10 GHz is shown on Fig. 4; the digital control unit (including microcontrollers, D/A converters, line-amplifiers and serial adapter) is shown on Fig. 5; RF unit (including splitters, attenuators, phase-shifters, RF amplifiers) is shown on Fig. 6.

Törölt: e

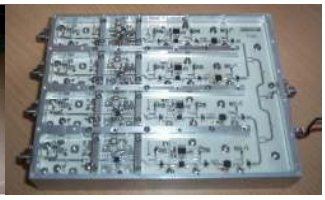


Fig. 5. DCU Fig. 6. RF block

The microwave RF signal is split and fed into a chain of attenuators and phase-shifters which have analogue control inputs. Amplifier stages are used to achieve the desired gain and power level and isolate the attenuator and phase-shifter stages. Digital control of signal properties is achieved by D/A converters and on-board microcontrollers. The controller software downloads the weighting vector components and the microcontroller produces the proper analogue wave-forms. The radiators will be microstrip patch antennas with linear polarization.

Törölt: ted

Törölt: -

Another possible solution of changing the feeding RF current is to use I-Q modulators. RF channel of our another transmitter antenna system for UMTS is on Fig. 7.

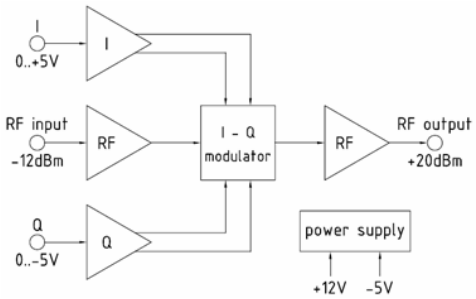


Fig. 7. Connection diagram of a 2 GHz RF channel

We have made another DCU for UMTS. The difference between DCU for 10 and 2 GHz is the reference voltage of the DACs, which are mounted in the DCU. The 4-channel RF block is on Fig. 8. and its DCU is on Fig. 9.

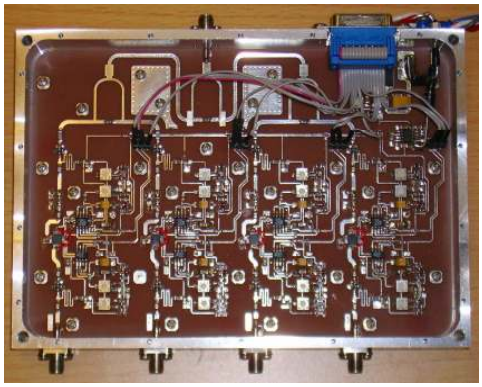


Fig. 8. 4-channel RF block for 2 GHz

The controller software is able to control the hardware to realize one or more different radiation patterns, to switch over among them and to scan in given angle range several times per second. To switch over it is necessary to give the different complex weightings for each radiation pattern (64 byte/radiation pattern), to scan, it is necessary to give the first and last angle of scanning and number of steps. The controller software is able to calculate and download them into the digital controller unit (amplitude and phase – 10 GHz, I and Q – 2GHz), then the computer is separable from the controller. In each radiation pattern, the main lobe direction, side lobe level and suppression are determinate. For one or more directions, the antenna can match null-points not to cause interference or disturbances for other radio systems.

Törölt: one

Törölt: s

Törölt: beginner

Törölt: the final

Törölt: zero-location

Formázott: Betűsz
Automatikus

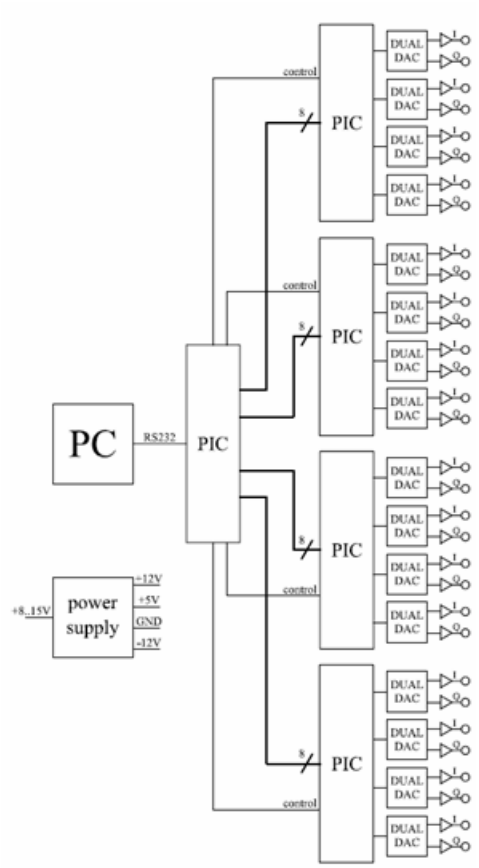


Fig. 9. DCU block diagram for 2 GHz

Calibration

Calibration process is necessary because the phase shifter attenuates according to its phase shift, and the attenuator shifts the phase according to its attenuation and these are non-linear versus the controller voltages (behavior of I-Q modulator is similar).

So, the calibration program stores the current value of amplitude and phase (or I and Q) data to DCU, controls the HP vector-network-analyzer and receives the measured complex S_{21} data.

The antenna controller program – which is shown on Fig. 10 – uses these complex element 3 dimensional databases. Its task is to look the right S_{21} element up in this database and send its coordinates (control voltages of amplitude and phase or I and Q) into the DCU.

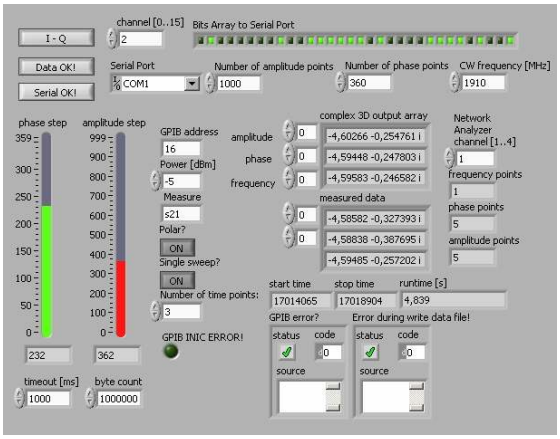


Fig. 10. Calibration program

In this way, the value of the transfer function of a channel in a defined frequency could be the calculated.

Measurement Results

We measured radiation patterns of a four-channel transmitter block (number of antenna elements is 4, and the distance between antenna elements is 1.5 wavelengths – because of technological reasons – 10 GHz patch; 0.8 wavelength – 2GHz patch, 0.5 wavelength – 2 GHz GP antenna).

The used antennas are shown on Fig. 11. (transmitter patch antenna row for 10 GHz), Fig. 12. (receiver horn antenna for 10 GHz), Fig. 13. (patch for 2 GHz) and Fig. 14. (monopole antenna for 2 GHz).

An anechoic chamber for antenna measuring is necessary, where the walls are coated of microwave occlusive material to be able to measure the far-field radiation pattern.

Formázott: Felsorolás számozás

Törölt: shielded

Törölt: room f

Formázott: Betűtípus (Alapérték) Arial

Törölt: unechoic cha

Törölt:

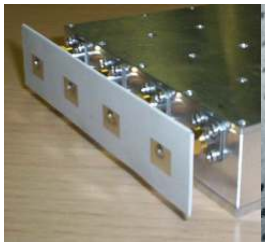


Fig. 11. Transmitter Fig. 12. Receiver

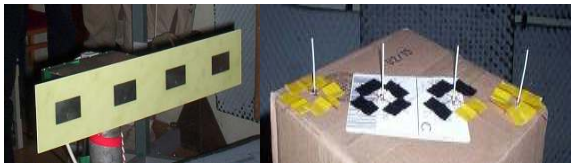


Fig. 13. Patch **Fig. 14.** GP

On X-band (10GHz):

We made different amplitude and phase distribution on antenna elements. The first has constant amplitude distribution (maximal output level) and 0 degree phase shift on each channel. This analyzed radiation pattern is on Fig. 15.

The measured, both non-compensated and compensated radiation patterns are shown on Fig. 16. and Fig. 17.

The main radiation direction is controlled by the progressive phase shift on the antenna elements. Fig. 18. and Fig. 19. show when the main radiation direction is 165 and 195 degrees.

The radiation pattern of a microstrip patch antenna as an elementary radiator is shown on Fig. 20. The radiation pattern of the antenna array is weighted by this radiation pattern, so the measured and analyzed patterns are different.

Törölt: A

Törölt: M

Törölt: ,

Törölt: -

Törölt: its

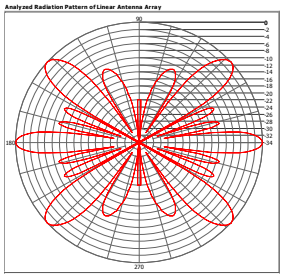


Fig. 15.

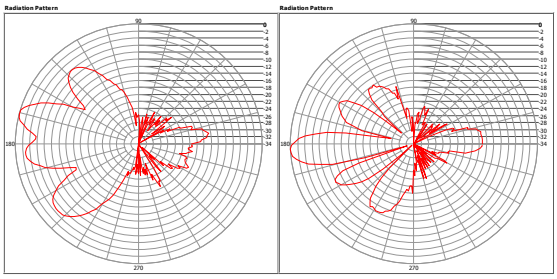
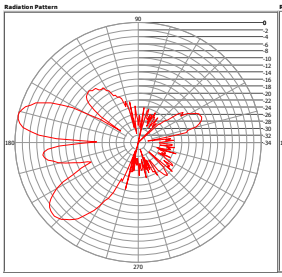


Fig. 16. Fig. 17.



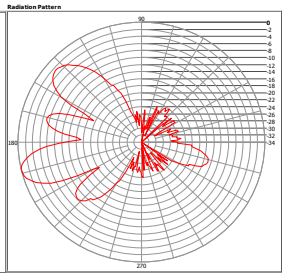


Fig. 18. Fig. 19.

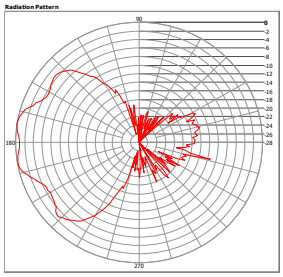


Fig. 20.

<u>On UMTS-band (2 GHz):</u>

We have adjusted triangle amplitude distribution on the antenna elements. The analyzed radiation pattern is on Fig. 21.

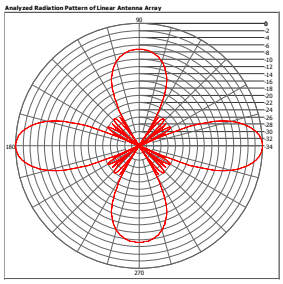
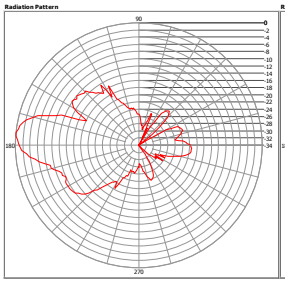


Fig. 21.

The difference between non-compensated and compensated radiation patterns is highly visible on Fig. 22. and Fig. 23.



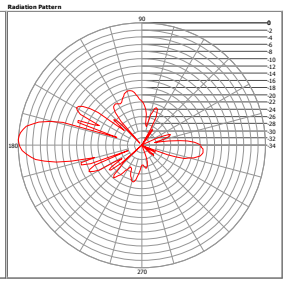


Fig. 22. Fig. 23.

If the amplitude distribution is constant, the side lobe level is higher (-13.5 dB) – on Fig. 24. (analyzed), Fig. 25. (non-compensated), Fig. 26. (compensated).

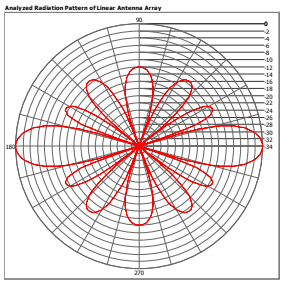
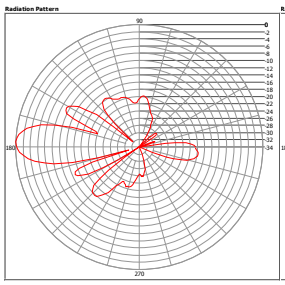


Fig. 24.



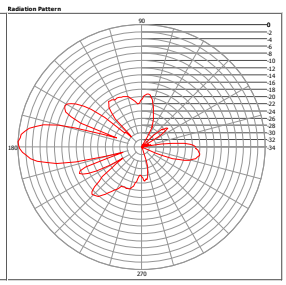


Fig. 25. Fig. 26.

We have measured the follows with monopole antennas (GP), where the distance between antenna elements is half wavelength:

Analyzed is on Fig. 27; non-compensated is on Fig. 28. and compensated is on Fig. 29.

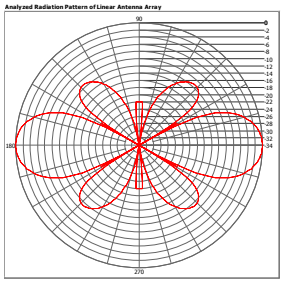
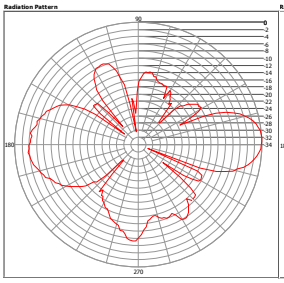


Fig. 27.



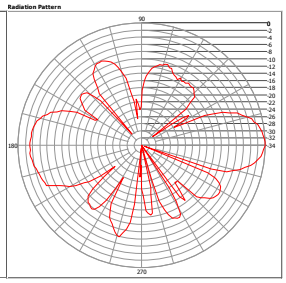


Fig. 28. Fig. 29.

In this case, we did not get the required radiation pattern, because of the too small measuring room. So in-situ measurement is necessary.

In-situ measuring had been in Budaörs Airport. The measuring equipment is on the following picture – Fig. 30. – antenna rotator, DCU, RF block, triple-leg, network-analyzer, etc.

Fig. 30.

When the calibration database consists of 10 amplitude points (dynamic is 10 dB), and 360 phase points (1 degree phase step), we measured the following:

the main radiation direction is 180 – Fig. 31; 150 – Fig. 32; 130 – Fig. 33; 220 degrees – Fig. 34.

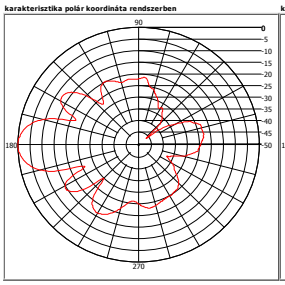


Fig. 31.

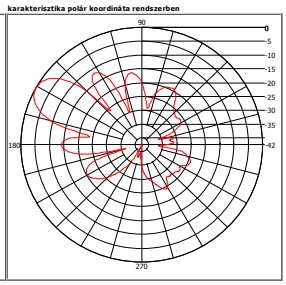


Fig. 32.

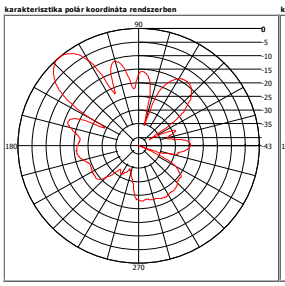


Fig. 33.

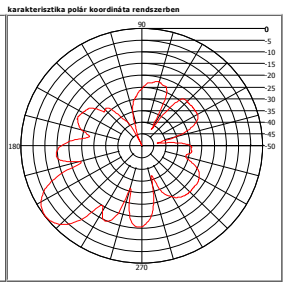


Fig. 34.

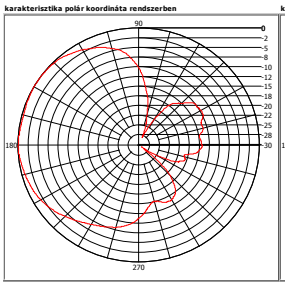


Fig. 35.

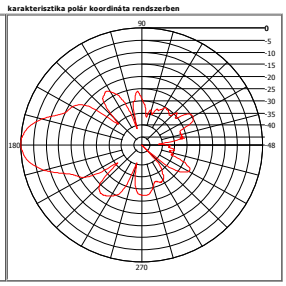
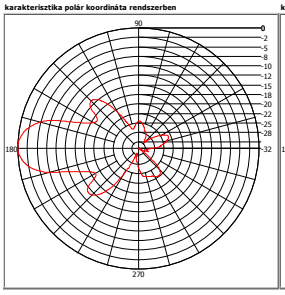


Fig. 36.

The radiation pattern of the elementary patch antenna is on Fig. 35. When the amplitude distribution is triangle, the side lobe level decreases to -27 dB – Fig. 36.

If we calibrated the antenna elements in 400 points of amplitude (26 dB dynamic) and 720 points of phase (0.5 deg phase step), we could measure the follows: the main radiation direction is 180 degrees – Fig. 37; 210 degrees – Fig. 38; 135 degrees – Fig. 39.



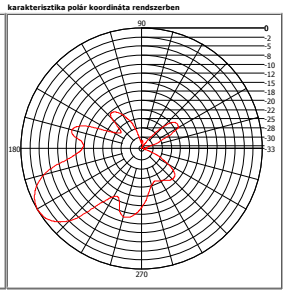


Fig. 37. Fig. 38.

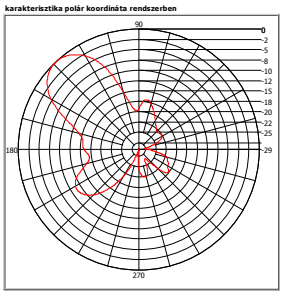
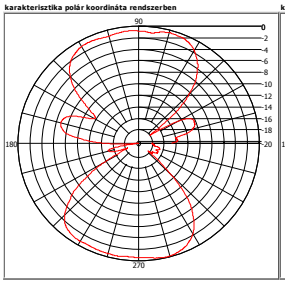


Fig. 39.

With GP antennas: the main radiation directions are: 90 – 270 (Fig. 40); 0 – 180 (Fig. 41); 5 – 175 (Fig. 42); 80 – 280 degrees (Fig. 43).



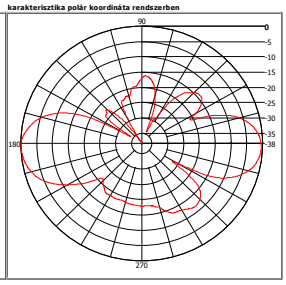
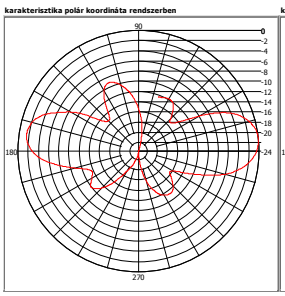


Fig. 40. Fig. 41.



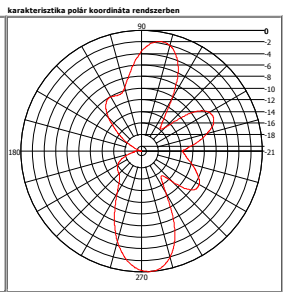


Fig. 42. Fig. 43.

Conclusion

The presented approach is a cost effective solution to make experimenting possible with digital beam forming applications, containing modern semiconductor devices either in RF or in digital parts.

We had developed one four-channel RF blocks for 2 and 10 GHz bands, the controller hardware and software, the calibration process and made databases.

It the future, we are making the further 12 RF channels and its calibration database.

The whole antenna system will contain 16 antenna elements, so its size increases. The anechoic-chamber is too small to make antenna measuring, so further in-situ measuring will be necessary.

Then, we want to integrate it with a radio-direction-finder-system to make it usable in interference-canceller-system for mobile-repeater application.

Acknowledgements

This work was supported by Ministry of Defence, Bonn Hungary Electronics and Mobile Innovation Center, Hungary.

References

[1] FARINA, A. Antenna-Based Signal Processing Techniques for Radar Systems. Artech House, Norwood, 1992.

[2] LITVA, J., KWOK-YEUNG LO, T. Digital beamforming in wireless communications. Artech House Publisher, 1996.

[3] RAPPAPORT, T. S. Smart Antennas. IEEE, 1998.

[4] KO, C. K., MURCH R. D. Compact Integrated Diversity Antenna for Wireless Communications. IEEE Transactions on Antenna and Propagation, 2001.

[5] Proakis J. G. Digital Communication. McGraw-Hill Higher Education, 2005.

Törölt: ¶

Formázott: Felsorolás és számozás

Törölt: the

Törölt: ¶

Formázott: Felsorolás és számozás

Törölt: ¶

Törölt: ¶

Formázott: Felsorolás és számozás

Törölt: <#>¶

Formázott: Felsorolás és számozás

Törölt: <#>¶

Formázott: Felsorolás és számozás

Törölt: <#>¶

Formázott: Felsorolás és számozás

Törölt: <#>¶

Formázott: Felsorolás és számozás

NÉMETH András

MOBILTELEFON HÁLÓZATOK ALKALMAZHATÓSÁGA A LAKOSSÁGI RIASZTÁS ÉS TÁJÉKOZTATÁS RENDSZERÉBEN

Bevezetés

Természeti katasztrófák, ipari-, vegyi-, nukleáris-, tömeges közlekedési szerencsétlenségek, vagy terrortámadások esetén, az áldozatok számát, illetve az anyagi kár nagyságát jelentősen befolyásolhatja az előre látható eseményeket megelőző, vagy a kialakult helyzetek kezelésére irányuló lakossági riasztás és tájékoztatás sebessége és minősége.

Napjainkban is folytatódik a mobil hírközlési technológiák és szolgáltatások térnyerése, ezért cikkemben elsősorban a mobiltelefon hálózatokon megvalósítható speciális – a hatóságok és a lakosság közötti egyirányú kommunikációt biztosító – riasztási- és tájékoztatási rendszerrel, illetve annak anomáliáival kívánok foglalkozni.

Jogszabályok

A veszélyhelyzeti hírközlés egyik meghatározó területe a lakosság rendkívüli helyzetekben történő riasztása és tájékoztatása az emberi élet- és vagyonbiztonság megőrzése érdekében. A korábban érvényben lévő vonatkozó jogszabályok idejét múlt szemléleten alapultak, hiszen kiindulópontjuk a „váratlan légitámadás” volt, és nem biztosították egy modern, a katasztrófavédelmi igényeknek is megfelelő riasztási- és tájékoztatási rendszer megalkotását.

Ehhez az állapothoz képest 2007. július 26-án pozitív irányú elmozdulás következett be, hiszen hatályba lépett a váratlan légitámadás esetén a légiriasztás rendszeréről szóló 186/2007. (VII. 18.) Kormányrendelet, amelyben megjelennek a mobiltelefon szolgáltatások riasztási- és tájékoztatási feladatokba történő bevonását lehetővé tevő megfogalmazások. A 6. § szerint „A gazdasági és közlekedési miniszter az elektronikus hírközlésről szóló törvényben kapott felhatalmazás alapján kijelöli a légiriasztás honvédelmi feladatának végrehajtásában résztvevő műsorszolgáltatókat és elektronikus hírközlési szolgáltatókat, valamint megállapítja feladataikat.” Tekintettel arra, hogy a rendelet tárgya nem változott, szóba kerülnek a katasztrófavédelem feladatai, azok azonban kizárólagosan a légiriasztásra vonatkozóan fogalmazódnak meg.

A katasztrófariasztás fogalmát kizárólag az óvóhelyi védelem, az egyéni védőeszköz-ellátás, a lakosság riasztása, valamint a kitelepítés és befogadás általános szabályairól szóló 60/1997. (IV. 18.) Kormányrendelet tartalmazza, amely azonban nem jeleníti meg lehetséges eszközként az elektronikus hírközlési szolgáltatókat. Ezen rendeletnek a 186/2007. Korm. rendelettel, valamint az elektronikus hírközlés veszélyhelyzeti és minősített időszaki felkészítésének rendszeréről, az államigazgatási szervek feladatairól, működésük feltételeinek biztosításáról szóló 100/2004. Korm. rendeletekkel való harmonizálása, valamint a kapcsolódó miniszteri rendelet(ek) megalkotása megteremtheti a lakossági riasztó és tájékoztató rendszer mobiltelefon szolgáltatásokkal történő kiegészítésének jogi feltételeit.

Jelenlegi állapotok

A lakossági riasztás és tájékoztatás aktuális helyzetével és anomáliáival, valamint a vezetékes- és mobil telefonok bevonásának lehetőségével Maros Dóra foglalkozik doktori (PhD) értekezésében, amelynek alapján a következő megállapítások tehetők:

- Magyarországon három platform áll a hatóságok rendelkezésére a polgári lakosság riasztásának és tájékoztatásának biztosítására: elektromos, vagy kézi szirénák, fixen telepített, vagy gépjárműbe szerelt megafonok, elektronikus média (rádió, televízió);
- az elektromos szirénák többsége elavult kézi indítású, és működése függ az energetikai hálózattól; a lakosság – megfelelő tájékoztatás híján – nem ismeri a különböző jelzéseket és az azok megszólalásakor tanúsítandó magatartásformákat; a Paks környéki rendszert leszámítva a szirénák karbantartása és próbája akadozik; a hangjelzések hallhatósága a megnövekedett környezeti zajszint miatt jelentősen lecsökkent;
- a megafonos tájékoztatás a beszédérthetőségi feltételek miatt (pl. korlátozott sávszélesség és hangerősség) miatt szintén nem elégíti ki a lakossági tájékoztatással szembeni igényeket;
- a rádió- és televízió csatornákon keresztül történő tájékoztatás alapvető feltétele, hogy a lakosság a kijelölt műsorszolgáltatók valamelyikét figyelje a közlemények időpontjában [4. p.90-93.].

Alapvető probléma, hogy a lakott területektől távol tartózkodók és a hallássérültek nem érhetők el a fenti megoldások egyikével sem. A hallássérültek veszélyeztetettsége ezért egy katasztrófahelyzetben lényegesen nagyobb, mint „egészséges” társaiké.

Ezek alapján – Maros Dóra megállapításával összhangban – az a következtetés vonható le, hogy a jelenlegi riasztó és tájékoztató rendszer elavult, nehézkes és nem biztosítja az érintettek megbízható elérését, így csak korlátozottan alkalmas feladatának ellátására.

Mobiltelefon rendszerek alkalmazhatósága

Mivel az európai lakosság jelentős része rendelkezik mobiltelefonnal, a legkézenfekvőbb megoldás a mobiltelefon hálózatok lakossági riasztó és tájékoztató rendszerbe történő bevonása lenne.

Megvalósításának alapja az előfizetők tartózkodási helyének legalább alap pontosságú (cella szintű) ismerete, de amennyiben ez nem biztosítható, a rendszer működési alapelvének köszönhetően minden esetben rendelkezésre áll az adott bázisállomás ellátottsági területén tartózkodó terminálok listája. Miután a szolgáltatók adatbázisaiban hozzáférhetők a veszélyeztetett területen tartózkodók hívószámai, – veszély-, vagy katasztrófahelyzetben, a kritikus esemény bekövetkezésével összefüggésben (megelőzően, bekövetkezéskor, követően) – központilag hívások kezdeményezhetők irányukba, vagy üzenetek küldhetők részükre. A szolgáltatás megvalósítására a jelenleg üzemelő mobiltelefon hálózatok technikailag alkalmasak. A feltétlenül szükséges átalakítások (befektetések) során vagy a meglévő SMS- és hangposta-szerverek szoftvereit kellene módosítani, vagy új rendszerelemként egy veszélyhelyzeti integrált üzenetkezelő szervert (megfelelő tartalékolással) üzembe helyezni. (Természetesen a rendszervezérlő- és hálózat-felügyeleti szoftvereket is módosítani szükséges.) A megoldás lényege, hogy a szervereken tárolt előreprogramozott szöveges-, hang-, valamint multimédiás üzenetek a riasztás típusától függően, a szükséges (pl. helyfüggő) információkkal kiegészítve kerülnek továbbításra a veszélyeztetett területeken tartózkodó minden előfizető készülékére.

A rendszer megvalósításakor az alábbi szempontokra tekintettel kell lenni:

- az adott felhasználó számára küldött üzenet típusa függ egyrészt az adott készülék képességeitől, másrészt az előfizetői adatoknál szerződéskötéskor feltüntetett esetleges fogyatékosságtól; ez annyit jelent, hogy multimédiás üzenetet csak MMS[24] képes készülékre továbbítson a rendszer, míg látássérült hangüzenetet, hallássérült szöveges üzenetet kapjon;
- az ilyen speciális hívások és üzenetek esetén kiemelt (a segélyhívásokéhoz hasonló, de azoknál egyel alacsonyabb szintű) prioritást kell biztosítani, ami hangposta üzenetek esetén annyit jelent, hogy minden rendelkezésre álló forgalmi csatornán (nagy előfizető szám esetén félsebességű csatornákat használva), akár fennálló összeköttetések bontása árán is, biztosítani kell a hívás felépülését (üzenetek esetén a riasztó és tájékoztató célú SMS[25]-ek és MMS-ek az esetleges várólisták élére kerülnek);

[24] Multimedia Message Service
[25] Short Message Sevice

- annak érdekében, hogy a riasztás a legnagyobb valószínűséggel sikeres legyen és tájékoztató közlemények célba érjenek, a bázisállomások a jelzéscsatornán küldött speciális, egyre emelkedő hangerejű csengetőjellel (pl. szirénahang) figyelmeztessék a felhasználót a közlésre váró információk fontosságára;
- a fenti lehetőséget lenémított, de ki nem kapcsolt készülékek esetén is biztosítani kell, a hangszóró tiltásának távirányítással történő feloldásával;
- gondoskodni kell az ilyen speciális üzenetek és hívások sikerességének ellenőrizhetőségéről [4. p.93.] (hívások esetén a fogadás detektálását követően a hívás időtartamából lehet következtetni, hogy az előfizető végig hallgatta-e azt, vagy az üzenet végén egy – az üzenet megértését és tudomásulvételét jelentő – nyugtázó gombnyomás végrehajtását kell kérni tőle; üzenetek esetén – a megnyitást jelentő – nyugtát kell kérni a készüléktől);
- sikertelen hívások és üzenetek esetén, azokat későbbiekben megismételve, vagy egymással kombinálva próbálkozik a hálózat tovább, a riasztás érvényességi idején belül; az érvényesség lejártát követően a sikertelenül elérni próbált hívószámokhoz tartozó előfizetőkről a rendszer jelentést készít, melyet a szolgáltató továbbít a hatóságoknak (a jelentés tartalmazza a valószínűsíthető tartózkodási helyet, valamint az esetleges fogyatékosságot is);
- az üzenetkészleteket úgy kell kialakítani, hogy azok mindegyike a lehető legrövidebb, de egyértelmű tájékoztatást adjon a felhasználók számára a kialakult helyzet jellegéről, súlyosságáról, a hatóságilag foganatosított intézkedésekről, valamint a tanúsítandó magatartásról (riasztás vezérlő számítógépről dinamikusan, gyorsan konfigurálható, bővíthető, kiegészítendő keretüzenetek);
- a hangüzenet az egyik leghatékonyabb módja, hogy katasztrófahelyzetekben, a riasztás mellett egyértelmű tájékoztatást kapjanak az érintett területeken tartózkodók; ez a megoldás minden – a legegyszerűbb szolgáltatásokat nyújtó – készülék esetén alkalmazható egészséges és látássérült személyek esetén is; azok az előfizetők, akiknek termináljai valamilyen oknál fogva adott időben nem üzemelnek, kikapcsolt állapotban vannak a saját hangpostafiókjukba is megkapják az üzenetet (a hálózat később újra próbálkozik szöveges- és hangüzenettel is);
- az MMS üzenetek lehetőséget teremtenek számos többletinformáció közlésére is, például menekülési útvonalak térképrészleten történő illusztrálására, és a szöveges üzenetek, hangüzenettel történő kiegészítésére, nyomatékosítására;

– az MMS és SMS előnye a hangposta-szerveres megoldáshoz képest, hogy szükség esetén a közlemény újra olvasható, az előfizető oldaláról később dokumentálható (időpontok), valamint kevésbé terheli a hálózatot (legalábbis a forgalmi csatornákat).

A fentieken felül előnye még a megoldásnak, hogy a riasztás és tájékoztatás különböző nyelveken is történhet, ezáltal növelve a külföldi állampolgárok biztonságát [4. p.93.]. Technikailag a nyelv kiválasztása az IMSI[26] azonosító, mobil országkód (MCC[27]) mezőjének segítségével történhet, amennyiben a regiszterekben (HLR[28], VLR[29]) biztosítjuk az előfizetői adatok mellett az anyanyelv tárolását is.

Megvalósíthatóság, és alkalmazhatóság szempontjából érdemes megvizsgálni a mobiltelefonos riasztó és tájékoztató rendszer megbízhatóságának, gyorsaságának, és hitelességének kérdését, ami esetünkben a hazai szolgáltatók hálózatainak minőségi paraméterek szempontjából történő vizsgálatát jelenti.

Megbízhatóság szempontjából az alapvető vizsgálandó paraméter a szolgáltatás rendelkezésre állása, ami jelen esetben a mobiltelefon szolgáltatások adott időintervallumra és a szolgáltatási területre vonatkoztatott rendelkezésre állását jelenti, azaz hogy mekkora a valószínűsége adott időszakban a szolgáltatásokhoz való hozzáférésnek:

$$R = \frac{T_{üz} - \sum_n T_{h_n}}{T_{üz}} \cdot 100\% \qquad [6]$$

ahol $T_{üz}$ a vizsgált üzemidő intervallum, míg a ΣT_h a vizsgált intervallumban bekövetkező üzemkiesések eredője.

Magyarországon a mobiltelefon szolgáltatók számára előírt rendelkezésre állás nem lehet kevesebb 95%-nál, ugyanakkor 2006-os évre vonatkozóan mindhárom szolgáltató paramétere meghaladta a 99%-ot. A Pannon 99,83%, a T-Mobile 99,94%, a Vodafone 99,06%-os értékkel járult hozzá az 99,61%-os országos átlaghoz [7. p.4.]. Ez naponta átlagosan – a fenti sorrendben – 2,45 perc, 51,84 másodperc, 13,64 perc, azaz átlagban 5,62 perc kiesést jelentett. (Összehasonlításként az EDR[30] rendszer előírt rendelkezésre állása 99,9% azaz átlagosan legfeljebb napi 1,44 perc kiesés megengedett.)

A megbízhatóságon belül lehet még említeni a hálózatok forgalmát is figyelembe vevő paramétert a sikertelen hívások arányát, ami a

[26] International Mobile Subscriber Identity (Nemzetközi Mobil Előfizető Azonosító)
[27] Mobile Country Code (Mobil Országkód)
[28] Home Location Register (Honos Helyzetregiszter)
[29] Visitor Location Register (Látogató Helyzetregiszter)
[30] Egységes Digitális Rádiótávközlő Rendszer

nagyforgalmú időszakban[31] kezdeményezett, de fel nem épülő összeköttetések arányát jelenti az összes híváshoz képest. Erre a paraméterre az előírás honos hálózatban legfeljebb 1,4%, míg más belföldi és nemzetközi hívás esetén 2,7%. A szolgáltatók összes hívásra vonatkoztatott sikertelen hívások aránya a 2006-os évben – a fenti sorrendben – 1,41%, 1%, 1,47%, azaz átlagosan 1,29% volt [7. p.5.].

Gyorsaság szempontjából a legfontosabb paraméter a kezdeményezett beszédhívások felépülési ideje, ami belföldi viszonylatban nem haladhatja meg 12 másodpercet. A hazai szolgáltatók eredményei ebben a tekintetben 5mp, 4mp, 4mp, azaz átlagosan 4,33 másodperc volt, ami lényegesen jobb az előírt határértéknél.

A hitelesség kérdése mobiltelefon hálózatok esetében a beérkező hívások és üzenetek azonosíthatóságát jelenti, tehát azt, hogy az előfizető egyértelműen képes-e azonosítani a hívó-, vagy küldő felet, illetve meggyőződhet-e a fogadott információ manipulálatlanságáról (sértetlenségéről). (Fontos, hogy ne fordulhassanak elő „téves riasztások”!)

A fenti adatok alapján megállapítható, hogy a minőségi paraméterek tekintetében a magyarországi mobiltelefon szolgáltatók rendszerei megfelelnek a lakossági riasztás és tájékoztatás alapvető követelményeinek mind a rendelkezésre állás, mind a gyorsaság tekintetében. A hitelesség kérdése oly módon rendezhető, hogy olyan speciális jelzéseket alkalmazunk mind az üzenet feladójának, mind a tartalmának azonosíthatóvá tételéhez, amelyet más módon illetéktelen (rosszindulatú) előfizető nem képes létrehozni. (Pl. a SIM kártyák telefonkönyvébe „égetett” lakossági riasztó és tájékoztató központok telefonszáma, speciális karakterekkel, szimbólumokkal kiegészített üzenetformátumok, a jelzéscsatornákon küldött speciális csengetőjelek stb.)

Másik fontos szempont a lakosság elérhetősége, amelyet egyfelől a hívásfogadásra képes aktív előfizetések száma, másrészt a hálózatok területi lefedettsége jellemez. Magyarországon 2007. júniusában 10 226 389 hívásfogadásra alkalmas aktív SIM kártya volt, amelyből 9 464 896 az utolsó három hónapban forgalmat is bonyolított, ami azt jelenti, hogy átlagosan minden lakosra legalább 1 aktív előfizetés jut [8. p.1.]. A valóságban természetesen a 100%-os ellátottság nem teljesül, hiszen számos felhasználó több előfizetéssel is rendelkezik, míg a gyermekek, és idősek egy része nem fér hozzá a mobil szolgáltatásokhoz. Összességében azonban elmondható, hogy mobiltelefonon keresztül a lakosság jelentős hányada nagyobb valószínűséggel érhető el, mint a jelenleg üzemelő megoldások együttes alkalmazásával. Ehhez természetesen a közel országos (~97-99%) lefedettség is nagyban hozzájárul.

[31] munkanapokon, hétfőtől péntekig 9-17 óráig

Ugyanakkor van még egy szempont, ami gondos vizsgálatot igényel a rendszer hatékonysága szempontjából. A riasztó és tájékoztató hívások és üzenetek által generált forgalom, és a rendszer áteresztőképességének kapcsolata, valamint az adott terület kiszolgálását végző VLR mérete is nagyban befolyásolja a közlemények továbbításának sebességét. Egy néhány cellát érintő katasztrófahelyzetben az értesítendők kikeresése, és a helyadatok kiértékelése egy több százezer, vagy akár egymillió előfizetőt tartalmazó adatbázisból jelentős időt igényelhet, ami adott esetben hátráltathatja a riasztások célbajutását, és így a rendszer hatékonyságát.

Ennél is nagyobb veszteséget jelent az érintettek hangüzenetekkel történő „végighívása", ami egy nagyforgalmú cella esetén óriási időkésleltetést jelent a kiértesítési lánc végén található előfizetők esetén. Természetesen az összes előfizető kiértesítésének időtartama nagyban függ a közlemények hosszától is. Például egy 200 előfizetőt tartalmazó cella esetén 20mp-es üzenetekkel 4mp-es hívás-felépülési idővel és 6mp-es egyéb járulékos késleltetéssel (hívás fogadási- és bontási idő stb.) számolva egy-adóvevős bázisállomással – 1 frekvencia, 8 időrés – optimális esetben 12,5 percig tart a kiértesítés. (Ez természetesen feltételezi a riasztó és tájékozató üzenetek elsőbbségét az előfizetők által kezdeményezett hívásokkal szemben.) Ez némiképp ellentmondani látszik Maros Dóra doktori értekezésében megfogalmazott azon állításnak, miszerint: „A bemondott információ korlátlan számban megismételhető akár automatikusan, akár a riasztott kezdeményezésére" [4. p.93.]. A realitás véleményem szerint sokkal inkább az, hogy bizonyos esetekben lehetőség nyílik az üzenetek megismétlésére, de csak akkor, ha azzal az értesítési lista végén található előfizetőket a további késleltetések már nem veszélyeztetik.

Vannak ugyanakkor olyan megoldások, melyekkel a teljes értesítési idő csökkenthető. A félsebességű forgalmi csatornák (TCH/H[32]) használata lehetővé teszi az egy vivőn egyidőben létrehozható összeköttetések számának, és így az adott területen kiszolgálható előfizetők számának megkétszerezését, azaz így az értesítési idő a felére csökken (az előző példa szerint 6,25 percre). A hatékonyság tovább növelhető úgynevezett „cella átforgatással", ami annyit jelent, hogy az érintett bázisállomásoknak szomszédaik megnövelt adóteljesítménnyel „besegítenek" a határterületen tartózkodók kiszolgálásában. Ezen módszerek együttes alkalmazása akár töredékére is csökkentheti a kiértesítési késleltetést, ezáltal jelentősen növelve a hatékonyságot.

SMS-ek esetében a fenti megállapítás annyiban módosul, hogy azok továbbítása nem forgalmi-, hanem jelzés csatornákon történik, melynek következtében nagy számban való egyidejű küldésük az adminisztratív és

[32] Traffic Channel/Half rate

vezérlő forgalomban okozhat torlódást. A szöveges üzenetek továbbítása optimális körülmények között gyorsabb és hatékonyabb megoldást jelenthet. Az MMS-ek átvitelére a szolgáltatók GPRS[33], EDGE[34], vagy UMTS[35] HSDPA[36] infrastruktúrájukat használják, melyek jelenleg többnyire sűrűn lakott települések környezetében, és nagyforgalmú területeken férhetők hozzá. Az alkalmazott csomagkapcsolt adatátviteli eljárás lehetővé teszi a rendelkezésre álló spektrum optimálisabb kihasználását, így is növelve a kiértesítés hatékonyságát.

A három megoldás egyidejű alkalmazásával és a rendelkezésre álló (2G, 2,5G, 3G, 3,5G) erőforrások optimális megosztásával lényegesen lecsökkenthető a veszélyeztetett területeken tartózkodók elérésének reakcióideje.

Ugyanakkor van egy lényegesen gyorsabb, de kevésbé rugalmas lehetőség az információk egyidejű, széles előfizetői kör számára történő eljuttatására. A hazai szolgáltatók közül mindössze egy alkalmazza ezt a megoldást a felhasználók tartózkodási helyének, végberendezésen történő megjelenítésére. Az úgynevezett BCCH szórócsatornán általában az adott bázisállomásra jellemző információk kerülnek kisugárzásra, melyeket a hatósugarában tartózkodó készülékek a cella azonosítására és a teljesítményszintek mérésére használnak. Ezek az információk kiegészíthetők riasztási és tájékoztatási üzenetekkel, melyek a kisugárzást követően egyidejűleg jeleníthetők meg az érintett területen tartózkodó valamennyi terminál kijelzőjén. Az ilyen típusú üzenetekhez speciális hangjelzések is társíthatók a figyelemfelkeltés érdekében. A rendszer rugalmatlansága a továbbítható információk mennyiségi és minőségi korlátaiból, valamint a közlemények címzetthez történő eljutásának ellenőrizhetetlenségéből adódik. Nagy előnye viszont, hogy egyáltalán nem terheli a mobil hálózatot, minimálisra csökkenti a kiértesítési időt, így alkalmazása gyakran célravezető lehet.

Összefoglalás

Összességében megállapítható, hogy felépítését, műszaki és minőségi paramétereit tekintve a hazai mobiltelefon hálózatok rendszertechnikailag, illetve a nyújtott szolgáltatások tekintetében egyaránt alkalmasak olyan országos lakossági riasztó és tájékoztató rendszer megvalósítására, amely nem kiváltani, hanem kiegészíteni hivatott a korszerűsítésre szoruló hagyományos megoldásokat. Egy ilyen rendszer képes biztosítani mind az egészséges, mind a hallás- és látássérült személyek gyors és megbízható tájékoztatását a nap 24 órájában, mind sűrűn lakott területeken, mind lakott

[33] General Packet Radio Service (2,5G)
[34] Enhanced Data Rates for GSM Evolution (2,5G)
[35] Universal Mobile Telecommunications Systems (3G)
[36] High Speed Downlink Packet Access (3,5G)

területektől távol, lokális, vagy nagyobb kiterjedésű katasztrófák esetén egyaránt. A leghatékonyabb és leggyorsabb megoldást a hang-, szöveges-, és multimédiás üzenetek, valamint a szórócsatornák optimális erőforrás-megosztással történő együttes alkalmazása jelentheti. A rendszer veszélyhelyzet esetén történő aktiválását – hatósági utasításra – a szolgáltatók által működtetett 24 órás ügyeleti szolgálatok végezhetik el. Az állam a készenléti díj mellett, a hálózatok igénybevételével arányos szolgáltatási díjat fizetne.

A szolgáltatás bevezetéséhez először a kapcsolódó jogi szabályozást kell módosítani, majd a megvalósíthatósági tanulmányok elkészítése és a szolgáltatókkal való egyeztetés után ki kell dolgozni a konkrét műszaki terveket és dokumentációkat. Ezt követően a megvalósítás és tesztüzem után, a lakosság megfelelő tájékoztatása és felkészítése mellett (kiadványok, szórólapok, gyakoroltatások stb.) kezdheti meg működését.

Felhasznált irodalom

[1] 60/1997. (IV. 18.) Korm. rendelet az óvóhelyi védelem, az egyéni védőeszközellátás, a lakosság riasztása, valamint a kitelepítés és befogadás általános szabályairól

[2] 186/2007. (VII.18.) Korm. rendelet váratlan légitámadás esetén a légiriasztás rendszeréről

[3] 345/2004. (XII. 22.) Korm. rendelet az elektronikus hírközlési szolgáltatás minőségének a fogyasztók védelmével összefüggő követelményeiről

[4] MAROS Dóra: Távközlési hálózatok működésének nemzetközi és hazai szabályozási kérdései veszély- és katasztrófahelyzetekben – Doktori (PhD) értekezés – Bp.: ZMNE – 2006.

[5] DÁRDAI Árpád: Mobil távközlés, mobil internet – Mobil Ismeret – Budapest – 2002. – ISBN 963 440 996 2 – p. 106-130.

[6] BODLAKI Ákos – CSERNAY Andor – MÁTYÁS Péter – MUHA Lajos – PAPP György – VADÁSZ Dezső: Informatikai rendszerek biztonsági követelményei (Miniszterelnöki Hivatal, Informatikai Koordinációs Iroda, Informatikai Tárcaközi Bizottság 12. sz. ajánlás) – Budapest – 1996. – 6.1. Információbiztonsági osztályozás a megbízható működés szempontjából

[7] (http://www.itb.hu/ajanlasok/a12/html/a12_6.htm)

[8] NHH: A mobil rádiótelefon szolgáltatás minőségi jellemzői 2006. (jelentés)

[9] (http://www.nhh.hu/index.php?id=dokumentumtar&mid=1525&lang=hu)

[10] NHH: Mobil gyorsjelentés, 2007. június (jelentés)

[11] (http://www.nhh.hu/index.php?id=dokumentumtar&mid=1054&lang=hu)

HÓKA Miklós

AZ ÖSSZHADERŐNEMI HARCÁSZATI RÁDIÓRENDSZER FEJLESZTÉSE

Az Összhaderőnemi Harcászati Rádiórendszer (Joint Tactical Radio System, JTRS) fejlesztése az Egyesült Államok Védelmi Minisztériumának kiemelt programja, amely fejlesztés nemzetközi partnerekkel közösen történik, a katonai harcászati rádiók továbbfejlesztésére. A JTRS program felhasználja a civil szoftverrádiós kutatások eredményeit, amely lehetővé teszi számos különböző hullámforma azonos platformon való futtatását, ezáltal erősíti az interoprabilitást a különböző szervezetek, a szolgáltatók és a koalíciós partnerek között.

A korszerű katonai rádiókból kialakított harcászati rádiórendszerben a beszéd- és adatüzenetek feldolgozása, a felhasználóhoz történő továbbítása szolgáltatások formájában jelenik meg. A beszédhang átvitel digitális hangkódoló (vokóder) egységeken alakul ki, míg az adatátvitel megvalósításához modemek kerültek beépítésre a rádiókba. Lehetséges a hang és adat egyidőben történő átvitele is, ekkor az információk – általában – időréseket biztosító keretrendszerben kerülnek továbbításra, amely időrések a csomagokra bontott hang és adatinformációkat közel valós időben közvetítik a címzettnek. A csomagkapcsolt adatátviteli képesség egy önálló üzemmódot eredményezett a rádiók kialakításánál –csomag(kapcsolt) vagy packet üzemmód –, aminek eredményeként például a fegyverirányítási rendszerek valós időben kapják a vezérlő adatokat.

A digitális rádiók, melyek hardverelemeibe speciális célú integrált áramköröket (Application Specific Integrated Circuits, ASIC) építettek, alapvető karakterisztikáinak37 a kialakítása ezekkel a digitális jelfeldolgozó egységekkel történik. Az ASIC áramkörök ugyanakkor lehetnek szoftveres programozásúak, de a beépített digitális jelfeldolgozó processzorok (Digital Signal Processor, DSP), – amelyek az információs csatorna jeleit dolgozzák fel –, itt még nem programozhatóak szoftveresen. A jelenleg rendszerben lévő digitális rádiók többsége ebbe a kategóriába tartozik, így a digitális rádió fogalmába a szoftver által programozható rádiók is beletartoznak.

[37] A rádió alapvető karakterisztikái alatt a moduláció típusait, az üzemelési frekvenciákat, a sávszélességeket, a csatornához történő többszörös hozzáférési eljárásokat, a forrás és csatorna kódolási/dekódolási eljárásokat, a frekvencia spektrumának szórási/sűrítési technikákat, és a titkosítási algoritmusokat értem.

A szoftver-vezérlésű rádiónál (Software-Defined Radio, SDR) az ASIC áramkörök és az információs csatorna digitális jelfeldolgozását biztosító DSP-k már minden funkciójukban szoftveresen programozhatók, és így egyszerűen megváltoztathatók a rádió karakterisztikái, külsőleg csatlakoztatott egység(ek) közreműködése nélkül. Ugyanakkor itt a rádiófrekvenciás bemeneti/kimeneti egységek (antennaszűrők, közösítő szűrők, nagyfrekvenciás erősítők) csak analóg jelek adás-vételére képesek, a digitális jelfeldolgozás csak az analóg-digitális átalakítás után következik.

A szoftverrádió hardverelemei az antenna bemenettől az ember-gép interfészen megjelenő felhasználói információ megjelenéséig teljes egészében digitális jelfeldolgozásúak és szoftver által programozhatóak. Itt jegyzem meg, hogy ennek a rádiókategóriának a megjelenésére még várni kell, a szoftverrádiós kutatás-fejlesztés célja éppen az ilyen készülékek megalkotása.

Területek	**Katonai**	**Rendvédelmi**	**Üzleti (civil)**
Felépítés	Integrált rádió, router és számítógép	Int. rádió és számítógép (esetleg router)	Integrált rádió és számítógép
Elkülönített csoportképzés	Rugalmas csoportképzés a feladat függvényében	Virtuális csoportképzés és zárt felhasználói csoport kialakítása	Virtuális magánhálózat kialakítása és ebben zárt felhasználói csoport
Csatlakozás más rendszerekhez	Multinacionális környezetben más katonai rendszerekhez	Csatlakozás a nemzetközi kereső-mentő rendszerekhez	Nemzetközi üzleti rendszerekhez
Speciális jellemző	Többszintű titkosított üzemmód	Hordozható állomás válsághelyzetekben	Üzleti helyzetismeret kialakításának lehetősége
Speciális szolgáltatások	• valós idejű rugalmas átkonfigurálás; • interoperabilitás speciális hullámformákkal;	• erőteljes vészhelyzeti kommunikáció; • hozzáférés személyi nyilvántartó adatbázisokhoz;	• e-mail; • hang üzenet; • internetes csatlakozáskor böngészés;

1. táblázat: SDR szolgáltatások minden felvevő piacra. (Forrás:[1])

Maga a szoftverrádió terminológiája a 90-es évek elején merült fel, kikerülve a 80-as évekre jellemző, rugalmatlan „hardveralapú” rádiós felépítést, amelyben a konstruktőröknek nem kis fejtörést okozott a legkisebb továbbfejlesztés is. A szoftver-által programozható rádiók olyan előnyös tulajdonsággal rendelkeznek a korábbi eszközökkel szemben, mint a nagyobb adatátviteli sebesség, a nagyobb sávszélesség, vagy az objektumorientált programozói technikákkal felépített szoftveres hullámformák által biztosított interoperabilitás.

A civil cégek által fejlesztett szoftver-vezérlésű rádiók nem csak a katonai igényeket fedik le: napjainkban a készenléti és a civil szektor számára is kínálnak nívós alternatívákat a kommunikációs rendszereik fejlesztéséhez, kialakításához. Ezt mutatja be az 1. táblázat, amelyben az alkalmazási terü-

letek szektoronkénti elkülönüléseit emelem ki. Az egyes területeken megjelenő speciális szolgáltatások a katonai szektor számára tervezett készülékeknél a leglényegesebb: az itt alkalmazott hullámformák száma egy nagyságrenddel nagyobb (számszerint 32), mint az egyéb kategóriák készülékeinél alkalmazottak, és ez járul hozzá a fejlett interoperabilitás biztosításához.

A JTRS rádiók jellemzői

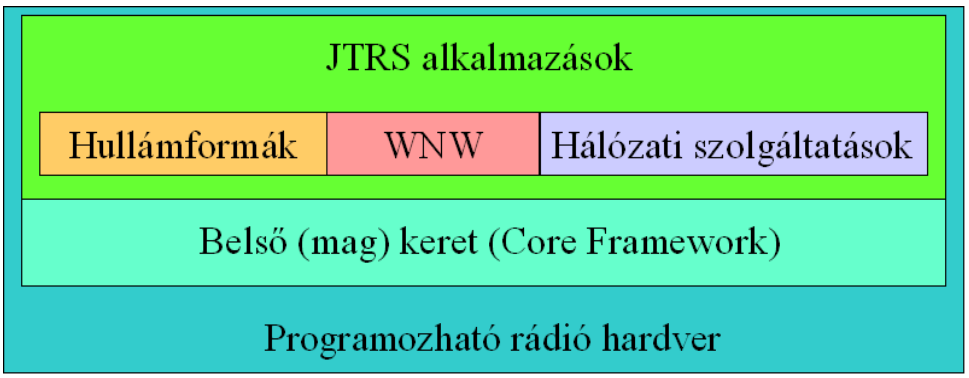
A sikeres szoftverrádiós kísérletek nyomán és a katonai műveleti doktrínák új meghatározásai alapján került kialakításra az összhaderőnemi harcászati rádiórendszer (JTRS), amely azért a katonai szlengben a "Jitters", vagyis „cidrizés” néven híresült el. A rádiócsalád, amely a 2 MHz – 2 GHz (terv a 3 GHz-ig való kiterjesztés) közötti sávban szolgáltat hang-, adat- és videoátvitelt az összhaderőnemi műveletekben, az alábbi kihívásoknak felel meg:

- Moduláris felépítés, rugalmas fejleszthetőség;
- Méretezhetőség – további sávszélesség és csatornabővítés lehetősége, nagyobb teljesítmény;
- Új technológiák beilleszthetősége: új processzorok, új hullámformák;
- Gerinchálózat kompatibilitás, illeszkedés a nagysebességű hálózatokhoz;
- Rádiócsalád, amely a légierő, a haditengerészet, a szárazföldi csapatok kommunikációs támogatásán túl fix állomásként is képes üzemelni;
- Interoperabilitás, intraoperabilitás, vagyis nemcsak a szövetséges rendszerek közötti szolgáltatásnyújtás és fogadás, de a haderőnemek közötti egységes felhasználás a követelmény;
- Hálózati szolgáltatások, adatforgalom irányítás.

A JTRS működése a szoftver érintkezési környezetre (Software Communica-tions Architecture, SCA)38 épül. Az SCA egy nyitott, szoftveres keretrendszer, amelyben a hardver és szoftver elemek harmonikusan üzemelhetnek, felhasználva egymás szolgáltatásait: a programozható hardverbe betölthetők a hullámformák, szoftveres alkalmazások futtathatók, és lehetőség nyílik a hálózatkialakításra. A nyitott keretrendszer adja meg a lehetőséget, hogy a szabványos interfészeken keresztül a hullámformák a többcsatornás üzemelést biztosító, párhuzamos felépítésű hardver egységeken egyidőben megjelenjenek.

[38] A szoftver érintkezési környezet 2000 óta folyamatos fejlesztés alatt áll, 2004. augusztusában már a 3.0 változat is kialakításra került, de ennek instabilitása miatt jelenleg a 2.2-re történik a fejlesztés.

Az 1. ábra szerint a szoftver érintkezési környezet (SCA) magában foglalja a belső (mag) keretet (Core Framework), amely a nyitott elven felépülő réteg-interfészeivel és szolgáltatásaival szabványos üzemeltetési környezetet biztosít a hardver és szoftver rétegekben futó alkalmazásoknak. A szoftveres alkalmazások magukban foglalják a hullámformákat, köztük a szélessávú hálózati hullámformát (Wideband Networking Waveform, WNW), és a hálózati szolgáltatásokat.



1.ábra: A szoftver érintkezési környezet elvi rétegződése. (Forrás:[2])

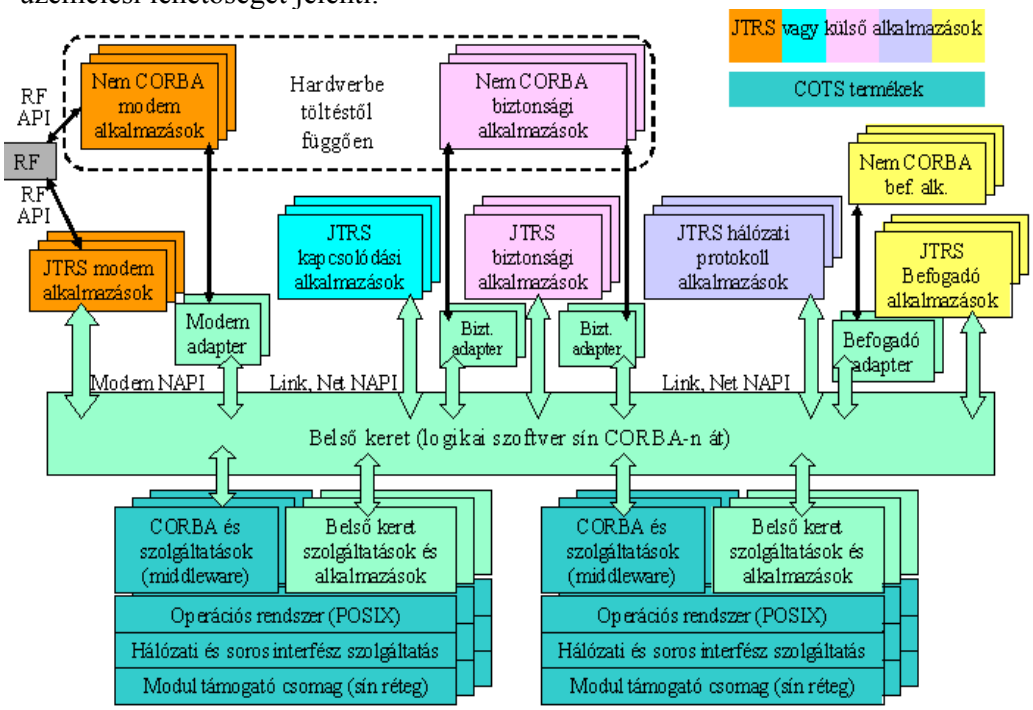
A szoftveres hullámformák hardvertől történő elszigetelésére a JTRS-nél három, virtuálisan önálló réteget alakítottak ki a tervezők (2.ábra): a processzor környezeti réteget (amely lényegében a hardver réteg), egy átmeneti réteget39, amely biztosítja a közös hardver-szoftver üzemelési környezet kialakítását, és a belső keret (Core Framework) réteget, amely egy logikai szoftveres adatsín. Ezen utóbbin keresztül csatlakoznak a futtatott szoftverek (a modem, a biztonsági, titkosítási alkalmazások, a kapcsolódási alkalmazások, a hálózati protokoll alkalmazások, és a befogadó alkalmazások) a hardverelemekhez.

A 2. ábra alsó részén a processzor környezeti (hardver)rétegek kerültek ábrázolásra. A modul támogató csomag (adatsín réteg) a működési környezethez való csatlakozást támogatja, amely magába foglalja a hibaellenőrzési és hibajavítási eljárásokat is. A lehetséges adatsínek: a PCI, a CompactPCI, a Firewire (IEEE-1394 szabvány szerint) és az Ethernet.

A hálózati és soros interfész szolgáltatás a soros és hálózati fizikai interfészeket támogatja: RS-232, RS-422, RS-423, RS-485, Ethernet, és 802.x. csatlakozók formájában. Ezen interfészeken számos hálózati protokoll használható.

[39] Ezt angolul middleware rétegnek nevezik. Szerepe egy logikai szoftveres adatsín létrehozása a nyílt felépítésű megosztott jelfeldolgozáshoz, mely a közös objektum kérés-közvetítés teljesítésének (CORBA) felépüléséhez kell.

Az operációs rendszer rétegnél a „hordozható” operációs rendszer interfész (Portable Operating System Interface, POSIX) egy elfogadott ipari szabványon alapul. A hordozhatóság jelen esetben a közös platformos üzemelési lehetőséget jelenti.



Rövidítések: API Application Program Interface; CORBA Common Object Request Broker Architecture; NAPI Network API; COTS Commercial-off-the-shelf;

2 ábra: A JTRS szoftver érintkezési környezetének rétegei. (Forrás:[3])

Az átmeneti (middleware) réteg az alkalmazások és a hardverelemek között helyezkedik el. Lényeges szerepe, hogy elválasztja a hardverelemektől a szoftver entitásokat. Ez a réteg olyan szolgáltatásokat biztosít, mint a hozzáférés azonosítás, a hitelesítés, a hardver és a szoftver közötti információcsere, a biztonság, és az osztályazonosítás. Az átmeneti réteg teszi lehetővé, hogy a különböző számítógépes nyelven megírt szoftveres alkalmazások közös platformon is képesek legyenek futni.

Mivel a JTRS kialakításánál követelmény volt, hogy már meglévő termékekre épüljön, így a széles körben alkalmazott közös objektumkérés közvetítő architektúra (Common Object Request Broker Architecture, CORBA) termékeket használtak fel a belső keret (Core Framework) kialakításnál.

A rendszerfejlesztés nem mentes a nehézségektől, amelyek mind költségnövelő hatással vannak a programra. Például a fejlesztőknek ki kellett

alakítani egy hullámforma XML modellt, hogy a számos API alkalmazkodni tudjon a különböző rendszer elemekhez, és egyszerűen használhassa az adatszállítási mechanizmusokat.

A JTRS rádiók szolgáltatásai

A JTRS rádiókban megjelennek a digitális rádióknál már ismertetett szolgáltatások: a beszédátvitel és az adatátvitel különböző formái. A fejlesztések eredményeként viszont kibővül a szolgáltatások köre, fejlettebb vezetési-irányítási képességet eredményez a valós idejű videó és a szélessávú videokonferencia lehetősége, egységes harctéri kép alakítható ki (például harcászati internetben történő alkalmazásokban), fejlett hely- és helyzetmeghatározás válik lehetővé a beépített modulok által, és hozzáférést biztosít a különböző hálózatokhoz, így

- az internet protokoll (IP) alapú hálózatokhoz;
- a műholdas rendszerekhez;
- a tűz- és manővervezetési, illetve a funkcionális adathálózatokhoz.

Megnevezés	Jelentése	Alkalmazás
Hagyományos AM, FM és ezek változatai	A klasszikus rádió modulációs módok	Főleg civil rendszereknél (pl.: műsorszórás)
SINCGARS / SINCGARS SIP	Egycsatornás harcászati rádiórendszer és annak továbbfejlesztése	US ARMY szárazföldi haderő
PR4G	4. generációs harcászati rádiórendszer	Francia szárazföldi haderő
SEM 93	Harcászati rádiórendszer	Német szárazföldi haderő
Have Quick I. és II.	Lassú frekvenciaugratás (>100 hop/sec, esetleg néhány száz)	USA és NATO légi és tengeri erők
Saturn	Gyors frekvenciaugratás (<1000 hop/sec)	NATO légi és tengeri erők
JTRS egyes harcos és szélessávú hálózati	Összhaderőnemi harcászati rádiórendszer	Amerikai haderőnemek között (esetleg NATO)
FM3TR	Többsávos, moduláris rádió teszthullámformája	Szoftverrádió fejlesztésekben

2. táblázat: Példák a katonai hullámformákra.

A szolgáltatások stabil biztosításához az egyes rádiórendszerekre jellemző hullámformák kerültek kidolgozásra. Jellemző katonai hullámformákról ad tájékoztatást a következő táblázat.

A hullámforma fogalmára számos megfogalmazást alkalmaznak a szakemberek, attól függően, hogy milyen hardveres platformon vagy milyen alkalmazásban használják. A digitális rádiók vonatkozásában a hullámformát egy olyan digitális jelcsoportként értelmezem, amely magában foglalja a készülék-specifikus modulációs módot, a jelpolarizáció értékét, a forrás-

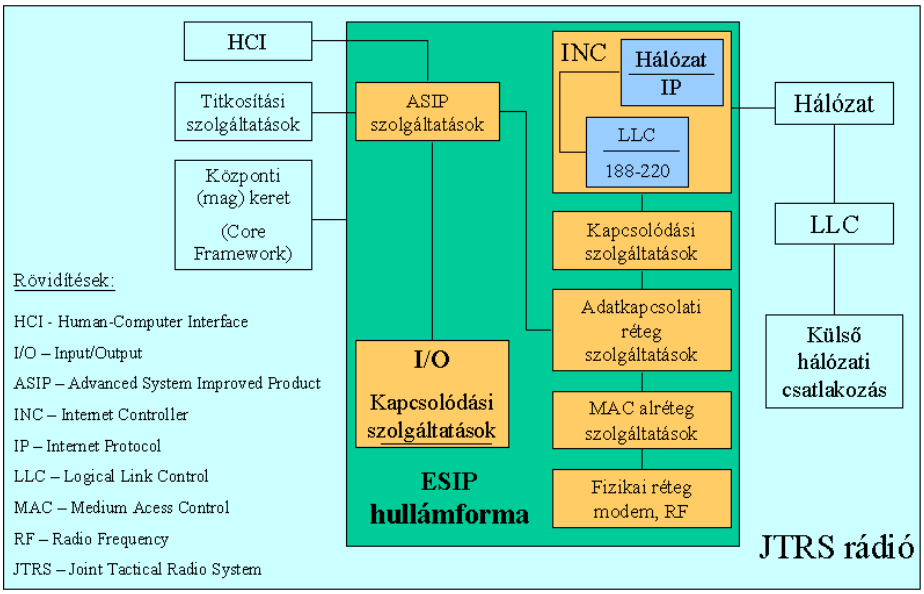
és csatornakódolást illetve dekódolást, a hibajavítást és az időzítési paramétereket.

A szoftverrádióknál alkalmazott hullámformák ezen túl magukban foglalják a bemenet /kimenet (Input/Output, I/O) interfész vezérlő információit, valamint a rendszer üzemeltetéséhez és az alkalmazások futtatásához szükséges adatokat is, amelyek szoftveres formában betölthetők a készülékekbe az alaphardver működtetéséhez.

Beszédátvitelnél a hangdigitalizálás paraméterei, a tömörítés mértéke; adatátvitelnél a beépített modem modulációs módja, a jelátviteli sebesség leírása, és számos egyéb paraméter meghatározása miatt a hullámforma igen tekintélyes nagyságú szoftvercsomaggá nőhet. Ennek igazolására egy szoftveralapú hullámformát mutatok be a továbbiakban.

Egy amerikai szoftverrádiós kutatásokat végző cég, az Assurance Technology Corporation (ATC) új hullámformát dolgozott ki a JTRS készülékek számára a harmadik generációs SINCGARS rádiókkal40 történő együttműködésre. A SINCGARS ASIP hullámforma már az objektumorientált technológiával került kialakításra és 33 önálló összetevőt integrál magába: az ember-gép interfész vezérlését, a titkosítást, a ki/bemenet (Input/Output, I/O) vezérlését, valamint a fizikai, az adatkapcsolati és a hálózati réteg szolgáltatásainak elérését és hozzáférési pontjainak vezérlését. A hullámforma a folyamatos fázisú frekvenciabillentyűzés (Continuous Phase Frequency Shift Keying, CPFSK) modulációval került kialakításra, 16 kbps adatátviteli sebességre optimalizálva, fix frekvenciás és frekvenciaugratásos üzemmódokban történő üzemelésre, használhatóvá téve a teljes frekvenciasávot (30 – 87,975 MHz) és az összes (2320 db) fix frekvenciaértéket. E mellett támogatja a helyi, a távvezérelt és az átjátszó állomás funkcionális üzemelési formákat.

40 A Single Channel Ground-Air Radio System (SINCGARS) rádiók 1988-ban kerültek rendszeresítésre, azóta három átalakításon estek át, felkészítve őket a szoftver általi üzemeltetésre.



ábra: A SINCGARS ESIP hullámforma blokkvázlata. (Forrás:[4])

A nyílt rendszerű kialakítás biztosítja a hálózatos képességeket: a hálózati hozzáférés vezérlésében megjelenik a harcászati internet hálózat egyik elemének, az internet szabályzónak (Internet Controller, INC) a vezérlési képessége. Ezzel a rádiórendszeren megjelenik a harcászati helyzetismeret kialakításának lehetősége, a fejlettebb vezetési-irányítási lehetőség, a hely- és helyzet-meghatározás, az internet protokoll (IP) alapú hálózathoz vagy a műholdas rendszerekhez történő hozzáférés. A hullámforma ezeken túl támogatja a MIL-STD 188-220 szabványú adatcserét (kifejezetten erre lett kialakítva), ami által megvalósul a hadsereg tűzvezetési hálózatának (Fire Control Net) kialakítása, a légierő HAVE QUICK rendszereivel való együttműködés, és a haditengerészet adathálózatához való hozzáférés.

Név	**Alkalmazás / Frekvencia** [MHz]			**Adatátviteli sebesség** üzemmódok		
	Land Warrior rendszer	UGS és intelligens lövedékek	UAV és UGV	Harci kommunikáció	Elektronikai hadviselés	LPI/LPD[41]
Soldier Radio Waveform	450 – 1000 és 1350 – 2700	225 – 450	1350 – 2700	450 Kbps – 1,2 Mbps	2 Kbps – 93,8 Kbps	2 Kbps – 23,4 Kbps

3. táblázat: Az egyes harcos rádiós hullámforma jellemzői. (Forrás:[5])

[41] Kis valószínűséggel elfogható adású (Low Probability Interception, LPI) és kis valószínűséggel érzékelhető (Low Probability Detection, LPD) üzemmódok.

A JTRS rádiórendszerben használt készülékek interoperabilitási képessége döntően a *szoftveralapú hullámforma* kifejlesztésén alapszik. A szoftveralapú hullámforma nemcsak a rádiófrekvenciás jeleket foglalja magában, hanem a rádió egységek működtetését is a felhasználói bemenettől a rádiófrekvenciás kimenetig, illetve a vett jelek érzékelésétől és feldolgozásától a felhasználónál történő megjelenítésig.

A Védelmi Kutatások Ügynökségénél (Defense Advanced Research Program Agency, DARPA) a kis létszámú harci egységek harcászati helyzetismeretének kialakításához egy új szoftveralapú hullámformát alakítanak ki: az egyes harcos rádiós hullámformát (Soldier Radio Waveform, SRW). A hullámforma üzemmódfüggő, ahogy az a következő táblázatból is kiderül.

A fejlett videoátvitelre és a videotelekonferenciára a szélessávú hálózati hullámformát (WNW) fogják alkalmazni, amely szintén fejlesztés alatt van. Ennek főbb jellemzői:

- Teljes multimédia képesség: folyamatos hang, adat és video;
- Igény szerinti, automatikus hálózat átkonfigurálás;
- Támogatja az IP routingot;
- Támogatja a független többszintű titkosítást.

A tervek szerint a JTRS hálózati szolgáltatások egymástól eltérő rádiókörnyezetben is üzemelni fognak (például: ad-hoc hálózatok, strukturált hálózatok). A szolgáltatás minőség (Quality of Services, QoS) a mobil felhasználóknál ugyanúgy meg fog jelenni, mint egy vezetékes, nagysebességű hálózatot használva.

A hálózati szolgáltatások között megjelenik az útválasztás (routing). Mobil ad-hoc útválasztás, hagyományos útválasztás és globális csatlakoztathatóság formájában az autonóm rendszer határai közötti csomagátvitel útválasztás (inter-domain routing) vagy az autonóm rendszeren kívüli csomagátvitel útválasztás (internal routing) között lehet választani. Ugyanakkor lehetőség lesz a sávkorlátozásos vagy a sávkorlátozás nélküli mobil kommunikációs környezet kiválasztására.

Az azonosítás és hitelesítés funkció biztosítja a globális hálózathoz csatlakozott felhasználó azonosítását (és annak helymeghatározását a hálózaton), de a topológiától független lokalizálás is programozható a földrajzi adatbázis felhasználásával.

A JTRS hálózatmenedzsment tudásalapú, távszabályzott hibaelhárítást és diagnosztikát tesz lehetővé akár a harcmezőn is, kezelve a felügyeletnélküli csomópontokon üzemelő eszközöket, valós idejű átkonfigurálást téve lehetővé, az elosztott elemek konfigurációs adatbázisainak felhasználásával. Az interfészeken működő mobilitást biztosító protokollokkal a végfelhasználók helymeghatározásán túl a mobilitási információk regisztrá-

lása is lehetővé válik a választható központosított, az elosztott vagy a többszörös kötésű (multi-tiered) regisztrációs struktúra formájában. A dinamikus szoftver-frissítési lehetőségek mellett valós idejű hálózati és felhasználói statisztikák jeleníthetők meg, a mobilitási információk regisztrálása és a dinamikus IP cím kiutalási képességekkel együtt. A hálózat összes menedzserénél egy valós időben frissített, közös hálózati kép jelenik meg, amelyből a hálózat minden eleme behatárolható és távfelügyelhető, de a rádiókészülékek konfigurációs információi is elérhetők. A hálózattervezéshez olyan menedzsment eszközök kerülnek kidolgozásra, amelyekkel a felhasználói igények függvényében a frekvenciasáv kiterjeszthető/csökkenthető, elérhetők a hálózati és útválasztó információk, a biztonsági előírások, a hullámforma változatok, a küldetés-specifikus követelmények, a prioritások és a rendszerkorlátozások.

Az előbb felsorolt képességek eddig csak az állandó telepítésű hálózatoknál voltak biztosíthatók, a mobilitást támogató protokollok használatával a JTRS rendszerekben mindez már mobil környezetben is megvalósíthatóvá válik.

A JTRS fejlesztési programjában a rádiók kialakításánál a miniatürizált formára törekednek és különböző csoportokba kerültek besorolásra.

Csoport	**Felhasználó**	**Rádiótípus**	**Frekvencia** [MHz]	**Fejlesztés kezdete**	**Új hullámforma**
Cluster 1	Szárazföldi haderő	Kézi, háti, járműbe épített	2-30; 20-600; 1350-2700;	2006	WNW
Cluster 2	Különleges Műveletek Parancsnoksága	Kézirádió	30-512;	2005	SRW
Cluster 3	Haditengerészet	Fedélzeti rádiók	n.a.	2008	WNW
Cluster 4	Légierő	Fedélzeti rádiók	n.a.	2006	WNW
Cluster 5	Szárazföldi haderő (Land Warrior)	Moduláris, többcélú felhasználás	450 -1000; 1350 - 2700;	2006	SRW

4. táblázat: A JTRS rádiók csoportosítása a fejlesztésekhez. (Forrás:[6])

A Cluster 1 csoportba tartozó rádiók nemcsak a földfelszíni platformokra készülnek, hanem az Apache, Chinook és Blackhawk helikopterekbe is beépítésre kerülnek, valamint a Légierő Harcászati Légiirányító részei (Air Force Tactical Air Control Party) is ilyen eszközöket kapnak.

Az 1. csoport (Cluster 1) szoftverrádió tervezett képességei:

- Interoperabilitás biztosítása a jelenlegi rádiókkal, a JTRS változatokkal;
- Hálózatosítás a jelenlegi hullámformákkal és az új szélessávú hálózatos hullámformával (Wideband Network Waveform, WNW);
- A rádiók többféle hullámformás üzemelése, a kézirádióknál 6, a hátirádióknál 10 hullámforma memóriában való tárolása;
- Többszintű titkosítás és programozható titkosítási algoritmusok.

A 2. csoport (Cluster 2) fejlesztése a THALES gyártotta AN/PRC-148 típusjelű kézirádión alapul, míg az 5. csoport (Cluster 5) kis méretű rádiói a tervek szerint olyan rendszerekben is használhatók lesznek, mint

- a felügyelet nélküli földi szenzorok (Unattended Ground Sensors, UGS);
- a pilótanélküli repülő járművek (Unmanned Aerial Vehicle, UAV);
- a felügyelet nélküli földi járművek (Unattended Ground Vehicles, UGV);
- az intelligens lövedékek (Intelligent Munitions);
- a hálózatos tűzösszpontosítás (Network Fires, Netfire).

A 3. és 4. csoportba tartozó rádiók fejlesztése még várat magára, de a legutóbbi hírek szerint ez a program kibővült egy új irányvonallal, amelynek során a Légierő-Haditengerészet stabil átjátszóállomásai is kiegészülnek a JTRS készülékekkel.

Összefoglalás

A napjaink gyakorlatában megjelenő szoftver-vezérlésű rádiók a fejlett szolgáltatásaikat csak egy stabilan működő üzemelési környezetben képesek maximálisan felkínálni a felhasználóknak. A szolgáltatások hatékony kihasználásához, a kommunikációs képességek fejlődéséhez az alábbi jellemzőket célszerű kialakítani:

- *Digitális harcmező*. Lényeges, hogy a kommunikáció mind függőlegesen (vezetés), mind vízszintesen (együttműködés) megvalósuljon.
- *A műveletek maximális információval való ellátása*. Hang-, adat- és lehetőleg videoszolgáltatás a harc, a művelet minden fázisában, előreprogramozott, zavarásmentes üzemmódokban.
- *A kommunikációs eszközök gyors hordozóeszközökbe építve*. Gyors előrevonás után rövid idejű telepítés, és gyors kommunikációs csatorna átadás (a felhasználónak) lehetséges.

- *Önkonfigurációra képes rádiórendszerek*. Olyan eljárások kidolgozása, amelyek a bekapcsolás után automatikusan felépítik a szinkronizációt, azonosítják a felhasználói készülékeket, és stabilan üzemeltetik magát a rádiórendszert.
- *Maximális interoperabilitás*. A kölcsönös szolgáltatások biztosítása a stabil vagy gerinchálózati rendszerekkel, mindez szövetségi keretekben is (NATO közös műveletek).
- *Integrált hálózatmenedzsment*. A hálózat tervezés, konfigurálás, felügyelet fejlett szoftverekkel történik, rugalmas és gyors beavatkozási lehetőséget adva a kritikus helyeken.

A szoftver-vezérlésű rádiók, szoftverrádiók rugalmas rendszerkialakítási lehetősége előnyösen használható ki az új katonai, feladatorientált szervezeti változásokban, **mivel a felhasználói igények változásai, a szolgáltatási paraméterek sokkal rugalmasabban és egyszerűbben köthetők az esetlegesen megváltozó szervezeti beosztásokhoz (vagyis csak programozás kérdése).**

Felhasznált irodalom:

[1] David B. Cotton: Software defined radio looks to three market. COTS Journal January 2003. (Internetes letöltés: cotsjournalonline.com honlapról.)

[2] Software Communications Architecture (SCA). (Internetes letöltés: http://jtrs.army.mil/sections/technicalinformation/technical_SCA.html)

[3] Joint Tactical Radio System (JTRS) SCA Developer's Guide. Contract No. DAAB15-00-3-0001. Document Number: Rev 1.1. 18 June 2002. Prepared for the Joint Tactical Radio System (JTRS) Joint Program Office. (Internetes letöltés cím alapján.)

[4] SINCGARS ESIP. (Internetes letöltés: http://www.assurancetechnology.com)

[5] Joint tactical Radio System (JTRS) operational requirements document (ORD). Version 3.2. April 2003. (Internetes letöltés a jtrs.army.mil honlapról.)

[6] A JTRS rádiók fejlesztési terve. (Internetes letöltés: http://jtrs.army.mil/overview_clusters)

KASSAI Károly

AZ ELEKTRONIKUS ADATKEZELÉSSEL KAPCSOLATOS KOCKÁZATOK KEZELÉSÉNEK EGYES KÉRDÉSEI

A Magyar Honvédség (MH) szervezeteinek működését, vezetését támogató elektronikus adatkezelő rendszerek itthon és külföldön, önállóan telepítve, vagy más nemzeti és nemzetközi rendszerekkel összekapcsolva szolgálják a felhasználói igényeket. A kezelt adatok minősítési szintje, kezelési jelölései, illetve az üzemeltetési környezet, a különböző jogosultsággal rendelkező felhasználók, a rendszer-specifikus tényezők, illetve a szervezeti célok, erőforrások dinamikus változásai együttesen olyan halmazt képviselnek, ami felveti a kérdést: *mit lehet és kell az adatok és adatkezelő rendszerek elégséges védelmének tekinteni?* Hogyan lehet meghatározni azokat a tényezőket, amelyek kritikus fontosságúak a védelem szempontjából, és melyek azok, amelyek másodlagosak? Ki és milyen formában jogosult dönteni egy-egy fenyegetés vagy sebezhetőség kapcsán a védelmi rendszabályok erősítése, vagy könnyítése ügyében az anyagi források, vagy más szervezeti érdek alapján?

Az említett kérdések aktualitását a környezetben tapasztalható kihívások naponta jelzik. A közigazgatási rendszerek fejlődése, az internethez kapcsolódó szolgáltatások bővülő köre, illetve a hálózat alapú képességekre (network enabled capability; NEC) való törekvés támogatja az egyre bővülő igények korszerű kiszolgálását, ugyanakkor új kapukat nyit a fenyegetések és a sebezhetőség területein. Előre definiált védelmi rendszabályokkal képtelenség lefedni minden elképzelhető helyzetet, így nyilvánvaló, hogy a NATO, EU, és nemzeti adatokat kezelő rendszerek számára jogszabályokban és az állami irányítás egyéb jogi eszközei kategóriájába tartozó minimum biztonsági követelményeket meghatározó szabályozók mellett szükség van a kockázatok felmérésére, értékelésére és ennek megfelelően a védelmi rendszabályok specializálására. A vázoltak alapján aktuálisnak tekinthető a közigazgatás és egyéb fontos szervezetek működéséhez szükséges kockázatelemzésre vonatkozó kormányzati követelmények áttekintése, és az MH szempontjából lényeges kérdések rövid vizsgálata.

Az adatkezeléssel kapcsolatos általános kockázatfelmérő és elemző feladatrend kialakításához a következő jogszabályban megfogalmazott követelmények állnak rendelkezésre:

- a közfeladatot ellátó szerveknek az elektronikusan érkezett irat átvételét meg kell tagadni, ha az biztonsági kockázatot jelent a fogadó szerv számítástechnikai rendszerére (kockázatelemzésre vonatkozó követelményt a jogszabály nem azonosít); [1]

- a NATO, EU elektronikus adatkezelő rendszerek biztonsági rendszabályait a NATO (és NYEU), EU biztonsági követelményeire és a helyszíni kockázat értékelésre kell alapozni (a jogszabály a kockázatelemzést nem részletezi); [2]
- a közigazgatási hatóságok iratkezelésére vonatkozó követelmény szerint az informatikai célrendszer biztonsági kockázatait kétévente felül kell vizsgálni, és a kockázatokkal arányos védelmet kell kialakítani; [3]
- a Pénzügyi Szervezetek Állami Felügyeletének ajánlása szerint a pénzügyi szervezetek védelmi rendszabályai a biztonsági kockázatokkal arányosak legyenek, [4] a kockázatelemzést legalább kétévente felül kell vizsgálni, melynek során célszerű a COBIT42 módszertan vonatkozó fejezetét alkalmazni, [5]
- a KIETB43 24. ajánlás szűk hatáskörben, a szoftverfejlesztés területén határoz meg általános feladatokat;44 [6]

A felsorolt jogszabályban foglalt követelmények mellett a kockázatelemzésre vonatkozó leírás a még érvényben lévő Informatikai Tárcaközi Bizottság (ITB) 8. sz. ajánlásában olvasható. [7] Az 1994-es ajánlás alkalmazhatóságának elemzését mellőzve csak annyit emelek ki, hogy a feladatrendszer általános leírása mellé csatolt fenyegetés és sebezhetőség-lista az eltelt tizenhárom év alatt bekövetkezett technikai fejlődés alapján mindenképpen felülvizsgálatra szorul. Ez azért fontos, mert *a közigazgatási rendszerek és a kritikus infrastruktúra elemeinek szükséges mértékű biztonsága egységes védelmi elgondolás és a védelmi rendszabályokkal kapcsolatos kérdések azonos megítélése nélkül nem képzelhető el.*

Az ajánlás alkalmazásával kapcsolatban érdemes megvizsgálni két központi kormányzati rendszerre meghatározott, kockázatelemzéssel kapcsolatos álláspontot. Az egységes digitális rádió-távközlő rendszerre (EDR) vonatkozóan a szolgáltatók és a rendszerhez csatlakozó szervezetek számára kialakított biztonsági szabályzatban kockázatelemzésre vonatkozó követelmény nem azonosítható. [8] A jogszabály csak azt tartalmazza, hogy az EDR-re vonatkozó szabályozás szervesen illeszkedik a többi jogszabályokhoz és egyéb követelményhez.

A Központi Elektronikus Szolgáltató Rendszer esetében a biztonsági követelményeket meghatározó jogszabály szintén nem azonosítja a szolgáltató szervezetek és a rendszerhez csatlakozó alkalmazó szervezetek kockázatelemzéssel kapcsolatos feladatait, csak több alkalommal utal a „kockázatokkal arányos védelmi rendszabály”-ra. Egyedül a változáskezelésnél ol-

[42] COBIT: Control Objectives of Information and related Technology (nemzetközileg elismert és alkalmazott informatikára vonatkozó vizsgálati módszertan).
[43] KIETB: Kormányzati Informatikai Tárcaközi Bizottság.
[44] A kockázat azonosítása, értékelése, tervezés, követés és ellenőrzés.

vasható, hogy a változáskezelési eljárásnak kockázatelemzést kell tartalmaznia, de módszertani vagy egyéb feladat azonosítása nélkül. [9]

A fentiek alapján megállapítható, hogy az elektronikus adatkezelő rendszerekre vonatkozó különböző jogszabályok közvetetten említik a kockázatelemzés témakörét, de ezzel kapcsolatosan átfogó követelményeket nem állítanak fel. Amennyiben ez az ITB 8. sz. ajánlásban foglaltak megerősítését jelenti, a kiadástól eltelt idő alapján célszerűnek látszik a felülvizsgálat. Ezt azért is fontos, mert *a központi szolgáltatókhoz csatlakozó szervezetek nem pontosan meghatározott feladatok esetén csatlakozó alrendszereiknél a fenyegetettség és a sebezhetőség megítélésében eltérő eredményre juthatnak, ami az adott hálózaton belül eltérő szintű védelmi rendszabályokat eredményez* (a védelmi alultervezés felesleges kockázatot hordoz, a túlméretezés pedig erőforrás pazarlás).

A fenti elektronikus adatkezelő rendszerekre vonatkozó követelmények bemutatása mellett szükségesnek látom annak ismertetését, hogy a közigazgatási szervezetekre milyen általános kockázatkezelésre vonatkozó követelmények vonatkoznak. E szerint a költségvetési szerv vezetőjének kockázatelemzési rendszert kell üzemeltetnie. Objektív kockázatelemzési módszer alkalmazásával fel kell mérni a tevékenységben rejlő kockázatokat és meg kell határozni azokat az intézkedéseket (és megtételük módját), amelyek csökkentik, megszüntetik a kockázatokat. [10]

Az *MH (vagy más közigazgatási szerv) adatkezelésével kapcsolatos kockázatfelmérésre és elemzésre vonatkozó részletes kormányzati követelmény nincs.* Az általános követelményeket meghatározó jogszabály alapján kialakított MH kockázatelemzési szabályzat meghatározza, hogy a kockázatelemzési folyamatokat évente felül kell vizsgálni, és a változásokat a kockázat-nyilvántartásban át kell vezetni. [11] A kockázatelemzési szabályzat *külső*, *belső* és *tevékenységi* kockázatokra bontja a vizsgálandó területeket. A szervezeti kockázatokra vonatkozó feladatokon túl az adatkezelésre vonatkozó kockázatok felmérésére és menedzselésére irányuló feladatrend nincs részletesen kidolgozva.

Az említett ITB ajánlás mellett nemzetközi szabványokat és ajánlások alapján, [11] figyelembe véve más nemzeti ajánlásokat *az MH-nál az adatkezelésre vonatkozó kockázatelemzési feladatokat* a következőként tartom célszerűnek kialakítani (a feladat meghatározása és a *kockázatelemzés feltételeinek megteremtése* (elemző és értékelő csoport kialakítása, munkafeltételek biztosítása) után):

- A szervezet elé kitűzött feladatok, és az ehhez szükséges információs képességek (és a rájuk vonatkozó követelmények) azonosítása.
- A védendő objektumok meghatározása és értékelése. Az információs szempontból fontos objektumok számba vétele: kommunikációs vagyontárgyak (hardverek, szoftverek, információk), személyek (felhasz-

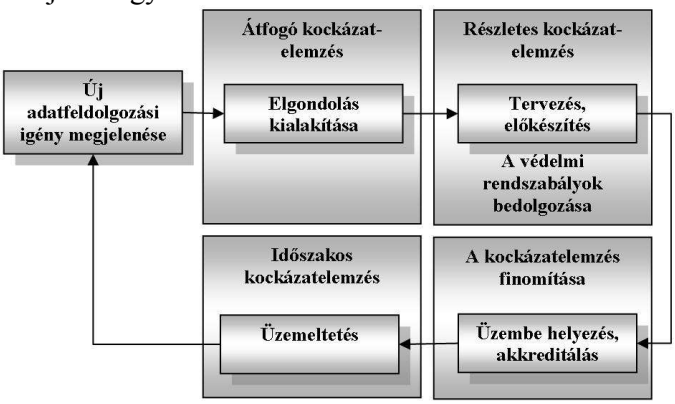
nálók, kiszolgálók és külső személyek), környezeti tényezők (épületek, létesítmények) és tevékenységek (műveletek). Az anyagi érték szerinti besorolással szemben a bizalmasság, sértetlenség vagy a rendelkezésre állás elvesztésének hatásának vizsgálatát részesítem előnyben (beleértve a helyreállítással kapcsolatos feladatokat is). Az értékeket elégségesnek tartom hármas skála szerint ábrázolni (pl. „alacsony", „közepes" és „magas").45

- A fenyegetettség megállapítása. A fenyegetések felmérése (és előfordulási valószínűségük meghatározása) gyakorlati tapasztalatokra támaszkodó fenyegetés-lista alapján, kiegészítve a helyi sajátosságokkal. A valószínűség a gyakoriság (a tapasztalatok, statisztikák), a motiváció (a lehetséges támadók által érzékelhető vonzerő és sebezhetőség, a rendelkezésre álló erőforrások) vagy a földrajzi tényezők (pl. ipari létesítmények közelsége, szélsőséges időjárási viszonyok valószínűsége) értékeléséből állítható össze, szintén hármas besorolás szerint.
- A sebezhetőség felmérése. A fenyegetésekhez hasonlóan összeállított sebezhetőség-listára támaszkodva hármas értékelési skálát alkalmazva a rendszerrel kapcsolatos sebezhető pontok számbavétele.
- A kockázati szint meghatározása. A sebezhető pontokra irányuló fenyegetések összerendelésével minden egyes eset kockázati szintjét meg kell állapítani. A vizsgálat azonosítja, hogy melyek azok a fenyegetések, amelyek nem irányulnak sebezhető pontra, illetve melyek azok a sebezhető pontok, amelyeket nem ér fenyegetés. Ezeket az ismétlődő kockázatelemzés során is ellenőrizni kell, mert változás esetén új tényezőként kerülhetnek be a kockázatmenedzsment hatáskörébe.
- A meglévő és tervezett védelmi rendszabályok azonosítása. Azonosítani kell a védelmi rendszabályokra vonatkozó követelményeket, a vészhelyzetekben alkalmazandó tevékenységeket, és a továbbfejlesztésre vonatkozó lehetőségeket.
- Javaslat a kockázatok kezelésére. Amennyiben a figyelembe vett fenyegetések, és a rendelkezésre álló védelmi lehetőségek között eltérés van, az illetékes vezetőnek dönteni kell, hogy a kimutatott kockázatokat elfogadja, vagy csökkenti (esetleg valamilyen módon áthárítja, vagy elkerüli). A védelmi rendszabályok által nem ellensúlyozott fenyegetésekre a szervezetnek működésfolytonossági, helyreállítási, szükség esetén vészhelyzeti terveket kell kialakítani.

[45] Hármas tagolást követ a nemzetközi ajánlások mellett az Egyesült Államok föderációs rendszereire vonatkozó irányelve is, de a szakirodalomban találhatók 4-6 fokozatú skálák is. Egy ausztrál kézikönyv pl. 7*6-os mátrixot alkalmaz a fenyegetések és bekövetkezési valószínűségek ábrázolásához, a spanyol nemzeti modell a fenyegetéseket tízfokozatú skálán jeleníti meg.

- A kockázatelemzési és menedzselési feladatok számtalan módszertan szerint feldolgozottak, *egységesen elfogadott nemzetközi, EU, vagy nemzeti módszertan nincs*.

A módszertani kérdéseket nem tárgyalva csak annyit emelek ki, hogy a vázolt kockázatelemzési folyamatnak az életciklust végig kell követnie,[46] dokumentáltnak kell lennie, és a kimutatott kockázatoknak, valamint ez alapján a meghatározott rendszabályoknak, feladatoknak az adatkezelésért felelős vezető jóváhagyásával kell rendelkeznie.



A kockázatelemzés beépülése az elektronikus adatkezelő rendszerek életciklusába

Kritikus fontosságúnak tartom a kockázatelemzést *az adatkezelő rendszerre vonatkoztatva komplexen végezni*, és nem az üzemeltetésben, alkalmazásban érintett szervezeti elemek között megosztani. A honvédelmi tárca szervei és szervezetei saját kockázatelemzési szabályzatukban megfelelő hatáskör hiányában nem képesek kezelni az MH érdekű, több szervezet által üzemeltetett és egyre több szervezet által alkalmazott központi infrastruktúra kockázati tényezőit. Emiatt *a központi elektronikus adatkezelő rendszerekre vonatkozó kockázatok kezelése érdekében szükség van a szervezet-centrikus feladatokról az érintett felek szoros együttműködésén alapuló rendszer-centrikus kockázatelemzésre való áttérésre. Ezt a meglévő belső rendelkezés kiegészítésével (vagy módosításával) kell kezdeni, a szakmai felső szintű követelményeket az információvédelem felső szintű szabályozására vonatkozó Információ Biztonságpolitikában kell meghatározni. A kockázatok feltárására, elemzésére és kezelésére vonatkozó általános formai és tartalmi követelményeket MH szintű szabályzatban kell kidolgozni.*

A központi szabályzatot a specifikus részletek meghatározása érdekében központi szakutasítással kell támogatni (pl. fenyegetés és sebezhetőséglista, módszertani kérdések).

[46] Egy szellemes brit megállapítás szerint a kockázatmenedzselés nem csak Karácsonykor, hanem a teljes életciklus alatt alkalmazandó.

A fenyegetések és sebezhetőség feltárásához nincs nemzetközileg elfogadott, egységes lista. A több mint tízéves nemzeti ajánlás frissítésekor a kezelhetőség, valamint az ismétlődések elkerülése érdekében egységes struktúrába kell önteni *a vizsgálati területeket, amit nemzetközi szabványok, jelentések, és más nemzeti ajánlásokra támaszkodva célszerű kialakítani, az MH esetében még a katonai sajátosságokkal kiegészíteni*. A kialakítás során a vizsgált rendszerelemek közé nem szabad még egyszer általános megfogalmazásban biztonsági célokat felvenni (pl. mint rendelkezésre állás), mivel azok fenyegetése vagy sebezhetősége *önmagában nem, csak valamilyen elemen (vagy azok halmazán) keresztül valósulhat meg*.

A listákat (adatbázisokat) *időszakosan felül kell vizsgálni*, különben a még érvényben lévő nemzeti ajánlás érvényességének és alkalmazhatóság dilemmája ismétlődik meg.

Felhasznált irodalom

[1] 335/2005. (XII. 29.) Korm. rendelet a közfeladatot ellátó szervek iratkezelésének általános követelményeiről, 25. §.

[2] 179/2003. (XI. 5.) Korm. rendelet a nemzetközi szerződés alapján átvett, vagy nemzetközi kötelezettségvállalás alapján készült minősített adat védelmének eljárási szabályairól, 2. §. (15.).

[3] 195/2005. (IX. 22.) Korm. rendelet az elektronikus aláírást lehetővé tevő informatikai rendszerek biztonságáról, együttműködési képességéről és egységes használatáról, 9. §. (1.).

[4] A PSZÁF elnökének 10/2001. számú ajánlása a pénzügyi szervezetek működésének biztonsági feltételeiről, 41. p.

[5] PSZÁF 3/2005. sz. útmutatója a pénztárak informatikai rendszerének védelméről, 2. p.

[6] A központi közigazgatási szervek szoftverfejlesztéseihez kapcsolódó minőségbiztosításra és minőségirányításra vonatkozó KIETB 24. ajánlás, 9. 7. p.

[7] Informatikai biztonsági módszertani kézikönyv, ITB 8. sz. ajánlás, 1994, 2. 1. p.

[8] 109/2007. (V. 15.) Korm. rendelet az egységes digitális rádió-távközlő rendszerről, 2. sz. melléklet, 3. p. Informatikai Biztonsági Szabályok

[9] 84/2007. (IV. 25.) Korm. rendelet a Központi Elektronikus Szolgáltató Rendszer és a kapcsolódó rendszerek biztonsági követelményeiről, 1. sz. melléklet, 7. 1. 2. p.

[10] 217/1998. (XII. 30.) Korm. rendelet az államháztartás működési rendjéről, 145/C. §.

[11] 14/2005. (HK 1/2006.) HM utasítás a folyamatba épített előzetes és utólagos vezetői ellenőrzési rendszer kialakításával kapcsolatos feladatokról, 5. §. (3).

[12] MSZ ISO/IEC TR 13335-3 Informatika. Az informatikai biztonság menedzselésének irányelvei szabvány, 9. fejezet

[13] MSZ ISO/IEC 27001:2006 Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények szabvány 4. 2. 1.

[14] ISO/IEC 2000-2 IT - Service Management, Part 2. Code of practice, szabvány. 6. 6. rész

RAJNAI Zoltán, KERTI András

AZ INFORMÁCIÓVÉDELMI SZAKÁLLOMÁNY TOVÁBBKÉPZÉSI RENDSZERE

Az információ védelem személyi biztonság kialakításánál nem elég, ha csak az információ védelmi szervhez kerülésekor figyelünk a megfelelő személyek kiválasztására, a jogszabályokban, NATO előírásokban előírt felülvizsgálatok, betekintési engedélyek megszerzésére, a képzések megszervezésre, hanem nagy hangsúlyt kell fektetni a szakállomány szakmai ismereteinek szinten tartására, továbbképzésére is. A kezdetben megszerzett ismeretek idővel megkopnak, a tevékenységek rutinszerűvé válhatnak, a technikai és jogszabályi háttér változhat. A személyi információ biztonság alkalmazás alatti célja: biztosítsuk, hogy az alkalmazottak legyenek tájékozottak az információbiztonsági fenyegetésekről és problémákról, felelősségükről, kötelezettségükről és legyenek felkészülve, hogy támogassák a szervezeti biztonsági politikát feladataik ellátása alatt, és csökkentsék az emberi tévedés kockázatát.[47] Ahhoz, hogy a megfelelő szintű tudatosságot, a biztonsági eljárásokban való képességet és az információ-feldolgozó eszközök helyes használatát biztosítsuk, célszerű egyrészt a jelenleg érvényben levő osztályos vizsgáztatási rendszert egy korszerűbb formában fenntartani, másrészt kialakítani egy folyamatos, ciklikusan ismétlődő továbbképzési rendszert.

Az osztályos vizsgáztatás rendszerének helyzete korszerűsítési lehetősége

Jogi háttér

Az osztályba sorolás rendszerének alapdokumentuma a 30/1999. (HK11.) HM utasítás az osztályba sorolás rendjéről. Ez az alapdokumentum az alapelveket fekteti le, a szakmai feladatokról nem rendelkezik. A bevezetőjében hivatkozott öt jogszabályból jelenleg már csak az 1996. évi XLIII törvény és a végrehajtására kiadott 140/1996. (VIII. 31.) kormányrendelet van érvényben. A 20/2002. (IV.10.) HM rendelet a Magyar Honvédség egyes beosztásaihoz kapcsolódó munkaköri követelményekről a 4§ (4) bekezdésében az osztályos fokozatokról megállapítja: „Az állomány azon tagjainak, akik a haditechnikai eszközöket közvetlenül üzemeltetik vagy vezetik, szakmai ismereteinek szintjét folyamatosan fejleszteni és osztályos fokozatba sorolással rendszeresen ellenőrizni kell.”

A híradó szakterületen dolgozók osztályba soroló vizsgáit a Honvéd Vezérkar híradó csoportfőnök 3/2000. (HK 7.) intézkedése „az osztályos

[47] Lásd: MSZ ISO/IEC 17799:2006 8. fejezet.

fokozatok követelményeiről, a követelmények teljesítésének, felmérésének rendjéről" szabályozza. A továbbiakban tehát tekintsük át a képzés és felmérés korszerűsítésnek legfontosabb feladatait. Ahhoz, hogy az osztályba soroló vizsgáztatás rendszere a kor színvonalának megfelelően tudjon működni, több feladat végrehajtása szükséges melyek közül kiemelkedő:

- A rendszer meghatározása

Az osztályba soroló rendszer a jelenlegi formában elavult, de ezt nem elvetni hanem korszerűsíteni szükséges. Ehhez a korszerűsítéshez új alapokra kell helyezni magát a rendszert is. Alapvetően szakítani kell a mechanikus, stopperórás mérési elveken alapuló szemlélettel, és sokkal inkább az elméleti alapok meglétének felmérésére kell alapozni, és ott ahol lehetséges, ezt az elméleti alapot kell felmérni a gyakorlati életben. Természetesen maradnak olyan a részterületek amelyek meglétének legjobb ellenőrzési módja az idő tényező felmérése, de nem szabad, hogy ez a szemlélet határozza meg rendszerét.

- Felelősség és illetékesség meghatározása:

Jogszabályban kell rögzíteni a különböző felelősségi köröket, jogokat és kötelezettségeket, mert a 30/1999. (HK 11.) HM utasításban szereplő szervezetek az átalakítás során megszűntek, vagy átalakultak.

- A kötelezettek pontosítása:

Kiemelten fontos, hogy nem a különböző MAK kódokkal jellemzett munkakörökhöz kell rendelni a vizsgakötelezettséget, hanem a feladatokhoz és eszközökhöz. Előfordulhat ugyanis hogy egy eszköz kezelését hosszabb időn át nem az oda kinevezett, beosztott állomány kezeli, hanem más MAK számmal számon tartott állomány (ilyen helyzet lehet pl.: létszám hiány, külföldi szolgálat). Ha a megszokott szisztémát követjük ebben az esetben a kezelő állomány nem osztályba sorolható. Ezért tehát az eszközökhöz, vagyis a tényleges kezeléshez kell kötni vizsgakötelezettségeket, és a vizsgakövetelményeket.

Az osztályos vizsga javasolt felépítése információ védelmi szakbeosztást betöltők részére

1. Általános biztonsági rész :

Az információvédelem területén dolgozó szakbeosztású személyek részére az alap ismereteket minden esetben szükséges az osztályba soroláskor ellenőrizni, mivel a különböző folyamatok végrehajtása nem lehetséges azok ismerete nélkül. Ennek a felmérési résznek az alábbi rész területeket célszerű érinteni:

- Ügyviteli, iratkezelési ismeretek

A beosztásból adódó feladatok mellett a szak állomány ismerje a szakügyvitel rendjét. Ez a készség csak úgy alakítható ki, ha a különböző dokumentumkezelési eljárásokkal a vizsgázó tisztában van.

- Fizikai biztonsági követelmények, és az
- Elektronikus biztonsági követelmények ismerete

Ahhoz, hogy a vizsgázó a különböző eszközök speciális fizikai és elektronikus biztonsági eljárásait tudatosan alkalmazni tudja szükséges, hogy az általános biztonsági követelményekkel, eljárásrendekkel tisztában legyen. Ezen ismeretek felmérésére azért is van szükség, mert az eszközök kezelőinek adott esetben egy parancsnoki döntés-előkészítő folyamatot is támogatnia kell, és ezt a feladatot csak alapos ismeretek meglétével teheti meg.

2. Eszköz ismereti rész
   - Eszköz speciális biztonsági, telepítési előírások ismerete

Mivel sok esetben azok az információvédelmi eszközök, amelyeknek a kezelését a vizsga során ellenőrizni szükséges, nem a vizsgázó kezelésében vannak, hanem számára a felügyelet és a különböző időszakos feladatok, beállítások végrehajtása a feladat, ezért nagyon fontos, hogy tisztában legyen az eszköz-specifikus követelményekkel.

- Eszközkezelési ismeretek

Az eszközkezelési ismeretek ellenőrzése során a tényleges eszközkezelési feladatokról tesz vizsgát a vizsgázó. Ebbe természetesen bele kell érteni mind a felhasználói, mind az eszköz-felügyelői feladatokat. Ebben a részben kell felmérni az eszközök esetében a vészhelyzetek során követendő cselekvési változatok felmérését is.

- Hibaelhárítás

Annak ellenére, hogy a korszerű berendezéseket már csak a gyártó cégek szervizelhetik, nagyon fontos, hogy a kezelő állomány felismerje a különböző hibaelhárítási feladatokat, amelyeket a helyszínen kezelni tud. Vagyis melyek azok, amelyeket felsőbb szintre jelenteni kell, és melyek azok, amelyekbe beleavatkoznia tilos.

A vizsga lefolytatásának gyakorlati megvalósítása

Javaslatunk szerint a vizsga végrehajtása 2 részből kell, hogy álljon. A vizsga végrehajtása előtt azonban lehetőséget kell adni az állománynak a felkészülésre, mely annál a katonai szervezetnél történik, ahol a vizsgázó feladatait végzi. A vizsgázók felkészülés-végrehajtása érdekében felkészülési kérdéseket és irodalom jegyzéket kaphatnak. A felkészülés során felmerült kérdések megválaszolására, konzultációra a vizsgát megelőző napon javasolt lehetőséget biztosítani. Mivel a vizsgázó a felkészülését a munkahelyén hajtja végre, ezért a vizsga előtti napon már csak a felkészülés problémás pontjaival kell és lehet foglalkozni. Nemcsak ismeret növelés, a problémás felkészülési kérdések megtárgyalása lehet tehát ennek programja, hanem egyfajta visszacsatolás: mi az, ami a végrehajtó állományt szak-

mailag foglalkoztatja, ami a napi életben illetve a felkészülés folyamán problémát okoz, okozott.

A vizsga tényleges végrehajtása:

Az általános biztonsági rész valamint az eszközismereti biztonsági telepítési előírások ismeretének ellenőrzése írásos vizsgafeladatok végrehajtásával történhet, míg a vizsga második részében a gyakorlati rész konkrét berendezések üzemeltetési, telepítési feladatainak felmérésére irányul.

Javaslat a folyamatos, ciklikusan ismétlődő továbbképzési rendszerre

Az információvédelem az egyik legdinamikusabban fejlődő szakterület, ahol a megszerzett tudás nem csak a felejtés miatt válik elavulttá, hanem az új tudományos és szakmai eredmények megjelenése, az újonnan megjelenő fenyegetettségekre adott válaszok, a jogszabályi, és NATO előírások változásai miatt is. Éppen ezért az információvédelmi alaptanfolyamokon megszerzett ismeretanyag bővítése, naprakészen, szinten tartása szinte életszükséglet. Ugyanúgy, mint ahogyan az információ védelmi engedélyek és bizonylatok is csak bizonyos időkorlátok között érvényesek, a megszerzett tudásanyag érvényességét is időkorláthoz kell kötni. A jelenlegi rendszerben a HM legfelsőbb szakmai szervezete által évi 1-2 alkalommal tartott továbbképzések nagyon fontosak és nagy ismeretanyagot fognak át, azonban az idő rövidsége miatt ezt a feladatot nem vállalhatják fel, ezeknek a foglakozásoknak a megtartása a javasolt továbbképzési rendszer esetén is szükségesek.

A javasolt továbbképzési rendszer két fő csoport részére kerülhet megtartásra, amelyből az egyik az információ védelmi vezető szakállomány, a második az információvédelmi beosztott szakállomány. Könnyen belátható, hogy míg az első állománycsoport inkább az információ védelem menedzselésével, vezetésével foglakozik, addig a második csoportnál sokkal jobban a feladatok gyakorlati végrehajtására kell koncentrálnia. A második csoportban szintén két alcsoportot célszerű kialakítani, mégpedig a számítógép- és hálózati biztonsággal foglalkozó szakállomány, illetve a rejtjelzéssel foglalkozó szakállomány alcsoportokat. Azonban ezeknek az alcsoportoknak a szakmai munkája nagyon sok helyen átfedi egymást, ezért a két alcsoport tanfolyami struktúrája esetenként azonos lehet a tematika, az eltéréseket a struktúrán belüli hangsúly eltolódások adhatják.

Elgondolás a továbbképzés tematikájáról

Mint arról már volt szó, az információvédelem folyamatosan változik, ezért célszerű a tanfolyamok tematikáját, óraelosztását időről-időre felülvizsgálni, korszerűsíteni (pl.: évente).

Így például az információvédelmi szakvezető állomány részére javasolt lehet az információ védelem irányításával foglakozó, stratégia döntéseket hozó állomány továbbképzésekor jellegében más ismeretanyag, tudásbázis oktatása mint azon személyek esetében, akik napi, esetenként csak rutinszerű feladatokat hajtanak végre. E területhez tartozhatnak

1. Általános alapismeretek amelyek magukban foglalják
   - Az információvédelmet érintő érvényben levő jogszabályok ismeretét, melyet indokol, hogy ma Magyarországon mindennek jogszerűen kell történnie, és a különböző cselekedetek is csak a jog tükrében vizsgálhatóak. Éppen ezért minden információ védelemmel foglalkozó szakember számára elengedhetetlenül szükséges az aktuális jogszabályok ismerete. Ez a megállapítás kifejezetten az információvédelem menedzselésével, irányításával foglakozó állományra kell, hogy vonatkozzon.
   - NATO direktívák, irányelvek, útmutatók ismeretét, mert a magyar jogszabályokra jellemző egy viszonylag nagy tehetetlenség, ami azt jelenti, nagyon lassan reagálnak a különféle változásokra, például a NATO információ védelmi előírásainak változására. Viszont hazánk kötelezettséget vállalt a NATO információinak NATO szintű védelmére. Éppen ezért a menedzsment állomány részére fontos a legújabb ez irányú NATO dokumentumok ismerete.
   - Információ biztonsági szabványok ismeretét. Bár a civil életben megjelenő szabványok alkalmazása önként vállalt, nem kötelező, ismeretük manapság már szinte nélkülözhetetlen az információ védelemben dolgozók számára. Ezek a szabványok egyfajta támpontot adhatnak a mindennapi munkához, az ismeretek alkalmazásához, adaptáláshoz.
2. A Magyar Honvédség információs infrastruktúrája

Az információvédelem nem egy önálló, l'art pour l'art szervezet, ezért nagy szükség van arra, hogy a rendszerszemlélet kialakuljon, az információvédelemmel foglakozó állomány tudja a helyét és szerepét az MH információs infrastruktúrájában.

3. Informatikai alapismeretek

Napjainkban a különböző informatikai rendszerek, rendszerelemek szinte naponta fejlődnek változnak, újabb és újabb szoftverek jelennek meg, amelyek valamilyen szinten hatással lehetnek a napi végzett munkára. Egyrészt ezeknek a szoftvereknek az ismerete, másrészt a rosszindulatú szoftverek, mobil kódok elleni küzdelem miatt nagyon fontos az informatikai alapismeretek naprakészen tartása. A tanfolyam idejét 60-80 órában

célszerű tervezni a Honvédelmi Minisztérium legfelsőbb szintű információvédelmi szervezetének vezetésével.

Elgondolás az információvédelmi beosztott állomány részére tervezett továbbképzésre

Az információ védelmi beosztott szakállomány gyakorlatilag a napi rutin feladatok végzésére szakosodott. Azonban ezeknek a feladatoknak a tartalma is idővel változik, melyet az ismeretanyag évenkénti felülvizsgálatával biztosítani kell. A tananyag alapvetően az információ védelmi alap és átképző tanfolyamokra támaszkodik, azok továbbfejlesztett, aktualizált változata. Ez alapján az alábbi témakörök oktatása célszerű:

- Információbiztonsági alapismeretek
- A nem minősített elektronikus adatkezelő rendszerek biztonsági előírásai.
- Minősített (nemzeti/NATO/EU) elektronikus adatkezelő rendszerek kialakítása,
- Rendszerüzemeltetési alapismeretek.

Szervezési kérdések

A fent vázolt képzési rendszerek tartalmi követelményeinek meghatározója egyértelműen a Magyar Honvédség legfelsőbb információvédelmi szerve kell, hogy legyen.[48] Ez azért fontos, mert ez a szerv az, amely „első kézből" kapja a vonatkozó információkat mind a szövetségesi rendszertől, mind a szakhatóságtól, és így a legszélesebb körű rálátása van a folyamatban levő eseményekre. A már meglévő tanfolyamok tapasztalatait és a szakmai elöljáró feladatszabását figyelembe véve a fenti tanfolyamok, osztályba soroló vizsgák lebonyolításában a ZMNE Híradó tanszék vállalhat nagy szerepet, így a

- Vizsga, illetve a konzultáció helyszínének biztosítását
- Az általános biztonsági rész kérdéseinek kidolgozását
- A vizsgáztatás koordinálását
- Vizsgabizottságokba tagok delegálását.

Felhasznált irodalom:

[1] MSZ ISO/IEC 17799:2006 Informatika. Biztonságtechnika. Az információ biztonság irányítási gyakorlatának kézikönyve.

[2] Talabos Tibor mk. ezredes előadása az információvédelmi továbbképzésen (Göd 2007. szeptember 21.)

[3] Kerti András őrnagy: Osztályba soroló vizsgáztatás in: Kard és toll, Budapest, 2007/2 pp: 108-114

[48] Amely jelenleg (2007. szeptember) az Informatikai és Információvédelmi Főosztály.

MODERNISATION PROCESS OF PUBLIC ADMINISTRATION SERVICES

Erik PÁNDI[49]

Preamble: The present publication – based on the wide-range opinion of experts dealing with this topic – outlines the status of domestic governmental reforms and the modernization of public administration services, during which in addition to mapping misinterpretation points, problems and dilemmas it also drafts alternative solutions to the questions concerning the alteration of the system being in the centre of public inquiry today.

Key words: electronic government, electronic public administration, information society

1. Dilemmas, aspects

In Hungary, the quality of the planning and operative activity of the government and that of the public sphere is based on the proper development pacing of information society. Modernisation (reforming) of public administration systems means first of all not only technological, but also organisational and approach-related tasks. The main purpose is not the informatisation itself, but the rationalization of the operative process of the system. Fulfilment of the requirements (commitments) prescribed by the European Union in principle serves the alteration process launched from upper decision making levels, however Hungary – *also based on the 2006 country-report of OECD* – is slow and sticky concerning the reform progress. Since the government-shift it seems, that the new governmental structure was set up in vain and it was also vain for the Hungarian strategies of information society to appear; without forming a more embracive and conscious practice there is no hope for any progress.

As for the real forming of e-government three basic initial aspects were set up in the countries more successful than Hungary, and in this way the following main tasks had been drawn up concerning the government:

[49] author: LtC Erik PÁNDI, Associate Professor at Zrínyi Miklós National Defence University

a) introduction and continuous development of modern information- and knowledge management solutions beyond information-technology solutions;

b) ensuring proper international interoperability;

c) acting as a „ government entrepreneurship", by applying and rotating various property elements rationally;

d) strengthening citizen's trust in public offices by setting up a client-focused service approach, where local administration centres and personal services are more active and emphasized;

e) new type of approaching and handling the public.

Taking the above fact into consideration, during the modernization of domestic public administration systems organisation and process shall be set up in a way, that in addition to the general quickening of economy it should set up new forms not damaging the various rules of competition on the one hand for the present and future dominant branch, for strengthening international competitiveness of Hungarian productive and servicing companies participating in the information- and science sphere. On the other hand as a strategic resource for public education, higher education, research and development and cultural fields and for considering these as investment targets and supplying priorities for this aim. Challenges of the information-technology era demand all-in alteration of the institutional system, by knowledge-management, installation of tenability demand on each level of planning and execution, furthermore with the forms of society justice and increasing equal chances adjustable to the requirements of the information-technology era.

2. Pressure of setting up electronic public administration

Expanding of client-connection systems, quick and simple forwarding of services to the citizens, service-provider's communication, furthermore the storing, forwarding, processing of data nowadays can be only solved with modern information- and communication technology tools. Modernisation of public administration systems embraces two inseparable fields:

a) supplier-side, that is modernization of procedures within public administration;

b) user-side, that is development of services in the connection of the client and the institutes of public administration.

Pursuant to the Act No. CXL. of 2004 (Ket.) on the General Rules of Public Administration Authority Action since November 2005 in Hungary

the clients do not have to visit various offices for data. If the data are included somewhere in the state of municipal data-bases, the citizen cannot be bound to acquire such data repeatedly. It is an urgent task therefore to work out a common platform, surface and standard solutions for the services used in several places, furthermore for the interior procedures taking part in the operation of every office and completing the same function. The preparation of rules and standards for the uniform handling of documents shall be continued, first of all in case of municipalities. Without modernisation on the supply side there is no hope for keeping the requirements of the above act (Ket.), it will be hopeless to expect client-focused user side services from civil administration.

In the European Union significant efforts are made for the realization of prompt measurability of the social-economic effects of projects aiming the electronic use of public administration. More than 5 % of the costs can be saved through electronic public administration, therefore the spreading of e-services is a really important question. On the user's side for the citizens and businessmen the most important advantage is the demand for quick and high quality, flexible services in connection with e-government services, that cannot be performed on paper by any huge organisation.

In Hungary the Tax Authority /APEH/ is the leader by the introduction of e-taxation, which is well arranged. The trouble is caused mainly by other (municipality, social insurance) systems, the introduction of electronic services there would mean beneficial force on the citizens for using and learning on-line services.

3. Obstacles

Modernisation process of public-administration services is basically impeded by the following factors in Hungary:

a) slight foresight on the side of public administration and political fields;

b) lack of citizens' awareness;

c) resistance of public servants;

d) deficiency of recognising citizens' demands;

e) low level of knowledge management and human resource development and education in the public administration sphere;

f) the lack of wideband connection;

g) un-coordinated development of back-office and front-office procedures, lack of interoperability;

h) unsatisfied interest and demand of the middle-aged and those living in small regions;

i) weak digital literacy;
j) unknown digital signature.

Slight foresight on the side of public administration and political fields is demonstrated by the feature, that modernisation of public administration systems does not emphasize the importance of electronic public services, means and facilities, however, for reaching the above mentioned purposes information and communication tools (ICT) are called for assistance in every developed country. Significant lag can be observed even in those cases in Hungary, where otherwise the Parliament legislates with exemplary prevision. The Act on the independence of electronic information is such, which is only executed by a few ministries in practice. The task seems to be simple, public administration only has to comply with the related law.

Lack of citizens' awareness means, that in Hungary more than half of the adult people think that digital services do not give any important, required possibility. The proportion of those having little direct contact with the basic system of the information society, with the internet has been slightly decreased for years. More than half of the people not using the web either live in such house, where there is no internet connection, computer or any person using the internet either. Most of the people no using the internet were never tried to be convinced, that it would be beneficial for them. The creation of the demand shall be assisted, it could by reached by – *possibly* – free or discount price education and by developing the human factor of the information society.

Resistance of public servants can be practically observed in each member-country, additionally this phenomenon is present with more or less intensity. Nowadays the number of public service workers is by 200 thousand less than it was in 1988. The number of employees in the public offices sphere decreased by 300 thousand, at the same time the number of employees in the public authority sector increased by 150 thousand persons. Consequently fulfilment of multiplied tasks is mainly managed by increasing the number of employees, instead of rationalizing the procedures on the servicing side. Little attention is paid to the fact, that information procedures in public administration mean first of all the modernisation of organisational procedures, making them more rational, which in several cases requires more changes in attitude, culture and work organisation. This process is much longer than the installation of an information-technology system, therefore it is worthy to focus on this field.

Deficiency of recognising citizens' demands is obvious, as no research or surveying were executed. The country fulfils the current requirement for the provision of 20 the electronic availability of minimum public

administration services prescribed by the European Union relatively well. Right now citizens' user demands and expectations, that would be a base for the elaboration of development programs, determining the main direction and priority of them are unknown in Hungary. At the same time in the EU the conception of the recipient e-administration has emphasized priority, with the aim that the needs of users shall be taken into consideration much more than before.

At present in Hungary public administration is featured by **low level of knowledge management and human resource development and education**. Comprehensive public administration reforms (New Public Management) are emphasized in the last decades both in the developed and in the developing countries. Rationalisation and practical reorganisation of public administration and governmental work make possible and even urge the adaptation of experience (aspect, models, expectations) from knowledge management in the civil sphere. Modernisation of governmental activities and the supporting of new structural culture, technological development programs, new methods of management can be only reached through a knowledge-base change process due to the complexity of subjects to be handled. Managing the content of services to be rendered for citizens, furthermore the setting up of one-gate e-governmental services requires effective division of data, information and knowledge and co-operation too between the various offices and also between the individual members. The reforms for the rationalisation and cutting of operational costs in the public administration work urge the screening and eliminating of existing overlaps and redundancy in the activity of the offices. For the above purposes the setting up of a uniform and at least compatible technological platform and central co-ordination are inevitable. Public utility data are produced at public organisations as a kind of data-property, that could be also used in the business sphere and the utilization of such data could be important for both market participants and for the public sphere. Fulfilment of the requirements of the former triple challenge could be assisted properly through the deep monitoring and drawing up of the present status of governmental information and knowledge management, based on this survey governmental knowledge management strategy could be elaborated.

The absence of wideband connection is perhaps the most obstacle to the modernisation progress. The directions of the European Committee are obvious for years as both the eEurope2005, and the i2010 emphasize the development of infrastructure required for joining wideband internet together with cutting the service prices affecting the spread of e-public administration services. On the level of end-users there is no competition between the internet providers and other technical facilities providing connection in most of the regions of Hungary. In case of small residential

places the situation is worse, as there was no break-through in the last years in the appearance of cheaper, alternative[50] technologies, however it would be the best solution for meeting the requirements of the EU directions. The spread of Wi-Fi, fibreglass and other alternative technologies has to be supported almost aggressively. Digital telecasting is also expected to develop in the near future, that could be efficiently used by local municipalities for communication with citizens. Preparations for this purpose could be executed already upon the setting up of proper services.

Taking action without harmonisation is a permanent trouble in Hungary. U**n-coordinated development of back-office and front-office procedures, the lack of interoperability** is only a field of this feature. As for the future, the forcefully separated central and municipal parallel electronic procedures have to be harmonised. Un-coordination in the development policy can be mainly observed in case of the development programs based on the division of EU funds, therefore the systems that cannot communicate with each other will cause troubles here too. The situation is the same with the parallel development of un-coordinated large systems. More than 40 e-municipality development programs were launched in Hungary, that mean milliards of HUF expenditure, though the on-line availability of public services in case of municipalities is still in initial stage. It is an enormous problem, that a part of the information-technology systems set up at local level will not be able to connect either the Client-gate or with each other, or even with the large state administration systems. These developments were beyond the authority of central state administration.

It is a trouble, that **the interest and demand of middle-aged citizens and those living in small regions is unsatisfied**, because against the low spread index of internet the higher application of e-administration services could be that leading industry, which would direct the concerned group towards the use of modern information-technology tools, or perhaps towards the investing into such devices. Almost half of the population consider electronic administration positively, 40 % of citizens being aware of the existence of electronic governmental and municipal services plan to try these services in the future. A forward-space in this field would be the supporting of such on-line public administration services,[51] which are highly concerned by the potential middle-aged and older users.

Weak digital literacy of Hungary is shown by the fact, that it is a negative leader of this field in the European Union. 57 % of the population has never used any information-technology tool, and two-thirds do not use

[50] Mainly using fibre optics or cordless
[51] E.g..: tax allowance

the internet either. In case of workplace computer using the situation is not better either. Only approx. 30 % of the employees use computer in their work in Hungary. The situation can be basically handled, as through workplace education most citizens can be reached.

Electronic signing is unknown to more than two-thirds of the population, but the remaining approx. 30 % does not know its definition either. The service was only used by not more than 2 % of the entire population. Most of the companies that do not use electronic signature, almost nine-tenth of them say, that there is no demand for such service in their company. Almost 65 % of the companies applying digital attestation keeps contact with the authorities through e-signature. For certain target groups[52] the provision of free digital signature could gear up mass introduction of the new service.

4. Modernisation outside the public sphere

Upon the application of ICT in the conservative Hungarian society there are several facilities to exploit positive outside effects and the emissive force can be also applied outside the public sphere. It can be for example the introduction of pioneering applications or the using of new assets. This direction can be efficiently amended with propagating the wide range of application of new ICT-tools, awareness raising. The success of the former could assist the increase in public trust for the new surroundings, the improvement of ICT-related safety and as a consequence indirectly the headway of e-economy.

Public administration and public services in general and the extension of electronic services providing direct benefits can assist the catching up of those digitally illiterate, and in this way social participation can be strengthened and the sense of responsibility could be also increased. It is a significant task of the modernization of public administration systems, however this duty is presently pushed into the background.

5. Summary

Due to recent economic-political decisions – *whether we like it or not* – Hungary became a country in the global economic region, that does not act prosperously in each field, therefore we had to *„enter”* the tight, sometimes pestering, permanent competition for the acquisition of investments in our

[52] E.g..: entrepreneurs, employees, university students

geographic region. In the global space the forces moving capital are for some consideration *„beyond any law”*, therefore those *„in need of something”* for necessity have to seek after the development of such interior surroundings, which assumes satisfactory public services. The application of ICT itself however does not improve governmental work, for successfulness it would be necessary that the introduction of new assets became an elemental part of the modernization of public administration and it requires the co-ordinated effort of each governmental institution and level. Since joining the EU Hungary has been developing significantly in this field, though we have to face new challenges in addition to the first encouraging and meritable technological developments.

Bibliography:

[1] Dr. Csáki Gyula Balázs: Környezetváltozás a közigazgatásban – szemléletváltozás nélkül, Infokommunikáció és jog III. évf. 13. szám melléklete, Budapest, ISSN 1786-0776, 2. oldal, 2006.

[2] Scenario Session Report – eGovernment Beyond 2005., http://europa.eu.int/information_society/activities/egovernment_research/doc/scenario_session_report.pdf

[3] Szittner Károly: Az elektronikus közigazgatás kezdetei Magyarországon, Magyar Közigazgatás LVI. évf. 3-4. szám, Budapest, ISSN 0865 736 X, 193-195. oldal, 2006.

[4] Dr. Várnay Ernő – Dr. Papp Mónika: Az Európai Unió joga, Budapest, ISBN 963-224-746-9, KJK-KERSZÖV Jogi és Üzleti Kiadó, 2005.

[5] Working paper on eGovernment beyond 2005 – an overview of policy issues, http://europa.eu.int/information_society/activities/egovernment_research/doc/working_paper_beyond_2005.pdf

[6] Z. Karvalics László – Molnár Szilárd – Pintér Róbert: Leszakadóban? Kormányzati reform és információs társadalom Magyarországon, Információs Társadalom VII. évf. 1. szám, Budapest, ISSN 1587-8694, 8-16. oldal, 2007.

NÉMETH András

SZOLGÁLTATÁSALAPÚ MŰHOLDAS HÍRKÖZLÉS VESZÉLYHELYZETI FELHASZNÁLÁSI LEHETŐSÉGEI

Bevezetés

Az emberi civilizációt fenyegető veszélyforrások számának globális növekedése, az érintett lakosság számának, illetve az okozott károk értékének emelkedése, egyre nagyobb erőfeszítést követel a helyi hatóságoktól, országos hatáskörű szervektől, kormányzatoktól és a nemzetközi szervezetektől egyaránt. A romló tendenciák elsősorban a klímaváltozás eredményeként egyre gyakoribbá váló szélsőséges időjárási jelenségeknek köszönhetőek. Korábban nem tapasztalt erejű viharok, hírtelen lezúduló nagymennyiségű csapadékok, árvizek, aszályok és erdőtüzek sújtják Európa és Magyarország lakosságát.

A természeti katasztrófák mellett fokozott veszélyt jelentenek a különböző terrorista szervezetek, illetve az általuk elkövetett támadások is, melyek jelentősen csökkentik az emberek biztonságérzetét, és gyakran közvetlenül fenyegetik nagyvárosainkat.

A katasztrófák megelőzése, az ellenük való védekezés és következményeik felszámolása fokozott együttműködést kíván az érintett készenléti és más résztvevő szervek, valamint gyakran a társadalom többi szereplője között. Az együttműködés, a védekezési munkálatok tervezése, szervezése, irányítása és vezetése nem képzelhető el korszerű, megbízható elektronikus mobil hírközlési rendszerek és eszközök nélkül.

2006. óta már Magyarországon is működik egy kifejezetten hatósági és kormányzati célokat szolgáló, a felhasználók számára egységes szolgáltatásokat, országos lefedettséget, valamint magas rendelkezésre állást kínáló készenléti rádiórendszer az EDR[53], amely normál időszakban és katasztrófahelyzetekben is biztosítja a szükséges mobilkommunikációs platformot, valamint szükség esetén az együttműködési híradást a kijelölt szervezetek számára. Az EDR a TETRA[54] technológián alapuló, a GSM[55]-hez hasonló, földi infrastruktúrára épülő cellás mobiltelefon rendszer, melynek elemei (bázisállomások, mobil kapcsolóközpontok, trönkvonalak stb.) ezáltal ki vannak téve mind a természeti, mind a civilizációs katasztrófák hatásainak.

[53] Egységes Digitális Rádiótávközlő Rendszer
[54] Terrestrial Trunked Radio
[55] Global System for Mobile Communications

Mivel a földfelszíni kommunikációs vonalak esetleges sérülése, hiánya katasztrófahelyzetben veszélyezteti a védekezési munkálatok vezetését, hatékonyságát, érdemes gondoskodni olyan alternatív megoldásról, amely ilyen esetben is biztosítja a híradás feltételeit. Cikkemben ezért a földi infrastruktúrától kevésbé függő műholdas rendszerekben rejlő lehetőségeket kívánom bemutatni.

Kommunikációs rendszereket fenyegető veszélyforrások

2004. december 26-án Szumátra nyugati partjai közelében elemi erejű (Richter skála szerint 9-es) földrengés rázta meg a Csendes óceán mélyét, melynek következtében több emelet magas hullámok indultak meg a délkelet-ázsiai partvidékek felé. Az egyre sekélyedő mederben feltornyosult víztömeg szökőárként tarolta le 12 ország partvidékét, csaknem 300 000 áldozatot követelve, és több mint 5 km mélységben elpusztítva többek között a teljes távközlési infrastruktúrát. A katasztrófa következtében megsemmisült földi hírközlési rendszerek mellett a kommunikáció biztosítására egyetlen lehetőség maradt volna, a műholdas telefonok alkalmazása. Mivel a térségben ilyen berendezések nem álltak rendelkezésre, csaknem egy teljes napot kellett várni az első telefonhívás létrejöttéig. Az INMARSAT[56], a „Távközlés Határok Nélkül"[57] karitatív együttműködés keretében, Sri Lankán nagysebességű műholdas vonalakat és koordinációs centrumot telepített, majd rövid időn belül hasonlókat hozott létre az ország több érintett településén is. A vonalak egy részét a mentésben résztvevők, másik részét a polgári lakosság használhatta. [1. p.25.]

A szökőárakon kívül számos más veszély is fenyegeti mind a stacioner, mind a mobil földi telepítésű hírközlő hálózatokat. Jelentős károsodást okozhatnak a földrengések, melyek a kommunikációs rendszerek trönkvonalainak szakadásával, a vezérlő rendszerek és kapcsolóközpontok, valamint a mobilrendszerek adótornyainak pusztulásával fenyegetnek (emellett az energiaellátó hálózat sérülése is okozhat károkat). A Magyarországot is érintő ár- és belvizek elsősorban a földben húzódó hírközlési és elektromos kábelekre jelenthetnek veszélyt (azokat beázással fenyegetik), ugyanakkor a rövid idő alatt lezúduló jelentős mennyiségű csapadék által felduzzasztott patakok is súlyos károkat okozhatnak, amennyiben az útjukba kerülő hidakat elmossák, így megszakítva az azon keresztülhúzódó vezetékeket és kábeleket. A globális éghajlatváltozás következtében hazai viszonylatban is jelentősen megnőtt a rendkívüli erejű viharok és nagyintenzitású csapadékok károkozásának valószínűsége. (A 2006. augusztus 20-ai tűzijátékot elsöprő budapesti orkánerejű vihar kitörését követően egyes

[56] International Mobile Satellite Organization (korábban: International Maritime Satellite Organisation)

[57] Telecom sans Frontiers

mobiltelefon szolgáltatók hálózata lokálisan hosszú időre használhatatlanná vált!) Ezen időjárási szélsőségek elsősorban a légvezetékeket, a mobiltelefon bázisállomások antennáit (bár ezek rögzítő mechanikáját nagy szélnyomásra tervezik) leszakadással, töréssel fenyegetik, azonban ilyen esetben is számolhatunk a kábelek beázásának következményeivel.

A természet elemi erői mellett egyre növekvő veszélyt jelentenek a terrortámadások és más civilizációs eredetű veszélyforrások. A hírközlő rendszerek (a mobiltelefon hálózatokat is ide értve), mint a kritikus infrastruktúra[58] részei stratégiai jelentőségűek az egyes országokon belüli és a nemzetközi gazdasági, társadalmi, politikai életben, és mindennapjaink elengedhetetlenül fontos részévé váltak. Ez a kommunikációs függőség jelenti az egyik legnagyobb veszélyt a modern társadalmakra és teszi vonzó célponttá különböző terrorista csoportok számára. Az információs terrorizmusnak nem csak eszköze, hanem céljai is lehetnek a kommunikációs infrastruktúra elemei, melyek működésképtelensége viszonylag gyorsan és akár hosszú időre is megbéníthatja teljes országok mindennapi életét, megrendítve azok gazdaságát, társadalmi bizonytalanságot okozva, félelmet keltve az emberekben. [2. p.187.]

Az információs támadásokat a végrehajtás módszere alapján két csoportba sorolhatjuk. A *fizikai támadások* egyes rendszerelemek megsemmisítésével, működésképtelenné tételével, míg az *információs támadások* (cyberterrorizmus) szoftveres úton „logikai rombolással" érik el, hogy adott területen ne legyenek hozzáférhetők a hírközlő hálózatok szolgáltatásai. Az első csoportba a hagyományos terrorizmus fegyvertárába tartozó – például robbantással végrehajtott –, a kapcsolóközpontok, bázisállomások, hálózatfelügyeleti- és vezérlőrendszerek, valamint az átviteli utak ellen irányuló támadások, vagy azok energiaellátását biztosító rendszerek „kiiktatása" tartoznak. [2. p.190.]

A második csoportba tartozó módszerek azt használják ki, hogy a 21. század hírközlő hálózatai globális rendszert alkotnak, számtalan kapcsolódási felülettel más távközlési, valamint informatikai hálózathoz (pl. internet), valamint hogy ezen hálózatok irányítása, felügyelete szintén számítógépes rendszerekkel történik. Ezekbe – az informatikai, vagy fizikai biztonsági rendszereket kijátszva – szoftveres, vagy hardveres úton behatolva lehetőség nyílik az adatbázisokban tárolt információk, manipulálására, hozzáférhetetlenné tételére (pl. előfizetői adatbázisok, azonosítók), vagy a rendszer vezérlésének megváltoztatására akár oly módon, hogy az egyes hardverelemek fizikailag is károsodjanak. [2. p.190.]

[58] Azok az infrastruktúrák, melyek rendeltetésszerű folyamatos működése elengedhetetlenül fontos a többi infrastruktúra működéséhez (pl. energiatermelő és ellátó rendszerek, köz-, és vasúthálózatok, repülőterek, kikötők stb.).

A kommunikációs rendszerek közvetlen támadása mellett azonban, súlyosabb problémát jelenthet, ha a kritikus infrastruktúrák közül a villamosenergia-ellátó rendszereket támadják a fent említett módokon. A hírközlő hálózat minden elemének működéséhez szükség van tápellátásra, melyet az energetikai hálózatból nyernek. Ennek tartós kiesése esetén a szünetmentes tápegységek lemerülését követően, a rendszerelemek működésképtelenné válnak. (Kivételt képezhetnek azok a stratégiai jelentőségű központok, amelyek saját biztonsági tartalék áramforrással, aggregátorral rendelkeznek. A mobil bázisállomások zavartalan működéséhez ezen eszközök nem állnak rendelkezésre.)

Az energiaellátó rendszereket azonban, nem csak szándékos támadások, hanem a növekvő energiafelhasználás is veszélyezteti, aminek következtében speciális időszakokban (pl. kiugróan alacsony, vagy magas hőmérséklet elleni védelemre használt elektromos fűtő és légkondicionáló berendezések tömeges alkalmazása esetén) kialakuló túlterheltség miatt akár kontinentális méretű üzemzavar is kialakulhat. Európai viszonylatban az egyes országok erőművei és hálózatai egymással összekapcsolva, nemzetközi szerződések alapján bonyolult szabályozási rendszert alkotva biztosítják a jelentős részben már liberalizált energetikai piac fogyasztóinak ellátását. Ez a komplex rendszer is sérülékeny, hiszen például valamely stratégiailag fontos erőműve, vagy szállítási vonala kiesik, a hálózat többi elemének növekvő terhelése továbbgyűrűzve újabb és újabb rendellenességeket generálhat, ami a folyamat végén a teljes rendszer összeomlását eredményezheti. Egy ilyen jelentős méretű üzemzavar napokra, sőt hetekre is megbéníthatja teljes országok, kontinensek mindennapi életét, a távközlés, közlekedés, termelés stb. ellehetetlenítésén keresztül. Ilyen eset történt például 2003. augusztus 14-én az Egyesült Államok és Kanada keleti partvidékén, és Olaszországban is több alkalommal előfordult hasonló jelenség, de a közelmúltban kiterjedtebb üzemzavarra is volt példa. 2006. november 4-én éjszaka a német villamos hálózatban keletkezett üzemzavar Németország, Franciaország, Spanyolország, Portugália, Olaszország és Belgium jelentős területein áramkimaradásokat okozott, amely meghaladta a fél órás időtartamot.

Az energiaellátó rendszerek meghibásodásának egyenes következménye, hogy az emberek információ iránti igénye megnő (segélykérés, családtagok, ismerősök, munkahelyek stb.), amit a távközlési hálózatok igénybevételével próbálnak enyhíteni. Mivel a mobiltelefon vált mára a legáltalánosabban elterjedt kommunikációs eszközzé, így ezek a hálózatok válnak a leggyorsabban működésképtelenné első időszakban a túlzott forgalmi igény által okozott telítődés, majd esetleg a bázisállomások akkumulátorainak lemerülése miatt. Ez a jelenség a készenléti rendszereket (EDR) is fenyegeti, bár azok rendeltetésükből adódóan ellenállóbbak, és a bázisállomások

kiesése esetén a készülékek még a hatótávolságukon belüli más terminálokkal tudnak közvetlenül kommunikálni akkumulátoraik lemerüléséig. (A készülékek a gépjárművek akkumulátorairól, valamint az aggregátoros tartalék áramforrásokkal rendelkező berendezésekről tölthetőek.) A következő áldozat a vezetékes hálózat, amin az emberek sikertelen mobil híváskísérletek után próbálnak információhoz jutni. Az internet elérhetetlenné válását követően a földi kommunikációs rendszerek már egyáltalán nem képesek megfelelni feladataiknak. Magyarországon ezt követően egy kialakuló veszélyhelyzet idején, az EDR nélkül semmilyen mobil hírközlő rendszer (a vezetékes zárt célú hálózatok egy részének vagy egészének működése még biztosítható a tartalék áramfejlesztőkről) nem áll rendelkezésre a védekezésben résztvevők vezetése, irányítása által generált forgalom lebonyolítására.

A legnagyobb probléma akkor jelentkezik, ha valamilyen katasztrófahelyzet idején következik be (akár azzal szoros, ok-okozati összefüggésben) a földi hírközlő rendszerek károsodása, hiszen ekkor jelenősen romolhatnak a védekezés hatékonyságát biztosító vezetés és irányítás kommunikációs feltételei. Problémát jelenthet például hogy gyakran az egyes mobil rendszerek bázisállomásai és antennái ugyanazokon a helyeken és infrastruktúrákon (pl. tornyokon) kerültek elhelyezésre, ami együttes (azaz több szolgáltató egyszerre történő) fizikai sérülésük valószínűségét jelentősen növeli. (A Magyarországon kiépített EDR rendszer antennái a T-mobile, míg máshol a BM[59] tornyain kerültek elhelyezésre.) Másik veszélyforrást a tartalék áramköröknek, a működőkkel azonos infrastruktúrán történő kialakítása jelenti, ami adott hálózaton belül mehet a működőképesség rovására kritikus helyzetekben.

A fenti hatások együttesen jelentkezve, egymás hatását erősítve képesek akár tartósan megbénítani minden földi hírközlő rendszert, ami nem csak a polgári lakosság, hanem a készenléti szervek híradását is ellehetetleníti.

Jelen állapotok szerint a magyarországi készenléti szervek nem rendelkeznek, olyan hírközlő rendszerrel, amely biztosítja akár a belső, akár az együttműködési híradást, a földi hírközlési infrastruktúra jelentős sérülése, meghibásodása, vagy üzemképtelensége esetén.

Ezeket a szempontokat figyelembe véve célravezető lehet a földi mobil távközlési hálózatoktól függetlenül is működni képes, alternatív kommunikációs lehetőség rendszerbe állítása, ami adott esetben gyorsan installálható tartalékként – ha jóval szűkebb keresztmetszetben is – képes biztosítani a veszélyhelyzeti híradást az ország egész területén. (Adott viszonylatban annál megbízhatóbb a kommunikáció, minél több alternatív platform áll rendelkezésre az információk továbbítására.)

[59] egykori Belügyminisztérium

Műholdas hírközlési szolgáltatások

Kutatásaim során arra a következtetésre jutottam, hogy a földi távközlési infrastruktúra sérülése, vagy üzemképtelensége esetén egyetlen olyan hírközlési platform létezik, amely képes rugalmasan alkalmazkodni akár gyorsan változó körülmények között is a védelmi/katasztrófavédelmi kommunikációs igényekhez. A globális műholdas kommunikációs hálózatokat felépítésük, rendszertechnikájuk, működési tulajdonságaik, valamint szolgáltatásaik alkalmassá teszik olyan komplex veszélyhelyzeti hírközlő rendszerek kialakítására, melyek tartalékként képesek a kieső kommunikációs csatornák egy részét vagy egészét helyettesíteni, pótolni.

Magyarországon jelenleg (1996 óta) a Magyar Honvédség rendelkezik bérelt műholdas és előfizetői kommunikációs csatornákkal, melyek nélkül külföldi kontingenseivel történő kapcsolattartása nem, vagy csak nehezen lenne biztosítható. (A hadműveleti területeken néha ezzel biztosítják az alegységek híradását is.) Az igénybe vett INMARSAT, Iridium és VSAT[60] szolgáltatások eddig igazolták a velük szembeni várakozásokat és folyamatos, megbízható kommunikációt biztosítottak[61].

A műholdas távközlési rendszerek segítségével bonyolultabb műveletek híradása is biztosítható, így alkalmasak akár katasztrófavédelmi feladatok kommunikációs támogatására is.

A műholdas szolgálatoknak csak egy szegmensét jelenti az űrtávközlés, amely a műsorszórás, és közcélú kapcsolt távbeszélő szolgáltatás mellett, magában foglalja az üzleti távközlési célokra kifejlesztett VSAT, illetve a mobilitást biztosító műholdas személyi hírközlő SCPS[62] rendszereket. Ez a két szolgáltatás csoport egymást kiegészítve lehetővé teszi a legkülönbözőbb célú, méretű és képességű komplex kommunikációs rendszerek kialakítását.

VSAT rendszerek jellemzői [3][4][6]

A VSAT elsősorban a nagyvállalati, illetve üzleti körök számára kifejlesztett űrtávközlési szolgáltatás, amely biztosítja az egymástól földrajzilag távoli telephelyek hírközlési és informatikai hálózatainak műholdak segít-

---

[60] Very Small Aperture Terminal

[61] A műholdas kommunikációs rendszerek sajátossága, hogy az összeköttetés meglétéhez közvetlen rálátásra van szükség a terminál és a műhold(ak) között. Bizonyos földrajzi adottságok mellett (Pl. magas hegységek, épületek árnyékában, sűrű erdőségben) nem, vagy csak kiegészítő eszközök, átjátszók segítségével lehet a szolgáltatásokhoz hozzáférni. Ez azonban elsősorban szervezési kérdés.

[62] Satellite Personal Communication System (más terminológiában: PSCS: Personal Satellite Communication System)

ségével történő összekapcsolását, illetve az egyes végberendezéseken különböző szolgáltatások elérését.

A VSAT rendszerek általános jellemzői a következők:

- három szegmensből állnak: vezérlő-, felhasználói- és űrszegmens (HUB, terminálok, műholdak);
- Az űrszegmenst az egyenlítő síkjában, 35786km magasságban keringő geoszinkron műholdak alkotják, melyeket a felhasználói terminálok transzparens ismétlőállomásként használnak egymás közti összeköttetések létesítésére;
- a földi terminálok antennáit elegendő egyszer irányba állítani és nem kell gondoskodni a műhold folyamatos követéséről;
- a pálya nagy földfelszíni távolságából adódik a jelentős késleltetési idő (föld-műhold-föld szakaszra: 238-278ms), ami a telefonösszeköttetések esetén zavaró hatású lehet, valamint a jelentős, 200dB körüli szabadtéri csillapítás, melyet az antennaméretekkel, és a beiktatott erősítéssel lehet ellensúlyozni;
- egyetlen műhold képes akár kontinensnyi területen szolgáltatások biztosítására, így néhány műholddal akár globális hálózat kiépítése is lehetséges;
- új végpont rövid időn belül (akár néhány óra) telepíthető és konfigurálható;
- a terminálok valamilyen többszörös hozzáférési metódus segítségével férnek hozzá az űrszegmens erőforrásaihoz;
- változatos hálózati struktúrák hozhatók létre: egyirányú/kétirányú/interaktív, pont-pont/pont-multipont, háló és csillagtopológiájú rendszerek;
- csillag topológiájú rendszerek esetén két terminál közti összeköttetés a HUB állomáson keresztül épül fel (több ugrás - nagy késleltetés);
- háló topológiájú rendszerek esetén két terminál közvetlenül a műholdon keresztül kommunikál egymással;
- kialakíthatók nyílt és zárt hálózatok egyaránt, melyeknél különböző a műszaki paraméterek megválasztásának szabadságfoka (kódolások, modulációk, adatsebességek stb.);
- az információátvitel minősége és rendelkezésre állása jól tervezhető illetve kézben tartható, valamint fölülmúlja a földi hálózatok megfelelő paramétereit (akár 10-12 BER, és 99,9% feletti rendelkezésre állás);
- a rendszerben alkalmazott hagyományos földi infrastrukturális elemek (mikrohullámú lánc, optika) csökkentik az eredő rendelkezésre állást;
- az egyes összeköttetések meghibásodása (amennyiben az nem a műhold fedélzeti berendezéseinek hardveres hibájának következménye) nem okoz más összeköttetésekre kiható hibát, továbbá a hibahely egy-

értelműen detektálható, ami csökkenti a karbantartásra fordítandó időt, a szükséges személyzet számát, növeli a rendelkezésre állást és gazdaságosságot;

- a távoli terminálok és a központi terminál között átjátszók nélküli közvetlen kapcsolat valósítható meg, így az összeköttetések felügyelete egyszerűen, akár központilag, akár a felhasználókhoz kihelyezve biztosítható;
- a nagytávolságú összeköttetések költsége a tranzitdíjaktól mentes, ami a szolgáltatás árának alacsonyabban tartását teszi lehetővé;
- szolgáltatások széles köre valósítható meg: adatgyűjtés, műsorszórás, transzparens hang- és adatkommunikáció, videokonferencia, interaktív kétirányú hang-/video-/adatszolgáltatások, bérelt vonali szolgáltatások stb.;
- lehetőség van komplett transzponder, illetve egy vagy több dedikált csatorna folyamatos bérletére (forgalom független költségek), vagy forgalommal arányos – akár folyamatos de alacsony intenzitású, akár időszakos magasabb intenzitású, vagy alkalomszerű jelentős intenzitású adatforgalom lekezelésére alkalmas – kapacitás igénybevételére.

A fenti tulajdonságok figyelembevételével a felhasználók igényeire optimalizált hálózatok és alkalmazások valósíthatók meg. Természetesen a választott megoldás költségeit nagyban befolyásolja az igényelt erőforrások biztosításához szükséges kapacitás tartalék is[63]. (Egy alkalomszerű jelentős kapacitásigényű összeköttetés biztosításához nagyobb tartalékolásra van szükség, mint egy viszonylag állandó forgalmat generáló előfizető esetén.)

Tulajdonságaik alapján a VSAT hálózatokat felépítésük és az általuk kínált lehetőségek alkalmassá teszik a földi stacioner hálózatok alternatívájaként/tartalékaként való felhasználásra is. Mivel sérülékenységük kisebb, megbízhatóságuk nagyobb, mint a jelentős földfelszíni infrastruktúrát igénylő rendszereké, alkalmasak a katasztrófavédelmi (védelmi) célú hírközlés speciális igényeinek kielégítésére is.

SCPS rendszerek jellemzői

Míg a VSAT rendszerek elsősorban a vállalatok FSS[64] igényeit hivatottak kielégíteni, addig a technikai és technológiai fejlődés mára már lehetővé teszi, hogy az egyéni felhasználók is a világ bármely pontján, bármely időpontban, az alkalmazási környezet infrastruktúrájától függetlenül hozzáférjenek beszéd- és adatátviteli műholdas szolgáltatásokhoz (MSS[65]). Ezt a

[63] Az erőforrások kihasználásának növelése az űrszegmens bérléséből eredő fajlagos költségek csökkenésével jár, míg a kihasználatlan tartalékok a meddő költségeket növelik.

[64] Fixed Satellite Service

[65] Mobile Satellite Service

mobilitást a műholdas személyi hírközlő rendszereknek biztosítják, melyek az egyszerű beszéd-összeköttetések mellett integráltan kínálják a mobil- és vezetékes telefonia fax- és adatátviteli szolgáltatásait, valamint az elektronikus levelezési, személyhívó és multimédiás alkalmazásokat.

Az SCPS rendszerek általános jellemzői a következők [4][5][6]:

- szegmenseinek megnevezése és rendeltetése megegyezik a VSAT rendszerekével;
- az űrszegmenst általában alacsony (LEO[66]), vagy közepes (MEO[67]) pályás, ritkábban geoszinkron (GEO[68]) műholdak alkotják;
- a pályamagasságtól függ a jelterjedésből adódó késleltetési idő, a szabadtéri csillapítás, a globális lefedettséghez szükséges műholdak száma, illetve a dopplercsúszás értéke;
- a területi ellátottság függ a műhold-konstellációtól, illetve a földi átjáró állomások (Gateway) elhelyezkedésétől;
- a cellák lehetnek földhöz rögzítettek, vagy mozoghatnak nagy sebességgel a felszínhez képest (handover-ek száma magas);
- a műholdak működhetnek átjátszóállomásként (nincs fedélzeti jelfeldolgozás és ISL, két terminál közötti összeköttetés csak a földi átjáróállomások segítségével jöhet létre), vagy megvalósíthatnak kapcsolási funkciókat is (van fedélzeti jelfeldolgozás és ISL, két terminál közötti összeköttetés közvetlenül a műholdakon keresztül jön létre);
- az utóbbi megoldásnál létrejövő kommunikációs csatornák függetlenek a földi infrastruktúráktól ezért, megbízhatóságuk lényegesen nagyobb, mint a „bent-pipe” struktúráké;
- a felhasználói terminálok kisméretűek, legtöbbször gyengén irányított antennával rendelkeznek, némelyek GSM kompatibilisek;
- az előfizetőkhöz rendelt hívószámok egyértelműen azonosítják a felhasználót a Föld bármely pontján;
- a szolgáltatások, valamint alkalmazások száma és minősége megközelíti, sőt egyes esetekben meg is haladja a földi mobil hálózatokét;
- a nagytávolságú összeköttetések esetén sem kell tranzitálás díját fizetni.

A négy legjelentősebb SCPS rendszer alapfunkciói megegyeznek, azonban műszaki megoldásaikban, kiegészítő szolgáltatásaikban jelentősen eltérhetnek. A fenti szempontok alapján összehasonlítva az Inmarsat, Iridium, Globalstar és Thuraya rendszereket a következő megállapítások tehetők [7]:

- a beszédszolgáltatások tekintetében a terjedési késleltetések minimalizálása érdekében a LEO műholdak (Iridium, Globalstar) alkalmazása

[66] Low Earth Orbit
[67] Medium Earth Orbit
[68] Geostationary Earth Orbit

előnyös, mégis az Inmarsat és Thuraya rendszereknél a geoszinkron pályákat preferálták, hiszen azonos földrajzi területek lefedéséhez lényegesen kevesebb GEO eszköz elegendő (nagy késleltetés);

- valós globális ellátottságról kizárólag az Iridium rendszer esetében beszélhetünk, amelynek űrszegmense 66db, hat polárpályán egyenletesen elosztott, átlapolódó lábnyomú, intelligens, kapcsolófunkciókkal is rendelkező, szomszédaival ISL-en kommunikáló LEO műholdat tartalmaz;
- az Inmarsat a sarkkörökön belül, míg a Thuraya az európai, közelkeleti, közép-ázsiai valamint észak-, és közép-afrikai régióban biztosítja szolgáltatásait négy, illetve kettő GEO műholddal;
- a Globalstar – bár nyolc, 52° inklinációjú pályasíkon keringő 48 db kisméretű, ISL nélküli, kizárólag átjátszó funkciókat megvalósító műholdjai lábnyom szerint biztosítják a földfelszín teljes lefedését – csak azokon a területeken biztosít szolgáltatást, ahol a „bent-pipe" struktúrához szükséges földi átjátszók és átjárók telepítésre kerültek69;
- a GEO műholdak föld forgásához szinkronizált mozgása földhöz rögzített cellarendszert eredményez, míg a Globalstar és Irídium cellái bonyolult nyalábvezérlés híján nagy sebességgel, a holdakkal együtt haladnak a felszínen, ami a hívásátadások számát jelentősen növeli;
- mind a négy rendszer biztosítja a hagyományos beszédösszeköttetésekhez, valamint az SMS, alacsony sebességű (9,6 kbit/s) adat- és faxtovábbításhoz kapcsolódó szolgáltatásokat;
- az Iridium műholdjai keringenek legközelebb a földhöz minimális terjedési késleltetést okozva, amihez az intelligens „égi háló" alacsony kapcsolási ideje adódik hozzá; mivel az összeköttetések felépülésében nem vesznek részt földi infrastrukturális elemek, a rendszer megbízhatósága, rendelkezésre állása nagyobb, a szolgáltatásokhoz való hozzáférés ideje kisebb, mint vetélytársaié;
- az adatátvitel tekintetében az Inmarsat különböző szolgáltatási osztályai 600 bit/s; 2,4; 4,8; 16; 32; 64; 128; 256; 492 kbit/s sebességet kínálnak, melyek segítségével riasztási, jelzési, flottakövetési alkalmazások mellett távoli hálózatok összekapcsolása, vagy az internet hozzáférés is biztosítható; DSL70 modem segítségével akár a Thuraya terminálok is képesek a 144 kbit/s-os sebesség elérésére, míg a másik két rendszer csak alacsonysebességű adatkapcsolat kialakítására képes (pl. Iridium: globális személyhívó szolgáltatás);

[69] Afrika középső és déli részén az indiai és dél-ázsiai területeken, a sarkvidékeken és az óceánok jelentős részén nem biztosított a hozzáférés.

[70] Digital Subscriber Line

- a Thuraya 100 m-es pontosságú helymeghatározást és speciális flottakövető szolgáltatást is biztosít;
- az Inmarsat legkorszerűbb rendszere a BGAN71 világelsőként képes hang- és adatkommunikáció egyidejű biztosítására egy szélessávú csomagkapcsolt összeköttetés (MPDS72) segítségével (max. 492 kbit/s); ez IP kapcsolaton kínálja az elektronikus levelezés, SMS küldés, telefon, Web böngészés, távoli LAN hálózatok és intranetek elérését, FTP szolgáltatásokat, e-kereskedelmet, valamint alkalmas biztonságos pontpont kapcsolat virtuális magánhálózat (VPN73) feletti létrehozására is;
- a felhasználói terminálok közül a Thuraya eszközei a legolcsóbbak, rendelkeznek a legkisebb fizikai méretekkel (mobiltelefon) és kínálják a legtöbb kényelmi szolgáltatást (GSM/GPRS74 kompatibilitás, technológiák közti roaming75, nagyfelbontású színes kijelző, beépített kamera, USB76, bluetooth és infra csatlakozási lehetőség, bővíthető memória), míg az Iridium készülékek robosztusabb felépítésükkel jobban megfelelnek a védelmi célú igénybevételnek; a Globalstar terminálok is megfelelnek a személyi hordozhatóság követelményeinek és biztosítják külső adatberendezések illesztését;
- az Inmarsat különböző szolgáltatási osztályaihoz különböző terminálok tartoznak, így léteznek hordozható-, kézi-, járműfedélzeti-, vagy integrálható modul eszközök, melyek alkalmazástól függően irányított, vagy gyengén irányított antennákkal lehetnek felszerelve (nagysebességű adatátvitel - erősen irányított antenna); a robusztus BGAN készülékek nagy környezeti ellenálló képességgel rendelkeznek, percek alatt telepíthetők és csatlakozhatók számítógéphez vezetékes (USB, Ethernet), vagy vezeték nélküli (WiFi77, bluetooth) kapcsolattal;
- a szolgáltatások díjai a Thuraya hálózatában a legalacsonyabbak, aminek következtében a térség egyik vezető szolgáltatójává vált; az Inmarsat és Iridium tarifái lényegesen magasabbak, amit a nagyobb lefedettség, rendelkezésre állás, és szolgáltatási tapasztalat (preferenciák), valamint a speciális globális szolgáltatások indokolnak; a Globalstar csak ez utóbbi két rendszerrel szemben kínál versenyképes díjakat, alacsonyabb szolgáltatási színvonal, kisebb lefedettség és megbízhatóság mellett;

---

[71] Broadband Global Area Network
[72] Mobile Packet Data Service
[73] Virtual Private Network
[74] General Packet Radio Service
[75] Ha nem érhető el földi GSM hálózat, a terminál automatikusan átkapcsol a műholdakra.
[76] Universal Serial Bus
[77] Wireless Fidelity

- védelmi preferenciái az Iridiumnak és az Inmarsatnak vannak, melyek szolgáltatásait a Magyar Honvédség mellett a világ számos országában igénybe veszik a fegyveres-, rendvédelmi- és készenléti szervek.

Összességében megállapítható, hogy mind a négy rendszer alkalmas műszakilag és szolgáltatásaikat tekintve a felmerülő katasztrófavédelmi kommunikációs igények jelentős részének biztosítására, ugyanakkor önmagában egyik rendszer sem kínál teljes körű, kompromisszummentes megoldásokat.

Műholdas rendszerek szerepe és jelentősége a veszélyhelyzeti hírközlésben

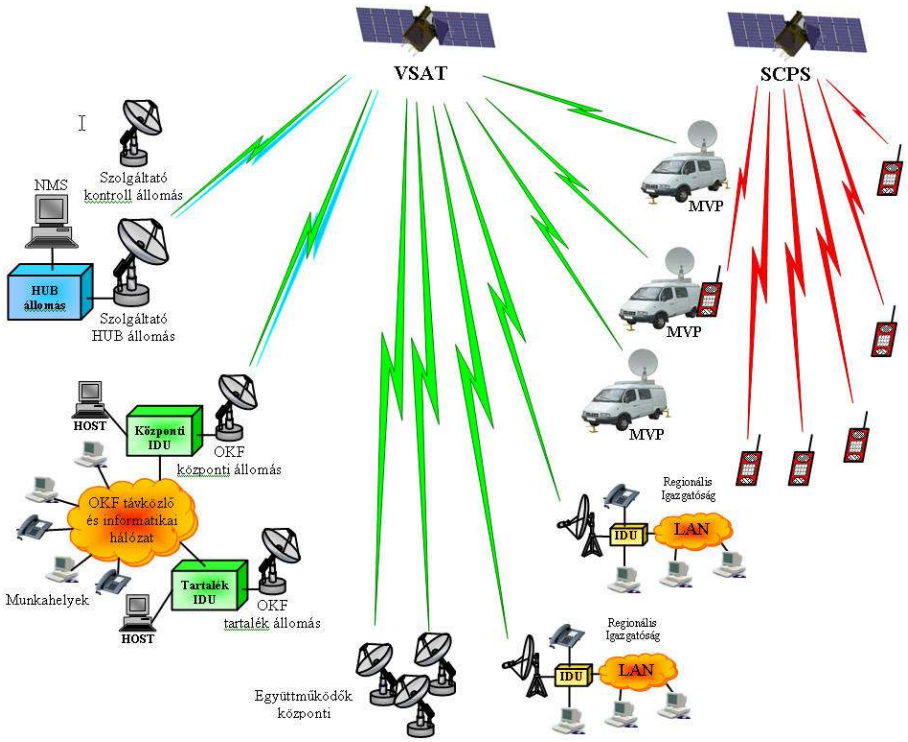
Az ismertetett VSAT és SCPS rendszerek struktúrája, működése, szolgáltatásai, tulajdonságai alapján belátható, hogy a polgári és üzleti alkalmazások mellett széles körben képesek lennének kielégíteni a védelmi kommunikáció mellett a veszélyhelyzeti hírközlés speciális igényeit is.

A VSAT rendszerek elsősorban a magasabb vesztési szintek irányítási, valamint a belföldi és nemzetközi együttműködési kommunikációs csatornák, míg az SPCS hálózatok a végrehajtó, alárendelt állomány vezetésének biztosítása alkalmazhatók.

A következőkben egy olyan megoldást kívánok bemutatni, mely kizárólag űrtávközlési szolgáltatásokra épülve képes a földi kommunikációs infrastruktúra jelentős sérülése, vagy akár a szolgáltatások teljes megszűnése esetén is a védekezés komplex rendszerének hírközlési szempontból történő támogatására. Ez a jelenlegi piaci és gazdasági körülmények között a legrövidebb időn belül megvalósítható alternatíva, melynek lényege, hogy a Magyarországon elérhető szolgáltatások közül előjegyzésre kerülnek azok, melyek képesek biztosítani minden szinten, a védekezési munkálatok hatékony tervezéséhez, szervezéséhez, irányításához és vezetéséhez szükséges műholdas vonalakat, erőforrásokat és eszközöket, illetve kiépítésre kerülnek az azok igénybevételéhez elengedhetetlenül szükséges, biztonságos földi infrastrukturális elemek (pl. központi állomások).

A kivitelezésre vonatkozó javaslatom az *1. ábrán* látható:

- az Országos Katasztrófavédelmi Főigazgatóságon telepítésre kerül egy központi állomás, amelyet illesztenek a meglévő hálózatokhoz (híradó, informatikai, EDR); a műholdas csatornákhoz való hozzáférési jogosultságok és prioritások a közvetlenül kapcsolódó központban hozzárendelésre kerülnek a minősített időszak esetén érintett számítógépes és telefonos munkaállomásokhoz;



1. ábra: Műholdas vezetési rendszer sematikus felépítése

- a központi állomás a számára kijelölt (az igény bejelentésekor aktiválásra kerülő) műholdas kapacitásokon keresztül közvetlenül, a szolgáltató (pl. HDT78) központi HUB állomásának igénybevétele nélkül kapcsolódik a regionális katasztrófavédelmi igazgatóságokhoz, valamint a kárhelyszínekre kivezényelt, megvalósításra javasolt mozgó vezetési pontok (MVP) VSAT termináljaihoz, mind számítógépes, mind távbeszélő összeköttetést biztosítva a különböző vezetési szintek között (a HUB állomás megkerülése csökkenti az igénybevett szolgáltatások díját, viszont a nagyméretű OKF központi állomás egyszeri kiépítésének költségét jelentősen megemeli); ezeken a csatornákon keresztül nagy mennyiségű adat továbbítására lehet számítani, amit a regionális parancsnokságok, valamint az MVP-k adatgyűjtő rendszereinek beérkező információiból értékelésre (döntéstámogatás céljából) felküldött jelentései generálnak;
- a regionális központok és MVP-k egymással is képesek kommunikálni az OKF központi állomásán keresztül, amely kritikus helyzetekben átmenetileg összekapcsolásra kerülhet a Magyar Honvédség központi állomásával is; az együttműködésre kötelezett szervezetek (Határőrség,

[78] Hungaro DigiTel Kft.

OMSZ79 stb.) parancsnokságai, mobil VSAT terminálokon keresztül szintén kapcsolódhatnak az OKF központjához;

- a nemzetközi segítségnyújtás keretében együttműködő külföldi társszervekkel, azok meglévő rendszerihez kapcsolódva szintén biztosítható a megfelelő VSAT irányok kialakítása;
- a szolgáltató telephelyén a szolgáltatás minőségének felügyeletére egy kontrol állomás, valamint az OKF központi állomás kiesése esetére egy tartalék állomás is telepítésre kerül; ez utóbbi feladata rövid időn belül részlegesen, vagy teljesen átvenni a központi állomás feladatait; ez a rendszer mind kétirányú MCPC, mind interaktív kétirányú TDM/TDMA struktúrában megvalósítható;
- mivel a speciális rendeltetésből adódóan, a szükséges műholdas kapacitásokra csak ritkán, ugyanakkor viszonylag nagy igénybevétel mellett van szükség, felesleges (gazdaságtalan) a forgalom-független bérelt csatornák folyamatos biztosítása; a VSAT rendszereknél – éppen a különböző típusú alkalmazások merőben eltérő igényei miatt – nem csak folytonos igénybevételt feltételező előfizetésekre, hanem (viszonylag) rövid idejű alkalmazások megvalósítására is van lehetőség (az első esetben az előfizetés mellett viszonylag alacsony forgalmi díjakat, míg az utóbbinál előfizetési díjat nem, csak magas forgalmi díjat kell a szolgáltatásért fizetni); ugyanakkor a szolgáltató is csak bérli az „űrszegmenst" és a kapacitásra vonatkozó igényeit előre le kell kötnie; a fent vázolt rendszer ezért csak úgy valósítható meg, ha bizonyos mértékű lekötött kapacitás mellett, prioritásos forgalomszervezést is biztosítunk, ezzel veszélyhelyzetben és minősített időszakban a földi hálózatok megbénulása esetén lehetőséget teremtve a polgári (üzleti) célokat szolgáló erőforrások, katasztrófavédelmi (védelmi) igények kielégítése érdekében történő átforgatására (természetesen a megfelelő jogszabályi háttár megteremtése szükséges);
- mind a központi állomás(ok), mind a végpontok esetében biztosítani kell azok energiaellátó hálózattól független tartós működését, akkumulátor-csoportok és aggregátorok segítségével;
- a fent ismertetett, a stacioner struktúrát kiváltani (pótolni) hivatott VSAT rendszer által alkotott gerinchálózat mellett, az alárendeltek vezetését bitósító SCPS szolgáltatások igénybevétele is szükségesé válhat; ilyen célokra több rendszer kínál különböző megoldásokat, melyek önállóan, vagy egymással kombinálva képesek kielégíteni a mobil hírközlési igényeket; a rendszerek kiválasztásánál számos tényezőt kell mérlegelni:

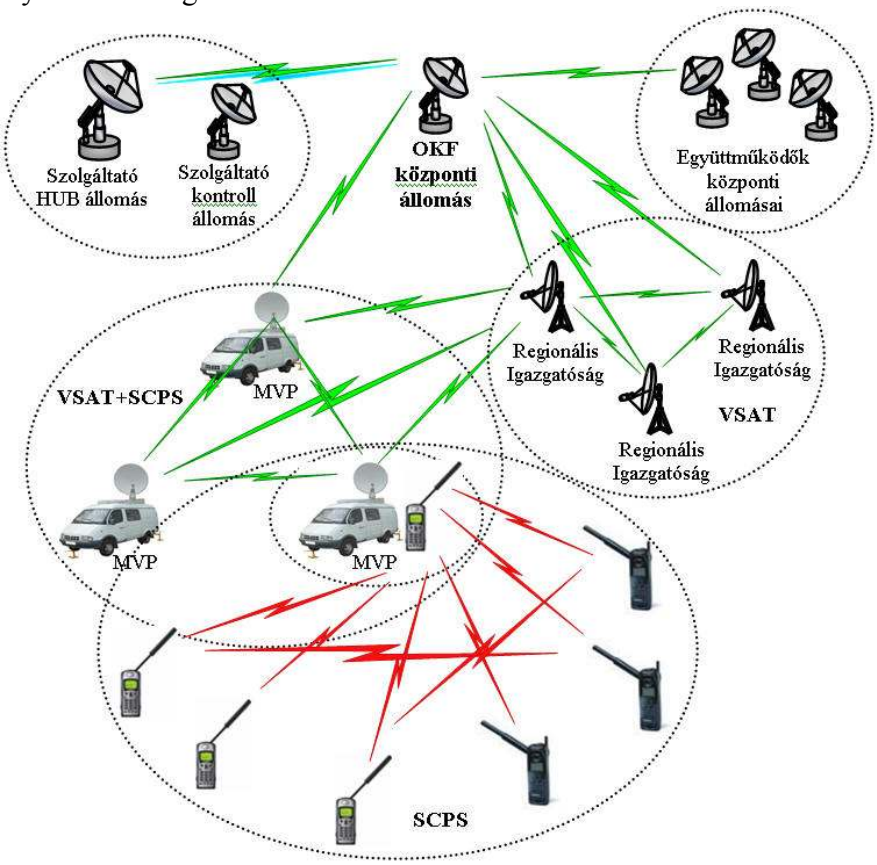
[79] Országos Meteorológiai Szolgálat, Országos Mentőszolgálat

- terminálok mérete, kialakítása: szélsőséges körülmények közötti alkalmazás lehetősége
- igénybevehető szolgáltatások: elsődleges fontosságú a beszédösszeköttetés biztosítása, de emellett SMS és adattovábbítás, járműkövetés is megvalósítható
- készülékek kiegészítő és kényelmi szolgáltatásai: beépített GPS80 és GSM
- pályamagasság: a beszédben okozott késleltetési idő miatt
- lefedettség: hazai alkalmazások esetében nem kritérium a globális lefedettség
- költségek: készülékek és szolgáltatások alacsony díjai
  - a fenti szempontok figyelembevételével, a szóbajöhető rendszerek vizsgálata alapján a következő megállapítások tehetők:
- az Iridium rendszer az amerikai kormányzati, biztonsági és védelmi területen már bizonyította életképességét, alkalmazhatóságát, ennek köszönhetően kifejlesztésre kerültek a fokozott igénybevétel mellett is működni képes speciális felhasználói készülékek; a terminálok árai és a szolgáltatások díjai azonban az elérhető rendszerek közül a legmagasabbak;
- a Thuraya rendszer esetén – a csak regionális lefedettséget biztosító műholdak nagy távolsága miatt (GEO) – nagy késleltetéssel kell számolni, ami a beszédkommunikációt kissé megnehezítheti, ugyanakkor a mobilitás, szolgáltatások és költségek szempontjából ez a legoptimálisabb választás; a piacon kapható legkisebb és legolcsóbb műholdas terminálok, a mai korszerű mobiltelefonokhoz hasonló kényelmi szolgáltatások mellett, integrált háromsávos GSM/GPRS moduljaik segítségével megvalósítják az automatikus, technológiák közti handover-t; a GPS funkció lehetővé teszi a műholdas helymeghatározással kapcsolatos alkalmazások egyetlen készülékkel történő igénybevételét;
- az Inmarsat szolgáltatásai közül elsősorban a flottakövetés (a védekezésben résztvevő szállítójárművek és munkagépek mozgásának koordinálására), valamint a BGAN nagysebességű adatátviteli képességének igénybevétele lehet célszerű (pl. adatok továbbítása olyan területekről, amelyek járművekkel nem közelíthetők meg)
- ezek alapján – minden szempontot mérlegelve – a Thuraya rendszer alkalmazását javaslom, szükség szerint Iridium és Inmarsat szolgáltatásokkal kiegészítve.

[80] Global Positioning System

Összefoglalás

Katasztrófák és más veszélyhelyzetek esetén valószínűsíthető a földi kommunikációs rendszerek sérülése, rombolása, ezáltal a vezetési lehetőségek jelentős csökkenése, esetleg megszűnése, ami szükségessé teszi olyan alternatív megoldás alkalmazását, amely akár az infrastruktúra teljes megsemmisülése esetén is képes biztosítani a veszélyhelyzeti hírközlés igényeinek kielégítését. A föld körül keringő műholdakon alapuló globális- és regionális hálózok felépítésükből, működésükből, szolgáltatásaikból adódóan képesek szélsőséges körülmények között is akár az együttműködő szervezetek különböző vezetési szintjeinek kommunikációs szempontból történő összekapcsolására, akár a munkálatokban résztvevők közvetlen irányításának megvalósítására.



2. ábra: A műholdas veszélyhelyzeti hírközlés struktúrája

Ezért a katasztrófavédelmi szervek hatékony munkáját biztosító komplex kommunikációs rendszert különböző űrtávközlési megoldásokkal, vagy azok kombinációjával is javasolt kiegészíteni.

A VSAT rendszerek rugalmassága lehetővé teszi a felső- és alárendelt parancsnokságok stacioner híradó és informatikai rendszereinek összekapcsolását a földi trönkvonalak kiesése esetén, míg az SCPS hálózatok által biztosított mobilitás a munkálatokban résztvevők közvetlen vezetését (*2. ábra*).

Felhasznált irodalom

[1] MAROS Dóra: Távközlési hálózatok működésének nemzetközi és hazai szabályozási kérdései veszély- és katasztrófahelyzetekben – Doktori (PhD) értekezés – Bp.: ZMNE – 2006.

[2] KOVÁCS László: A terrorizmus veszélye a Magyar Köztársaság információs infrastruktúrájára – Kommunikáció 2005 – Bp.: ZMNE – 2005. – ISBN 963 7060 11 1 – p. 187-198.

[3] PÁPICS József, KASZAVITZ Iván, KOCSIS Ferenc, DOBREFF Csaba, SZARKA Gábor, VENYINGI Teofil: Bevezetés a digitális üzleti űrtávközlésbe – hallgatói segédlet – Bp.: SAT-NET Műholdas Szolgáltató Kft. – 1993. – p. 11-40.

[4] GÖDÖR Éva: Műholdas hírközlés – tansegédlet – Bp.: BME – 2003. – p. 11-35. (http://micro3.mht.bme.hu/MuTa/muholdas.pdf)

[5] MIHÁLY Zsigmond: A legfontosabb tudnivalók az INMARSAT globális műholdas rendszerről – Bp.: BME – 1997. – p. 11-35. (http://www.hit.bme.hu/people/mihaly/mobil.hir/inmarsat.pdf)

[6] DÁRDAI Árpád: Mobil távközlés, mobil internet – Mobil Ismeret – Budapest – 2002. – ISBN 963 440 996 2 – p. 175-180.

[7] www.guards.hu

Andras KERTI, Dr. Zoltan RAJNAI

INTERNETTERRORISME

(a Bolyai Kutatási Ösztöndíj támogatásával)

L'absence de débats publics dans les régimes autocratiques ou son insuffisance dans les régimes démocratiques, ont permis de donner encore plus de relief à l'émergence d'un nouveau média, internet, qui non seulement dispense des informations non institutionnelles, mais facilite également la connexion des opinions publiques entre elles. Cette mondialisation de l'accès à l'information s'est également accompagnée d'une tentative de récupération de cette fenêtre de communication par les franges les plus radicales de nos sociétés. En effet, si internet a facilité les échanges et rapproché les civilisations, il a donné également la possibilité aux mouvements terroristes de profiter d'un certain nombre d'opportunités technologiques avec ce que cela comporte en terme de réduction des distances, de simplification des processus de décision et d'imagination du mode opératoire des attentats et d'impact sur les médias ainsi que sur les opinions. Le basculement dans le terrorisme islamiste mondial se fait à partir du moment où internet prouve son efficacité, c'est-à-dire la seconde moitié des années 1990. Ce n'est donc pas un hasard si de plus en plus de rapports et d'analyses révèlent la présence d'un nombre croissant d'informaticiens et d'ingénieurs au sein de la mouvance djihadiste. Plus inquiétant, l'accès aux informations comprend un volet très dangereux avec la recherche de données en matière d'armes de destruction massive. Des terroristes arrêtés en Grande-Bretagne et en Italie ont reconnu lors de l'enquête leur intérêt pour la possession de substances chimiques, bactériologiques ou nucléaires. Après avoir montré comment les terroristes, essentiellement djihadistes, utilisent internet comme vecteur de puissance, il conviendra d'analyser quelles sont les réponses apportées par les Etats pour lutter contre ce phénomène et de mettre en évidence les difficultés auxquelles ils restent confrontées.

Pour comprendre la stratégie des terroristes de récupération du web et en déduire qu'elle constitue un vecteur de puissance, il faut tout d'abord examiner sa logique fondée sur la déterritorialisation et la dématérialisation de ses acteurs pour ensuite s'arrêter sur les effets recherchés, à destination tant du monde musulman que des occidentaux.

Depuis la montée en puissance d'internet, le terrorisme a muté sur le fond comme dans la forme. Sur le fond, la toile a permis aux stratégies terroristes d'amplifier la dynamique de déterritorialisation de leur combat dans un monde de plus en plus globalisé. Dans la forme, le net a favorisé le

développement de nouvelles techniques terroristes poussées par les phénomènes de dématérialisation que l'outil virtuel pouvait suggérer en matière de circulation des données, de prosélytisme et de communication entre terroristes. Internet crée des communautés qui peuvent ainsi s'émanciper de l'emprise d'un imam local et s'approprier l'islam par l'intermédiaire d'une autorité virtuelle devenue la nouvelle référence. L'incarnation des terroristes est de moins en moins importante au fur et à mesure qu'ils deviennent des icônes, que l'on peut consulter à tout moment sur le web. De plus, sur le réseau, le temps aussi est aboli et c'est ainsi que des textes médiévaux particulièrement guerriers seront reproduits sans aucune adaptation pour des auditoires qui n'ont pas forcément le recul pour les relativiser. Des injonctions dépassées, décontextualisées prennent grâce à internet, des accents de modernité. Ce phénomène se trouve amplifié par la mise en oeuvre sur le net du principe de l'irresponsabilité par la non-signature.

Internet permet donc aux terroristes de produire un effet de puissance de leur mouvement, de montrer qu'ils sont plus nombreux qu'on ne le pense. Il agit comme une caisse de résonance et donne visibilité et intelligibilité aux terroristes. Certains individus basculent ainsi progressivement de la sympathie pour des chefs insaisissables, véritables icônes du djihad, à l'action terroriste elle même. Les attentats sont calculés pour leur caractère audacieux et spectaculaire afin d'être sûr de créer un événement médiatique qui récolte un maximum d'audience. Il y a une pensée de la société du spectacle, à savoir que c'est avec la "mise en scène" de l'attentat que celui-ci prend sa signification. Internet permet de véhiculer l'émotion par les images et l'idéologie par les textes et les discours. Le but étant de renverser les signes, les conventions : l'idéologue planétaire exposera en arabe la rationalité de l'action et l'exécutant s'exprimera dans le langage normalement universel, l'anglais. C'est notamment ce qui s'est produit lors de la revendication des attentats de Londres de juillet 2005.

Incontestablement, les attentats de New York, de Washington, de Madrid et de Londres ont changé la donne en matière de lutte contre le terrorisme. Mais au-delà des dispositions prises à l'ONU, aux Etats-Unis, ou dans l'UE, la question d'équilibrer le volet répressif et le respect des libertés individuelles n'a pas trouvé de solution consensuelle. En cela, l'internet met en exergue ce problème majeur. Les sites du djihad posent un dilemme aux services de renseignement. Les méthodes varient d'un pays et d'un contexte à l'autre. A Londres, pendant longtemps, la tactique suivie consistait à surveiller les sites djihadistes. Depuis les attentats des 7 et 21 juillet 2005, les policiers britanniques sont passés à l'action systématique de fermeture de ces supports du djihad. Les partisans du suivi du net estiment quant à eux que c'est en identifiant certains individus avec des écoutes

téléphoniques et en remontant les réseaux, que l'on peut obtenir des résultats. C'est de cette manière qu'ont été identifiés et arrêtés les deux grands opérationnels des attentats du 11 septembre. De plus, afin notamment de traquer le djihadisme en ligne, un projet de loi contre le terrorisme a été présenté courant automne 2005 par le gouvernement et vient d'être adopté par l'Assemblée nationale. Il contient deux volets concernant internet : la surveillance des cybercafés et des fournisseurs d'accès.

C'est d'ailleurs l'enjeu de toutes les législations qui sont en train de se mettre en place. Les logs, les données internet des cybercafés, des fournisseurs d'accès, des hébergeurs seront légalement stockés pendant plusieurs mois, voire des années. L'intérêt est qu'en cas d'interpellation d'un présumé terroriste, les services de renseignement pourront remonter toutes les communications sur du long terme. Sur le web, la surveillance des réseaux est l'une des missions de l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication. La police du net repère les sites dont le contenu est sensible, surveille les forums où les propos tenus sont violents et trace les origines des sites internet impliqués. Viennent ensuite la localisation des auteurs et l'identification des visiteurs assidus des sites djihadistes. Pour ce faire, des logiciels permettent de remonter aux origines d'un serveur (localisation géographique d'un site) ou de tracer une adresse IP. Dans cette chasse aux contenus illégaux, des entreprises privées peuvent mettre à disposition leur expertise. Par exemple, la société Advestigo a mis au point un système qui permet de trouver sur la toile toute forme de contenu dès lors qu'il en possède une copie. Ce "renifleur" du web, conçu originellement pour traquer la contrefaçon numérique, peut être utilisé dans la lutte antiterroriste. En effet, il pourrait automatiser la recherche des sites publiant des manuels terroristes, ou les "recettes" pour réaliser une bombe.

Les services de renseignement américains ou européens et ceux dont les pays sont souvent visés par le terrorisme, se heurtent à des contraintes technologiques, politiques et judiciaires. Sur le plan technologique, l'usage du logiciel Skype permet à ses utilisateurs de communiquer sur la toile sans passer par un serveur susceptible d'être traqué par les services de sécurité. Selon les experts, les groupuscules extrémistes musulmans recourent aussi à la stéganographie adaptée à internet: les messages, ordres ou cartes passent via des photos anodines, des morceaux de musique MP3 et de la vidéo. Il existe également des experts en système de sécurité sur internet qui apportent leur concours à des groupes terroristes. L'un d'entre eux collabore avec les terroristes en mettant en ligne leurs vidéos et en protégeant leurs sources originales. Il est notamment entré dans un serveur STP de l'Etat pour y mettre des vidéos de décapitation.

Sur le plan judiciaire, la lutte contre le terrorisme relève encore de la compétence des Etats, alors que le terrorisme est un phénomène transnational. Certains pays dans lesquels les organisations islamistes radicales sont parfaitement légales laissent des sites publier des discours qui ne seraient pas diffusables. Aux Etats-Unis, les sites révisionnistes sont tolérés, protégés par le premier amendement de la constitution. Il y a dans ce domaine encore trop de disparités alors qu'une harmonisation des législations s'impose. Sur le plan politique, partis, syndicats, organisations non gouvernementales et opinions publiques sont plus ou moins sensibles à la protection des libertés individuelles et à la cause défendue par les terroristes. Pour les spécialistes américain des questions de cyberterrorisme, le problème est triple. Outre les difficultés techniques, il pointe du doigt l'absence de coordination stratégique entre les services de renseignement occidentaux. Il souligne aussi le manque de savoir ou encore l'absence de formation des agents (langue et technologies) dans ce domaine. Une filière universitaire dédiée à la politique antiterroriste vient d'ailleurs d'être créée aux Etats-Unis, avec un séminaire consacré à la lutte contre le djihadisme en ligne. Dans le même registre, c'est bien souvent le personnel chargé de traiter la masse d'informations concernant ce phénomène qui est en nombre insuffisant. Or l'exploitation des données doit s'effectuer à chaud notamment dans le but de se prémunir efficacement contre la réalisation d'un attentat. Comme nous venons de le voir, l'utilisation par les réseaux terroristes du virtuel à des fins terroristes est bien une réalité. La lutte, bien engagée, contre ce nouveau vecteur du terrorisme doit pour gagner en performance et en efficience, se poursuivre en portant l'effort sur l'harmonisation et la formation. S'agissant de l'harmonisation, il est nécessaire d'aboutir à l'instauration d'une véritable législation internationale en matière de lutte contre le cyberterrorisme. Celle ci pourrait d'ailleurs s'inspirer de celle qui vient d'être adoptée en France. Il est primordial d'apporter une réponse unique et mondiale à un problème clairement transnational. Cette harmonisation passe également par une coopération renforcée au niveau international des services nationaux en charge des questions de terrorisme: échanges accrus de renseignements, actions communes, facilitation des investigations, autant de pistes qui méritent d'aboutir sur des initiatives concrètes. Sur le plan de la formation, l'effort doit porter tant sur l'approfondissement et l'actualisation des connaissances que sur des actions de sensibilisation. Les professionnels chargés de surveiller la toile ont en effet besoin d'étoffer en permanence leurs bases de données.

Farkas Tibor

A BLACKBERRY RENDSZER

Napjainkban az infokommunikációs társadalom megköveteli az informatikai és a kommunikációs eszközök folyamatos fejlesztését. Nap, mint nap új eszközök és alkalmazások kerülnek a felhasználókhoz, amelyek első megközelítésben nem minden esetben tűnnek fontosaknak, szükségeseknek. A hordozható telefon megjelenése előtt is képesek voltak az emberek maradéktalanul elvégezni a munkájukat, de annak használatával megszűntek egyes korlátok, és biztosabbá vált az emberek elérhetősége.

A mai rohanó világban nagyon fontos a mobilitás. A legtöbb fejlesztés, mint a vezeték nélküli hálózatok, a vezeték nélküli perifériák ebbe az irányba mutatnak. A laptop, a mobiltelefon és más hasonló praktikus eszközök megjelenésével új lehetőségek tárultak a felhasználók elé. Ezt az irányvonalat hivatott erősíteni a BlackBerry rendszer is, mivel mára rengeteg ember végzi irodájától távol a munkáját, amelynek nélkülözhetetlen kellékévé váltak a mobil eszközök.

A BlackBerry rendszert elsősorban nagyvállalatok vezetői-, menedzseri beosztásaiban dolgozó alkalmazottak igényei alapján fejlesztették ki. A rendszer a mobiltelefon és a számítógép fontosabb tulajdonságait egyesíti. Természetesen a BlackBerry eszközökhöz hasonló készülékek, mint például a PDA-k, már több éve a felhasználók igényeit hivatottak kielégíteni, de mint minden új eszköz, a BlackBerry is valamivel több lehetőséget nyújt az alkalmazók számára.

Mi is az a BlackBerry!?

A BlackBerry eszköz, egy olyan mobiltelefon méretű készülék, amely biztonságos, folyamatos és gyors elérést biztosít különböző információkhoz. A rendszer lehetővé teszi, hogy a felhasználó a számítógépét (irodáját) elhagyva ellenőrizni tudja az elektronikus leveleit, a naptárát szinkronizálja, és mindezek mellett mobiltelefonként is használhassa készülékét.

A BlackBerry által nyújtott alkalmazások előnyei

A felhasználó irodájától távol ellenőrizheti naptárát, saját és a vállalati címlistáját. A munkahelyétől távol megtekintheti a számára megszabott

feladatokat, milyen tárgyalásra, konferenciára kell mennie, stb. Mindezt úgy, hogy a BlackBerry legfontosabb szolgáltatása lehetővé teszi, hogy a felhasználó a cég levelező rendszeréhez online hozzáférjen a GSM és az Internet hálózaton keresztül.

A rendszer nagy előnye abban rejlik, hogy ezeket a műveleteket anélkül teheti meg a felhasználó, hogy a szinkronizálással, csatlakozással kelljen időt töltenie. Ebből adódik, hogy olyan egyszerűen érkeznek meg a levelei, akár az SMS-ek.

Nincs szükség jelszavakra, letöltésre, az üzenetek automatikusan megérkeznek. Természetesen a fordított irány, a levelek küldése is hasonló egyszerűséggel működik.

A levelekhez csatolt fájlok, dokumentumok is megjelennek a készülék kijelzőjén, anélkül, hogy külön le kellene tölteni azokat.

Hasznos lehetőség az üzenetek szűrése is, amely a nagy mennyiségű levelek áradatának szab határt.

A BlackBerry készülékek Internet-böngészővel rendelkeznek, így az Internet korlátok nélkül használható. Jegyzettömbbel, és emlékeztetővel is ellátták a készülékeket más előnyös funkciók mellett.

Alapvető biztonsági megoldások

Mint minden kommunikációs rendszer esetén, a BlackBerry alkalmazása során is alapvető biztonsági követelményeknek kell megfelelni. A telepített BlackBerry szerver az adott cég hálózatán belül kerül telepítésre, így működése teljes mértékben ellenőrizhető. Közvetlenül kapcsolódik a levelező szerverhez, a teljes adatforgalom a szervertől a készülékig titkosítva és tömörítve kerül továbbításra. A három alapvető feltétel a biztonságos működéshez a következők; megbízhatóság, amely csak a címzettnek engedélyezi az üzenet és tartalmának elolvasását; a sértetlenség, amely jelzi egy harmadik fél hozzáférését a levélhez; és a hitelesség, amely a címzett számára azonosítja az üzenet küldőjét.

A BlackBerry rendszer felépítése

A BlackBerry rendszer három alapvető részből tevődik össze:

1. BlackBerry Enterprise Server (BES)
2. BlackBerry készülék
3. Kliensszoftver

A három rész együttes működtetése teszi lehetővé a rendszer használatát a felhasználók számára.

BES:

A BlackBerry szervert a szervezet informatikai rendszerében kell elhelyezni, levelező szerveréhez kell csatlakoztatni. A BlackBerry támogatja a Microsoft Exchange, Novell Groupwise és a IBM Lotus Domino levelező-rendszereket egyaránt, ezekkel képes kommunikálni.

A szerver az ellátott funkciója szerint két részre osztható.

Az egyik rész az a szolgáltatás, amely a leveleket továbbítja a GSM hálózaton keresztül a készülékekre. Ennek megvalósítása úgy történik, hogy egy speciális felhasználó kerül kialakításra, aki minden postafiókhoz hozzáfér, képes levelet küldeni és fogadni a felhasználó „nevében". A rendszer így automatikusan végzi el a szolgáltatást.

A másik része a szolgáltatásnak egy adatbázis, amely minden információt tartalmaz a felhasználókról, a készülékekről, és a szerver szolgáltatásairól, annak működéséről, úgynevezett házirendjéről.

A felhasználó adatai:

- Név
- Postafiók neve
- Levelező szerver
- Postafiók tároló

A készülék adatai:

- Készülék típusa
- Mely felhasználóhoz van rendelve

Az üzemeltető állománynak ezt az adatbázist célszerű folyamatosan lementenie, így egy esetleges újratelepítés során, nem kell újrakonfigurálni a szervert, és adatvesztés sem történik.

A készülék:

A készülék az általános telefonfunkciókon kívül alkalmas vezeték nélküli adat- és hangkommunikációra. Saját operációsrendszerrel, és „Qwertz" billentyűzettel rendelkezik, amely a nagyméretű kijelzővel megfelelően alkalmas szöveges üzenetek kezelésére. A szerver szolgáltatásaihoz kell felkonfigurálni a készüléket, amely hatására egy közös kulcs generálódik,

amelyet csak a két fél (szerver, készülék) ismer. A titkosítást ezen kulcs alapján valósítják meg.

A készülékeket két csoportra bonthatjuk, típustól függően.

1. BlackBerry készülékek:

A BlackBerry márkájú készülékek kifejezetten a BlackBerry szolgáltatás támogatására lettek kifejlesztve. A RIM[81] által készített készülékeket a saját (RIM) menedzser szoftverével lehet a felhasználóhoz, szolgáltatáshoz rendelni. Konfigurációt nem igényel, mivel az első csatlakoztatáskor felismeri a készülék szoftverét, és a további beállítások központilag megtörténnek.

1.kép: BlackBerry készülék
Forrás: www.blackberry.com

2. BlacBerry kompatibilis készülékek

Azok az eszközök tartoznak ebbe a csoportba, melyeket más gyártók fejlesztettek ki, és képesek a BlackBerry alkalmazásra. Ezek is rendelkeznek BlackBerry szoftverrel, de nem a RIM által kifejlesztett változattal, ezért a szolgáltatáshoz való csatlakozást követően konfigurálni kell a készüléket, mivel a házirend nem érvényesül teljes mértékben.

A kliensszoftver

[81] Research in Motion vállalat

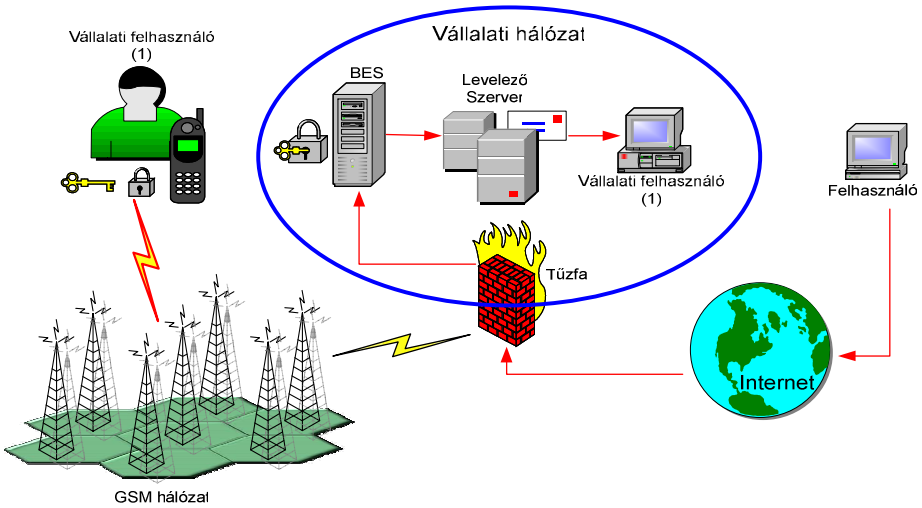
A szoftver végzi el a készülék és a számítógép közötti szinkronizációt. A Mail for Exchange alkalmazással a készülék hozzáférhet a felhasználó (pl. Microsoft Exchange) fiókjának e-mail, címjegyzék, feladatok, stb. funkcióihoz. A szinkronizálás során egyezteti és frissíti a postafiókban lévő elemeket a BlackBerry készüléken lévőkkel.

A BlackBerry működése

A rendszer működése igen egyszerű, amely a következő:

A vállalat levelező szerverére érkezik egy levél az Interneten keresztül, a vállalati tűzfalon át, az egyik felhasználó számára. Amellett, hogy a címzett számítógépére megérkezik a levél, a levelező szerverrel összekapcsolt BES lekéri a levél másolatát, tömöríti és titkosítja, majd továbbítja azt az Interneten és a GSM hálózaton keresztül a címzett BlackBerry készülékére is. A felhasználó így elolvashatja levelét a munkaállomásától távol. A folyamat visszafelé is ezen az elven működik.

A szerver mindig csak akkora részt küld el a levélből a készülékre, amekkora elfér a kijelzőjén, majd folyamatosan „adagolja”, ahogyan a felhasználó nézegeti tovább az üzenetet.



1. ábra: A BlackBerry rendszer működési vázlata

Miután a felhasználó elolvasta a levelét BlackBerry készülékén, a számítógépén is olvasottként jelenik meg. Az üzenet törlése is hasonló elven működik.

A kézi készülékre beérkező levelek továbbítása is kíméli a rendszer leterheltségét, mivel ilyenkor a levelet nem küldi vissza a BES-re az előzőekben leírtak szerint, hanem csak egy parancsot továbbít, amely utasítja a szervert, hogy a levelet továbbítsa a megadott címzettnek.

A levelezésen kívül az Internet, a naptár és értekezlettervezés funkciók eléréséhez is lehetőséget biztosít a BlackBerry. Ha naptárbejegyzés teljesítését követően a felhasználó törli a jegyzetet, akkor a levélhez hasonlóan, mindkét készüléken törlődik.

Összegzés

A BlackBerry egy vállalatok számára kifejlesztett rendszer, amely lehetővé teszi a számítógépétől távol lévő felhasználó hozzáférését elektronikus leveleihez, naptárbejegyzéseihez.

A kézi készülékek állandó kapcsolatban vannak a BES-el, így a készülékeket nem kell minden bekapcsoláskor, levélküldéskor csatlakoztatni, szinkronizálni a szerverrel. Az adatforgalom lecsökkentését is előtérbe helyezi a BlackBerry rendszer, így a kapacitás csökkentése mellett, a költségek is lecsökkennek.

Lehetségesnek tartom a rendszer katonai alkalmazását, mivel nem kizárólag a vállalatok vezető beosztású személyei, menedzserei végzik irodájuktól távol a munkájukat, hanem a vezető beosztású katonák is.

Bibliográfia

[1] http://it.news.hu/hirek/2004-09- 09/telefonkent_hasznalhato_uj_blackberry.html
[2] www.vodafone.hu/business/szolgaltatasok/blackberry.html
[3] www.piksys.hu/ujdonsag2005.html
[4] www.blackberry.com
[5] www.rim.com
[6] www.blackberrypearl.com
[7] www.discoverblackberry.com

MEDVECZKI Zoltán

AZ ORRLÉGZÉS MÉRÉSI MÓDSZEREI

Történeti áttekintés

Az orrüreg vizsgálatát egyiptomi orvosok már több mint 3 ezer évvel ezelőtt végezték (Ebers papirusz) és a fáraók mumifikálása során is említik, amikor az agyvelőt az orron keresztül távolították el. Görögországban Hippokratész (élt i.e. 460-377-ig) írta le az orrüreg vizsgálatát. Különböző módszereket javasoltak az orrüreg minél jobb beláthatóságára. Guy de Cehauliac [82] a XIII. században egy orrspekulum használatáról tesz említést.

Az orrlégzés rendszerezettebb vizsgálatát a XIX. század végén Zwaardemaker írta le, melyet Glatzel pontosított 1901-ben. Az orr két oldalának légzésben lévő különbségét egy fém lapra lerakódó vízpára területének nagyságából ítélték meg. Ezt a fémlapot az orrüreg elé helyezték a kilégzés során. Egy másik, legalábbis többé-kevésbé mennyiségi vizsgálati módszer volt például a Spiess által használt zörej-teszt (1902-ben), ahol az orrüreg jól lélegző felét kívülről lezárták, és az erőltetett orrfújás során keletkező zörej hangmagasságát vizsgálták, vagy egyszerűen az orrüreg egy-egy oldalának külön-külön, erőltetett kilégzéssel keltett hangjaiban lévő különbségeket mérték (Bruck, 1901). Ezek a módszerek, melyek közül néhány manapság is használatos, nagyban függnek a belégzés módjától és attól, hogy a vizsgálati alanyok mennyire alkalmasak e teszteknek a végrehajtására. Az orrüregben fellépő nyomásesést mérte meg és írta le passzív áramlás során Courtade 1903-ban. Ez volt a rhinomanometria egyik legelső leírása. Azóta a rhinomanometriáról több mint 500 tudományos vizsgálatot közöltek különböző nemzetközi folyóiratokban. Az első cikk, amelyben az akusztikus rhinometriáról szó esik, 1989-ben jelent meg.

Optikai módszerek

z orrüreg átjárhatóságának mérésére leggyakrabban használt optikai módszer a rhinoszkópia. Bár a rhinoszkópia az orr átjárhatóság minden egyes klinikai vizsgálata során jelen kellene, hogy legyen, különféle tanul-

Lásd részletesen:

[82] RAUCH FUSS A. The nasal speculum. Its historicai development and remarks on the history of rhinoscopy. Laryngol Rhinol Otol Stuttg 1985; 64: 551-558.

mányok azt mutatták, hogy nincs minden alkalommal egyértelmű kapcsolat az elülső rhinoszkópia és az említett vizsgálatok, vagy más tesztek között.[83]

A flexibilis rhinoszkóp használatával javíthatjuk az orr kórfolyamatainak vizsgálati eredményeit, és bizonyos esetekben a műtétek kimenetelét is, de az endoszkópos vizsgálatok nyújtotta eredmények nem feltétlenül esnek egybe a rhinometria alkalmazása során az orr átjárhatóság vizsgálatáról kapott eredményekkel. [84]

Különféle optikai eszközöket használtak az orr átjárhatóság mennyiségi jellemzésére. A rhinosztereometria módszere az orrüreg mediális és laterális fala közötti távolság mérésére szolgál. Ezt a távolságot egy, a mikroszkópba épített mérce segítségével állapítják meg, ám a fej helyzetét rögzíteni kell annak érdekében, hogy a későbbi megismételt mérések során ugyanezt a helyzetet lehessen felvenni. Ez a módszer csak korlátozott tájékoztatást nyújt az orrlégutak egyes struktúrájáról, nem ad képet az orrlégutak nagyobb részeiről.

A flexibilis endoszkópia során alkalmazott videó felvétel lehetővé teszi az eredmények későbbi értékelését, de ez még mindig egy invazív eljárás, s ez által nem tekinthető optimális módszernek az orr átjárhatóság vizsgálata szempontjából.

Mennyiségi akusztikus vizsgálati módszerek

A légútban keletkező hangokat vagy azok elemzését használják a légutak átjárhatóságának, vagy azok elzáródásának jellemzésére a gégében, az orrüregben és az orrmelléküregekben, illetve ebből határozzák meg a horkolást eredményező szűkület helyét a felső légútban, az epipharynxban.[85] Ezen erőfeszítések ellenére, melyek során többé-kevésbé a vizsgálati alany által keltett hangokat értékelték, s ebből következtettek a légutak átjárhatóságára, ezek a módszerek eddig nem bizonyultak túlságosan sikeresnek.

---

[83] HUVGEN PL, KLAASSEN AB, DE LEEUW TJ, WENTGES RT. Rhinomanometric detection rate of rhinoscopicallyassessed septal deviations. Rhinology 1992; 30: 177-181. munkájában.

[84] ZEDALIS D, DOLEN WK, GLOVER GC, WIENER MB, SELNER JC, WEBER RW. Evaluation of nasal patency by fiberoptic rhinoscopy. J Allergy CEn Immunol 1989; 83: 973-978.

[85] COLEMAN RF, SCHECHTER GL. A basic model to study acoustic evaluation of airway obstruction. Arch Otolaryngol Head Neck Surg 1991; 117: 1144-1149.

Áramlási módszerek

Az orrlégutak átjárhatóságának értékelésére használt áramlási módszereket többé-kevésbé rendszeresen használták az elmúlt 5 évtized során. Ennek legegyszerűbb módja a maximális, vagy orrcsúcs áramlás mérése volt. Ebben az esetben a mozgatóerő hevessége, vagyis a mellkas és az alsó légutak befolyásolják az orr kilégzési és belégzési csúcsáramlását. Számos szerző próbálta csökkenteni ezt a tényezőt az orr és a száj csúcsáramlása közti index kiszámításával.[86] Azon tény ellenére, hogy egybeeséseket figyeltek meg az orr csúcsáramlása és az orr elzáródás értékelésére használt más módszerek között, az orr csúcsáramlás tűnik a legalkalmasabbnak arra, hogy ugyanannál az alanynál, ismételt vizsgálatok során a változásokat megmérjük.[87]

Rhinomanometriában egyszerre mérik az áramlást és a nyomást. A különféle technikák során vagy a vizsgálati alanyok saját légáramlását (aktív módszerek), vagy külső áramlási generátort használtak (passzív módszerek). Az egybeeső áramlást mérik az orrüreg elülső részében (elülső mérési módszerek), illetve a garatban is (hátsó mérési módszerek).

Az aktív módszereket gyakrabban használják, mint a passzív elülső, vagy passzív hátsó módszert. Az elülső és a hátsó módszerrel kapott eredmények eltérhetnek,[88]bár egyes kutatók egészen hasonló eredményeket kapnak e módszerekkel is. [89]

A rhinometriával kapott eredmények egybevágnak más, általában a tüdő funkció mérésére használt módszerek eredményeivel, mint például a test plethysmográfia és a forszírozott oszcillációs technika segítségével kapott adatokkal. Ezek során meglehetős egybeesések mutatkoztak.

A rhinomanometriás mérések megismételhetősége 10 és 30 % között mozog, ezért néhány szerző ezt alkalmatlannak találja az orrlégzés precíz mérésére.

---

[86] HOLMSTROM M, SCADDING GK, LUND VJ, DARBV YC. Assessment of nasal obstruction. A comparison between rhinomanometry and nasal inspiratory pe ak flow. Rhinology 1990; 28: 191-196.

[87] WIHL JA, MALM L. Rhinomanometry and nasal peak expiratory and inspiratory flow rate. Ann Allergy 1988; 61: 50-55.

[88] KORTEKANGAS AE. Significance of anterior and posterior technique in rhinomanometry. Acta Otolaryngol (Stockh) 1972; 73: 218-221.

[89] DVORACEK JE, HJLLIS A, ROSSING RG. Comparison of sequential anterior and posterior rhinomanometry. J Allergy CEn Immunol 1985; 76: 577-582.

Az egyik lényeges probléma az áramlás és nyomás viszonyának leírása. Tekintve, hogy az áramlás és a nyomás közötti kapcsolat nem lineáris, ezért itt (egy meghatározott áramlás, vagy nyomás érték során) különböző módszereket alkalmaztak, mint például az ohmikus ellenállást. Egy teljesítmény függvényt, illetve más modelleket is alkalmazva (például a Rohrer-féle egyenletet) végezték a méréseket. Az abszcissza (áramlás) és a nyomás-áramlási görbe kereszteződése által bezárt szög mérése, valamint egy kör alkalmazása a koordináta rendszerben (Brom-féle rendszer), vagy a két oldal közötti relatív különbség mérése, azaz a lateralizációs index, szintén használatos volt.

A rhinomanometriás ellenállást úgy is ki lehet fejezni, mint az orrüreg minimális keresztmetszeti területét, s néhány szerző ezt véli a legjobb módszernek az ellenállás megjelenítésére. Ez egy bonyolult áramlási modellt használ az orrüregben, és az alkalmazott modellek nem mindig adják „a valódi" területet a különböző áramlási alkalmazások során. A rés-szerű felépítés sajátos modellkövetelményeket állít, mivel az áramlási profil az orrüregben nem minden esetben egyforma, áramlási formája a lamináris és turbulens között változhat.

Mindezeken túlmenően az eltérés lokalizációja is befolyásolhatja a rhinomanometriával értékelt ellenállást. Az orrcimpánál lévő orrsövényferdülés jobban befolyásolja az ellenállást, mint az orrüreg hátsó részében lévő orrsövényferdülés.

Különféle kísérleteket tettek a rhinomanometria szabványosítására[90] annak érdekében, hogy a különböző tanulmányok nyújtotta eredmények összehasonlíthatóvá váljanak. Rhinomanometriát az orrtudomány többféle aspektusában használtak, például a különféle orrbetegségek diagnosztikájában, allergia tesztekben, pharmakológiai tanulmányokban, de élettani elemzések során is. Bizonyos szerzők úgy találták, hogy a rhinomanometria hasznos a kezelési mód megválasztásában is, így például annak eldöntése során, hogy szükség van-e műtétre, vagy nincs. Hasznos eszköznek találták az operációs beavatkozások értékelésére is, míg mások e technikákat, ilyen célokra alkalmatlannak vélik.

Néhány tanulmányban egyértelmű egybeesést találtak a vizsgálati alany által érzett orr eldugulás és a rhinomanometriás értékek között, más tanulmányok viszont gyér egybeesésről számolnak be,[91]mivel más tényezők is,

[90] CLEMENT PA. Committee report on standardization of rhinomanometry. Rhinology 1984; 22: 151-155.

[91] JONES AS, WILLATT DJ, DURHAM LM. Nasal airflow: resistance and sensation. J Laryngol Otol 1989; 103: 909-911.

nem csupán az ellenállás befolyásolják az orr eldugulás érzését. Jól ismert, hogy a mentol csökkenti az orrdugulás érzését, miközben az orr ellenállása ilyenkor a légáramlás tekintetében nem változik.[92]

A rhinomanometria néhány hátránya közé tartozik viszont a viszonylag alacsony reprodukálhatóság, az alacsony egyezőség a vizsgált személy által érzett orrdugulással, az eredmények leírásának hiányzó egységes módszere, valamint az, hogy számos különböző technikát alkalmazhatnak, mint például az elülső, a hátsó, az aktív vagy a passzív mérést, s ezek így, néhány kutató laboratórium kivételével nem kerültek be a napi klinikai rutinvizsgálatok közé.

Radiológiai módszerek

Radiológiai módszereket ritkán használnak az orr átjárhatóság vizsgálatára, bár röntgen vizsgálatot alkalmaznak az orrmelléküregek jellemzése során.

A röntgensugaras vizsgálatokkal szemben egyre gyakrabban fordul elő a komputeres tomográfia (CT) használata, különösen az orrmelléküregek értékelése során.

A mágneses rezonanciás vizsgálat (MRI) szintén használatos az orr átjárhatóság értékelésében, elsősorban akkor, ha kóros elváltozásokat gyanítunk a háttérben, mint például rosszindulatú daganatok megjelenését az orrüregben és az orrmelléküregekben. Ilyen esetekben az MRI valószínűleg helyettesíteni fogja a CT-t a nyálkahártya leírása során is.

Egyéb módszerek

Az orr átjárhatóság mérésére használt egyéb módszerek, mint például a külső ellenállás növekedésének szubjektív értékelése, vagy a tiszta oxigén belégzésének mérése, illetve más áramlás mérési módszerek, melyeket fentebb már említettünk, szintén előfordulnak, ugyanakkor ezek egyike sem bizonyult sikeresnek. [93]

---

[92] EccLEs R, JAWAD MS, MORRIS S. The effects of oral administration of menthoion nasal resistance to airflow and nasal sensation of airflow in subjects suffering from nasal congestion associated wi th the common cold. J Pharm Pharmacol 1990; 42: 652-654.

[93] OPHIR D, ELAD Y, DOLEv Z, GELLER BERNSTEIN C. Effects of inhaled humidifled warm air on nasal patency and nasal symptoms in allergic rhinitis. Ann Allergy 1988; 60: 239-242.

Akusztikus tükröződések

Történeti áttekintés

Az akusztikus tükröződés technikája folyamatosan fejlődött ki a keresztmetszeti területek meghatározására, mint a humán légutak távolságának függvénye. Kezdetben, mintegy 40 évvel ezelőtt, a tüdők mechanikus akusztikai tulajdonságait vizsgálták és ennek elektronikus analóg módszerét vezették be a légutak átfogó modellezésének elősegítésére. Akusztikus tükrözéseket elsősorban az Egyesült Államokban, geofizikai kutatásokban használtak, olaj után kutatva. Az 1950-es, 60-as években különösen nagy érdeklődést váltott ki az akusztikus tükröződések használata a légutak vizsgálatával kapcsolatban. Akkoriban a hangképző utak geometriájának leírására használták ezt a módszert, a beszéd rekonstrukcióval kapcsolatban. A későbbiekben leírt módszerekhez hasonlóakat alkalmaztak az ajkaktól a glottiszig terjedő távolság funkcionális leírására. Az egyik legnagyobb probléma abban az időben a vizsgálat számítógépesítésének módszere volt, mely a visszatükröződési tényező megállapításához volt szükséges. Egy új módszer, melyet később Ware-Aki algoritmusnak neveztek el, került kifejlesztésre, mely még mindig az egyik leghatékonyabb algoritmusnak számít az inverz probléma megoldásában, azaz egy impulzus válaszból származó impedancia kiszámítására.[94] Az akusztikus tükröződés technikáját az 1970-es, 80-as években vezették be a garat és a légcső mérései során.

Módszertani aspektusok

A keresztmetszeti területek meghatározására, a légutakban mérhető távolságok függvényeként használt módszer viszonylag egyszerű. A véletlenszerű hang impulzus, vagy a pszeudorandom zaj a hallható frekvencia tartományban összehasonlításra kerül a kapott válasszal, vagyis a légutakból jövő visszatükröződésekkel. Természetszerűleg, ha a légutak bejáratának méretét ismerjük, akkor a visszatükröződések mérete a légutak méretének változását jelenítheti meg. A visszatükröződések között eltelt idő megadhatja a változások közötti távolságot a hang sebességének függvényében. Ily módon lehetséges a terület meghatározása a légutakban mért távolságok függvényében. Adott terület-távolság függvény alapján különféle változókat lehet meghatározni. Az orrban a minimális keresztmetszeti terület, az orr űrméret 0-5, vagy 0-7 cm az orrbemenettől, amennyiben a görbe integ-

[94] MARSHALL 1. lmpedance reconstruction methods for pulse reflectometry. Acustica 1992; 76: 118-128.

rációja alapján becsüljük meg, illetve amennyiben egyes sajátos anatómiai struktúrák alapján ítéljük meg (lásd lentebb).

Csőrendszerben egydimenziós hang terjedés esetén az akusztikus impedancia változásai egyenesen arányosak a keresztmetszeti terület változásaival. A számítógépek technikai fejlődése lehetővé tette a visszatükröződések mintavételét, tárolását és kiszámítását.

Az akusztikus visszaverődési technika ösztönösen egyszerű elve ellenére a terület-távolság függvény kiszámítása a véletlenszerű és visszavert impulzusokból mégis egy némileg összetett számítási átalakítást igényel. Az eredeti beállítások (az orrban és az alsó légutakban, rövid impulzussal keltett véletlenszerű hullám, illetve a visszaverődések közötti időszakos szünet révén) a rendszert viszonylag érzéketlenné teszik a hangimpulzusban és a mikrofon linearitásában bekövetkező kisebb változások iránt, mivel a véletlenszerű és a visszavert hullám jeleit a frekvencia tartományban hasonlítják össze. Ezért el kell végezni az adatok Fourier-féle és inverz Fourier-féle átalakítását is.

Két bemeneti jelet használnak: a rendszer és a mérés kalibrálásáét. Az első bevitt adat (a kalibráció) a mérési rendszer impulzusra adott válasza beleértve a hangforrás és a mikrofon jellemzőit is. Gyakorlatban ezt az impulzusra adott választ úgy mérik, mint a véletlenszerű impulzusnak a visszatükröződését, melynek során ez a véletlenszerű impulzus nagy ellenállású zárt csövön keresztül terjed, amely össze van kötve a mérőcsővel. Ez megszabja „a mérőrendszer" sajátosságait, meghatározza a mérés kiindulópontját és megadja a terület méretét. A második bevitt adat az aktuális üreg mérési adata, melyben a terület-távolság függvényt a műszerrel kell megbecsülni. A visszatükröződésnek az üregből történt felfogását követően a műszer jellemzőinek a visszatükröződésre gyakorolt hatását elnyomja az első adat bevitel „convolutiója". Az ezt követő „deconvolutio" a Hunt-féle algoritmust használja, mely egy frekvencia tartomány számítási technika az amplitúdó eltérések kompenzálására. Mivel a deconvolutio-t a frekvencia tartományban végzik az algoritmus két kötelező jellegű FFT átalakítást tartalmaz (előre-vissza). A deconvolutio-ból származó output (származó adat) az üreg megmért impulzus válasza. Az utolsó lépés során a megmért impulzus választ át kell alakítani terület-távolság függvénnyé. Ahhoz, hogy ezt az inverz problémát megoldjuk, mint ezt a fentiekben már leírtuk, a Ware-Aki-féle algoritmus került alkalmazásra.[95]

[95] WARE JA, AKI K. Contimous and discrete inverse scattering problems in a stratified elastic medium. 1. Plane waves at normal incidence. J Acoust Soc Am 1969; 45: 911-921.

Elméletileg ahhoz, hogy ezzel a technikával megbízható mérési adatokat kapjunk egy sor előfeltételnek kell teljesülnie.

Az első feltételezés az, hogy a hanghullám terjedése lapos (sík) hullámszerű a kereszt módozatok elkerülése érdekében, melyek a számításokat nehézzé tennék. Az elmélet alapján ki lehet számítani azt a frekvenciát, ahol a kereszt módozatok elkezdenek megjelenni. A képlet csak csőre érvényes és az orr bonyolult geometriája lehetetlenné teszi azon frekvencia határok előrejelzését, ahol a kereszt-hullámalakok megjelennek, s így az eredményeket érvénytelenné teszi. A mérések során a kereszt-hullámalakzatokat felismerhetjük, mint a visszavert jel csengetéseit. Normál orrban úgy tűnik, hogy a kereszt-hullámalakzatok nem jelennek meg 12 kHz alatti tartományban és normál körülmények között 15 kHz-ig terjedő, sőt attól magasabb frekvenciákat is használhatunk. A második feltevés az, hogy a súrlódási veszteség elhanyagolható. Amennyiben az orr nagyon szűk az orrbemenetnél, a súrlódási veszteség a szűkületben az ezután következő területek alulbecslését eredményezheti. Nem csak a szűkületnek a mérete, de az alakja is jelentőséggel bírhat. Ezért lehetetlen meghatározni egy olyan rögzített értéket, mely alatt a kapott eredmények megbízhatatlanná válnak. Az aktuális beállítás, különösen az alacsony átmeneti szűrési frekvencia szintén befolyásolhatja a kapott eredményeket. A kapott eredmények azt sugallják, hogy a 0,35 cm2-es terület lehet ez a határ néhány beállítás során. A harmadik feltevés, mely szerint bármely elágazás szabályos (vagyis szimmetrikus) az epipharynx-ig terjedő területre érvényes, ahol a két orrüreg egyesül. Modelltanulmányok és az egyik orrüreg vízzel történt feltöltése azt sugallják, hogy a másik oldalnak az epipharynx-ig terjedő kiegészítő tere csekély jelentőséggel bír és leginkább az epipharynx mögött látható. Végezetül az orrüreg falai merev felületként kell, hogy viselkedjenek. A csontos részek eléggé merevek, de a nyálkahártya már nem annyira. Az emberi szövet vonatkozásában (az arc és a légcső) eredményei azt mutatták, hogy a szövet merev felszínként viselkedik a 120Hz-es frekvenciánál magasabb tartományokban. Az orrnyálkahártya hatásának vizsgálata céljából annak akusztikus tulajdonságait tanulmányozták laser vibrometriával egy férfi vizsgálati alanyon. Ezzel a technikával az orrnyálkahártya specifikus akusztikus elnyelési képességét vizsgálták. Ezt az értéket egy szimulációban alkalmazták a növekvő hangveszteségek hatásának tanulmányozására a visszanyert terület-távolság függvényen (mely hangvesztések az orrnyálkahártya nem merev sajátosságaiból erednek). Összességében a hangvesztésnek több, mint százszorosára kell növekednie mielőtt jelentős változásokat figyelhetünk meg.

Annak ellenére, hogy az összes előfeltétel nem teljesült egészében, az akusztikus visszatükrözési technikát alkalmazó mérések hitelesítése az

orrban (lásd a „Hitelesítés az orrüregben való használatra” c. alfejezetben) elfogadható eredményeket nyújt.

A garatban és az alsó légutakban, akusztikus visszatükrözési technika használatával folytatott méréseket különféle technikákkal hitelesítették. A légcsővel folytatott kezdeti tanulmányokban modelleket, bemetszett légcsöveket és kutyákat használtak, melyek során meglehetősen jó összefüggéseket tapasztaltak.[96] Embereken folytatott vizsgálatok során elsősorban a röntgenográfiás technika alkalmazásával végzett összehasonlítások adtak elfogadható egyezéseket.[97]

Az élő modelleken és például hullákon végzett vizsgálatok eredményei között lévő eltérések egyik oka az, hogy a halál beállta után a légutak mérete megnő.[98] Ez lényegesen megnövelheti az orrmelléküregek behatását. Megvizsgálták, vajon a falak „nem merevségére” vonatkozó feltevés és a behatárolt felbontás részben ellensúlyozható-e egy 20%-ban oxigént és 80%-ban héliumot tartalmazó keverék használatával a környezeti levegő alkalmazása helyett a csőrendszerben és a légutakban. Ebben a keverékben a hang sebessége majdnem megkétszereződik (340m/s-ról 620m/s-ra). Ez lehetőséget nyújt a frekvenciasáv növelésére anélkül, hogy a keresztfrekvenciák elkezdenének megjelenni és mielőtt a felbontást növelni, illetve a pontosságot javítani kellene. A felbontást ugyanakkor nem növelték, mivel a hullámhossz „változatlan” marad. Továbbá a magasabb frekvenciák és a hélium alkalmazása magasabb technikai körülményeket támaszt a felszereléssel szemben. Néhány héliumot alkalmazó tanulmányban a hanggenerátor képessége arra, hogy elegendő energiát sugározzon magas frekvenciákon, kérdésessé vált. Bár a mikrofonok frekvenciatartománya megnő héliumos közegben, ezen a ponton szintén jelentkezhetnek technikai problémák. A hélium legfőbb hatása valószínűleg az, hogy csökkenti a frekvenciasáv alsó részét (a levegőhöz viszonyítva), ahol is a falmozgások hatásai befolyással lehetnek a mérésekre, bár néhány szerző ezt más nem részletezett tényezőknek tulajdonítja.

---

[96] JACKSON AC, KREVANS JRJ. Tracheal cross-sectional areas from acoustic reflections in dogs. J Appl Physiol 1984; 57: 351-353.

[97] D'URzo AD, LAWS ON VG, VASSAL KP, REBUCK AS, SLUTSKY AS, HOFFSTEIN V. Airway area by acoustic response measurements and computerized tomography. Am Rev Respir Dis 1987; 135: 392-395.

17GUILMETTE RA, WICKS JD, WOLFF RK, MAUDERLY JL. In vivo measurement of human nasal airway dimensions. ITRI Annual Report. Alberquerque, NM: ITRI, 1992; 101-104.

A garatban hélium használatával nem kaptak egyértelműen jobb eredményeket. Ugyancsak nem volt javulás az eredményeket illetően, ahol egy modellben levegőnek, vagy 80% hélium és 20% oxigén keverékének használatával is azonos eredményeket kaptak.

„A hullámot szállító közeg" sűrűségének hatása mellett vitatták azt is, vajon egy másik algoritmusnak a terület-távolság számítás utolsó lépcsőjében történő használatával javíthatóak-e a kapott eredmények. A tanulmányokban különféle algoritmusokat használtak, de a mai napig nem találtak olyan algoritmust, mely jobb visszanyerést produkált volna, mint a Ware-Aki algoritmus. A Ware-Aki algoritmust nagyon időigényesnek tartották, de az új számítógépek megjelenésével ez már nem jelent problémát. Szimulációs modelleken nyert, eddig még nem publikált adatok azt sugallják, hogy a visszatükrözött jel egyszerű integrációja a legtöbb esetben összehasonlítva a Ware-Aki számítással meglehetősen jó eredményeket fog adni.

Akusztikus rhinometria

Az akusztikus visszaverődési technika alkalmazása az orrüregben

Az akusztikus visszaverődés módszerének alkalmazása az orrüregben először 1989-ben került leírásra. Mint említettük, a humán légútban már 20 évvel korábban történtek vizsgálatok ezzel a technikával. 1989-ig 35 tanulmány foglalkozott a pharynx és a trachea állapotával az akusztikus visszaverődés alkalmazásával. 1989 és 1999 között 230 közleményben említik e módszert az orrüreg leírására. Ugyanakkor ebben az időszakban csupán néhány közlemény jelent meg a garat és az alsóbb légutak akusztikus visszaverődés technikájával történő vizsgálatáról. Ennek fő oka a vizsgálatok technikai jellegében rejlik. Először is, az orr hozzáférhetőbb a vizsgálat szempontjából, mint az alsóbb légutak. Másodszor, a szájtól a garat és a légcső irányában a jelentős keresztmetszeti felület-változás megnöveli a torzulások előfordulásának kockázatát. Speciális száj-adapterrel ugyanakkor sikerült a torzulást kiküszöbölni, s ez lehetővé tette magasabb frekvenciák használatát, javítva ez által a felbontó képességet. Egy másik közlemény a száj-adapter nélkülözhetőségét vizsgálja, ugyanakkor itt a felbontó képesség nem minden esetben volt optimális.[99] A módszer klinikai alkalmazása az orrban elterjedtebb, mint a légcsőben, de pontossága a garatban igencsak vitatható, a hang száj felé történő elszivárgása következtében, ha a

[99] RUBINSTEIN 1, McCLEAN PA, BOUCHER R, ZAMEL N, FREDBERG JJ, HOFFSTEIN V.
Effect of mouthpiece, noseclips, and head position on airway area measured by acoustic reflections. J Appl Physiol 1987; 63: 1469-1474.

mérést az orron keresztül végzik, vagy az orr felé történő elszivárgás során, ha azt a szájon keresztül vizsgálják. Végezetül, a számítógépek alacsonyabb ára is közrejátszhatott abban, hogy a módszer iránt megnőtt az érdeklődés.

Ezek a tényezők kedveznek az akusztikus visszaverődési technika alkalmazásának az orrüregben.

Technikai aspektusok a módszer alkalmazására az orrüregben

Az akusztikus visszaverődés technikája az orrüregben nem tér el lényegesen az alsóbb légutakétól.

Mint az már a Módszertani vonatkozások fejezetben említésre került, néhány alapfeltételnek (lapos hullámok, elhanyagolható viszkozitásvesztés, szabályos elágazások és merev falak) teljesülnie kell az optimális eredmény elérése érdekében.

A hangvesztéssel kapcsolatos sajátos aggodalmak miatt különleges figyelmet fordítottak erre a területre, mivel az orrüreg szűk résekből tevődik össze, melyek hangvesztést indukálhatnak a falakon való súrlódás következtében. A nem merev falak következtében fellépő hangvesztés elhanyagolható, amint azt lézeres vibrometriával demonstrálták (lásd a módszertani vonatkozások alfejezetben).

Az orrüreg speciális felépítésének következtében fellépő hangvesztést különféle módszerekkel mérték.

Ez magában foglalt olyan modell konstrukciókat, melyekben a megnövelt felülethez állandó keresztmetszeti felület tartozott. Egy további modell konstrukcióban a keresztmetszeti terület ugyanakkora, mint az orré, de itt „cirkularis geometriával” értékelték a felület-távolság függvény hiba előfordulását a kerülethez viszonyítva, melyet a vizsgált személyekben MRI segítségével határoztak meg.

Nem találtak összefüggést a felszín vonatkozásában sem a sztereolitográfiás modellel (az egyén orrüregének MRI-vel történt vizsgálata alapján), sem pedig a felszín-kerület arányú modell alkalmazásával, illetve a felszín-távolság függvényének állandó felszínű, de megnövelt felületű modellezésével sem.

Egy másik tanulmányban, melyben az MRI vizsgálatok eredményét hasonlították össze az akusztikus rhinometriáéval, a kerületet az orrüreg minden egyes távolságának vonatkozásában megmérték és kiszámították az eltérést az MRI és az akusztikus rhinometria által adott adatok között.

A maximális eltérést a legnagyobb kerület vonatkozásában találták, mely arra utal, hogy a nagy kerület és a potenciálisan kiterjedt hangvesztés jelentősége nem nagy a vizsgált személyekben.

A hélium (80%) és az oxigén (20%) levegő helyett történő alkalmazásának hatását már tárgyaltuk (lásd a Módszertani vonatkozások alfejezetben).

Később modell tanulmányok segítségével bebizonyították, hogy különösen az arcüreg ostium mérete és a sinus mérete befolyásolhatja a felület-távolság függvényt.

Egy különleges technikát: szterolitográfiát alkalmaztak az in vivo orrüregek, beleértve az orrmelléküregek ekvivalencia modellezésére.

Ezeket a modelleket más tanulmányokban is alkalmazták. A vizsgált személy MRI képét digitális úton átviszik a CAD rendszerre, ahol a zajt manuális úton eltávolítják. Ezt követően a modellt ezekből az adatokból építik fel, egy folyékony műanyaggal telt medencében, mely ultraibolya fény hatására megszilárdul. Ezt az eljárást a modell scanelési képének és a vizsgált személy MRI képének összehasonlításával hitelesítették.

Nagyon közeli egybeesést figyeltek meg a vizsgált személy és a modell letapogatási képe között.

Ezen eredmények alapján az arcüreg vízzel való feltöltése lényegesen megváltoztatja a terület-távolság függvényt élő személyben.

A tanulmány következtetése az volt, hogy az orrnyílástól számított 6 cm-en belül az üreg űrtartalma és a terület-távolság függvény mérése úgymond pontos, de ettől nagyobb távolságban az arcüreg már befolyásolhatja az eredményt, legalábbis, ha az orr nincs eldugulva.

E tanulmányok és a Módszertani vonatkozások fejezetben leírtak alapján számos technikai és fizikai tényező befolyásolhatja a terület-távolság függvény akusztikus visszaverődés technikával való mérését az orrban.

Ugyanakkor ez úgy tűnik, hogy csekély jelentőséggel bír, amint azt az orrüregben alkalmazott technikára vonatozó hitelesítési adatok szemléltették (lásd a „Hitelesítés orrüregben való alkalmazása” című alfejezetben).

Mégis, más tényezők fontosak lehetnek. Néhány szerző állványt javasolt a fej mérés közbeni rögzítésére, míg mások úgy találták, hogy ez valójában megnöveli a variabilitást.[100]

Élő személyeken és modelleken folytatott vizsgálatokra alapozva megvitatták, hogy a normális orrkagyló vajon jelentős szűkületként fog-e szerepet játszani, befolyásolja-e a mérést, illetve, hogy ezek a mérések mennyire pontosan esnek majd egybe a szubjektív értékeléssel.[101] A szűkület hatását

[100] FISHER EW, BOREHAM AB. Improving the reproducibility of acoustic rhinometry: a customized stand giving control ofheight and angle. J Laryngol Ot ol 1995; 109: 536-537.

[101] TOLEDANO A, GALINDO A, GAVILAN J. Relation between minimal cross section and subjective nasal obstruction. Acta Otorrinolaringol Esp 1999; 50: 439-442.

már vizsgáltuk (lásd a Módszertani vonatkozások alfejezetben). Az orr átjárhatóság objektív értékelésének a szubjektív értékeléssel való egybeesése általános probléma, melyet itt részleteiben nem tárgyalunk.

Egy másik fontos tényező a képfelbontás. Szigorúan véve a képfelbontás ebben az összefüggésben az abszcisszán elhelyezkedő értékpontok közötti távolságot jelenti. A pontok közötti távolság fordítottan arányos a műszer mintavételi frekvenciájával. A jel alacsony átmenetű szűrése következtében a mintavétel gyakoriságának növekedése nem biztos, hogy az eredmények információ értékének növekedésével jár. Ezért mind a mintavételi gyakoriság, mind pedig az alacsony átmenetű szűrés hatását lépcsős modellen tesztelték. Úgy találták, hogy a rendszer képessége egy lépcsőfok kiküszöbölésére egyenesen arányos az alacsony átmenetű szűrés gyakoriságával. Azt is megállapították, hogy a mintavétel gyakoriságának az alacsony átmenetű szűrés frekvenciájánál több mint 3-5-ször nagyobbra növelése nem javította tovább a terület mérési pontosságát.

Hitelesítés az orrüregben való alkalmazásra

Az akusztikus visszatükröződés technikájának orrüregben való alkalmazásra történő hitelesítését számos cikkben leírták.

A kezdeti tanulmányban az orrüreg vízzel történő feltöltésének egyszerű technikáját alkalmazták. Az orrüregbe belépő űrmennyiséget mérték együtt az orrnyílásoknál fellépő nyomással, mely az orrüregben lévő víz magasságát jelölte. A megnövekedett űrtartalommal (dV) feltöltött orr részének keresztmetszeti területét becsülték meg a dV/dP értékből, és ezt a távolság függvényében ábrázolták. Jelentős egybeesést találtak mind a modellben, mind pedig a vizsgált alanyokban. Cadaver réteg felvételt hasonlítottak össze akusztikus terület-távolság függvénnyel, melynek során jó egybeesést tapasztaltak. Akusztikus rhinometria során kapott eredményeket hasonlítottak össze MRI felvételekkel, a fő problémának a szövet-levegő határ pontos meghatározása bizonyult. Az elnyelési együtthatókban fellépő viszonylag kis változások (ellentétben az MRI-nél tapasztaltakkal) lényegesen befolyásolhatják a becslési területet.

Továbbá, a levegő és a szövet közötti határ kézi körvonalazása szintén befolyással lehet az eredményekre. Az említett probléma miatt fellépő ingadozások 10-15 %-os eltérést mutattak az eredményekben.

Úgy találták, hogy az elülső rész letapogatási eredményei között nagyobb egybeesés mutatkozott, mint a hátsó részben. Ennek a feltételezésnek a bizonyítására, miszerint ez az eltérés az akusztikus területek és az MRI területek közötti tengely elhajlásának tulajdonítható, egy hátsó letapogatási tengelyt állítottak fel az orralaphoz képest 45-50 fokos szöget bezáró síkra.

Ez jobb egybeesést eredményezett, de még mindig lényegesen túlbecsülte az akusztikus rhinometriával mért területek nagyságát. Az üreg kerületén alapuló korrekciót szintén kipróbálták, de csekély eredménnyel. Ez azt mutatja, hogy a komplex geometria az orrüreg egyes részeiben nem gyakorol jelentős befolyást az eredményekre.

Összehasonlították az orrban akusztikus rhinometriával, illetve a nyomás-áramlási arány meghatározásával (rhinomanometria) kapott legkisebb terület nagyságát. Ez azon a feltételezésen nyugszik, hogy az orr egészében mérhető teljes nyomás különbség kinetikus energiává alakul a legkisebb keresztmetszeti területen. Az eredmények azt mutatták, hogy a rhinomanometriával meghatározott legkisebb keresztmetszeti terület az AR-val mért terület mindössze egy harmada volt. Ennek más magyarázata is elképzelhető, pl. a várt áramlási mintától való eltérés: turbulens / lineáris.

Ez arra utal, hogy az orr egészében a teljes nyomásvesztés nem egy kis szegmentumra korlátozódik.

Más szerzők is nagyfokú egybeesésről számoltak be az MRI-vel, illetve akusztikus rhinometriával vizsgált szabad orrlégzésű személyek keresztmetszeti terület értékei kapcsán. Ugyanakkor rosszabb eredményeket kaptak decongesztánssal nem előkezelt személyeknél.

Egy tanulmányban nagy felbontású orrüreg és melléküreg CT felvételeit hasonlították össze félautomata, terület-távolság függvény alapján kapott számításokkal, illetve akusztikus rhinometria mérés adataival.

Az orrüreg elülső részében összehasonlítható adatokat kaptak, de más eredményekkel összevetve az akusztikus nyom nem volt ilyen kifejezetten körülhatárolható az orrüreg hátsó részében.[102]

Szintén összevethető adatokat találtak egy ugyanilyen technikát alkalmazó tanulmányban 14 krónikus sinusitisben szenvedő betegnél.[103] Hasonló adatokat írtak le egy tanulmányban 9 orrkagyló túltengésben szenvedő betegnél, akiknél CT, illetve akusztikus rhinometria vizsgálatokat alkalmaztak.

A terület- távolság görbén keresztmetszeti területeket mértek a három elhajlásnál, illetve legkisebb szűkületnél és ezt összehasonlították az orrüreg elülső, középső és hátsó részében CT-vel mért 3 legszűkebb keresztmetszettel.

---

[102] DASTIDAR P, HEINONEN T, NUMMINEN J, RAUTIAINEN M, LAASONEN E. Semiautomatic segmentation of computed tomographic images in volume tric estimation of nasal airway. Eur Arch Otorhinolaryngol 1999; 256: 192-198.

[103] PRASUN D, JURA N, TOM! H, PERTTI R, MARKUS R, ERKKI L. Nasal airway volume tric measurement using segmented HRCT images and acoustic rhinometry. Am J Rhinol 1999; 13: 97-103.

Nagyfokú egybeesést találtak az első 2 szűkületnél (P<0,005), de a hátsó részben rossz volt a korreláció.[104]

Egy nemrégiben megjelent, 85 személy merev endoszkóppal és akusztikus rhinometriával kapott adatait összehasonlító tanulmány alapján megerősítést nyert, hogy a terület- távolság görbén az első elhajlás az orr „valvét" tükrözi, míg a második az alsó orrkagyló elülső végét. A terület-távolság görbéből számos személy esetében meglehet határozni a choanákat is, mint a keresztmetszeti területben bekövetkező hirtelen változást.[105]

Három személynél helyi érzéstelenítésben kis golyóknak a középső orrjáratba történő bevezetésének hatását vizsgálták. Ennek során azt tapasztalták, hogy az 5 mm-nél kisebb átmérőjű golyócskák hatását nem sikerült megfelelően megjeleníteni a terület-távolság görbén a középső orrjáratban.[106]

Ennek oka részben a felállított rendszerben és a felbontó képességben is kereshető, de közrejátszhatnak bizonyos fizikai körülmények is, mint pl. egy nagy középső orrkagyló, mely eltakarja a golyócskákat.

Más szerzők hasonló, modelleken és tetemeken végzett tanulmányokban jobb érzékenységet találtak az AR-s vizsgálatra vonatkozóan, ahol 0,3 cm3 golyócskákat is sikerült kimutatniuk (226). A megismétlési tesztek során kevesebb, mint 5 %-os variabilitást mértek az orrüreg űrméretének ismételt mérésénél (227).

Az akusztikus elszivárgás jelentősen befolyásolhatja a mérési eredményeket.[107]

Leírták, hogy a terület-távolság függvényt a légzés is befolyásolja és, hogy ennek következtében a mérés során javasolt a légzés visszatartása.

---

[104] GILAIN L, COSTE A, RICOLFI F, et al. Nasal cavity geometry measured by acoustic rhinometry and computed tomography. Arch Otolaryngol Head Neck Surg 1997; 123: 401-405.

[105] COREY JP, NALBONE VP, NG BA. Anatomic correlates of acoustic rhinometry as measured by rigid nasal endoscopy. Otolaryngol Head Neck Surg 1999; 121: 572-576.

[106] FISHER EW, DALY NJ, MORRlS DP, LUND VJ. Experimental studies of the resolution of acoustic rhinometry in vivo. Acta Otolaryngol (Stockh) 1994; 114: 647-650.

[107] HAMILTON JW, McRAE RD, JONES AS. The magnitude of random errors in acoustic rhinometry and reinterpretation of the acoustic profile. CI in Otolaryngol 1997; 22: 408-413.

Bemutatták azt is (a gyártó nem publikált adatai alapján), hogy a légzési zavarok igen nagymértékben függenek attól, hogy a műszerben lévő mikrofon szellőztetett vagy nem, de nem érzékeny az alacsony frekvenciás nyomás-változásokra.

A terület-távolság mérésének időskáláján a légzést tekinthetjük úgy, mint állandó nyomást, mely befolyásolhatja a mérést.

Azt a kérdést is feltették, vajon megbízható-e az akusztikus rhinometria abban az esetben, ha a környezeti hőmérséklet változik.[108] Sajnálatos módon ebből a tanulmányból nem derül ki, vajon újra kalibrálták-e a rendszert a különböző hőmérsékleti értékek, illetve nagy eltérések esetén (több mint 10 fok Celsius), s hogy vajon a hangsebesség beállításait korrigálták-e. Ebben a cikkben azt is kifejtették, hogy a mérés néhány esetben megbízhatatlan lehet. Ez nem a rendszerben rejlő hibáknak tudható be, hanem az inkább nem kellőképpen felkészített vizsgáló személyeknek. Ezért ugyanezen szerzők azt javasolták, hogy a mérések során szabványosított protokollt kell alkalmazni.[109]

Az orrüregben terjedő hang tengelye, melyet már a korábbiakban leírtunk, befolyásolja a mért területet, de a tengely úgy tűnik párhuzamos az orr alappal az orr „valve”-től kezdve. Bevezetésre került az I-vájat és a C-vájat fogalma a terület-távolság görbén található első két elhajlás leírására.

Azt a feltételt vették alapul, hogy az elhajlások az orr ishtmus és az alsó orrkagyló fejének felelnek meg.[110]

[108] TOMKINSON A, ECCLES R. The effect of ch anges in ambient temperature on the reliability of acoustic rhinometry data. Rhinology 1996; 34: 75-77.

[109] TOMKINSON A. Acoustic rhinometry: its place in rhinology [editorial]. Clin Otolaryngol 1997; 22: 189-191.

[110] LENDERS H, SCHOLL R, BRUNNER M. [Acoustic rhinometry: the bat principle of the nose]. HNO 1992; 40: 239-247.

Dobák Imre

COMMUNICATIONS-GEOGRAPHY - SHORT OVERVIEW OF THE SITUATION OF THE PUBLIC SAFETY COMMUNICATIONS NETWORKS IN THE CENTRAL-EASTERN EUROPEAN COUNTRIES

Introduction

In the last two decades many geopolitical changes have happened in our region. The European Union and NATO have been enlarged and their security policies were also modified. Of course, as the security threats changed, other aspects of security came to the focus, such as environment protection, dangers of disasters, terror threats, or illegal immigration. In the meanwhile the governmental agencies realized that they need new, effective, supporter communications networks to answer the challenge, and it was the time to replace their conventional radio systems, which had been in use for over 20-30 years. This essay tries to give a short brief of the current situation of the Public Safety communications networks in our region (especially in the Czech Republic, Slovakia, Slovenia, Serbia and Romania). The forthcoming Schengen membership of the countries in the region and the eastwards moving EU external borders gives the importance of the topic, but we should not forget about the Hungarian Public Safety communications network which was finished in the first half of this year.

Instead of going into the deep technical details I would like to concentrate on the overview of the Public Safety radio communications networks of our neighbours which would help us evaluate where we are in this field.

The Public Safety communications networks in our region

According to the free encyclopedia on Internet (Wikipedia) „a Public Safety Network is a wireless communications network used by emergency services organizations, such as police, fire and emergency medical services, to prevent or respond to incidents that harm or endanger persons or property". Though Wikipedia is a non-authentic source, the approach in this definition conceives the essence of public safety communication. The most important thing in an emergency situation (traffic accident, environmental disaster or industrial accident, etc.) is that the public safety organizations, such as police, ambulance or fire brigades are able to provide appropriate answer for the event in the shortest time. It's evident that it is feasible with using modern technical equipment, so every PS organization in the world attempt to develop their PS networks in order to improve the efficiency of their work.

At the beginning of the last decade the communication systems of the Eastern-European countries were almost on the same level, which could mainly be characterized as follows:

- old analogue systems,
- independent networks for the different organizations,
- expensive operation and maintenance,
- capability of mostly voice communication,
- obsolescence,
- lack of cooperation capability among emergency communication systems.

So the current users in the different countries defined their expectations related to a new public safety communications network, as:

- wide coverage and capacity of the network,
- cooperation needs with other authorities, can say "interoperability" between agencies and organizations,
- wide spectrum of users,
- ability to operate in crisis situation as well,
- high level of security (authentication, encryption, and other security aspects),
- data services,
- group communication,
- technical interoperability (among the equipment of different vendors) in the network, easy use of devices and broad range of equipment,
- interoperability with the old analogue systems,
- cost effectiveness,
- standard interfaces,
- spectrum efficiency, etc.

Taking everything into account, the list above isn't full but includes the two most relevant technical dimensions: the capacity and the coverage. The network operator has to provide adequate coverage everywhere and anytime, outdoors and indoors, and has to fulfill the capacity demands in densely populated area in an emergency situation too.

Parallel with the development of telecommunications, we have met with the inevitable incursion of new technologies. The technical specifications have been formed in Europe, which created the basis for the public safety communication. Nowadays there are two technologies in Europe, which meet the Schengen requirements: the Tetrapol and TETRA. TETRA is an open digital trunked radio standard defined by the European Telecommunications Standardization Institute (ETSI). Tetrapol, which is based on Ma-

tracom technology, today is a single source proprietary technology of EADS.

In the last years the Tetrapol and TETRA created a wide market in the World and in Europe as well, for many communications companies. The number of TETRA and Tetrapol contracts continuously increased, but it is to be mentioned that in 2005 EADS (as a leading Tetrapol provider) bought Nokia's TETRA branch, so EADS became the supplier of the two technologies standards for public safety telecommunications solutions.

At the end of the nineties the countries of our region felt the need of change, but the planning and the implementation started in different periods. Some countries chose the Tetrapol, others chose the TETRA to build their own nationwide networks. Some already have a nationwide, modern, digital communication network, while others are at the beginning of the process. While the demands of users and experts were constant, the process from the decision to actually establish the networks took a long time for many reasons, such as financial capabilities or the changing of governments.

Czech Republic

In our region the Czech Republic was the pioneer country that appreciated the necessity of a new, digital public safety communications network. The maintenance costs of different analogue systems and the obsoletion of these systems explained the change. The decision was already made in 1994, but the real building-up of the network started in 1999 and finished in 2003.

The implementation of national coverage started in 1999 and the "Prague network" was already built by 2000, before the conference of IMF and World Bank. The success has given countenance to necessity of expansion (14 regional network)[111]. The Czech organizations effectively used the Prague digital network during the flood in the capital, and the network fulfilled the users' expectations during the NATO Summit Conference as well. According to press-matter that can be found on Internet „..In the course of the summit more than 7,000 terminals were deployed on the Prague network providing direct links with the Prague police command center…[112]."

The authorities of Czech Republic chose the Tetrapol standard when they decided to create their public safety communications network. The operator of the network is the Ministry of Interior, but because the efficient and economical utilization they share with other emergency services such as police, fire-fighters, Ministry of Defense, Civilian Protection and Minis-

[111] source: www.tetrapol.com

[112] Double success for TETRAPOL during the NATO summit in Prague (Czech Republic) and US President's visit to Romania - www.eads.net

try of Health. The fully built up Tetrapol network ensures nationwide coverage. The PEGAS provides independent communication capability to each organization, but in the case of emergency situation they can work together.

Frequency band of PEGAS is 380-400 MHz, which is the assigned, harmonized frequency band for public safety networks in the Schengen area.

Main features[113]**:**

- **technology:** Tetrapol
- **coverage:** Nationwide
- **users:** Ministry of Interior, Ministry of Defense, Ministry of Health, police, fire-fighters, etc.
- integrated transmission of speech and data
- compatible with existing analogue radio systems
- capability of end-to-end encryption
- 30 000 users (data from 2004)
- 20 000 terminals (data from 2004)
- 218 Base Stations (data from 2004)
- 42 switches (data from 2004)

Republic of Serbia

At our southern neighbour we have met with 20-30 years old analogue VHF and UHF radio systems, as was the case in the ex-socialist countries in this region as well. The use of the old systems wasn't efficient concerning the liaison communication among the emergency services from the different organizations during their activities, moreover these systems were used mostly for voice communication.

After the decision to establish a new digital network for the Ministry of Interior (MOI) and the Police Force, the contract was signed at the end of 2003 with Motorola (the Serbian distributor is Vlatacom Ltd). A year later the implementation phase (Phase-1) started, and - according to a press release - the whole building-up of the network will take (over three phases) to 2008.

The TETRA network for the Serbian MOI based on DIMETRA IP (IP based TETRA) and consists of 4 switches, 250 base stations, and 20,000 MOI users (the capacity is planned up to 50,000). There are four master sites: Region Belgrade, Region southeast, Region southwest, Region north.

According to the Phase-1 overview of Mladen Vratonjic's TETRA presentation, in Belgrade there are 16 BS, and 25 will be needed to cover Bel-

[113] source of data: Hubert Azemard – Tetrapol Strengths - presentation 2004. and www.tetrapol.com

grade's wider area, where there are already more than 2500 terminals in operation. The network114:

- sized for 7000 users,
- 24 remote dispatcher console in 14 different control sites,
- 4500 encrypted terminals (subscribers),
- 120 mobile data terminals,
- full encryption (air interface),

Concerning the nationwide TETRA network of the Serbian Ministry of Interior and the Police Force we have to mention that - besides Motorola - Sepura, as a network independent supplier has signed a contract to supply TETRA radios to the Serbian Border Police[115].

Main features:

- **frequency band:** 380-385 MHz and 390-395 400 MHz
- **technology:** TETRA
- **coverage:** Beograd, Novi Sad, Niš and Corridor E10 (March 2005)
- Beograd coverage is 95% (street level), and 75% (indoor).
- **users:** Ministry of Interior, police force, etc.

Slovak Republic

In Slovakia the SITNO has been the biggest project concerning the Schengen membership to create a nationwide digital radio communications network. The original supplier's contract was signed in 1997 between the government and the French company Matra Communication (transformed into MCTS), but came into force in 1998. The planed execution (1999) was often delayed, first to 2000 and later to 2003.

Initially the Interior Ministry calculated the cost at 64.5 million Euros, but – according to a relevant article - 122 million euros had been spent on SITNO until 2005[116].

The SITNO project installed by MCTS to three Slovak districts: Bratislava, Nitra and Trnava, so the network is operating in these territories. The network has been developed continuously, according to a Slovakian website[117] the Ministry of Defense invested on Tetrapol terminals for the military police in 2004, which can contribute to the cost effective application of SITNO.

---

[114] Source: May 02. 2007 – Mladen Vratonjic - MOI Republic of Serbia – Tetra Mou – Belgrade

[115] www.tetramou.com

[116] Magdalena MacLeod Spectator staff http://www.slovakspectator.sk/clanok-18376.html [1/17/2005]

[117] Jozef Andacký - Vnútro buduje infraštruktúru pre nové vodičské preukazy – Rezort obrany sa pripravuje na aktívne začlenenie do NATO 20.04.2004.- http://technologie.etrend.sk

Main features[118]:

- **technology:** Tetrapol
- **coverage:** nationwide
- **users:** the National Police, Fire department, Civil Protection, Emergency Medical Services, Security agencies and other authorities.
- 20,000 users
- coverage: Nationwide
- more than 8000 terminals
- 88 Base Station
- 21 Radio Switches
- A/D interface
- voice and data communication
- it's interconnected with the telephone networks

In January 2006 the Slovak authorities signed another contract with EADS where the closing date is November 2007. By the end of 2006 the coverage had to be expanded towards the eastern Slovak-Ukrainian border zone, as it may become an external Schengen border, and - besides the regional networks Bratislava Trnava and Nitra - in the regional networks of Kosice, Presov, Banska Bystrica and Zilina had to be created. In 2007 the main task is to finish the implementing of SITNO.

The network will be the part of the Slovakian "Integrated Defence System" (Integrovaný zachranný systém), and different Ministries (Interior, Health, Economic, Telecommunications) could be among the planned users.

Romania

The authorities of Romania inherited outdated communication systems where the maintenance slowly became expensive. The authorities realized the need of change, and in 1996 started to form the governmental will to create a new, digital radio communications network. So in April 1997 a big step was made towards modernization and a contract was signed with Matra Communication to create the Tetrapol technology Phoenix. Building up of the Phoenix network took from 1998 to 2002.[119] The contract mainly focused on equipment, radios, etc., but in the beginning they didn't think in a wide Public Safety network.

It is in operation since 1998, and is dedicated to the security forces, but the network itself is a multi-users one. The Phoenix is managed and operated by the Special Telecommunication Service (STS).

[118] source of data: Hubert Azemard – Tetrapol Strengths - presentation 2004.
[119] Hubert Azemard – Tetrapol Strengths – presentation, Budapest 2004

Main features of the network: [120]

- **frequency band:** 380-400 MHz
- **technology:** Tetrapol
- **coverage:** Nationwide
- **users:** different security organizations, military and civil forces, etc.
- 40 switches (in 2004)
- 94 Base Stations (in 2004)
- 26 PABX (in 2004)
- voice and data integration
- end to end communication privacy with a high level of encryption

According to press releases on Internet sites there were some successes for the application of the Tetrapol network, for example at the time of George W. Bush's visit to Bucharest in 2002 the digital network was used successfully. On the other hand, the opinion of some Romanian experts and the EADS is different regarding these successes. According to a related Romanian study, during the Pope's trip to Romania in May 1999, there were lots of problems with the network:

- the coverage wasn't enough everywhere (e.g.: there were zones in Bucharest where the users couldn't communicate)
- problems concerning the group communication
- the number of users was decided not in accordance with the users' demands
- some equipment were of poor quality
- etc.

The debate among the Romanian agencies and EADS takes in these days too.

Collaterally with the forthcoming Schengen membership we have found other technical projects concerning the defence of external Schengen borders, which are only indirectly associated with the public safety matter.

In 2004 a contract was signed between Romania and EADS concerning an integrated system for surveillance and securing (including TETRA standard digital mobile radio communications system) for the Romanian border police. It has two phases, and should be completed by the end of 2009.

According to articles on the "Romanian Daily" website the contract's value was 650 million euros but involved duplication with other European programs for the Danube, Danube Delta and the Black Sea surveillance systems, so in 2005 the government renegotiated and eliminated the duplications (the value decreased to 542 million euros). Some months ago there

[120] source: www.eads.com

was another contract with EADS, but the Romanian press is loud again from the scandal of finance of border project.

Slovenia

The Ministry of Interior of Slovenia in 2003 chose the Tetra technology to create such a new digital communications network which meet the Schengen's operational and security requirements and expectations.

The establishment of the nationwide TETRA network is a multi-year project in Slovenia. The first segment started to operate in November 2003 (SELEX Communications). Later, parallel with the forthcoming Schengen membership, Slovenia decided to extend the network and in July 2007 has announced that the SELEX Communications won the contract for extend, so it is the second segment of Slovenia's TETRA Network for Public Safety (Ministry of Interior). The 2 million Euro value contract extends the coverage to 75% of Slovenia and provides service to 3,000 users.[121]

Main features of the network (after the extension):

- **technology:** TETRA
- **coverage:** Nationwide (75%)
- **users:** Ministry of Interior, police forces, etc.

Reportedly the nationwide coverage extension will be made in about 2 years (2009), depending on the financial situation of the government.

Sources:

[1] Jonathan Dolby - Double success for TETRAPOL during the NATO summit in Prague and US President's visit to Romania
[2] IulianBulandra, EADS contract was legal, says former Interior minister – Romania daily
[3] Hubert Azemard – Tetrapol Strengths - presentation Budapest 2004.
[4] Magdalena MacLeod Spectator staff http://www.slovakspectator.sk/clanok-18376.html [1/17/2005]
[5] Misterul celor 200 mill. Din Afacerea Frontiera – www.hotnews.com
[6] Popa Razvan - Securizarea frontierelor – ori 800 milioane, ori 1 miliard de euro – adevarul – 2007.09.26.
[7] Sitno za 800 miliónov – www.hnonline.sk
[8] Sute de milioane de enro tocati si de STS – 2007.05.10. www.stiri.kappa.ro
[9] http://www.dmeurope.com
[10] http://www.bretschneidernet.de
[11] http://www.tetrapol.com
[12] http://www.tetramou.com
[13] http://www.tetrapol.com
[14] http://www.tetrawatch.net/national/tetrapolprofiles.php
[15] http://www.mrrb.government.bg/pdocs/doc_1342.doc.

[121] http://www.unstrung.com és http://www.selex-comms.com

Tibor FARKAS

INFORMATIC NETWORK MANAGEMENT IN THE HUNGARIAN DEFENCE FORCES

As in case of every civilian and military establishments, prominently important for the Hungarian Defence Forces too to control and to ensure his own communication and informatics network in the adequately way. The stationary military networks of the Hungarian Defence Froces has lots of new part and it has to measure up to higher expectations forasmuch it is getting even bigger and labyrinthiner system. It follows, the operation and supervision are more complex works than before. If only one part of the network is getting fail that could cause serious problems and only a well-conducted network management is able to prevent and reconstruct. So the network management is an automatically monitor system that organises different networktools and workstations, using software- and hardwaretools which help the supervisory and maintenance work of duties and managers.

The Network Management Center was created to perform supervision of the network. The twenty-four hours duty ensures uninterrupted functioning of the network system.

Network Management Center (NMC)

Communication and Information System Duty Center

The NMC responsible for the management of the HDF's communication and informatic networks.

The duties supervise:

- microwave communication transport network,
- digital communication network,
- analogue communication network,
- satellite communication lines,
- HDF WAN[122].

In my humble opinion the different parts of the network are performed by different persons. Basically the duty is devided in half. The first one is the signal part, and the second one is the informatic part. The head of these two parts is the Signal Officer on Duty.

[122] HDF WAN: Hungarian Defence Forces Wide Area Network

My firm belief the following duties are necessary to manage a reliably network.

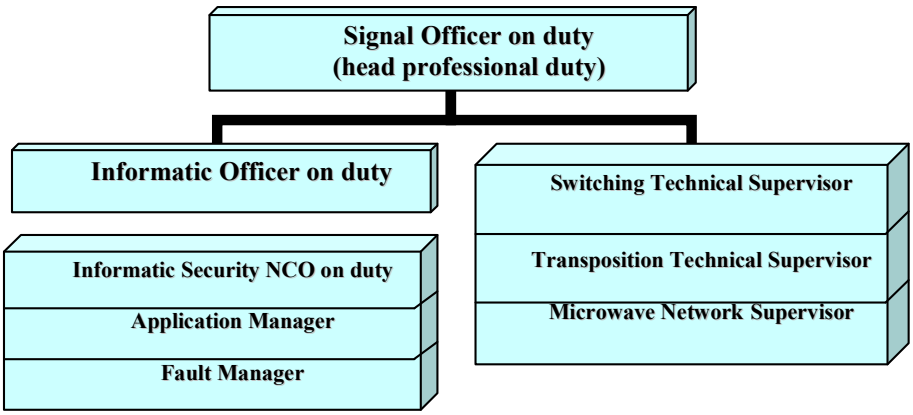


Figure 1: Duty Buildup (possible version)

Informatic Duty (Informatic Network Management)

Generally, the scopes of duties could supervise informatic services, bacground services like virusguard, SPAM, firewall, log file analysis, intruder detection, and some other responsibility areas. The other areas like the HDF WAN and services which are working on it, for example VTC[123], mailing, Internet, Intranet, SMS[124], etc.!

Let's see the scopes of duties in detail.

Informatic officer on duty:

The Informatic Officer on duty responsible for analysing, controlling the elements of the HDF Informatic Network by supervisory appliances. He monitoring the HDF Informatic Network, do the error-rectification, and if it is necessary, the troubleshooting. He always co-operate and co-ordinate with participant of troubleshooting.

The informatic officer on duty is the head of the informatic duty, so he supervise the workgroup (Informatic Security NCO on duty, Application Manager, Fault Manager), assign tasks to them, and when they complete tasks, keep check on results.

The Informatic Officer on Duty has to keep the Signal Officer on Duty posted, because he is head of the duties. Very important task for the effective management, to co-operate with the other duties (Switching

[123] VTC: Video TeleConnference
[124] SMS: Systems Management Server

Technical Supervisor, Transposition Technical Supervisor, Microwave Network Supervisor) and assistance them.

The other important scopes of the officer are the follows:

- keep in touch with military and civilian service companies towards the expidite troubleshooting,
- assistance of missions and manoeuvre,
- hand over the special informatic assignment to the Informatic Main Center (administrators), civilian service companies.

As I wrote previously, the duty monitors the network, and if he finds or gets some errors about the network or appliances, he will record necessary informations by supervisory appliances.

Very important assignment to monitor the frequent occurrence errors, to give variant solutions (to administrators) and to make an end of them

Informatic Security NCO on Duty

He has got some assignments which are the same as the Informatic officer on Duty's, and he has got some different ones.

The Security NCO monitors the Internet and Intranet networks and carry virus-checking out on the network. The NCO always freshenes the virus information, and he installs the last versions. After these steps, he collects the reports wich were made in the course of virus checking, and in case of necessity he can research it.

Always check the firewalls by manager softwares. He does the software freshening and he backups them, beyond that he analyses Log-files and he archives them. He always supervises active network elements.

He has got some special assignments. He has to ensures dispatcher function of HDF Unified Digital Radio System[125], and he has to supervise the FMX2's[126] server. In access networks the FMX2 is able to provide a wide range of analogue and digital leased line services with different transmission rates.

He also keeps in touch with military and civilian service companies, and with the signal parts of the duty.

[125] UDRS: TETRA System
[126] FMX: Flexible Multiplexer

Application Manager

The Applicaton Managers primary assignment to monitor active network elements of the system by supervisory appliances, and to ascertain the causes of structural changes. After that, he enters these datas into NetViz system (for example).

The NetViz is a visualization solution that provides data and information and their relationship in the form of interconnected diagrams.

He setups the last versions of softwares, and follows-up the version-changes. He continually calendars the IP adresses of the network elements and active appliances, and he specifies datas which are in connection with them.

He always analyses the accessibility of the servers and the access control of services. In scope of duties there are other important parts wich are the follows: to create, to erase, to alter users case and to alter users passwords.

In case of failure, he checks the network and the elements, and if it is neccessary, he will configures the active elements. He specifies the detectived errors cause for the fail-safe network.

Fault Manager

The fault manager manages the errors in HICOM system, and monitors the WAN by for instance „Cisco Works LMS" software. „Cisco Works" is a suite of powerful management tools that simplify the configuration, administration, monitoring, and troubleshooting of networks.

He ensures dispatcher function of Unified Digital Radio System, and he monitors the network.

He has to find the error-causing element, and he clears it. If it is required, (failure, configuration) he will check reboot and switch off the ports, cards, trunks. He will change network control, if a data switching exchange turn off.

Troubleshooting and management softwares

The informatic duty's assignment in case of receiving error could the follows:

- Record the informations of the user (name, announcement date, ect.)
- Record the informations of incident

- Appoint professional
- Monitor troubleshooting
- Record results

The management softwares help to make assignments of duty quick, exact and smooth. These could be the follows:

Service Desk

The Service Desk helps the duty control autamate processes, services and infrastructure for all departments of the IT organization. With this software, the duty could manage servicelevel agreements. It shows the infrastructure components on which a service relies, and who is supporting the service.

By the same token:

- Demonstrate the relationship between customers, service-level agreements, and of course support level objectives,
- By multi-tiered SLA capabilities it provides a hierarchical service structure
- Oofers the capability to customize forms, wies and fields ont he fly, withouth the need to bring the server down

VTC Manager

This software is a management tool that enables the administrators/duties to easily support Video Teleconference scheduling, VTC management.

It makes easy for support to reliably video, voice or conferencing services.

Main potentials are as follows:

- Display ongoing conferences
- Manage multiple conferences
- Change video layouts
- System configuration, software downloading
- Advanced conference scheduling

Cisco Works LMS

This application provides for the users/duties a centralized system for sharing device information all LAN management applications, improving manageability, and increasing systemwide awareness.

More provides:

- Network discovery, topology views, end-station tracking and VLAN management
- Monitoring the network, appliances
- Real-time network fault analisys, configureing network appliances
- Hardware and software inventory management, centralized configuration tools
- Syslog monitoring

These management tools could help the duties to manage a faultless network.

If the professionals have many accomplishments, and the applications are higher grade, the management duty will capable carry his work out, actuates fail-safe network.

Erika Kucsera Magyarné

NEW POSSIBILITIES OF WIRELESS TRENDS IN THE AREA OF MOBILE INFOCOMMUNICATION AND MANAGEMENT

In the info communication in field conditions security and flexibility are supposed to be mixed in the appropriate measure. It is not beneficial or possible to use fixed means of telecommunications in general through missions and exercises. Some of the mobile connection means (for example satellite communications) are very expensive, although they are more protected from eaves dropping , and illegal access to information. Some of the voice and data transfer does not require special protection, so in these areas it is advisable to be more open towards more cost effective implementations. Besides, in some areas and situations there is no possibility for the installation of stationer, e.g. cable connections, so it is recommended to be open towards radio implementation both in voice and data communication and in management. There are more and more possibilities to establish good quality telecommunication services, capable of quick movement with the help of more secure WLAN[127] solutions, GSM[128] and WIFI[129] cooperations and femtocells.

The quick cost effective installation of WLAN and bluetooth devices is a great advantages on territories lacking infrastructure and in places where the staff is stationed for a short time and where the physical work of laying the cables necessary for the non radio based data transfer would take unrealistically much time and would incur high expenses.

The satellite communication in the case of certain natural phenomena (e.g. sun spot activity) or technical fault, maintenance is not capable of providing stable connection. However, permanent connection with the operational staff is a basic requirement, therefore, for secondary connection mode, it is highly recommended to use of GMS bridges, adapters, which, in a given area, can be flexibly combined with the WLAN network eventually with bluetooth devices through UMA[130]. I would definitely emphasize that this form of implementation cannot, or only under strict restrictions, be used in operational areas.

127 WLAN: Wireless Local Area Network
128 GSM: Global System for Mobil communication
129 WiFi:Wireless Fidelity
130 UMA: Unlicensed Mobile Access

The security of WLAN

In the field communication, taking into consideration quick installation, secure wireless based and flexible network management, the WLAN solutions can be easily applied but great attention is needed for the basic security of the network,

Although the WLAN solutions are not the most secure connection modes, the bad experience mainly comes from the fact that along with their revolutionary application in the civil sphere the users were not (and are not even today) aware of why and how they need to protect their wireless connections.

For the basic security function, on the routers, (which usually have the AP function), it is important to set the password and encryption methods. The supported codification of WLAN cards AP[131]-s and routers is to be identical, if our equipment supports it, it is more advantageous to use, instead of WEP, the more secure WPA[132] codification which, with dynamic encryption and effective validation and codification, can eliminate the security gaps occurring with the application of WEP due to the fact that the WEP can be cracked with freely accessible devices in a short time by all the users. A common key for validation and encryption with the WEP but for WPA 802.1x[133] protocol is needed and the users' individual keys are produced and updated by the PS-s. The 802.1x is a flexible validation protocol based on an EAP.

The safety of operation for the wireless technologies can be ensured with the appropriate installation conditions, by installing the device in a protected area and by the installation of two-antenna devices which, if possible, operate in a diversity mode and which monitor the quantity of the received sign and which send and receive the packages in the more favorable way.

Although the WAN networks are not the most secure connection modes, they correspond to the requirement of open transmission if the above mentioned WPA or WPA2 protocols are used and with careful user behavior and with the application of VPN[134]-s, their management can also be carried out. Their use can be valuable in the course of mission activities and participation in exercises alike. Due to this fact, they can substitute or com-

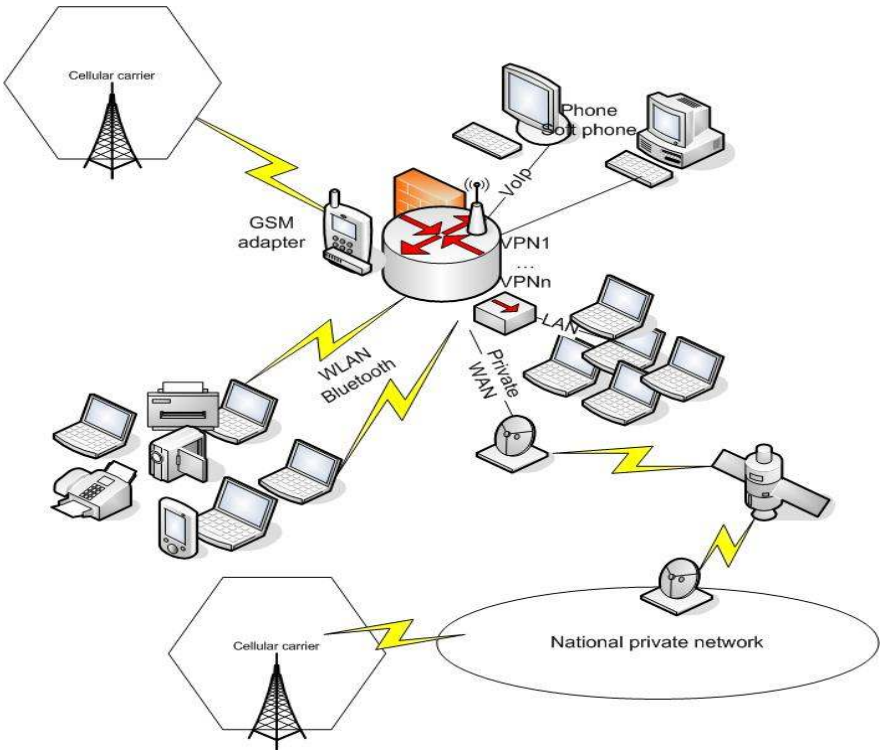
131 AP: acces point

132 WPA: Wi-Fi Protected acces

133 802.1X: IEEE 802.1X is an IEEE standard for port-based Network Access Control; it is part of the IEEE 802 (802.1) group of protocols.

134 VPN: Virtual Private network

plement suitable equipment, until their installation, the voice and data services provided by satellite connections.



Implementation with secure router

In the commercial market it is very easy to buy such integrated WLAN routers which, as multifunctional devices, provide routing, switching and double firewall functions, offering necessary access to public or private networks. They support the previously mentioned WPA and 802.1x user validation as well as the VPN access from the point of you of security functions. All of these means provide continuous broadband connection for the devices of the network which the user can access wireless or through the built in switch.

These WLAN routers are capable to satisfy the informatics needs of the operational staff on unreachable areas either through GSM or cable based and complemented with a mobile center or with IP telephony they can satisfy the requirement of voice communication very cost effectively. When planning, it must be taken into consideration how many AP-s are needed on the operational area (depending on type: containers, yards, buildings). The actual implementation from the host nation can only be planned in theory

based on rules of general validity. As there can be a difference between an empty or equipped container in spreading conditions it is vitally important to supervise in practice the quality of the covered area on the previously equipped working area and to optimize the conditions accordingly.

The network connection to the host nation can be, according to the most often used method, for example the VSAT[135] connection. In highly separated places where after an armed conflict it is difficult to quickly install the necessary antenna, indoor system, temporary communication and management of perfect security can be ensured even by temporary portable satellite connection. With this solution the necessary position for the special task can be occupied in a very short time and even on an area with considerably damaged infrastructure the required voice and data transmission and management can be safely ensured.

On areas lacking infrastructure the weak point of the telecommunication services can be the provision of energy supply. It can be a good solution, besides minimizing the energy consumption, to open up to new solutions besides the reliable applications. When the local electricity network is damaged and the necessary energy supply is hindered, the use of generators and, as an alternative, for example photocell-based battery energy supply is a good solution.

Alternative solutions

In exercises, when for example there is a possibility to test communication task solutions in a multinational cooperation, in a country with GSM system there is a chance to integrate, to use and to test a newly spreading technology UMA which uses mobile telephone networks and WIFI applications. With this technology, which is provided by the mobile company in several countries, voice and data transfer can be performed through WIFI and GSM networks in a way that roaming between them does not interrupt the transmission. The greatest advantage of this technology can be seen in places where the mobile providers already support the free voice connection through WLAN hot-spots, and this way the info communication needs of deployable troops can be covered on a large area cost effectively. Taking into consideration the present world tendencies, these services will be accessible in every country where there is no civil war in a short time.

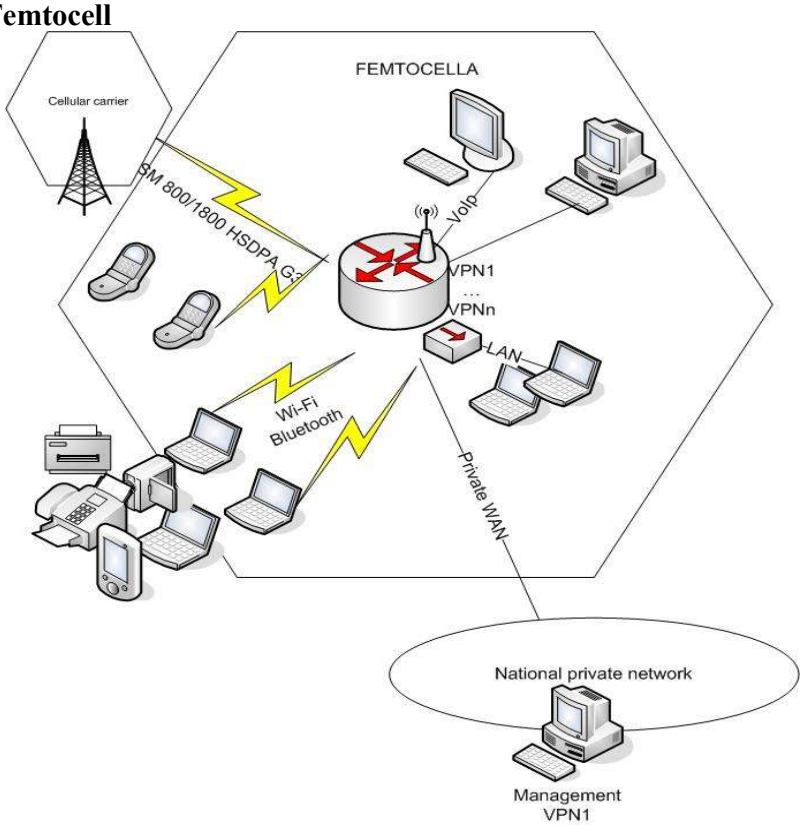
From the point of security, the product developed by a well known company supports the convergence of service providers of UMA and WLAN. This offers a new and multi-managed solution designed for the protection of service providers, IP and voice infrastructures and a secure fix

135 VSAT:Very Small Aperture Terminal

mobile convergence. According to the preliminary promise, the IPsec and VPN technology ensures safe roaming cellular and WLAN networks.

The UMA technology, based on estimations of world market tendencies, will be available on a large scale in countries with a developing and with a developed market in a short time. After this happens it is recommended by all means to test usability because this technology expectably a needs very flexible use of equipment and low expenses.

Femtocell



The femtocell is a special mobile mini cell of 50-30-meter range and the device which produces this is available for users at a very low price. The device, which can be installed anywhere by the use,r expends, besides others, the areas of application of high speed mobile services (3G[136], HSDPA[137]) due to the fact that these services can be accessed on the areas covered by cell provided by the router with devices with mobile phones and data cards. The router will have WLAN and WAN ports and this way it will give the possibility of combining the wireless and cable based broadband

136 3G: the third generation of mobile phone standards and technology
137 HSDPA: High-Speed Downlink Packet Access

services. Using IP telephony, through the router's VoIP[138] port making a phone call will be even more cost effective. Mobile service providers are planning to obtain permission also for a cable based broadband network connection.

Considering energy management, it can be a great advantage that our mobile devices can connect to femtocells with a lower transmitter performance and so the battery operation time can become longer.

Mobile service providers' market offers are still not completely known. Its initial series were designed with SIM cards by the providers, thus securing the exclusive services of their own devices. However the second series designed without SIM cards, usable for all authorized service providers' devices, can be more favorable for operational info communications.

According to statements the femtocells designed for the market by the end of the year, will provide great advantages for operational info communications on territories where it can ensure even partial coverage because the quality of the connection with the deployed staff will be increased by the combination of WIFI and cable based technology.

The quick spread of femtocells all over the world is expected in five years.

Summary

One of the most important needs of mobile telecommunications is to ensure the conditions of quick movebility, which certainly cannot hinder the security of the network. WLAN networks can be used well in open info communication both in missions and in exercises because they perfectly satisfy the above mentioned needs due to the mobile and flexible equipment provision. The WLAN routers ensure the access to the WAN, LAN networks with different connection modes, their usability for the operational staff and for the host nation. Considering safety, the codification and encryption standards presented in the article provide the necessary protection at present in the face of the actual threats. Unfortunately, however it is almost impossible to provide complete protection because the techniquesand methods of illegal intelligence are continuously developing, therefore it is justified to establish only real protection (corresponding to the importance of the information). This goal is fulfilled by the facts mentioned above.

It is recommended by all means to test the UMA and the femtocell technology after they have become accessible. They can be used on areas where

138 VoIp: Voice over Internet Protokoll

there is at least partial mobile coverage because of their connection to mobile infrastructures in the area of field communication. This fact can be a serious obstacle in mission activities on operational areas and where the infrastructure is damaged. But in exercises and in some peacekeeping missions their use, especially when broadband services are also applied, can be favorable. The femtocell version offers more possibilities because besides involving the network it can converge the mobile, WLAN cable based communication at areasonable costs. The degree of the adaptation in field telecommunications of the development tendencies here presented can be specified only after testing in national and international exercises. However the services mentioned above are to be considered by all means.

References

[1] Joseph Davies: Biztonságos vezeték nélküli hálózatok: Microsoft Windows alatt az IEEE 802.11 szabvány. Bicske Szak., 2005.

[2] Jim Geiger: Vezeték nélküli hálózatok. Budapest Panem, 2005.

[3] Edney, Jon. - Boston, Mass. [etc.]:Real 802.11 security. Addison-Wesley, 2004.

[4] Halácsy Péter: Hatalom a mobiltömegek kezében. Budapest Typotex, 2007.

[5] Marcin Wojnicz,Lukasz Rygiel, Michal Martynkiewicz, Lukasz Sawicki: Segédlet WLAN hálózat tervezéséhez. Ostel-invest 2007.

[6] Kristóf Csaba: Nem lesz olcsó a WLAN biztonság. / 2007. szeptember 4., 08:08 http://computerworld.hu/hir/44913/print

[7] Mick Buer: WLAN-ok védelme WPA és freeRadius alkalmazásával./ 2005 május 133. szám www.linuxjournal.com/article8134

[8] Berta Sándor: Dániában debütált az első UMa szolgáltatás 2006. augusztus 31. 21:08. http://www.sg.hu/cikkek/46876/daniaban_debutalt_az_elso_uma_szolgaltatas

[9] Ady Krisztián: A helyi mobilcellák jelentik a mobilkommunikáció jövőjét? http://www.hwsw.hu/hirek/33678/netgear_zonegate_femtocella_3g_hsdpa.html

[10] Bizó Dániel: Wi-Fi helyett 3G: robbanás előtt a femtocellák elterjedése? http://www.hwsw.hu/hirek/34017/femtocell_femtocella_in-stat_3g_hsdpa_wifi-wi-fi_wimax.html

[11] Computerlinks Kft. A Check Point új biztonsági megoldása a konvergált szolgáltatói kommunikációhoz http://www.computerlinks.hu/html/np.php?contentid=4747

[12] http://www.computerlinks.hu/html/np.php?contentid=4748

[13] http//en.wikipedia.org

NÉMETH András

TÁVLATI MŰHOLDAS MEGOLDÁSOK A KATASZTRÓFAVÉDELMI KOMMUNIKÁCIÓ TERÜLETÉN

Bevezetés

Veszély és katasztrófahelyzetekben a védekezési és elhárítási munkálatok hatékonysága nagymértékben függ a rendelkezésre álló híradó és informatika vonalak, és a vezetéknélküli csatornák számától és minőségétől. A kommunikáció megbízhatósága és rendelkezésre állása, azaz a híradó biztonság attól függ, hogy adott információ továbbítására hány alternatív megoldás, hány hírközlő rendszer vehető igénybe.

A rendelkezésre álló, földi infrastrukturális elemekre épülő rádiótávközlő rendszerek (EDR[139], GSM[140]) mellett – azok sérülése, meghibásodása esetén, vagy ha a rendelkezésre álló kapacitások nem képesek kielégíteni a felmerülő igényeket – a különböző űrtávközlési megoldások is alternatívát jelenthetnek. A kizárólag VSAT[141] és SCPS[142] alapú műholdas szolgáltatásokra épülő híradás azonban nem az egyetlen lehetőség.

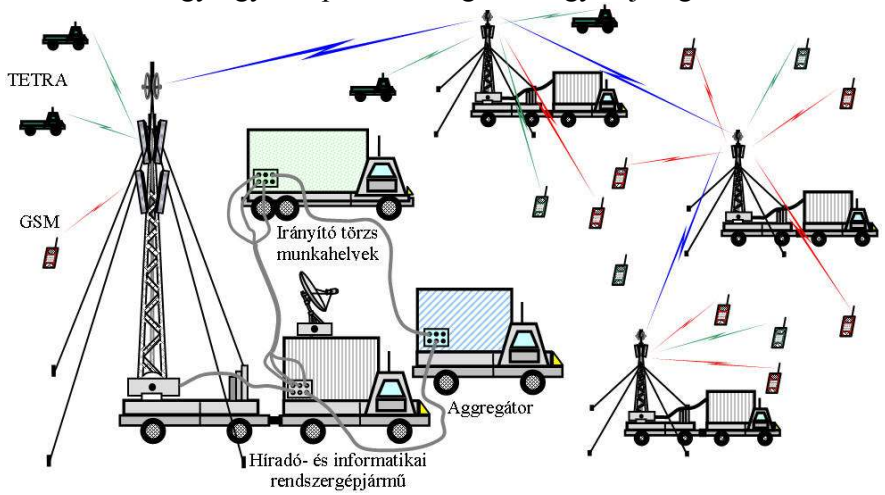
Vegyes struktúrájú megoldás a veszélyhelyzeti hírközlésben

A híradó biztonság növelésének egy lehetséges módja a műholdas megoldásokra épülő gerinchálózati struktúrát, illetve az alárendeltek vezetését biztosító EDR illetve más mobiltelefon hálózatok képességeit integráló rendszer kialakítása. Ehhez olyan mobil vezetési komplexumok kialakítására van szükség, amelyek az OKF[143]-fel és a regionális igazgatóságokkal továbbra is VSAT műholdakon keresztül biztosítják a megfelelő számú hang- és adat-összeköttetést a különböző vezetési szintek között, míg a kárhelyszíneken az alárendelt (végrehajtó) állomány vezetését a mobil vezetési pont (MVP) híradó és informatikai rendszergépjárművébe (HIR) integrált TETRA[144] és mobiltelefon bázisállomások teszik lehetővé. Nagyobb területek lefedésére a rendszerbe további mozgó bázisállomások telepíthetők, melyek mikrohullámú relén, vagy optikai kábeleken csatlakoztathatók az ideiglenes kommunikációs központba. A rendszer egyes elemeinek tápellátását autonóm áramforrások, aggregátorok biztosítják. Az így kialakított ideiglenes hálózat a HIR HiPath központjának trönkkártyáin keresztül bármely helyi, országos, vagy nemzetközi hírközlő rendszerhez

[139] Egységes Digitális Rádiótávközlő Rendszer
[140] Global System for Mobile Communications
[141] Very Small Aperture Terminal
[142] Satellite Personal Communication System
[143] Országos Katasztrófavédelmi Főigazgatóság
[144] Terrestrial Trunked Radio

közvetlenül is illeszthető, ha azok megfelelő csatlakozási felületei rendelkezésre állnak. Ez a konstrukció lehetőséget biztosít a kialakult helyzet által megkövetelt, vegyes felépítésű kommunikációs rendszer kialakítására, ami a földi (fix) telepítésű infrastruktúra különböző mértékű sérülése – akár teljes megsemmisülése – esetén is képes a védekezésben résztvevő készenléti és együttműködő szervezetek vezetési, valamint szükség esetén polgári személyek információs igényeinek kielégítésére.

A koncepció az *1. ábrán*, míg a híradó- és informatikai rendszergépjármű felépítse a *2. ábrán* látható. A HIR interfészein keresztül csatlakozik a hálózathoz a védekezést a helyszínen irányító törzs számítógépes és telefonos munkahelyeit magába foglaló komplexum, de illeszthető hozzá mobil diszpécserközpont is, melyben a központi munkahely mellett minden résztvevő szervezet egy-egy diszpécsere dolgozhat egyidejűleg.

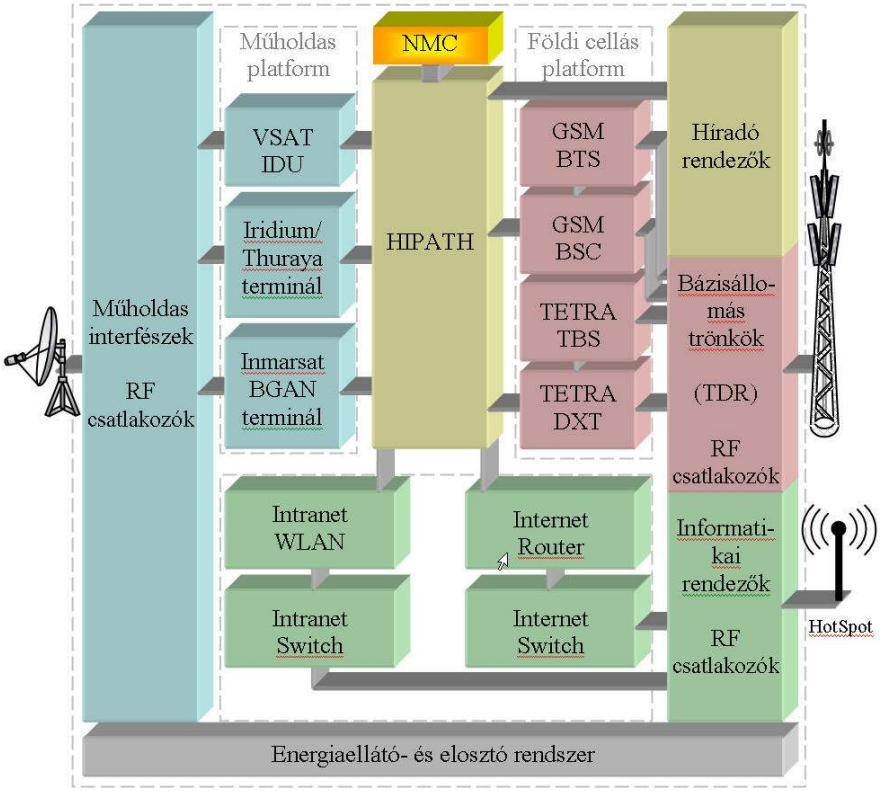


1. ábra: Vegyes műszaki megoldásokat alkalmazó koncepció

A híradó- és informatikai rendszergépjármű az űrtávközlési szolgáltatások közül a VSAT-ot alkalmazza a magasabb vezetési szintek felé történő információtovábbításra, míg az alárendeltek felé elsődlegesen TETRA és GSM felületet biztosít, akár a fixen telepített rendszerektől teljesen függetlenül, akár azok integráns részeként. A többi műholdas eszköz elsősorban a tartalék szerepét tölti be, biztosítva ezáltal a közvetlen műholdon keresztül történő vezetés lehetőségét is. A vezetési pont környezetében a vezeték nélküli eszközök HotSpot-on keresztül is kapcsolódhatnak az informatikai hálózathoz.

A komplexum fizikai kialakításánál figyelemmel kell lenni az alkalmazás körülményeire, például hogy a felázott talaj következtében kialakuló terepviszonyok miatt a járművek nem képesek megközelíteni a kritikus területek ellátásához szükséges magaslatokat, vagy a kialakult helyzet

gyors megoldást tesz szükségessé (hirtelen kialakuló váratlan katasztrófa-helyzet).



2. ábra: A híradó- és informatikai rendszergépjármű (HIR) felépítése

3. ábra: Katonai kivitelű mozgatható bázisállomás komplexum (Illusztráció, Forrás: ARMCOM)

Ilyen esetekre kifejezetten a védelmi (katasztrófavédelmi) igények kielégítésére alkalmas olyan mozgatható komplexumok és bázisállomások kialakítása célszerű, melyek rendkívüli viszonyok között is a jelenleg alkalmazottaknál jóval gyorsabban telepíthetők és üzembe helyezhetők. Ezen

követelményeknek kizárólag katonai szempontrendszer alapján kivitelezett eszközök felelnek meg. A speciálisan kialakított, a környezeti hatásoknak ellenálló konténert, és a mozgatható univerzális antennatornyot a telepítő személyzettel együtt, akár magas terepjáró-képességű katonai tehergépjárművel (*3. ábra)*, akár szállítóhelikopterrel a helyszínre lehet juttatni.

Ez a megoldás nagyobb egyszeri befektetést igényel ugyan, hosszútávú üzemeltetése azonban költséghatékonyabb.

Speciális védelmi- és veszélyhelyzeti műholdakra épülő híradás

A katasztrófavédelem kommunikációs igényeinek saját műholdas rendszerrel történő kielégítése valószínűleg a legnagyobb egyszeri befektetést igénylő megoldás, azonban óriási előrelépést jelenthet mind a védelmi, mind a kormányzati hírközlés területén.

Egy saját kommunikációs műhold előállítása és pályára állítása egy kis ország számára akkor lehet reális és hosszútávon gazdaságos, ha biztosítani tudja annak hatékony kihasználását és széleskörű alkalmazását a védelmi célú igények kielégítésén túl, polgári szolgáltatások megvalósítására is. Magyarország jelenleg nem tagja az Európai Űrügynökségnek (ESA[145]), melynek következtében a magasan kvalifikált elméleti és gyakorlati beállítottságú hazai szakemberek (kutatók, mérnökök) nem vehetnek részt közvetlenül a kontinens fejlett űrtevékenységében, pedig ez nagy lendületet adhatna a hazai kutatás-fejlesztésnek. Az Űrügynökség tagjaként lehetőségünk lenne közösségi forrásokat is bevonni az anyagi fedezet megteremtésébe (akár 50%), míg a szükséges berendezések jelentős részét hazai egyetemek (BME[146], ELTE[147], ZMNE[148]), kutatóintézetek (KFKI[149]), fejlesztő cégek és távközlési vállalatok közösen – a meglévő ESA infrastruktúrát is igénybe véve – képesek lennének megtervezni és megépíteni. A vállalkozás gazdaságélénkítő hatása mellett a hazai szakembergárdának és high-tech iparnak is lehetőséget adna, hogy új területen bizonyítsa képességeit.

A műholdas rendszerre vonatkozó elképzeléseim a következők:

- a rendszerrel szemben támasztott részletes követelményeket elsődlegesen a védelmi szféra határozza meg (dolgozza ki) az érintett tárcák szakembereinek bevonásával (HM[150], IRM[151], GKM[152]);

[145] European Space Agency
[146] Budapesti Műszaki és Gazdaságtudományi Egyetem
[147] Eötvös Lóránd Tudományegyetem
[148] Zrínyi Miklós Nemzetvédelmi Egyetem
[149] Központi Fizikai Kutatóintézet
[150] Honvédelmi Minisztérium
[151] Igazságügyi és Rendészeti Minisztérium
[152] Gazdasági és Közlekedési Minisztérium

- az űrszegmenset alkotó műhold geoszinkron pályán kering olyan pozícióban, ami biztosítja Magyarország mellett az európai, észak-afrikai, közel-keleti és közép-ázsiai területek lefedését, ezáltal lehetővé téve a Magyar Honvédség külföldi missziókban tevékenykedő alegységeinek anyaországgal történő, illetve szükség esetén belső híradását;
- a műhold korszerű fedélzeti berendezései az elektronikus hírközlési szolgáltatások széles körének megvalósítását teszik lehetővé a nap 24 órájában az év 365 napján (a földárnyék által okozott üzemkiesés kiküszöbölése, illetve az ellátott terület növelése érdekében egy 15°-kal eltolt másik GEO[153] műhold pályára állítása is célravezető lehet);
- a központi műholdvezérlő földi állomás a Magyar Honvédség Támogató Dandárjának felügyelete alatt üzemel egy megfelelően védett katonai objektumban, míg gateway-ek kerülnek telepítésre több kulcsfontosságú szervezetnél (HM, MH ÖHP[154], légierő objektumok, OKF, IRM, NBH[155] stb.);
- a műhold szélessávú transzponderein rugalmasan konfigurálható dedikált kapacitások kerülnek kijelölésre katonai, rend- és határvédelmi, kormányzati, nemzetbiztonsági, katasztrófavédelmi, és polgári célokra; egyes speciális feladatok (pl. missziós híradás) biztosítására állandó kapacitás van fenntartva, míg az erőforrások többsége csak speciális helyzetekben (veszélyhelyzet, minősített időszak stb.) kerül védelmi/katasztrófavédelmi célzattal igénybevételre; normál időszakban az erőforrások üzleti célú bérbeadásával, a rendszer létrehozási- és fenntartási költségeinek egy része, vagy egésze fedezhető lenne;
- a költségek fajlagos csökkentése a térség államainak bevonásával, vagy részükre történő szolgáltatások biztosításával tovább csökkenthető;
- a rendszer által a védelmi és katasztrófavédelmi szféra számára biztosított szolgáltatások:
    - a rendszer minden felhasználó számára (terminálóktól függően) biztosítja a hang-, adat-, videó-összeköttetések, SMS[156] küldés/fogadás, számítógépek és hálózatok összekapcsolásának lehetőségét. (polgári felhasználóknak normál időszakban)

[153] Geostationary Earth Orbit
[154] Magyar Honvédség Összhaderőnemi Parancsnokság
[155] Nemzetbiztonsági Hivatal
[156] Short Message Sevice

- a zártcélú hálózatok gerincvonalainak tartalékolása, valamint az együttműködő szervezetek hálózatainak összekapcsolása a földi hálózatok sérülése esetén (VSAT jellegű)
- összeköttetések biztosítása a missziókban tevékenykedő alakulatok parancsnokságaival (VSAT jellegű)
- a műveletei területeken történő híradás taralék vonalainak biztosítása. (SCPS jellegű)
- katasztrófahelyzetben az OKF, regionális igazgatóságok, MVP-ok, valamint az együttműködők különböző vezetési szintjeinek összekapcsolása a földi infrastruktúra sérülése esetén (VSAT jellegű)
- katasztrófahelyzetben a védekezésben résztvevő állomány vezetésének biztosítása a földi infrastruktúra sérülése esetén. (SCPC jellegű)
- flottakövetés a védekezési munkálatokban résztvevő szállítójárművek és munkagépek mozgásának koordinálására (GPS[157]/EGNOS[158]/ GALILLEO vevőkkel kombinált műholdas kommunikációs eszközök)
- „digitális harctér" megvalósítása: harci repülőgépek és helikopterek, szállítógépek, szállító- és harcjárművek, „digitális katonák" követése, felderítési adatok (csapat- és mélységi felderítő, tűzmegfigyelő, radar, harctéri szenzorok stb.) gyűjtése szétosztása, célkoordináták terítése, tűzvezetés (fegyverterminálok, tűzvezető komplexumok stb.) pilótanélküli repülőgépek, harctéri robotok, fegyverek távvezérlése.

Összefoglalás

A katasztrófavédelmi és együttműködő szervek híradásának biztonsága párhuzamos kommunikációs vonalak alkalmazásával jelentősen növelhető. A műholdas rendszerek veszélyhelyzetekben megoldást jelenthetnek egyes felmerülő hírközlési anomáliák kezelésére a földi mobil rádiótelefon hálózatok által nyújtott szolgáltatások kiegészítésével, vagy adott esetben pótlásával. Rövidtávon a VSAT és SCPS rendszerek szolgáltatásainak megvásárlása jelentheti az űrtávközlési alternatívát, azonban speciális híradó és informatikai komplexumok alkalmazásával optimálisabb erőforrás-gazdálkodás valósítható meg, a földi cellás rendszerek képességeinek integrált felhasználásával. Hosszútávú javaslatom bár messze túlmutat a katasztrófavédelem felmerülő hírközlési igényeinek kielégítésén, a „saját" műholdas rendszer – éppen a tervezés rugalmasságából adódóan – maximálisan képes biztosítani a szükséges mennyiségű és minőségű alternatív hír-

[157] Global Positioning System
[158] European Geostationary Navigation Overlay Service

adó vonalat. A járulékos előnyök és komplex védelmi alkalmazási lehetőségek figyelembevételével ez egy optimális megoldásnak tekinthető. A megbízhatóság tovább növelhető a három űrtávközlési koncepció különböző elemeinek vegyes alkalmazásával.

Felhasznált irodalom

[1] PÁPICS József, KASZAVITZ Iván, KOCSIS Ferenc, DOBREFF Csaba, SZARKA Gábor, VENYINGI Teofil: Bevezetés a digitális üzleti űrtávközlésbe – hallgatói segédlet – Bp.: SAT-NET Műholdas Szolgáltató Kft. – 1993. – p. 11-40.

[2] GÖDÖR Éva: Műholdas hírközlés – tansegédlet – Bp.: BME – 2003. – p. 11-35. (http://micro3.mht.bme.hu/MuTa/muholdas.pdf)

[3] DÁRDAI Árpád: Mobil távközlés, mobil internet – Mobil Ismeret – Budapest – 2002. – ISBN 963 440 996 2 – p. 175-180.

Zoltán MEDVECZKI

METHODOLOGICAL MEASUREMENT OF NASAL AIRWAY

Methods to evaluate nasal patency

History

Examination of the nasal cavity has been described more than 3000 years ago (Papyrus Ebers), for instance by Egyptian medical doctors and also in the mummification process of the Pharaohs, where the brain was removed through the nose. Examination of the no se has also been described by Hippocrates in Greece (460-377 B.C.). To improve the view into the nasal cavity different means have been used. Guy de Cehauliac has referred to a nasal speculum in the 13th century.

More systema tic evaluation of nasal patency was described in the late 19th century by Zwaardemaker and modified by Glatzel in 1901. Differences in patency of the two sides of the nose was evaluated by the difference in the condensed area of water on a metal plate placed in front of the nasal cavity during expiration. Other, at best semiquantitative methods included the hum-test by Spiess (1902), where external occlusion of the nonoccluded side of the nasal cavity is experienced as a change in the timbre of sound during humming or simply as a differencein the sound during forced expiration for each side of the nasal cavity separately (Bruck, 1901). These qualitative methods, some of which are still in use, are highly dependent on the mode of respiration and the capability of the subjects to carry out the tests. A measurement of the pressure drop over the nasal cavity at a passive flow has been described in 1903 by Courtade and is one of the first descriptions of rhinomanometry. Since then, rhinomanometry has been used in more than 500 studies described in international papers. The first paper describing acoustic rhinometry was published in 1989.

Opticai methods

The most commonly used opticaI method for evaluation of the nasal cavity passage is rhinoscopy. Although rhinoscopy should be included in all clinical evaluations of nasal patency, different studies have shown that a clear-cut relation between anterior rhinoscopy, subjective evaluation or other tests is not always present.

Using a flexible rhinoscope may improve the results of the examination of nasal pathology and in certain cases for operations, but the results using the endoscopic examination do not necessarily correlate with

rhinomanometry for evaluation of nasal patency.

Different optic devices have bé en used to characterize or quantify nasal patency. Rhinostereometry is a method for measurement of the distance between the medial and lateral wall of the nasal cavity. The distance is determined using an inbuilt scale in a microscope, and the he ad position has to be fixed to assure measurements at the same position during repeated measurements. This gives only limited information of isolated structures and not of the larger part of the nasal airway.

Video recording during flexible endoscopy allows sub se que nt evaluation of the results, but is still an invasive procedure and may not be the optimal method for evaluation of nasal patency.

Quantitative acoustic methods

Methods using sound or analysis of sound in the airways have been used to characterize the size of the airways or an obstruction in the larynx, nasal cavity, and paranasal sinuses, to determine the location of snoring problems, and in the upper airways and epipharynx. Despite these attempts to use more or less subject generated sound to evaluate the patency of the airways the methods have so far not been very successful.

Flow methods

Flow measurements for the evaluation of the nasal airway passage have been used more or less systematically for the last five decades. The simplest way is to measure the maximum flow - the nasal peakflow. In this case the power of the driv'ing force, the chest wall, and lower airways, have influence on the nasal expiratory or inspiratory peakflow. Different authors have tried to reduce the factor by calculating an index between nasal and oral peakflow. Despite the fact that correlations between nasal peakflow and other methods to evaluate nasal occ1usion have been found, nasal peakflow seems to be most suitable to measure changes in the same subject during repeat ed measurements.

In rhinomanometry simultaneo"\ls measurements of flow and pressure are performed. Different techniques have been applied using the subjects own respiration flow (active methods) or using an external flow generator (passive methods). The matching flow is measured in the anterior part of the nasal cavity (anterior methods) or in the pharynx (posterior methods).

The active methods are more frequently used th an the passive anterior method and the passive posterior method. Results may differ between the anterior and posterior method although others find quite similar results with the methods.

Rhinomanometry has also been correlated with other tests normally used

for pulmonary function, e.g. body plethysmography and the forced oscillation technique and reasonable correlations have been found.

The repeatability in rhinomanometric measurements ranges from 10 to 30% and therefore some authors find it unusable for precise evaluation of nasal patency.

One essential problem is the description of the flow-pressure relationship. Because of the nonlinear relationship between flow and pressure, different methods have been adopted, e.g. using an Ohmic resistance at a specified flow or pressure rate, using a power function in the description, or other models (e.g. Rohrer's equation). The angle between the abscissa (flow) and the intercept between the pressureflow curve and a circle in coordinate system (Brom's system) or the relative difference of the two sides; a lateralization index, have also been used.

The rhinomanometric resistance may also be expressed as a minimum cross-sectional area of the nasal cavity and some authors find this to be the best way to depict resistance. It assumes a complicated model of the flow in the nasal cavity and the models being used may not always give the 'true' area at different flow regimes. The slit like structure demands special requirements of the models since the flow profile in the nasal cavity may be nonuniform and change between laminar and turbulent flow.

Furthermore, the localization of a deviation affects the resistance evaluated by rhinomanometry. A deviation of the septum at the nasal valve affects the resistance more than a deviation in the posterior part of the nasal cavity.

Different attempts have been made to standardize rhinomanometry to allow comparison of the results from different studies. Rhinomanometry has been used in different aspects of rhinology, e.g. in the diagnosis of different rhinologic diseases, in allergy tests, in pharmacological studies, and in physiological studies. Certain authors have found that rhinomanometry is usefuI in the selection of treatment, e.g. operation or not, or as a tool for evaluation of operative procedures, whereas others find the present techniques unsuitable for these purposes.

In some studies a clear correlation between the subjective fee1ing of nasal occlusion and rhinomanometry has been found, in others a poor correlation, because other factors than just resistance influence the fee1ing of nasal obstruction. It is well known that menthol relieves the feeling of nasal obstruction, whereas the nasal resistance to airflow is unchanged.

Some of the drawbacks of rhinomanometry are relatively low reproducibility; low correlation to subjective fee1ing of nasal obstruction, no uniform way of describing results, different techniques may be used- viz anterior, posterior, active, passive, and it is therefore not used in daily clinic routine, except in a few laboratories.

Radiological methods

RadiologicaI methods are seldom used in the investigation of nasal patency, although X-ray examination has been used in relation with evaluation of the paranasal sinuses.

Computer aided tomography (CT) is increasingly used instead of X-rays especially in evaluation of the paranasal sinuses.

Magnetic resonance scanning (MRI) is also used for evaluation of nasal patency, primarily if pathological changes are suspected, e.g. malignancies in the nasal cavity and paranasal sinuses, and will probably replace CT for evaluation of the mucosa.

Other methods

Other methods for evaluation of nasal patency have been described, e.g. subjective evaluation of increasing extemal resistance, measurements of O2 while breathing pure oxygen, other flow methods than described above. None of these methods have been successful.

Acoustic reflections

History

The acoustic reflection technique for determining the cross-sectional area as a function of distance in the human airways has developed gradually. The mechanoacoustical properties ofthe lungs were initially examined 40 years ago and electrical analogues were introduced to facilitate comprehensive modelling of the airways. Acoustic reflections have been used in geophysical investigations especially in the United States of America with regard to search for oil. The use of acoustic reflections from the airways gained special interest in 1960-70 for determining the geometry of the vocal tract with reg ard to speech reconstruction. Methods similar to those described later were used to examine the area as a function of distance from the lips to the glottis. One of the main problems at that time was the computational procedure for recovering successive areas from the coefficients of reflections. A new method (later named 'the Ware-Aki algorithm') for this procedure was developed and is still one of the most efficient algorithms for solution of the inverse problem calculation of the impedances from an impulse response. In 1970-80 the use of the acoustic reflection technique was introduced for measurements in the pharynx and trachea.

Methodological aspects

The method for determining the cross-sectional area as function of distance in the airways is relatively simple. The incident sound impulse or pseudorandom noise in the audible frequency range is compared with the response - the reflections from the airways. Intuitively, if the size of the entrance to the airways is known, the size of the reflections may reflect changes of the airway size. The time between the reflections may give the distance between the changes dependent on the speed of sound. In this way it is possible to determine the area as function of distance in the airways. Given the area-distance function different variables can be determined. In the no se the minimum cross-sectional area, the nasal volume O-5 cm or O-7 cm from the nostril estimated by integration of the curve and areas at particular anatomical structures could be of interest (see below).

In a tube system with one-dimensional sound propagation, changes in the acoustic impedance are proportionate to changes in the cross-sectional area. The technological development of microcomputers has made it possible to sampie, store, and calculate the reflections. Figure 1 depicts the reflection pattern of an incident pulse from a tube with multiple changes in acoustic impedance (cross-sectional area).

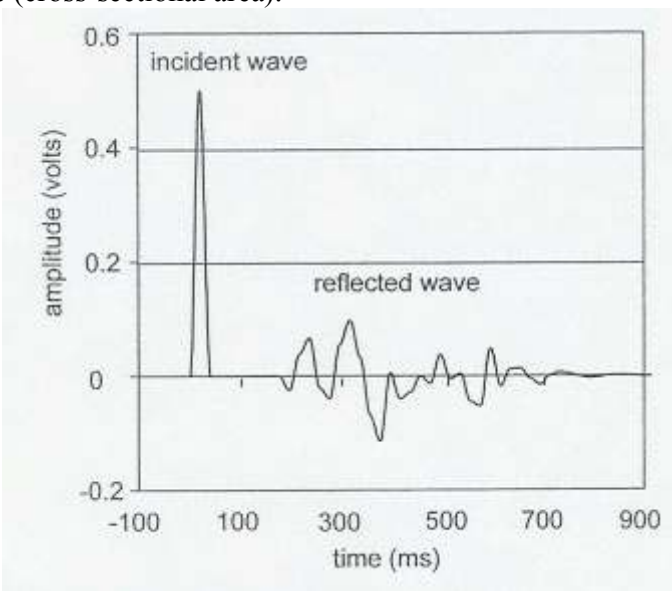


Figure 1. The reflected signal from a nasal cavity.

Despite the intuitively simple principle of the acoustic reflection technique, the calculation of the areadistance function from the incident and reflected impulses requires somewhat complicated arithmetic transformations. The original set-up, for the nose and lower airways with a

short impulse and a temporal space between incident wave and reflections, make the system relative insensitive to minor changes in the sound impulse and the linearity of the microphone, since the signals of the incident wave and reflected wave are compared in the frequency domain. Therefore, it is also necessary to do the Fourier and inverse Fourier transformations of the data. Figure 2 shows the different steps in the calculation.

Two inputs are used: the calibration of the system and the measurement. The first input (calibration) is the impulse response of the measurement system inc1uding the characteristics of the sound source and the microphone. In practice this impulse response is measured as the reflection of the incident pulse from a high impedance (closed tube) connect ed to the mea sur ing tube. This sets the properties of the 'measuring system', defines the starting point of the measurement and sets up the area size. The second input is the measurement of the actual cavity in which the area-distance function (AD-function) is to be estimated by the equipment. After having obtained the reflection from the cavity, the influence of the equipment characteristics on the reflection is suppressed by convolution with the first input. The following deconvolution employs the Hunt's algorithm, which is a frequency domain technique to compensate for amplitude differences. Since the deconvolution is perforrned in the frequency domain, the algorithm contains two implicit FFT transforms (forward/inverse). The output from the deconvolution is the measured impulse response of the cavity. The last step is to transform the measured impulse response into an AD-function. To solve this inverse problem, as described above, the Ware-Aki algorithm has been implemented.

Theoretically, to obtain reliabe measurements wi th this technique a number of assumptions have to be fulfilled.

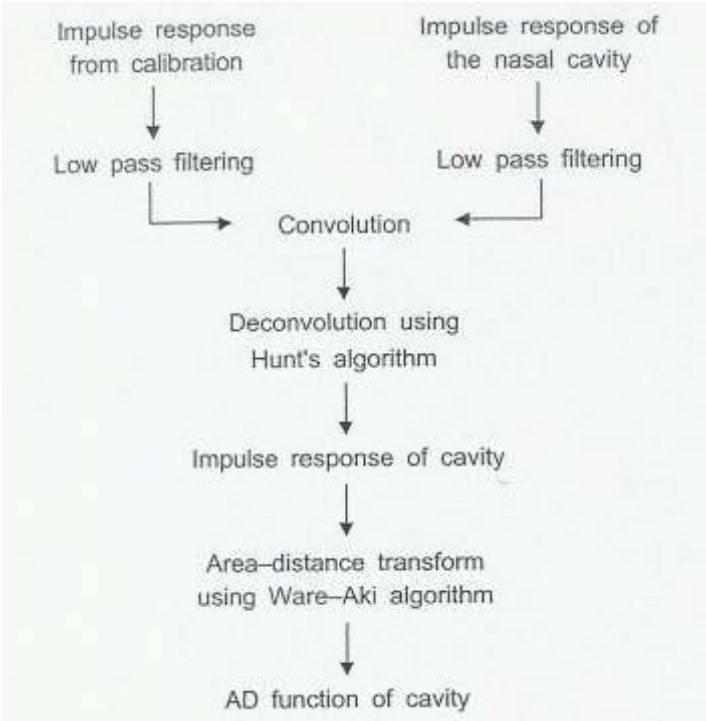


Figure 2. The calculation of the area-distance function for acoustic rhinometry.

The first assumption is that the sound waves propagate as plane waves to avoid cross-modes, which will make the computations difficult. Based on theory it is possible to calculate the frequency at which crossmodes start to appear. The formula is only valid for a tube and the complex geometry of the no se makes it impossible to predict the frequency limit where cross-modes appear and make the results invalid. During the measurements cross-modes can be recognized as a 'ringing' of the reflected signal. In a normal nose cross-modes seem not to appear below 12 kHz and normally frequencies up to 15 kHz or more can be used. The second assumption is that viscous losses are negligible. If the nose is very narrow at the anterior end, viscous loss in the constrietion may induce underestimation of the areas beyond. It is not only the size of the constrietion but also the shape that may have an influence. Therefore, it is not possible to identify a fixed value below which the results could become unreliable. The actual set-up, especially the low-pass filtering frequency may also influence the results. Results suggest the area of 0.35 cm2 in some set-ups could be alimit. The third assumption, that any bifurcations are regular (Le. symmetric), is valid for the distance to the epipharynx where the two nasal cavities join. Model

studies and filling one nasal cavity with water suggest that the influence of the other side adding space to the epipharynx is of minor importance and is mainly seen behind the epipharynx. Finally, the walls in the nasal cavity should behave rigidly. The bony part is rather rigid but the mucosa may not be so. For the human tissue (cheek and trachea) results have indicated that the tissue is behaving rigidly at frequencies greater than 120 Hz. To examine the effect of the nasal mucosa - its acoustic properties were studied in one male subject who was examined by laser vibrometry. By this technique the specific acoustic admittance of the nasal mucosa was examined. This value was used in a simulation to study the effect of increasing sound losses (due to nonrigid properties of the nasal mucosa) on the recovered area-distance function. In summary, the sound loss should be inc re as ed a 100 times before significant effects are se en (see Fig. 3).

Despite all assumptions having not been completely fulfilled; validation of measurements using the acoustic

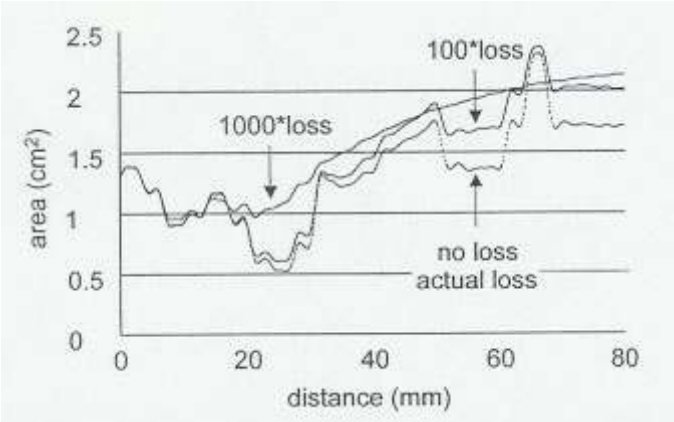


Figure 3. The sound loss due to wall motion, 4 curves are depicted (no loss and actualloss are on top of each other). The error is increased by losses and by increasing distance.

reflection technique in the nose (see the subsection on Validation for use in the nasal cavity) reveals acceptable results.

Use of the acoustic reflection technique for measurements in the pharynx and lower airways has been validated by use of different techniques. In the initial studies of the trachea, models, excised tracheas, and dogs were used and a reasonab1e correlation was found. In humans, comparisons primarily wi th roentgenographic techniques had acceptable correlations.

One of the reasons for differences using in vivo models and, e.g. cadavers is that the size of the airways increases after death. This may increase the influence of the paranasal sinuses considerably. It has been

examined whether the assumption of nonrigidity of the walls and limited resolution could partly be overcome using a mixture of 20% O2 and 80% He instead of atmospheric air in the tube system and in the airways. In this mixture the speed of sound is almost doubled (from 340 mis to 620 mis). This provides' the opportunity to increase the frequency band before cross-modes start to occur and should increase resolution and improve accuracy. The resolution is however, not increased since the wavelength is 'unchanged'. Furthermore, the higher frequencies and the use of He increase the technicai demands of the equipment. The ability of the sound generators, in some of the studies using He, to deliver a sufficient energy content at high frequencies has been questioned. Although the microphones frequency range increases in He (see Brüel & Kjaer manual) technical problems may arise at this point too. The main effect of He is probably to reduce (relative to air) the lower part of the frequency band where effects of wall motion may influence the measurements, although_some authors believe it to be other unspecified factors.

In the pharynx no clear improvement in results were found using He. Neither was there improvement in nasal cavity where identical results were observed using ei ther air or He (80%), O2 (20%) in a model and 8 nasal cavities.

Besides the effect of the density of the 'wavetransporting medium' it has been debated whether a different algorithm for the last step in the area-distance ca1culation would improve the results. Studies have employed different algorithms but, until now (year 2000), no algorithm has shown better recovery than the Ware-Aki algorithm. The Ware-Aki algorithm has been con side red very time consuming but with new computers this is no longer a problem. Unpublished data from simulation models suggest that simple integration of the reflected signal will give reasonable results in most instances, compared with the Ware-Aki-ca1culation.

Acoustic rhinometry

The acoustic reflection technique applied in the nasal cavity

The use of the acoustic reflection technique in the nasal cavity was first described in 1989. As mentioned, the first measurements with the technique in the human airways were done more than 20 years earlier. In the meantime, approximately 35 papers were published in which the acoustic reflection technique was used to study the pharynx and trachea. In the period from 1989 to 1999, more than 230 papers have been published where the acoustic reflection technique has been utilized in the nasal cavity. In contrast, in the same period, few studies on the pharynx llnd lower airways have been reported. The main reason for this is technical aspects.

Firstly, the accessibility of the no se is much easier than the lower airways. Secondly, the significant change in cross-sectional area from the mouth to the pharynx and trachea increases the risk of cross-modes to appear, but a special mouth piece was designed to avoid cross-modes and made it possible to use higher frequencies and thereby increase resolution. Another study indicates that the mouth piece may not be necessary but the resolution may not have been optimal. The clinical application in the nose is wider than in the trachea and the accuracy in the pharynx is debatable due to sound leakage to the mouth if the measurement is done through the nose or to the no se if done through the mouth. Finally, the lowered costs of computers may als o be a factor for the increased interest for the method. These factors favour the use in the nasal cavity of the acoustic reflection technique.

Technical aspects for use in the nasal cavity

In principle, use of the acoustic reflection technique in the nasal cavity does not differ significantly from its use in the lower airways. As mentioned in the subsection on Methodological aspects, some basic assumptions (plane waves, negligible viscous loss, regular branching, and rigid walls) have to be fulfilled for optimal results. Special concerns with regard to sound loss have drawn attention since the nasal cavity consists of narrow slits that may induce sound loss due to friction at the walls. The sound loss due to nonrigid walls is negligible as demonstrated by laser vibrometry. Sound loss due to special geometry of the nose was also examined in different ways. These included construction of a model with increasing surface but constant cross-sectional area, construction of a model with the same cross-sectional area as the nose but with a circular geometry and by evaluating the error of the area-distance function in relation to the circumference determined in subjects by MRI.

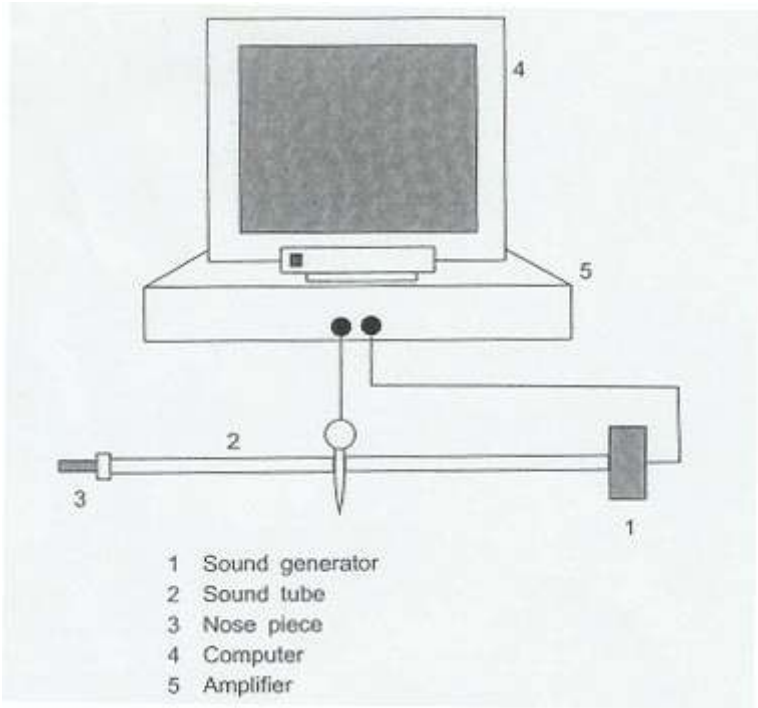


Figure 4. The set-up for acoustic rhinometry.

No effect of the surface was found comparing both a model made by stereolithograhy (based on a MRI scanning of the nasal cavity of a subject) and the area equivalent circular model and also the area-distance function in a model with a constant area but increasing circumference.

In another study comparing MRI and acoustic rhinometry, the circumference was measured at every single distance in the nasal cavity and the deviation between MRI and acoustic rhinometry was ca1culated. The circumference was not directly compare-Ei-with the deviation but is shown in Fig. 5. The maximum error is observed beyond the maximum circumference indicating that large circumference and potentially large sound loss is not important in the measured subjects.

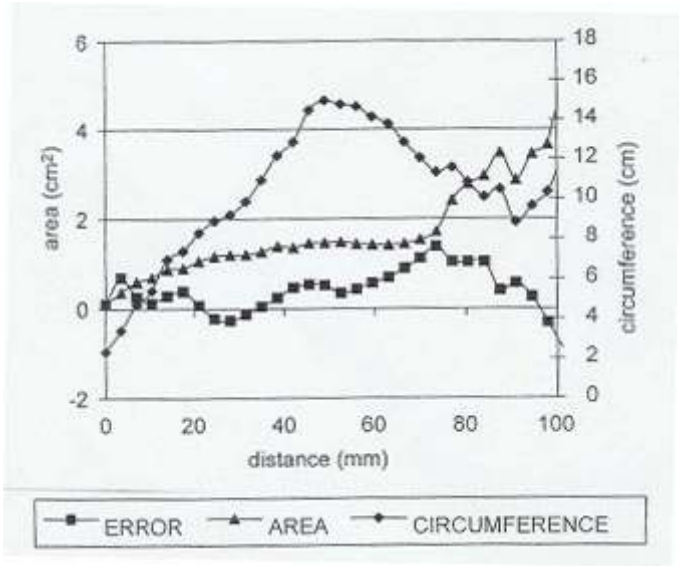


Figure 5, The error in area as a function of the distance in a model. It is seen that the error is not affected by increasing circumference (surface).

The effect of using He (80%), O2 (20%) instead of air has already been discussed (see the subsection on Methodological aspects). Figure 6 shows no effect on the area-distance function in the one subject.

The paranasal sinuses may also influence the measurement, although in the first paper on acoustic rhinometry the ostia were considered too small. It has later been demonstrated by model studies that especially the ostium size of the maxillary sinus and the size of the sinus may influence the area-distance function. A special technique - stereolithograhy was employed to make equivalent models of the in vivo nasa1 cavity including the paranasal sinus es. The models have also been used in other studies. A MRI scan of a subject is digitally transferred to a CAD system where noise is removed manually. Then the model is built from this data, in a bath with liquid plastic, which solidified when exposed to u1traviolet light. The procedure was validated by comparing a scanning of the model with the subject's MRI.

Very close agreement was seen between the original scanning of the subject and the scanning of the model.

In accordance with these results (see Fig. 7) filling of the maxillary sinus with water significantly changes the area-distance function in vivo.

The conclusion of the study was that up to 6 cm from the nostril, the volume of the cavity and the area-distance function are measured 'correctly' but the re after the maxillary sinuses may influence the result at least in the decongested nose.

Based on these studies and as discussed in the subsection on Methodological aspects, many technical

and physical factors may influence the measurement of the area-distance function in the nose by the acoustic reflection technique.

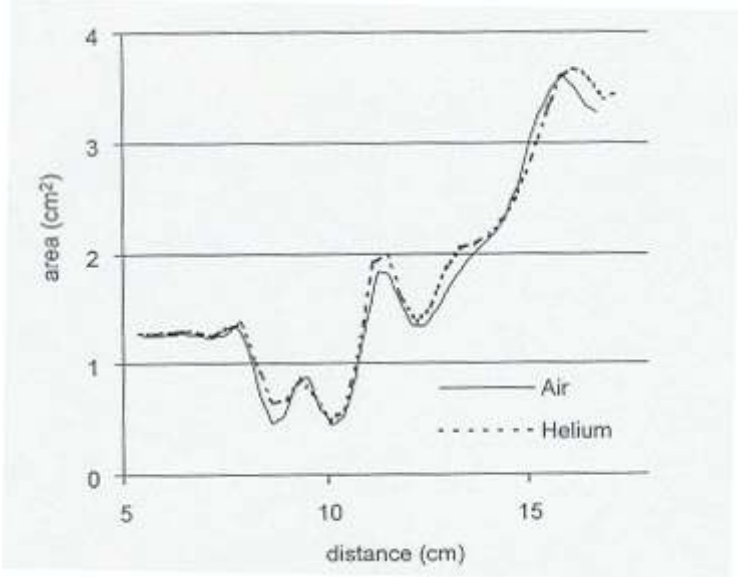


Figure 6. The effect of helium on the area-distance function in a subject.

However these seem to be of minor importance as demonstrated by the validation data for the technique implemented in the nasal cavity (see the subsection on Validation for use in the nasal cavity).

Still, other factors may be important. Some authors have suggested a stand to fix the position of the head during the measurement while others have found that this in fact increases the variability.

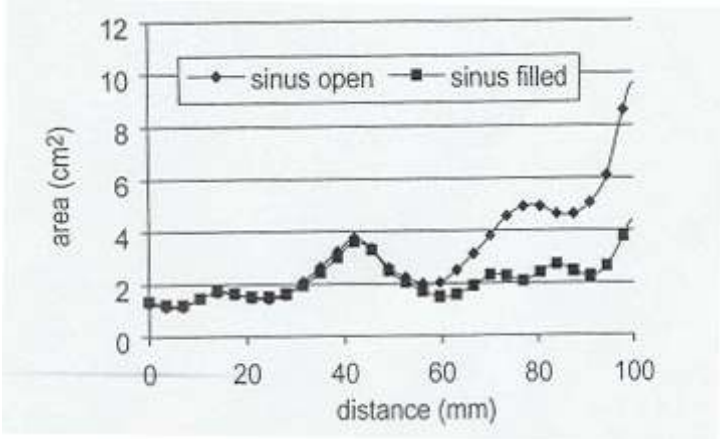


Figure 7. The area-distance function before and after fiIling the maxiIlary sinus with water in one subject.

It has been discussed based on model and in vivo studies whether the normal nasal valve will act as a considerable constriction and affect the measurement and how weIl these measurements correlate with subjective evaluation. The influence of a constriction has already been discussed (see the subsection on Methodologica1 aspects) and the corre1ation between objective evaluation of nasal patency and the subjective evaluation is a general problem, which is not going to be discussed in detail here.

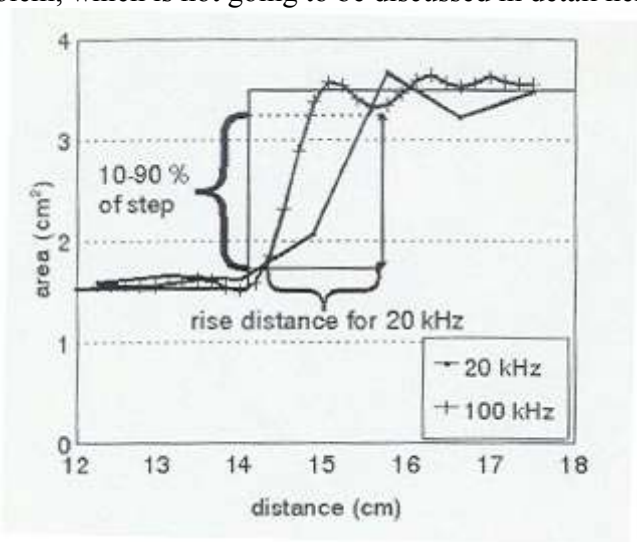


Figure 8. The area-distance function of a step cavity model measured at two different frequencies.

Another important factor is the resolution. Strictly, the resolution in this context is the distance between the data points on the abscissa. The distance between the points is inversely proportional to the sampling frequency of the equipment. Due to low-pass filtering of the signal an increase of the sampling frequency may not increase the information in the results. Therefore, the influence of both sampling frequency and low-pass filtering was tested in a step model. It was found that the system's ability to recover a step is proportional to the low-pass filtering frequency and that increasing the sampling frequency more than 3-5 times the low-pass filtering frequency did not further improve the accuracy of the area measurement. Figure 8 depicts the effect of different sampling frequencies at a constant low pass filtering (10 kHz) in a step model.

Validation for use in the nasal cavity

Validation of the acoustic reflection technique for use in the nasal cavity has been described in a number of papers. In the initial study a simple technique by filling the nasal cavity wi th water was employed. The volume entering the nasal cavity was measured to gether with the pressure at the nostril representing the height of water or distance in the nasal cavity. The cross-sectional areas ofihe portion of the no se filled by the incremental volume (d v) was estimated from d *V/dP* and plotted as function of distance. Reasonable correlation was found in both a model and 5 subjects. In the same study a CT-scanning of a cadaver head was compared with acoustic area-distance function and good correlation was found *(r=0.937, N=48).* Here, as in the following study of 10 subjects comparing acoustic rhinometry and MRI the main problem is the definition of the exact tissue-air boundary. Relatively small changes in the absorption coefficients (contrast in the MRI) may affect the area estimation considerably.

Furthermore, the manual delineation of the border between air and tissue may als o influence the results. The results were found to vary up to 10-15% because of these problems.

In another study of a stereolithographic model where the original scanning of a subject was compared with the scanning of a model (and the procedure had to be performed twice), a deviation of only a few percent was seen.

A study comparing MRI in 10 subjects with the volume of the decongested nasal cavity measured by acoustic rhinometry showed an acoustic volume of 6.47 cm3 (SD = 1.83) and MRI volume of 5.65 cm3 (SD = 1.34) (Paired *t-test P=O.Oll).* The regression line (for alI 20 cavities, comparing alI data points) was Vac= slope x Vmri + intercept with a correlation coefficient = 0.70, *P=0.0007,* intercept=1.11, and slope=0.95. It was found that there was better correlation in the anterior part of the scanning than in the posterior part. To test the hypothesis that this difference was due to deviation in the axis of the acoustic areas and the MRI areas, a posterior scanning perpendicu1ar to a plane tilted at *45-50°* relative to the nasal floor was performed. This gave a better correlation but still a considerable overestimation of the areas by acoustic rhinometry. Correction based on the circumference ofthe cavity was also tried, but no significant effect was seen. This indicates that the complex geometry in certain parts of the nasal cavity do es not significantly influence the resu1ts (e.g. in terms of error in the area determination by MRI or sound loss during acoustic rhinometry), see Fig. 6. As an example the effect of decongestion of the nasal cavity evaluated by MRI and acoustic rhinometry I is presented in Fig. 9.

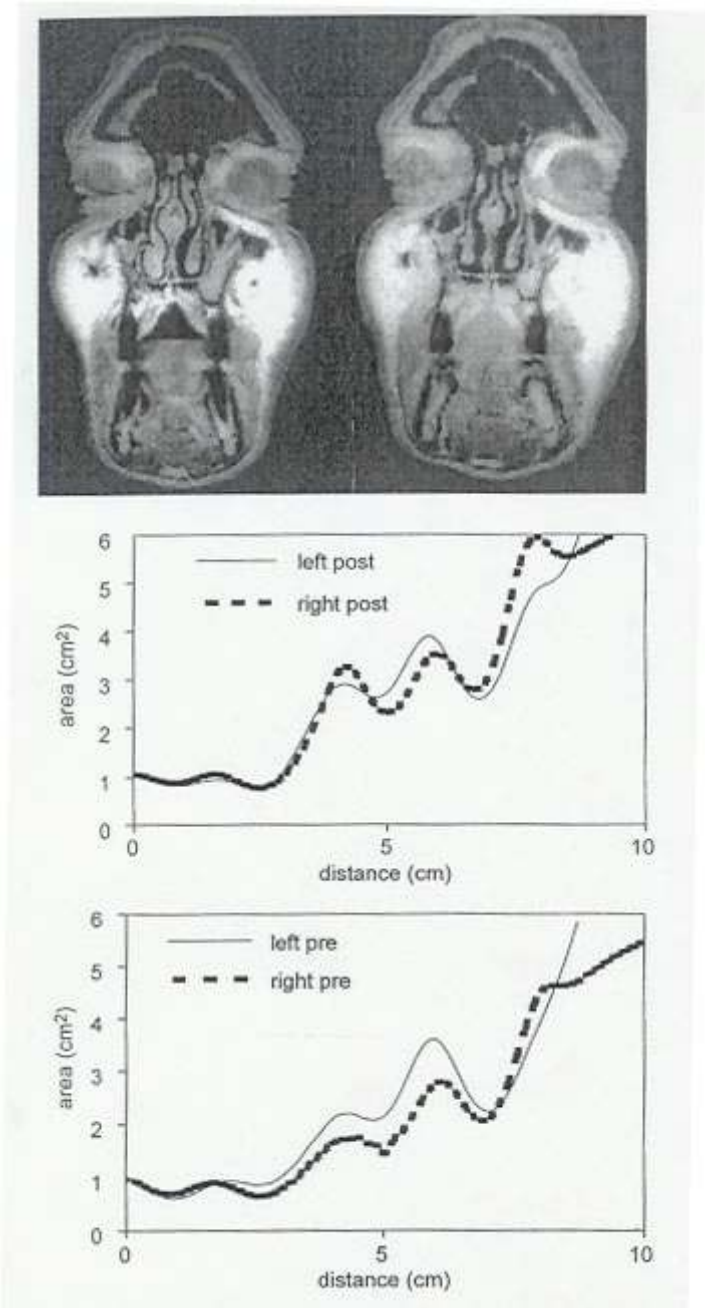


Figure 9, The acoustic area-distance function and MRI before and after decongestion in a subject.

In the initial study 10 subjects were exarnined in a 'normal congested' state, decongested state after nose drops, and post congestion by histamine.

The minimum area obtained by acoustic rhinometry and the minimum area determined by the pressure-flow relationship (rhinomanometry) in the no se were compared. This is based on the assumption that the total pressure difference across the no se is con verted to kinetic energy at the minimum crosssectional area. The results showed that the minimum cross-sectional area determined by rhinomanometry was only one of the area determined by acoustic rhinometry. Other reasons (e.g. deviations from the expected flow regimen: turbulent vs. laminar) could be possible but unpublished data comparing a stereolithographic model of a subject and circular model with equivalent cross-sectional areas, revealed the same difference indicating that the total pressure loss over the no se is not located at a small segment. This is in contrast with earlier studies.

Others have a1so demonstrated a high correlation between the cross-sectional areas obtained by MRI and by acoustic rhinometry in decongested subjects (0.969) whereas a poorer result was observed in the non-decongested nose. In a study, high resolution CT of the nasa1 cavity and sinuses was compared with a semiautomatic calculation of the area-distance function and acoustic rhinometry in 5 subjects. Comparable results were found in the anterior part of the nasal cavity but in agreement wi th other results the acoustic trace was not so well defined in the posterior end of the nasal cavity. Comparable results were also found using the same technique in a study of 14 patients suffering from chronic sinusitis. Similar results were seen in a study of nine patien ts with turbinate hypertrophy who underwent CT -examination and examination with acoustic rhinometry. The cross-sectional areas at the three deflections or minimum notches on the area-distance curve were measured and compared with the 3 narrowest crosssections in the anterior, middie and posterior part of the nasal cavity determined by CT. High correlation was found for the two first notches *(P* <0.005) but was poor in the posterior part. A recent study comparing the findings by rigid endoscopy and acoustic rhinometry in 85 subjects has confirmed that the first deflection on the area-distance curve reflects the nasal valve and the second the anterior end of the inferior turbinate. The choanae may also in a number of subjects be identified from the area-distance curve as an abrupt change in cross-sectiona1 area. Overestimation of the areas in the posterior part of the nasal cavity was also seen in another study comparing acoustic rhinometry and CT -scanning. In examining the effect of small spheres introduced into the nasal valve and middie meatus in 3 anaesthetized subjects spheres with a diameter less than 5 mm were not well recovered on the area-distance recording in the middie meatus. The reason for this may partly be due to the actual set-up and resolution of the system but also some physical circumstances, e.g. a large middie turbinate hiding the sphere. Others have in similar studies in models and cadavers

found better sensitivity for acoustic rhino metry, being able to detect spheres of 0.3 cm3. Test of the repeatability has shown variation less than 5% in repeated measurements of the nasal cavity volume.

As expected, an acoustic leak may affect the measurement considerab1y. It has been described that the area-distance function is affected by breathing and that breath hold is recommended during the measurement. It has been shown (unpublished data from the manufacturer) that breathing disturbances are very much dependent on whether the microphone in the equipment is ventilated or not and is insensitive to low frequency pressure changes. In the time scale of an area distance measurement, breathing could be considered as an offset, DC, or constant pressure that may affect the measurement. It has also been questioned whether acoustic rhinometry is reliable if the ambient temperature is changed. Unfortunately, it is not clear in that particul ar study whether the system has been recalibrated at different temperatures and if major changes (more than 10°C) whether the speed of sound setting was corrected. It has also been discussed in that paper that the measurement in some instances may be unreliable. This may not be due to inherent errors in the system but untrained operators, and the same authors have suggested that standard operating procedures should be used.

The axis in which sound travels in the nasal cavity may, as already described, affect the area measured, but the axis appears to be parallel with the nasal floor from the nasal valve. The terms I-notch and C-notch were introduced to describe the first two deflections (notches) on the area-distance curve. It was hypothesized that the deflections represent the Isthmus nasi and the head of the inferior turbinate (Concha).

PÁNDI Balázs

A TÁBORI ALAPHÍRHÁLÓZAT ERŐFORRÁSAINAK MODELLEZÉSE

PÁNDI Balázs:[159]

Előszó: Az analóg tábori alaphírhálózat erőforrásai nyilvántartásának és menedzselésének rendszere a hagyományos szabályzatokon alapuló megoldások szerint történik napjainkban is. Jelen közlemény a digitális rendszer kiépítéséig alkalmazható rendszermodellel kapcsolatos fejlesztés egy részirányát mutatja be

Kulcsszavak: tábori alaphírhálózat, erőforrás-kezelés, rendszermodell

1. A jelenlegi rendszer

Állandóan változó világunkban a katonai híradás eszközeit, szervezési elveit, a megvalósítás feltételeit és módjait a mindenkor érvényben lévő szabályzatok és utasítások tartalmazzák, de a gyors változásokat ezek követni – *jellegüknél fogva* – nem tudják, illetve sajátos felépítésük, tartalmi követelményeik miatt sem teszik lehetővé a bennük rögzített elvek, eljárások, eljárási módok sokoldalú indoklását, a problematikusabb, nehezebben érthető részek megvilágosítását.

Ettől függetlenül, a Magyar Honvédség csapatainak tevékenységét, a csapatvezetés milyenségét erőteljesen befolyásolja, annak működését meghatározza a vezetési szintek híradása, melyek üzemeltetése különösen hadműveletek időszakában a tábori hírrendszer komplex alkalmazásában valósul meg. Ez a hírrendszer a kommunikáció, az információcsere lehetőségét biztosítja a hírközpontok és a felhasználók között, legyenek azok személyek, vagy végződtető eszközök. Ezt a rendszert a csapatvezetési és fegyverirányítási rendszer egyik alrendszereként kell értelmezni, mely egységes elgondolás és terv (híradóterv) alapján telepített, kölcsönösen illesztett és összekapcsolt, különböző rendeltetésű hírközpontokból, az azokat összekötő híradó vonalakból áll, és biztosítja a különböző vezetési rendszerek működésének híradó feltételeit, az információk továbbításának lehetőségeit, bele értve az azt kiszolgáló személyi állományt is.

Az alaphírhálózat tevékenységének vezetése, irányítása, manőverezési képessége nem tudja követni a gyors helyzeteket, ahhoz alkalmazkodni csak lassan képes. A vezetés zömében a hierarchikusan szervezett híradás vezetési rendszerén belül valósul meg, ahol a katonai szervezetek híradófő-

[159] szerző: Pándi Balázs okleveles közgazdasági programozó matematikus, a ZMNE Hadtudományi Doktori Iskola PhD-hallgatója. Kutatóhely: Híradó Tanszék

nökei a rendelkezésre álló közvetlen összeköttetéseken, vagy szolgálati csatornán, a híradó hadműveleti-technikai ügyeleti szolgálatok útján irányítják az alárendelt szervezetek híradóalegységeinek tevékenységét. Az alaphírhálózat szakmai vezetése a híradófőnök felelősségi körébe tartozik, aki a hálózatot telepítő híradóegység parancsnok és törzse részére minden szükséges információt meg kell, hogy adjon ahhoz, hogy az alaphírhálózat telepítése, létesítése és üzemeltetése a hadműveletek lefolyása során biztosított legyen. Vezetői tevékenységét elsősorban szakmai ismereteire, tapasztalataira támaszkodva végzi, ez azonban nincs a kornak megfelelően informatikai eszközökkel és programokkal alátámasztva. Az alaphírhálózat felépítésének, terepen történő elhelyezkedésének tervezéséhez a szakszolgálatok nem rendelkeznek a szükséges szoftverekkel, térinformatikai- és speciális tervezőprogramokkal, melyek megkönnyítik az összeköttetések megtervezését, a viszonylatok, vagy a hálózat működésének modellezését. Az ilyen szoftvercsomagok működtetéséhez megkövetelt informatikai eszközpark nem biztosított a szükséges minőségben és mennyiségben a híradó szolgálatok részére sem.

A híradás létesítése után a hadműveleti-technikai ügyeleti szolgálatok kiemelt fontosságú feladata a csatornák állapotának folyamatos ellenőrzése, nyilvántartása, azok megszakadása esetén a helyreállítás, vagy a manőverek megtervezésének és végrehajtásának vezetése. A tábori alaphírhálózat e tekintetben nem képes az alaphírközpontba érkező és az onnan kimenő csatornák állapotáról elektronikus úton információt nyújtani a híradó ügyeleti szolgálatok részére; a távfelügyelet a hálózatban nem funkcionál a NATO-tagországokban alkalmazottaknak megfelelően.

A tábori alaphírhálózat nem kapcsolható össze az állandó jellegű közcélú, egyes zártcélú és különcélú hálózatokkal azok nagyfokú digitalizáltsága miatt. Ugyanez a helyzet áll fenn a NATO Integrált Híradó Rendszerével (NATO ICS[160]) és a NATO-tagországok tábori (harcászati) híradó rendszereivel is, melyek együttes üzemeltetése multinacionális környezetben elengedhetetlen feltétel a csapatvezetés érdekében. Az analóg technikai eszközök kezelése bonyolult, a kezelőállomány kiképzéséhez szükséges idő aránytalanul magas. Figyelembe véve, hogy a sorkatonai szolgálat ideje fokozatosan csökken, az állomány felkészítése még a kiképző központokban is nagy nehézséget okoz, a felkészítés eredményessége jelentős mértékben függ a sorállomány szakképzettségétől, iskolai végzettségétől.

Az alaphírhálózat elemei technikailag és erkölcsileg elavultak, egy részük elektroncsöves technológiájú, már nem képesek felvenni a versenyt a kor színvonalán álló távközlési eszközök szolgáltatásaival. Fenntartási költ-

[160] NATO ICS (NATO Integrated Communication System) NATO Integrált Híradó Rendszer

ségük nagyon magas; ipari felújításuk a magas költségek és a gyártó vállalatok megszűnése miatt évek óta elmarad. A szükséges javítóanyagok beszerzése nehézkes, egyes berendezésekhez már lehetetlen. A meghibásodások valószínűsége nagy, az eszközök sokrétűsége miatt egymással nem felcserélhetők, blokkcserék a tartalékegységek hiánya miatt nem alkalmazható. Az üzemfenntartáshoz nagy mennyiségű és sokféle javítóanyagra van szükség, a korszerű és gyors panelcserék a jelenlegi eszközöknél nem lehetségesek; a javítások ideje és műszerigénye nagy, azok végrehajtása az eszközök jelentős részénél már nem oldható meg.

A híradás vezetési rendszerét kiszolgáló típusgépjárművek csak munkahelyet biztosítanak a hadműveleti-technikai szolgálatok részére, elektronikus csatornaállapot-vizsgáló berendezésekkel, eszközökkel, a csatornaviszonylatokat kijelző grafikus megjelenítőkkel a szolgálatok nem rendelkeznek. A kevés számú és kézi kapcsolású szolgálati csatorna a hálózat operatív, gyors és rugalmas vezetését nem teszi lehetővé, gyakran ezeket a csatornákat is a hadműveleti vezetés érdekében használják fel. A hírrendszer megtervezéséhez és megszervezéséhez a manuálisan elvégzendő munka (térképek, intézkedések, vázlatok, tervek, stb.) sok, az erre fordított idő igen jelentős.

A csapatvezetés oldaláról megnőtt az igény a digitális szolgáltatások harcászati szintű alkalmazására éppúgy, mint:

- a multimédiás információtovábbítására,
- a digitális hálózatok szolgáltatásainak igénybevételére,
- a papír alapú információcsere csökkentésére a döntés-előkészítés és döntéshozatal folyamatában,
- a gyors és hiteles adattovábbításra,
- a katonai üzenetkezelő (MMHS)[161] rendszer üzemeltetésére, mely a korszerű NATO rendszerekben már alapkövetelményként jelen van.

Mindezek alapján kijelenthető, hogy a Magyar Honvédség szárazföldi csapatai tábori alaphírhálózata vezetési (menedzsment) rendszerének korszerűsítése, fejlesztése időszerű és szükséges.

2. A tábori alaphírhálózat erőforrásai kezelésének újszerű megközelítése

A tábori alpahírhálózat erőforrásainak újszerű kezelésében nézőpontom szerint első lépés a hírhálózat számítógépes modellezése. Az általam kialakított modell a következő elemeket tartalmazza:

- <u>2.1. Csapatok, katonai szervezetek:</u>

[161]MMHS (Military Message Handling System)= Katonai üzenetkezelő rendszer

Az tábori alaphírhálózat által kiszolgált alegységek hierarchikus szervezete. A szervezet a hierarchia tetején a helyet foglaló zászlóaljak, esetleg dandártól a hierarchia alján lévő egyes alegységek (századok, illetve ütegekhez) tartozó híradó járművekig terjed. Az egyes alegységeknél szolgálatban lévő szolgálati személyek (katonák) szintén a modell részét képezhetik. A szervezeti felépítés több módon is modellezhető, például szervezeti fával, vagy organogrammal, illetve úgynevezett szülő-gyerek táblázattal, amelyben az egyes katonai szervezetek szerepelnek és minden egységnél (alegységnél) fel van tüntetve az elöljáró szerv. Az általam kialakított modellben mindkét lehetőség lényegében megvalósításra került.

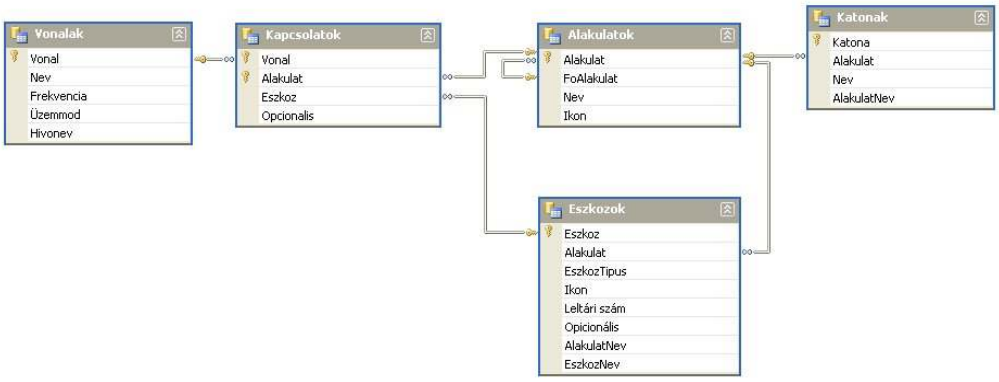
- 2.2. A rádióhíradás, illetve vezetékes távközlési eszközök rendszere:

Az egyes alegységekhez tartozó járművekben egy, vagy több rádiós, illetve vezetékes híradó eszköz található. Az eszközök számos tulajdonsága feltüntethető a modellben, így például a típus, leltári szám, stb.

- 2.3. Átviteli utak, csatornák:

Előre lefektetett, illetőleg kialakított vezetékes átviteli utak, valamint megszervezett és kiosztott rádiócsatornák, amelyekre az egyes rádiók és vonalas eszközök csatlakozhatnak (összességében: vonalak). A vonalak tulajdonsága feltüntethető a modellben, így például a hívónév, a frekvencia, valamint az üzemmód.

- 2.4. Egyéb kapcsolatok:

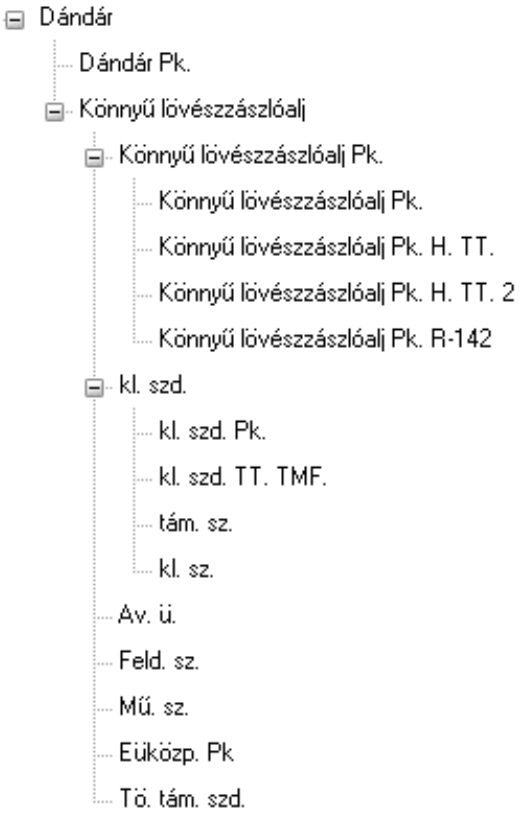


1. számú ábra: relációs adatbázis séma (forrás: szerző)

A híradás eszközeinek kapcsolatai az egyes vonalakhoz. Egy eszköz alapértelmezésben egy-egy vonalra csatlakozik (de a modell több másodlagos kapcsolatot is lehetővé tesz). A kapcsolatok több módon reprezentálhatók, például kapcsolati listával, amely a kapcsolódó eszközöket és vonalakat sorolja fel, kapcsolati mátrixszal, illetve gráffal. Az általam kialakított

modellben egyelőre a kapcsolati lista, illetve kapcsolati mátrix reprezentációk kerültek megvalósításra.

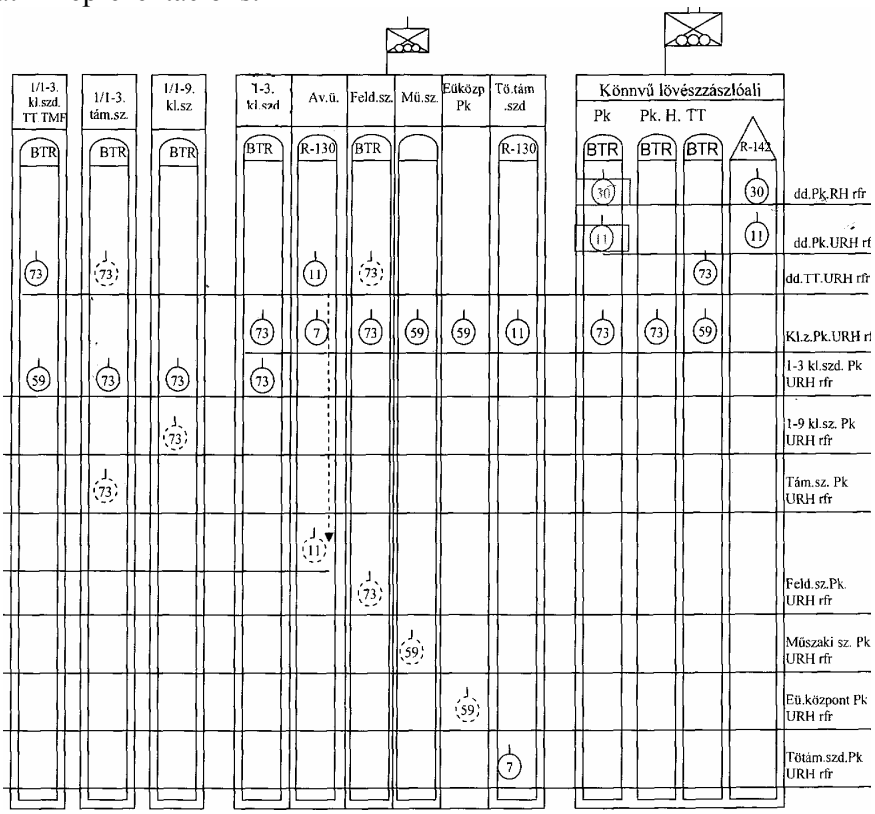
A fentiekben felállított modell jól reprezentálható az alábbi relációs adatbázis sémának egy lehetséges megoldási módjával:



2. számú ábra: szervezeti fa-reprezentáció egy lehetséges variációja (forrás: szerző)

Fenti reprezentáció azért célszerű, mivel kellőképpen rugalmas a változások karbantartásához, új alegységek könnyű felvételéhez és rombolások hatásainak szimulálásához, illetve alkalmas nagymennyiségű kapcsolódó adat tárolására, például akár a hírhálózat egyes pontjain szolgálatban lévő katonák és azok adatainak tárolására. A relációs adatbázis sémában az egyes katonai egységek (alegységek) szervezeti felépítésének modellezése szülő-gyerek táblázat reprezentációval történik, ami alapján előállítható a szervezeti modellezésnél gyakran használt szervezeti fa-reprezentáció is:

A kapcsolatok modellezése az adatbázis sémában, kapcsolati lista reprezentációval történik. A táblában szereplő opcionális mező azt jelöli, hogy az adott kapcsolat alapértelmezett vagy opcionális. Ez alapján például szintén előállítható a rádióhíradás vázlatának ábrázolásánál elterjedt kapcsolati mátrix reprezentáció is:



3. számú ábra: a rádióhíradás vázlatának egy megoldása (forrás: ZMNE Híradó Tanszék)

3. Összegzés

A tábori alaphírhálózat a katonai magasabb egységek (egységek, alegységek) híradásának alapját biztosító hálózat, amely a híradás, az információcsere lehetőségeit biztosítja a vezetés és az alárendelt (al)egységek részére. Ez a hálózat analóg technikai eszközeivel szükségszerűen szolgálja ki a csapatvezetési igényeket alapvetően távbeszélő üzemmódú csatornákon.

A katonai vezetésben, a döntés-előkészítésben és döntéskialakításban az 1990-es évek második felétől fokozatosan jelentek meg a személyi számítógépek és az informatikai hálózatok, melyek a béke elhelyezési körletek-

ben, stacioner telepítési helyeken biztosítják a vezetés informatikai és információtovábbítási igényeinek kielégítését. A kialakított információs rendszerek alkalmazásával szemben a felhasználók jogosan várják el, hogy a megszokott formában és tartalommal információs rendszerként a hadműveleti területen is hozzájussanak adatbázisokhoz, küldhessenek képet, hangot, vagy adatot az alárendelt és elöljárói viszonylatokon párhuzamosan a beszédkapcsolatokkal.

A korszerű digitális tábori rendszer bevezetéséig azonban ki lehet alakítani az analóg rendszer erőforrásainak korszerűbb kezelésének módszertanát, amelynek kezdeti lépéseivel kapcsolatos kutatás-fejlesztési tevékenységem részeredményét fentiekben ismertettem.

Felhasznált irodalom:

[1] Fekete Károly: A korszerű katonai kommunikációs eszközök csatlakoztatása az ISDN-hez (Akadémiai Közlemények 1996/211. szám 131-156. oldal)

[2] Fekete, Karoly: Evolving possibilities of the strategic military networks „Kommunikáció 2003." Nemzetközi szakmai tudományos konferencia, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, ISBN 963 86229 6 2, 2003. október 15.

[3] Hamar Sándor: A katonai híradás fejlődésének és fejlesztésének lehetséges útjai, „Kommunikáció 2002." Nemzetközi szakmai tudományos konferencia, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, ISBN 963 86229 2 X, 2002. október 30.

[4] Honvéd Vezérkar Híradó Csoportfőnökség: A Magyar Honvédség híradásának és FRISZ biztosításának részletes, hosszú távú fejlesztési terve (1999-2013) Nyt.szám:070/2000

[5] Rajnai Zoltán: A tábori alaphírhálózat vizsgálata és digitalizálásának lehetőségei egyes NATO tagországok kommunikációs rendszereinek tükrében, doktori (PhD) értekezés, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2001.

[6] Dr. Sándor Miklós: A gépesített hadtest híradása (Új Honvédségi Szemle 1996/9. szám 33-39. oldal.)

[7] Dr. Somos András: A katonai kommunikáció és a hírközlés felkészítésének viszonya, „A katonai kommunikációs rendszerek fejlődési irányai – kihívások és trendek a XXI. században" nemzetközi szakmai tudományos konferencia, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, ISBN 963 00 8819 3, 143-146. oldal, 2001. november 28.

[8] Szakutasítás a szárazföldi csapatok híradásszervezési elveire és követelményeire (tervezet). HIR/126. HM 1984.

[9] Ternyák István: A magyar katonai kommunikációs rendszerszervezés [A kommunikáció (híradás) helye és szerepe a vezetés rendszerében 2000 – ZMNE Országos tudományos konferencia anyaga 49. oldal.]

[10] Ternyák István: A NATO-csatlakozás és a katonai telekommunikáció (Új Honvédségi Szemle 1998/3. szám 105-109. oldal)

TAKÁCS Péter

A WIFI HÁLÓZATOK ESETLEGES KATONAI FELHASZNÁLÁSÁNAK LEHETŐSÉGEI

Bevezetés

Az elmúlt évtizedek felgyorsult világa magával hozta az információ fontosságát, az ahhoz való gyors hozzáférés igényének megnövekedését. Ez elmondható minden szervezet életére, igaz ez a kisebb szervezetektől a nagyobb szövetségi rendszerekig mindre, mint például a NATO-ra is. Ez a folyamat együtt járt az informatika világának robbanásszerű fejlődésével, ám ezt a gyors technikai jellegű fejlődést sokszor nem követték e szervezeteknek az informatikára vonatkozó szabályzói, direktívái. Ilyen volt például a minősített informatikai hálózatok üzemeltetésének témaköre, mely szabályozása hazánkban, a Magyar Honvédségben igazából a NATO/EU tagságunk óta kezdődött el ténylegesen.

Napjainkra egy ilyen új, szabályozatlan, illetve „tiltott" terület jelent meg. Ez a vezeték nélküli alapokon nyugvó informatikai rendszerek témaköre. Míg az USA-val az élen több ország dollár milliárdokat fordít az ilyen jellegű hálózatok katonai célú felhasználásának kutatására, addig a különböző ajánlások, direktívák –mind nemzeti, mind tagságunkból eredő NATO -, informatikai szabályzók érintőlegesen sem foglalkoznak, illetve elvből tiltják ezen megoldások használatát. Pedig, ahogy azt már az elmúlt évtizedekben tapasztalhattuk, nehéz mesterségesen állított szabályzókkal a technikai fejlődés útjába állni.

Véleményem szerint hosszú távon lassan elhalad az idő a gyors helyváltoztatásra kényszerített, vezetékalapú helyi hálózatok felett, miközben a vezeték nélküli hálózatok bevezetésére, azoknak jóval eltérőbb tulajdonságaik miatt szükséges szabályzás hiányában még nem vagyunk felkészülve.

Erre a technikai kihívásra adhat választ a polgári életben megjelent wifi hálózatok felhasználása. Természetesen ennek a technológiának katonai környezetben történő felhasználása több kérdést is felvet, például a biztonság területén. Jelen munkámban ezzel a területtel foglalkoztam. Mivel a Magyar Honvédségben ez nem elterjedt technikai így a polgári életből vettem mintákat.

Napjainkra a vezeték nélküli hálózatok egyre nagyobb teret nyernek, gomba módra szaporodnak az access pointok[162], továbbiakban AP-k. Ezen hálózatoknak hatalmas előnye a mobilitás, de ez az előny sokszor nincs

[162] Hozzáférési pont

összhangban a velük együtt járó veszélyekkel, biztonsági kockázatokkal, melyeket rádiós, szabadtérben terjedő mivoltuk képez.

Mivel rengeteg írás jelent meg a 802.11 szabványról, a Wifi[163] hálózatok paramétereiről, működésükről, azokra nem térek ki, inkább a konkrét vizsgálataimra fókuszálok.

A wifi hálózatok elterjedésével együtt járt egy újfajta „sport", „hobby" elterjedése is, melynek lényege, hogy vezeték nélküli eszközökkel, esetleg GPS[164]-szel kiegészítve, feltérképezik egy adott területen elérhető wifi hálózatokat. Ez a wardriving (gépjárművel), illetve warchalking (gyalog). http://www.wardrive.net

Fontosnak tartom megjegyezni, hogy ilyenkor semmilyen illetéktelen behatolási kísérlet nem történik az adott hálózatokra, ahogyan én sem próbálkoztam semmi ilyennel, mindazonáltal az elterjedtebb hálózatfeltörési módszereket a saját tesztüzemű hálózatomon kipróbáltam, és ezek tapasztalatait e munkámban meg is osztom az olvasóval.

1. ábra: ZMNE területe

Forrás: googleearth.com

2. ábra Budapest - részlet

Forrás: googleearth.com

Két nagyobb területet térképeztem fel 2007-ben, az elérhető vezeték nélküli hálózatok szempontjából. Ezek a következők:

- Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem területe: a 47,491401/19,120696 (Zách utca-Salgótarjáni utca sarka), valamint a 47,496360/19,108899 (Hungária krt. - Hős utca sarka,

[163] Wireless Fidelity, az IEEE által kifejlesztett vezeték nélküli mikrohullámú kommunikációt megvalósító szabvány népszerűsítő neve.

[164] Global Positioning System

MOL kút) földrajzi koordináták által kifeszített, 382m x 600m-es téglalap alakú területen belül gyalog mozogva.

- Budapest: a 47,51,47,89/19,043140 (Margit sziget bejárata a Margit híd felől), valamint a 47,491401/19,120696 (Zách utca-Salgótarjáni utca sarka) koordináták által kifeszített, 5,82km x 2,63km-es téglalap alakú terület, gépkocsival mozogva. Szeretném megjegyezni, hogy a hatalmas terület csekély részének bejárása miatt a felderített hálózatok száma csak töredéke a teljes területen fellelhető hálózatok számának, de statisztikai alapnak megfelelőnek tekintettem.

A wifi hálózatok biztonsági kockázatairól általában

Sokat hallunk veszélyekről, melyek hálózatunkat, számítógépeinket fenyegethetik. Ebben a fejezetben át szeretném tekinteni azokat a kockázatokat, amik kifejezetten a vezeték nélküli, azok közül is a nyílt vagy gyenge titkosítást használó hálózatokra jellemzőek.

Mindenképpen első helyen szeretném megemlíteni a számítógépeink védelmét: bárki, aki hatótávolságon belül helyezkedik el, kontrolálatlan formában hozzáférhet a számítógéphez, megfelelő tűzfal és vírusvédelem hiányában az azon futó operációs rendszer biztonsági réseit kihasználva hozzájuthat az összes rajta tárolt adathoz, a rajta begépelt jelszóhoz, stb.

Ennek sikertelensége esetén még mindig a támadó előtt nyitva áll a teljes hálózati forgalom lehallgatásának lehetősége, aminek során felhasználónevekhez, jelszavakhoz, személyes adatokhoz, felhasználói szokásokhoz juthat.

Manapság egyre nagyobb problémát jelentenek a zombi hálózatok, az azok által indított spam áradat, illetve DoS[165] támadások. A védtelen hálózatok könnyen áldozatául eshetnek ilyen tömeges támadást kiszolgáló törekvéseknek.

Ennél is nagyobb problémát jelenthet, ha valamilyen célzott betörést a mi hálózatunkról indítanak, amit még vissza is követnek. Képzeljük el, ahogy magyarázkodni próbálunk egy internetes betörés gyanúsítottjaként.

Nyílt Wifi hálózatok

Ezen hálózatoknak legfontosabb és egyben leghátrányosabb tulajdonsága, hogy a rajta továbbított adatok teljesen nyíltan, úgynevezett „plain text” formában kerülnek továbbításra, egy esetleges támadó szöveges formában képes olvasni az átvitt adatot, mint például jelszavakat.

[165] Denial of Service attack / szolgáltatás leállítási támadás

Az alábbi ábrán egy webes bejelentkezése folyamata látható egy titkosítatlan hálózaton a „teszt felhasznalo”, „test jelszo” felhasználónév/jelszó párossal.

```
5d 49 64 3d 63 6f   .,.....f ormId=co
73 41 75 74 68 26   mmands.P lusAuth&
74 70 25 33 41 25   backurl= http%3A%
51 69 6c 2e 68 75   2F%2F[redacted]email.hu
55 73 25 32 46 61   %2Flevel ezes%2Fa
5d 64 25 33 44 63   uth.fm%3 Fcmd%3Dc
36 70 61 67 65 25   heckuser %26page%
73 26 63 6d 64 3d   3Dlevele zes&cmd=
55 6d 6f 74 65 66   plusauth &remotef
3d 74 65 73 7a 74   orm=1&us er=teszt
5c 6f 40 66 72 65   +felhasz nalo@[redacted]
73 65 72 77 69 74   [redacted]mail.hu &userwit
3d 74 65 73 7a 74   houtdoma in=teszt
5c 6f 26 70 61 73   +felhasz nalo&pas
5c 73 7a            s=teszt+ jelsz
```

3. ábra Sniffing

Készítette: a szerző

Manapság általában három esetben találkozhatunk ilyen „elavult ” hálózat típussal:

1. Az eszközök régiek, nem támogatják az újabb titkosító eljárásokat.
2. Újabb eszköz esetén gyári, úgynevezett „default” beállításokkal kerül telepítésre a hálózat, mely nagyfokú veszélynek van így kitéve.
3. Egyes szolgáltatók ilyen formában nyújtanak internet szolgáltatást, melynél az elsődleges szempont a könnyű konfigurálhatóság a kliens részéről. Ilyenkor úgynevezett „captive portálok”, magyarra fordítva elkapó, begyűjtő portálok kerülnek alkalmazásra a hálózat hozzáférés szabályozásának céljából, mely a kliens számára védelmet nem nyújt.

Titkosított Wifi hálózatok

Ebben a fejezetben a wifi hálózatok tikosításának lehetőségeit szeretném bemutatni a teljesség igénye nélkül. Mivel dolgozatom figyelemfelkeltő célú és a WPA[166] TKIP[167] és WPA AES[168] hálózatok megfelelő beállí-

[166] Wi-Fi Protected Access
[167] Temporal Key Integrity Protocol
[168] Advanced Encryption Standard

tás esetén megbízható biztonságot nyújtanak, azok rendszerspecifikációjával ebben a cikkben részletesen nem foglalkozom.

WEP[169]

A legelső, széles körben elterjedt titkosítási eljárás wifi hálózatok számára. Bár a 802.11 szabvány tervezésekor már megjelent az igény a biztonságra, ezt a WEP alkalmazásával nem érték el, a biztonság messze alulmaradt az elvárásoknak. Ennek fő oka a hibás protokolltervezés volt. Egy WEP alapú hálózat feltörése ma *általában* 2-7 óra között kivitelezhető, ahogy azt saját teszt üzemű hálózatomon ki is próbáltam.

Hogy jobban megértsük a WEP gyengeségét meg kell vizsgálni annak működését. Vezeték nélküli hálózatoknál általában három biztonsági kérdés merül fel:

1. a hálózat lehallgatása
2. a hálózat szolgáltatásainak illetéktelen használata
3. a hálózat bénítása

A WEP az első két problémára próbált megoldást kínálni. Az első problémát a forgalom titkosításával, a másodikat az eszközök hitelesítésével szerette volna megoldani.

A WEP hiányosságai, sebezhetőségei:

A következő fejezetben megpróbálom összefoglalni a WEP hiányosságait a különböző szakirodalmak, valamint saját tapasztalataim alapján.

A WEP hibái

1. A hitelesítés egyirányú, mindig csak a mobil állomás hitelesíti magát, így sohasem lehetünk biztosak, hogy a saját bázisállomásunkhoz (AP) csatlakoztunk és nem egy támadó által felállított, ugyanolyan nevű AP-n keresztül jutnak el az adataink a célba.
2. A hitelesítés csak a hálózathoz való csatlakozás pillanatában egyszer történik meg. Ezután már bárki küldhet üzenetet az egyszer már hitelesített kliens nevében, annak MAC address-ét használva. Elsőre azt gondolhatnánk, hogy ez nem lehet baj, hiszen a támadó nem ismeri a WEP kulcsot, így ennek semmi értelme. De ha a támadó egy elkapott, titkosított üzenetet küld vissza, akkor arra az AP titkosított formában újra és újra válaszolni fog. Ez a kiinduló pontja az úgynevezett visszajátszásos, angol nevén „replay” alapú támadásoknak, ahogy, azt később bemutatom.
3. A hitelesítés és a rejtjelzés ugyanazzal a kulccsal történik, így az egyik megszerzésekor a másik birtokába is jutunk.

[169] Wired Equivalent Privacy

4. Ha a támadó elkapja a hitelesítés előzőekben bemutatott 4 teljes ütemét, akkor az „A” kihívásból és a rá kapott, T = A xor K válaszból képes kiszámítani a „K”-t (A xor T = K), aminek birtokában bármilyen kihívásra - „authenticate challenge” - képes válaszolni a kliens nevében.
5. Az integritás védelem sem hibamentes: a CRC lineáris voltából adódóan a támadó az üzenet bármely bitjét képes úgy módosítani, hogy közben nem is ismeri az üzenet tartalmát. Általánosságba elmondható, hogy CRC védelem lenne hivatott kivédeni az üzenet visszajátszásos támadásokat, ami a WEP-ből teljesen hiányzik.
6. Titkosítás. A legnagyobb biztonsági rést pont maga a rejtjelzés jelenti: a problémát a lehetséges IV-k beláthatóan véges száma adja. Mint azt már említettem az IV 24 bit hosszúságú, ami kb. 17 millió lehetséges IV-t jelent. Tapasztalataim szerint ideális körülmények között egy támadás közben 60-70 IV-t lehet másodpercenként gyűjteni. 70 IV x 60 x 60 = 252.000 IV / óra. 16.777.216/252.000=66,5 óra. Ez azt jelenti, hogy 67 óra hallgatózás után már ismétlődnek az IV-k. Tovább rontja a helyzetet, hogy általában az IV-k nem véletlenszerű helyről, hanem mindig nulláról indulnak, így több eszköz esetén hamarabb előfordulnak ugyanazok az IV-k.

Az ebben a pontban felsoroltakat kihasználva kriptográfusok egy csapata egy bonyolult statisztikai, valószínűségi alapokon nyugvó támadó algoritmust készített, amivel a valóságban már 200.000 - 500.000 összegyűjtött IV alapján sikeres támadást lehet indítani a WEP kulcs ellen.

WPA

A WEP hibái nem sokkal megjelenése után már napvilágot láttak és az IEEE új biztonsági megoldások után nézett. Teljesen új alapokon és algoritmusokon nyugvó rendszert dolgozott ki a wifi hálózatok védelmére. Mivel ez egy jóval összetettebb és bonyolultabb eljárás, annak hosszadalmas részletezését most ebben a munkámban mellőzöm és csak ismeretterjesztő jelleggel összefoglalom ennek az új szabványnak a fontosabb újításait.

Egyik legfontosabb módosítás az adatátvitel során alkalmazott új titkosító algoritmus. A régi RC4 folyamkódolót leváltotta az AES algoritmus. Itt szeretném megjegyezni, hogy ez a váltás a régi típusú készülékeken software és firmware frissítéssel nem megoldható, mindenképpen új hardware-t igényel, így egy további irányzatot is kialakítottak: annak érdekében, hogy a régi eszközökből egy software frissítés után a WEP-nél erősebb védelmű hálózatot lehessen kialakítani. Ez a hálózat továbbra is az RC4 folyamkódolót használja több módosítással. Ezt az irányvonalat ne-

vezték el WPA TKIP-nek, míg az AES algoritmust használó WPA lett a WPA2, vagy másik nevén WPA AES.

További fontos újítás, hogy itt már külön kulcs van a hitelesítésre és az adatfolyam titkosításra, sőt még az integritás védelemre is.

A hitelesítés teljesen új alapokra került, a forgalmazás során dinamikusan változik a titkosításhoz használt kulcs. Az ilyen hálózatok IV-k gyűjtésével már nem törhetőek, egy hitelesítési folyamatot kell elkapni, majd ez ellen szótár alapú támadást intézni. Ez megfelelően erős kulcsválasztás esetén akár több évtizedig is eltarthat.

Wifi hálózatok felmérése, azok támadása

Eszközök

A felméréshez, valamint a hálózat biztonságának teszteléséhez kizárólag kereskedelmi forgalomban kapható eszközöket használtam. Ezek 1-2 kivétellel könnyen beszerezhetőek.

A felméréshez használt valamennyi program az internetről letölthető.

Mivel a dolog jórészt a wifi kártyán áll vagy bukik, arra részletesen kitérnék:

Általában a wifi kártyák nem alkalmasak támadó jellegű tevékenységre. A speciális funkciók, mint például az eszköz promiscuous üzemmódban (ami a hálózati forgalom figyeléséhez, illetve csomaginjektáláshoz szükséges) történő üzemeltetése csak bizonyos chipset-ű (Atheros, Prism) kártyákkal valósítható meg. Nekem több hónap keresése után, nagy nehézségek árán sikerült ilyent beszereznem.

További jellemzőjük, hogy áraik a kibővített képességek miatt jóval a „hétköznapi” kártyák felett van.

A felmérések során használt hardware:

- HP nx 8220 laptop beépített bluetooth képességekkel.
- HTC 3300 PDA beépített GPS vevővel, bluetooth képességekkel.
- „SuperRange Cardbus 300mW 802.11 a/b/g” PCMCI wireless kártya
- 5 dB nyereségű botantenna MMCX aljzattal
- 18,6 dB nyereségű Yagi antenna, RPTNC aljzattal. Horizontális nyílásszöge 18° , vertikális nyílásszöge 18°. A nagytávolságú felderítés mellett iránymérésre, az AP-ok földrajzi helyzetének meghatározására, valamint a gyengébb teljesítményű mobil eszközök forgalmának távolról történő megfigyelésére is hasznos.
- N – RPTNC antenna kábel a Yagi antennához.
- N – MMCX pigtail (a wifi kártya és az antenna kábel közé)

Felhasznált, kipróbált software-ek:

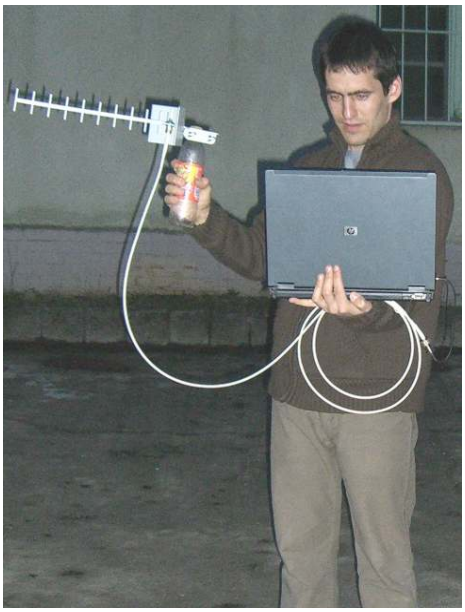
Software-ek Linux

- Back Track 2 Linux LIVE CD
- Red Hat Fedora 6 Linux
- Software-ek linux alatt:
    - Airmon, Kismet, Airodump, Aireplay, Aircrack, Wireshark, Airsnort, Ettercape

- Software-ek Windows alatt:
- Wirelessmon170
- Netstumbler - ingyenes program

4. ábra: Kellékek

Készítette: a szerző



5. ábra Munka közben…

Készítette: a szerző

WIFI hálózatok feltérképezése, azok eredménye

Mielőtt a fejezetbe belekezdenék, szeretném kijelenteni, hogy az adatok (MAC ADDRESS-ek, SSID[171]-k, stb.) kizárólag statisztika célokkal

[170] http://www.passmark.com/products/wirelessmonitor.htm

kerültek begyűjtésre, melyek a vonatkozó törvények értelmében további tárolásra, második félnek kiadásra nem kerültek.

Két területen térképeztem fel a wifi hálózatokat.

Ezek a következők:

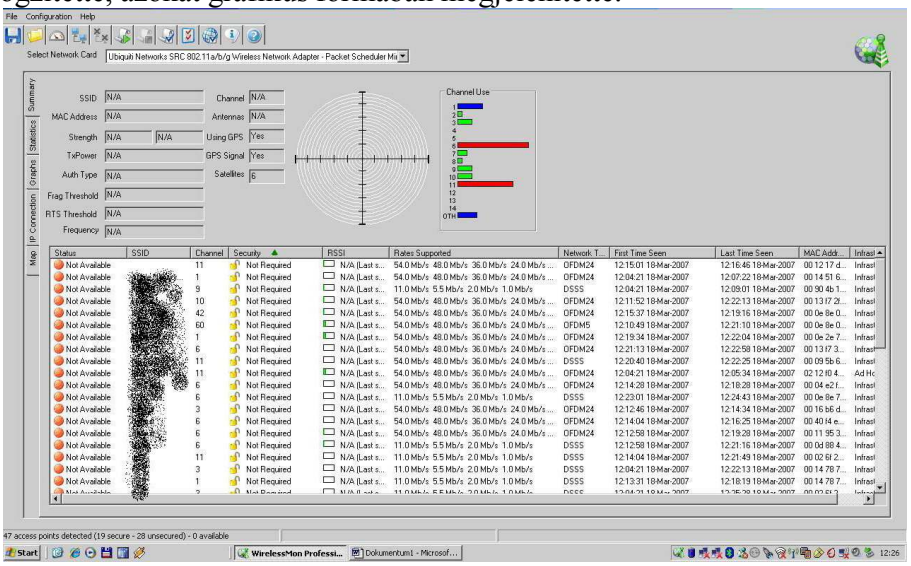
- Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem területe
- Budapest – Pest

ZMNE területe

A 47,491401/19,120696 (Zách utca-Salgótarjáni utca sarka), valamint 47,496360/19,108899 (Hungária krt. - Hős utca sarka, MOL kút) földrajzi koordináták által kifeszített, 382m x 600m-es téglalap alakú területet mértem fel, gyalog mozogva.

Itt szeretném kijelenteni, hogy a felfedett hálózatok egyike sem tartozott a Zrínyi Miklós Nemzetvédelmi Egyetemhez, csupán annak területén volt fogható.

A feltérképezéshez a Microsoft Windows alapú Wirelessmon illetve Netstumbler nevű alkalmazást használtam. Az alábbi ábrákon a Wirelessmon alkalmazás látható, mely a wifi jelek mellett a GPS jeleket is rögzítette, azokat grafikus formában megjelenítette.



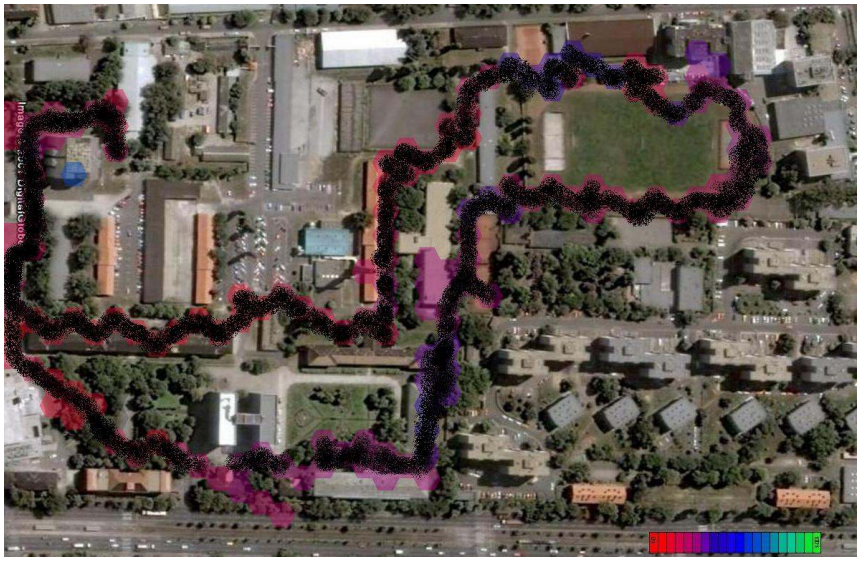
6. ábra: Wirelessmon működés közben

Készítette: a szerző

A vizsgálat során 47 AP-ot sikerült felderítenem, melyből csak 19 volt valamilyen módon védve, **28 semmilyen védelemmel nem rendelkezett**. A 19 védett hálózatból 9 volt a WPA valamilyen fajtájával védve.

[171] Service Set Identifier Egy wifi hálózat neve

Ez azt jelenti, hogy a hálózatok kb. kétharmada volt közvetlenül vagy közvetve kitéve potenciális veszélynek, mint például lehallgatás, illetve illetéktelen használat.

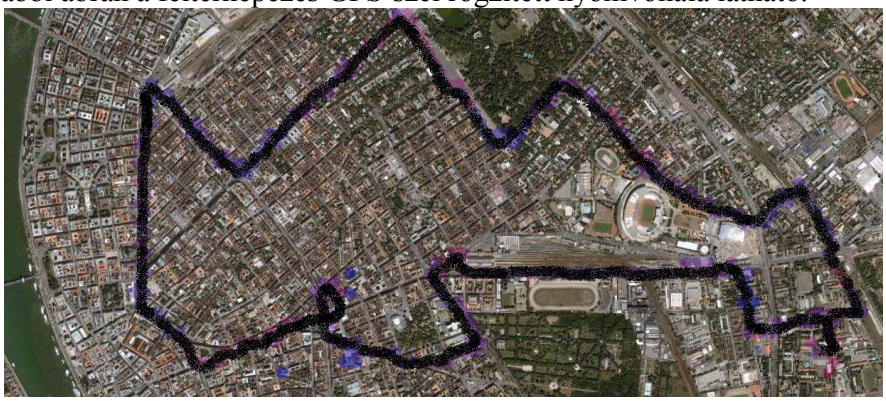


7. ábra: Bejártam az egyetemet

Forrás: googleearth.com

Budapest területe

A következő állapot a 2007. május elejei állapotot tükrözi. Az alábbi ábrán a feltérképezés GPS-szel rögzített nyomvonala látható.



8. ábra: A feltérképezés nyomvonala Budapesten

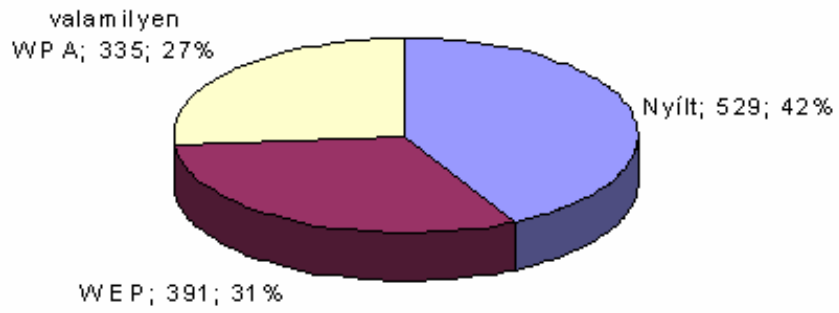
Forrás: googleearth.com

A feltérképezés során hasonló arányokkal találkoztam, mint, amiket az előzőekben bemutattam, bár az SSID-k alapján a wifi hálózatok jóval

szélesebb körű felhasználása, azok színesebb világa tárult elém. Az SSID között a hálózatnévben telefonszámmal internet elérést kínáló hálózatoktól orvosi rendelők hálózatán keresztül, különböző rádiók, magánnyomozó irodák, politikai töltetű hálózati nevű hálózatokig szint minden megtalálható.

A csatornakihasználtság vizsgálata érdekes eredményeket hozott: vannak csatornák melyek használata fokozottabb a többinél, ezek a következők: 1-es, 6-os, 11-es, míg vannak csatornák – 4-es, 5-ös – melyeket szinte nem használnak.

A csatornakihasználtság vizsgálatának egy másik érdekes adata, hogy a 802.11b és 802.11g szabványok jóval elterjedtebbek, mint a 802.11a. Az 1255 hálózat közül csupán csak 41 használja ennek a szabványnak a csatornáit, ami az újabb, korszerűbb eszközök alacsony elterjedtségét feltételezi. Hihetetlen adat, hogy e közül a 41db 802.11a típusú hálózat közül csupán csak 2 volt titkosított miközben szinte biztos, hogy ezek a korszerű eszközök már ismerik az újabb titkosítási eljárásokat. Ugyanilyen rossz a helyzet a titkosítottság általános vizsgálatakor is, az összes hálózat 42%-a teljesen nyílt volt, 31% pedig WEP alapú, mely bizonyítottan feltörhető pár óra alatt.

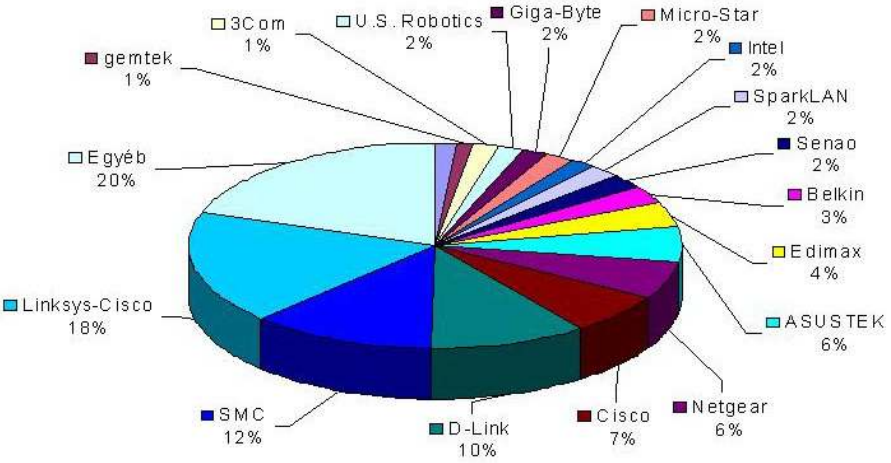


9. ábra: A titkosítottság megoszlása

Készítette: a szerző

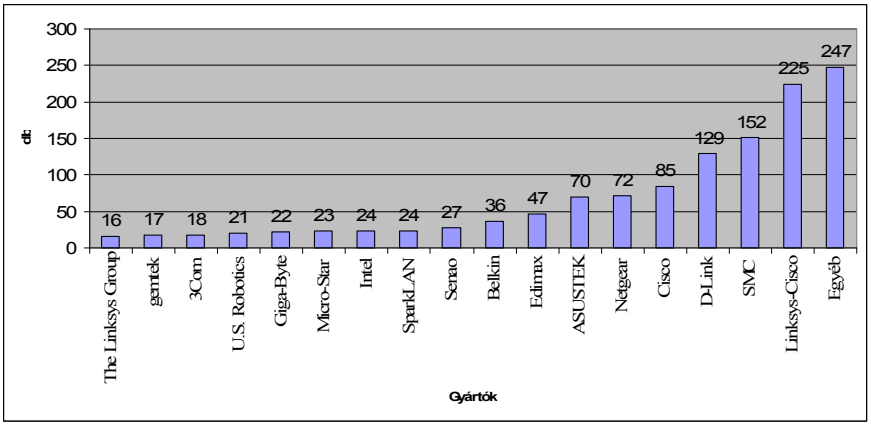
A sebesség tekintetében mindössze 204 AP működött kizárólag a 11 Mbps-os sebességen, a többi a nagyobb sebességekkel is elbírt, mint például a 36, vagy 54 Mbps. Ebből következtetést levonni csak óvatosan szabad, mert a korszerű eszközök is leszabályozhatóak, hogy kizárólag az alacsony sebességeket támogassák, de ilyen beállítás nem valószínű, az AP-k gyári beállítása is általában az, hogy képes minden általa támogatott sebességen dolgozni, a kliensállomás képességei és az átviteli út minősége fogja meghatározni a hálózat pillanatnyi sebességét. Ebből kiindulva úgy tűnik, hogy az elsőgenerációs, elavult eszközök lassan kihalófélben vannak.

Vizsgáltam az eszközök gyártóit is, melyek megoszlását az alábbi grafikonok szemléltetik:



10. ábra: A gyártók megoszlása I.

Készítette: a szerző



11. ábra: A gyártók megoszlása II.

Készítette: a szerző

Mindezeket összevetve arra a következtetésre jutottam, hogy bár sokszor lenne lehetőség magasabb színvonalú hálózat kialakítására, mégsem törekednek arra a hálózat telepítői, fenntartói.

WIFI hálózatok támadása

Ebben a fejezetben a WEP alapú hálózatok biztonsági kérdéseiről, azok kihasználásának lehetőségeiről ejtek pár szót. Röviden bemutatom

azokat az eszközöket, amikkel a wifi hálózatok linux alatt felderíthetők, a WEP, illetve WPA alapú hálózatok támadhatók.

A téma részletezése előtt szeretném kijelenteni, hogy kizárólag saját, tesztelési célokra létrehozott hálózatomon próbáltam ki a technikákat, amelyekhez a szükséges ismereteket, software-eket az internetről szereztem be.

A támadás kivitelezéséhez Linux Radhat Fedora 6 operációs rendszert, valamint az alá telepített speciális software-ek, software csomagok kerültek alkalmazásra. A téma iránt érdeklődőknek mellékelem a hivatkozó weblapokat.

Aircrack-ng „software csomag": http://www.aircrack-ng.org/doku.php

Legfontosabb összetevői:

- Airmon-ng: a wifi kártya „promiscuous", más néven „Monitor" üzemmódba való kapcsolására szolgál.
- Aireplay-ng: Többek között az elkapott, titkosított csomagok „visszajátszására", újra küldésére való alkalmazás, mellyel IV-k generálhatók az Airodump-ng számára. Egy másik „hasznos" funkciója a már hitelesített mobil eszközök leszakítása a hálózatról, azok kényszerítése az újra authentikálásra.
- Airodump-ng: a csatornákat használó AP-k, valamint a velük asszociált mobil eszközök felderítésére használható eszköz. Számunkra legfontosabb funkciója az előző fejezetekben tárgyalt IV-k gyűjtése, file-ba történő kiírása.
- Aircrack-ng: az összegyűjtött IV-k statisztikai alapú támadására alkalmas software, mellyel a titkos WEP kulcs visszafejtése a cél.

A támadás folyamata:

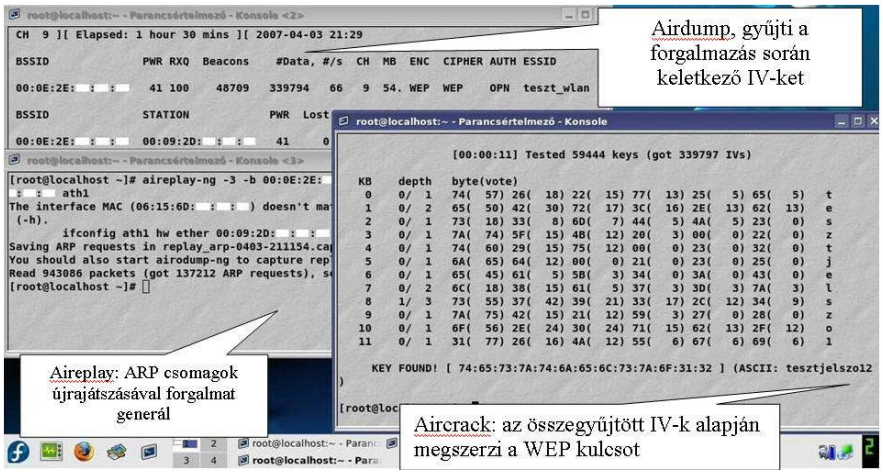
1. A wifi kártyát promiscuous üzemmódba kell kapcsolni. Erre alkalmas az „*airmon-ng start wifi0*" parancs.
2. Feltérképezésre kerül a rádiós tér. Ez történhet például a Kismet vagy az Airdump programokkal: „*airodump-ng ath1*".
3. Meg kell határozni a cél AP bssid[172]-jét, az általa használt csatorna számát, a biztos siker érdekében egy, a hálózaton érvényes kliens MAC[173] address-ét. Ez az esetleges MAC address alapú szűrések kijátszásához hasznos. A kliens MAC address megszerzésének feltétele, hogy az eszköz hatósugarában kell lenni. Mivel

[172] Basic Service Set Identifier. Tulajdonképpen az Access Point MAC address-e.
[173] Media Access Controll. Hálózati eszközök egyedi azonosítója.

ezek általában kis teljesítményű eszközök, érdemes egy nagy nyereségű antenna beszerzése.

4. El kell indítani az IV-k fogadását. Pl.: „airodump --ivs --write adatok --channel 9 ath1”.
5. A támadás felgyorsításának, az IV-k számának növelése érdekében „érvényes” forgalmat kell generálni. Ez történhet például „ARP request” csomagok elkapásával, azok visszajátszásával. ARP csomagok megjelenése felgyorsítható, ha leszakítjuk a hitelesítetten forgalmazó klienseszközt a hálózatról, kényszerítve azt a hálózati kapcsolat újra felépítésére. Ha ezt nem szeretnénk, akkor türelmesen várva, előbb utóbb el fogunk kapni ilyen, számunkra megfelelő ARP csomagot. Egy másik, hasonló megoldás lehet az érvényes forgalomgenerálásra a csomagok fabrikálása is a packetforge-ng alkalmazás segítségével.
6. Szükség esetén - bizonyos AP-k esetén - 20 másodpercenként újra kell hitelesíteni a kapcsolatot a mobil kliens MAC address-ét használva.
7. Az Aircrack-ng program segítségével a WEP kulcs feltörése az összegyűjtött IV-k alapján.

A következő ábrán láthatóak a sofware-ek a támadás befejeztével. Jól látható, hogy 1 óra 30 perces hálózati forgalom generálása alatt 339794 IV került begyűjtésre, amik alapján az Aircrack-ng software 11 másodperc alatt törte fel a jelszót.



12. ábra WEP törés

Készítette: a szerző

Összegzés: lehetőségek a honvédségi használatra

Amint azt láthattuk a wifi hálózatoknak számtalan előnyös tulajdonságaik mellett, sok veszélye is lehet. Mindez adódhat szakszerűtlen telepítésből, illetve korszerűtlen eszközök alkalmazásából.

A begyűjtött SSID-kból következtetve nagyon sok eszköz gyári beállításokkal működik, kicsomagolás után nem került bekonfigurálásra. Rengeteg eszköz teljesen nyílt adatforgalmú, vagy elavult titkosítási eljárást használ, potenciális veszélynek kitéve a hálózat állomásait, felhasználóit.

A felsorolt hibák ellenére dolgozatom nem elrettentő, hanem inkább figyelemfelkeltő céllal íródott, a wifi nagyon hasznos eszköze lehet hálózatok kiépítésének. A WPA alapú hálózatok megfelelő kulcs kialakításával, azok rendszeres cseréjével kielégítő védelmet nyújthatnak az alacsonyabb biztonsági szintet igénylő hálózatok részére.

Több olyan, a dolgozat eddigi részében nem tárgyalt hátránya van, melyek további vizsgálata szükséges a honvédségi használathoz.

Ezek például a következők:

- nagyon könnyen felderíthetőek,
- nagyon könnyen zavarhatóak, már egy mikrohullámú sütő is bezavarhat,
- WPA használat esetén is feltörhető, bár igaz nagyon időigényes tud lenni,
- A legnagyobb problémát a folyamatosan megjelenő driver hibák jelentik. Ilyen hibát mutatott be például David Maynor és Jon Ellch a 2006-os Black Hat USA konferencián. http://www.802.11mercenary.net/~johnycsh/publications/ http://www.blackhat.com/html/bh-usa-06/bh-usa-06-speakers.html

Honvédségi felhasználáshoz további vizsgálódás és később nagyon szigorú szabályzás szükséges. A legkorszerűbb eszközök és a legmagasabb biztonsági beállítások használata esetén megbízható hálózat alakítható ki.

Sebestyén Attila

CSÖKKENTHETŐ-E A „SUPERUSER”-EL KAPCSOLATOS BIZTONSÁGI KOCKÁZAT?

„Soha ne tévesszük szem elől az embert, amikor gépről beszélünk!”

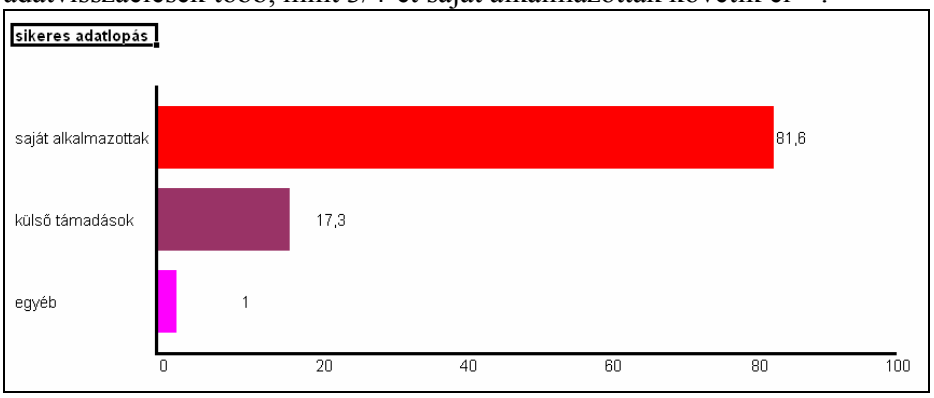
Az információs technológiák elterjedésével az információ biztonság kérdése jelentős kockázati kérdéssé vált. Az elmúlt évtizedekben a számítástechnika alapú rendszerek általánossá és meghatározóvá váltak a személyes felhasználásban éppúgy, mint az állam működésében. A közigazgatás, a rendvédelem, a honvédelem ma már elképzelhetetlen információs technológia nélkül, az adatok gyűjtése, továbbítása, tárolása, felhasználása, az eljárások és módszerek alkalmazása nélkülözhetetlenné vált működésükben. Az információ biztonsággal kapcsolatos kutatások eredményeként az informatikai piac egyik jelentős, dinamikusan fejlődő részévé vált az információ védelem. A hazai és nemzetközi szabványok, ajánlások sora foglalkozik e témával (pl.: ISO/IEN17799 – az informatikai biztonság menedzsmentje, TCSEC – kritériumok a számítógéprendszerek megbízhatóságának kiértékeléséhez, ITSEC - információtechnológia biztonsági értékelési kritériumok, ISO9000-3 szoftverfejlesztések minőségvizsgálatára, COBIT – információ technológia irányítása, kontrollja és ellenőrzése, ISO15408 – közös követelményrendszer, ITIL – informatikaszolgáltatás módszertana, és az Informatikai Tárcaközi Bizottság ajánlásai közül 8.,12. és 16.).

Tapasztalatom azonban az, hogy az un. „superuser”-ekkel (administrator, root, supervisor, sysadmin, dbadmin, stb.) érintőlegesen, kizárólag az általános elvekből következően foglalkoznak a források. Az informatikai alrendszer jellemzően centralizált, erősen hierarchikus működésében a privilegizált jogosultságokkal rendelkező superuser ellenőrzése és az ehhez szükséges módszerek szegényesek. A superuser az informatikai rendszerben betöltött pótolhatatlan szerepe és a feladat végrehajtáshoz rendelt privilegizált jogosultság következtében lényegében „korlátlan hatalommal” rendelkezik, mindezek ellenére szerepüket nem tekintjük alapvető kockázati tényezőnek. A szakirodalom nem foglalkozik érdemben a superuser munkáját, tevékenységét befolyásoló önálló biztonsági rendszabályok megfogalmazásával.

Ez egyrészt érthető, hiszen a rendszerben betöltött „korlátlan hatalma” szaktudásába, lojalitásába, becsületességébe vetett bizalom hiányában el-

képzelhetetlen, másrészt éppen a speciális – kivételezett – tudás birtokában nehezen fogalmazhatók meg egy „kívülálló” részéről, mit és hogyan kell ellenőrzés alá vonni tevékenységében, miként biztosítható a szakfelügyelet.

E gondolataim mellett jogosan vetődhet fel a kérdés: - Valóban ilyen fontos téma ez? Ténylegesen szükséges a superuser tevékenységét is „felesleges” adminisztratív és egyéb „csinált” szabályokkal „akadályozni”? A választ legegyszerűbben a statisztika segítségével lehet megadni. A sikeres adatvisszaélések több, mint 3/4-ét saját alkalmazottak követik el[174].



1. számú ábra

Igen, szükségesnek tartom a superuser, mint kockázati tényező, vizsgálatát. Ezt a szándékot erősíti bennem az is, hogy az általam megismert informatikai biztonsági politika175, informatikai biztonsági szabályzat176, vagy erre épült adatvédelmi intézkedés rendszer177, jellemzően a felhasználóval kapcsolatos normatívákat taglalja, amelyek természetesen analóg érvényesek a superuser-re is, de éppen a rendszer működésében betöltött szerepből következően nem lehetnek elégségesek.

Előadásomnak nem témája az informatikai biztonság teljes spektrumának bemutatása, így csak érintőlegesen szeretném újólag rögzíteni, hogy az általánosan megfogalmazott normák, természetesen vonatkoznak a superuser tevékenységére is, így:

---

[174] Visnyei Aladár – Dr. Vörös Gábor: a számítógépes információ biztonság alapjai – LSI Oktatóközpont – ISBN 963 577 128 2

[175] http://www.bm.hu/proba/bmtvtev.nsf/e59c75bcdbbc3613c1256835004755d5/3b0a71a8b6e30855c1256eed004abee9?OpenDocument&High light =0,informatika* - a Belügyminisztérium Informatikai Biztonsági Politikájának kiadásáról szóló 12/2004. (B.K. 12) BM utasítás

[176] A Határőrség Informatikai Biztonsági Szabályzata – kiadás előtti koordinációs példány

[177] A Határőrség Adatvédelmi Szabályzatának kiadásáról szóló 47/2001. számú Országos Parancsnoki parancs

1. az alapelvek tekintetében:

    a. a hitelesség – egy információ akkor tekinthető hitelesnek, ha mind tartalmának, mind létrehozójának sértetlensége garantálható
    b. a bizalmasság – az információhoz vagy adathoz, csak az arra jogosultak, és csak az előírt módon férhetnek hozzá
    c. a sértetlenség – az információ, vagy rendszer sértetlen, ha csak az arra jogosultak változtathatják meg, vagy minden kétséget kizáróan megállapítható az a tény, hogy az előállítás óta változatlan maradt
    d. a rendelkezésre állás és működő képesség (elérhetőség és visszaállíthatóság) –az erőforrások olyan állapota, amelyben eredeti rendeltetésének megfelelő szolgáltatásokat nyújtani képesek (működőképesség), meghatározott helyen és időben (elérhetőség).
    e. bizonyíték biztosítás és nyomon követés (*naplózás*) – az illetéktelen, jogosulatlan, illetve a jogosult események naplózása, rendszer- és felhasználói tevékenységekre vonatkozóan. (az informatikai szervezettől független biztonsági felügyelet)

2. a védelmi intézkedések tekintetében:

    a. a szervezethez kapcsolódó
    b. az infrastruktúrához kapcsolódó
    c. az eszközökhöz (hardverekhez) kapcsolódó
    d. az alkalmazásokhoz (szoftverekhez) kacsolódó
    e. a dokumentációkhoz kapcsolódó
    f. az adatokhoz kapcsolódó
    g. az adathordozókhoz kapcsolódó
    h. a kommunikációhoz kapcsolódó
    i. a személyekhez kapcsolódó
    j. az eljárási rendhez kapcsolódó szabályok.

A szakirodalom az adatbiztonsággal kapcsolatos emberi motívumokat az angol szavak kezdőbetűjével azonosítva 7-E –vel jelöli, amelyek: 178

- hiúság - ego
- sikkasztás - embezzlement
- lehallgatás - eavesdropping
- ellenségeskedés - enmity
- kémkedés - espionage
- zsarolás - extortion
- hibás döntés - error

Mint emberi tényezők ezek egyike, vagy bármelyike érintheti a superusert is, gondolkodjunk csak el a hiúság (ego) és a hibás döntés (error) kategóriákon.

A superuser a rendszer működése és fenntartása szempontjából „kivételezett" helyzetben van, hiszen dönthet „lét vagy nem lét" kérdésében, "kegyet gyakorolhat" a felhasználó támogatásban, így személyiségének, devianciájának „áldozatául eshet" az adatfeldolgozás része, vagy egésze.

Másod sorban számolnunk kell a szándékosság, vagy gondatlanság mellett azzal is, hogy a jelentkező feladathoz mérten szaktudása, tapasztalata nem elegendő.

Harmadik előfordulása lehet e kockázati tényezőnek a „kivételezettségből" eredő pótolhatatlanság, azaz olyan speciális tudás felhalmozódása a superuser -ben – majd ennek megosztás nélküli birtoklása -, amely a helyettesíthetőséget veszélyezteti, így tartós távolléte esetén szintén a működés kerül veszélybe.

Mind három esetben erősíti, vagy generálja a személyiségbeli tulajdonság a működési kockázatot, így a superuser tevékenységét úgy kell kialakítani, hogy ezek a tényezők minimálisan jelentkezhessenek a rendszer életciklusában. A kiválasztás során fokozott figyelemmel kell lenni a szakmai felkészültség mellett a személyiségbeli tulajdonságokra is. Fontos tisztában lenni a szervezeten belüli strukturális hatalmi pozíció elérésének Thompson -i modelljével179, amely szerint a szervezeten belül egy adott személy (superuser?) vagy csoport hatalmi pozíciója három dologtól függ:

178 http://www.cryptox.hu/crypto02.php - Virasztó Tamás: titkosítás és adatrejtés – NetAcadémia oktatóközpont

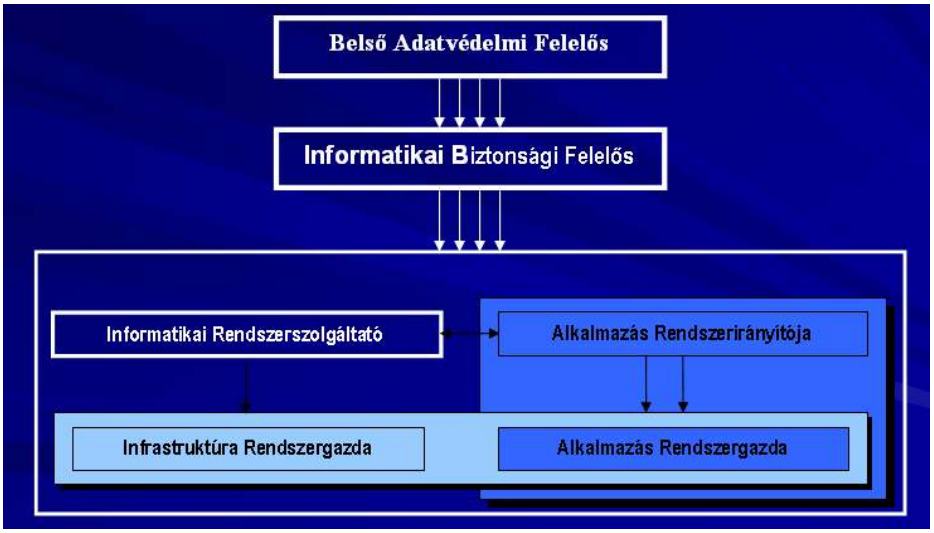
179 http://sugi.uni.hu/munka/bevmunka.doc - Csukonyi Csilla: A munkapszichológia története, vizsgálati területei, kérdései

- Az általa végzett tevékenység mennyire fontos a szervezet számára.
- A tevékenység átláthatósága: akik a nem átlátható területeket ellenőrzik, nagyobb hatalmi pozícióra tehetnek szert, amint azok, akiknek tevékenysége átlátható, mérhető. A kérdés úgy is feltehető, hogy mennyire ellenőrizhető a tevékenység, mennyi bizonytalan elem van benne?
- Lecserélhetőség (helyettesíthetőség): ha a csoport tevékenysége, vagy a személyek nem lecserélhetőek, akkor ez a csoport / személyek hatalmi helyzetét növeli.

Azt gondolom nem kell különösebben indokolni az összefüggést a superuser és a szervezet esetleges kiszolgáltatottsága között. A kérdés felvetés nem csak helyes, szükséges is: „Csökkenthető-e a „superuser" –el szembeni biztonsági kockázat?" Igen, ismertek ilyen módszerek, amelyekkel csökkenthető a kockázat. Ezek a módszerek általánosan alkalmasak minden „kiszolgáltatott" helyzetből következő szervezeti kockázat csökkentésére, megfelelő eszközt adnak a vezető kezébe.

1. Feladatkörök szétválasztása: [7]

Vannak olyan feladatkörök (szerepek), amelyek egymással össze nem egyeztethető tevékenységeket tartalmaznak, ebből következően kizárják egymást. Nem lehet a fejlesztő és az üzemeltető egy személyhez rendelt. A fejlesztés eredményességét, teljesítését minősítő nem lehet a fejlesztő szervezet alkalmazottja. A biztonsági felügyelő nem lehet az informatikai szervezet alkalmazottja stb. Az összeegyeztethetetlen munkaköröket a biztonsági szabályzatban rögzíteni kell, és gondoskodni kell arról, hogy még helyettesítés szintjén se fordulhasson elő a munkakörök ideiglenes kapcsolódása.



2. számú ábra – a Határőrség információ biztonsági szereplői (szerepkörei)

Munkakörök rotálása:180

A módszer valamilyen időközönként (erősíti a módszer hatását, ha rendezetlen időközönként történik) megcseréli a munkakörökben dolgozó alkalmazottakat, esetünkben a superusereket. A váltást véleményem szerint legkésőbb 1-2 évente szükséges végrehajtani.

Több előnyt is jelent a módszer alkalmazása. A superuserek rövid idő alatt a teljes informatikai rendszerről megfelelő tudást szereznek. Egymás helyettesíthetőségével kiküszöbölődik a pótolhatatlansági tényező. Könnyebbé teszi az ellenőrzést, hogy a több szereplő elegendő formális és informális adatot képes nyújtani a rendszerről és rendszer állapotról. A közösen ismert „téma" innovatív lehetőséget is biztosít, verseny helyzetet teremt a szakmai elismertség megszerzéséhez. Nő az üzembiztonság, hiszen több, magasabban képzett szakember van jelen a rendszerben.

2. Kötelező szabadság elve: [7]

A superuser váratlan és hosszabb távú (minimálisan 10 munkanap) „eltávolítása" a rendszerből. Kényszerű információ megosztást eredményez, illetve a kizárólagos tudás megszerzését ellensúlyozza a helyettesítő „képbe" kerülésével.

[180] Kő Andrea: információrendszerek auditálása – Budapesti Közgazdaságtudományi- és Államigazgatási Egyetem, Információrendszerek Tanszék – 2003. (címszavak a 15. oldalról)

3. Dokumentálás:[7]

A dokumentálás több lábon álló biztonsági rendszer. Első sorban minimálisan három szintű dokumentációval kell rendelkeznie minden alrendszernek (műszaki leírás, vagy rendszerterv; felhasználói leírás; rendszergazdai kézikönyv, segédlet). Másodsorban a rendszer üzemeltetésével és fenntartásával kapcsolatos feladatrendszert és szerepköröket, illetve az ehhez rendelt jogosultságok és kötelezettségek rendszerét leíró normatív szabályzó, üzemeltetési szabályzat, vagy utasítás. Harmadszor az üzemeltetési tapasztalatokat feldolgozó segédletek, jegyzetek (operátori napló, hibajavítási- vagy szervizkönyv, egyéb munkaokmányok), amelyeket időnként szükséges a korábbi két dokumentum forrás részévé tenni.

4. Hozzáférés és jogosultság szabályozás:[181]

Nem tekintem önállóan megjelenő biztonsági elemnek, hiszen a biztonsági politika, illetve a biztonsági szabályzat részeként jelenik meg. Ténylegesen, a rendszerekhez kötődő listaként az egyes alrendszerekről szóló üzemeltetési utasításban kell rendelkezni róluk. A listának, az egyes alrendszerekre vonatkozóan, minimálisan tartalmaznia kell a felhasználó azonosító adatait, a jogosultság kezdeti és végdátumát, az alkalmazáson belüli moduláris és adathozzáférési szinteket. Az ezekben a forrásokban rögzített jogosultságokat kell a superusernek érvényesítenie a rendszerekben, mind infrastruktúra, mind alkalmazás rendszer szintjén.

Az alapelv a szükséges és elégséges hozzáférés biztosítása. Az adott alrendszerhez kizárólag annyi jogosultságot szükséges a felhasználóhoz (superuserhez) rendelni, amely a feladatköréből következően elegendő a feladatok ellátásához. Ez jelenti azt, hogy az Oracle sysadmin nem feltétlenül kell, hogy superuser jogosultsággal rendelkezzen az Oracle alatt működő operációs rendszer szinthez, sőt a feladatkörök szétválasztásának elve, hovatovább ki is zárja ezt.

5. Üres íróasztal politika:[182]

Az elv ténylegesen és képletesen is tartalmazza azt az elvárást, hogy csak az éppen végzett munkafeladathoz tartozó papíralapú iratokat, vagy megnyitott dokumentumokat, alkalmazásokat hagyjunk az „asztalon”. Az iroda elhagyásakor gondoskodnunk kell arról, hogy az illetéktelen hozzáférést ne mi váltsuk ki, azaz minden papíralapú iratot, adathordozót biztonsá-

[181] U.a.
[182] U.a.

gosan el kell zárni, illetve a számítógépünkön gondoskodni kell a munkaterületünk (session, vagy task) zárolásáról. Meg kell követelni a superusertől is, hogy soha ne hagyjon felügyelet nélkül adatot, terminált, vagy számítógépet.

6. Hulladék megsemmisítése:[183]

Függetlenül az adathordozó anyagától, a feleslegessé vált adatok megsemmisítéséről gondoskodni kell. Nem elegendő a szemétkosarat, vagy a „gyors formázást" elégséges megsemmisítésnek tekinteni. A tárolt adatok minősítése szerint a biztonsági szabályzatban ki kell térni az egyes adatfajtáknak és adathordozóknak megfelelő megsemmisítési eljárásra a zúzógéptől, az égetésen keresztül az „ecetes olló" használatának előírásáig. A superuserek munkamorálját a hulladék felismerésétől, annak szabályzat szerinti megsemmisítéséig fejleszteni kell.

Azámítógépes üzemeltetői tapasztalataim szerint további módszereket javaslok figyelembe venni:

7. Szükséges és elégséges mérték:

A superuser jogosultság nem kiváltság, hanem munkaeszköz. Olyan munkaeszköz, amelyhez a rendszer életciklusában különleges feladatok elvégzése van hozzárendelve, így például hardver vagy szoftver elem telepítése, felhasználók és jogosultságok létrehozása, hozzárendelése és törlése stb. Ez azonban azt is jelenti, hogyha a superuser nem ilyen megkülönböztetett jogosultságot megkívánó feladatot kell ellásson a rendszerben, akkor a rendszer használatához „egyszerű" felhasználói, vagy kiemelt felhasználói jogosultsággal kell hozzáférnie. Azért is tudatosítanunk kell ezt a korlátozást a superuserekkel, mert az azonosító megszerzése, vagy a felhasználó nevében való eljárás (például egy vírus esetében), azokkal a privilégiumokkal bír, amelyet a megszerzett jogosultság enged. Az elvégzendő feladathoz szükséges mértékű, de elégséges hozzáférési jogosultságot kell alkalmazni, amellyel az adott feladatkör, vagy definiált szerep érdemben és maradéktalanul elvégezhető.

Napló és monitoring rendszer:

A rendszer és alkalmazás szintű naplózás elengedhetetlen segédeszköze a fenntartási tevékenységnek és kiegészítője a biztonság és adatvédelem

[183] U.a.

eszközrendszerének. Tudomásul kell venni, hogy a naplózás nem preventív, hanem utólagos eszköz, ugyanakkor elsődleges forrása a rendszer-, vagy felhasználói tevékenység tendenciáinak monitorozására, illetve a sikertelen műveletek, jogosulatlan hozzáférések megismerésére (a bizonyíték biztosítás és nyomon követés elvének alkalmazása).

A superuser felhasználó jogosultságát a napló állományok esetében csak olvasásra szabad engedélyezni. Ez megvalósítható úgy, hogy a napló állományokat egy központi tárhelyre készíttetjük el, amelyhez csak a saját alapértelmezett (helyi) superuser felhasználói jogosultsággal lehet hozzáférni, amely hozzáférést kizárólag az informatikai biztonsági felügyelő részére biztosítunk, illetve ezen az eszközön semmilyen szintű egyéb felhasználói tevékenységgel összefüggő szolgáltatatást nem nyújtunk.

8. Megszemélyesítés:

Az alapértelmezett superuser felhasználók használatát a rendszerben következetesen tiltani kell. Ez azt jelenti, hogy azokat a feladatokat, amelyek a superuser jogosultságot megkívánják, olyan nem superuser névvel azonosított felhasználói jogosultsággal kell elvégezni – amely rendszerben ez lehetséges -, amely egyedileg azonosítja a jogosultságot használót. Azaz nem rendszergazda felhasználói névvel, hanem pl.: Sebestyén Attila felhasználói névvel kell a superusernek dolgoznia, amely felhasználói névhez rendelhető a superuser jogosultság. Kívánatos, hogy egy-egy alrendszerben 2-5 főnél ne legyen több aktív superuser jogosultságú felhasználó. Rendkívüli beavatkozást igénylő rendszeresemény bekövetkezésekor, ha a beavatkozó személy nem rendelkezik aktív superuser jogosultsággal, lehetővé kell tenni az alapértelmezett superuser felhasználói névvel való bejelentkezést. Ezt egy előre kialakított rezsim mellett, például az operátori szolgálatnál elzárva (rendszerenként borítékban, vagy kulcsdobozban), és felfektetett jelszónyilvántartással, kell biztosítani. Az alkalmazását követően a ellenőrizni kell a superuser jogosultsággal rendelkező felhasználók körét, illetve az alapértelmezett felhasználói névhez tartozó jelszót cserélni kell.

A felhasználói hozzáférés naplózásának, monitorozásának a superuserek esetében csak az egyedi felhasználói név esetében van értelme.

9. Az egyszemélyű vezetés:

A superuserek tevékenységét az üzemeltetési és fenntartási tevékenységgel megbízott szervezeti elem vezetőjének kell felügyelnie. Ez jelenti a napi feladatszabáson, koordináción, szakfelügyeleti ellenőrzésen túl azt is, hogy neki kell gondoskodnia a rendszerek alapértelmezett superuser jogo-

sultságainak felügyeletéről, jelszó módosításairól. Alapszabály, hogy egyéb tevékenységei során a vezető is saját felhasználói név és jelszópárossal dolgozzon, amelyek hozzáférési jogosultságának a szükséges mértékben meg kell felelnie az elvégzendő tevékenységnek.

Előadásom hangsúlyosan NEM a superuser felhasználókkal szembeni bizalmatlanságot kívánta életre hívni és főleg nem minősíteni szerette volna az ilyen tevékenységet ellátó személyeket. Egyszerűen csak fel kívántam hívni a figyelmet arra, hogy a superuser jogosultság munkaeszköz, és mint ilyen az alkalmazójára is érvényesek minimális alkalmazói követelmények normatívák. Tapasztalatom szerint az informatikai rendszerekben megfogalmazott normák a felhasználói tevékenységek „kordában tartására" irányulnak, pedig adatvédelem, informatikai biztonság tekintetében a superuser is „csak" egy felhasználó a rendszerben, még akkor is, ha privilegizált jogosultságokkal rendelkezik.

Felhasznált irodalom:

[1] Visnyei Aladár – Dr. Vörös Gábor: a számítógépes információ biztonság alapjai – LSI Oktatóközpont – ISBN 963 577 128 2

[2] http://www.bm.hu/proba/bmtvtev.nsf/e59c75bcdbbc3613c1256835004755d5/3b0a71a8b6e 30855c1256eed004abee9?OpenDocument&High light =0,informatika* - a Belügyminisztérium Informatikai Biztonsági Politikájának kiadásáról szóló 12/2004. (B.K. 12) BM utasítás

[3] A Határőrség Informatikai Biztonsági Szabályzata – kiadás előtti koordinációs példány

[4] A Határőrség Adatvédelmi Szabályzatának kiadásáról szóló 47/2001. számú Országos Parancsnoki parancs

[5] http://www.cryptox.hu/crypto02.php - Virasztó Tamás: titkosítás és adatrejtés – NetAcadémia oktatóközpont

[6] http://sugi.uni.hu/munka/bevmunka.doc - Csukonyi Csilla: A munkapszichológia története, vizsgálati területei, kérdései

[7] Kő Andrea: információrendszerek auditálása – Budapesti Közgazdaságtudományi- és Államigazgatási Egyetem, Információrendszerek Tanszék – 2003.

RÉVÉSZ Gyula

MISSZIÓS HÍRADÓ FELKÉSZÍTÉS SOKSZÍNŰSÉGE

Társadalmunk a gyökeres átalakulások korát éli. Egész társadalmunk fejlődésének egyik kulcskérdése és nélkülözhetetlen feltétele a tudati viszonyok gyorsabb ütemű fejlesztése, az emberek gondolkodásának erősítése, erkölcsi arculatuk megváltozása, műveltségük gyarapítása, valamint a mai „rohanó" világ gyors ütemű fejlődésének –mind a számítástechnikai, a híradó és informatikai fejlődésnek- szinte azonos ütemben való követése.

A békefenntartás az egész világban,így térségünkben és Magyarországon is átértékelte a biztonság- és védelmi politikát, a haderő átalakítását, a Magyar Honvédség felkészítését. Az elmúlt évtizedben a magyar haderő óriási utat tett meg a statikus országvédelemtől, a missziós hadsereggé történő átalakulásig. Ma a Magyar Honvédség elsősorban nemzetközi békeműveletekre szakosodott, professzionálissá való önkéntes haderő, amelyek hajtóereje egyértelműen a külföldi missziós tevékenység.

A katonai klasszifikáció szerint a béketámogató műveletek magukba foglalják a békefenntartást, a békekikényszerítést, a konfliktus megelőzést, a humanitárius feladatokat és a békeépítést. A változó missziós nemzetközi követelményrendszer újra és újra felveti a kérdést, hogyan lehetne a magyar békefenntartói jelenlétet-lehetőségeinknek és képességeinknek megfelelően- dinamizálni, az elért eredményeket tovább javítani.

A békeműveletek teljesen átalakították a magyar haderő mindennapjai, a szolgálati viszonyokat, a kiképzést, a feladatok minden oldalú biztosítását. A missziók a kihívások, a jobb fizetés és a kiszámítható feladatrendszer miatt vonzóak a katonák körében.

Mindezek egy szakmailag jó felkészültségű kiképzők révén, akik megfelelő oktatói, nevelői és pedagógiai módszerek alkalmazásával válnak megvalósíthatóvá. Itt kell hangsúlyozni a megfelelő nevelői, pedagógiai módszerek alkalmazását, mely nélkül eredménytelen lenne a csupán szakmai oldalról való megközelítés.

„Társadalom, pszichológia pedagógia" sajátos katonai elemek egymásra hatóan rendeződnek el, s az erőtényezők fókuszában ott van az a bizonyos legnemesebb anyag, az ember, mint személyiség és nemléli lényegénél fogva humanizmust, egyéni bánásmódot, nevelői tapintatot követel.

A személyi állomány kiképzése és felkészítése javításának egyik legfontosabb iránya az intenzifikálás,- azaz az alegységek fokozása az által, hogy erősödik a parancsnokok és a beosztottak által végzett- a maga színvonalú, végső eredmények elérésére irányuló katonapedagógiai tevékenység feszítettsége. Ez a kiképző-felkészítő feladatok részletes, konkrét meghatározásával, a kiképzés és felkészítés korszerű módszertanának, legújabb techni-

kai és egyéb eszközeinek alkalmazásával, a tapasztalatok elemzésével - kutatásával, azoknak a kiképző-felkészítő folyamatban való rendszeres alkalmazásával érhető el.

De aztán a legeredményesebb munkát a programozott oktatás perspektívája adja. Ez a perspektíva társadalmilag determinált. Egyrészt a kiképzési idő csökkenésével, ugyanakkor az oktatás hatékonyságának növelésével, erősítésére irányuló törekvésekkel és természetesen még nagyon sok mindennel függ össze. Egyet leszögezhetünk: a programozott oktatás rejti magába a legtudatosabb kiválasztott, illetve a tanári, programozói munkával legmódszeresebben feldolgozott tananyagot, azokat a fogalmakat, szakanyagot és összefüggéseket, amit a tanuló, ez esetben a katona személyiségére, már meglévő ismereteire szabtak, a további követelmények reális kialakítása mellett. A híradó és informatikai felkészítés célja a kiképzés folyamatában oktatott valamennyi kiképzési ág ismeretanyagát logikailag integrálva felkészíteni a katonákat a korszerű harc követelményeiből adódó- a vezetésigényeit kielégítő- híradás létesítési és biztosítási feladatok ellátására egyszerű és bonyolult viszonyok között.

A missziókban részt vevő erők általában a legjobb (sokszor legújabb) felszerelést, új vagy felújított harci-technikai eszközöket, műholdas, híradó és informatikai rendszereket kapnak. Bár jól tapasztalható a KFOR műveletekben fenn álló akadályok amelyeket a kapcsolattartás, információ áramlás és vezetés terén jelentkező interoperabilitási problémák (korszerű híradó eszközök hiánya, a rosszul felfogott alkalmazási szabályok „roe” felszerelési gondok szülnek. Ezen problémákat csak tudatos, jól felépített szakmai felkészítéssel lehet orvosolni).

A műveletek helyszínen, a missziók részére szükséges technikai eszközök döntő többsége a Magyar Honvédség rendszeresített technikai eszközeiből kerül biztosításra. Ezek mellett speciális technikai eszközökre is szükség van, amelyek nem tartoznak a Magyar Honvédség rendszeresített eszközállományába, így ezeket külön kell beszerezni és külön kell kiképzést szervezni. Fel kell készíteni a híradó szakbeosztású katonákat, kezelőszemélyzetet a technikai eszközök telepítésére, üzembe helyezésére és üzemeltetésére. Miután megfelelően begyakorolta a szakállomány a különböző elemek-eszközök szakszerű telepítését, üzemét ekkor valósulhat meg az információ gyors pontos és megbízható továbbítása a lehetséges üzemmódokban és vezérlési változatokban, valamint az egyéb állomány folyamatos képzése-oktatása a napi feladatok teljesítése érdekében.

A kiképzés-felkészítés a soros KFOR misszió esetében is követte ezen kialakult tematikát. Megállapításra került a híradással összefüggő feladatok, tevékenységi körök, majd ezt szem előtt tartva került a kiképzés.

A kapcsolattartás és a vezetés alapját biztosító információ átadása, cseréje, továbbítása döntően technikai eszközök alkalmazásával történik. A

kommunikáció fejlődése, fejlesztése elkerülhetetlen folyamat. A magas szintű elvárásoknak, követelményeknek a haderő- jelen esetben a misszió teljes állománya, sofőröstől, őrkatonástól szakácsig – akkor és csak akkor volt képes megfelelni, amikor a kommunikációs eszközökre megkapta a kiképzést. Ezen távközlési szolgáltatásra jelenlegi helyzetéből fakadóan többrétegű képzés során készült fel az állomány.

A felkészítés „I.” és „II.” csoportra osztható fel, melyből a „I.” csoportot a híradó szakbeosztású katonák a „II.” csoportot pedig az egyéb beosztású katonák alkották.

A híradó szakbeosztású állomány szakkiképzése rendkívül fontos, de sokrétű felkészítést vont maga után. Már korábban megállapításra került, hogy milyen fontos a célirányos, igazán nagy tudású és felkészült kiképző állomány szerepeltetése. A technikai eszközök széles skálája mutatja a békeműveletet híradó biztosításának sokrétűségét, összetettségét. Mind a vezetés, mind a kapcsolattartás (honi és helyi kommunikáció terén) híradó feladatai szükségessé tették az eszközök komplex és egyedi megismerését is.

A KFOR szolgálatra való felkészítést megelőzte a híradó szakállomány kiválasztása és az ismert technikai eszközökre vonatkoztatva gyakorlati foglalkozások megtartása. Itt a katonák meglévő szakmai múltjára építve került összekovácsolásra az állomány. A későbbi szakkiképző állomány ezekre a széles alapokra építette a speciális híradó eszközök és a vásárolt szolgáltatások megismertetését. Mivel a misszió fő feladata az őrzésvédelem, így fontos részt képezett a felkészülés során a vezetékes eszközök (telefon, TBK, TKV-100, stb.) megismerése, kezelésének, telepítésének elsajátítása. A honi bázison folyó előzetes felkészítésben ez nagyrészt töltött ki. A speciálisabb híradásra való felkészülés keretében a nemzeti híradás alapjául szolgáló „AN PRC-138” (RF-5200-val) rádióállomás megismerése jelentette az alapokat.

Kiképzés alkalmával megismerte az állomány a rádióállomás harcászattechnikai adatait, telepítésének módozatait, részeit valamint programozásának módjait és a működési elvét. Az „AN PRC-138” berendezés használatát a felkészítés keretében szimuláltuk és különböző helyzetekben a kiképzők útmutatásainak megfelelően lemodelleztük a szabályos híradó forgalmazást. Ezen feladat különös fontosságú hiszen a nemzeti híradás alapja és a hírközpontba telepített rádióállással napi három alkalommal, folyamatos működés mellett kapcsolatteremtést kezdeményezett a híradó szakállomány a hadműveleti területről Magyarországgal. A forgalmazás normál távbeszélő üzemmódban nyílt és zárt csatornán történt meg, valamint adatátvitel végrehajtására is sor került Pc. segítségével.

A stabilan működő rádióösszeköttetésen túl a híradás legfontosabb eszközének – egy „speciális”, vásárolt szolgáltatás, - a VSAT rendszer vált.

A műhold alapvetően és eredendően kommunikációs eszköz, de arra is jó, hogy átjátszó állomásként vegye a Föld egyik pontjáról kiinduló rádióadást, felerősítse, majd adóként tovább sugározza a Földnek egy másik helyére. Ezen a felismerésen alapul a műholdas adattovábbítás, a műholdas műsorszórás és a műholdas telefonálás.

A „VSAT" rendszer egy speciális űrtávközlési rendszer, amelynél a földi pontok között műholdon keresztül létesül egy vagy kétirányú kapcsolat. Az angol elnevezés (Very Small Aperture Terminál) a felhasználóknál elhelyezett kis méretű antennákkal egybeépített egységekre, termálokra utal. A távközlési műholdakat űrtávközlési szervezetek üzemeltetik, és tőlük lehet csatornakapacitást bérelni. A kis méretű földi terminálok az alábbi csoportokba oszthatók:

- csak vételre szolgáló terminálok
- adó-vevő terminálok

Csak vételre szolgáló terminálokkal felépített rendszerek műsor- vagy adatszórásra, úgynevezett egyirányú összeköttetésre alkalmas rendszerek. Egy központi állomásból és csillagalakzatban elhelyezett vevő terminálokból állnak, a központ és a terminálok között műholdon keresztül létesül egyirányú kapcsolat. A központi állomásról kisugárzott jelet a műhold közvetítésével minden, a rendszerhez tartozó terminál egyidőben veszi. Adóvevő terminálokkal kétirányú összeköttetéseket hozhatunk létre, elsősorban adatátviteli célból. Az adatátviteli sebesség általában 64 kb/s vagy ennek egész számú többszöröse. A kapcsolat műholdon keresztül létesül a központi állomás és az egyes terminálok között, és csak ritkán két terminál között, ezért ez a rendszer is többnyire csillag felépítésű.

A műholdas összeköttetés használatára való felkészítést a szolgáltatást nyújtó cég, a Hungaro Digitel Kft. végezte. A szakkiképzés során a híradó katonák fel lettek készítve a hírközpont területén, stabilan letelepített eszköz használatára. A kiképzés alkalmával megszerzett tudás felvértezte a szakállományt a berendezés folyamatos üzemeltetésére és az esetleges kisjavítások, áttelepítésből adódó feladatok elvégzésére. A felkészítés során szerzett ismeretek, így kielégítő volt az üzemeltetés idejére. Az üzemeltető céggel a kapcsolattartás folyamatos volt és szakszerű, azonnali segítések nyújtottak problémák elhárítása esetén.

Ezen letelepített szolgáltatás, VSAT rendszer, 8 darab csatornát biztosított a kommunikáció továbbítására, stabil működéssel.

Csatornák elosztása:

1. PK. közvetlen vonal
2. FAX vonal

3-4. Telefonfülke szolgáltatás magánbeszélgetés céljára

5-8. HM vonal szolgálati beszélgetés céljára.

A híradó szakbeosztású katonák speciális felkészítése itt folyt össze egy másik eszköz, a HICOM Központ megismerésével. A VSAT rendszeren biztosított híradó csatornák a HICOM Központban végződnek, amelyről már a híradó kezelő kapcsolja tovább a megfelelő végpontra.

A szakfeladat dandárja a telefonhívások lekezelése, dokumentálása és kapcsolása tette ki. A híradó szakállomány folyamatosan, napi 24 órában működtetve kezelte ezen eszközöket.

A fentiekben felsorolt híradó eszközök (rádió, VSAT, HICOM) üzemeltetésének – kezelésének elsajátítása a Magyarországi szakfelkészítéseken csak az első lépcsőfok volt. Ugyanilyen hangsúllyal lehet beszélni a már műveletei területre kiérve, a hírközpontban letelepített eszközök folyamatos üzemeltetésével kapcsolatban megszerzett tudás elmélyülésének fontosságáról. A híradó szakbeosztású katonák kiképzése tehát nem ért véget Magyarországon, hanem a helyszínen, a már gyakorlattal rendelkező, leváltásra kerülő szakállomány tudásának – tapasztalatának átadásával teljesedik ki. A megszerzett tudás szinten tartásának érdekében nem csak a folyamatos munkavégzés, hanem havonta egy alkalommal – rangidős parancsnok vezetésével – szinten tartó foglalkozások megtartása a biztosíték.

A nemzeti híradás, valamint a „vezetékes-műholdas" összeköttetések biztosításán túl a szakállomány elsajátította néhány speciális híradó eszköz használatát is. Ezen eszközök a hagyományos vezetékes (TBK, Telefon, FAX) és rádió (R-159, R-173) berendezéseken túl biztosította a napi szolgálati tevékenységet. Ez nagy felelősséggel járt, mivel oktatni kellett az eszközöket kezelői, felhasználói állományt is.

Ilyen híradó berendezések voltak a Motorola GP300 vagy GP340, MATRA rádió, Mobil telefonok és az Immarsat műholdas telefon.

A napi szolgálati tevékenység kommunikációjának alapja a Motorola rádiók voltak. Ezek a 16 csatornás, max. 5 Watt teljesítményű készülékek könnyen kezelhető, nagy számban megjelenő eszközök tették ki a szolgálati kommunikáció 90 %-át. A nagyarányú felhasználás okán ezen eszközöknél nagy számban jelentkezett meghibásodás, programozásból eredő problémák. A híradó katonák a leváltott szakállomány útmutatása, felkészítése révén jó szinten elhárította a fellépő hibákat.

A MÁTRA rádiók a KFOR parancsnokságról kapott berendezések, amelyek a fontosabb szolgálati személyek összeköttetésének létesítésére szolgált. A berendezés stabilan működött, mobiltelefon elvei alapján, telepített átjátszó adókon keresztül.

Fontos híradó eszközként jelent meg az INMARSAT műholdas telefon, amely virtuális és globális lefedettséget biztosít a Földön. A műhold és a távközlési hálózatok közötti kapcsolatot a Földi állomások biztosítják.

Összegezve jól látható milyen összetett technikai állománnyal, összetett feladatokkal került szembe a híradó szakállomány. A fent említett technikai

eszközök széles skálája mutatja a békeműveletek híradó biztosításának sokrétűségét, összetettségét. De ezen feladatok megismerésével, leküzdésével még nem ért véget a híradó katonák feladat komplexuma. A korábban említett „II" csoport – azaz a misszióba beosztott egyéb szaktudású katonák felkészítése és folyamatos ellenőrzése is nagy terhet rótt a híradó katonákra.

Alaprendeltetésből álló feladataikat végző katonák részére híradó ismereteket kellett nyújtani mind eszközkezelésből, mind forgalmi szolgálat helyességéről. A legegyszerűbb híradó berendezés (TBK-67, TAP-77) kezelésétől a kis teljesítményű rádiók (R-159) használatán keresztül egészen a műholdas telefonig. Itt már mint szakoktatók jelentkeztek a híradó katonák.

A kezdeti időkben hetente került oktatásra a felsorolt eszközök használata, forgalmi szolgálat szükségessége.

Később, a missziós időben előlépve, megszerzett tapasztalatokkal felvértezve már a havonta ismétlődő híradó foglalkozások is kielégítőek voltak. Általában a szolgálati helyeken rendszeresített híradó eszközök szerint kerültek végrehajtásra az oktatások.

A tábor őrzését-védelmét ellátó őrség részére rendszeresített eszközök (TBK, Telefon, Motorola) folyamatos ellenőrzése a híradó szakállomány munkafolyamatába tartozott. A napi használatot elősegítette, hogy folyamatosan ellenőrizték a működőképességet, valamint a havi híradó foglalkozások megfelelő alapot teremtettek az eszközök zavartalan működtetésére.

A külső bázis őrzésének híradó biztosítására telepített eszközök hetente kerültek, szakellenőrzésre, illetve hibafeltárás esetén azonnali javításra. A bázis őrségnél használatban lévő eszközökre (TBK, R-159, R-173, Mobiltelefon, Műholdvevő klt., MÁTRA rádió) szintén folyamatos felkészítés teremtette meg a működés szakszerűségének alapjait.

A KFOR parancsnokság őrségénél rendszeresített eszközök az előbbieknek megfelelően hetente kerültek szakellenőrzésre, illetve hibajelenség esetén azonnali szervizelésre. Az őrségnél rendszeresített eszközökre (TBK, R-159, R-173, Motorola, MÁTRA rádió, Telefon) a felkészítést, kiképzést az előbbi rendnek megfelelően végezte a híradó állomány. Visszatekintve a híradó szakfeladatok sokrétűségére jól látható milyen fontos szerepet töltött be a szakfelkészítés, komoly tudással rendelkező szakembergárda által, valamint hogy a megszerzett tudást még ha egyszerűsítettebb formában is, de tovább kellett adni.

A régen megszerzett tapasztalatok és az új kihívások által nyert tudás vegyítése viszi előre a szakembert.

Erik PÁNDI, Attila TAKÁCS

UNION SUPERVISION OF THE REGULATORY SYSTEM OF ELECTRONIC INFORMATION

Erik PÁNDI-Attila TAKÁCS[184]

Preamble: The rules of the European Union concerning electronic information have been operative since 2003, as a strategic element of the restarted Lisbon Strategy to inspire advancement and competitiveness. The present publication – based on the wide-range opinion of experts dealing with this topic - outlines the European Committee motions supervision last year the system of governance, with special regard to the reform of information market analysis.

Key words: electronic information, governance, European Union, European Committee, national regulating authority

1. Background

The purpose of regulating electronic communication and services – *in compliance with the Lisbon Strategy*[185] – is triple, that are: acceleration of competition, assisting the development of interior markets, furthermore the protection of European citizens' and users' interest. The framework of governance included the following five directives between 2003-2006:

a) Directive 2002/19/EC of the European Parliament and of the Council of 7, March, 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive – AcD);

b) Directive 2002/20/EC of the European Parliament and of the Council of 7, March, 2002 on the authorisation of electronic communications networks and services (Authorisation Directive – AuD);

c) Directive 2002/21/EC of the European Parliament and of the Council of 7, March, 2002 on a common regulatory framework for

[184] authors: LtC Erik PÁNDI Ph.D., Associate Professor at Zrínyi Miklós National Defence University, LtC Attila TAKÁCS M.Sc., head of department of PMO, PhD-student at Communications Department of ZMNDU

[185] Motion i2010 of the European Committee also emphasizes the cardinal part of information and communication technologies (ICT) in reaching the increase and workplace generating purposes of the Lisbon Strategy. These aims are supported by a regulatory framework concerning European electronic information, that serves the boosting of market competition, by investment and innovation ensuring assortment, quality and lower prices for the customers.

electronic communications networks and services (Framework Directive – FD);

d) Directive 2002/22/EC of the European Parliament and of the Council of 7, March, 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive – USD);

e) Directive 2002/58/EC of the European Parliament and of the Council of 12, July, 2002 concerning the processing of personal data and the protection of privacy in he electronic communications sector (Directive on privacy and electronic communications – Dpec).

Perhaps the most important member of the regulatory frame is the so called market analysis mechanism pursuant to article seven, with the essence that in those electronic information markets, where there is no effective competition national authorities shall run market analysis periodically and based on the result they shall lay obligations on the supplier with determined significant market force. Regulatory authorities of the member countries have to report to the EC the result of market analysis and tyke the necessary action, in connection with which the EC has observing – *and in certain cases* – veto right. Regulation can cease continuously, if effective competition takes place in a certain market.

2. Operation and efficiency of the present system

A report of the EC issued on European information governance and markets[186] came to the conclusion, that emerging competition means more benefits to the users, and that there is positive expectation for innovation and investment inside the member countries and beyond boundaries too. The regulation frame ensures for the consumers to use basic services at allowable price. Additionally this branch has been developing successfully and dynamically. The branch of ICT technologies is the most dynamic part[187] of European economy. The value of investments into the sector has reached the volume of that in North-America and Asia, which is not characteristic to any other European branch. Most of the investments moved inside Europe to the place, where the regulatory model was applied effectively and competition-focused.

[186] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions – European electronic communications regulations and markets 2005 (11th Report)

[187] Total increase in income continued on an estimated 3,8% and 4,7% level. The production and use of ICT amounted to approx. 40 % of the increase in efficiency, and reached one-fourth of the total European increase.

Based on the EC opinion this regulatory frame resulted more consistent rules and clear procedure. During the three years following commencement the EC analysed and closed almost 470 cases, from which only five were vetoed and the national regulating authorities withdrew their declaration in 17 cases. During the negotiation before the supervision of the frame system[188] many of the member countries urged simplifying market analysis beside spectrum economization. The EC came to the conclusion that the present FD is basically satisfactory, there is no need for radical changes, however in some places the system shall be supervised.

3. Supervision of the system, significant changes

Supervision of the system was executed in two parallel ways. The EC submitted for open negotiation its documents concerning the supervision of the directives and the directive on relevant markets (Rec) on 29 June 2006. The negotiation lasted until the end of the year, so significant changes came into force this year and will come into force .[189] Fields of the changes:

a) changing the system of spectrum regulation;

b) decreasing the burden on national regulatory authorities through modifying the system of market analysis;

c) strengthening the consolidation of the interior market and the protection of consumers' and users' interest, increasing safety and cancelling out-of-date rules.

4. Procedure pursuant to article seven, furthermore supervision of the Rec

During the years between 2003-2006 the co-operation between the national regulatory authorities and the EC was generally normalised and flexible, though during the supervision process however the professional organisation answering the „Call for Input" form gave almost a uniform answer saying, that the procedure indicated in article seven shall be simplified.

4.1. Changes in article seven

As a reply to the demand the EC in its motion considered possible – based on the experience so far – simplifying the procedure in a way, that

[188] The reason for the supervision is partly formal, as it is also included in the FD that the EC has to supervise the operation of the system for the first time three years after coming into force. On the other hand the supervision is rather worthy, because experiences of using a brand new system are valuated, taking into consideration the related questions and possible solutions too.

[189] The commencement of supervised directives is only expected by 2009, that is innovations beyond market-analysis fields are subject to a longer process.

the system of market analysis would exist in general, but in case of some market fields and procedure would be more simple, like:

a) in case of such markets, where the earlier market analysis found effective competition, except when competition conditions have been significantly changed since the supervision;

b) in case of such reports, where there are only slight alterations compared to the earlier reported actions.

In the framework of the simplified procedure national regulatory authorities shall fill in only one – *according to general rule* – standard application. A part of the rules for the procedure according to article seven is included in the FD, while the other part is included in the Rec. According to the long-term conception of the EC all these procedure rules would be fixed in one decree, which in addition to these procedure rules would also include the compulsory rules for starting and ending future market analysing actions.[190]

If the national regulatory authority finds, that there is no effective competition in a certain market and it identifies the supplier with significant market force, based on the FD at least one obligation shall be levied on the supplier. Perhaps the most important part of the market analysis is the imposition of obligations, as market troubles in the market can be solved in this way. Authorities shall impose such obligations, that are reasonable and proportional to the regulatory purposes indicated in the FD. Most of the observations in the cases analysed by the EC relate to the proposed obligations, as in several cases the national regulatory authorities would like to use such obligations, that are not or only partly proper for solving the competition observed. [191] Additionally, the authorities have not always set the same commitments in case of identical markets, which causes difficulties in the operation of the interior market, as the operation of pan-European suppliers is getting more difficult.

We shall also add to the above, that the EC does not have resources for following the imposed obligations, however it would be important as the national regulatory authorities do not have to accept EC remarks.[192] The existence of remarks in this form does not guarantee, that the authority really accepts them and it was relatively regular, that EC remarks were

[190] e.g.: each analysis shall be closed within 12 months from the beginning of the market-analysing process.

[191] E.g.: the cost calculation method to be implied was not proper, that is it related not symmetrically to suppliers having significant market force, or results would be reached too late.

[192] At the same time consideration is compulsory

ignored with or without any reason. The EC could have in this way an important right, if it could effect its veto right upon imposing obligations. The motion for supervision confirmed at the same time, that the EC could not replace obligations concerned inadequate with any other, but it could note it in the justification what the problem is with the obligations. The new right could really assist the making of the European regulatory surroundings more uniform and clear.

4.2. Supervision of the Rec

The creation of Rec is prescribed in article 15 of FD. Based on this article the EC accepted in the autumn of 2003 the Rec, where taking into consideration competition right principles, 18 such markets were identified, where the application of ex-ante regulation could be justified. It is of great importance therefore, what the EC considers a market to be regulated in the Rec, as this advance analysis is a kind of standard for the national regulatory authorities. The authorities will analyse only those markets in general, that are included in the Rec, however the authorities could identify other markets too.

The EC applies the so called triple criteria test for defining which markets make this kind of special governing necessary. The cumulative conditions required of the introduction of ex-ante regulation are the following:

a) high entrance barriers;

b) behind the entrance barriers the certain market does not move forward effective competition;

c) competition-law itself is not proper for handling market problems.

In the EC supervision material it became obvious, that in case of markets in Rec national regulating authorities do not have to run the three-criteria test, as in case of such markets the fulfilment of criteria can be assumed. It is also an innovation, that the Rec exactly defines those aspects, by the measuring of which the authorities can identify new markets not included there. The review material also cleared, – *among others* – the question of emerging markets. According to the FD early regulation of emerging markets shall be avoided. The EC standpoint says that those markets can be considered emerging, which are so new and fluid, that the realisation of the above mentioned triple criteria test is uncertain. The decision itself is of course difficult and we can expect interesting new in this field, with special regard to the strong technological and supply convergence.

The Rec then included 18 markets, seven of which were retail markets. The markets were basically divided upon the distinction of

immovable/mobile, voice-/data transmission services, the supervision material did not depart from it – *in general.* The applied logical division is the following:

a) immovable retail markets in the phone supply system;

b) immovable wholesale markets in the phone supply system;

c) immovable retail- and wholesale markets in the field of data exchange;

d) markets of hired lines;

e) markets of mobile services.

In the field of **immovable retail markets of phone service supply** six retail markets were defined, from which two are access (private and not private) and four call-market (local, regional, international private and international not private) type. The norm for specifying markets relevant from the point of view of regulation is that controlling is only justified, if there is no effective competition in the certain retail market, despite the regulation of the related wholesale markets and the setting of commitments. The EC motion upon analysing retail admittance markets came to the conclusion, that the division of the market into community and corporate spheres is not reasonable, but keeping the market in Rec is justified. The reason for it is that the only wholesale market, the regulation of which would affect this market is the market of joining the local loop, entrance into which requires time-consuming and expensive investment. Additionally, the realization of these investments does not grant either competition in this retail market, as suppliers usually invest into joining the local loop not or not only for call access.

In case of the immovable phone supply markets the EC came to a different conclusion. Regulating the wholesale markets connected to this retail market would significantly decrease market barriers. This face is confirmed by the appearance of alternative market suppliers all over Europe. The appearance of suppliers operating based on medium-selection and advance medium selection, furthermore the spreading of wideband voice-services in these markets move towards effective competition, so according to the EC motion the markets of immovable phone services would be taken out from the Rec. At the same time, if national regulatory authorities justify that, they will have the possibility of analyse these markets in the future, if those comply with the conditions of the triple criteria test.

Immovable wholesale markets in the field of phone-supply services call termination is the least replaceable unit from among the components necessary for retail calls. Taking into consideration, that there is not such factor, which could replace it and suppliers terminating calls have advantage in their own network, keeping of this wholesale market in the

Rec is still reasonable. In addition to call termination, the least replaceable element necessary for call set up is the calling service, that can be alternatively replaced by the setting up of a new network or buying an existing network. Experiences show, that neither the installation of alternative-access networks or the assignation of the local loop reach such level, where significant pressure could be laid on the market position of incumbent suppliers.

In case of **immovable retail and wholesale markets** two such markets shall be mentioned, which would have needed ex-ante regulation, these are the wholesale market of transferring metallic loop and sub-loop and the wholesale market of wideband service admittance. The EC wanted to keep both of them in Rec, together with further disqualification of retail markets.

In the **market of hired lines** the Rec identified three markets, on retail level: the market of minimum stock of hired lines, on wholesale level: the termination and trunk segment markets of hired lines. Experience shows, that in the market of termination competition has not become more intensive, while in the trunk segment market there are countries, where alternative suppliers made significant investments and competition began. Although this phenomenon is not relevant to the entire Union. Pursuant to the EC motion it is expedient to keep two wholesale markets in Rec, but not the retail market, because in case of wholesale regulation there is not such obstacle to entrance, that would account for keeping the market of minimum stock in Rec.

In the field of **mobile service markets** there were basically three wholesale mobile markets, that is the market of public mobile phone-network admittance and calling, the market of talk-purpose call termination in individual mobile network, furthermore the national market of international rooming through public mobile networks. After the identification of mobile markets in 2003 the spread of mobile use and the proportion of number carrying increased all over Europe. In more than half of the member countries mobile suppliers concluded contracts with virtual mobile suppliers, increasing in this way the intensity of competition. The sector is consolidated in some member countries and 3G suppliers have also entered the market. The market of call termination was still considered by the European Committee, that it is kept in Rec with the fact, that the market covers not only the termination of calls but also that of SMS messages. The market of admittance to the public mobile phone network and of calling was adjudged more complicatedly, as there is close competition on the retail market in several member countries, and in many member countries virtual mobile suppliers are also present. Some samples show, that it could be the suppliers' interest to impede competition in order to retain the existing market share and price level.

Based on the experiences, keeping the national market of international roaming through public mobile networks in Rec was not enough and proper itself for decreasing high tariffs. The European Committee launched several cartel acts, then by the elaboration of a decree it could decrease roaming tariffs by 2007. Upon the 2006-year supervision there was no definite decision for keeping the market in Rec.

Summing up the result of Rec supervision it can be stated, that the number of 18 identified markets decreased by at least one-third, which makes nowadays the everyday official work of national regulatory authorities easier.

5. Summary

The result of the 2006-year review cannot be considered as basic alteration of regulation, we can rather speak about rectification. Although we can say, that the inspection brought along and will bring measurable changes both for branch participants and for the national governing authorities. This observation is true mainly for the market analyzing system, however the other motions were not unimportant corrections either. The motions last year aimed the intention to make interior market more uniform and at the same time those tried to get the consequences of technological development, convergence regulation too, taking into consideration the needs of market participants. The application of motions in practice assists more intensive and more uniform governance in some fields, while in other places deregulation is assisted, which is at the same time a new step forward the achievement of the more uniform European information market.

Bibliography:

[1] Boytha Györgyné – Hargita Árpád – Sárai József – Tóth Tihamér (szerk.): Versenyjogi esetek – Az Európai Bíróság gyakorlata, ISSN 1218-9855, Osiris Kiadó, Budapest, 2000.

[2] Forgács Imre (szerk.): Gazdasági szektorok és jogharmonizáció, ISSN 1218-9588, Osiris Kiadó, Budapest, 2000.

[3] Dr. Gál Gábor: Az európai elektronikus hírközlési keretszabályozás rendszerének felülvizsgálata, különös tekintettel a hírközlési piacelemzés rendszerének reformjára, Infokommunikáció és jog III. évf. 15. szám, ISSN 1786-0776, 158-164. oldal, Budapest, 2006.

[4] Pasa, Barbara – Benacchio, Gian Antonio: The harmonization of civil and commercial law in Europe, ISSN 1786-1438, CEU Press, Budapest, 2005.

[5] Dr. Várnay Ernő – Dr. Papp Mónika: Az Európai Unió joga, ISBN 963-224-746-9, KJK-KERSZÖV Jogi és Üzleti Kiadó, Budapest, 2005.

CZAP László, ZÖMBIK László

ADAPTÍV, ELOSZTOTT DÖNTÉSHOZÁS KÜSZÖBKRIPTOGRÁFIÁVAL

Czap László[*], *Zömbik László*[*#]

[*]BME-TMIT, [#] Ericsson Hungary

Az elosztott biztonsági döntéshozó rendszerek esetében már nem az elosztott kommunikáció, hanem annak biztonsága a lényegi kérdés. A leggyakrabban alkalmazott módszer küszöbkriptográfián alapul. Munkánk során, olyan dinamikus döntéshozó rendszert terveztünk, mely kompromittálódott vagy hibás komponenseket képes kiszűrni.

Bevezetés

Ha egy döntés megszületéséhez több, egymástól távol elhelyezkedő résztvevőt kell bevonnunk a folyamatba, a döntéshozás mechanizmusa ugyancsak komplexszé válhat.

Ilyen döntéshozás lehet például harctéri környezetben több megfigyelőpontból az ellenséges csapatok helyzetének meghatározása, vagy azonos rangú, csapatok stratégiai vagy taktikai lépéseinek összehangolása.

Ezekben a helyzetekben ráadásul kritikus kérdés, hogy a döntéshozás biztonságosan történjen egy nem megbízható környezet dacára. Az elosztott környezet miatt komplex feladat flexibilis, de biztonságos kommunikációs csatornák kiépítésére, ezzel szemben jogos igény, hogy az ellenség se ne hallgathassa le, se ne szólhasson bele döntéseinkbe, még akkor sem, ha a hálózat bizonyos részei az ellenség kezébe kerülnek. A vázolt probléma megoldásához a küszöb kriptográfia eszköztárát hívjuk segítségül. Bemutatjuk, hogy hogyan lehet biztonságos, több résztvevős döntéshozó rendszert létrehozni. Egy ilyen rendszer a küszöbnek megfelelő *k* megbízhatatlan résztvevőt képes tolerálni. Úgy szeretnénk fokozni a biztonságot, hogy adaptívvá tesszük a rendszert oly módon, hogy a kompromittálódott résztvevők kizárásával hozunk létre egy új struktúrát. Megmutatjuk az adaptivitás lehetőségét, és megvizsgáljuk az adaptív rendszer biztonságát.

Küszöb kriptográfia

A küszöb kriptográfia alapötlete, hogy egy szervezet privát kulcsát osszuk részkulcsokra, és ezeket a részkulcsokat adjuk a résztvevőknek. A részkulcsok önmagukban nem elegendőek egy művelet végrehajtásához, de *k* együttműködő már képes végrehajtani egy kriptográfiai műveletet a privát

kulccsal. Egy *n* résztvevős rendszer esetén ez azt jelenti, hogy egy támadó akár *k-1* részkulcsot is megszerezhet, nem képes használni a kulcsot, illetve *n-k* meghibásodott csomópont esetén is működőképes még a szolgáltatás. Ha pedig a kriptográfiai művelet egy döntéshozást jelent, akkor biztosak lehetünk abban, hogy ez a döntés legalább *k* entitás egyetértésével született. Ily módon hiba- és támadástűrő rendszerek állíthatók fel.

Elsőként Shamir dolgozott ki matematikai eljárást tikok szétosztására [1]. A módszer alapja, hogy egy *k-1* fokú polinom tetszőleges pontjának meghatározásához a polinom *k* pontja elégséges. Például ha ismert egy másodfokú polinom három pontja *(x,y): {(1,4),(-1,0),(2,9)}*, akkor ebből meghatározható az *x=0* helyen a függvény értéke, hiszen ez a három pont meghatározza a $y=x^2+2x+1$ egyenletet.

Lássuk a módszer matematikai hátterét részletesebben.

Tekintsünk egy *k-1* fokú *f* polinomot valamely test felett. A titkos kulcs ennek egy tetszőleges *x* helyen felvett értéke. A továbbiakban *x=0*, azaz *K=f(0)*. Ekkor az *i.* résztvevő részkulcsa legyen $K_i=f(i)$, vagyis a polinom *i*-ben felvett értéke. Mivel a polinom *k-1* fokú, *k* pontja meghatározza, így *k* ismert K_i érték esetén ismert *f(0)=K* is, azaz a szétosztott titok rekonstruálható. A rekonstrukció Lagrange interpolációval történik. Legyen adott a részkulcsok halmaza, *B*. $|B| = k$. Ismert, hogy melyik részkulcs melyik résztvevőé, azaz adott egy π_B: B → {1,2,…,n} függvény. Ekkor

$$f(x) = \sum_{i \in B} K_{\pi_B(i)} \prod_{j \in B, j \neq i} \frac{x - x_{\pi_{B(j)}}}{x_{\pi_{B(i)}} - x_{\pi B(j)}}$$

Egy ilyen művelet végrehajtásához, mint látjuk rendelkezésre kell állnia kellő számú részkulcsnak. Ha tehát valamely tag használni szeretné a kulcsot, a többiek részkulcsát is meg kellene tudnia. Így egy privát kulcs csak egyszer lehetne használható, mivel nem lenne többé titkos használója előtt. Ezt azonban a homomorfizmus fogalma segítségével kiküszöbölhetjük [2].

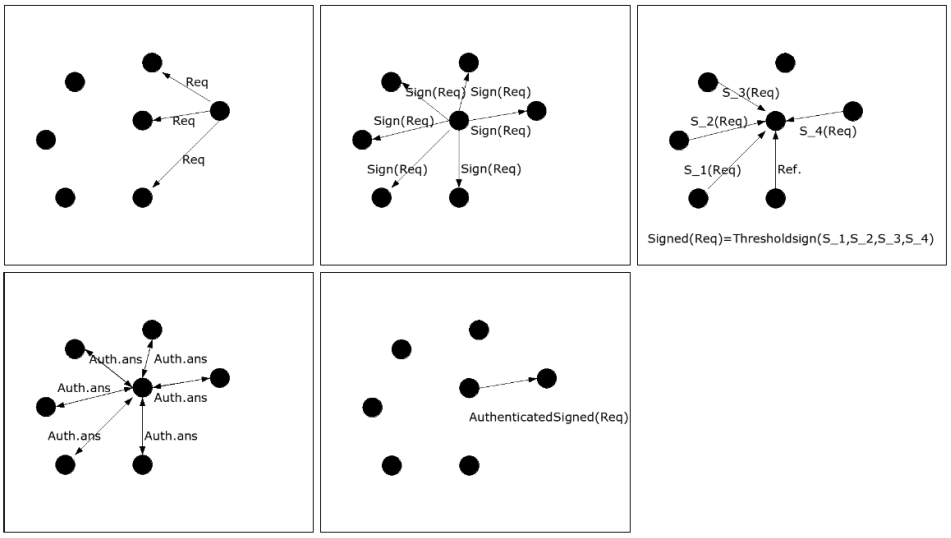
Homomorf kriptográfiai rendszerekre igaz, hogy ha egy *g* műveletet az *input* bemeneten a *k* kulccsal végezve $g_{input}(k)$ jelöl, akkor $g_{input}(k_1+k_2)=g_{input}(k_1)g_{input}(k_2)$. Könnyen ellenőrizhető, hogy pl. az RSA és ElGamal rendszerek is homomorfak. Ez a tulajdonság teszi lehetővé, hogy a részkulcsok felfedése nélkül lehessen használni a titkos kulcsot úgy, hogy minden résztvevő végrehajtja a műveletet a saját részkulcsával, majd ezeket a részeredményeket egyszerűen összeszorozva kapjuk meg az eredményt. A részeredmények ugyanúgy semmit nem árulnak el a részkulcsokról, mint ahogy klasszikus kriptográfiánál egy titkosított adat nem árul el semmit a titkosító kulcsról (lévén, matematikailag sem különbözik a művelet).

Elosztott, biztonságos döntéshozás

Egy több résztvevős, elosztott döntéshozó rendszert kapunk, ha *n* entitás között a bemutatott módszerrel szétosztjuk egy szolgáltatás privát kulcsát, majd ezt a titkos kulcsot digitális aláírás létrehozására használjuk. Az aláírás megszületése jelenti a döntés meghozatalát. A döntés csak úgy jöhet létre, ha azzal legalább *k* tag egyetértett.

Tehát, ha például az egymástól földrajzilag távol elhelyezkedő tábornokok közös döntést szeretnének hozni, a felhasználva a szolgáltatás szétosztott rész-privát kulcsait, saját döntésüket digitális aláírással hitelesítve aláírják, majd elküldik. A döntéseket bárki összesítheti és abból egy közös többségi döntést készíthet. Ez a többségi döntés is hitelesített, mégpedig a szolgáltatás privát kulcsával (mely egyébként nem áll rendelkezésre egyik tábornok számára sem).

Ez egyfajta szavazásnak is tekinthető: az egyes résztvevők megkapnak egy kérést, amelyet elbírálnak, és vagy egyetértenek és aláírják azt, vagy elutasítják. Kellő számú egyetértő résztvevő esetén a döntés megszületik.



A protokollfutam lépései: a) kérés elküldése b) kérés szétosztása c) aláírt válaszok d)rendszer aláírása és eredmény szétterjesztése e)válasz küldése a kezdeményezőnek

Megvalósításban munkánk kiindulópontja a CODEX (COrnell Data Exchange) [4], amely egy küszöb kriptográfián alapuló elosztott működésű rendszer, amely titkokat tárol kliensei számára. Ezt a rendszert bővítettük az általunk kidolgozott *sign* protokollal. A protokollunk pozitív válasz ese-

tén garantálja n-ből k résztvevő egyetértését, így $k-1$ megtámadott csomópont tolerálását is. A protokoll főbb lépései:

1. A kliens elküldi kérését k szervernek. Mivel $k-1$ megtámadott csomópontot viselünk el, így legalább egy megbízható résztvevő megkapja a kérést.
2. A kérést eljuttatja a szerver az összes többi résztvevőnek, és várják a válaszokat.
3. A szerverek elbírálják a kérést, és választ küldenek, amely elfogadás esetén a saját részkulcsukkal létrehozott részaláírást is tartalmazza.
4. Ha k pozitív válasz összegyűlt, a részaláírásokból összeáll a rendszer aláírása.
5. A válaszüzenetet hitelesítés céljából szintén aláíratja a szerver a többiekkel, ha ezek a válaszok is megérkeztek, a kliensnek elküldi a választ, amely tartalmazza a rendszer aláírását a kérésre.

Vizsgáljuk meg a rendszer biztonságát. Egy támadó akkor sikeres, ha össze tud gyűjteni legalább k részkulcsot, mivel ezek segítségével rekonstruálni képes a szolgáltatás privát kulcsát, és ennek segítségével a rendszer nevében döntéseket hozhat.

Mivel $k-1$ hibás vagy megtámadott csomópontot tolerálni szeretnénk, legfeljebb $n-k+1$ szerver válaszára számíthatunk, hiszen a hibásaktól nem várhatjuk el, hogy válaszoljon. Ezen kívül azzal is számolnunk kell, hogy a megtámadott résztvevők szándékosan rossz választ adnak, vagyis összesen $(n-k+1)-(k-1) = n-2(k-1)$ válaszról lehetünk biztosak abban, hogy helyes. A protokoll sikeres lefutásának garantálásához tehát $n-2(k-1) \geq k$ mindenkor igaz kell, hogy legyen.

A CODEX proaktív küszöb kriptográfiát használ [3], ez azt jelenti, hogy a részkulcsokat időről-időre lecseréli, anélkül, hogy a szolgáltatás kulcsát meg kellene változtatni. Ez védelmet nyújt egy olyan támadó ellen, aki az idő előrehaladtával képes újabb és újabb részkulcsokat megfejteni. A támadónak így korlátozott ideje van csak a részkulcsok gyűjtésére, hiszen kulcsfrissítés után az addig összegyűjtöttek már nem használhatók. A proaktivitás nem véd azonban egy olyan támadó ellen, aki tartósan felügyelni tud csomópontokat, az elfoglalt szerver ugyanis szabályosan lefolytathatja a kulcsfrissítést. Ha idővel egyre több csomópont kompromittálódik, a támadó sikerrel járhat. Javaslatunk szerint a megoldást adaptivitás alkalmazása jelentheti.

Biztonság adaptivitással

A bemutatott rendszer fix (n,k) struktúrán működik, n csomóponttal, k küszöbbel. Úgy szeretnénk fokozni a biztonságot, hogy ha valamely cso-

mópontról kiderül, hogy a támadó felügyeli, akkor kizárjuk őt, létrehozunk nélküle egy új *(n',k')* struktúrát, így a későbbi döntésekbe már nem szólhat bele.

A CODEX az APSS (Asynchronous Proactive Secret Sharing) protokollt [5] alkalmazza a proaktivitás biztosítására. A kulcsfrissítés folyamata kihasználható a struktúraváltás lebonyolítására a protokoll kisebb változtatásával, ahogy már a szerző is utal rá [5-6].

A kizárás mechanizmusa az elosztott környezetben további kérdéseket vet fel. Ha a kompromittálódott csomópontokat szeretnénk kiszűrni, egyrészt fel kell azokat ismerni, másrészt a résztvevők egyetértésével dönteni kell a kizárásáról. Továbbra is meg kívánjuk tartani a rendszer támadástűrő tulajdonságát, vagyis *k* megtámadott szerver tolerálását. A kizárásról való döntés protokolljának tervezésénél tehát az alábbi két elvárást kell szem előtt tartanunk:

1. Legalább *k* résztvevő egyetértése legyen szükséges ahhoz, hogy egy kizárási döntés történhessen.
2. Legalább *k* résztvevő ugyanazt a döntést hozza.

Az általunk javasolt megoldás a fenti célokat is küszöb kriptográfia alkalmazásával éri el. Az egyes résztvevők hitelesített listákon tartják nyilván az egyes döntéshozatalok során gyanúsan viselkedett szervereket. Olyan kizárási stratégiákat vizsgáltunk, amelyek szerint akkor zárnak ki a többiek egy résztvevőt, ha az az utolsó *l* döntéshozásból *s* alkalommal gyanúsan viselkedett (a továbbiakban egy ilyen stratégiát *l%s* fog jelölni). Arra, hogy mi számít gyanús viselkedésnek számos megközelítés lehetséges az alkalmazástól függően. Az egyszerűség kedvéért azt feltételeztük, hogy a helyes viselkedés egy döntés támogatása, az elutasító hosztokat tekintjük gyanúsnak.

A *sign* protokoll kibővítésével kidolgoztunk a fenti követelményeket kielégítő protokollt a kizárásról való döntés meghozatalára, így lehetőség nyílik adaptív döntéshozó rendszer felállítására.

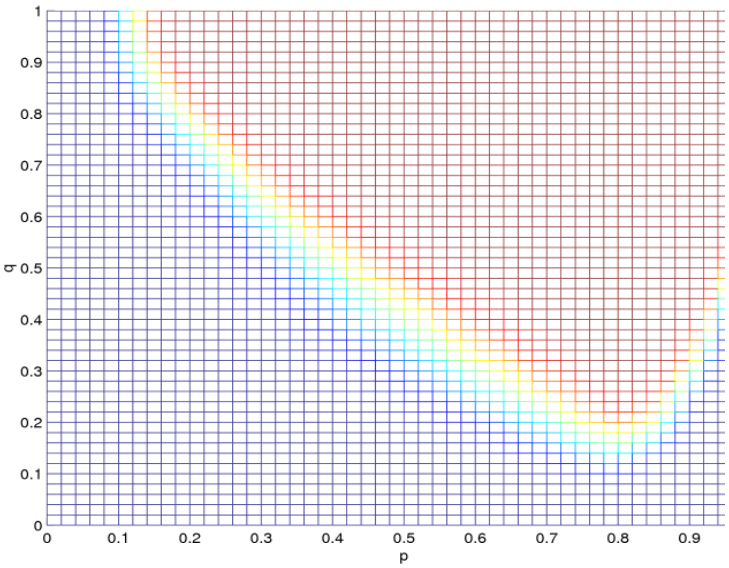
A kizárás kockázata

Az adaptivitás bevezetésének biztonsági kockázata is lehet. A CODEX aszinkron működéséből következően a $n \geq 3(k-1)+1$ összefüggésnek minden pillanatban teljesülnie kell. Vagyis, ha csökkentjük a résztvevők számát, *n*-t, akkor bizonyos esetekben kénytelenek vagyunk a küszöböt is csökkenteni. Ez biztonsági kockázatot jelent azokban az esetekben, amikor nem tudjuk garantálni, hogy csak ténylegesen megtámadott hosztokat zárjunk ki. Ha egy megbízható résztvevő nem 0 valószínűséggel gyanúsan viselkedik, akkor előfordulhat, hogy a többiek kizárják. Megbízható résztvevő kizárásával és a küszöb csökkentésével pedig megtörténhet, hogy a

megtámadott csomópontok száma eléri a küszöböt, így kitűzött célunkkal ellentétesen a támadó malmára hajtjuk a vizet.

Modelleztük az a helyzetet, amikor egy megbízható résztvevő *p* valószínűséggel gyanúsan viselkedik, egy megtámadott pedig *q* valószínűséggel helyes viselkedést színlel. A legkritikusabb helyzetet vizsgáltuk, amikor nemcsak $n \geq 3(k-1)+1$, hanem $3k \geq n$ is fennáll, továbbá $k-1$ hoszt már kezdetben kompromittált. Több *l%s* stratégiára vizsgáltuk a rendszer viselkedését.

Figyelembe kell vennünk, hogy a rendszerben többségben levő hibásan viselkedő, de megbízható résztvevők (*p* nagy értékei) mellett nagy valószínűséggel nem születik döntés, így gyanús hosztokat sem regisztrálhatunk. Ennek megfelelően annak valószínűsége, hogy egy megbízható résztvevő ténylegesen gyanússá válik:



1. ábra: Kompromittálódott szolgáltatások aránya p és q függvényében (a kék-piros szinek a 0-1 értékeket jelölik)

.

$$p \cdot \sum_{i=k}^{n-1} \sum_{j=0}^{i} \binom{n-k}{j} (1-p)^j p^{n-k-j} \binom{k-1}{i-j} q^{i-j} (1-q)^{k-1-(i-j)}$$

Hasonlóan határozható meg a kompromittált hosztokra is. Az *l%s* stratégia miatt a kizárás valószínűsége markovi modellből nyerhető. *p* és *q* értékeinek függvényében megvizsgáltuk a helyes illetve helytelen kizárási döntéseket. Azt láttuk, hogy *p* alacsony értékeinél egy megbízható csomó-

pont túlélési esélye nem függ q-tól, a kompromittált hoszt esélyei viszont egyaránt függnek p-től és q-tól. Ez azt jelenti, hogy ha p értékét kézben tartjuk, és alacsonyan tudjuk tartani, akkor a megtámadott csomópontokat még akkor is ki tudjuk szűrni, ha nagy valószínűséggel színlelnek helyes működést.

Nemcsak az egyes csomópontokra számítottuk ki a kizárás esélyét, hanem megvizsgáltuk a rendszer egészének viselkedését adaptív működés esetén. A vizsgálat során több mint ezer szimulációs kísérletet hajtottunk végre, különböző *l%s* stratégiákat vizsgálva.

Egy szimulált rendszer sorsának három kimenetele lehetett:

1. A rendszer működőképes maradt. Ez azt jelenti, hogy a támadók száma nem érte el a küszöböt, és a küszöböt nem kellett 1 alá csökkenteni.
2. A rendszer leállt. A sok kizárás miatt a küszöböt 1 alá kellett volna csökkenteni.
3. A rendszer kompromittálódott, vagyis a helytelen kizárási döntések nyomán a megtámadott csomópontok száma elérte a küszöböt.

A kompromittálódott szolgáltatások arányának tipikus karakterisztikája látható az ábrán. Ez a karakterisztika függetlennek bizonyult a kizárási stratégiától. Ez alapján elmondhatjuk, hogy ha $q<1-p$, akkor a támadó nem jár sikerrel. Ez a feltevés annyit jelent csupán, hogy egy megbízható résztvevő kevésbé gyanúsan viselkedik, mint egy megtámadott.

A kizárási stratégia megválasztásával tehát a másik két eset között kell egyensúlyt teremtenünk. Egy szigorú stratégia (amely kevesebb hibázást enged) gyorsabb kizárást eredményez, amely csökkenti a támadó esélyét arra, hogy ez idő alatt újabb csomópontot tudjon elfoglalni, viszont veszélyezteti a szolgáltatás rendelkezésre állását. Így ez egy óvatosabb, biztonságot szem előtt tartó hozzáállásnak tekinthető. Egy elnézőbb stratégia viszont nagyobb rendelkezésre állást biztosít, de hosszabb időkeretet ad a támadónak újabb hoszt elfoglalására. A konkrét alkalmazások más-más követelményeket támaszthatnak, ezek figyelembevételével kell a legmegfelelőbb stratégiát kiválasztanunk, a biztonság és a rendelkezésre állás közti optimális egyensúlyt megkeresve

Összegzés

Bemutattuk, hogy küszöb kriptográfia alkalmazásával hogyan lehet elosztott, biztonságos döntéshozó rendszert létrehozni. A CODEX-be épített új protokollal valósítható meg az elosztott döntéshozás.

A rendszer biztonságát kívánjuk fokozni annak adaptívvá tételével. Esetünkben ez azt jelenti, hogy a megtámadott csomópontok kizárásával új struktúrát hozunk létre, így a további döntésekből már kihagyva ezen résztvevőket. Maga a kizárásról való döntés is egy elosztott döntés, melyre kidolgoztunk egy olyan protokollt, amely képes *k-1* megtámadott csomópontot tolerálni.

A módszer hatékonyságát matematikai módszerekkel mutattuk meg. Megvizsgáltuk annak ez esetnek a kockázatát, amikor nem 0 valószínűséggel megbízható résztvevőket is kizárhatunk. Úgy találtuk, hogy a rendszer kompromittálásának esélye nem nő az adaptivitás bevezetésével, hanem a kizárási stratégia megválasztásával a biztonság és a rendelkezésre állás között kell kompromisszumot kötnünk.

Hivatkozások

[1] A. Shamir. How to share a secret, *Commun. ACM* 22:612-623, November, 1979.

[2] Y. Desmedt. Some recent research aspects of threshold cryptography. In E. Okamoto, G. Davida and M. Mambo, editors, *Information Security, Proceedings (Lecture Notes in Computer Science 1396)*, pp. 158-173. Springer-Verlag, 1997.

[3] Ostrovsky, R. and Yung, M. How to withstand mobile attacks. In Proceedings of the 10th ACM Symposium on Pronciples of Distributed Computing. 51-59. 1991.

[4] M.A. Marsh and F.B. Schneider. CODEX: A Robust and Secure Secret Distribution System. IEEE Trans. Dependable and Secure Computing, vol. 1, no. 1. 34-47. 2003.

[5] Zhou, L., Schneider, F. B., and Van Renesse, R. APSS: Proactive secret sharing in asynchronous systems. Technical Report TR 2002-1877, Computer Science Department (Oct.), Cornell University, Ithaca, New York, 2002.

[6] Desmedt, Y. and Jajodia, S. Redistributing secret shares to new access structures and its applications. Technical Report ISSE TR-97-01, George Mason University, July, 1997.

Erik PÁNDI, Balázs PÁNDI

STRUCTURAL CHANGES AMONG DOMESTIC CLOSED-PURPOSE NETWORKS

Erik PÁNDI – Balázs PÁNDI:[193]

Preamble: Closed-purpose networks have been supporting the everyday operation of public administration authorities for more than a half century. By the conversion of technological surroundings drastic changes were made in the organisational and technological solution of networks too, following the changes in the obligations of supplying organisations and the expectations of the users; furthermore taking into consideration of changes in the requirements. In the first decade of the 21st century for the realization of the „supplying state" model the question of electronic governance came to the fore, that has to be handled by Hungary and the Union member-states as first-rate priority. The present publication sums up the changes in the structure of domestic closed-purpose networks.

Key words: electronic information, closed-purpose networks, electronic government

1. Legal background of closed-purpose networks

Independent of functioning for several decades, the closed-purpose networks in the communication structure of Hungary have appeared for the first time – in *new legal concept ional quality* – in the Act No. LXXII of 1992 (Ttv.) on telecommunication.[194] The Ttv. Act therefore can be considered a milestone, as the systems operated and developed according to unique rules before, serving the single participants of state administration

[193] authors: LtC Erik PÁNDI Ph.D., Associate Professor at Zrínyi Miklós National Defence University (ZMDU), Balázs PÁNDI M.Sc., PhD-student at Communications Department of ZMDU

[194] Article 29 of the appendix of the Ttv.: „Telecommunication networks and installations serving exclusively governmental, national safety, public safety and protection interests – separated by function, which provide the fulfilment of special demands, the operation of closed organisations and technique. The application (operation) of them is not concerned telecommunication service."

have been "legalised" and adjusted to the domestic law and order. The Ttv. Act ensured for the government a facility to regulate basic issues of closed-purpose networks in decrees[195], which was only realized more than a half decade later in the Governmental decree No. 50/1998 (III.27.) on closed-purpose telecommunication networks (R.). The wording of the R decree had been modified twelve times within one decade[196], in this way the delayed publication and the unusual high number of alterations definitely show, that the entire telecommunication sphere was deeply changed. In my opinion these changes were based on three main trends– *mutually affecting each other*:

a) due to the changes in the political conditions of the country the economic structural changes, reforming economic sphere for market-economy conditions and then the liberalization of the information market. Headway of globalisation procedures;

b) intrusion of such technologies into the opening telecommunication market, that had been already used by the developed countries but banned before in the country. The appearance of technological convergence and its getting general-purpose;

c) the launching of activities for making the information society model accepted by the community, that became compulsory upon Hungary's joining the EU. In the new social model governance is present as – *among others* – the supplying state, the difficult way for reaching which is included – *on organisational side* – in re-forming public administration, – *on technical side* – in the realisation of electronic governance (public administration) in practice.

The alteration therefore was drastic, which is shown in the frequent changing of adjusting systems, as on statutory level three acts were announced within one decade:

a) Ttv.;
b) Act No. XL of 2001 on telecommunication (Htv.);
c) Act No. C of 2003 on Electronic Information (Eht.).

[195] Ttv. 2. § article (3).

[196] Last time on 1 January 2007, by the announcement of the Gov.decree 276/2006. (XII.23.)

The valid Eht Act brought in the definition of **electronic telecommunication**[197] into our law and order, as a significant segment of which closed-purpose network as a category still exists,[198] we can state therefore, that – *despite several legal and technological changes* – closed-purpose networks can be identified as a relevant segment of electronic telecommunication.

2. Changing of the structure

Upon reviewing the related articles of the valid R, with an effect from this year's 1st January the following state administration organisations are entitled to have (or to use) individual closed-purpose networks for serving their unique information transmission tasks due to national safety, jurisdictional, public safety, defence interests:

a) under the control of the Minister of Jurisdiction and Provost: the police force, border-guards, law enforcement and the offices having national scope of activities under the control of the disaster protection forces, furthermore the offices with national scope of activities under the governance of the Minister of Jurisdiction and Provost;

b) under the control of the Municipal and Regional Development Minister the disaster protection forces;

c) under the control of the Minister of Defence, as the network host, the Hungarian Army and the army national safety services;

d) under the control of the attorney general, as the network host: the Prosecution of the Hungarian Republic;

e) under the control of the minister leading Prime Minister's Office, as the network host:

ea) civil national safety services,

eb) organisations entitled (bound) to use the EDR /Integrated Digital Radio System,

ec) organisations entitled (bound) to use the EKG /Integrated Central Main Line Network,

ed) organisations entitled to use the Security Network as a sub-system of the EKG.

[197] Eht. 188.§ article 15.: „Electronic information activity: such activity, that serves the transferring of any sign, writing, picture, voice or other kind of communication through a communication network to one or more users, thus especially the provision of electronic information service supply, operation of electronic information network or equipment, distribution of end-installations and the related services."

[198] Eht. 1.§ article (2)

From this listing it can be observed, that **on the one hand**, the government has reorganised the structure of organisation having closed-purpose systems and the structure of network hosts too based on the Act No. LV of 2006 on the assignment of the ministries of the Hungarian Republic, according to the content of the issued government program.[199]**On the other hand,** the regulation mentions three network hosts, these are: the minister leading the Prime Minister's Office, the Minister of Defence and the Attorney general; two ministers (the Minister of Jurisdiction and Provost and the Municipal and Regional Development Minister) only have supervisory right in case of such state administration organisations, which have their own network, or can use such networks. As the rights and obligations of the hosts are fixed in the R.,[200] it is obvious, that the organisations under control (e.g.: Police, Border-guards, Disaster protection, etc.) and only use closed-purpose (sub)systems, they do not have the right to maintain and operate a system. **The third fact is** that the minister leading the Prime Minister's Office, as the network host has the most and widest range of closed-purpose networks under control.

3. Reasons-motivation

At first sight the list does not give adequate explanation for the **recent basic structural changes**, for giving an answer other processes shall be also known. Earlier evidences became of information value, if we review the version of R. valid on 31 May 2006 [201] (let us call it: R2.), that is according to the regulation for governmental, national safety, jurisdictional, public safety, defence reasons and for performing their unique information transferring tasks those can have individual closed-purpose network, or can use such networks. These are the following organisations:

a) under the control of the Minister of the Interior, as the network host: the police force, border-guards, disaster protection forces, furthermore the offices with national scope of activities under the governance of the Minister of the Interior;

b) under the control of the Minister without portfolio leading civil national safety services as the network host: civil national safety services;

c) under the control of the Minister of Defence as the network host: the Hungarian Army and the army national safety services;

[199] The governmental program aims the forming of such service-focused state, which instead of the slow, overdimensioned, bureaucratic and expensive public administration system implements a rational organisation, small in number, effective, having client focusing structure and operational mode.

[200] basically R. 3.§

[201] The situation before the present, second Gyurcsány-government

d) under the control of the Minster of Finance, as the network host: the customs- police and the Tax Authority;

e) under the control of the Minister of Justice, as the network host: law enforcement;

f) under the control of the attorney general, as the network host: the Prosecution of the Hungarian Republic;

g) under the control of the Minister leading the Prime Minister's Office, as the network host: the organisations entitled (bound) to use the EDR;

h) under the control of the Minister leading the Prime Minister's Office, as the network host: the organisations entitled (bound) to use EKG

When studying the statute the following facts can be observed: **on the one hand** the higher number of network hosts (six legal persons, as the points b) and g)-h) covered one minister at the time of the negotiation), **on the other hand** the fact, that most of the provost organisations could have individual closed-purpose network under the supervision of a network host, **and the third fact is** that the dominant part of the Minister leading the Prime Minister's Office cannot be observed yet in the controlling of closed-purpose networks.

For making this picture more shaded some more relevant data (information) shall be discovered, mentioned. First of all we have to lay down that by the middle of the decade in Hungary – *independent of those included in the regulation* – basically three significant closed-purpose networks were formed. It was the **EKG** (host: MeHVM), closed-purpose networks under the supervision of the Minister of Interior Affairs, as network host and the **Egységes Belügyi Digitális Hálózat** (EBDH) **United Interior Digital Network** as the common platform for these as a multifunctional transportation network, furthermore the **network of the Hungarian Army** (MHH) under the supervision of the Minister of Defence as the network host. This fact is supported by R2.[202] too indirectly, which declared that the main parts of the EBDH and the MHH that can be replace with the EKG shall not be ceased, in contrast to the other closed-purpose networks.

It is also considerable, that in 2003 before the final installation of the EKG, as a result of the unique position[203] of the Ministry of the Interior within public administration, and due to the technical abilities of the

[202] R2. 10/A.§ article (2)

[203] It was special in way, that mainly through the municipalities it had executed organisational and supervision rights in the wide territory of public administration, to which the security functions were also connected

EBDH, a theoretic agreement was reached concerning the co-operation between the EKG and EBDH, about which the governmental representative of the Prime Minister's Office and the public administration under-secretary of the Ministry of the Interior gave the following information to the public administration under-secretary of the Ministry of Finance: *„During the elaboration process a conclusion arose, that we could make a more expedient, economical solution for the entire government, if a more integrated connection is set up between the Integrated Central Main Line Network and the network remaining according to the governmental decree 50/1998. (III.27.) of the Ministry of the Interior on closed-purpose telecommunication networks."* [1]. For the wider support of the program such integrated schedule of tasks was fixed and approved in 2004 between MeH-BM-IHM, that includes the factual technical realisation phasing of connecting the EKG-EBDH and the public network-EBDH [2]. The integration of EKG and EBDH became reality by 1st of this January, as the Security Network[204] replacing the EBDH has become an integrated part of EKG, it is operated further as a sub-system of that.

We can state that in the "large family" of closed-purpose networks, the core was significantly relocated during last year, and the government starts to break down the traditions based on first of all the unwritten rules of operating and developing old structures, that is:

a) the number of network hosts is cut radically (to half);

b) for the practical setting up of electronic public services the controlling of the operation and development of modern technological networks is under the leadership of one host (the Minister leading the Prime Minister's Office);

c) several important state administration organisations having their own closed-purpose network before do not have the possibility to use any closed-purpose network either (e.g.: tax authority, customs and finance guards), or use is permitted them in case of the systems maintained by hosts in other organisations of the state administration structure (e.g.: Police, customs guards, disaster protection).

It is important to emphasize - from the aspect of being familiar with the topic- the earlier relevant ascertainment of Dr. Gábor TÖRÖK[205] saying,

[204] The Security network (RH) was mentioned by the Gov.decree No. 276/2006. (XII.23.) article 4 at first, however its exact definition is not included either in any legal act or the R. I can be observed indirectly, that the RH includes the entire former EBDH, the wire- and cordless network of the Police and the Border-guards, furthermore the radio system of them, that is the EDR

[205] Dr. Gábor TÖRÖK, university professor

that: *„…significant changes took place in the approach to telecommunication in the last decades. The progress started in the USA and was taken over by the European Union after some time. The earlier approach considered it obvious, that the company supplying telecommunication services in a country shall be partly state-owned, on the other hand it had monopolist position. First sign of changing this approach was the issue, that army and interior safety interests can be ensured without keeping state property right too, consequently privatisation became possible in this field."* [3]. The EDR was set up [206] and is being operated[207] pursuant to this conception – *it is also approved by the R.*[208] – , and the dark optical fibres forming the base structure of the EKG were also supplied[209] accordingly.

In the practice of maintaining and developing closed-purpose networks – *mainly by the MeHVM, as the network host* – outsourcing (OS) actions have become more intensive in the last five years, which progress is already a practice in Europe. Two main tendencies can be observed in the governmental OS market in Hungary. According to one of them the main purpose of outsourcing is the raising of efficiency[210] without radical changes in the organisational and operation processes. In this case short-term, smaller assignments for a well separated task form the subject.[211] The other approach intends to realize wide-range and clear governmental reforms and reorganisation by the long-term outsourcing of individual operational territories and activities. On this level of the OS activity opposite to the outsourcing of the information-technology structure and business solutions the practice of outsourcing activity-monitoring systems is more characteristic.[212] For this reason the suppliers usually struggle for an information-technology OS contract, in order to get BPO agreements later easily in the possession of an OS contract [4].

Recent structural changes – *that seem to be aggressive according to some opinions* – in the closed-purpose networks predict paradigm changes, by which a period full of interior professional-financial arguments between governmental participants seems to get to its end. This change however can

[206] The EDR was officially handed over on 28 February 2007, after a long and difficult period of time from the announcement of the first Gov.Decree 1074/2001. (VII.13.) ordering the setting up of the system

[207] Operation is executed by Pro.M Zrt. Under the interest of the T-group

[208] R. 3. § a) article

[209] Optical fibres are rented from the T-group of companies by Kopint-Datorg Zrt. supervised by the Prime Minister's Office

[210] Cutting costs and improving quality

[211] contracting out

[212] BPO: business process outsourcing

be the precursor of the development of a new quality, that is indicated as *„electronic governance (government)”*.

4. Summary

The existence of domestic closed-purpose networks is dominant in the progress of introducing and spreading electronic public administration services. Pursuant to the related legal regulations, nowadays closed-purpose networks form a part of the domestic electronic information infrastructure, as those through their technical features and the applied technology are proper for co-operation with the systems of market participants. In the last half decade such organisational, knowledge, technological and capital concentration compiled up in the field of public administration information-technology co-ordinated by the Prime Minister's Office, which made possible, that Hungary could partly fulfil the requirements of the Union and those controlling actions reached, that by the reorganisation of the organisational and governing structure of the closed-purpose systems serving unique branch interests before, a dominant core has to be formed for further development of electronic governance.

References:

[1] BM KÁT-MeH PÁT, Együttműködés tárgyában készült átirat, Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala irattár, Budapest, Iktatási szám: XIX-2044-1/2003., 1. oldal, 2003. július 16.

[2] IHM miniszter-MeH PÁT-BM KÁT, Feladatterv az Elektronikus Kormányzati Gerinchálózatnak (EKG), illetve a Közhálónak az Egységes Belügyi Hálózattal (EBH) történő összekapcsolására, Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala irattár, Budapest, Iktatási szám: 228-7/2004. ált. (63-386/1/2004.), 1-5. oldal, 2004. július 29.

[3] Dr. Török Gábor: Az új hírközlési törvény néhány polgárjogi problémája, Az információs társadalom és a jog átalakulása – Magyarország az ezredfordulón, Stratégiai kutatások a Magyar Tudományos Akadémián, Műhelytanulmányok, Magyar Tudományos Akadémia, Budapest, ISBN 963 508 377 7, 210. oldal, 2002.

[4] Erik Pándi: Outsourcing of communication service in the field of public administration, „Kommunikáció 2006.” nemzetközi szakmai tudományos konferencia, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, ISBN 978-963-7060-18-2, 280. oldal, 2006. október

Peter TAKÁCS

POSSIBLE WIRELESS NETWOKS ON THE BATTLEFIELD

Demands

The last 5-10 years made great demands against of the IT sector, especially referring to the high speed data access and mobile networking. This is the same situation in the Hungarian Defence Forces, too. By this time the military IT slowly set up a bone network for informatic needs in „peace" time, but almost nothing happened in the aspect of field networking. We don't have special equipment in order to supply the tactical, fighting forces on the battlefields in their hunger for information. Besides this lack the old tactical accessories such as radios, computers got obsolate. We need a complete network with up to date solutions.

New technologies shown up by the dozen in the civilian sector which ones could be appropriate to solve the problem, or we can wait for the results of the expensive explorations such as the researches of the DARPA. Anyway these achievements will not solve our problems but the researcher country's.

So we have to stick to the existing solutions, new wireless techniques such as bluetooth, wifi, wimax, etc. From these parts it is possible to build up a working mobile network, there are ready to use solutions out there, the only thing we have to do is to draw up our needs.

The other important trend must be kept in mind is the fusion of the communication and informatics which has almost finished. We are living in the age of IP telephony, voice and data are one and the same, travelling on the same wire.

Organisation structure

The technical solutions are not everything. They are „almost" nothing comparing them to the organizational questions. First we have to choose an operating unit size which could be the top size at the battlefield at a given time like brigade or battalion and we have to start planning the fieldnetwork downward from this level not forgetting out the connection to the bone network. In this paper I am not dealing with specific bandwidths and speeds, but at the examination of these topics bidirectional thinking is required, not just planning downwards.

This top level must have the ability to clamp and control the lower levels. What do i mean? For example this level must have to deploy the key

equipment such as the Network Management Systems, Authentication Systems, etc.

There must be a some kind of key management for this Authentication System and a central database for the access control which raises other organisational questions.

Since we are talking about military questions we have to think about casualties which requires duplications in the system adding new issues.

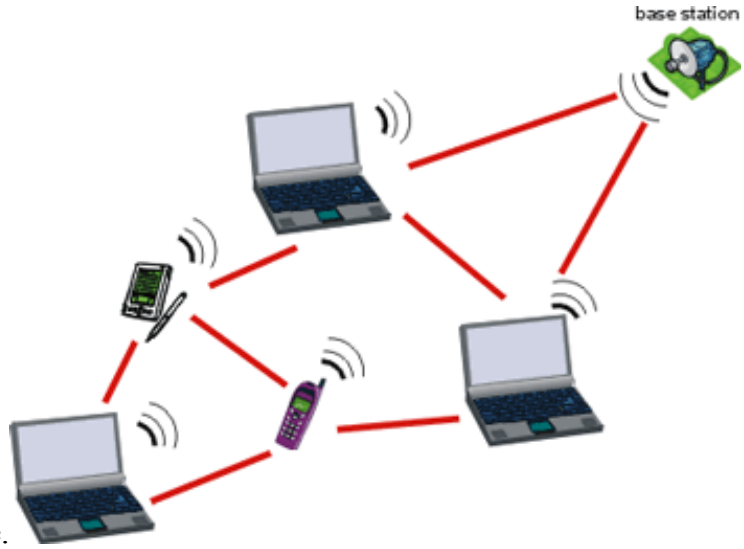
The other important question could be the possibility of cooperation between same levels. From a technical view this is an easy question but not from the organizational aspect.

The network must be modular and this is one of the most important question if we want a cost effectiveness and easily sustainable solution. What do i mean? Each organisation unit depending on it's on own functions requires differing information means for example the number of computers, VoIP devices or type of applications, equipment. This mean we need a homogenious network with same devices, protocols, etc. Following this way it is easy to add or take units, tracking monitoring the whole network

Mobility

The mobility is a key question in setting up a tactical battlefield network. The routing and the terrain could be one of the biggest problem in this section.

For a long time there was no good solution for these topics. Specialists were trying to set up mobile networks using wifi. This is the MASH networking. Ere now there is now pretty good solution in MESH networking for military



use.

Mesh networking

Source: http://www.ercim.org/publication/Ercim_News/enw57/santi.html

The wifi because of its nature is not appropriate for fighting down obstacles such as hills, elevations. Besides this the range of wifi is small.

The solution could be the WIMAX. This technology could be a bridge between wifi hotspots, this was designed to serve out moving object from a bigger distance, nominally up to 50 kms.

Mesh networks in military environment

Source: Mitre corp. The Edge newsletter (http://www.mitre.org)

Security

For long the security of wireless networks were nightmare. This has changed. In the past we had WEP and WPA supported wifi without any special authentication features. This could be hacked in a few hours.

Today we have robust authentication methods for wireless networks such as RADIUS server techniques. Switches controlled by Radius servers using centralised client-access databases could be a good solution for access control. By now excellent Intrusion Detection Systems has grown up. These could be used for monitoring network anomalies, intrusions. It could be important when a device getting to a third parity. These equipment must be identified and locked out from the network right at the start.

Not just an organizational question of the acquisition of the equipments but security. These equipments must be tested in the aspect of security, too. For example many wireless devices carrying security breaches in their drivers, etc.

Future

We are living in a rapidly changing world and we have to follow these changes. The tasks of the military forces has changed, too. They are not facing against of big stationary armies but fast and hard to catch teams. The time of positional warefare has expired.

In these new days we have to look forward and reorganise our structure such as our communication means using simple, secure and cheap solutions. These solutions are already out there in the civilian sector, we have to „just" find and reclothe them into a military form.

Bibliography

[1] http://www.darpa.mil
[2] http://www.knowledgebasednetworking.org
[3] http://en.wikipedia.org/wiki/Mesh_network
[4] http://www.darpa.mil/sto/solicitations/index.html
[5] http://mitre.org
[6] http://ercim.org

Attila BLEIER, Zoltán RAJNAI

OPTIMIZATION OF A TRANSMISSION NETWORK

Introduction

U.S. Defense Agency, D.A.R.P.A. has recently issued a tender called C.O.R.O.N.E.T , for it's next generation core network environment. The RFQ contains strict requirements for the transmissionation network , and will pave the way for the new technologies to be deployed in ten years timeframe in the U.S, and perhaps 12-15 years in Europe. The requirements are strict in terms of bandwidth, reliability, scalability and network quality of service providing capabilities. Building up such a network with today's technology would be extremely challenging, and is far and away from real world scenario, where technology, resources, and several other constraints limit the possibilities. Two well defined paths lead to such an advanced network –

1. good definition of backbone network requirements, and forward-looking architecture design,
2. leveraging present resources as long as it can be done.

The following paper will describe the second option how to leverage and design, based on a scientific basis, and will show the findings of a real-life optical transmission network audit and redesign project.

The paper discusses a transmission network optimization project, first in Chapter 2 generally describing one suggested way of handling a network optimization project in general. Chapter 3 focuses on the characteristics of a Transmission network optimization – as a subclass of network optimizations. Chapter 4 discusses certain mathematical background used for reaching practical results. Chapter 5 describes one practical example, and the results reached. The paper is organized in a way that it starts with a general overview, then goes into more details, and finally shows one practical example. In Chapter 6 we give a brief summary of the paper.

Phases of a network optimization project

A network optimization is a general term. The process itself can have a number of different meaning depending on the network environment, and the goal of project. Without going into details (because [1] is entirely dedicated to optimization of networks), a few cases will be listed up in order to show its complexity.

The term network itself can be different depending on its type: eg. it can be transportation network, a telecommunication network or network model of a phenomenon, or device. Each have its on characteristics, in this chapter we are focusing on telecommunication networks in general.

Telecommunication networks can also be very different depending on the technology being used. From Chapter 4 the paper will focus on a subclass of telecommunication networks, namely traffic demand optimization of transmission networks. In this Chapter, we are focusing on the common characteristics of Telecommunication network optimization.

Not only the term network, but the term optimization can mean a number of things,, depending on the goal of the optimization, and the optimization environment. Greenfield optimizations differ greatly from optimization of an existing network, and the parameter (eg. network parameter as link capacity, delay etc.) to be optimized greatly influence the end result and the methods to be used. Further in this chapter we will focus mainly on optimization of an existing network, and the main parameter to be optimized is link capacity.

To make the paper more understandable we would like to remark the following terminology related things: further in this paper I will use need or needs as customer requirements, and demands as traffic demands between two points.

A network optimization project contains several phases – either stated in the project specification, or contains these parts as logical steps of the optimization. These phases are common in most network optimization projects.

Phase I – Defining the requirements

In the first phase of a network optimization project we need to find out the following:

- what the objective of the project is
- what the required input information should be

These have to be stated as clearly as possible, as the goal is to build up a model based on the information we received.

So the first phase of a network optimization project is finding out what the current needs are. This can be done by making a survey of current and future needs.

The survey starts with an informal understanding of problem. So that it can work efficiently a workgroup (of team members) needs to be set up, and the following topics are to be discussed:

1. The purpose of the project – this has a huge impact on the whole process. This defines what to optimize the project for – eg. the aim of the project
2. Current and/or future needs : the discussion within the workgroup has to cover what the current needs are, the possible future needs as well as the important perspectives and characteristics of the demands
3. Introducing characteristics of the topology: this should cover what the main characteristics of the topology, eg. what sort of network and traffic type is being discussed (IP/Transmission Network/Circuit switched network/ATM/MPLS), and those characteristics that are the specific nature of the topology (Tree networks / rings/meshed networks)
4. Additional needs regarding QoS : Different traffic profiles need to be defined in this case in the network, and there specific QoS needs: this highly effects the classification
5. Protection mechanisms to be used: it has to be addressed clearly, what sort of protection mechanisms are to be used and for which traffic flows/demands should these protection mechanisms used

The result of this survey and discussions need to be put into a formal document – eg. Customer Requirements Document. Further in this document the required data from the customer need to be specified.

These are only the most important aspects that have to be covered in the first phases of the discussion. Besides these many other important questions can be discussed eg. characteristics of traffic types, special customer requests regarding nodes, traffic demands and so on.

After the defining the aim of the project, and clarifying the current requirements a snapshot of the network is needed. This can be achieved a number of ways – if there is an inventory management system available, the most obvious idea is to take a snapshot of the actual status of the inventory management system. This will form the basis of the next Phase. In case of a greenfield deployment, there is no current network – so there is nothing to take a snapshot of.

Phase II – Feasibility study

The main purpose of this Phase is to find out, whether it worth making a network optimization, or the network is in a state that efforts spent on optimization (and possible commission of the optimized network) will overweight the benefits. This is more of a business benefit which is worth tak-

ing a look at. This Phase might not be needed, in case there is a clear decision that the optimization is needed.

At the beginning phase the topology of the network should be clearly visible – with all its pros and cons. From the data acquired, after preprocessing probably it turns out that some optimization parameters are far from the optimum . This have a number of reasons, most important of which is that the demands are changing over a certain time period, and a solution being appropriate in a certain stage of network development, might seem awkward or improper in a latter stage.

Of course, these assumptions can not form the basis of feasibility study – a very rough search for optimization must be done in this Phase, in order to be in a position to clearly state how much benefit an optimization can bring to the network. The result of such a rough estimation can by no means be the optimal network structure – it is to be reached in the next Phase, but it must be good enough to be able to make an effort estimation / how much benefit can the optimization bring. We have to select some criteria, that will form the basis of our study –

a. it has to show approximately how far the network parameter to be optimized is from the optimum,
b. from this criteria we need to be able to estimate the efforts required to fulfill the optimization and rerouting phases – eg. the following phases.

Selection of such criteria is to be covered in Chapter 5.

Phase III Optimization

Using a scientific approach for finding an optimum is necessary, because the optimization problem is too complex once the network size has reached a certain limit (10xn nodes+), and the problem has further constraints. This problem will be described further in Methods for transmission network *optimization*. This is the main purpose of the Optimization phase.

The purpose of this Phase is to do the actual optimization, eg. to find a reconfiguration of the network close to an optimum, that is acceptable. The optimization itself is usually a very complex problem – depending on the network type and objective of the optimization it can be an NP – complete problem. The effectiveness of the network optimization highly depends on a number of factors – number of nodes, edges, and demands in the network, as well as the requirements. Before this Phase, a new snapshot of the network is needed – which will form the basis of the optimization, because there could be several changes since the previous snapshot in a real life

network.The reason for this step is that significant amount of time might have passed between the previous phase, and this phase.

Finding the optimum method for developing the optimum includes theoretical research, development of algorithms, testing, and actual running of the algorithm itself. Due to the long-lasting nature of finding, or developing a method for finding the optimum it is important to develop a method for the project that is repeatable.

It is important to note that – during the time of the actual optimization – the network itself is subject to change, so what actually will be optimized is a different network to what the network is at the end of the network. The change (whether it is change in topology or traffic demand, or any relevant network parameter)in most cases is not so significant, but it is important to note. If it is a factor to count with , therefore it is important that after the initial development of an optimum finding algorithm, using the optimum on a slightly modified traffic demand matrix should not take significant amount of time

At this Phase in order to be able to find the correct mathematical model for the optimization the following criteria should be met:

1. Topology of the network has to be available
2. Traffic demands must be available
3. Objective function must be selected

These are the preliminary requirements for finding a good mathematical representation of the network – that can form the basis of the optimization. The optimization model is also highly dependent on the purpose of the project, eg. in our understanding, what would be an optimal network(objective). Different models are being used for topology optimization or traffic demand optimization, or any other optimization problem. The different models are well described eg. in [1].

The mathematical model used for such an optimization will be discussed in *Methods for transmission network optimization*..

Phase IV Commissioning the changes

The whole purpose of network optimization is to reach an optimum state of network parameter(s) but a very important aspect should not be forgotten. After the network optimization there will be an optimal network available – on paper, or on computer, but not in the real network. Depending on the complexity and amount of work of commissioning the changes in the network, commissioning work itself could be a very important part of a Network optimization project. In certain cases, the amount of commissioning work, after doing a optimization of the network, will be so much that

1. Will never be done (in case Phase II is done well, this should not happen because in Phase II a good estimation is given for optimum, and the efforts)
2. must be done automatically somehow because the manual commissioning is such a tedious work – and manually could take too much time and effort.

Phase V – Conclusions

After the optimization is done, a very important Phase has to be done: the result must be evaluated. Questions to be answered are: is the result is according to what was expected. Should the process be made a regular process, if so how often is to be repeated. What conditions should occur to do a network optimization project once more (if not done regularly).

Transmission network traffic optimization

Transmission network optimization is subclass of network optimizations. The general phases of such a project have been covered in the previous chapter. In this chapter, the specific characteristics of a traffic demands optimization are covered.

Transmission network providers often reach a state of the network after few years of service, when they figure out that the current state of the network – due to the network evolution over the years – is far from being the optimum. Network owners are sometimes aware of this fact but they do not know, how much effort would be required to rearrange the network.

Characteristics of the transmission network optimization project

As the title implies, the current section deals with the *optimization* of existing network link capacities. This is an important characteristic of the problem because it means that there are *capacity constraints* on the network, imposed by current network resources (more on this in Methods for transmission network optimization), which must be taken into account in the mathematical model. This is one important characteristic of such a problem.

The second important characteristic of the project is that the optimization is a link capacity optimization task. Demands are given as certain traffic between the nodes, and the optimum routing is to be found in the network, given there are certain link capacities as constraints. The link capacities are modular.

Third important characteristic is that this is a *transmission network* with its network topology and all the characteristics for protection and quality characteristics. It is important, that protection and quality requirements must be discussed. (Only one aspect of quality, demand availability is understood in this case), in certain cases like the one discussed in this paper, it is subject to optimization as well.

In short:

- modular link capacities are constraints in the optimization problem
- optimum routing is to be found for the traffic demands
- characteristics of the transmission network are to be taken into account

Availability and protection as a subject to optimization

Protection and availability is an inherent nature of transmission networks. Transmission network designers, and engineers in many cases think that all traffic should be protected. This is very good, from the availability perspective – it provides the well known 99,999% availability for the path.

This might be very good from the technical perspective – on the other hand path protection is an overkill, from the network capacity perspective, whether this is economically viable is up to the service provider to decide. A huge amount of network capacity can be saved by rethinking the current strategy for protecting certain traffic. Eg. it is a viable alternative, to lose some traffic in case of node or link outage from the business perspective, if on the other hand we save a lot of link capacity. Of course this highly depends on customer requirements.

The questions is now what is the acceptable availability (as a measure of demand quality), and how it should be decided what to protect, and what shouldn't.

In order to be able to decide we need to classify the traffic. A certain suggestion will be discussed here, how to do this classification. By no means this is the only possible way of classifying, this is one method, that can be used. In this case, we are considering a multi service provider, that provide voice, and data services, and the majority of the revenue comes from a voice traffic.

We have considered 3 different traffic types for classification:

a. Signalling traffic, signaling does not require too much bandwidth in a typical network however it carries very important traffic. It is a very risky not to protect signalling traffic - with very few business benefits. Signalling traffic should be protected.
b. Voice traffic: This brings most of the revenues for most service providers, however this requires most of the traffic also. A clear decision must be made how much, and what sort of traffic should be protected (Voice Switches are usually configured in load balancing fashion, eg. only part of the traffic is lost, at a single link.). Of course the characteristics of the core voice network need to be taken into account The traffic is to be classified how important it is

c. Data traffic: Data services at the concerning service provider are anyhow only 99,9% availability services. Because of the lower availability requirement in most cases they should not be protected.

Once made that decision, the traffic is to be arranged accordingly.

Methods for transmission network optimization

Optimization problems are in general LP/MIP problems. A short introduction to LP in general is discussed in 5.1.. In general Transmission network optimization problems are Mixed-Integer Problems (MIP). (See [i]). Because of this fact they are NP-Complete , which results in the following : solution time increases exponentially with the number of nodes.

It is important to highlight this – and its effect on a real example is to be discussed further in *One practical example*

Linear Programming (LP), Mixed Integer Programming(MIP)

LP, IP , MIP problems are the subject of Operation research theory, and they formulate problems that needed to be optimized within certain boundaries. According to, can be formulated as follows:

LP Problem

indices

j = 1, 2, ..., n variables

i = 1, 2, ...,m constraints

constants

a_{ij} coefficient for variable j in constraint i

b_i right-hand side of constraint i

c_j cost coefficient of variable j

variables

x_j j-th variable

objective

$$\min z = \sum_j c_j x_j$$

constraints:

$$\sum_j a_{ij} x_j \leq b_i$$

i= 1, 2, ..., *m*.

In ordanary words it can be formulated so: we have a vector of variables (x_j), which is with certain weight values (a_{ij}) is bounded by another vector (b_i). These inequalities are the **constraints**. The goal of the problem is to find a feasible variable vector x (eg. an x that fulfills all inequalities), that is

optimal. The criterium for optimality is to minimize (or to maximize) a certain function called **objective** function.

If all x_j are real numbers then it is a *linear problem*.

If some x_k of x_j can only be integers, then it is a *Mixed Integer Problem (MIP)*. If all x_j can only be integers then it is *Integer Problem (IP)*.

Models for transmission network optimization

Three design problems have been taken into consideration, the mixed integer problem (Modular Flow Allocation) uncapacited problems and capacited problems. (See 1 pp. 106-115). These problems are discussed in the following section.

Mixed integer Problem Modular Flow Allocation

"The requirement of integral flow arises naturally when we wish to allocate demand volumes in certain demand modules. For example, in transmission networks, demand volume is usually given in terms of modular units such as the number of Optical careers OC-3s needed between two nodes." (See 1 pp. 123-125)

Its mathematical model is as follows.

MIP: A/MFA

Modular Flow Allocation

constants:

δ_{edp} = 1 if link e belons to path p realizing demand d; 0 otherwise

L_d = demand module for demand d

H_d = volume of demand d expressed as the number of demand modules

h_d = demand volume ($h_d = L_d H_d$)

c_e = capacity of link e

variables:

x_{dp}= flow allocated to path p of demand d (continuous non-negative)

u_{dp}= non-negative integral variable associated with variable x_{dp}

constraints:

$x_{dp}=L_d*u_{dp}$, d = 1,2,…, D ; p=1,2,… P_d.

$$\sum_p x_{dp} = h_d \quad \text{d = 1,2,…, D}$$

$$\sum_d \sum_p \delta_{edp} x_{dp} \le c_e \quad \text{e=1,2,…, E}$$

Please note that there is no objective function selected for the MIP problem. At this stage this is purposely done so, this will be discussed in Section *Objective function.* In the following 2 sections we have covered two

simplification of this problem – in order to get through the NP – Completeness barrier, which significantly limit the number of nodes.

Uncapacited problem – LP – Simple Design Problem

The goal of the uncapacited problem, is to find an optimal solution to the transmission network optimization problem, without the link capacity constraints fixed.

The formulation of the uncapacited simple design problem was the following, that we considered. The mathematical formulation will be as follows (See 1 pp 108-110):

LP:D/SDP : Simple Design Problem

indices

d=1,2, … D demands

e=1,2,… E edges /arcs/links

v=1,2,...V nodes, vertices

constants:

a_{ev} = 1 if link e originates at node v; 0 otherwise

b_{ev} = 1 if link e terminates at node v; 0 otherwise

s_d = source node of demand d

t_d = sink node of demand d

h_d = volume of demand d

ξ_e = unit cost of link e

variables:

x_{ed} = flow realizing demand d allocated to link e (continuous non-negative)

y_e = capacity of link e (continuous non-negative)

objective:

minimize $F = \sum_e \xi_e y_e$

constraints:

$$\sum_e a_{ev} x_{ed} - \sum_e b_{ev} x_{ed} =$$

= a. h_d = if v= s_d

b. 0 if v<> s_d , t_d v=1,2…V d=1,2…D

c. -h_d = if v= t_d

$$\sum_d x_{ed} \leq y_e \quad \text{e=1,2,….,E}$$

Please note that in this particular case there is an objective function. This is due to the fact that there is no capacity limit imposed on the links (or the capacity limits are also variables).

The capacited problem – LP- Pure Allocation Problem

The capacited problem, is basically the Linear variant of the MIP, without the modular nature of transmission network.

The formulation of the problem we considered for the transmission is the following:

LP:A/PAP: Pure Allocation Problem

constants:

δ_{edp} = 1 if link e belons to path p realizing demand d; 0 otherwise

h_d = volume of demand d

c_e = capacity of link e

variables:

x_{dp}= flow allocated to path p of demand d (continuous non-negative)

$$\sum_p x_{dp} = h_d \quad \text{d = 1,2,…, D}$$

$$\sum_d \sum_p \delta_{edp} x_{dp} \le c_e \quad \text{e=1,2,…, E}$$

Please note 2 things. 1, objective functions is not selected, and 2 the similarities, and the key differences with *Mixed integer Problem Modular Flow Allocation*

Objective function

So far we have not selected an objective function. The selection of an objective function in itself can be a challenging task. The literature referred to in this book, suggests an objective function:

minimize $F = \sum_d \sum_p \rho_{dp} x_{dp}$

where $\rho_{dp} = \sum_e r_e \delta_{edp}$ is the unit revenue from path P_{dp} of demand d in terms of link revenue r_e.

However this is by far not the only objective function that can be used, but a well usuable one. So we will use a modification this (the sum of all number of hops of all demands).

Simplifying the network

As the number of nodes in the real life problem is close to … it is important to think over what sort of modifications of the network can be used. A few of these modifications are:

a. removal of non-sink and non-source nodes with exactly 2 edges. (These are the so called boosters or repeaters) or 2 degree nodes

b. aggregating of some sources and demands into a supernode aggregating sources and demands.

They have a drawback also : the interconnection traffic might not be correctly calculated between such nodes.

In our network a simplification of a different kind has been used:

the nodes at each site have been merged into a supernode (see figure)

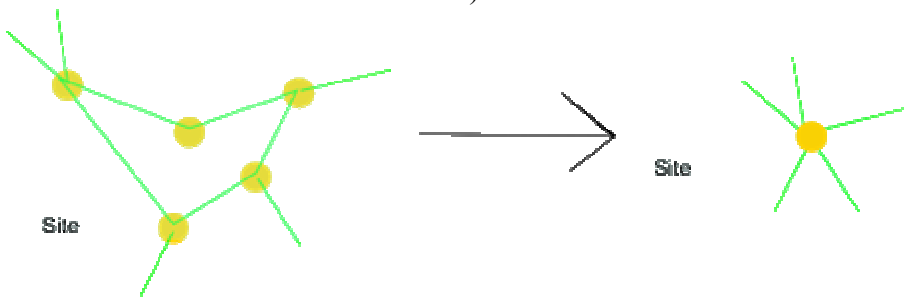


Figure 1

a. the trivial links have been removed (see figure)

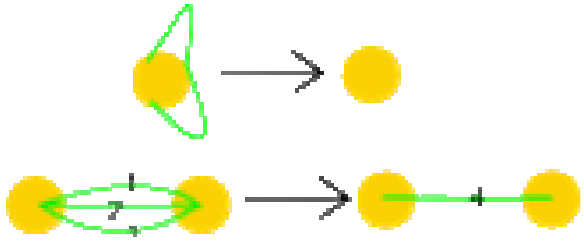


Figure 2

b. we substituted the n parallel links with one link with the sum of the original capacities (see figure)

One practical example

The following chapter deals with the practical results of an optimization project. Our goal in this chapter is to show that optimization techniques are beneficial to network operators. The measure that we are going to take into consideration is the comparison of the network to a optimum stage, where the link capacities (according to our objective function) are at a minimum level, while fulfilling the demand, and link capacity constraints.

The quality measure, that we used in the network to present the quality, is the average length of the paths – as they are somehow in connection with link capacities. This quality measure is a general unit for measurement, by no means the only possible measurement unit, however – as our figures will show, it gives an easy comparison for the results.

Introduction of the example network

The transmission network itself is divided into 4 optical rings(thick lines) and 6 microwave radio rings (thin lines), the access network consists of PDH trees (in which there are no chances for optimization – as there is always one path from the nodes to the boundary of the SDH transmission network).

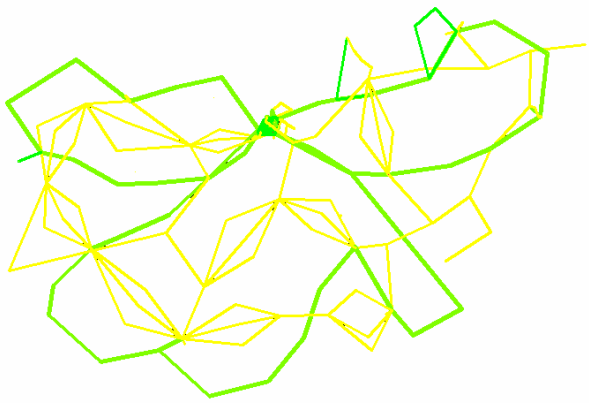


Figure 3

Initial results

We followed the process described in Phases of a network optimization project for reaching the practical results.

After finishing Phase I and II (referring to *Phases of a network optimization project* chapter here) we have figured out that because of the network evolution over time, the actual network is predicted to be far from optimal.

In Phase I, we created a statistics of the network with the current demands, showing the actual path lengths in terms of edge/link sections.

Eg. there were trails in the network that were using up too much capacities, and containing too many hops.

Such typical trails are depicted on the following figures:

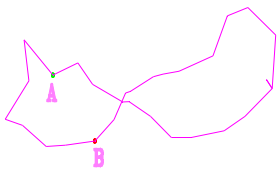


Figure 4

A trail from A to B is directly connected, however its protection trail travels through an extra ring (at the right-hand side).

Figure 5

A similar trail from A to B is directly connected, its protection trail goes trough ring in the left-hand side. An even more extreme example:

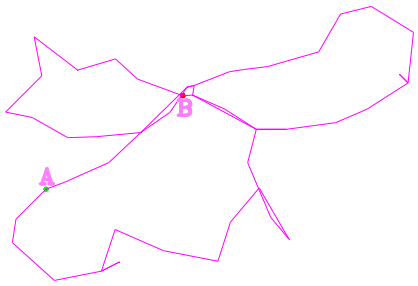


Figure 6

The trail from A to B travels through all the optical rings.

The other major discovery of Phase I was that the network is flat – eg. not divided into hierarchies. All traffic demands are handles as equal.

The two main characteristics we identified were:

- flat topology
- trail lengths are long

Feasibility study

In Phase II, we tried to do an estimation for optimum. For this we used a method of finding the shortest paths or trails for a certain traffic demand. We considered 4 cases for this:

1. Uncapacited links, shortest paths – in this case we considered unlimited capacities on the network links, and we used the method of shortest paths (Dijkstra algorithm, [2]) for finding the shortest paths for a demand
2. Capacited shortest paths – in this case we took the link capacities into consideration, and we still used the Dijkstra shortest path algorithm for a given demand
3. Protected demands, uncapacited links shortest paths. In this case we took protection of demands into consideration (eg, for the protection path for a demand we removed all the nodes and links of the active path except for the start and end node) (The protection and active paths were link and node disjoint).
4. Like in case 3 we took protection into consideration but this time with capacity constraint on the links

Our findings after Phase 2 is summarized in the following table:

	current situation	Uncapacited links	uncapacited with protection	capacited	capacited with protection
# of edges	%	%	%	%	%
1-10	85.26	98.16	98.16	97.28	95.53
1-5	***65.40***	***78.40***	***78.42***	***77.58***	***78.57***
6-10	***19.86***	***19.76***	***19.74***	***19.70***	***16.97***
11-20	11.14	1.84	1.84	2.72	4.45
21-30	1.26	0.00	0.00	0.00	0.02
>31	0.80	0.00	0.00	0.00	0.00
average:	**5.50**	**3.75**	**3.75**	**3.81**	**3.83**

Table 1

Taking into account that the methods used here do not provide in every case a global optimum, they provide only near-optimum situation state we an average of 30% saving is estimated in capacities after the actual Optimization.(Phase III).This is estimated from the figures that the average hop count went down from 5.5 to 3.83.

Optimization - Finding the global optimum

Simplifying the problem

The actual network to be optimized consists of 251 nodes, 399 edges/links, and 3874 2Mbit/s demands. In order to find a global optimum, the *Mixed integer Problem Modular Flow Allocation* should be solved. But due to the fact that the problem is a MIP problem, and therefore it is NP complete (See Linear Programming (LP), Mixed Integer Programming(MIP)). NP – completeness means in practice, that the number of nodes determine the solution time, and the solution time grows exponentally with the number of nodes.

Therefore this is far too big problem for a MIP problem solver, so the problem had to be simplified. The methods for simplification have been discussed in section Simplifying the network

After making the simplifications, the network dimensions have dramatically decreased:

- The number of simplified nodes went down to126
- The number of simplified edges went down to 173
- The number of simplified demands went down to 342

This is a much smaller problem in size, but unfortunately it still can not be solved if it is an MIP problem. Therefore we used a further simplification – in order to reach practical results on time.

As the problem still can not be solved if the Mixed integer Problem Modular Flow Allocation model is used, we need to consider an LP problem. This can easily result in a situation, that we haven't found the actual optimal solution of the original problem, but we are going to find a solution close enough to the optimum, which is acceptable.

Formulating of the LP problem

The formulation of the LP problem is not trivial. The mathematical definition of the problem is described in Section (The capacited problem – LP- Pure Allocation Problem). Formulation of the LP problem consists of the following steps:

- Formulating the constraints for the problem(demand and edge constraints)
- Formulating the objective function

After the formulation the problem can be solved with an LP Solver like "LP_Solve". Our purpose in the following part of the paper is to generate an example file, with constraints and an objective function which can be used as an input for LP_Solve.

So first the constraints must be defined, we start it by defining the so called demand constraints.

A *demand constraints* looks like this in its formulation:

D204375734425243631651958: +C91 +C92 +C93 +C94 +C95 +C96 +C97 +C98 +C99 +C100 = 62720; [6.4.2. a]

Dxxx, is an abbreviation for a certain demand. Each demand is uniquely generated from a summarized traffic demand with its source and destination (using topological information). Cxxx are variables, each variable represent a demand-path pair (each demand has a set of candidate paths). This is the so called link-path formulation[1].

A demand constraint represents that the actual traffic demand in bit/s from Node A to Node B, must be equal to its actual value, no matter which path we choose (eg. irrelevant of the actual value of the Cxxx variable). This is shown in the above example (the sum of the variables equals the total demand.)

An *edge constraint* looks like this in the LP problem definition:

E085250584720080700628900: +C433 +C542 +C543 +C1041 +C1252 +C1253 +C2172 +C2173 +C2631 +C2873 +C2874 +C3055 <= 186624; [6.4.2.b]

The Exxx denote the link or edge constraint, Cxxxx denote the path variables in the function. This constraint represents that the link flow must not be over the capacity of the link.

The selection of the *objective function* – or the goal to which we want to optimize is an important task. In this case we used the sum of the link flows as an objective function in order to minimize link flows – or to maximize link capacities.

Such a line looks like this in the LP formulation:

min +2 C1 +3 C2 +3 C3 +3 C4 +3 C5 +… +4 C8548 +4 C8549 +4 C8550 [6.4.2c]

The min shows that we are looking for the minimum of the function, and the sum of the link flow variables is the function to be optimized.

The LP formulation consists of therefore:

- demands constraints [6.4.2a]
- edge constraints [6.4.2b]
- objective function [6.4.2c]

The LP problem in an LP_Solve formulation consists of over 3000 lines and it includes over 8550 variables in a typical case(the number of the variables depends on the number of paths for each demand, and the number of demands).

The typical calculation time for such a problem on a Celeron M 800 Mhz, is 25 paths is approximately 1 minute.

The following table shows the actual calculation times in terms of the depth of the path finding, and the number of paths.

Description	**Runtime [sec]**	**Depth of Path finding**	**Number of Paths**	**Number of variables**
Path finding 1.	66.50	20	25	8550
Path finding 2.	71.50	20	10	3420
Path finding 3.	272.894	25	100	34200
LP solution time 1.	3.185	20	25	8550
LP solution time 2.	1.45	20	10	3420
LP solution time 3.	18.5	25	100	34200
Total time 1.	70.2	20	25	8550
Total time 2.	74.3	20	10	3420
Total time 3.	297.099	25	100	34200

Table 2

Results of the optimization

The optimization resulted in a set of paths for all demands that is the optimum of the LP problem, this we do not want to include here due to size limitations. Interestingly enough, in most cases the optimum path was the shortest possible path, this was due to the fact that there were enough free capacities in the network.

If there are enough free capacities in the network the shortest path algorithm gives a good estimate. However if the free capacities are getting less, there might be a situation where because of the lack of free capacities the shortest path calculated one by one (each path calculated independently, one after another) could result in situation in which the path calculated later, must be a long path (as the free capacities have been utilized) . In this case the overall paths might be longer than in a situation where the calculation for the paths is based on variables effecting the whole network.

Since there was enough free capacity in the network our first estimation in Phase II was close to the actual optimum.

It is important to cover in this Section as well the potential errors, that may have occurred:

- The LP problem formulation we covered so far, has not dealt with the problem of protection paths, but in practice we have to cover this problem as well. This is not discussed in this paper
- The optimum of the LP problem might not be the optimum of the original problem. For this, we need to find an estimate, how acceptable our solution is, and what percentage is it better than the original. If it is close to the optimum of the original problem, the LP solution is acceptable.
- Currently we are in this phase (3), and we have not yet reached rerouting, and final conclusion drawing – it might be that we are going to find some of the errors that we have made in a latter phase.

Based on the following assumptions we made several simulations with several cases changing the edge capacities. At 100 % capacities the results were exactly 3.75 as with Dijkstra. At 70 % capacities the results were approximately 3.8, slightly better than Dijkstra. At 50%, 40% capacities, there were no solution with Dijkstra, only with the LP calculation method.

To summarize the results optimum solution with 100% utilization is based on the Dijkstra algorithm.

Summary

Our intention with this paper was to give a systematic overview of network optimization, and to introduce some methods we have used in a live network.

In this paper we have covered:

- A systematic approach and project phases for a network optimization project in Chapter : *Phases of a network optimization project*
- Characteristics of a transmission network traffic optimization project in Chapter *Transmission network traffic optimization*
- Mathematical methods for transmission network traffic optimization in *Methods for transmission network optimization*
- Results based on this methodology in a live network in One practical example

In Chapter 5 we tried to show that using well built mathematical models for optimization results in an optimum network in terms of link capacity. This has brought up to 30% better utilization in the given network, which results in cost savings mostly in CAPEX, and with in case it is used well it can help network designers in finding free capacities in the network – which helps network designers when planning future extensions and investments.

In short, using this methodology a set of tools can be built up for the transmission network designers, that enable them to use their own network resources in a more efficient way. An even better performance can be achieved by applying automatic methods for rerouting.

List of acronyms

CAPEX – Capital Expenditure
D.A.R.P.A - Defense Advanced Research Projects Agency
C.O.R.O.N.E.T - Dynamic Multi-Terabit Core Optical Networks: Architecture, Protocols, Control and Management
RFQ – Request for Quotation
IP – Internet Protocol
ATM – Asynchronous Transfer Mode
MPLS – Multiprotocol Label Switching
QoS – Quality of Service
LP – Linear Programming
MIP – Mixed Integer Programming
NP - non-deterministic polynomial time
SDP – Simple Design problem
PDH - Plesychronous Digital Hierarchy
SDH – Synchronous Digital Hierarchy

Bibliography

[1] M. Pióro, D. Medhi: Routing Flow and Capacity Design in Communication Networks, Morgan and Kaufman, June 2004. [pp. 625-638]

[2] Pióro, Medhi: Routing Flow and Capacity Design in Communication Networks [pp. 153-154]

[3] Pióro, Medhi: Routing Flow and Capacity Design in Communication Networks [pp.114]

[4] Planning reliable UMTS terrestrial access networks :Szlovencsak, A. Godor, I. Harmatos, J. Cinkler, T. Ericsson Res.;Communications Magazine, IEEE, Jan 2002 Volume: 40, Issue: 1 [pp66-72]
Kommunikációs hálózatok költséghatékony tervezése a forgalomeloszlás periodikus változásainak figyelembevételével , Tamási Levente, Józsa Balázs Gábor, Orincsay Dániel, Híradástechnika 2004

[5] Stalled information based routing in multidomain multilayer networks
Szigeti, J. Tapolcai, J. Cinkler, T. Henk, T. Sallai, G. Telecommunications Network Strategy and Planning Symposium. NETWORKS 2004, 11th International pp[297- 302]
Kommunikációs hálózatok költséghatékony tervezése Orincsay Dániel és Józsa Balázs Gábor, Híradástechnika 2003

József MÁTÉ

STATUS OF IMPLEMENTATION OF THE MONITORING AND PUBLIC WARNING

(MoPuWa, in Hungarian MoLaRi) System to be installed in the areas of hazardous chemical plants under the SEVESO II Directive

Nowadays, when the entire world lives in the shadow of environmental pollution, natural and man-made disasters, together with biological and chemical terrorism, there is a high priority demand to set up a nationwide authority qualified for managing emergencies and disasters, acting, at the same time, as a coordinator and an executive body, capable of providing real-time information and being an instrument for the governmental decision-making process in the course of disaster management.

Ensuring security for the citizens of the Republic of Hungary, moreover the protection of the national economy and national heritage constitute tasks of high priority for each citizen and organization. The role and function of preventing disasters and the prompt elimination thereof has significantly enlarged. Public opinion is paying an increased attention to everyday actions of disaster management due to numerous disasters and emergencies occurring in the last years.

During the last decades, several chemical plant accidents occurred in the member states of European Community and investigations of the occurrence thereof purported flaws in the course of control procedures relating to industrial activities: [3]

1 1976, Seveso, Italy – dioxin[213]
2 1984, Bhopal - methyl-isocyanides[214]

[213] **1976, Seveso, Italy.** 10 July 1976, Northern Italy, due to an accident in the Hoffmann La Roche Givaudan chemical plant for fumigants in *Seveso* (a small village near Milan), air pollution of dioxin occurred. The poisoning caused by dioxin clouds led to the emergency slaughter of some 100,000 livestock. The accident did not claim human lives, however several hundreds of citizens needed to be evacuated.

[214] **1984, Bhopal, India**. At Union Carbide Corporation, a chemical plant producing fumigants and polyurethane, seriously toxic gases (methyl-isocyanides) were released from an underground reservoir. In a short time, approx. 400 thousand citizens suffered health impairment or poisoning. 3,135 casualties were reported.

In 2002, the Directive was aggravated due to the following cases:

1 2000, Baia Mare, Romania, cyanide[215]

2 2000, Enschede, Netherlands, pyrotechnical substances[216]

The demand for a stable command and control required the upgrade of the Directive. In 1982, according to the aforementioned, the European Commission elaborated Directive 82/501 (SEVESO I). Later, it was re-drafted due to industrial accidents occurring in the meantime and transformed into Directive 96/82/EC (SEVESO II), approved on 9 December 1996 [1].

1 Legal provisions providing reasons for the implementation of the system:

Directive 96/82/EC (SEVESO II) as an adaptation of the chapter on the environment protection of the EU, law harmonization was implemented in Chapter IV of Act 74 of 1999 on the Direction of the Protection against Disasters and the Protection against Major Accidents involving Hazardous Materials, furthermore by virtue of Government Decree 2/2001 (I. 17.) on the Protection against Major Accidents Involving Hazardous Materials. The domestic implementation of the SEVESO II Directive set out extremely consistent tasks for the three parties: the authority, the plant and the local government (citizens). The three parties should achieve the common objective, i.e. safety, through partnership.

The Directive refers to industrial, biological, agricultural, chemical accidents, which, in case of an uncontrolled situation, may jeopardize and impair human health, the environment, the safety of life and property. Hazardous plants coming under the Directive are bound to identify the hazardous activities and risks of accidents, carry out risk analysis, develop security and control system, perform assessment of impacts relating to major

[215] **2000,** Cyanide pollution on the Tisza River (Eastern Hungary). **Baia Mare, Romania:** 30 January 2000, the jerrybuilt embankment of a cyanide reservoir of Aurul Mining Co., due to the high water pressure, breached in the length of 25 m. At least 100 thousand cubic meters of highly toxic wastewater were released, which contained 120 tons of cyanide, equivalent to the deadly dose for approx. two million people. The poison flow streamed down the whole inland passage of Tisza River, not sparing the Novi Sad region, nor the Danube and the Black Sea.

[216] **2000, Enschede (the Netherlands):** In May 2000, a warehouse of pyrotechnical materials exploded in the outskirts of city of Enschede, where approx. 100 tons of pyrotechnical materials were stored behind the Mayor's Office and close to the citizens. 21 persons were killed and some. 1,000 were injured. The explosion destroyed all buildings in a circle of 400 m.

accidents, determine the so-called domino effect and develop internal protection plans217 . [2]

The authority and the local government develop external protection plans218 for preventing effects outside the plant and responding to them, indicating, in the plan of settlement, the hazardous zones and border-lines of individual and social risks as well, furthermore providing conditions for a public information, warning and alerting system, guaranteeing personnel and equipment, designated by external protection plans, needed in the course of detection, intervention, life-saving, decontamination and recovery. [2]

The continuous supply of data on these cases is required. The transfer of this information is mandatory to the European Commission through a software provided. The objective of the Convention on the Transboundary Effects of Industrial Accidents (also called the Helsinki Convention), released by UN ECE, to prevent cross-border effects of serious accidents occurred, provide assistance and inform immediately in the framework of international cooperation. [1]

Both provisions of law, the SEVESO II Directive and the Helsinki Convention came into effect simultaneously in Hungary on 1 January 2002.

According to the Agreement, the National Center for Prevention of Industrial Accidents has been designated to the National Directorate General for Disaster Management (NDGDM). The parties concerned ensure the exchange of information, notification and assistance.

Act 37 of 1996 on Civil Protection (hereinafter: Act on CP), together with Chapter IV of Act 74 of 1999 on Disaster Management (hereinafter: Act on DM), furthermore current Government Decisions and Decrees (e.g. 18/2006 (I. 26.) on the protection against major accidents involving hazardous materials) stipulate the scope of duties and functions. All these objectives and disaster management endowed with expectations relating to authoritative and special authoritative functions challenged NDGDM and its regional/territorial organs.

---

[217] **Internal protection plan:** The plant management elaborates an internal protection plan for responding to hazards revealed. In the course of elaboration through a systematic analysis, it reveals the tasks relating to the protection against major accidents, indicating conditions, personnel and equipment. ***Handbook on Industrial Safety*** -2003- ISBN 963 224 716 7 – p. 106.

[218] **External protection plan:** … summarizes the extent of danger and determines tasks and requirements for the protection of citizens, resources, the built and natural environment, furthermore certifies that the operation, equipment, training of a settlement's protection bodies are appropriate for carrying out the planned protection tasks, even relating to the infrastructure to be involved in addition, as well. ***Handbook on Industrial Safety*** - 2003- ISBN 963 224 716 7 – p. 313.

Section 14 of the Act on DM stipulates the integration and running of telecommunication and IT systems designated for disaster management. Section 5 (e) declares that the formation of the information system of disaster management shall constitute a Government task.

Government Decree 179/1999. (XII. 10.) disposes of the enforcement of the Act on DM and at the same time stipulates the composition and objectives of Governmental Coordination Commission (hereinafter GCC). Government Decision 2266/2000. (XI. 7.) disposes of the organization and operation of GCC, together with the adoption of rules of procedure.

Section 8 (f) of Government Decree 179/1999 stipulates that GCC shall develop a plan on the formation, operation and development of the telecommunication and information system of disaster management.

2 Structure of the system to be implemented: [4] [5]

The data collection and control transfer tracks are secure and are duplicated through highly secured networks. The power supply needed for the operation is ensured by the recourse of the national power supply network and alternative source of power, respectively.

The supervision of the status of the monitoring and warning and information systems and alarming are a real-time and a continuous operation.

A very important requirement in the course of configuring the endpoints is that the integration of supplementary and supporting services into the system should be performed without critical alterations (the installation of web cameras, written announcement, etc.).

2.1 The implementation of the monitoring system: [4] [5]

According to a contract concluded in December 2005, Siemens Co. as the general contractor will establish the system elements in the area of 20 plants, affecting 9 counties (Borsod-Abaúj-Zemplén, Csongrád, Fejér, Győr-Moson-Sopron, Komárom-Esztergom, Szabolcs-Szatmár-Bereg, Tolna, Veszprém and Zala) and the capital city in the period of 2006 - 2012.

Based on studies of the project plan or rather the engineering documentation, four meteorological sensors and 14 sensors for gases will be installed on site of each plant, thus altogether 84 meteorological and 294 gas measuring points. Probes to be installed at meteorological measuring points will provide data necessary for estimates on the atmospheric spread, whilst the gas probes are able to measure data specific for the plant.

Main elements of the monitoring endpoints improved by meteorological stations:

- indicator for direction of wind
- indicator for wind speed
- indicator for air temperature (2 m, 10 m)

- hygrometer,
- selective gas sensor (2 EA)
- interfaces for communication
- power supply unit

94 monitoring endpoints will be installed without meteorological sensors.

Data gained by probes of the monitoring systems will be continuously gathered in collection centers installed in the areas of hazardous plants, then transferred to the duty office of the (Civil Protection) Disaster Management Directorate of competent county (capital city). In case of reaching the dangerous threshold, an automatic alarm will be generated, based on which the alert of the population will be performed manually.

Access to the measured data is possible at the following locations: NDGDM, duty offices of competent County Directorates for Disaster Management, duty office of professional municipal fire brigades and the dispatcher services of chemical plants concerned.

In 2006, a model system was installed at five plants affected in Borsod-Abaúj-Zemplén County (Borsodchem Co., French-Hungarian Fine-Chemical Ltd., North-Hungarian Chemical Works Co., Tisza Integrated Chemical Factory Co., MOL Co., Tisza Refinery), as a result of which 90 monitoring sites in all (20 of them supplemented by meteorological stations) were established.

In 2007, in Pest and Veszprém Counties, altogether 76 monitoring (20 of them supplemented by meteorological) stations will be established, respectively at four plants concerned (Prímagáz Co. Gógánfa Storage Unit, Nitrogen Works Co., MOL Co. Százhalombatta, Huntsman Corporation Hungary Co.), together with 14 external monitoring endpoints in seven villages.

Figure 1 TVK monitoring & meteorological endpoint

Figure 2 TIFO monitoring endpoint

2.2 The public warning and notification system: [4] [5]

The establishment of the system will be carried out in settlements endangered by the aforementioned 20 plants, the quantity of which is included in the table below:

Endangered settlement	Year of installation	Sirens needed (EA)
Algyő	2008	9
Budapest	2008-12	385
Dorog	2010	6
Dunaújváros	2009	27
Gógánfa, Ukk	2007	6
Kazincbarcika, Berente	2006	9
Oszlár	2006	2
Berhida,	2007	10
Pétfürdő, Várpalota, Ősi (2 plants)	2007	33
Pincehely	2008	4
Sajóbábony	2006	4
Sajószentpéter	2006	6
Tiszapalkonya	2006	3
Tiszaújváros (Leisure time center, Power Plant residental area)	2006	7
Újudvar	2011	4
Százhalombatta, Ercsi, Szigetcsép, Ráckeresztúr	2007	50
Total:	2006-2012	565

Control centers enacting and performing alert will be installed at duty offices of the concerned county directorate for disaster management (Civil Protection Directorate of the Capital), the endpoints can be activated based on free grouping.

The alerting and notification system will be manually activated based on alarming signals from the monitoring system. The construction of the system enables the enlargement of the system itself, the integration of the former established electronic instruments into the system to be established.

Main elements of the alarm endpoints are as follows:

In 2006, 31 public warning and notification endpoints were installed in seven settlements endangered by hazardous chemical plants in Borsod-Abaúj-Zemplén County.

In 2007, 110 public warning and notification endpoints will be installed in 10 settlements in Pest and Veszprém County, respectively.

Figure 3 Siren loudspeaker

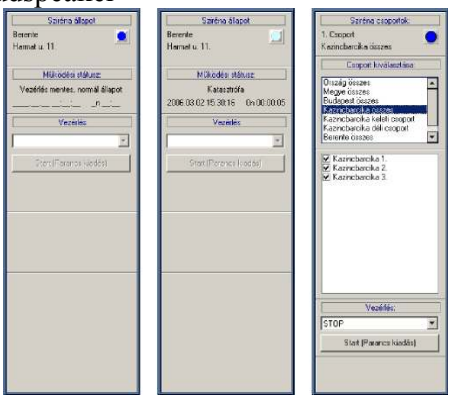


Figure 4 Alarm control software

Figure 5 Electronic siren on a roof

Figure 6 Electronic siren on a pillar

Literature

Legal provisions

[1] Council Directive 96/82/EC on the Control of Major Accident-Hazards Relating to Dangerous Substances

[2] Act 74 of 1999 on the Direction of the Protection against Disasters and the Protection against Major Accidents involving Hazardous Materials

[3] Act 37 of 1996 on Civil Protection

[4] Government Decree on the Protection against Major Accidents Involving Hazardous Materials /2/2001. (I.17.)/

[5] Government Decree 128/2001. (VII.13.) on the Promulgation of the Convention on the Transboundary Effects of Industrial Accidents (Helsinki Convention), released by UN ECE in Helsinki on 17 March 1992
[6] Government Decree 179/1999. (XII. 10.) on the Direction and Organization of Protection against Disasters and the Implementation of the Act on Disaster Management
[7] Government Decree 60/1997. (IV. 18.) on the General Rules of Protection of refuges, supplying of individual arms, public warning, together with evacuation and hosting
[8] Government Decree 114/1995. (IX. 27.) on the Rules of Classification of Settlements relating to Civil Protection and the Requirements of Protection
[9] Decree of the Minister of the Interior 18/1996. (VII. 25.) on the Classification of Settlements Relating to Civil Protection

Studies, handbooks

[10] CIMER Zsolt, CSEH Gábor, DEÁK György, GYENES Zsuzsa, HOFFMANN Imre, KÁTAI-URBÁN Lajos, Prof. Dr. SOLYMOSI József, Dr. SZAKÁL Béla, VASS Gyula: *Handbook on Risk Management in the Industry* - 2004- ISBN 963 224 816 3 – p. 46.
[11] CSEH Gábor, KÁTAI-URBÁN Lajos, KOZMA Sándor, Dr. POPELYÁK Pál, SÁNDOR Annamária, Dr. SZAKÁL Béla, VASS Gyula: *Handbook on Industrial Safety* -2003- ISBN 963 224 716 7 –p. 112.
[12] Dr. KÁTAI-URBÁN Lajos: Assessment and Development of Conditions of the Application of Protection against the Transboundary Effects of Industrial Accidents Doctorate (PhD) dissertation in 2006.
[13] IT and Telecommunication Department of NDGDM and Pantel Technokom Ltd., Techno-Tel Ltd.: Feasibility Study on the Implementation of the Monitoring Systems in the Areas of Lower and Upper Tier Hazardous Plants under the SEVESO II Directive.
[14] IT and Telecommunication Department of NDGDM: *Tender for the MoPuWa System*, together with Siemens Co.: *MoPuWa Technical Tender*

Beatrix FREGAN

CERTAINS ACTEURS DU NOUVEL ENVIRONNEMENT MONDIAL

Alors qu'il était le principal moteur des relations internationales dans le modèle occidental, l'Etat possède désormais des concurrents dans le jeu d'influence internationale. Il ne constitue plus la seule entité qui utilise les instruments diplomatiques, informationnel, militaire ou économique. Etatique, non étatique, les organisations internationales, les organisations privées ou les compagnies internationales possèdent tous désormais le contrôle et utilisent quelques-uns ou tous les instruments de pouvoir d'un Etat.

Acteurs diplomatiques

Avec une longue tradition de réseaux diplomatiques et de relations protocolaires, les Etats ont profité de leur monopole sur le pouvoir diplomatique. A travers ce monopole, ils ont créé des organisations pour favoriser leurs interactions. Ces organisations ayant grandi, les Etats cèdent à présent leur monopole à leurs propres créations ou à de nouvelles organisations influençant et façonnant le pouvoir diplomatique.

Les Nations Unies (ONU) ont depuis longtemps été un acteur dans la sphère d'influence diplomatique. L'ONU est passée d'un forum pour action diplomatique entre Etats à un acteur supra-étatique qui exerce sa propre action diplomatique à travers ses propres moyens. Grâce à ses ambassadeurs spéciaux et ses représentants, l'ONU entame, dirige, et conclue des négociations entre états et avec les états individuels.

Des organisations telles que l'Union Européenne (UE) ou l'Organisation pour le Développement Economique de l'Afrique du Sud (ODEAS) représentent collectivement des acteurs dans les négociations diplomatiques. Servant comme « porte-parole » pour les états; ces derniers abandonnent leur influence individuelle à une organisation inter-étatique pour une plus grande représentation collective à l'extérieur de la région.

Les Organisations Non Gouvernementales (ONG) sont aussi entrées dans la réalité des acteurs diplomatiques au sein du nouvel environnement mondial. La création de la Cour Pénale Internationale (CPI) est le résultat de négociations menées par un collectif d'ONG. Les ONG ont individuellement aussi agi dans des rôles diplomatiques pour négocier entre gouvernements et groupes de rebelles des « cessez-le-feu » ou des trêves dans des zones de conflit. Aussi les organisations internationales ont une

influence diplomatique à la fois à travers les lobbyistes et de manière indépendante. Du reste, Les lobbyistes agissent sur la scène diplomatique en finançant les partis politiques pour soutenir les campagnes électorales de politiciens.

Acteurs informationnels

Dans le domaine des acteurs informationnels, il y a les acteurs de l'information institutionnels tels que les masses média, mais le plus important des nouveaux acteurs de l'information sont les citoyens du monde. Ces derniers, aidés de réseaux de télécommunication modernes et le développement d'accès plus facile et plus rapide à l'Internet, ont maintenant la vaste majorité de l'information disponible des États entre leurs mains . En conséquence, les individus ne sont pas seulement individuellement mieux informés des événements se passant de l'autre côté du monde mais ils peuvent communiquer aussi entre eux pour discuter, organiser et agir en réponse à ces événements. La révolution de l'information a aussi donné la capacité à des individus éloignés de communiquer et de conspirer des attaques asymétriques en évitant des déplacements physiques à travers les frontières qui pourraient attirer l'attention des autorités. Le deuxième groupe d'acteurs informationnels, le média, procure l'outil informationnel de pouvoir aux individus qui ne l'exercent pas eux-mêmes.

Les acteurs médiatiques au sens informationnel incluent la presse écrite, les transmissions radio-télévisuelles et les réseaux dont ils font partie, allant des journalistes indépendants aux réseaux câblés et satellitaires des entreprises multinationales émettant des informations vingt-quatre heure sur vingt-quatre. Ces acteurs procurent de l'information aux masses plus rapidement que jamais à plus grande échelle et dans un bombardement d'information permanent. Le média fournit positivement un sens de transparence et de responsabilité aux gouvernements qui sont ainsi toujours sujet à l'examen minutieux de l'information. Cet examen minutieux doit souvent être pris en considération avant qu'une action soit décidée ou prise par un gouvernement. Les médias peuvent aussi jouer un rôle négatif dans le traitement, le filtrage, et les commentaires inappropriés qu'ils fournissent sur l'information alors qu'elle transite par les réseaux médiatiques à destination du public. Le même événement en Iraq aura des niveaux de couverture différents et sera commenté différemment selon la source qui couvre l'événement.

Acteurs militaires

Le plus sûr monopole historique de l'État, le monopole sur l'usage de la force, est révolu. Ce monopole a été brisé par deux causes différentes. Le

premier nouvel acteur dans le domaine militaire se trouve souvent dans les crises, les conflits, l'environnement des «failed states» et est une cause de tels environnements. L'héritage de la guerre froide, les «petites guerres» et «conflits périphériques» qui ont frémi entre les deux superpuissances ont laissé des armements disséminés dans le monde sans armées pour les utiliser. Armées privées et milices sont un facteur déstabilisant dans les crises, les conflits, et les «failed states». Ils constituent souvent un grand risque pour les acteurs de la reconstruction et de toute paix consentie ou imposée. Le deuxième groupe d'acteurs militaires est semblable dans la mesure où ce sont des «armées privées». La différence est qu'ils travaillent pour les Etats ou d'autres acteurs légitimes.

Qu'ils agissent comme sous-traitants pour un Etat ou sous contrat pour le compte d'un groupe d'aide ou d'une organisation multinationale, des capacités militaires considérables restent maintenant dans les mains de sociétés privées. Suivant les termes des contrats de sécurité, de formation, d'assistance ou de soutien, ces sociétés privées ont accès aux armes allant des mitrailleuses à l'artillerie, aux chars et aux avions de combat. Ces nouveaux acteurs ne rivalisent pas nécessairement avec l'usage étatique du pouvoir militaire; ils donnent à l'état une nouvelle gamme d'options pour employer le pouvoir militaire. Les fournisseurs contractuels de capacités militaires peuvent exécuter les tâches que les forces armées des Etats ne peuvent pas réaliser pour des raisons légales, techniques ou de volonté. Les fournisseurs contractuels peuvent assumer aussi des fardeaux logistiques pour projeter, déployer ou soutenir la force qu'il est peu économique pour les Etats de posséder, maintenir ou entretenir.

Cela peut libérer aussi les forces étatiques pour d'autres missions plus conformes au métier des armes.

Littérature:

[1] Note d'analyse, Groupe de recherche et d'information, Bruxelles, 2007.

KOZÁK Piroska

FÉSÜLETLEN GONDOLATOK A FŐISKOLAI KÉPZÉS ÜRÜGYÉN

2002-ben felvételiztem a Zrínyi Miklós Nemzetvédelmi Egyetemre, a Bolyaira, műszaki informatika szakra. Nagyon komolyan vettem ezt a felvételit, de ennek megvolt az oka. Ez volt az egyetlen felsőoktatási intézmény, ahova beadtam a jelentkezésemet. Pontosan tudtam,hogy mit akarok csinálni az életben és azt is, hogy mi vár rám, ha ide bekerülök, illetve majdnem pontosan tudtam. Nem gondoltam volna, hogy ennyire fontos lesz nekem egy iskola valaha az életemben. Nem csak egyszerűen iskola, annál sokkal több, mert nem csak diplomát ad, hanem annál jóval többet. Szerencsések azok a fiatalok, akik, a katonai főiskolába felvételt nyernek és eredményesen el is végzik. Nyilvánvalóan többet kell tudnia egy hivatásos katonának, és jobban ki kell tudnia használni a képességeit, mint egy civil diplomát szerzett fiatalnak és ebből adódóan többet is kell kapnia a képzés során, így nem is lehet meglepő, hogy több mindent foglal magába egy katonai főiskola a többi főiskolához képest.

Sikeres felvételim után megkezdtem tanulmányaim a Bolyai János Katonai Műszaki Karon. Az elején természetesen nem volt könnyű és rengeteg parancsnokom volt, akik egyetlen percre sem könnyítették meg az életem, de igazán egyszer sem fordult meg a fejemben az alapkiképzés során, hogy rossz helyen járok és az sem, hogy feladjam és hazamenjek. Rengeteg új feladat állt előttem, amit napról napra végre kellett hajtani és korábban még hasonlóval sem találkoztam a civil életemben. Meg kellett küzdeni mindennel és nem lehetett elmenekülni semmi elől. Legfőképpen magammal kellett harcolnom és ez volt a legnehezebb. Felül kellett kerekedni egy csomó apró dolgon, hogy a nehéz feladatokat meg tudjam oldani. Ezek az apróságok ugyan nem nagy dolgok, de ha sok van belőlük, akkor az embert próbáló lehet. A tűző nap, a hideg szél, hajnali ébresztő, eső, vigyázzállás, sebes sarkak és kezek, reggeli tornák, állandó rend és fegyelem, estig tartó foglalkozások, katonai ismeretek gyors elsajátítása és a rengeteg szabály. A főiskola kezdő hallgatói ezekkel egész biztos, hogy találkoznak és én sem voltam kivétel. Az alapkiképzés végeztével büszkén és nagy örömmel tettem esküt, azonban akkor még nem láttam előre, hogy az alapkiképzés még csak egy lépcső az ezerből a célhoz vezető úton. Lépcsőn felfelé menni mindig nehezebb, mint lefelé és ezt az is híven tükrözte, hogy a sok nehézség, amit az egyenruha felhúzása utáni hetekben sikeresen túléltünk és szerettünk volna elfelejteni, ott folytatódott, ahol abbahagytuk, és nemcsak a

főiskolán kell legyőzni a sok apró dolgot, hanem egész katonai pályánk alatt.

Sajnálatos módon a tanulmányi nehézségek következtében szakot kellett váltanom a főiskolán, amely évhalasztással is együtt járt. Informatika szakról villamosmérnök szakra váltottam, azon belül pedig híradó szakirányra. Ezt a lépést azóta sem bántam meg és visszatekintve sokkal jobban örülök, hogy ezen a szakon végeztem és ezzel együtt azt sem bántam, hogy öt évig tartott számomra a főiskola.

Bátran kijelenthetem, hogy rengeteg előnnyel és pozitívummal rendelkezik a katonai főiskola a többi főiskolához és egyetemhez képest, függetlenül attól a ténytől, hogy soha nem jártam más főiskolára. Azonban ezek az előnyök és pozitívumok csak azoknak a hallgatóknak jelentenek előnyt, akik az átlagosnál komolyabb értékrendet képviselnek.

A legnagyobb különbség a többi iskolához képest az életvitel. Nagyban más életet él egy katonai főiskolás, mivel szigorú napirend van, meg van határozva, hogy milyen ruhába kell lenni, mit kell magával vinnie, mettől meddig mehet ki az iskolából, mikor mehet haza, szolgálatot kell adnia, szabályok szerint kell viselkednie és még arra is szabályok és előírások vannak, hogy kivel hogyan kell beszélnie. Egy civil fiatal számára ez valószínűleg szörnyen hangozhat, ettől függetlenül mégis évről évre többen gondolják úgy, hogy ezt az iskolát választják.

A legfontosabb dolog a főiskolán eltöltött évek alatt, hogy a hallgatók életében és felfogásában nagy szerepet kap az emberség fogalma. Talán sokan nem is gondolnák milyen nagy szerepe van ebben az egyenruhának. A katonai főiskolán meghatározott öltözet és az egyforma ruha viselete az egyik legfontosabb a szabályok között, ahogy az egész Magyar Honvédség életében is, itt viszont sokkal nagyobb jelentőséggel bír. Az egyenruha viselése a mai világban nagyon sokat jelent ennek a közösségnek ez emberséges magatartás és emberségre való törekedésében. Az egyenruha több szempontból vált közösségépítővé: az összetartozás és az egységesség megteremtése mellett az egyik legnagyobb társadalmi problémát kerüli meg, amely nem más, mint az anyagi helyzet alapján történő megítélés. Sajnálatos módon egyre többször és több helyen tapasztalható, hogy az iskolaköpeny használatának megszűntetése óta az általános és középiskolákban a tanulók megítélése közösségen belül függ az öltözködéstől, amelyből leszűrhető az anyagi helyzet. Köztudott manapság minden felnőtt ember számára, hogy egy gyermek szociális fejlődésében mekkora szerepet játszik, hogy az iskolatársai miként ítélik meg öltözködésének minősége alapján és ebből anyagi helyzetére következtetve hogyan viselkednek vele, a közösségi szellemet és az összetartozás lehetőségét rombolva. Ezen az igen gyakori szociális társadalmi problémán átsiklik a katonai főiskola hallgatói állománya és kijelenthető, hogy minimálisra csökken az ilyesfajta megkü-

lönböztetések száma. Ez pedig a mai anyagias és egyre inkább pénzközpontú társadalmunkban nagy dolognak számít, legfőképpen az iskolai közösség megalakítása szempontjából.

Egy érettségizett fiatal számára, aki sikeresen felvételt nyer a katonai főiskolára, amellett, hogy az esetleges öltözködési és anyagi nehézségei miatt ért megkülönböztetéstől elbúcsúzhat, még ennél is több segítséget kaphat szociális szempontból. Egy civil főiskolás számára a diploma megszerzéséig rengeteg költséggel kell számolnia, függetlenül attól, hogy államilag finanszírozott felsőoktatási intézményben tanul. Ha lakóhelyétől távol helyezkedik el az iskola, akkor gondoskodnia kell az utazásáról, szállásáról, amely kollégiumi férőhely esetén kisebb összegből is finanszírozható, egyéb esetben az albérlet kerül szóba, melynek kifizetése havonta még több fő esetében is magas költségekkel jár. A katonai főiskolán nem kell ezzel a problémával megküzdenie egy hallgatónak sem, hiszen a kollégiumban való bentlakás amellett, hogy kötelező egyben ingyenes is, és bármely fővárosi kollégiumhoz viszonyítva jó körülményekkel rendelkező épület. Ennek ismételten nagy jelentősége van a jelenlegi magyar felsőoktatásban. Ezen kívül, a katonai főiskola az év minden napján gondoskodik a hallgatók étkeztetéséről, a távollét esetében pénzösszeg utalásával, valamint illetményt utal a hallgatók bankszámlájára. Kevés egyetem, illetve főiskola büszkélkedhetne azzal, hogy ilyen mértékben tudna gondoskodni a hallgatóiról, habár nem szabad figyelmen kívül hagyni, hogy ami ingyenesnek látszik az valójában nem az. Az a katona, aki sikeresen elvégzi a főiskolát és legalább négy évig szolgál a Magyar Honvédségben, annak valóban ingyenes a képzés, ezzel szemben, aki nem végzi el, annak vissza kell fizetnie a költségeket. Ez a hallgatók életében és a sikeres végzés érdekében kényszerítő eszközként szerepel, amely a küzdőszellemet a hallgatókban még inkább motiválja, legfőképp annak tekintetében, hogy a katonai főiskolán tanulók többsége közepes, nehézkes, vagy kifejezetten nehéz anyagi körülmények közül érkezik. Bármi, ami akadályként merül fel a hallgatók életében és leküzdésre kell, hogy kerüljön, csak és kizárólag erősíti a katonai jellemet. A főiskolán belül a napi megélhetési gondokat mellékelve sokkal több ideje és energiája marad a hallgatóknak arra, hogy azzal foglalkozhassanak, amiért ebben az intézményben vannak. Ez a tény ismételten csak az iskola előnyei közé sorolható.

Az egyenruhának egyébként egy egész sajátos jelentése is van, amely az egész Magyar Honvédségre jellemző. Miután mindenki egyforma ruhát hord szervezeten belül, így olyan személyiségfejlesztő feladat áll az ember útjába, amely teljes egészében az önmegvalósításról szól. Önkénytelenül is benne van minden emberben attól a pillanattól kezdve, hogy először közösségbe kerül, hogy valamilyen formába kitűnjön a környezetében a többiek közül. Az egyenruha viselése eleve elveszi annak lehetőségét, hogy valaki

az öltözködésével hívja fel magára a figyelmet, ami azt eredményezi, hogy ennél többet kell adnia magából és a személyiségéből. Az önmegvalósításnak pedig éppen ez a kulcsa, hogy az ember minél többet mutasson önmagából és a képességeiből és ne külsőségekkel próbálja eltakarni a lényeget saját személyiségéről, hogy az lehessen, aki valójában. Az, aki él ezzel a lehetőséggel nagy lépést tesz az éretté és felnőtté válás útján, mivel személyiségét erősítheti ezzel, amellett, hogy tükörképet kapva önmagáról valódi hibáival szembesülhet, és azok kijavítására kap lehetőséget. Ennek tekintetében az önmegvalósításnak nagy szerepe van az egyén fejlődésében, amely mindenképpen jót tehet a csapatszellem és egységesség kialakításakor. Ha valaki tisztában van az erősségeivel és a gyengeségeivel, akkor lehet leginkább egy csapat hasznára. Egységesség és csapat nélkül pedig nem létezik hadsereg, amely működőképes lenne. Ez a mozgatórugója a csapat működésének szellemi és gyakorlati feladatok elvégzésében egyaránt. Levezetve az egységesség és az egyenruha közötti összefüggések sokaságából egy szálat megállapítható, hogy mennyivel többet jelent, ha valaki katonai főiskolát végez más polgári iskolákhoz képest.

A hallgatók évről évre jutnak egyre magasabb szintre, hogy igazán egységet alkossanak, azt erősítsék, és sokan csak a főiskola kapuit végleg átlépve figyelnek fel saját magukban a változásra, amelyen keresztül mentek, miszerint örök életükben keresni fogják az egységességet, amely mindenkit felemel önmagából és kiegészít.

A katonai főiskolán eltöltött éveim alatt rengeteg pozitív élményben részesültem az egységesség, az összetartás és az összetartozás miatt, ezért több ezer példát tudnék felsorolni, arról beszámolva, hogy ezek következtében milyen pozitív és kellemes perceket kaptam. A sok ezerből mégis van néhány, amely örök életemre emlékezetes marad: ha valaki sírt, megvigasztaltuk; ha lelkileg összetört, összeszedtük és bizalmat öntöttünk belé; ha féltünk egy vizsgától, akkor együtt féltünk és együtt tanultunk; testnevelés órán egymást húztuk; sportversenyeken mindenki kihozta magából és a társából a legtöbbet a győzelemért, a közös győzelemért; segítettük egymást szolgálatban, szolgálaton kívül; odafigyeltünk egymásra és szerettük egymást, mert összetartoztunk. Mindenki segített a másiknak, hogy elvégezhesse a főiskolát és diplomát kapjon. Sajnos ennek a csodálatos közösségnek egy nap vége lett és csak kevés ideig örülhettünk egymásnak, de az a kevés idő a tisztavatásig nagyon sokat jelentett számunkra. Még ha a távolság és a feladataink szét is választottak bennünket és talán soha nem alkotjuk már azt a bizonyos kis egységet a Honvédség keretein belül, akkor is örökre ott lapul majd mindenkiben az egység lényege, amely elkísér majd minket éltünk végéig.

Az összetartás ezen formáját legfőképpen azok a hallgatók tanulták meg igazán, akik velem együtt híradó szakon tanultak és végeztek.

Az iskolában több kiemelkedő tanszék is létezik, amely olyan nevelésben részesíti a hallgatóit, mely főként az összetartás és egységesség irányába tereli a közösséget. A Híradó Tanszék mellett kiemelhető a Hadtáp- és Pénzügy Tanszék és természetesen a lövészek.

Az iskola falain belül és kívül több problémát is észleltem az évek során. Az iskolán belül három fő problémával találkoztam, melyeken mindenképpen változtatni kellene, már csak abból az elgondolásból is, hogy minden hiba és hiányosság következményekkel jár.

A katonai főiskolán belül történt összevonások során a hallgatók 1-2 év alatt túltették magukat az eseményeken és összehangolódtak, egységesedtek és az esetleges karok közötti ellentétek szép lassan eltűntek a színről, azonban az iskola vezetésben ez a probléma és ellentét a mai napig érezhető. Az iskolát vezető főtisztek és tisztek sokkal nehezebben teszik túl magukat az összevonásokkal kapcsolatban, amely egy okból megérthető több okból kifolyólag viszont semmiképp sem. Nyilvánvalóan a feszültségek fő oka abból adódik, hogy a szervezeti felépítés megváltozása egyúttal a tisztek legtöbbjének beosztására hatással volt, a beosztásuk körüli bizonytalanságok pedig természetesen a megélhetésüket veszélyeztetik, amely akár elegendő ok lehet arra, hogy ne vegyék könnyedén az átalakításokat. A hallgatók oldaláról nézve azonban káros hatása lehet, ha az egységesség és összetartás felé törekedve ilyen példák állnak előttük. Véleményem szerint ez igen nagy probléma egy olyan főiskolán, ahol a példamutatás kötelező a vezetők, illetve tisztek részéről a hallgatók és beosztottak felé. A tisztek megosztottsága érezhető és rossz hatású volt, és ez a viselkedés a jövőben sem vezet jóra.

A második fő probléma az iskolán belül, hogy a hallgatók sokszor találkoznak igazságtalansággal, saját magukkal és másokkal szemben. Ez főként abban mutatkozik meg, hogy a hallgatók melyik század kötelékébe tartoznak. Sajnálatos módon nem minden századparancsnok bánik egyenlően a hallgatóival. Századok között igen nagy különbségek vannak, és néhány parancsnok még a saját századán belül sem bánik egyenlően mindenkivel különösebb magyarázat nélkül, veszélyeztetve ezzel az egész iskola egységességét.

A harmadik fő probléma az aktív sportélet hiánya, amely talán a legnagyobb méretű a katonai főiskolán belül, hiszen az itt kialakult hiányosságok a hallgatók katonai jellemének kialakításában képeznek hiányt és a végzettek további pályájának alakulásában.

Tulajdonképpen aktív sportéletről nem nagyon beszélhetünk, abból kifolyólag, hogy az iskola létszámát tekintve bőven 50 % alatt van a naponta és rendszeresen sportoló hallgatók száma nemtől és évfolyamtól függetlenül. Egyébként a lehetőségek adottak a sportolásra, legfőképpen a kötelezően felmérendő sportszámok esetében, hiszen a főiskola rendelkezik sportpá-

lyával, két tornateremmel, tornakerttel, gyengén felszerelt kondicionáló teremmel és uszodával. Ezek a lehetőségek saját tapasztalatomból kiindulva alkalmasak a mindennapi edzésre és a testnevelési felmérésre való felkészülésre, amely már csak és kizárólag egyéni szorgalomtól függ. A tapasztalat mégis azt mutatja, hogy a hallgatók nem tolakodnak tömegével a sportolás utáni fékezhetetlen vágyukban sem a futópályán, sem a tornatermekben. Az uszoda ez esetben kivételt képez, ugyanis annak kihasználtsága már mutat valami előrelépést. Azonban nem csak az egyéni szorgalomtól függő, szabadidőben folytatott sportolás hiánya akadályozza az aktív sportélet meglétét, hanem a testnevelésért felelős személyek munkájának lekorlátozása anyagi és időbeni szempontból. A katonai főiskola Testnevelési Tanszékén évről évre csökken az oktatók száma, melynek több oka is van: lecsökkent a hallgatói állomány létszáma, így a szakaszokra jutó tanárok száma ezzel arányosan csökken, és ami még ennél is nagyobb probléma, hogy a kötelező testnevelési óraszám is csökken. Délutánonként nincsenek a hallgatók számára edzések, közös sportolás, versenyekre való készülés.

A reggeli torna eltörlésének gondolatával már sokan foglalkoztak, azonban ennek kiiktatására csak abban az esetben hajlott volna az iskola vezetése, ha valamilyen formában pótolva lenne a nap bármely szakában a kötelező mozgás. Tapasztalatom szerint a reggeli torna meglétéért kizárólag abból kifolyólag ragaszkodtak, hogy a kötelező ébresztő hatékonyságát fokozzák. A hallgatók napi kötelező mozgásának és fizikai erőnlétének formában tartásához valamint az egészség megőrzéséhez csekély mértékben sem járul hozzá a reggeli torna.

Véleményem szerint a katonai főiskola hallgatói számára nagyon fontos lenne az aktív sportélet létrehozása. A jelenlegi, rendszer nélkül működő sportoláson pedig mindenképpen változtatni és javítani kellene, melynek jelentősége túlmutat a hallgatók fizikai erőnlétének fejlesztésén abból kifolyólag, hogy az iskola felelős a Magyar Honvédség számára a hallgatók tisztté való képzéséért, katonai jellemének fejlesztéséért, küzdőszellemének kialakításáért, fizikai teljesítőképességéért. Olyan tiszteknek kellene ebből az iskolából kikerülnie, akik képesek példát mutatni a jövőbeni beosztásukban, elsősorban alárendeltjeik számára és nemcsak elviekben, hanem gyakorlatban is, hogy megvalósíthassák az ideális katonai modellt, miszerint a parancsnok fut elől és utána az alárendeltjei. Ezen felül pedig legyen képes példamutatásán keresztül beosztottjait is arra késztetni, hogy fejlesszék fizikai teljesítőképességüket.

A jelenlegi helyzet alapján a főiskola nem képes ilyen típusú tisztek tudatos nevelésére, amely az egész Magyar Honvédség szellemiségének alakulásában komoly hátrányt jelenthet a jövőben.

Véleményem szerint csak és kizárólag tudatos és jól felépített többlépcsős sportolási rendszer segítene a hallgatók aktív sportéletének kialakítás-

ban. Az első lépcsőben az egyéni szorgalommal rendelkező, rendszeresen, napi szinten sportoló hallgatókra kellene nagyobb figyelmet fordítani, és képességeik, erőnlétük megvizsgálása után versenyeken való részvételre ösztönözni. A rendszertelenül, vagy egyáltalán nem sportoló, valamint a testnevelési követelményekkel folyamatosan küszködő hallgatókkal pedig képességeik alapján csoportokra osztva folyamatosan kellene foglalkozni és rendszeres sportolásra való nevelést alkalmazni. A második lépcsőben - melynek elérésekor a hallgatók 100%-ban részesei a sportéletnek, azaz minden egyes hallgató napi szinten, rendszeresen és elfogadható eredménynyel sportol és képes ennél tovább lépni - akkor következhet a csapatsportokban és egyéni sportszámokban való aktív részvétel, melynek fejlesztése következtében a katonai főiskola a Magyar Honvédségen kívül rendezett versenyeken a lehető legjobb eredmények és helyezések reményében indulhat a Magyarországon meghirdetett versenyeken.

Mindennek megvalósítása természetesen anyagi vonzattal jár. Az aktív sportélet többlépcsősen felépített rendszerében az első lépcső tulajdonképpen anyagilag kisebb kiadással járna mint a második lépcső, mivel az első lépcsőnél legfőképpen csak szervezési kérdések döntenek a megvalósításról. A szervezésnél a hallgatók időbeosztásának megváltoztatására; a testnevelésórák hatékonyságára, mennyiségére; és a délutáni edzések megszervezésére kell törekedni, s ezzel egy ütemben a testnevelő tanárok létszámát növelni. Ezen kívül, ami a technikai és szervezési feladatokon túl a legfontosabb kérdés, a hallgatók motiválása illetve ráhangolása a napi sportolásra. Ennek több módja is lehetséges. A hallgatók figyelmét fel kell hívni a megkezdődő aktív sportéletre, melynek ők maguk lesznek a főszereplői, azaz a meggyőzés módszere a részvétel biztosítására. Azonban előfordulhat, hogy ez a módszer kevésnek bizonyul a ráhatásban, mivel a hallgatók önszorgalmának hiánya is hozzájárult a jelenlegi helyzet kialakulásához. Ebben az esetben az iskola vezetésének a terv és a cél megvalósítása érdekében - amely az egész iskola javát szolgálja – olyan döntést kell hoznia, amely nem veszi figyelembe a hallgatók jelenlegi álláspontját az aktív sportélet megvalósításában, azaz kötelezővé kell tenni a hallgatók számára minden esetben az órarendszerinti és a délutáni testnevelésen való részvételt.

A második lépcső az első lépcső megvalósításának sikerességétől függően már sokkal inkább anyagi kérdés. Hiszen az aktív és versenyképes csapatsportokban és egyéni sportokban való megfelelő szint elérésére a jelenlegi technikai feltételek mellett kevésnek bizonyulhatnak.

A mindennapos edzések a különböző sportokban, különböző szinteken történő végrehajtása több helyet igényel, ezáltal minimum még egy tornacsarnok megépítésére lenne szükség, továbbá a csapat- és egyéni sportok űzéséhez szükséges eszközök beszerzésére, amely szintén komoly költsé-

gekkel jár. Nyilvánvalóan a sportba befektetett összeg a versenyeken elért legjobb eredmények esetén sem fog anyagi szempontból megtérülni, ezért az iskola vezetésének, illetőleg az aktív sportélet megvalósítását támogatóknak és az ellenzőknek el kell döntenie, illetve meg kell egyeznie abban, hogy az iskola jó hírét szeretnék e növelni, és egyáltalán a katonai főiskola rendeltetésének meg akarnak e felelni, vagy a jelenlegi rendszeren semmit se változtatva megvárni az aktív sportélettől mentes katonai főiskolán történő nevelés következményeit.

Ezért tartom a legnagyobb problémának a tiszti főiskolán a sportolás hiányát és több mint valószínű, hogy ez a probléma nagymértékben hozzájárul az egész Magyar Honvédségben a sportélet színvonaltalanságához, legfőképpen a napi mozgáshoz való negatív hozzáállás miatt, függetlenül attól, hogy minden alakulatnál biztosított a napi egy óra sport és a legtöbb laktanyában minden feltétel adott a sportoláshoz. Ez a tény pedig önmagában nagyon elszomorító a hadsereg szempontjából és mindenképpen elgondolkodtató a Honvédség jövőjének alakulásával kapcsolatban.

A katonai főiskolán és a Magyar Honvédségen kívül a katonai pályát érintően több problémával is találkoztam, azonban ezek közül a legsúlyosabbat szeretném kiemelni, amely a magyar katonák és a civil lakosság közötti elszigetelődés egyre erősödő folyamata. Ennek két fő oka van és még ennél is több egyéb oka, azonban súlyos társadalmi következménye rengeteg akad.

A legfőbb okok mindenki számára ismertek. Természetesen a hadsereg létszámának radikális csökkentése elsősorban, illetve a sorkatonai szolgálat szüneteltetése, amely a szüneteltetés megkezdése előtt már össze se volt hasonlítható a korábbi évek helyzetéhez képest.

A NATO elvárásainak megfelelően szüneteltetésre került a Magyar Honvédségbe történő sorozás 2004. novemberétől. Ez a lépés a Honvédség szempontjából gazdaságilag mindenképpen előnyösnek tűnik, azonban társadalmi szempontból tekintve több mint károsnak mondható, amely feltétlenül hozzájárult Magyarországon a katonák és a polgári lakosság közötti szakadék kialakulásához.

A szüneteltetés előtti néhány évben már érezhető volt a sorozáskor bevonultak és a Honvédség önkéntes katonái számára egyaránt, hogy óriási különbség van már a ’90-es években létező sorkatonai állományhoz képest is, nemhogy a ’80-as években és az ennél korábbi évtizedekben szolgáló sorkötelesek között, mind a letöltött időtartam, mind a letöltendő idő alatti szolgálat szempontjából. Az évek múlásával csökkent a sorkatonai szolgálat időtartama, de sokkal lassabb volt a szolgálati idő csökkentése 1990 előtt, hiszen ezután rohamosan lerövidült és végül teljesen el is fogyott 14 év alatt.

20-30 évvel ezelőtt komoly tekintélyt jelentett katonának lenni, akár hivatásosként akár sorkatonaként, manapság viszont elmondható, hogy már odáig fajult a helyzet, hogy egy katona, rangtól függetlenül akár még kellemetlenül is érezheti magát, ha köznapi egyenruhában felszáll egy tömegközlekedési eszközre, ami a jelenlegi helyzetet nem szépítve, bizony elkeseredettségre adhat okot a Honvédség katonái számára, és még inkább ahhoz vezet, hogy a civil emberek és a katonák között tovább mélyüljön a szakadék.

Sajnos a mai 30 év alatti fiatal férfiak legtöbbjén meglátszik, hogy nem volt soha katona és talán még laktanyát sem látott közelről, de még tálán egyenruhát sem, ezáltal nem fejlődött éppenséggel előnyére ez a generáció a férfiasság, a tartás és néhány igen fontos emberi tulajdonság szempontjából. A mai magyar társadalom tájékozatlansága a Magyar Honvédségre vonatkozóan meglehetősen szembetűnő. Azonban a helyzetet tovább súlyosbítja, hogy nemcsak nő az elszigetelődés az önkéntes hadsereg és az ország lakossága között, hanem egyre inkább megfigyelhető egy teljes érdektelenség a hadsereg irányába, sőt manapság már az ellenszenv és a rosszindulat sem kerüli el az egyenruhát viselőket. Magyarországon a rendőrök iránti ellenszenv - amely mára bizonyos rétegekben divattá vált és szétterjedt a lakosság körében – a katonákat is magával rántja. Ezért természetesen a katonáknak nem a Rendőrséget kell felelőssé tennie. Olyan ellenszenv övezi az állampolgárok részéről a katonákat a rendőrökkel szembeni tiszteletlenség miatt, amelyre egyrészt nem szolgáltak rá, másrészt olyan civil emberek részéről, akik a rend és a szabályok felrúgásán szórakoznak, tevékenykednek, és semmilyen tiszteletet nem mutatnak egyetlen egyenruha iránt sem, sőt a katonai egyenruhát a sorkatonai szolgálat alól kikerülve sokan még csak nem is ismerik. Így nem is csoda, ha manapság nem érzi a társadalom megbecsülő támogatását egy katona, ha egyenruhában jelenik meg.

Ha a társadalom ezen az úton halad tovább és a rendbontás divatosabbá válik, mint az egyenruha, akkor a Honvédség tagjai, illetve a rendszerető, egyenruhát becsülő állampolgárok számára komoly aggodalomra adhat okot a jelenlegi helyzet, amely alapján a jövő generációja nem túl bíztató és megnyugtató.

A Magyar Honvédség több misszióban teljesít szolgálatot, olyan országokban, ahol a fegyverhasználat, robbantás, öldöklés és erőszak mindennapos dolog.

A veszélyt vállalva mégis sok katona szolgál ezeken, a NATO által felügyelt területeken, nem beszélve arról, hogy bármikor előfordulhat egy váratlan támadás esetén, hogy néhányan soha nem térhetnek haza Magyarországra. Ezek a katonák helytállnak ezekben a veszélyes országokban, amelyektől a legtöbb magyar férfi és nő még a televízióban látott képek

alapján is megrémül. A probléma sajnos ott merül fel, hogy az állampolgárok a minimális kötelességüknek sem tesznek eleget, hogy legalább a hozzáállásukkal támogatnák a magyar katonákat, akikkel egyébként kifejezetten elégedett a NATO. Véleményem szerint a magyar emberek részéről ez a mentalitás és érdektelenség a missziós katonákkal szemben rendkívül igazságtalan és cseppet sem hazafias.

Magyarországon, a civilek és katonák közötti mély szakadéknak tehát több oka és összetevője megtalálható és bizonyítható. Azonban meg lehet e elégedni a Honvédség részéről annyival, hogy megállapítjuk a problémát? Vagy esetleg megoldás is lehetséges? Több mint valószínű, hogy nem jelentene megoldást, ha hirtelen a sorkatonai szolgálatot újra elrendelnék, és még az sem jelentene megoldást, ha hirtelen tízszeresére növelnék a hadsereg létszámát. Egy út azonban mégis járható lehet, bár teljes értékű megoldás ettől sem remélhető, hiszen a rendbontók tevékenységeire felbuzdulva a mai társadalom modern gondolkodása odáig süllyedt, hogy nem egyértelműen elítélendő egy szolgálatot teljesítő egyenruhás megdobálása, hanem akár hazafias hőstett is lehet. Ekkor talán már körvonalazódhat, hogy mi is kell legyen a jövő katonai kommunikációjának fő iránya a Magyar Honvédség szervezetén kívül a társadalom felé, amely természetesen nem kizárólag a kommunikáció területén tevékenykedő katonákra háruló feladat, hanem a Honvédség minden egyes tagjának részvételére épül.

Zárásként és annyit jegyeznék meg, hogy a magam részéről nem kívánok megválni az egyenruhámtól, mert szeretem és vállalom továbbra is, és mindent, ami ezzel jár. Minden probléma és hiányosság ellenére egy nagyon jó főiskolára járhattam, és az egyik legjobb szakon végeztem. Az elmúlt öt év alatt minden percnek haszna volt. A problémák, amelyek véleményem szerint léteznek és felmerültek számomra az évek során a katonai főiskolával és az egész Honvédséggel kapcsolatban, a legkevésbé sem vették el a kedvemet attól, hogy katonatiszt legyek. Inkább arra inspirálnak, hogy részt vegyek ezeknek a problémáknak a megoldásában és a további felmerülő gondokkal való küzdelemben is részt vállaljak, mert a Magyar Honvédségen belül nemcsak az egyenruha közös, hanem a probléma is, de a megoldásra való törekvés még annál is közösebb feladat.

SCI-Network Távközlési és Hálózatintegrációs zRt.

CERAGON PONT PONT ÖSSZEKÖTTETÉSEK - NAGYSEBESSÉGŰ IP ÉS INFORMÁCIÓ VÉDELEM A LEVEGŐBEN

http://www.scinetwork.hu/

Tel.: +361 467 7030

Fax: +361 467 7049

info@scinetwork.hu

Központ:

Erzsébet királyné útja 125.

Budapest, H-1142

Magyarország

A SCI-Network Távközlési és Hálózatintegrációs zRt. hálózati rendszerintegrációval foglalkozó szakértő vállalkozás. A szűkebb értelemben vett hálózati rendszerek mellett a cég alaptevékenységébe tartozik a mikrohullámú átvitel, a hálózati biztonság és a rendszerfelügyelet is. A SCI-Network teljeskörű szolgáltatást nyújt ügyfeleinek a hálózatok terén a feladat felmérésétől kezdve, a tervezésen, eszközszállításon, üzembehelyezésen, oktatáson keresztül a garanciális és garancián túli szolgáltatásokig. A folyamatosan gyarapodó létszámmal, bővülő ügyfélkörrel és növekvő forgalommal rendelkező vállalat az informatikai vállalkozások felső harmadába tartozik.

A SCI-Network célja, hogy ügyfelei számára magas színvonalú megoldásokat biztosítson, valamint megismertesse kiváló minőségű termékeit és szolgáltatásait leendő ügyfeleivel.

A vállalat kiemelt figyelmet fordít a minőségbiztosításra, melyet ISO 9001 és AQAP2110 minősítése is tükröz.

SCI-Network Távközlési és Hálózatintegrációs zRt.

Ceragon pont pont összeköttetések - Nagysebességű IP és információ védelem a levegőben

A SCI-Network termék és szolgáltatási palettájában jelentős szerepet tölt be a Ceragon mikrohullámú összeköttetések szállítása, üzembehelyezése, felügyelete és rendszerbe integrálása.

A Ceragon Networks Ltd. a nagy kapacitású vezeték nélküli backhaul összeköttetések vezető szállítója.

Szerte a világon a mobil szolgáltatók, a fix vezeték nélküli megoldásokat nyújtó operátorok és a különféle magánhálózatok és szervezetek sikeresen alkalmazzák a Ceragon kínálta innovatív megoldásokat az egyre növekvő sávszélesség igények kielégítésére.

A Ceragon cég a szélessávú a gerinchálózati csatlakoztatási ún. backhaul megoldásokra fókuszál, ami jelentős előnyt jelent, hiszen mindenféle típusú elérési technológiát és hálózati megoldást kiszolgál.

A fő termékkör a moduláris rendszerű **FibeAir** termékcsalád, amely nagy sebességű mikrohullámú összeköttetéseket biztosít IP és SDH hálózatok felett nyújtott szélessávú szolgáltatások számára.

A Ceragon egyedülálló a világon a kiemelkedően nagy IP kapacitás (800 Mbps), valamint a titkosított változatú nagy sebességű IP összeköttetések szállítása terén.

A célpiac

A Ceragon berendezések a költséghatékonyság, skálázhatóság, és a jövő-álló funkcionalitások révén abban a három fő piaci szegmensben alkalmazhatók sikeresen, ahol a kapacitás növelés a fő hajtóerő:

Celluláris szolgáltatók: A Ceragon rugalmas, nagy kapacitású vezeték nélküli összeköttetései lehtővé teszik a szolgáltatóknak hálózataik bővítését. A Ceragon SONET/SDH megoldásai 155-622 Mbps közötti sebességgel ideálisak az új generációs hálózatok számára, mint pl. a 3G HSDPA. Az új viszonteladó (wholesale) szolgáltatók is sikerrel alkalmazzák, mint a bérelt vonalak költséghatékony alternatíváját.

Fix hálózati szolgáltatók: Ahol a kapacitás igényeket a az IP és konvergens szolgáltatások bővülése generálja, a Ceragon, mint vezető a mikrohullámú IP backhaul megoldások szállításában, hatékony eszközt ajánl a Triple play szolgáltatások biztosításához.

A fix vezeték nélküli szolgáltatóknak IP gerinchálózati felcsatlakozást biztosít rádiós access hálózataik számára (WiMAX és WiFi hálózatok).

Magánhálózatok: A Ceragon gyors szélessávú vezeték nélküli szolgáltatások nyújtását teszi lehetővé olyan területeken, ahol vezetékes megoldások nem állnak rendelkezésre, vagy költséges a kiépítésük.

A Ceragon összeköttetések ideális megoldást jelentenek a biztonsági és készenléti erőknek, közműveknek, oktatási, egészségügyi, kormányzati és katonai hálózatoknak, valamint a vállalati magánhálózatok számára.

A termékkör

A Ceragon FibeAir termékcsalád főbb típusai az alábbiak:

FibeAir 1500P

Többféle kapacitást, frekvenciát, modulációs módot és konfigurációt támogat.

Nagy kapacitású rendszer, mely 622 Mbps sebességű átvitelt biztosít szoftveres úton konfigurálható modulációs sémával (QPSK, 16,32, 64, 128, és 256 QAM) és sokféle csatorna raszteren (10, 28, 30, 40, 50, és 56 MHz).

Ugyanez a rendszer képes 45-800 Mbps sebességű átvitelre az adott hálózati topológiára és konfigurációra optimalizált módon. A FibeAir 1500P a teljes 6-38GHz közötti frekvencia tartományban működik.

A berendezés upgrade-elése kisebb kapacitásról a nagyobbra egyszerűen megvalósítható egyazon 1U magas beltéri egységgel (IDU), mivel két melegtartalékolt rádió vivőmodul helyezhető el benne. Az IDU 1+0, 2+0, 2+2 Hot Standby elrendezést támogat tér és/vagy frekvencia diverzitivel.

A FibeAir 1500P közös csatornás duál polarizációs üzemmódban működik kereszt polarizációs interferencia elnyomás (XPIC) algoritmust használva. Két STM-1 jel továbbítása történhet egyetlen 28 MHz-es csatornán keresztül, függőleges és vízszintes polarizáció alkalmazásával. Ez dupla kapacitást jelent ugyanazon a sávszélességen.

A FibeAir 1500P tökéletesen integrálható bármely SDH/SONET, IP és ATM hálózatba, miközben az Ethernet és TDM interfészek sokaságát támogatja, úgymint nxE1, nxSTM-1, STM-4, nxFast Ethernet, és Gigabit Ethernet.

FibeAir 1500HP

Új generációs nagy távolságú vezeték nélküli rádiórendszer, mely különösen nagy távolságú összeköttetések kialakítására alkalmas.

Újdonságot jelent, hogy a FibeAir 1500HP az első olyan osztott kivitelű rádió, amely valódi nagy távolságú átvitelre optimalizált.

A Ceragon egyedülálló térdiverziti megoldása a két vivőmodulos architektúrával, a kiemelkedően magas adóteljesítmény, és a KF összegző algoritmus garantálják a magas performanciát, és a hibamentes átvitelt.

Az üzemeltetőknek mindez nagy megbízhatóságú megoldást biztosít, kevesebb berendezést és kisebb méretű antennákat tudnak használni, és ezzel jelentős költségmegtakarítás érhető el a kezdeti beruházási és az üzemeltetési költségekben egyaránt.

FibeAir 1500P-AES

EncryptAir – Az első beépített nagy kapacitású titkosított megoldás

Napjainkban egyre növekvő igény van a pont pont vezeték nélküli összeköttetéseken továbbított információk magas szintű védelmének biztosítása iránt, ezért a Ceragon kifejlesztette a védelem magasabb szintjével rendelkező FibeAir 1500P-AES termékcsaládját.

Az eszközök nagy biztonságú védelmet nyújtanak az illetéktelen lehallgatás ellen az air interfészen, valamint védenek a tetőkön elhelyezett eszközökhöz történő jogosulatlan hozzáférésekkel szemben.

Ez a gyártóspecifikus megoldás egy olyan rendszert jelent, amely az információ biztonság legmagasabb szintjét valósítja meg a vezeték nélküli médiumon keresztül anélkül hogy a link performancia, azaz az átvitel minősége romlana. Az integrált védelmi rendszerrel ellátott FibeAir 1500P-AES az első szolgátatói minőségben titkosított pont pont összeköttetés, amely iránt fokozott érdeklődés mutatkozik különösen a védelmi erők részéről.

A világ egyik vezető hadiipari óriásvállalata, az amerikai General Dynamics C4 Systems ez évben jelentős mennyiségű Ceragon FIPS140-2 biztonsági szabványnak megfelelő FibeAir 1500P-AES összeköttetést szállított az Amerikai Védelmi Erők (US Air Force) számára, melyek biztosítják a védelmi erők vezeték nélküli hang és adatáviteli szolgáltatásai magas szintű információvédelmét.

A FibeAir titkosított változatánál a vonali interfészen érkező nyílt titkosítatlan adatot kódolják és így kerül továbbításra a rádió csatornán keresztül. A túlvégi eszköz fogadjai a kódolt jelet, dekódolja az eredeti nyílt szöveg formátumra és továbbítja a vonalon a felhasználónak.

Az alkalmazott rejtjelzési eljárás az AES (Advanced Encryption Standard) algoritmust használja, ahogyan ezt FIPS 140-2 Level 2 biztonsági szabvány specifikálja.

Az AES egy 256 bites szimmetrikus kulcsú blokk kódolási eljárás, amelynél AES kódoló algoritmus az egy blokk hosszúságú 128 bites

titkosítandó adatot egy állapotmátrixba rendezi és ezen négyféle transzformációt hajt végre többször egymás után, ezzel biztosítva a magasfokú adatbiztonságot és nehéz feltörhetőséget.

Vezeték nélküli titkosítás

A rádiós összeköttetéseket titkosítani összetett feladat. Le kell szorítani a bit hibaarányt (BER) és a fading-et a rádiócsatornában, hogy a titkosítási folyamat hibamentesen megvalósuljon.

A titkosítatlan adatot a FibeAir beltéri egysége (IDU) kódolja és továbbítja a rádiófrekvenciás kültéri egységbe (ODU). A titkosított adat védi az információt a lehallgatás ellen. Az AES algoritmus alkalmazásával a Ceragon által biztosított magas minőségű rádiós átvitel valósul meg az összeköttetésen.

Az AES alkalmazása mellett a Ceragon titkosítási eljárása kiegészül egy saját fejlesztésű algoritmussal. Ez egy random kulcs generátorból és gyakran ismétlődő kulcs cseréből áll, valamint minden összeköttetés egyedi kulcskészlettel rendelkezik, amely lehetővé teszi több link hibamentes működését egyazon területen, anélkül hogy egymás információ átvitelét lehellgatnák.

Ez a FibeAir beltéri egységbe integrált rejtjelzési algoritmus tökéletes transzparenciát biztosít az üzemeltetőnek, automatikusan működik anélkül hogy manuálisan kellene betölteni és cserélni a kulcsokat.

FibeAir IP-MAX – a nagy kapacitású szolgáltatói minőségű vezeték nélküli Ethernet összeköttetés

A Ceragon széleskörű Ethernet megoldása Fast és Gigabit Ethernet vezeték nélküli átvitelre optikai átviteli minőségben.

A legnagyobb átviteli kapacitással rendelkező natív Ethernet megoldás a legkisebb késleltetést biztosítva optimális a nagy sebességű IP alapú alkalmazások megvalósítására, beleértve az IP-DSLAM csatlakoztatásokat a

triple play szolgáltatásokhoz, WiMAX hálózat felcsatlakoztatást és egyéb késleltetés-érzékeny alkalmazásokat.

Upgrade-elhető módon **50-400 Mbps** közötti kapacitást biztosít rádióvivő csatornánként, két vivő elhelyezésével a kapacitás **800 Mbps** –ra növelhető.

Főbb jellemzői:

- 6-38 GHz frekvenciákon áll rendelkezésre.
- Támogatott interfész választék: 10/100BaseT Ethernet vagy GbE adat portok és 8xE1, voice port dinamikus allokációval
- Konfigurációk: 1+0, 2+0, East-West, 1+1 hw védelem, frekvencia és tér diverziti
- Szoftveresen konfigurálható modulációs sémák: QPSK, 16, 32, 64, 128, 256 QAM
- 10-56 MHz raszter (egy vagy két vivős kialakítás)
- Osztott kivitelű vagy all-indoor kivitel

A FibeAir IP-MAX alkalmazási területe:

Nagy kapacitású Ethernet összeköttetést biztosít vállalati és kormányzati magánhálózatok (kampuszok, telephelyek összekötése, oktatási, katonai, pénzügyi szektor) valamint fix és mobil szolgáltatók részére.

A Ceragon FibeAir IP-MAX Gigabit Ethernet összeköttetést sikerrel alkalmaztuk az ez évi ZMNE COMMIT-2007 francia magyar híradó gyakorlaton a két bázis (Üllői út és Hungária krt) nagy sebességű IP összeköttetésének biztosítására.

További információ:

SCI-Network Távközlési és Hálózatintegrációs zRt.

http://www.scinetwork.hu/

Tel.: +361 467 7030

Fax: +361 467 7049

info@scinetwork.hu

CÉGISMERTETŐ

2007. március

A KOPINT-DATORG zRt.

A társaság cégneve:	KOPINT-DATORG Infokommunikációs zártkörűen működő Részvénytársaság
A társaság rövidített cégneve:	KOPINT-DATORG zRt.
A társaság postai címe:	1389 Budapest, Pf.: 133.
Központi telefonszáma:	459-4200
Központi telefax száma:	303-1000
Internetes honlapjának címe:	www.kopint-datorg.hu, www.kopdat.hu
Központi e-mail címe:	info@kopdat.hu
A társaság cégjegyzékszáma:	Cg. 01-10-041633
Adószáma:	10585560-2-42
Statisztikai számjele:	10585560-7230-114-01
Társadalombiztosítási folyószámla száma:	1188125
Bankszámla száma:	ING Bank 13700016-01527010-00000000 UniCredit Bank 10900028-00000005-31830004
A társaság törvényességi felügyeletét ellátó szerv:	Fővárosi Bíróság, mint Cégbíróság
A társaság alaptőkéje:	830 080 000 Ft, azaz: nyolcszázharmincmillió-nyolcvanezer forint.
Az Alapító Okirat kelte:	1991. július 1.
A társaság időtartama:	határozatlan

Tulajdonosi szerkezet:

Tulajdonos részarány

Tartós állami tulajdon a Miniszterelnöki Hivatal kezelésében 100 %

Foglalkoztatottak száma:

Redukált átlagos statisztikai állományi létszám: (2006) 145 fő

Év	értékesítés nettó árbevétele (MFT)
2001	1866
2002	2378
2003	3156
2004	3076
2005	2721
2006	3379

A Kopint-Datorg zRt. jogelődei révén 43 éves múltra tekint vissza. Az 1964-ben alapított Konjunktúra- és Piackutató Intézet (KOPINT) és az 1968-ban létrehozott Datorg Külkereskedelmi Adatfeldolgozó és Szervező Rt. 1987-ben történt összevonásával jött létre a Kopint-Datorg. Részvénytársasági formában 1991. július 1. óta működik, 2005 júliusától egyedüli tulajdonosa a magyar állam. 2005. november 22. óta „zártkörűen működő" részvénytársaság.

A társaság korábbi legfontosabb megrendelőit megtartva, és újabb üzleti partnereket megnyerve fokozatosan növekvő, stabil üzletmenetet alakított ki. Legnagyobb megrendelői államigazgatási szervek, országos hatáskörű intézmények voltak, de gazdálkodó szervezetek is igénybe vették szolgáltatásait, vásárolták termékeit.

2006-ban a szervezet – igazodva a megváltozott cégstratégiához – nagymértékben módosult: az informatikai tevékenység egy része és az ezzel foglalkozó szakember-gárda a társaság többségi tulajdonában álló Kopint-Datorg Informatikai és Vagyonkezelő Kft-be szerveződött át, a gazdaság-, piac- és stratégia-kutatás pedig a cégcsoporttól független szervezetekben folyik tovább.

A KOPINT-DATORG jellemzően a közigazgatási informatika dinamikusan fejlődő közegében működik. Az európai integrációba szervesen beépülő hazai közszféra előtt álló innovációs kihívások egyszersmind a Társaság kihívásai is.

A technikai és tartalmi üzemeltetők személyének kiválasztásánál alapkövetelmény a nemzetbiztonsági ellenőrzés megkövetelt szintjeinek való megfelelés.

Ma a Kopint-Datorg zRt. elsőszámú partnere a kormányzati szektor, azon belül is a Miniszterelnöki Hivatal. Stratégiai céljai között első helyen az e-közigazgatási megoldások támogatása áll.

A társaság főbb tevékenységei

- a Kormányzati Portál és ehhez kapcsolódó rendszerek (Ügyfélkapu) üzemeltetése és fejlesztése;
- az Elektronikus Kormányzati Gerinchálózat üzemeltetése és fejlesztése;
- más informatikai rendszerek fejlesztése és üzemeltetése (közösen többségi tulajdonában lévő vállalatával, a Kopint-Datorg Informatikai és Vagyonkezelő Kft-vel);
- e-kormányzati elemzések és tanácsadás;
- műszaki kutatás.

A felhalmozódott tapasztalat, az informatikai-távközlési felkészültség, a makrogazdasághoz is értő szakértők egy szervezeten belüli koordinált tevékenysége komplex feladatok jól megalapozott megoldására is alkalmassá teszik a Kopint-Datorg cégcsoportot

A Kopint-Datorg szolgáltatásait az informatika és telekommunikáció élvonalbeli eszközeinek alkalmazásával és új, saját fejlesztések megvalósításával igyekszik a legkorszerűbbé tenni.

Minőségbiztosítási rendszer

A Kopint-Datorg fontosnak tartja, hogy megbízható és magasan kvalifikált partnere legyen mindenkori ügyfeleinek, és szakmai elvárásaiknak minden területen megfeleljen. A vevői megelégedettség biztosítása érdekében a vezetés rendszeresen értékeli a szervezet minőségi munkavégzéssel kapcsolatos eredményeit is, és ehhez igazítja minőségcéljait.

A társaság alkalmazottai tanulással, és a munka minőségének állandó javításával szélesítik a szolgáltatások választékát és biztosítják megbízhatóságát. A fenti törekvések megvalósítását elősegítő elemként a Társaság 1998-ban szerezte meg először a minőségügyi tanúsítványt. Valamennyi tevékenység, így a szoftverfejlesztés, programozás, szoftvertesztelés, - karbantartás, adatfeldolgozás, távközlési üzemeltetés, e-kormányzat kutatás is az ISO 9001:2000 szabvány követelményeinek megfelelően folyik. Ez a Kopint-Datorg megrendelőinek nem csak a fejlesztés végeredményét jelentő termék megbízható működésére, megjelenésére jelent garanciát, hanem a fejlesztés eseményeinek egyértelmű hivatkozási alapot szolgáltató dokumentálására is.

A TÜV CERT tanúsítvány nyilvántartási száma: 75 100 7314. A jelenleg érvényes tanúsítványt a TÜV Rheinland InterCert Kft. rendszertanúsító helye bocsátotta ki.

A Társaság tevékenységét a minőség alakulásának állandó figyelemmel kisérése jellemzi. A projektek indításakor a minőségbiztosítási feladatokat kiemelt fontossággal kezelik, a feladatok megtervezésére ill. végrehajtására a projekt méretétől függően külön szakembert/szakember csoportot biztosít a cég. Emellett az ügyfelek igényeinek megfelelően nyújt informatikai projektek során külön minőségbiztosítást is.

A FŐBB TEVÉKENYSÉGEK ISMERTETÉSE

A Kormányzati Portál ÉS AZ ÜGYFÉLKAPU fEJLESZTÉSE ÉS ÜZEMELTETÉSE

Formázott: Felsoro
számozás

Alkalmazásmenedzsment, szoftverfejlesztés

A magyar közigazgatási rendszerek alapja egy moduláris struktúrájú rendszer (a „Központi Rendszer”). A különböző funkciókat heterogén környezetben működő, nyílt technológiákon alapuló modulokon futtatjuk. A modul struktúrának köszönhetően nem csak nagyobb teljesítmény érhető el, hanem a fejlesztés során is jobban szétválaszthatóak a különböző feladatok. A magasabb szintű folyamatok (pl. folyamatirányítás, rendszerfelügyelet, naplózás stb.) vezérlését egy integrátor modul végzi, amely mindegyik modullal közvetlen (web-szolgáltatásokon alapuló) kapcsolatban van. A hozzáférhető szabványok és megoldások alkalmazása a rendszer fejlesztésének főleg implementációs és teszt fázisában kerül előtérbe. A követelmény-felmérés, elemzés és tervezés fázisában inkább kereskedelmi termékek jönnek szóba.

A Kormányzati Portál és az Ügyfélkapu folyamatos fejlesztése lehetővé teszi a kormányzati és a közigazgatási e-szolgáltatások bővítését, a kormányzati hírek, információk, adatok széleskörű terjesztését, az EU közigazgatási e-szolgáltatásokra vonatkozó előírásainak teljesítését. A fejlesztők - igény esetén - más kormányzati honlapok kialakítását is támogatják. Központi eleme olyan alkalmazások kialakítása, amely az állampolgárok számára folyamatosan biztosítja információs szabadságjogaik kiteljesítését egy messzemenően biztonságos közigazgatási informatikai térben. Az Ügyfélkapu elsődleges feladata (hiteles személyazonosítás) magával hozta az önkormányzatok elektronikus rendszereinek a Központi Rendszerhez való csatlakozását. A csatlakozás előkészítése, szoftvertechnikai megvalósítása szintén a Kopint-Datorg feladatai közé tartozik. A fejlesztési munkák a legszigorúbb biztonsági körülmények között, zárt labor-, központi fejlesztői-, és teszt rendszerekben történnek, ISO minőségbiztosítás alatt. A biztonsági és minőségi megfelelőség a cég minden alvállalkozójára kötelező érvényű.

A portálok

A Társaság által, részben szabad szoftverek felhasználásával fejlesztett és üzemeltetett honlapokat szakértő munkatársak, szerkesztők frissítik, biztosítják az információk teljességét.

A fejlesztett és üzemeltetett közigazgatási portálok közül a legnagyobb a Kormányzati Portál (www.magyarorszag.hu), ami az elektronikus kormányzati szolgáltatások centruma (így az Ügyfélkapué is). Működtetésének alapvető célja, hogy az állampolgárok számára lehetővé tegye az internetes kapcsolattartást a közigazgatással, ugyanakkor működésével és felépítésével szabványt alkot a közigazgatási honlapok és ágazati portálok számára.

A Kormányzati Portál teljes mértékben megfelel az Európai Bizottság "i2010"-közleményében foglalt az interoperabilitásról, az esélyegyenlőségről és a digitális jogbiztonságról szóló követelményeinek. Az üzemeltetés teljes folyamata az ISO 9001:2000 szerint tanúsított, folyamatos, független adatvédelmi kontroll alatt áll.

A Kormányzati Portál főbb profiljai:

- az Ügyfélkapu megjelenítése, működtetése, és a hozzá kapcsolódó ügyfélszolgálat támogatása;
- köz- és államigazgatási információk gyűjtőhelye;
- e-szolgáltatások gyűjteménye;
- állampolgári közszereplést biztosító, személyes azonosításon alapuló Fórum.

A Kormányzati Portál a szolgáltatásokra és az ügyekre, ügyleírásokra, valamint a köréjük szerveződő információkra épül. Az élethelyzeteknek megfelelő ügyleírásokból közel ezer található a portálon. Mindezt katalógusos formában, a felhasználói státusz szerint teszi elérhetővé. Ennek megfelelően vannak információk állampolgároknak, vállalkozóknak és a közigazgatás szereplőinek.

Emellett létezik általános tájékoztatás: Kapcsolat, Hivatalok, Hírközpont, Országinfó, Európai Unió és a Mellékletek.

Az Ügyfélkapu

A Kormányzati Portálon üzemelő Ügyfélkapu a magyar kormányzat elektronikus ügyfélbeléptető és azonosító rendszere. Segítségével a felhasználók egyedi személyi azonosítójukkal elektronikus úton, biztonságosan és hitelesen azonosítva léphetnek kapcsolatba a hatóságokkal, közigazgatási szervekkel, és ügyeiket elektronikusan intézhetik. Kormányzati és közigazgatási adatbázisokat, lokális hálózatokat és informatikai rendszereket kapcsol össze, és különböző kormányzati szolgáltatások elérhetőségét biztosítja a magánszféra számára is.

Az Ügyfélkapun 2007. májusáig közel 540 ezren regisztráltak. A rendszer közigazgatási környezete rohamosan fejlődik, két év alatt elérte a

magyarroszági magánszemélyek 20%-át, és a vállakozások 100%-át. Jelenleg az Ügyfélkapun keresztül érkezik havonta több százezer vállalkozás adó- és járulékbevallása, valamint adatszolgáltatása, azon keresztül folyik a foglalkoztatottak bejelentése, a nyugdíj e-ügyintézése, a TAJ-szolgáltatások, az elektronikus felvételi, az adatszolgáltatás letiltása. A rendszer folyamatosan bővül új szolgáltatások bekapcsolásával: 2007-ben csatlakoznak az önkormányzati e-szolgáltatások, és az e-NYENYI-rendszer.

Fórum

A Kormányzati Portálon az állampolgárok közszereplést is vállalhatnak: az Ügyfélkapun keresztül azonosítva a hozzászólók olyan kommunikációs térbe kerülnek, amely garantálja számukra a megszólalók őszinteségét, ugyanakkor a fórumozók hozzászólásaik büntetőjogi felelősségét is vállalják. Az állampolgárok nevesített magánszemélyként ezen a felületen nyilvánosan kommunikálhatnak a közigazgatási szervekkel is.

Egyéb honlapok

A Kopint-Datorg több közigazgatási honlapot fejlesztett, üzemeltet. A legfontosabbak: a Miniszterelnöki Hivatal, az Államreform-bizottság, a Kormányzati Személyügyért Felelős Államtitkárság, az Elektronikuskormányzat-központ, és a Gönczöl-bizottság honlapjai.

Az Elektronikus Kormányzati Gerincháló üzemeltetése

Formázott: Felsoro
számozás

A Társaság heti 7*24 órában üzemelteti a nemzetbiztonsági és nemzetstratégiai jelentőségű Kormányzati Elektronikus Szolgáltató Rendszert (KR). Ezen belül kiemelt fontosságú az Elektronikus Kormányzati Gerinchálózat (EKG), ami kapcsolódik az Európai Unió ún. TESTA ("Trans-European Services for Telematics between Administrations") hálózatához, amely az Európai Unió adminisztrációja és a tagországok kormányzatai közötti adat- és információcserét teszi lehetővé, valamint az Ügyfélkapu. Ennek az alapinfrastruktúrának a megteremtésével vált lehetővé a kormányzati rendszerek elektronizálása, új, hatékony, távolról is elérhető szolgáltatási rendszerek bevezetése, az e-kormányzat kialakítása, az informatikai biztonsági központ működtetése. Az Ügyfélkapu a Központi Rendszerben 2007 első félévében - a magyar közigazgatási informatikában eddig példátlan nagyságrendben – havi 2-3 millió bevallást, illetve adatközlést fogadott be.

A Társaság infokommunikációs támogatást nyújt intézményi szakrendszerek működéséhez is, az állami vagyon tételeiként nagy mennyiségű informatikai eszközt tart nyilván. Ez a szám - 2002 és 2006 között - kevesebb, mint négy év alatt a nyolcszorosára emelkedett.

Más informatikai tevékenységek

A Kopint-Datorg informatikai szakemberei több mint harminc éve vesznek részt államigazgatási intézmények és vállalkozások informatikai rendszereinek kidolgozásában és üzemeltetésében.

A cégcsoport az informatikai jellegű feladatok megoldására az elvi megfogalmazástól a hardver és szoftver eszközök beszerzésén, az egyedi igényeket kielégítő alkalmazások kifejlesztésén, a típusszoftverek készítésén át az üzemeltetésig – tehát a teljes vertikumra - vállalkozik. A Társaság számos - ma is sikeresen működő - egyedi rendszert alakított ki. Az informatikai tudás mellett a gazdaságirányítás szakmai követelményeit is teljesíteni tudta, mivel kvalifikált közgazdasági kutatás is folyt a cégnél. Ilyen egyedi, összetett megoldások elsősorban a közigazgatásban jellemzőek.

Szoftverfejlesztés

A cégcsoport munkatársai nagy tapasztalattal és sokéves gyakorlattal fejlesztenek nagy méretű adatbázisokon alapuló adatfeldolgozó rendszereket. A fejlesztéseket a legújabb eszközök és módszerek felhasználásával végzik. Ide sorolható fő referencia-munkák: a KSH részére Intrastat és Extrastat statisztikai adatfeldolgozó rendszerek, valamint a Szolgáltatás-külkereskedelmi statisztika adatgyűjtő rendszere, komplex engedélyezési rendszer teljes IT megoldása a Magyar Kereskedelmi Engedélyezési Hivatal részére.

Üzemeltetés

- Alapszoftver rendszergazdai tevékenység
- Adatbázis-adminisztrátori tevékenység
- Alkalmazást felügyelő rendszergazda biztosítása
- Szerviz szolgáltatás

Referenciák: KSH: adatgyűjtés, adatfeldolgozás és IT-üzemeltetés,

MKEH: engedélyezési rendszer IT üzemeltetése

Korábbi és jelenlegi szoftvereink

Külkereskedelmi Termékforgalmi Statisztika

A Kopint-Datorg 1968-tól vett részt az országos külkereskedelmi termékforgalmi statisztika kialakításában és üzemeltetésében, a Gazdasági és Közlekedési Minisztérium és jogelődei, majd 2002 májusától a KSH megbízásából. A Társaság kidolgozta a KSH igényeinek és az Európai Unió követelményeinek megfelelő INTRASTAT rendszer fizikai rendszertervét, elvégezte az informatikai megvalósítására irányuló feladatokat, az Extrastat és Intrastat projekteket kivitelezte, a rendszereket üzemelteti. A feladatokat

Formázott: Felsorolás és számozás

Formázott: Felsorolás és számozás

Formázott: Felsorolás és számozás

Formázott: Felsorolás és számozás

a Kopint-Datorg Informatikai és Vagyonkezelő Kft-vel együttműködve hajtja végre a cég.

Szolgáltatás-külkereskedelmi Statisztika

A szolgáltatás-külkereskedelmi statisztika az exportőrök/importőrök által időszakonként benyújtott - a szolgáltatás-exportot-importot regisztráló - adatlapok adatai alapján készült.

Külkereskedelmi engedélyezési rendszer

A külkereskedelmi engedélyek nyilvántartását, elbírálását, a teljesítésigazolások nyilvántartását és a határozatok elkészítését támogató ügyviteli rendszer, amely a Magyar Kereskedelmi Engedélyezési Hivatalban működik. A rendszer a külkereskedelmi szabályozások, piacvédelmi intézkedések gyakori változásaihoz alkalmazkodva rugalmasan paraméterezhető. Kiemelendő, hogy az EU Bizottság központi informatikai rendszeréhez való adatátviteli és ügyviteli csatlakozást először az általunk fejlesztett komplex engedélyezési rendszer valósította meg.

Váminformatikai szoftverek

A Vám- és Pénzügyőrség megrendelésére készült szoftverek a vámhivatalok, a regionális parancsnokságok és a Vám- és Pénzügyőrség Országos Parancsnoksága vám-, jövedéki igazgatási és folyószámla-kezelési feladatainak elvégzéséhez nyújtottak informatikai segítséget. (2005-től ez a tevékenység - áthelyezett munkatársaink révén - a VPOP keretein belül folyik.)

A szoftverek akkor 6 központi adatbázissal mintegy 250 vámkezelőhelyen, 57 jövedéki vámhivatalnál működtek.

OSAP rendszer

Az OSAP rendszer a kábítószerek és pszichotrop anyagok tiltott gyártásához is használt vegyi anyagokkal végzett tevékenységek szabályozásáról szóló rendelet hatálya alá tartozó ellenőrzött anyagok forgalmáról az Országos Statisztikai Adatgyűjtési Program szerinti éves statisztikai jelentések feldolgozását, nyilvántartását, a szükséges összesítéseket, kimutatásokat támogató, feldolgozó, összesítő szoftver.

Belkereskedelmi Idegenforgalmi Feladatok Információs Rendszere (BIFIR)

A BIFIR a belkereskedelmi és idegenforgalmi tevékenységek nyilvántartására, a határozatok elkészítésének támogatására alkalmas ügyviteli rendszer, ami a Gazdasági Minisztérium Engedélyezési és Közigazgatási Hivatala részére készült.

Agrárinformációs Rendszer

A Mezőgazdasági és Vidékfejlesztési Hivatal alaptevékenységeit ellátó egységes, integrált, operatív informatikai rendszer.

Bírósági Integrált Információs Rendszer

Az Országos Igazságszolgáltatási Tanács Hivatala a bíróságok új, országos integrált információs rendszerének kialakítását célzó PHARE-tender lebonyolításával kapcsolatos szakértői tevékenység egy részének ellátására a Kopint-Datorg zRt.-nek adott megbízást, melynek keretében a Társaság elkészítette a rendszer részletes követelményjegyzékét, valamint folyamatosan biztosította a projekt során az alkalmazásfejlesztés követelményspecifikációnak történő megfelelőségét (minőségbiztosítás).

Országos Közhiteles Nyilvántartások

Az Országos Igazságszolgáltatási Tanács Hivatala megbízásából készült az Országos Közhiteles Nyilvántartások adatbázis-kezelő rendszere.

Prekurzorok Forgalmi Engedélyeit Lekérdező Rendszer

A Kopint-Datorg zRt. 2002 végén a GKM EKH-nál a kábítószerek és pszichotrop anyagok tiltott gyártásához is használt vegyi anyagokkal végzett tevékenységek szabályozásáról szóló rendelet hatálya alá tartozó ellenőrzött anyagok export–import engedélyezése céljából működő Prekurzorok Forgalmának Információs Rendszeréhez (PREFIR) kapcsolódó lekérdező rendszert fejlesztett ki.

Nemzeti számlák szerinti külkereskedelmi termékforgalom havi bontású adatbázisának kialakítása

A Kopint-Datorg zRt. fejlesztette a nemzeti számlákba beillesztésre kerülő külkereskedelmi termékforgalmi adatok kiegészítését szolgáló vizsgálati szoftvert, és kialakította a Nemzeti számlák szerinti külkereskedelmi termékforgalom havi bontású adatbázisát 1995-2002 évekre.

Főbb referenciáink és együttműködő partnereink, beszállítóink az infokommunikáció területén

Referenciáink a közigazgatásban:

- Miniszterelnöki Hivatal Elektronikuskormányzat-Központ
- Központi Statisztikai Hivatal
- Magyar Kereskedelmi Engedélyezési Hivatal
- Vám- és Pénzügyőrség Országos Parancsnoksága
- Mezőgazdasági és Vidékfejlesztési Hivatal
- Foglalkoztatási Hivatal
- Földművelésügyi és Vidékfejlesztési Minisztérium
- Gazdasági és Közlekedési Minisztérium
- Külügyminisztérium
- Oktatási Minisztérium
- XII. kerületi Önkormányzat

Együttműködő partnereink, beszállítóink:

- SAGEM Magyarország Kft.
- ICON Zrt.
- Magyar Telecom NyRt.
- Netlock Kft.
- Sun Microsystems Kft.
- Egroup Kft.
- PanTel Kft.
- KFKI-LNX Zrt.
- IDOM2000 Zrt.
- Cisco Networks
- Oracle Hungary Kft.

e-közigazgatási elemzések, tanácsadói tevékenység

2007. január 1-étől ugyan megszűnt a társaságnál az alkalmazott gazdaságkutatói tevékenység, a korábban e-közigazgatási elemzéssel foglalkozó munkatársak egy új szervezeti egységet alkotva, továbbra is szakértői támogatást nyújtanak az elektronikus kormányzat magyarországi fejlődésének, a közigazgatási informatika stratégiai irányai meghatározásának és programtervezésének területén. Ezen belül fontos kompetencia maradt a hazai fejlesztési elképzelések ütköztetése az összehasonlítható külföldi gyakorlatokkal és ajánlásokkal. Az elemzők igény esetén a többi üzletágat segítik a döntések előkészítésében, és az eredmények gazdasági-társadalmi hatásainak értékelésére vonatkozó tanulmányok elkészítésében. Széles körű kutatási tapasztalattal rendelkeznek az információs társadalom témájában.

Az e-közigazgatási elemző és tanácsadó tevékenység kiterjed

- az információs társadalom fejlődésének vizsgálatára – annak mind nemzetközi, mind a magyar vonatkozásaira,
- az infokommunikáció nemzetközi tapasztalatainak a hazai viszonyokra történő adaptálására,
- hazai és nemzetközi e-közigazgatási megoldások nyomon követésére, azok hasznosítására projekt-támogatások és megvalósíthatósági tanulmányok keretében,
- államigazgatási szervezetek számára döntéselőkésítő háttértanulmányok készítésére.

Folyamatban lévő tevékenységek:

- A Bevált Gyakorlatok Műhelye (BGyM) működtetése, közigazgatási benchmarking:
- az Európai Unió égisze alatt működő Good Practice Framework hálózattal kialakított kapcsolatrendszer alapján a magyar e-közigazgatás számára hasznosítható legújabb nemzetközi gyakorlatok közvetítése, ma-

gyar nyelvű összegzése, valamint a magyar közigazgatásban kialakított gyakorlatok gyűjtése, tárolása, ezek értékelési és minősítési rendszerének kialakítása.

- Részvétel az EU FP6-os programja által finanszírozott OneStopGov projektben (élethelyzet-orientált keretrendszer és platform az egyablakos kormányzat számára).

Válogatás eddigi, releváns kutatásokból:

- Az eMagyarország pontok jövője (2006)
- Szélessávú Internet kiépítése Jász-Nagykun-Szolnok megyében – Társadalmi-gazdasági felmérés (2006)
- Szélessávú Internet kiépítése Hajdú-Bihar megyében – Megvalósíthatósági tanulmány (2006)
- Tanulmány a Magyar Posta Zrt.. Nemzetközi Üzletága által megadott egyedi ügyfelek körében, telefonon végzett ügyfél-elégedettség vizsgálat tapasztalatairól (2006)
- A közigazgatás hatékonysága mérésének módszerei, különös tekintettel a nemzetközi összehasonlításokat végző intézmények által alkalmazott elemzési, illetve adatbeszerzési gyakorlatra (2005)
- Összefoglaló tanulmány az e-kormányzati szolgáltatások monitoringjáról (2004-2005)
- Gyorsjelentés a Synergon image-kutatásról a cég jövőbeni terjeszkedésének fő célpontjait jelentő kkv-k vezetői körében (2005)
- Szabolcs-Szatmár-Bereg megye kommunikációs infrastruktúrájának korszerűsítésére vonatkozó megvalósíthatósági tanulmány (2004)
- Az információs szabadság (Freedom of Information) európai uniós gyakorlatának feltérképezése (2004)
- „eTartalom: Piaci Iránytű" (2004)
- Magyar Információs Társadalom Stratégia és Monitoring /államigazgatási felmérés/ (2003, 2004)
- Közösségi Internet hozzáférési pontok: külföldi tapasztalatok: a hazai pontok adatbázisának összeállítása, tipizálása, és térbeli megjelenítése: egy döntéstámogató monitoring rendszer megalapozása (2003)
- Intézményi adatgyűjtés a központosított közbeszerzési rendszerrel kapcsolatos igényekről (2003)
- Elektronikus aláíráshoz és alkalmazásaihoz kapcsolódó piacokat bemutató piaci monitoring jelentés módszertanát megalapozó kutatás (2003)
- Intézményi adatgyűjtés a központosított közbeszerzési rendszerrel kapcsolatos igényekről (2003)

- Az infokommunikáció kormányzati irányításának nemzetközi tapasztalatai: az intézmények, az államigazgatás kapcsolatai a vállalatokkal és a lakossággal (2002)
- A kis- és középvállalkozások bejuttatása a beszállítói piacra (2002)
- Országos Piaci Agrárinformációs Rendszer (OPAR) - Pilot-projekt (2002)
- Az Európai Unió nemzeti hírközlési hatóságai információgyűjtési mechanizmusa, annak jövőben várható változásainak irányvonalai (2001)
- Az információs társadalom versenyszabályozási követelményei az EU irányelvek alapján (lisszaboni deklaráció) (2001)
- Elektronikus ügyintézéssel kapcsolatos lakossági attitűd és véleménykutatás (2001)
- Elektronikus Közbeszerzési Rendszer használatához szükséges infrastruktúra felmérése (2001)
- Az Elektronikus Kormányzati Gerinchálózat kialakítását megalapozó kutatás (2001)
- Pedagógusok és köztisztviselők informatikai kultúrájának és eszközellátásának fejlesztési lehetőségei állami segítséggel
- Elektronikus ügyintézéssel kapcsolatos lakossági attitűd és véleménykutatás (2001)
- Az infokommunikáció kormányzati irányításának nemzetközi tapasztalatai (2000)
- Háromhavonta ismétlődő monitoring kutatás, az évezredváltással kapcsolatos várakozások, illetve a tájékoztatással, felkészítéssel kapcsolatos vélemények, attitűdök vizsgálata a lakosság körében (2000)
- Információs Társadalom /a magyar informatikai piac szereplői körében végzett primer kutatás/ (2000)
- Fogyasztói szokás vizsgálat a Szerencsejáték Rt. vevői körében (2000)

EGYÉB INFORMÁCIÓK

Alkalmazott számítástechnikai eszközök

A cégcsoport az informatikai rendszerek fejlesztésénél alkalmazott szoftvereszközök kiválasztásakor folyamatosan igazodik a szoftvertechnológia fejlődéséhez.

A fejlesztő szakemberek

A cégcsoport szakemberei informatikai rendszerszervező, folyamatszervező, programozó matematikus és programtervezői képesítéssel rendelkeznek. A programozási feladatok megoldásához - azokhoz igazodva - a különböző programnyelvek széles skáláját alkalmazzák a programozók.

Hardver eszközök

A fejlesztési, üzemeltetési feladatok ellátásához használt hardver eszközöket a feladatok optimális ellátásához szükséges minőségben és mennyiségben szerzi be és korszerűsít a Társaság, figyelembe véve a technika fejlődési tendenciáit.

ELISMERÉSEK

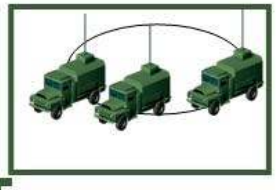
1. A világ vezető hálózatgyártójának, a Cisco Systems Inc. 2004. évi Networkers konferenciáján az első alkalommal meghirdetett "Operational Excellence" kategóriában közel 200 ország jelöltje közül a Társaság vehette át a „Networkers Innovation Award" díjat az EKG kifogástalan üzemeltetéséért - olyan vállalatokat és intézményeket megelőzve, mint a Deutsche Telekom, a Nestlé Global Center, a Statoil vagy az Egyesült Arab Emirátusok Egészségügyi Minisztériuma.
2. Az Üzemeltetési Divízió 2004 decemberében elnyerte a Kiváló Hálózatüzemeltető Díjat az EMEA régióban, amely 128 országot foglal magában (Európa, Közel-Kelet, Afrika).
3. 2004-ben a társaság egyik igazgatója lett a Hírközlési Tudományos Egyesület által adományozott „Az Év Projektmedzsere" cím birtokosa. Ugyanebben az évben a Társaság elnyerte a CISCO Premier Partnerség fokozatot.
4. A Kormányzati Portál a Magyar Marketingszövetség „Az Év Honlapja 2005"-díját kapta a „Kormányzat és Települések" kategóriájában.
5. A portál a Magyar Tartalomipari Szövetség „eFestival Hungary 2005" versenyének II. helyezését érte el a „Közérdekű Információszolgáltatás" kategóriában.
6. A portál 2005-ben Hannoverben az „Európai Kiválóság a Multimédiában" díj ezüst fokozatát kapta.
7. A portál fórumának eGames részprojektje az EU „eEurope Awards for eGovernment 2005 - Good Practice in Transforming Public Services" pályázatának döntős résztvevője lett Manchesterben a „Transforming Public Services eGovernment eEurope Awards-2005" konferencián.
8. Az ENSZ 2005. évi, elektronikus kormányzati szolgáltatásokat elemző jelentése példaként állította a kormányzati portál világszínvonalúnak ítélt szolgáltatásfejlesztését és fórumszolgáltatását.

Budapest, 2007. május

WIMAX & ARMY MOBILE INFRASTRUCTURE

WiMAX for army: a wide range of applications

Command Posts



Tactical Command Posts

Point-to-Point & backhaul

Office & Headquarter

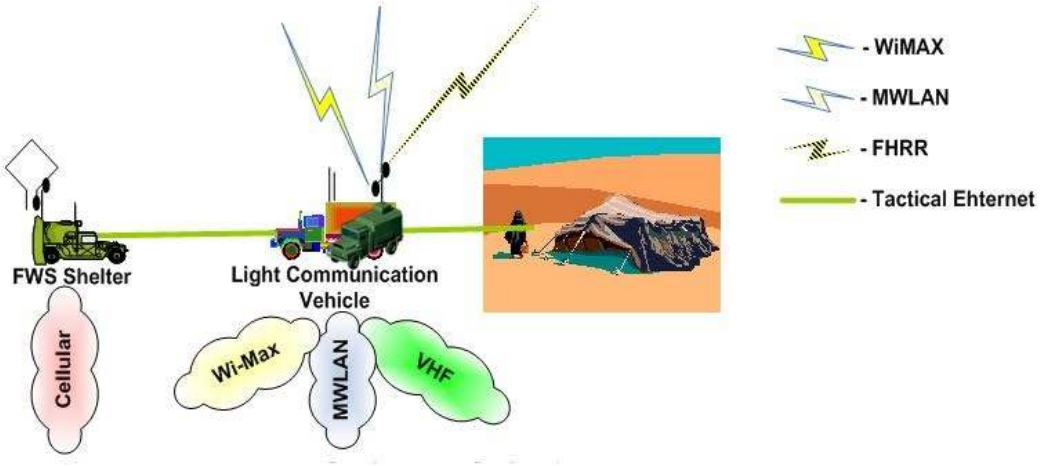
Acquisition & observation

All Rights Reserved © Alcatel-Lucent 2007

Alcatel·Lucent

Example: TCS program for digitisation of army corps - deployment concept

WiMAX Base Stations could be installed in Divisions, Brigades, and Battalions Command Posts to create on the move multimedia capabilities and backhauling redundancies



All Rights Reserved © Alcatel-Lucent 2007

Alcatel-Lucent WiMAX solution in the Army : recent demonstrations

Russia (May 2007)

Tests on the move on a Jeep : 100 km/h uplink @ 512 kps

Hungary (May 2007) : COMMIT 2007 Exercise

2 BS deployed.

One on a tactical mast

World premiere interconnection of TBMSS, ISDN, Satellite on WiMAX

Video, data transmission on the move (pieton)

All Rights Reserved © Alcatel-Lucent 2007

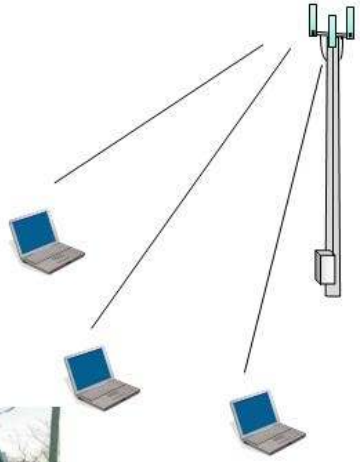
Alcatel·Lucent

WiMAX Alcatel-Lucent BS on a military vehicle

All Rights Reserved © Alcatel-Lucent 2007

Alcatel·Lucent

WiMAX Peace-Keeping : Fast deployment-Natural Disasters

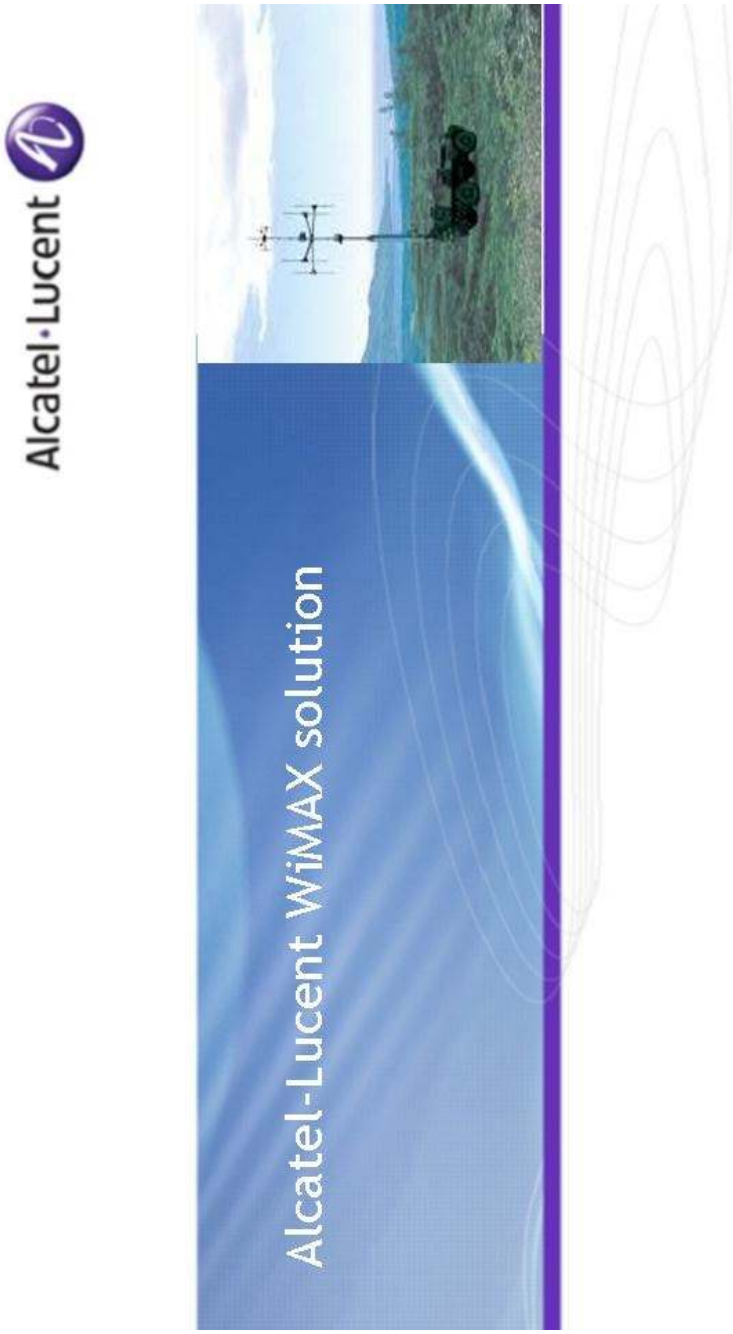


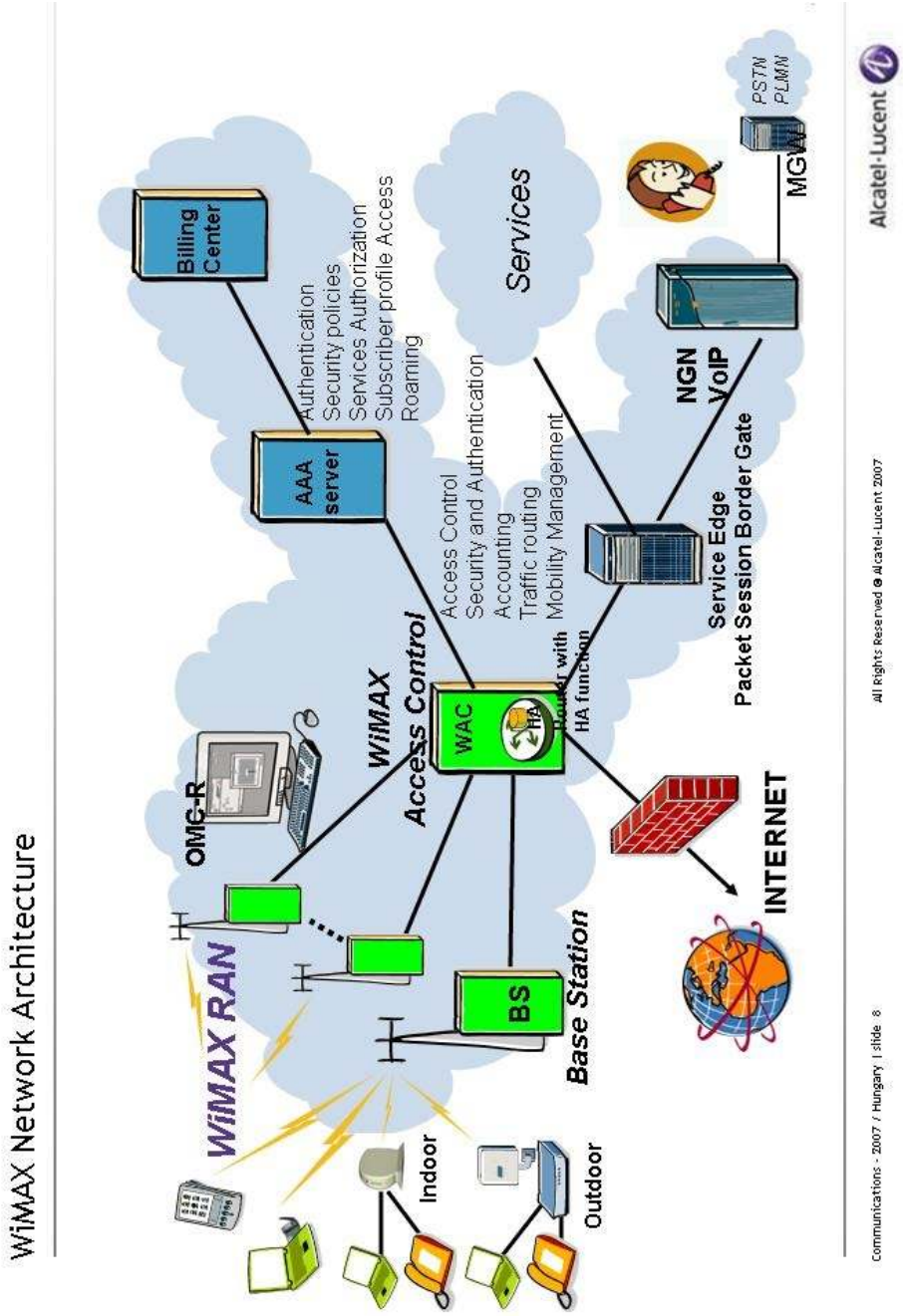
Katrina Huricane

- Real time Images from planes sent to ground military engineering forces
- Communications to seek for missing families

All Rights Reserved © Alcatel-Lucent 2007

Alcatel·Lucent


Alcatel·Lucent
Alcatel-Lucent WiMAX solution


WiMAX Network Architecture
Billing Center
Authentication
Security policies
Services Authorization
Subscriber profile Access
Roaming
AAA server
Services
PSTN
PLMN
MGW
NGN
VoIP
Access Control
Security and Authentication
Accounting
Traffic routing
Mobility Management
Service Edge
Packet Session Border Gate
WiMAX
Access Control
WAC
HA
Router with
HA function
OMC-R
INTERNET
WiMAX RAN
BS
Base Station
Indoor
Outdoor
Alcatel·Lucent
Communications - 2007 / Hungary | slide 8
All Rights Reserved © Alcatel-Lucent 2007

Alcatel-Lucent WiMAX BS on a tactical mast

1. A diversified Base Station portfolio

- Tailored for maximum coverage
- Adapted for low to high density areas
- Multi Carriers & Multi Standard
- Indoor & outdoor matching all sites conditions (-33°C to +45°C)

2. High Radio performance

- High Output Power (35 dbm)
- Advanced Antenna Technology : Beamforming + MIMO > coverage+capacity

3. Flexible/easy to install & operate

- Light and compact equipment easing transportation and deployment (32kg/54l)
- Plug and play feature (auto-connection)
- Complete Operation & maintenance tool including localization

40' for installation

All Rights Reserved © Alcatel-Lucent 2007

Alcatel·Lucent

Examples of devices available from our Open CPE partners

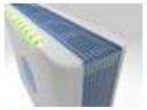
For nomadic and mobile usage

- **PCMCIA**

- **Compact Flash**

For fixed and portable usage

- **Simple CPE**
  - Indoor Self-install
  - VoIP
  - 1 Ethernet & 1 POTS plug



- **Multi-Users CPE**
  - Indoor Self-install
  - VoIP
  - 4 Ethernet & 2 POTS plugs
  - WiFi Access Point

- **Outdoor CPE**
  - High gain outdoor antenna
  - VoIP
  - 4 Ethernet & 2 POTS plugs
  - WiFi Access Point

WiMAX ruggedized CPE for Military applications

Ruggedised WiMax Terminal

All Rights Reserved © Alcatel-Lucent 2007

Alcatel·Lucent

Alcatel-Lucent WiMax WAC (Wireless Access Controller)
a very small footprint solution

BS

ASN
Network interface

OMC-R

AAA

DHCP/DNS

HA

Power supply

Legacy 802.16e solution
(Core Network)

✓ Ready for transportable & tactical use cases

✓ Improved Reliability

ASN, AAA, DHCP, HA servers integrated in a single computer

✓ Improved performances

All WiMAX network functions integrated on a single laptop

All Rights Reserved © Alcatel-Lucent 2007

Alcatel·Lucent

Alcatel-Lucent WiMAX Deployments

12
Regional and National Deployments Awards since January 2007

>70
Trials & Deployments

Telmex, Chile & LAM
Wireless DSL expansion & mobile evolution projects

India
Ramping up C-Dot-Alcatel Research Center
Field trials launched with major operators

Russia & CIS

Korea Telecom, Korea
Wimax Reality Center

BellSouth, USA

Other major operators in:
- Brazil
- Angola
- Venezuela
- Moldavia
- Ukraine
- Greece
- Philippines
- Nigeria ...

Acca, Japan

Primus, Canada

Onemax Dominican Republic

Chunghwa Telecom Taiwan

Maxis, Malaysia

WiMAX Telecom, Austria, Slovakia & Croatia

SHD, France

Lebanon
Contract with Tier 1 ISP for nationwide network deployment

Pakistan
Contract for 1st Market Launch in 2 cities

References in pink are awards

All Rights Reserved © Alcatel-Lucent 2007
Alcatel·Lucent

www.alcatel-lucent.com

Antók Péter:

HÁZIG VEZETETT FÉNY

(EGY MEGOLDÁS A FTTH-RA)

TÁVKÖZLÉS

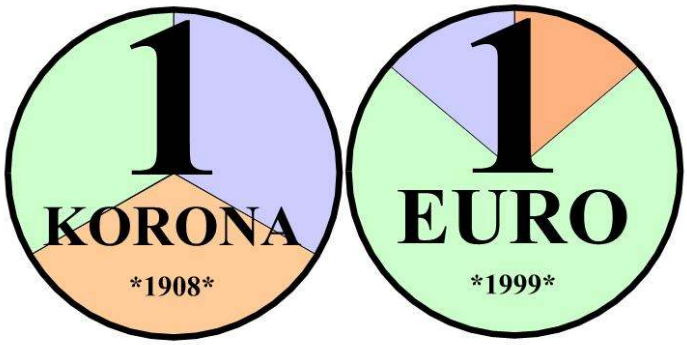
A világ legnagyobb, működő emberi alkotása

TÁVKÖZLÉS

A világ harmadik leggyorsabban megtérülő beruházása

ZMNE Kommunikáció 2007 3

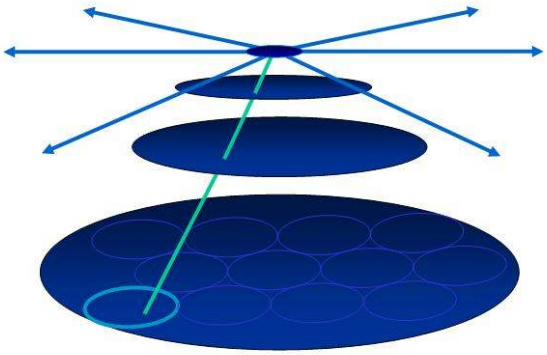
TÁVKÖZLÉS



Épület + technika + hálózat

ZMNE Kommunikáció 2007 4

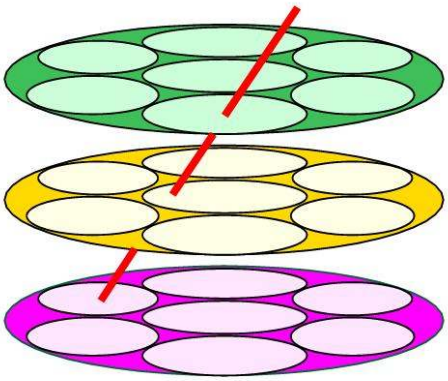
TÁVKÖZLÉS



Síkokra szervezett hálózat

ZMNE Kommunikáció 2007 5

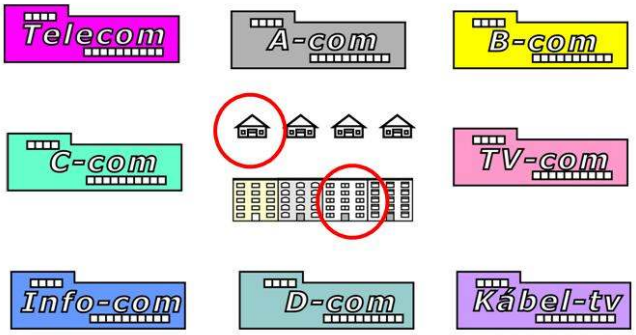
TÁVKÖZLÉS



Több szolgáltatós hálózat

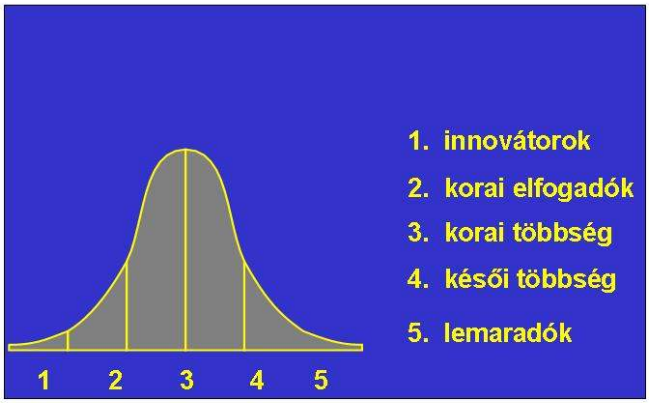
ZMNE Kommunikáció 2007 6

TÁVKÖZLÉS + INFORMATIKA



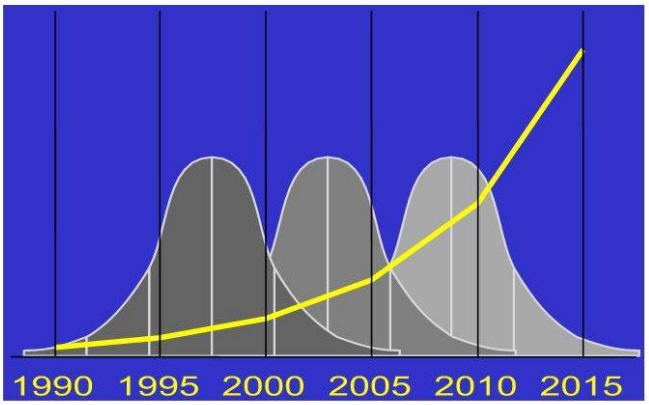
Verseny

TECHNOLÓGIA FEJLESZTÉS



Fogyasztói elfogadás

TECHNOLÓGIA FEJLESZTÉS



Sávszélesség igény

KORLÁTOS ERŐFORRÁS

-Frekvencia

-Azonosító

-Nyomvonal

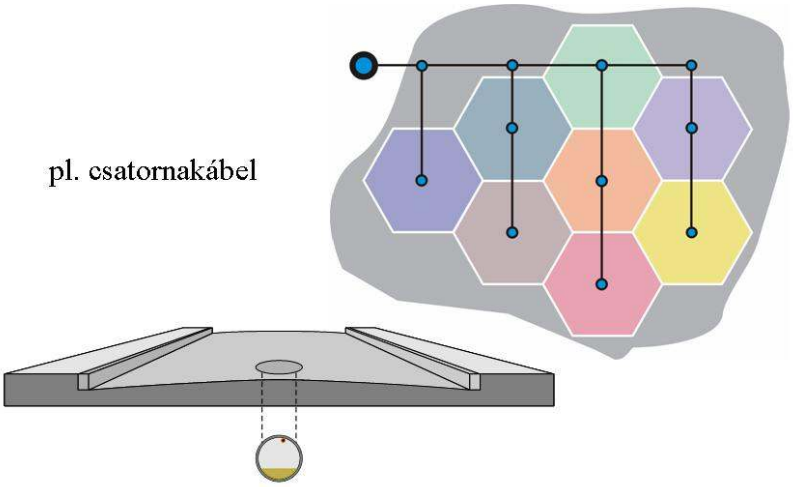
KORLÁTOS ERŐFORRÁS

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

ZMNE Kommunikáció 2007 11

ÚJ NYOMVONAL ?

pl. csatornakábel



ZMNE Kommunikáció 2007 12

MEGOLDÁS:

ÚJ ALÉPÍTMÉNYI HÁLÓZAT STÍLUS

ZMNE Kommunikáció 2007 13

ÚJ ALÉPÍTMÉNYI HÁLÓZATI STÍLUS

CÉL:

-piaci környezetben,

-közterületen,

-távközlési-, adat- és műsorelosztó kábeleket befogadó, földalatti hálózati infrastruktúra

ZMNE Kommunikáció 2007 14

ÚJ ALÉPÍTMÉNYI HÁLÓZATI STÍLUS

CÉL:

-Elsősorban belterületi, földalatti csőhálózat,

-Biztosítja a piaci résztvevők szabadságát,

-Növeli az érdekérvényesítési lehetőséget

-Csökkenti a kockázatot,

-Biztosítja a nyomvonaljog esélyegyenlőséget

ÚJ ALÉPÍTMÉNYI HÁLÓZATI STÍLUS

STÍLUSJEGYEK:

-Minden végpontot két irányból lát el
-Minden irányból legalább 3-3 független csővel
-Többsíkú hálózat
-Gyűrűs szerkezet
-Gyűrű csomópontok
-Csomóponti sík-átmenetek
-Multiplex kiépítés

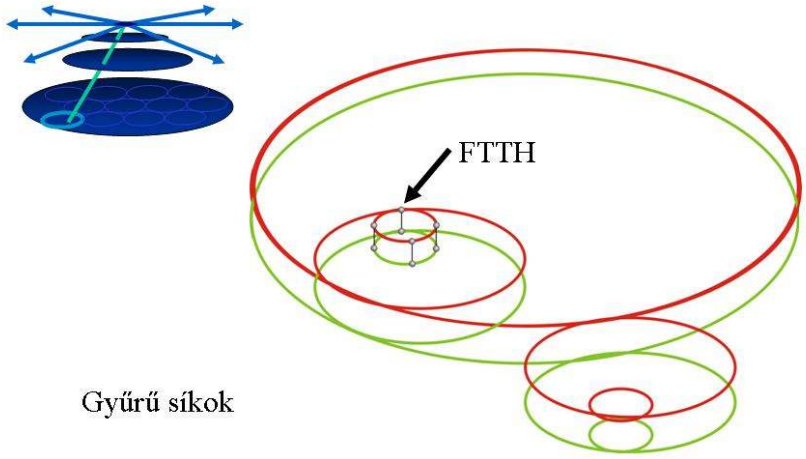
ÚJ ALÉPÍTMÉNYI HÁLÓZATI STÍLUS

MEGSZAKÍTÓ LÉTESÍTMÉNY TÍPUSOK:

- kábelbehúzó
- csőirány rendező
- síkváltó
- csomóponti
- kábelelosztó
- kábelszerelő
- elágazó

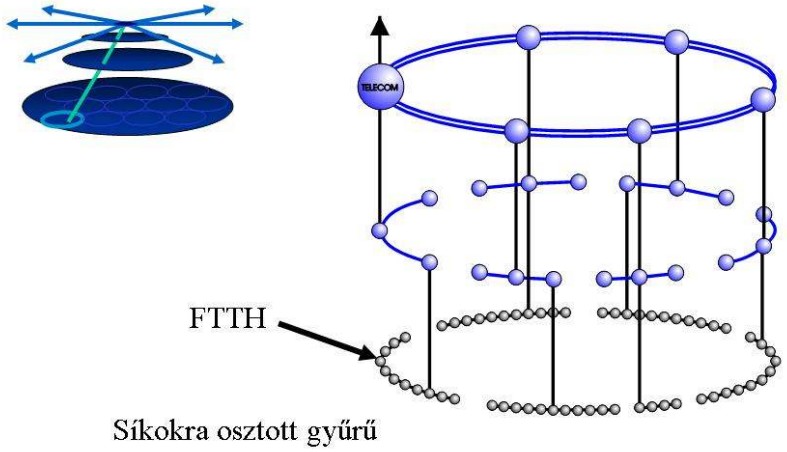
ZMNE Kommunikáció 2007 17

HÁLÓZATSZERVEZÉS



ZMNE Kommunikáció 2007 18

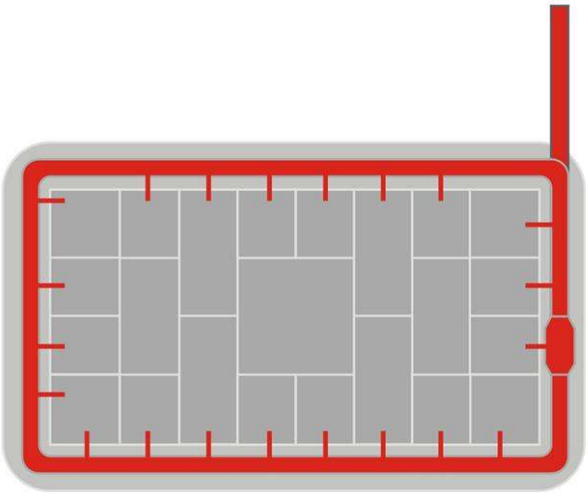
HÁLÓZATSZERVEZÉS



FTTH ALSÍKOK

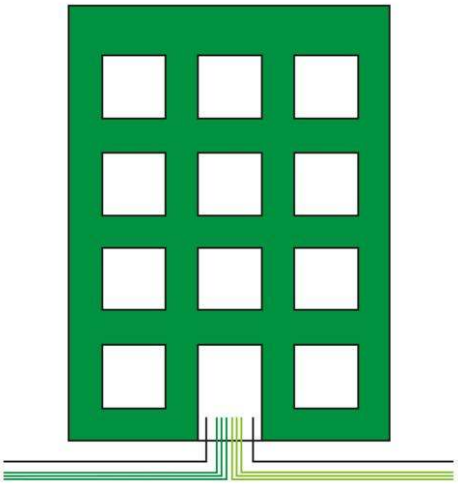
- Rendszer
- Fényvezető szál
- Kábel
- Nyomvonal

Háztömb, mint alapgyűrű



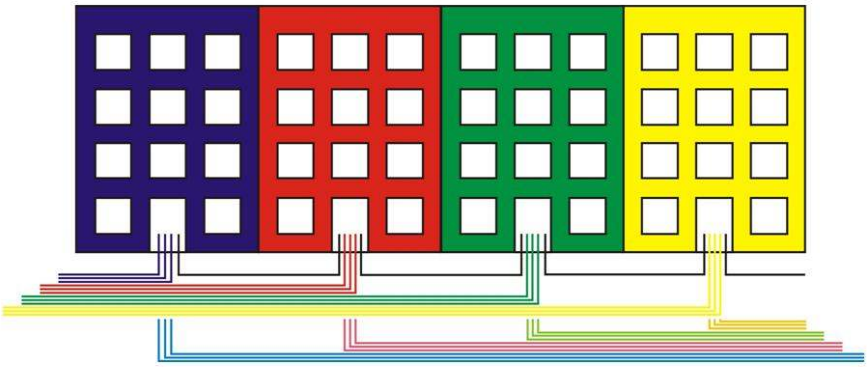
ZMNE Kommunikáció 2007 21

ÉPÜLET CSŐBEKÖTÉS



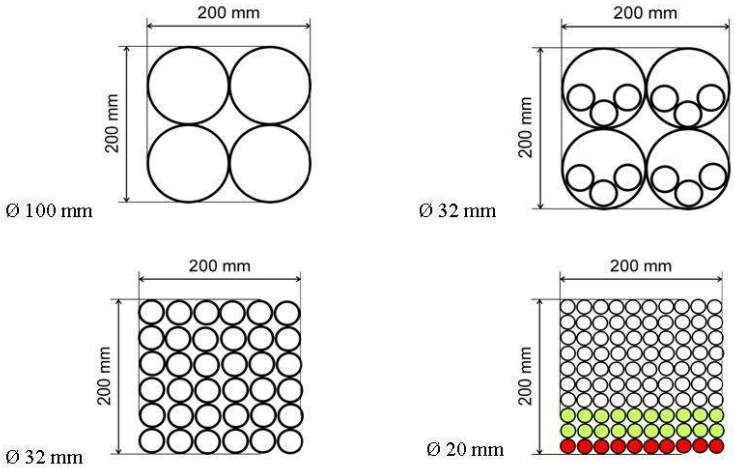
ZMNE Kommunikáció 2007 22

ÉPÜLET CSŐBEKÖTÉS



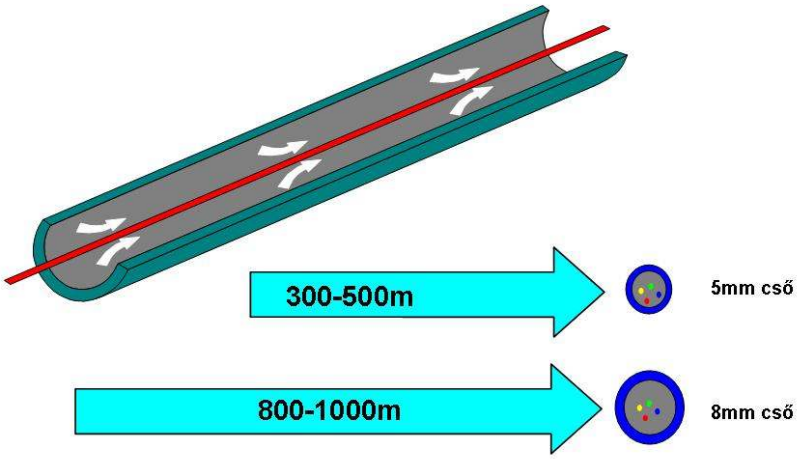
ZMNE Kommunikáció 2007 23

FAJLAGOS CSŐSŰRŰSÉG



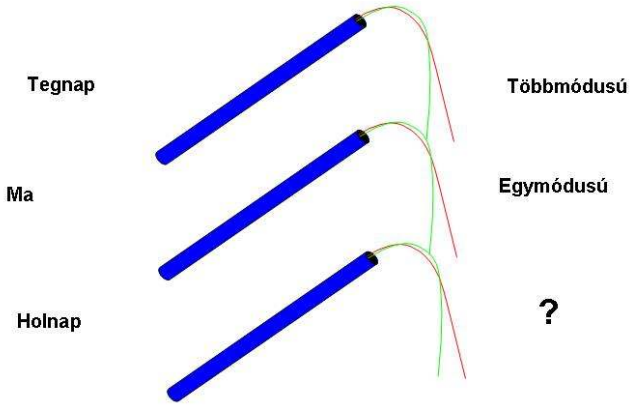
ZMNE Kommunikáció 2007 24

FÉNYVEZETŐKÁBEL BEFÚJÁS



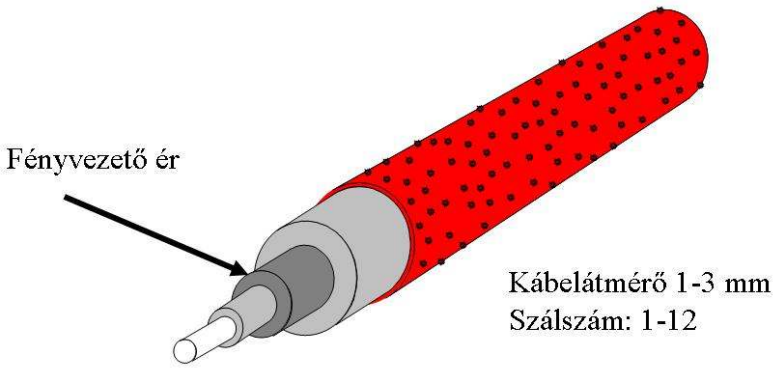
ZMNE Kommunikáció 2007 25

FÉNYVEZETŐKÁBEL BEFÚJÁS

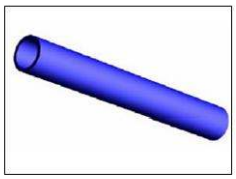


ZMNE Kommunikáció 2007 26

BEFÚJHATÓ FÉNYVEZETŐ KÁBEL



BEFÚJÓ CSŐ

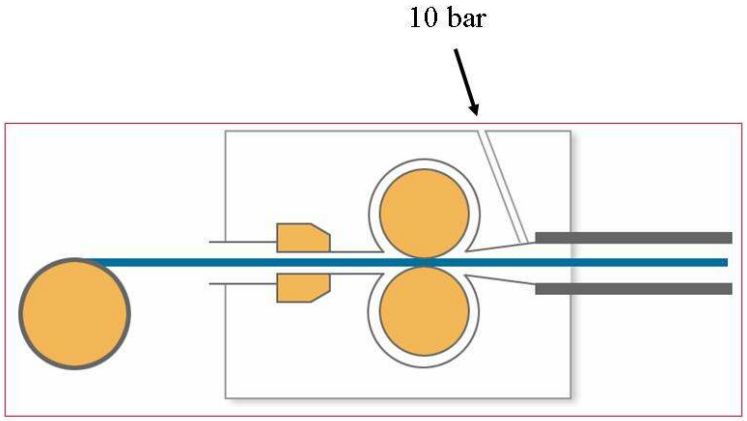


BEFÚJÁSI KISÉRLET

Csőátmérő: 8/10 és 10/12
Kábelátmérő: 6,0 mm és 6,5 mm
Átfújt hossz: >2000 m

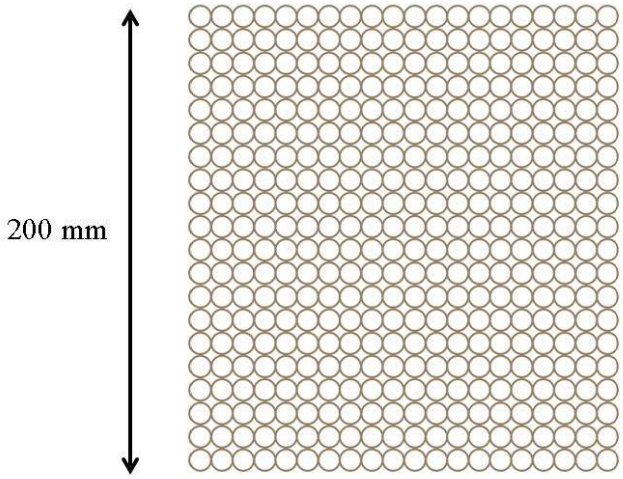
ZMNE Kommunikáció 2007 29

BEFÚJÓFEJ



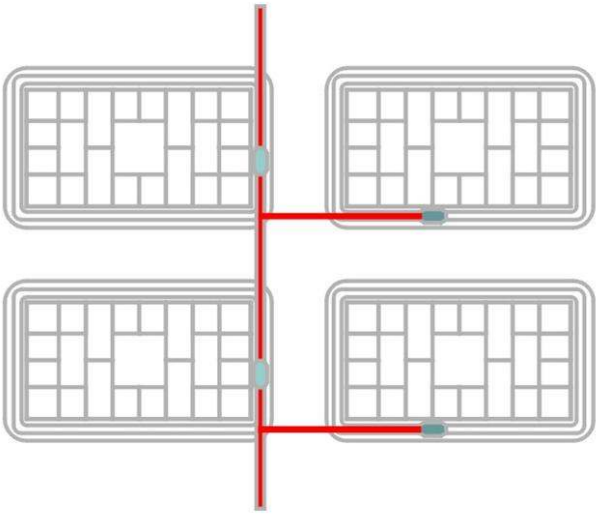
ZMNE Kommunikáció 2007 30

400 DB BEFÚJÓ CSŐ



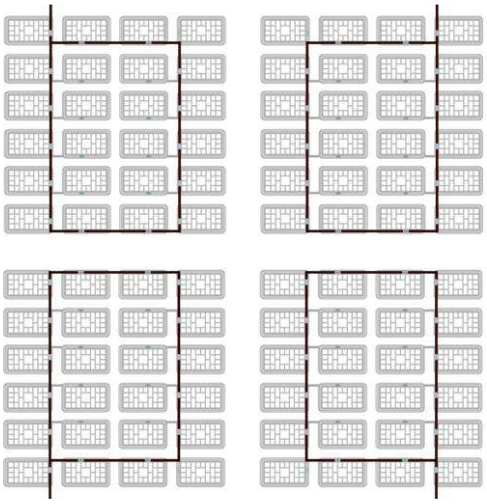
ZMNE Kommunikáció 2007 31

HÁZTÖMB FELFŰZÉS



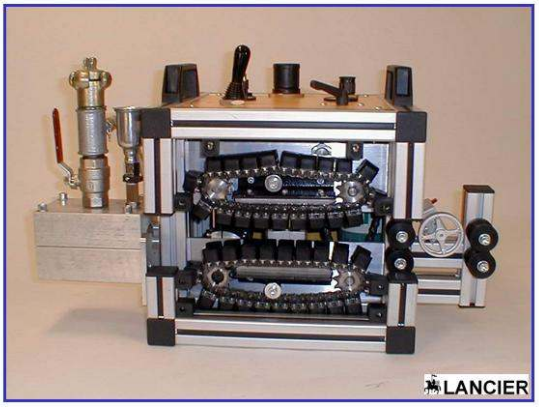
ZMNE Kommunikáció 2007 32

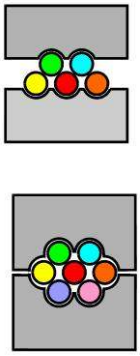
MÁSODIK GYŰRŰSÍK



ZMNE Kommunikáció 2007 33

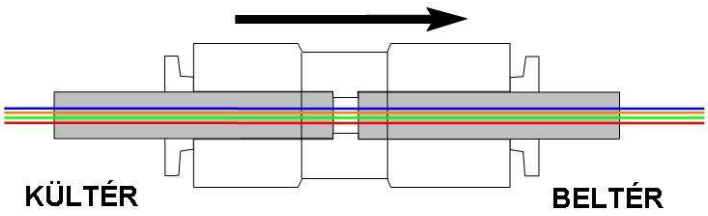
BEFÚJÓCSŐ BEFÚJÁS





ZMNE Kommunikáció 2007 34

ÁTMENET



KÖSZÖNÖM A FIGYELMÜKET

PROFESSZIONÁLIS SZOLGÁLTATÁSOK A KR-EN

Professzionális szolgáltatások a KR-en

Bódi Antal

ügyfélkapcsolati igazgató-h.

bodia@kopdat.hu

KOPINT-DATORG
Infokommunikációs ZRt

KOPINT-DATORG
Infokommunikációs ZRt

Professzionális Szolgáltatások

- ✓ **Szolgáltatásfejlesztés**
- ✓ **Szolgáltatásmenedzsment**
- ✓ **Üzemeltetés**

Szolgáltatásfejlesztés

3

Szolgáltatásfejlesztés
Magyarország.hu Kormányzati Portálon

•Magyarország.hu Kormányzati Portál az elektronikus kormányzati szolgáltatások centruma az állampolgárok felé.

•A Társaságunk a MEH-EKK megbízásából folytatott szolgáltatásfejlesztés keretében a Kormányzati Portált hírközpontú portálból szolgáltató portállá alakította át.

•A Magyarország.hu a legnagyobb kormányzati tartalomszolgáltató.

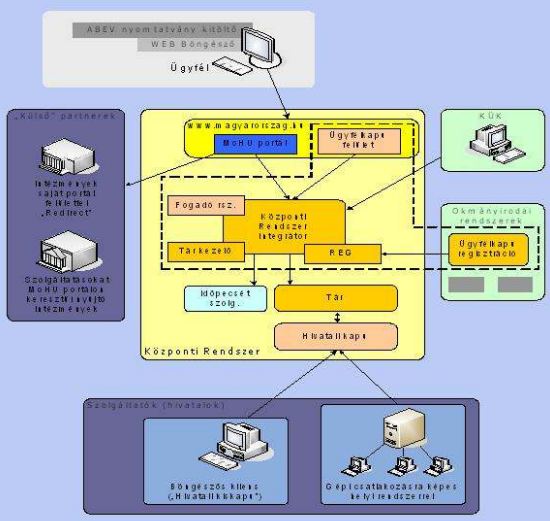
•A Társaság jelen van az előző oldalon bemutatott szolgáltatásfejlesztési ciklus valamennyi elemében. Ezáltal az E-kormányzati stratégia kialakításában is fontos szerepet tölt be.

Magyarország.hu

- Iránytű a közérdekű információkhoz
- A közérdekű információszolgáltatás (ügyleírások, adatbázisok, jogszabályok, országinfó stb.)
- Az ügyintézés eszköze (Ügyfélkapu, e-szolgáltatások)
- A véleménynyilvánítás színtere (Fórum)
- Közvéleménymérés (eGAMES, Kérdőív)

KOPINT-DATORG Infokommunikációs Zrt.

KR-jelenleg

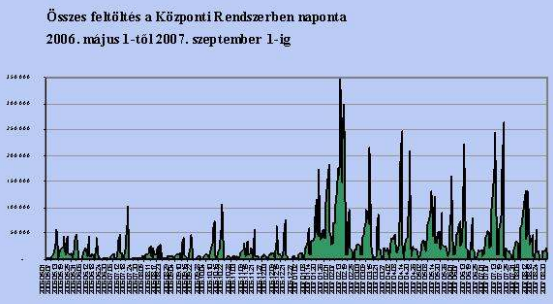


KOPINT-DATORG Infokommunikációs Zrt.

KR szolgáltatás állampolgárok felé

KOPINT-DATORG
Infokommunikációs Zrt.

KR szolgáltatás állampolgárok felé



KOPINT-DATORG
Infokommunikációs Zrt.

KR szolgáltatás állampolgárok felé

KOPINT-DATORG
Infokommunikációs Zrt.

KR szolgáltatás állampolgárok felé

KOPINT-DATORG
Infokommunikációs Zrt.

KR szolgáltatásai a kapcsolódó rendszerek felé (g2g) 1

- Hálózati kapcsolat
- Védelmi rendszerek az Internet felé
- ÜK2 viszontazonosítás
- ÜK-felhasználó általi ügyindítás felülete (bizonyos rendszereknél)
- Dokumentumtár
- Időpecsételés

KOPINT-DATORG
Infokommunikációs Zrt.

KR szolgáltatásai a kapcsolódó rendszerek felé (g2g) 2

- Szervezeti postafiók (automatizált rendszerrel vagy böngészővel történő hozzáférés)
- Kulcstár-hozzáférés (ügyfél kérésére történő titkosításhoz)

KOPINT-DATORG
Infokommunikációs Zrt.

Csatlakozás a KR-hez

- Jelenleg az 5/2004-es kormányrendelet meghatározza az EKG-hoz mint a KR hálózatához történő csatlakozás feltételeit. Ezt a rendelet a technológiai szintig szabályozza.
- A 182/2007 a KR-ről szóló kormányrendelet a részletesen szabályozza a KR szolgáltatások igénybevételét. Viszont nem rendelkezik a szolgáltatások elérését biztosító technológiai feltételek vonatkozásában.
- Jelen helyzetben a szakrendszerek fejlesztése érdekében indított projektek számára nem állnak rendelkezésre a KR rendszerhez történő csatlakozás technológiai dokumentációi, vagy legalábbis az információk megszerzése hosszas egyeztető megbeszéléseket igényel.

KOPINT-DATORG
Infokommunikációs Zrt.

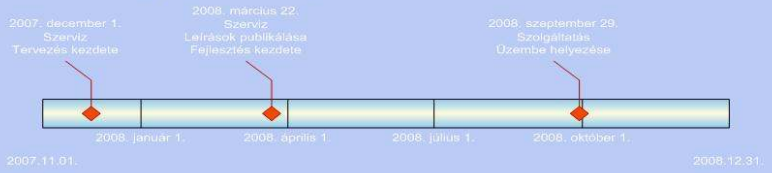
KR-kapcsolódó felületei jelenleg (protokollok)

- IP/IpSec
- Soap(IOP (Kietb 21.-es ajánlás))
- HTTP-redirekt

KOPINT-DATORG
Infokommunikációs Zrt.

KR-architektúra váltás

- KOPINT-DATORG Infokommunikációs zRt. az előzőekben ismertetett referenciák és tapasztalatok alapján szükségesnek tartja a KR szolgáltatások elérésének egységes technológiai leírását.

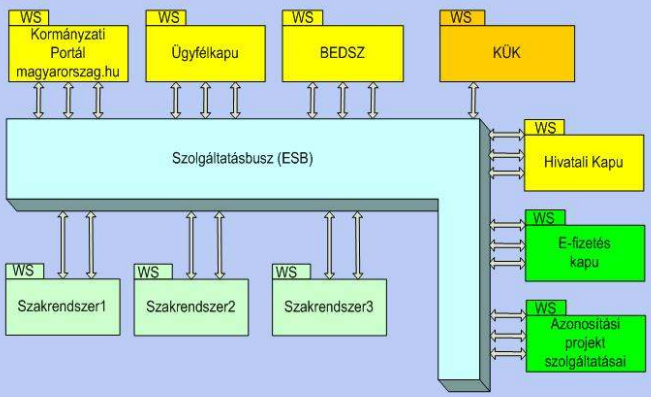


A KR bővítési projekt keretében leírások várhatóan 2008 első negyedévben publikálásra kerülhetnek és az EKOP keretében párhuzamosan folyó projektek felhasználhatják.

2008 harmadik negyedévtől pedig a KR felkészült lesz arra, hogy a publikált leírások szerint fejlesztett szakrendszerek a szükséges tesztelést lefolytatva azonnal integrálni tudja.

KOPINT-DATORG Infokommunikációs ZRt.

KR-jövőbeli szoftverarchitektúrája



KOPINT-DATORG Infokommunikációs ZRt.

Szolgáltatásbusz (ESB)

- A KR bővítési projekt keretében a szolgáltatásbusz kialakításával elérhető eredmények:
- Létrejönnek a KR modulok szolgáltatásai által fogadott, és válaszként küldött egységes XML sémák.
- Elkészül XML sémák pontos dokumentációja, amely a szakrendszerek fejlesztői számára publikálható.
- ESB (Enterprise Service Bus) rendszer üzembe helyezésével a KR modulok szolgáltatásait webszervízként vehetik igénybe a szakrendszerek.
- Létrejön a KR menedzselhető web-szolgáltatásokon alapuló kommunikációs infrastruktúrája.

KOPINT-DATORG
Infokommunikációs Zrt.

Szolgáltatásbusz (ESB)

- A kialakított egységes XLM sémák mintájára a jövőben fejlesztett szakrendszerek szolgáltatásait a Kormányzati portál fejlesztésekor web-szervízként be lehet építeni.
- Ezáltal megteremtődne annak lehetősége, hogy a több szakrendszert érintő ügyeket (Pl. a közbeszerzésekhez előírt 0.-ás igazolások beszerzését) egy ügyként lehetne kezelni a kormányzati portálon.
- A menedzselt ESB által nyilvántartott szolgáltatások elérhetőségéről a KÜK folyamatos információt kapna.

KOPINT-DATORG
Infokommunikációs Zrt.

KR-kapcsolódó jövőbeni felületei (protokollok)

- Webservice (SOAP)
- HTTP-redirekt (webfelület esetén)

KOPINT-DATORG
Infokommunikációs ZRt.

Szervezeti szintű kommunikációs megoldások
2007. október 16.

Fejlesztési irányok

1, Technikai orientált fejlesztés

Egy meghatározott feladat támogatásához vagy szervezet működéséhez szükséges rendszer létrehozása.

Előnyei:
- rövid távon olcsó
- viszonylag gyorsan megvalósítható

Hátrányai:
- minden egyes feladatra vagy szervezethez új rendszert kell létrehozni
- rugalmatlan

Fejlesztési irányok

2, Szolgáltatás orientált fejlesztés

Szervek, vagy szervezetek működéséhez, feladatainak ellátásához szükséges távközlési szolgáltatások összességét biztosító rendszer létesítése.

Előnyei:

- szolgáltatások széleskörű biztosítása
- feladatokhoz, szervezeti változásokhoz történő rugalmas alkalmazhatóság

Hátránya:

- magas beruházási költség

EDR = TETRA technológia = szolgáltatás orientált fejlesztés.

Mit is jelent?

A készenléti szolgálatok vezetéséhez, irányításához, sajátos szakmai igényei, működési követelményei érvényesítéséhez szükséges távközlési szolgáltatások technikai feltételeinek összessége.

Szolgáltatások:

1. Beszédkommunikáció:
    - csoporthívás (40.000 forgalmi csoport létrehozásának lehetősége)
    - hálózaton belüli egyéni hívás /telefonszerű duplex, gyorshívás félduplex)
    - más távközlési hálózatokba történő bekapcsolódás lehetősége
    - konferencia hívás
    - vészhívás
    - környezeti befigyelés

2. Rövidüzenet küldés lehetősége:
   - szituációs üzenet
   - állapot üzenet
   - SDS üzenet (max. 140 karakter)
3. Adatátviteli lehetőség
   - Bruttó 7.6 kbit/sec
   - Nettó 2.4 kbit/sec
4. Magasfokú védettség
   - levegőben történő titkosítás
   - végkészülékig történő titkosítás lehetősége

Részleteiben:

Technikai megvalósítást, a szolgáltatások igénybevételének lehetőségét, a rendszer üzemeltetését külső távközlési szolgáltató a Pro-M Zrt. végzi, illetve biztosítja.

A testreszabás, a szervezet feladatainak, vezetési, irányítási rendszerének, szervezeten belüli és kívüli együttműködésének, alá- és fölérendeltségbeli viszonyainak EDR működtetésében történő megjelenítése, a felhasználó feladata.

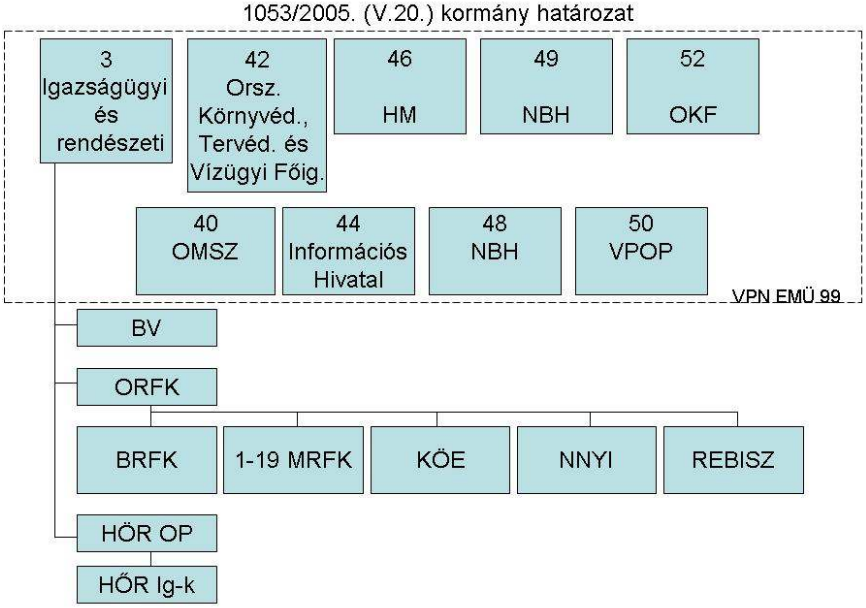
Tartalmazza:

1, A rendszer szerződésben rögzített kiépítettségének figyelembevételével az eszközök, tartozékok, szolgáltatások, feladatok jellegéhez történő kiválasztását. (pl.: zajos környezet, kézirádió besugárzottságának hiánya = gateway)

2, Szolgáltatások, felhasználói jogosultságok meghatározását.

EDR FELHASZNÁLÓI KÖR

1053/2005. (V.20.) kormány határozat



A felhasználók részére létrehozott 9 VPN-nel biztosítottuk az EDR-t használó országos szervezetek részére a rendszer virtuális felosztását.

Ez nem testreszabás!

Régi, elkülönült, technikai orientált gondolkodásunk alapján a szervezeti elkülönültség látszatának meghagyása.

A rövid felhasználói tapasztalatok alapján indokoltnak látszik a VPN kialakítás felülvizsgálata feladat, együttműködési kötelezettség és szolgáltatás szempontjából.

A rendőrség, határőrség és a polgári titkosszolgálatok szoros együttműködése, a zárt önálló forgalmi csoportok kialakításának igényei csak közös VPN-n belül valósíthatók meg.

Szervezet önállósága, az információk védelme a szervezet által létrehozott forgalmi csoportok használatának jogosultságával, ellenőrzési lehetőségeivel biztosított.

A VPN biztosítja az együttműködő szervvel közös forgalmi csoportjainak gyors létrehozási feltételeit.

Testreszabás menete a Budapesti Rendőr-főkapitányságon

1. Vezetők tájékoztatása

a) rendszer szolgáltatásairól

b) ISSI, GSSI számkiválasztási lehetőségeiről

c) főkapitányság és szervei tervezett vezetési rendszeréről (csoportkiosztás, körözvényhívás)

d) más szervekkel történő együttműködési lehetőségeiről

e) javasolt jogosultságokról:

- egyéni hívások
- más távközlési hálózatokba történő bekapcsolódás lehetősége
- beolvasási lehetőség (szkennelés biztosítása)
- csoporthívások kikapcsolásának lehetősége

2. Vezetői javaslatok összegzése, a szervezet irányítási struktúrájának meghatározása

3. Rendszerbeállításhoz a belső normajavaslat elkészítése

Egyéni hívások engedélyezése a BRFK-n

/erőforrásgazdálkodás, prioritás alkalmazás hiánya/

- az arra jogosult kézrádiók egymást is, (vezetői, bűnügy, KMB) a "járőr" készülékek csak a saját diszpécsert tudják egyéni hívásként hívni. (ügyeleti stabil rádióval történő ellátása esetén -például őrs- külön szervezeti egység kerül zárt összeköttetéshez létrehozásra)
- a magasabb prioritású készülékek egyéni hívásként, RH, városi, és mobil *hívásokat is tudnak kezdeményezni.
- közcélú hálózatból hívás fogadása csak kezelői közreműködéssel, RH hálózatból közvetlenül (04 előhívóval) biztosított
- csoporthívás jelzése

* tarifaszámlálás

EDR kézirádióról egyéni hívás indításának lehetősége (duplex, félduplex)

Rendészeti hálózatról az EDR rádió egyéni hívásának folyamata

(központok beállítása)

CSOPORTHÍVÁS BRFK-n létrehozott mapparendszer

/célszerű a közös terminológia kidolgozása/

1. **Szervezeti**
   a) **Rendőrkapitányságí /Kerületi Rk-k, DVRK)**
   b) **BRFK központi közbiztonsági szervek**
   c) **BRFK központi bűnügyi szervek**
   d) **BRFK hivatali szervek**
2. **BRFK Ügyeleti**
3. **BRFK biztosítási**
4. **BRFK Rendőrkapitányságí**
5. **Országos csapatszolgálati**
6. **Országos EMÜ**
7. **PMRFK**
8. **Külső EMÜ**
9. **DXT hiba**
10. **Sziget üzemmód**

MAPPÁK

BRFK Rk bi.
BRFK Ügy.
RFK emü.
Szervezeti
Sziget mód

FORGALMI CSOPORTOK

1. **Statikus:**
   Állandó, belső normában szabályozott, a tervezés alapja.

2. **Dinamikus:**
   Feladat végrehajtására, a feladatokra bevont felhasználók rádiókészülékeire. A szolgálati jegyek, hiradótervek alapján kerül létrehozásra, a szakszolgálatoknak szükségességét folyamatosan felül kell vizsgálni.

Statikus forgalmi csoportok BRFK Rendőrkapitányságokon

Szervezeti	BRFK ügy.	BRFK Rk.bi.	RFK emü.	
BRFK emü.	I.ker. szolg.	I.ker. tart.	Országos emü	
BRFK biz. vezetői	II.ker. szolg.	II.ker. tart.	ORFK emü	
BRFK biz. közbiz.	III.ker. szolg.	III.ker. tart.	KÖE emü	
BRFK biz. közr.1	IV.ker. szolg.	IV.ker. tart.	REBISZ emü 1	
BRFK biz. közr.2	V.ker. szolg.	V.ker. tart.	REBISZ emü 2	
BRFK biz. bűnügy	VI.ker. szolg.	VI.ker. tart.	Baranya emü	
BRFK biz. közlek	VII.ker. szolg.	VII.ker. tart.	Bács-Kiskun emü	
BRFK biz. tart.	VIII.ker. szolg.	VIII.ker. tart.	Békés emü	
BRFK bü. szolg.	IX.ker. szolg.	IX.ker. tart.	BAZ emü	
... ker. vezetői	X.ker. szolg.	X.ker. tart.	Csongrád emü	
... ker. szolg.	XI.ker. szolg.	XI.ker. tart.	Fejér emü	
... ker. tart.	XII.ker. szolg.	XII.ker. tart.	GYMS emü	
KGJSZO szolg.	XIII.ker. szolg.	XIII.ker. tart.	Hajdú-B. emü	
Akció O. szolg.	XIV.ker. szolg.	XIV.ker. tart.	Heves emü	
KVFO szolg.	XV.ker. szolg.	XV.ker. tart.	JNSZ emü	
KLFO szolg.	XVI.ker. szolg.	XVI.ker. tart.	Komárom emü	
Régió City	XVII.ker. szolg.	XVII.ker. tart.	Nógrád emü	
Régió Belvárosi	XVIII.ker. szolg.	XVIII.ker. tart.	Pest emü	
Régió Budai	XIX.ker. szolg.	XIX.ker. tart.	Somogy emü	
BRFK bü. tart.	XX-XXIII.ker. szolg.	XX-XXIII.ker. tart.	SZSZB emü	
BRFK közb. tart.	XXI.ker. szolg.	XXI.ker. tart.	Tolna emü	

Statikus forgalmi csoportok BRFK Központi Bűnügyi Szerveknél

Szervezeti	BRFK ügy.	BRFK Rk.bi.	RFK emü.	
BRFK emü.	I.ker. szolg.	I.ker. tart.	Országos emü	
BRFK biz. vezetői	II.ker. szolg.	II.ker. tart.	ORFK emü	
BRFK biz. bűnügy	III.ker. szolg.	III.ker. tart.	KÖE emü	
BRFK biz. tartalék	IV.ker. szolg.	IV.ker. tart.	REBISZ emü 1	
KGJSZO szolg.	V.ker. szolg.	V.ker. tart.	REBISZ emü 2	
KVFO szolg.	VI.ker. szolg.	VI.ker. tart.	Baranya emü	
KLFO szolg.	VII.ker. szolg.	VII.ker. tart.	Bács-Kiskun emü	
Akció O. szolg.	VIII.ker. szolg.	VIII.ker. tart.	Békés emü	
Akció O. tart.	IX.ker. szolg.	IX.ker. tart.	BAZ emü	
BRFK bü. szolg.	X.ker. szolg.	X.ker. tart.	Csongrád emü	
FFO szolg.	XI.ker. szolg.	XI.ker. tart.	Fejér emü	
FFO tart.	XII.ker. szolg.	XII.ker. tart.	GYMS emü	
BÜFO I. GBEO	XIII.ker. szolg.	XIII.ker. tart.	Hajdú-B. emü	
BÜFO I. Élet	XIV.ker. szolg.	XIV.ker. tart.	Heves emü	
BÜFO I. Rablás	XV.ker. szolg.	XV.ker. tart.	JNSZ emü	
BÜFO I. Betörési	XVI.ker. szolg.	XVI.ker. tart.	Komárom emü	
BÜFO I. Zseblop	XVII.ker. szolg.	XVII.ker. tart.	Nógrád emü	
BÜFO I. SZBEO	XVIII.ker. szolg.	XVIII.ker. tart.	Pest emü	
BÜFO I. KBEO	XIX.ker. szolg.	XIX.ker. tart.	Somogy emü	
BÜFO II. Szolg.	XX-XXIII.ker. szolg.	XX-XXIII.ker. tart.	SZSZB emü	
Gazd. Véd. Főo.	XXI.ker. szolg.	XXI.ker. tart.	Tolna emü	

Forgalmi csoport használatának jogosultsága

1. Valamennyi rendőrségi rádiókészülék részére engedélyezett:
   a) BRFK biztosítási, együttműködési
   b) BRFK rendőrkapitányságí szolgálati
   c) BRFK rendőrkapitányságí tartalék

   forgalmi csoportok használata
1. Csak az érintett szervezet részére biztosított rádiókészülékeknél engedélyezett használatuk:
   a) a központi bűnügyi főosztályok osztályai, hivatali szervek részére létrehozott forgalmi csoportok
   b) a rendőrkapitányságok un. vezetői forgalmi csoportjai
   c) a BRFK felső, közbiztonsági és bűnügyi szervek részére létrehozott forgalmi csoportok

Forgalmi csoportok területi használata

A területi korlát bevezetése központi hálózatgazdai szabályozást igényel.

Területi korlátozást indokolja:

- az erőforrásokkal történő gazdálkodás
- az adatvédelem

Teljeskörű területi jogosultságot indokolja:

- a mindenkori ellenőrizhetőség és elérhetőség (Teljes hálózat – változó terület beállítás)
  Fix terület beállítás tilos!!!

KÖRÖZVÉNYHÍVÁS
/Háttérmappák/

1. KIEMELT

valamennyi BRFK készüléken

2. Általános

csak a szolgálati állomány készülékeiken

A háttérmappa készülékre és nem forgalmi csoportra vonatkozik, s ezért a biztosítási feladatok végrehajtását nehezíti.

Megoldás:

Forgalmi csoportok összerendelése (max. 16) összerendelt forgalmi csoportok tagállomásai részére a diszpécser kiemelt prioritással utasítást adhat.

Szituációs üzenetek

/követett egységek menüben a diszpécser láthatja/

- Szolgálatban
- Intézkedem
- Szolgálaton kívül
- Pihenőben
- Átvezényelve
- Megkülönböztetett jelzést használok

Állapotüzenetek

Állapotüzenetek	Állapotüzenetek	Állapotüzenetek
Szolgálatban	Erősítést kérek	Nem szerepel
Szolg. helyen	Segítséget kérek	Fogja el
Intézkedem	Mentőt kérek	Nem léphet be
Intézkedés vége	Tűzoltót kérek	Kísérje be
Pk.-t kérek	Előállításhoz gk	Tartózkodási hely
Pihenőben	Váltást kérek	Írjon jelentést
Pihenő vége	Kerület elhagyva	Körözött tárgy
Beindultam	Kerületben	
Szolg. befejezve	Ellenőrzés	
Helyszínbiz.vége	Szolg.pk-nál jel	
Rendkív. esemény	Vonuljon be	
Megsérültem	Halott szállítót	
	Orvost kérek	

Állapotüzenetek

Személy, gépjármű korrózési adatbázis használata 1. Adatbevitel

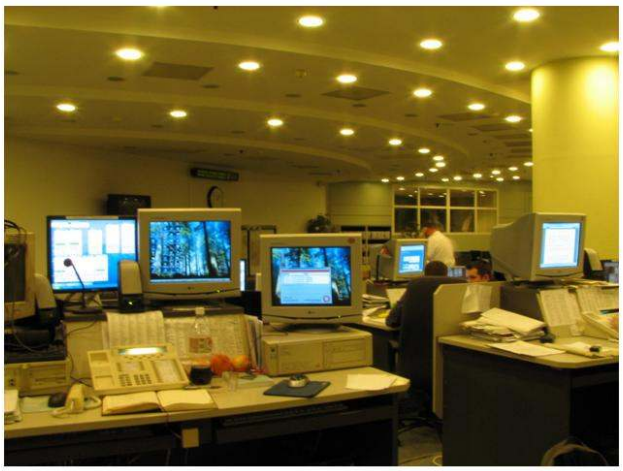
Személy, gépjármű korrózési adatbázis használata 2. Üzenetküldés

Személy, gépjármű körözési adatbázis használata
3. Válasz

VÉSZHÍVÁS

- a gomb 3 mp-ig történő folyamatos nyomásával, a készülék 15 mp-ig segélyhívást ad.

Az átfedőcsoportok hiánya miatt a vészhívások a BRFK Központi Ügyeletének diszpécseréhez futnak be



Diszpécser, ügyelet feladatának szabályozása, lehetőségei

a) forgalmi csoportok felügyelete (1-16-ig)
b) új tag felvitele, kizárása
c) dinamikus forgalmi csoportok létrehozása
d) követett egység funkció
e) jelentéstárolás, dokumentálás
f) AVL
g) bejövő hívás átadása

Bevezetés tapasztalatai:

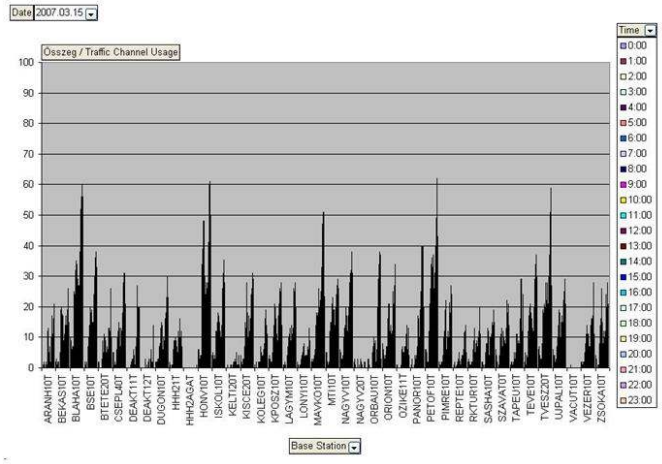
Csak a szolgáltató és a felhasználó közös tanulásával, közös gondolkodásával lehet a rendelkezésükre álló technológia és a szervezet valós szolgálati igényeinek összhangját biztosítani.

Testreszabás valamennyi szervezet saját feladata, és felelőssége.

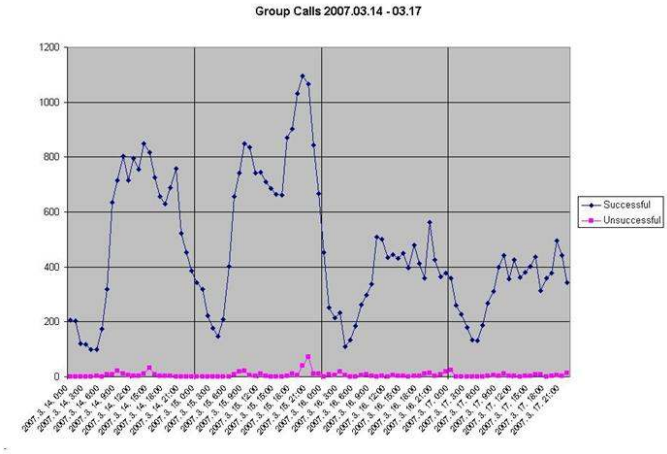
A RENDSZER

1. **Jól terhelhető**
   2006. október 23-án 15^{00} és 16^{00} között a fővárosban 1900 sikeres csoporthívás, 1100 egyéni hívás
2. **Országosan kiépített**
   A magyar rendőrség 2007. március 15-i biztosításnál országos vezetési, jelentési rendszeréhez első ízben alkalmazott rádióhíradást.
3. **A beszédkommunikáció mellett már új szolgáltatásokat is biztosít**
   a) csapatszolgálati századainak helyzetét AVL-en figyelemmel kísérhettük
   b) lehetővé vált a körözési adatbázisok rövid üzenet formájában történő lekérdezése
4. **Szélesítette más készenléti szervekkel (mentők, tűzoltók) történő együttműködés lehetőségét, gyorsította szolgáltatásaik igénybevételét.**
5. **Információvédelem technikailag biztosított.**

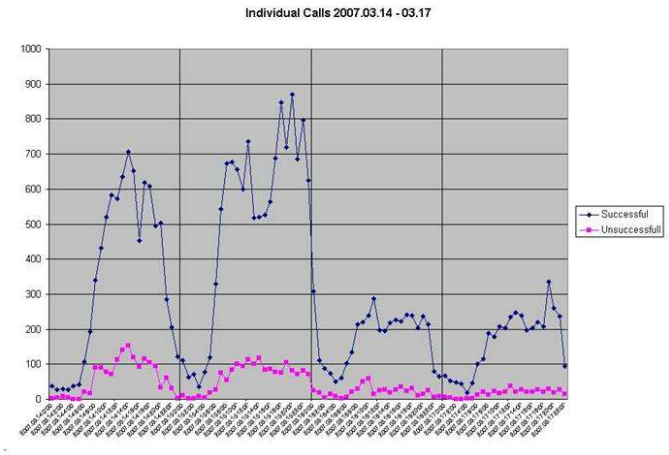
2007. március 15-i adatok
Terheltségi összesítés Budapest



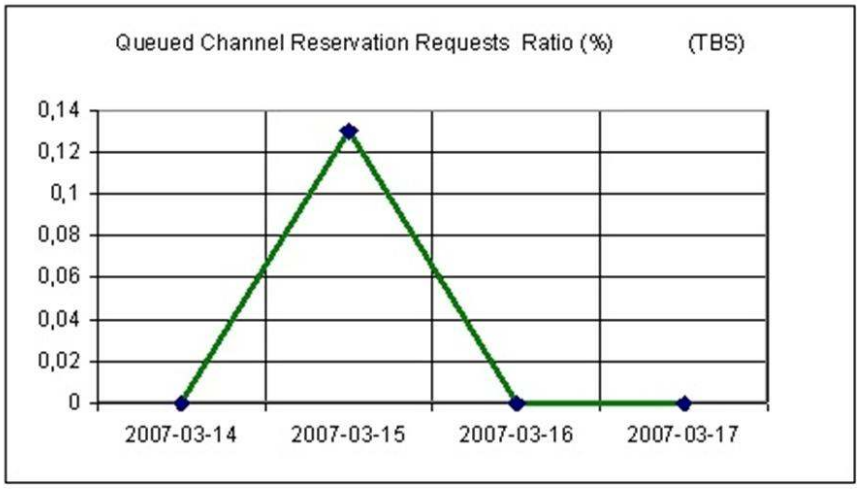
2007. március 15-i adatok
Csoporthívások



2007. március 15-i adatok
Egyéni hívások

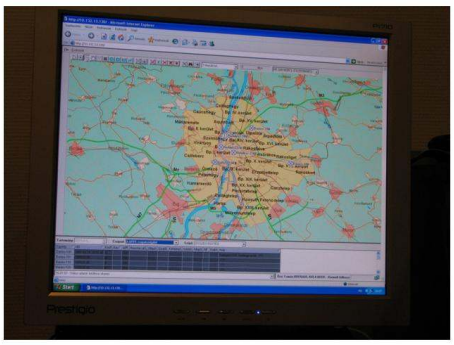


2007. március 15-i adatok
Sorbanállás



2007. március 15-i adatok

Csapatszolgálati századok mozgásának követése AVL-en



Igényelt szolgáltatások

1. Forgalmi csoportok összerendelése
2. Átfedő csoportok létrehozása
3. Prioritás
4. Erőforrás gazdálkodás

Köszönöm a figyelmüket!

Gabor EGRI

INTEGRATION OF THE SCHENGEN INFORMATION SYSTEM IN HUNGARY

Integration of the Schengen Information System in Hungary

Gabor Egri
Central Office for Administrative and Electronic Public Services

September 2007

Content

- Introduction
- Legal aspects of the SISone4ALL project
- Organisations using SIS information
- General overview of the National Police
- The organisational structure of the Border Guard
- The upcoming integration of the Police and the Border Guard
- The integrated organisation
- Fundamental duties of the Central Office
- Suitability of the Central Office
- The Central Office as NHU.SIS
- The role of the Central Office in the SISone4ALL project

2

Content

- The SIRENE bureau in the HU law enforcement
- The cooperation within the SIS and the logical architecture of the Hungarian national system
- Data protection and authentication
- Technical details, system architecture
- The main HW and SW components of the NHU.SIS
- The main databases involved in the SIS operation
- Dataflow main functions
- Hungarian databases by SIS categories
- The current status of SIS II development in HU
- Summary

3

Introduction

- During preparation for joining the Schengen area in Hungary, we prepared for integration to SIS II.
- December 2006: decision of SISone4ALL project and parallelly SIS II development
- The main role of Central Office in the Hungarian project
- Fruitful cooperation between the organisations concerned in SISone4ALL

4

Legal aspects of the SISone4ALL project

EU

- The Schengen Agreement and the Schengen Convention
- Legal instruments in the fight against terrorism
- EAW

HU - legal instruments for SIS operation

Basis for cooperation:

- The Acts for fulfilling the Schengen requirements (Act CV of 2007 on cooperation in the framework of CISA.)
- Governmental and ministerial decrees for the process at executive level

5

Organisations using SIS information

- Judiciary (courts, prosecution's office)
- Public administration and law enforcement
  - Office of Immigration
  - Police and Border Guard
  - Customs Authority
  - Ministry of Foreign Affairs and Consulates
  - Document Offices
  - Central Office for Administrative and Electronic Public Services
- SIRENE bureau
- Data Protection Commissioner's Office

6

General overview of police

National police HQ — central level

1…20 County/Budapest Police HQ — regional level

1…154 City Police stations

1…154 City Police stations — local level

7

The organisational structure of the Border Guard

National Headquarters — Central level

1-10. Border Guard Directorates — Regional level

- Local Office (51)
  - BCP (112)
    - Road (70)
    - Railway (26)
    - Air (8+2)
    - Water (6)
- Criminal Investigation Service (22+1) Operational Subunit (3)
- Mobile Forces (15)
- Guarded facility for aliens (6)

Local level

8

The upcoming integration of the Police and Border Guard

Central level

Regional level

Local level

Criminal investigation

Border policing

Public order and traffic

Administration

9

The integrated organisation

- Personnel ~45.000
- Schengen external region 30 local offices
- Schengen internal region 20 police station
- Criminal investigation and control – emergency police (bereitschaftpolizei)

10

Fundamental duties of the Central Office

- **Data processing and data source** (citizens' personal data)
- **Operation and management of registers** (supervision of the central register, control over territorial and local registers)
- **Elections** (preparation and organization of elections and national referenda)
- **Issuing** personal identification numbers and residence certificates for Hungarian nationals living abroad
- Tasks related to birth, marriage and death registry and name alteration
- **Issue of documents (e.g.):**
  - Identity cards;
  - Passports;
  - Certificate of no criminal records;
  - Vehicle registration certificate,
- **Documents issued by the Central Document Office, that are not of central issuance:**
  - Residence certificate,
  - Registration book for cars,
  - Parking certificates for disabled persons.

11

Suitability of the Central Office

1. Long and extensive experience in system development and project management;
2. Extensive experience in operating high availability, high security IT systems;
3. Competence in protection of personal data
4. SIS II competence is already available;
5. Implementing NS.VIS and NS.CP at the same organization is cost effective
6. A significant part of the SIS source data are available at the Central Office;
7. Extensive, reliable data connections with governmental and other institutions (e.g. Document Offices, Police, Immigration Office, etc.)
8. Protection of national security interests does not require significant additional efforts

12

The Central Office as NHU.SIS

- Technical and personal conditions for 24/7 operation of the NHU.SIS
- Access to the SIS database for legally qualified organisations
- C/U/D of alerts in the NHU.SIS and sending data to C.SIS
- Recording of activities of data management, data processing and access right in the NHU.SIS
- Informing the SIRENE bureau and the issuing organisation about the initiating of multiple alert
- Compliance with data security and data protection requirements
- Already high IT security fine tuned for SIS requirements

All data processing, query and alert activities in the NHU.SIS can be done only through the Central Office.

13

The role of the Central Office in the SISone4ALL project

- Coordinating IT activities of installation of the SISone4ALL
- Implementing the national system (NHU.SIS) and ensuring its availability
- Organisational, administrative and system development tasks for ensuring data service capability of the national registries of the Central Office
- Participating in the execution process activities of law for joining Schengen
- Participating in training and education organised by EU
- Keeping in touch with Portuguese partners, the Austrian coaching partners and with C.SIS
- Training of the users concerned with the system

14

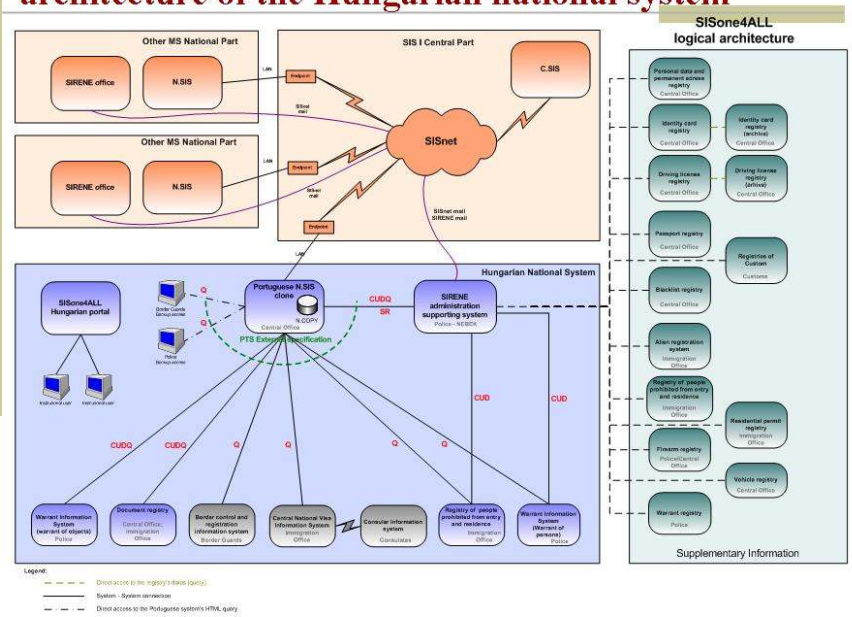
The SIRENE bureau in the Hungarian law enforcement

- The SIRENE within the National Police HQ

- Tasks of SIRENE bureau:
  - Exchange of supplementary information, controlling quality of data entered into NHU.SIS
  - Keeping contact with the organisations sending the data in order to correct or add further information
  - Access to data stored in the SIS
  - Records the input and forwarding of additional information and the access of them

15

The cooperation within the SIS and the logical architecture of the Hungarian national system



16

Data protection and authentication I

Data protection

- The Data protection commissioner as an independent national authority supervises data processing in the framework of SIS.
- The Central Office and the SIRENE bureau records the data management of SIS (data processing registry).
- The SIRENE bureau is responsible for informing the concerned individual upon request, if his/her data are processed in SIS.
- The concerned individual may also turn for information to the data protection commissioner.

Authentication

- The Central Office takes security measures in the interest of security function of NHU.SIS system
- The head of Central Office determines security requirements and conditions of NHU.SIS development and operation.
- The Central Office ensures data protection and authentication training for employees of NHU.SIS accessing to the SIS data.

17

Data protection and authentication II

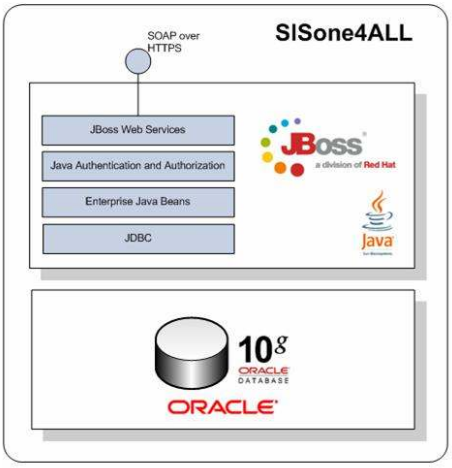
Legal redress

- Alerts can be inserted in the SIS by Hungarian authorities authorized in the relevant acts . The legal remedy is granted according to national law.
- If the alerts of external states have false data or malfeasance it is possible to have legal redress according to the laws of the state inserting the alert.
- Legal remedy (eg. complaints concerning the legality of processing of data in connection with an alert) can be initiated through the SIRENE bureau, in accordance with Paragraph 19 of Act CV of 2007 or through the data protection commissioner.

18

Technical details, system architecture

- The architecture of PT clone



19

The main HW and SW components of the NHU.SIS

HW elements:

- 5 piece IBM System x3755 server
- 8 piece IBM System x3650 server
- IBM System Storage DS8100

SW elements:

- Red Hat LINUX operational system
- JBoss application server
- Oracle 10g database management system

The number of end-user stations (C/U/D of data or downloading and query)

- 20 000 db (nationwide)

20

The main databases involved in the SIS operation

- Central system for border guard
- Warrant information system of police
- Consular information system of Ministry of Foreign Affairs
- Document information systems of Central Office

21

Dataflow main functions

The main elements of C/U/D of alerts:

- Insertion of alerts is based on any national system.
- The alert of any person is done by cooperation of SIRENE bureau.
- The alert of any goods is automatically done by the systems.
- Any alert has got its own Schengen ID in the NHU.SIS.
- The SIRENE officers have the right to use any supplementary information of the national systems.
- The downloading and access process is fulfilled by cooperation of the national systems. Some end-users have direct access to NHU.SIS web interface.

22

Hungarian databases by SIS categories

Alert Category		Affected System		Organisation
WP	art 95	HERMON	Warrant information system	Police
	art 96	BTT	Registry of People prohibited from entry and residence	Central Office
	art 97	HERMON	Warrant information system	Police
	art 98	HERMON	Warrant information system	Police
	art 99	HERMON	Warrant information system	Police
VE	art 99	HERMON	Warrant information system	Police
	art 100/A.	HERMON	Warrant information system	Police
	art 100/B.	HERMON	Warrant information system	Police
	art 100/F.	HERMON	Warrant information system	Police
	art 100/F.	JÁROK	Vehicle registry	Central Office
FA	art 100/C.	HERMON	Warrant information system	Police
DB	art 100/D.	HERMON	Warrant information system	Police
	art 100/D.	REALK	Registration plate distribution system	Central Office
	art 100/D.	STB	Blank document registry	Central Office
ID	art 100/E.	HERMON	Warrant information system	Police
	art 100/E.	ÚTLEVÉL	Passport registry	Central Office
	art 100/E.	SZIG	Identity card registry	Central Office
	art 100/E.	VEN	Driving license registry	Central Office
	art 100/E.	IDR	Alien registration system	Immigr. Off.
	art 100/F.	HERMON	Warrant information system	Police
	art 100/F.	JÁROK	Vehicle registry	Central Office
BK	art 100/G.	HERMON	Warrant information system	Police

23

The current status of SIS II development in Hungary

- The IT infrastructure for SIS II operation is installed (separate from SIS I).
- The central part of National System (NS.CP) and the SIRENE application development is done.
- The system development and integration process for ensuring the data services of the national systems is fulfilled.
- The Hungarian party is ready for integration and operational tests with CS.SIS.

24

Summary

- Hungary fulfilled all the technical developments for SISone4ALL project (necessary tests have been completed.)
- Hungary has prepared the legal and organisational environment for Schengen operation.
- (Hungary is ready for lifting of the Schengen borders.)

25

Questions

26

Thank you very much for your kind attention

Gabor Egri

MOTOMESH SOLO ÁTTEKINTÉS

MOTOMESH Solo áttekintés

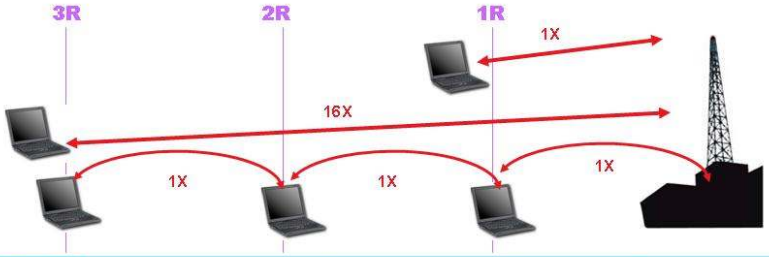
Motorola Confidential Proprietary, File Name, Rev Number, RM
MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office.
All other product or service names are the property of their respective owners. © Motorola, Inc. 2005

A bemutató felépítése

- Előzmények
- Elvi működés
- Az eszközök
- Alkalmazások

A tényezők

- Modulációtól függetlenül az RF vevő működéséhez egy minimális energia/bit arány szükséges
- Adott teljesítmény mellett a készülékek a Távolságot vagy Adatsebességet csak egymás rovására növelhetik
- Mesh technológia (vagyis a Multi-Hopping) használatával a fizika törvényei bennünket segítenek



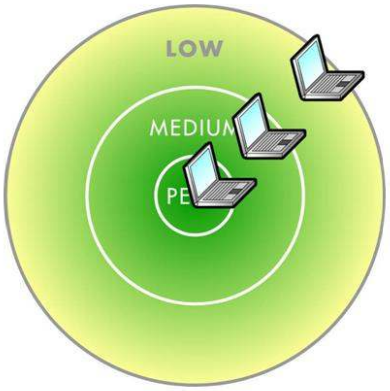
Motorola Mesh hálózati megoldások

Fercom

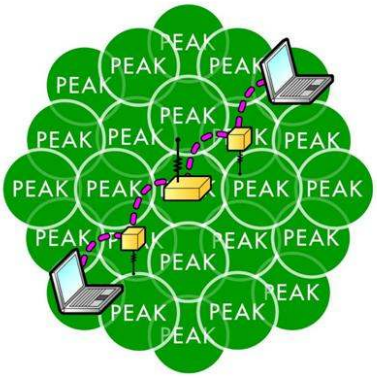
MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners. © Motorola, Inc. 2005

MOTOROLA

Adatsebesség és Kapacitás



Cella alapú hálózati infrastrukturáknál **Távolság/Sebesség** probléma:
A legtöbb készülék nem tudja a legnagyobb kapacitást kihasználni – **Alacsony hatékonyság**



Minden csatorna és készülék csúcs átviteli kapacitással működik – **Maximális hatékonyság**

Motorola Mesh hálózati megoldások

Fercom

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

Ad Hoc *és* Infrastruktura együttműködése

Teljesítmény, méretezhetőség és túlélőképesség támogatása ***ad hoc és infrastruktura alapú*** működéssel

Ad Hoc Mód

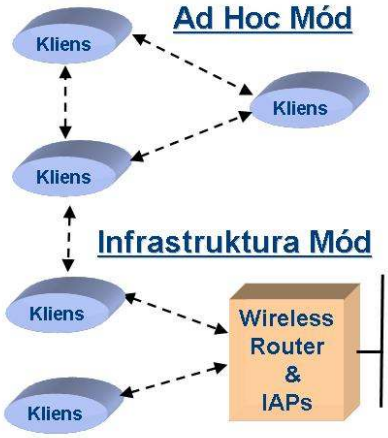
- Kliens – Kliens kommunikáció
- A kliensek egymáson keresztül is elérhetnek más klienseket vagy a hálózatot

Infrastruktura Mód

- A kliens közvetlenül kapcsolódik a Wireless Router-ekhez vagy az Intelligent Access Point-okhoz

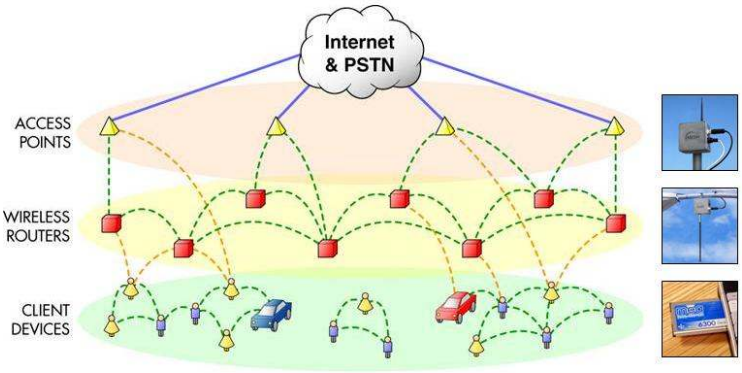
Mindkettőt egyszerre támogató egyedi megolás

- Lefedettség és megbízhatóság növelése a rendszer egésze teljesítményének növelésével



Valódi Mesh hálózat

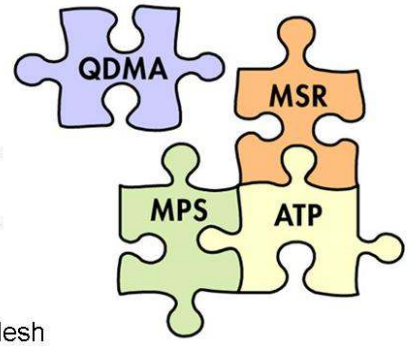
Veleszületett nagy teljesítmény és méretezhetőség



Motorola Mesh hálózati megoldások
Fercom
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

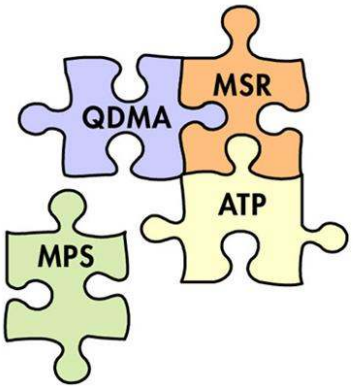
QDMA: Quadrature Division Multiple Access Radio

- 2.4 GHz ISM II sáv
- Mesh Optimalizált Rádió
- Többcsatornás
  - 3 adat és egy kontroll csatorna
- Csomagonkénti dinamikus csatorna választás
  - Hatalmas interferencia elnyomás
  - Nagy adatsűrűség
  - Optimalizált spektrum-használat
  - Nagyobb méretezhetőség más Mesh megoldásokkal szemben



MPS: Mesh Positioning System

- Beltéri és kültéri működés
  - Nem GPS alapú
- 3 követési mód:
- Abszolút
  - Referencia a hálózat infrastrukturából
    - Telepített hálózat
    - GPS koordináták
- Relatív
  - Hordozható router-ekhez viszonyított
  - Pozíció a területen belül
- Közelség
  - A közeli csomópontokhoz való közelséget mutatja



Motorola Mesh hálózati megoldások
Fercom
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

MEA 2.4 termékek

Motorola Confidential Proprietary, File Name, Rev Number, RM
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

MEA Előfizetői Hálózati Elemek
WMC6300 Vezetéknélküli Modem Kártya

- **Ad Hoc kliensek közi hálózatok**
- **Kliens és infrastruktura kapcsolatok**
- **Eszköz meghajtó támogatások**
  - –Windows támogatás
  - –Pocket PC 2002/2003
- **Type II PCMCIA kapcsolat**
- **Rádiós távkezelés**

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

MEA Előfizetői Hálózati Elemek
VMM6300 Jármű telepített modem

- **Teljes WMC6300 funkcionalitás**
- **Gépjárműben telepített**
  - 12 vdc
  - Mágnestalpas antenna
- **RJ45 Ethernet csatlakozó**
  - Három külön IP cím támogatás
- **Belső ventillátor**
- **Folyamatos hívásátadás minden csatlakoztatott eszköz számára**
  - 402 kph sebességig

MEA Infrastruktura Hálózati Elemek
MWR6300 Wireless Router

- **Vezetéknélküli lefedettség**
- **Automatikus hálózat kiegyenlítés**
- **Rádiós távkezelés**
- **Pozíció meghatározási referenciapont**
- **NEMA4 foglalat**
- **AC vagy DC (5-14 vdc)**

MEA Infrastruktura Hálózati Elemek
EWR6300 Továbbfejlesztett Vezetéknélküli Router

- **Minden PC kártya és vezetéknélküli router funció**
- **Kettő az egyben készülék**
- **RJ45 Ethernet port**
  - Három külön IP cím támogatás
- **NEMA4 foglalat**
- **AC vagy DC (5-14 vdc)**

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

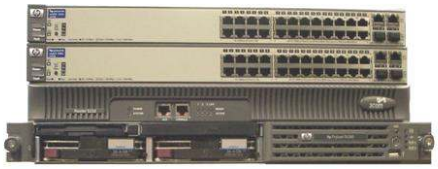
MEA Infrastruktura Hálózati Elemek
IAP6300 Intelligens Hozzáférési Pont

- **Vezetékes hálózati hozzáférés**
- **6Mbps Burst Rate**
- **Hálózati kapacitást biztosít**
- **Rádiós távkezelés**
- **Pozíció meghatározási referenciapont**
- **NEMA4 foglalat**
- **AC vagy DC (5-14 vdc)**

Motorola Mesh hálózati megoldások
Fercom
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

MEA Kezelő Rendszer (Management System) MeshManager™

- **Linux alapú**
- **Nagyteljesítményű hálózat és végkészülék kezelő eszköz**
- **Azonosítás és jogosultság kezelés**
- **Szabvány IP VPN kezelés**
- **Távoli rádiós (Over the Air, OTA) frissítés**
- **Csak szoftverként elérhető**
  - A felhasználók maguk biztosítják helyben a HP eszközt
  - Helyi tápfeszültségi és garancia viszonyok biztosítása
- **Futási licencek szükségesek**
  - Azonosítás és jogosultság funkciók biztosítása
  - 50 felhasználónként



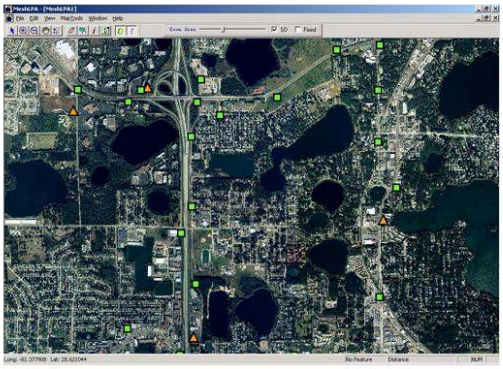
MeshManager EZ

- **Microsoft XP Pro rendszeren fut**
- **Max 50 hálózati elemet támogat**
- **Csak software eszköz**
- **SnapGear SG300 funkció szükséges a DHCP Szerver képességhez**
- **A Windows Szerver 2003 ezt kiegészítés nélkül biztosítja**

Motorola Mesh hálózati megoldások
Fercom
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

Mesh Positioning Application - MPA

- Az infrastruktura és a végfelhasználói készülékek helyzet-meghatározására és követésére szolgál
- A World Geodetic System 1984 (WGS84) formátumot használja
  - Készülékek követése és pozicionálása:
    - Valósidőben a térképen
    - Műholdképen
    - WGS84 formátumú képen
- Elérhető világtérképpel konfiguráltan



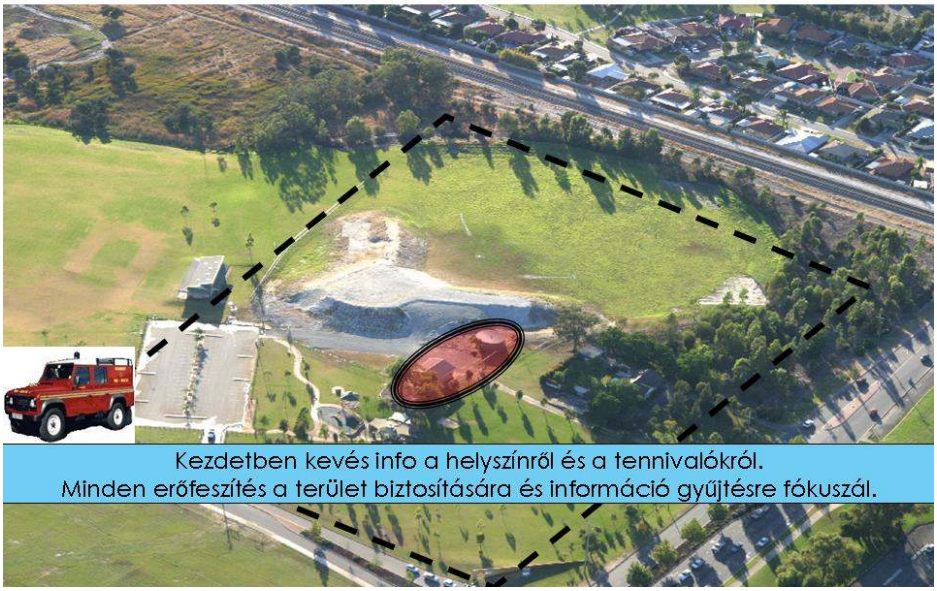
MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office.
All other product or service names are the property of their respective owners. © Motorola, Inc. 2005

Gyorsreagálás

Taktikai megoldás

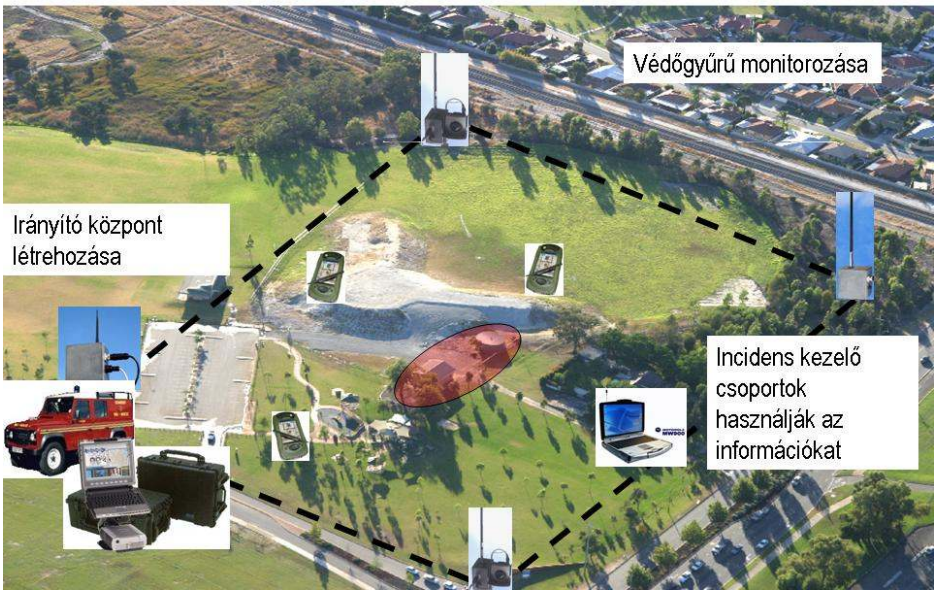
Motorola Confidential Proprietary, File Name, Rev Number, RM
MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office.
All other product or service names are the property of their respective owners. © Motorola, Inc. 2005

Gyorsreagálású csapatok – Védőgyűrű felállítása



Gyorsreagálású csapatok – mobil adatátviteli gyűrűt állítanak

Beszéd, Videó & Pozíció info áll rendelkezésre



Gyorsreagálású csapatok – mobil adatátviteli gyűrű eszközei

Motorola Mesh hálózati megoldások

Fercom

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

Vezetéknélküli Szélessávú Adateszközök
MeshNetworks Termékcsoport
Sony Kamera Project

SONY

Motorola Confidential Proprietary, File Name, Rev Number, RM

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 Mesh hálózat alapú Digitális Videó Megfigyelő Rendszer

IP Video adatfolyam a Motorola Mesh hálózati technológiával

- Automatikus,önformáló, önjavító, nagy túlélő képességű vezetéknélküli kommunikáció
- Mobil videó elérést biztosít járművekből és felé (autók, buszok, vonatok stb.)
- Szélessávú adatátvitel biztosítja a kiváló minőségű videó jel áramlását
- Korszerű IP biztonság

Sony Digitális Videó és Mesh Hálózat előnyei

- Vezetéknélküli videó kamerák könnyen telepíthetőek bárhová
- A telepítési költségek jelentősen alacsonyabbak
- Meshing lehetőséget nyújt vészhelyzetben Ad-Hoc telepítésekre
- Kliens-kliens kommunikációval infrastruktura nélküli üzemelés

Digitális Videó Megfigyelő alkalmazások

- Közbiztonsági alkalmazások – Rendőrség, Tűzoltóság, Katasztrófavédelem stb.
- Azonnali eseménykezelés és védőgyűrű felállítás
- Iskolák, közparkok, repterek, alagutak stb. biztonsági megfigyelése
- Ideiglenes megfigyelés különleges rendezvények vagy események idején

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 & Sony Videó Megfigyelő Megoldások - MeshCam

Sony kamerák támogatják a Motorola Mesh termékcsaládot

- Sony a MeshNetwork Linux driver-eket integrálta a Multi-Codec IP Product Line firmware-be – a Sony IP kamerák Mesh kommunikáció képesek

Sony Multi-Codec kamerái támogatják a Motorola Mesh PCMCIA kártyákat

- SNC-RX550N(NTSC) vagy P (PAL) fekete-fehér kamera
- SNC-RZ50N or P
- SNC-CS50N or P

IP kamera telepítési költségek csökkentése

- A Sony kamera Mesh kliensként viselkedik a hálózatban
- Nincs szükség kiegészítő Ethernet eszközökre
- Szorosra font Motorola/Sony együttműködés, közös megoldás
- Egyszerű telepítés, alig észrevehető a lámpaoszlopon

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

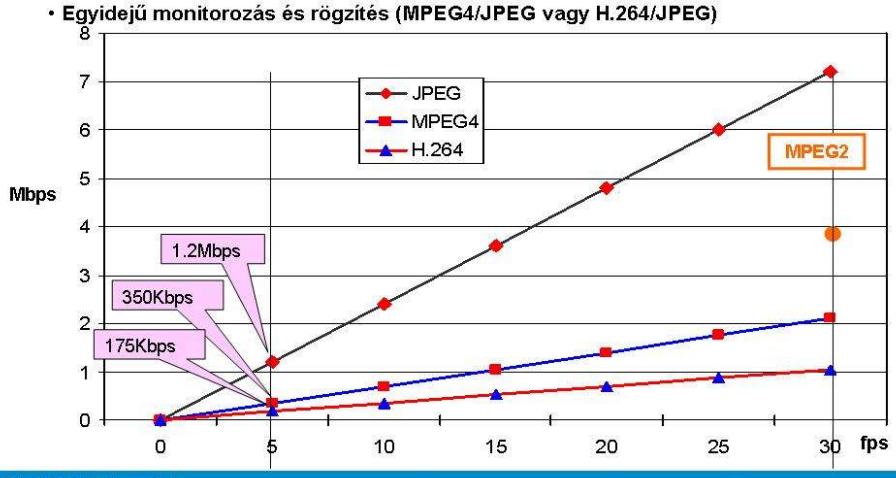
Sony kamera funkciók

Feature	SNC-RX550	SNCRZ50	SNC-CS50
Key Features	Pan 360 continuous, Tilt 0 to +90	Pan +/-170, Tilt +25 to -90	Super Exwave CCD, High sensitivity Fixed Camera
Zoom	26x optical 12x digital	26x optical 12x digital	Lens Selected by Customer
Data Interface	PCMCIA Card Bus, Local recording w/ ATA memory card	PCMCIA Card Bus, Local recording w/ ATA memory card	PCMCIA Card Bus, Local recording w/ ATA memory card
Other Interfaces	Local recording, Accepts Memory Stick Pro	Compact Flash, Local recording w/ ATA memory card	---
Privacy Zone Masking	Spherical (3-D) tracing	Spherical tracing	---
Sensor I/O	Input x 2, Output x 2	Input x 2, Output x 2	Input x 2, Output x 2
RS-232C	Data Transparency, VISCA control	Data Transparency, VISCA control	Data Transparency
PoE	No	No	Yes
Available	1Q06	3Q06	3Q06

Sony-Motorola kamera megoldás

Why Multi-codec? Multi-codec termékek

- Kisebb sávszélesség igény
- Kisebb tárhely igény
- Egyidejű monitorozás és rögzítés (MPEG4/JPEG vagy H.264/JPEG)



Köszönjük a figyelmet !

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

Hungaro DigiTel Kft.

MŰHOLDAS MEGOLDÁSOK AZ ÁLLAMI SZERVEK TÁVKÖZLÉSI IGÉNYEINEK KISZOLGÁLÁSÁRA

Műholdas szolgáltatás adottságai

- A Hungaro DigiTel Kft. kétirányú adatátviteli utat biztosít (szükség esetén egyirányút is)
- Magas rendelkezésre állás (Csillag topológia)
- Alapvetően aszimmetrikus adatátviteli sebességek

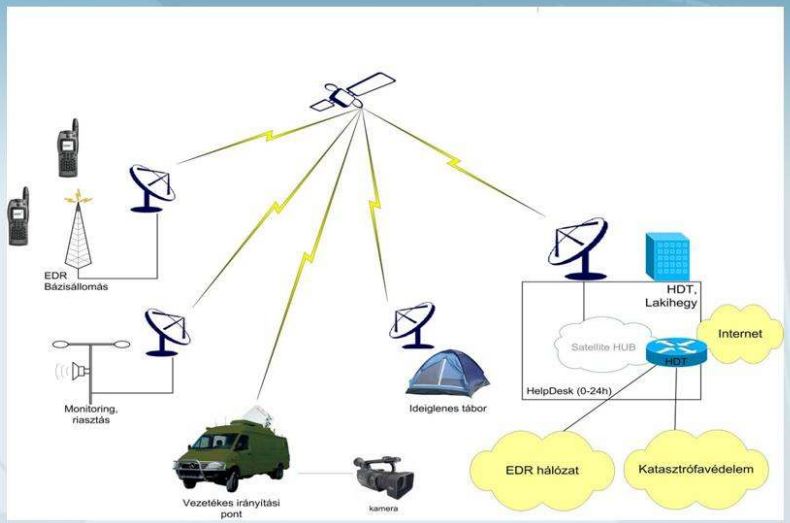
Alacsony sávszélességet igénylő alkalmazások kiszolgálása X.25 és IP technológián

Alkalmazási területek:

- Felügyelet nélküli telephelyek automatizálási, beléptető, stb. rendszereinek távközlési kiszolgálása
- Adatgyűjtő rendszerek (vegyvédelmi vagy árvízvédelmi mérőhelyek távközlési ellátása)

Szélessávú szolgáltatások

- VPN hálózatok részleges vagy egységes kiszolgálása
- Teljes értékű backup (Földi hálózattól független összeköttetés biztosítása)
- HDTSat Express (ideiglenes helyszínek kiszolgálása)
- Felügyelet nélküli telephelyek kamerás megfigyelése on-line vagy riasztáskori képfelküldés



Elérhető adatátviteli sebesség

Alacsony sávszélességű rendszerek

Letöltési irány: < 512 kbps

Feltöltési irány: < 76.8 kbps

Szélessávú rendszer

Letöltési irány: < 6 Mbps

Feltöltési irány: < 1 Mbps

Tipikus szélessávú sávszélességek:

256/64 kbps *512/128 kbps*

384/64 kbps *1M/256 kbps*

Hálózat-felügyelet

- 24/7 órás HelpDesk
- Proaktív hibakezelés
- Elektronikus hibajegy rendszer
- Országos szervízhálózat,nemzetközi partnerekkel kiegészítve
- Igénytől függően – akár 4 órás hibaelhárítás

- Beállításokat távolról képes módosítani
- A rendszer állapotáról az NMS segítségével mindig pontos információkat tud adni

Pont-Pont (SCPC) összeköttetések

- Földi béreltvonalak analógiájára
- Dedikált sávszélesség/műhold szegmens
- Nagy adatátviteli sebesség (n x 64kbps-től akár E3 34 Mbps)
- Távközlésben használatos bármely interfész biztosítható
- Szinte a világ bármely két pontja összeköthető
- Versenyképes ár

Pont-Multipont (MCPC) összeköttetések

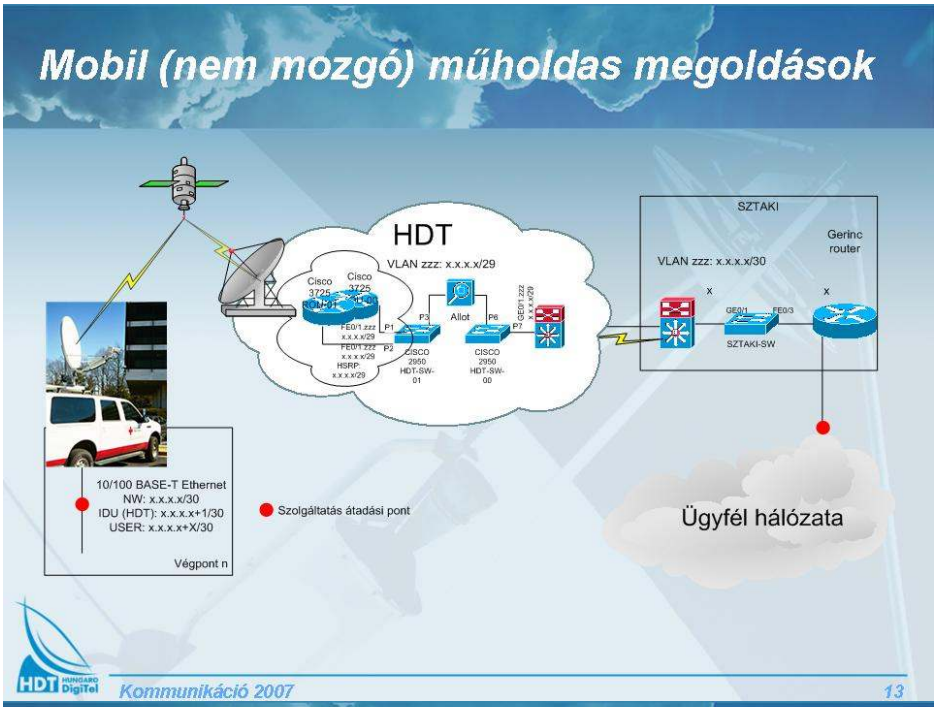
- Az SCPC-hez hasonló szolgáltatás, azonban dinamikus sávszélleség allokációt alkalmaz.
- A rendszer a műholdas kapacitást automatikusan, a leghatékonyabb módon rendeli hozzá ahhoz az állomáshoz, mely átviteli kapacitást kér.
- A valós idejű adat és a nem valós-idejű adat párhuzamosan kerül átvitelre, a különböző prioritási szintek segítségével, a garantált szolgáltatási minőség megtartása mellett.

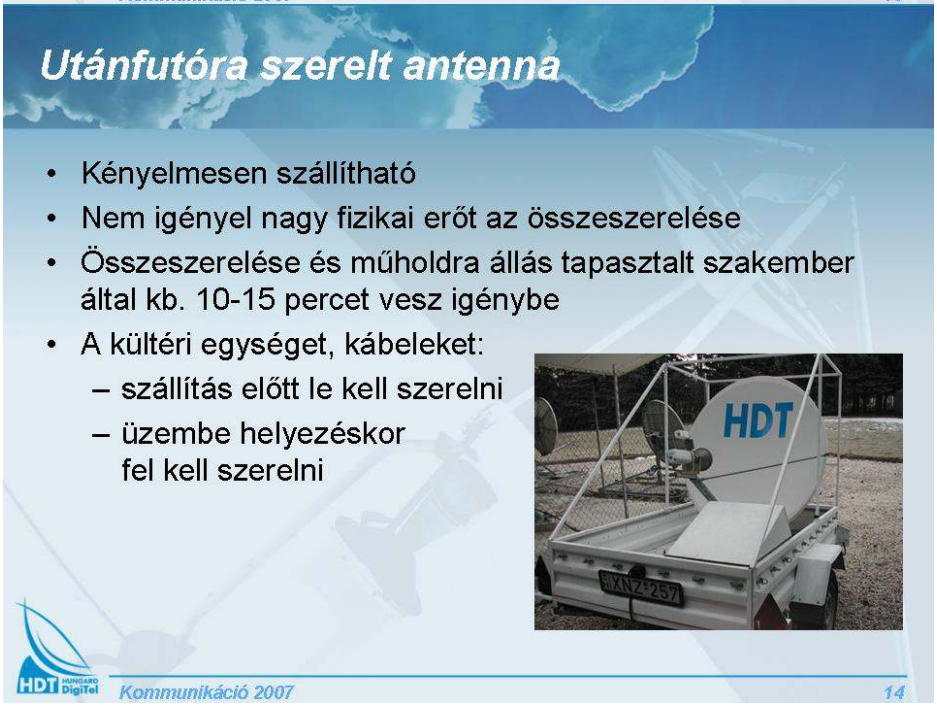
Az MCPC hálózatok jellemzői:

- Csillag, hibrid vagy háló hálózati topológia
- Magas burst képesség 64 kbit/s-tól 8.75 Mbit/s-ig
- Dinamikus Sávszélesség Allokáció IP és Frame Relay adatok átviteléhez, mely 70 Mbit/s teljes hálózati kapacitást biztosít
- Optimalizált sávszélesség felhasználás
- Garantált sávszélesség a valós-idejű szolgáltatásoknak
- Választható Ethernet / Fast Ethernet port
- Beépített IP Routing és TCP gyorsítás

Alkalmazási példák

- EDR bázisállomások
  - Tartalékolása
  - Elsődleges kiszolgálása a földfelszíni hálózattal nem elérhető helyeken
- Telefonközpont kihelyezés
- Szélessávú Internet/Intranet elérés
- Videokonferencia


Mobil (nem mozgó) műholdas megoldások
HDT
VLAN zzz: x.x.x.x/29
Cisco 3725
Cisco 3725
FE0/1.zzz x.x.x.x/29
FE0/1.zzz x.x.x.x/29
HSRP: x.x.x.x/29
P1
P2
P3
P6
P7
Allot
CISCO 2950 HDT-SW-01
CISCO 2950 HDT-SW-00
GE0/1.zzz x.x.x.x/29
SZTAKI
Gerinc router
VLAN zzz: x.x.x.x/30
x
x
GE0/1
FE0/3
SZTAKI-SW
10/100 BASE-T Ethernet
NW: x.x.x.x/30
IDU (HDT): x.x.x.x+1/30
USER: x.x.x.x+X/30
Végpont n
Szolgáltatás átadási pont
Ügyfél hálózata
Kommunikáció 2007
13


Utánfutóra szerelt antenna
• Kényelmesen szállítható
• Nem igényel nagy fizikai erőt az összeszerelése
• Összeszerelése és műholdra állás tapasztalt szakember által kb. 10-15 percet vesz igénybe
• A kültéri egységet, kábeleket:
– szállítás előtt le kell szerelni
– üzembe helyezéskor fel kell szerelni
HDT
Kommunikáció 2007
14

Gépjárműre szerelhető antennák

- 1 gombnyomásra üzemképes
  kb. 5 perc
- Automatikus műholdra állás
- Gyors műholdra állás
- Könnyen szállítható
- Nem kell minden helyszínen
  - összeszerelni
  - szétszerelni
- Nem igényel szakértelmet
- Nem igényel fizikai munkát

Gépjárműre szerelhető antennák

Működési környezet:

Hőmérséklet:

-15°C – 52°C

Szélsebesség:

max. 72 km/h

(szállítás esetén max. 161 km/h)

Áramfelvétel:

110-240VAC, 1 fázis, 50/60 Hz

max. 6/3 A csúcs,

max. 1 A folyamatos

Mobil műholdas felhasználási példák

- Mobil ellenőrzési pont felállítása
- Parancsnoki gépjárművek bekötése a belső hálózatba
- Katasztrófavédelmi feladatok szervezése a helyszínről
- Videó jel továbbítás a helyszínről/helyszínekre
- Hang továbbítás a helyszínről
- Központi adatbázisok elérése változó helyszínekről

Bemutatkozás

Fő tulajdonosaink:

– Antenna Hungária Rt. (TDF csoport) : 55%

– PT Ventures SA (Portugal Telecom csoport): 45%

Piaci részesedés:

Magyarország és Közép-Európa piacvezető VSAT szolgáltatója

Piaci részesedése több, mint 60 %

Alaptőke: ~ 900 M Ft

Éves árbevétel: ~1,5 Mrd Ft

Végpontszám: >2800 db

Köszönöm megtisztelő figyelmüket.

Továbbiakban is szívesen áll rendelkezésükre

Lázár János
kereskedelmi igazgató
e-mail: lazar@hdt.hu

Zautasvili Péter
fejlesztési igazgató
e-mail: zautasvili@hdt.hu

2310 Szigetszentmiklós-Lakihegy, Komp u.2.
Tel:+3614888500
Fax:+3614888501
WEB: http://www.hdt.hu

MÁTÉ József

A KATASZTRÓFAVÉDELEM 2007. ÉVI FŐ PROJEKTJEI

Országos Katasztrófavédelmi Főigazgatóság

A
Katasztrófavédelem
2007. évi főbb projektjei

Kommunikáció 2007
konferencia
ZMNE
2007 október 17.

Máté József pv. ezredes
Informatikai és Távközlési főosztály főosztályvezető

2007.10.01. 1

A Katasztrófavédelem feladatrendszerét az alábbi törvények, kormányrendeletek határozzák meg:

Az 1996. évi XXXVII. törvény a Polgári Védelemről, valamint a 1999. évi LXXIV. Törvény (továbbiakban: Kat. Tv.) IV. fejezete, továbbá 1996. évi XXXI. törvény a tűz elleni védekezésről, a műszaki mentésről és a tűzoltóságról és az érvényben lévő kormányhatározatok és rendeletek.

A Kat. Tv. 14. paragrafusa határozza meg a katasztrófavédelmi célú távközlési és informatikai rendszerek egységes irányítási rendszerbe történő kialakítását és működtetését). Az Kat. Tv. 5.§ e. pontja kimondja, hogy a Kormány feladata a katasztrófavédelmi információs rendszer létrehozása.

2007.10.01. 2

A Katasztrófavédelem híradó rendszerei

- Egységes Digitális Rádiótávközlő rendszer
- Dunai Információs Segélyhívó Rendszer
- Tiszai Információs Segélyhívó Rendszer
- Balatoni és Velence-tavi Viharjelző Rendszer
- Lakossági riasztó és tájékoztató rendszerek
- Monitoring és Lakossági Riasztó Rendszer (MoLaRi)

2007.10.01. 3

Egységes Digitális Rádiótávközlő Rendszer

Megye	kézi EDR készülék		mobil EDR		asztali EDR	tartalék kézi EDR készülék	tartalék mobil EDR Készülék	kézi EDR megyei célzott tartalék
	alap	gps	1 kezelős	2 kezelős				
Baranya	115	8	30	30	13	20	10	25
Bács-Kiskun	181	9	56	48	27	22	11	25
Békés	119	9	35	28	17	19	11	25
Borsod-Abaúj-Zemplén	193	12	55	45	22	27	14	25
Csongrád	124	8	32	32	15	21	10	25
Fejér	113	8	36	28	18	17	8	25
Győr-Moson Sopron	125	8	32	30	12	22	10	25
Hajdú-Bihar	129	9	41	33	21	17	9	25
Heves	106	8	32	24	14	18	9	25
Jász- Nagykun- Szolnok	144	9	42	39	20	20	11	25
Komárom- Esztergom	126	7	39	31	19	18	9	25
Nógrád	76	7	26	13	13	15	7	25
Pest	221	14	68	50	31	27	14	25
Somogy	139	8	43	34	20	20	10	25
Szabolcs-Szatmár Bereg	168	10	52	41	26	20	10	25
Tolna	102	8	34	21	16	16	8	25
Vas	110	8	36	25	18	17	8	25
Veszprém	147	9	43	38	21	21	11	25
Zala	122	9	36	28	15	20	9	25
Összesen	2560	168	768	618	358	377	189	475
Összesen bruttó	5513							

EDR készülékek

NOKIA THR 880

NOKIA TMR 880

SEPURA SRH 3800s

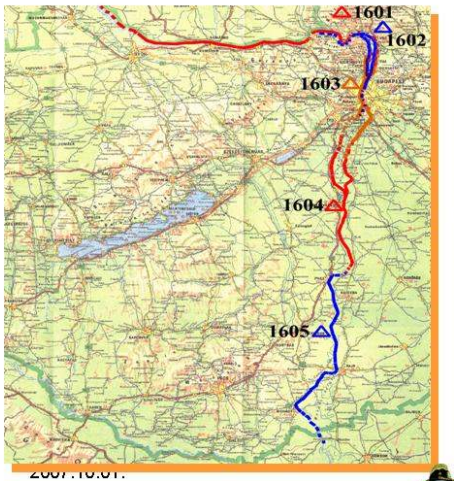
Motorola MTM 800

Sepura gateways mobil

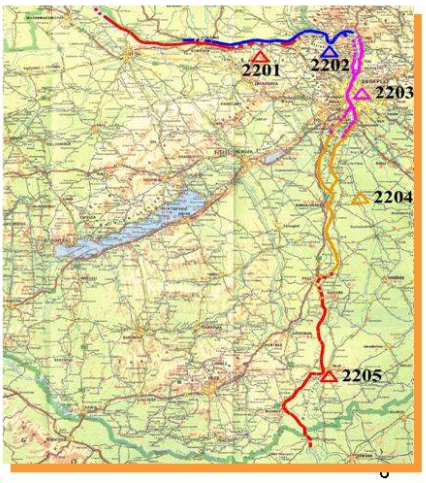
2007.10.01. 5

A Duna magyarországi szakaszán telepített átjátszó állomások

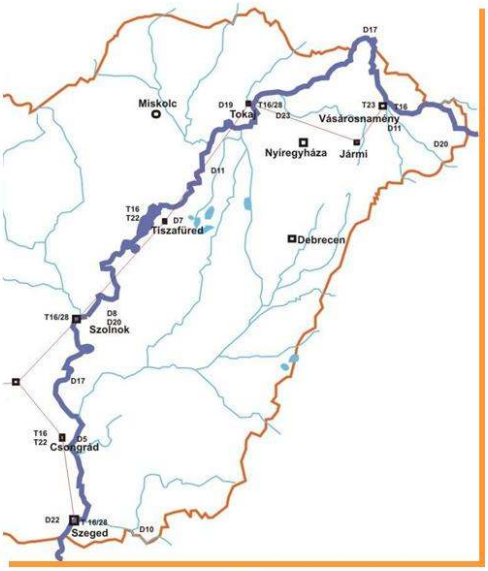
16. Segélyhívó csatorna



20. Információs csatorna

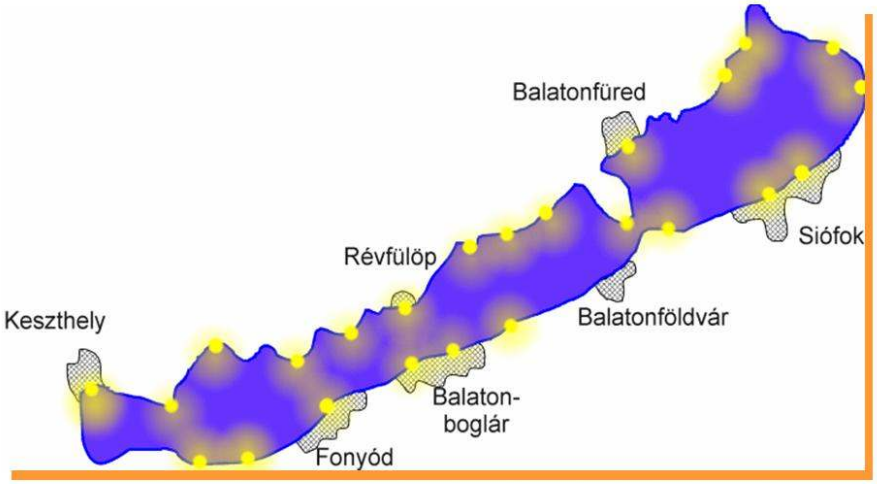


A Tiszai Információs Segélyhívó Rendszer átjátszóállomásai :



2007.10.01. 7

A Balatoni viharjelzőrendszer



A parton található viharjelző egységek elhelyezkedése

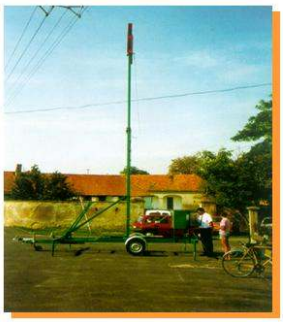
2007.10.01. 8

A Balatoni és Velence-tavi viharjelző rendszer

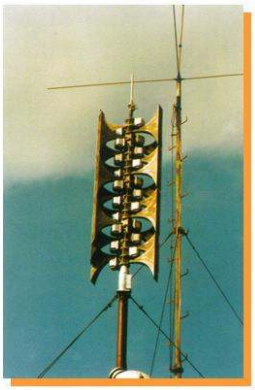
2007.10.01. 9

Lakossági riasztó és tájékoztató eszközök

Vasbeton oszlopra telepített motorsziréna



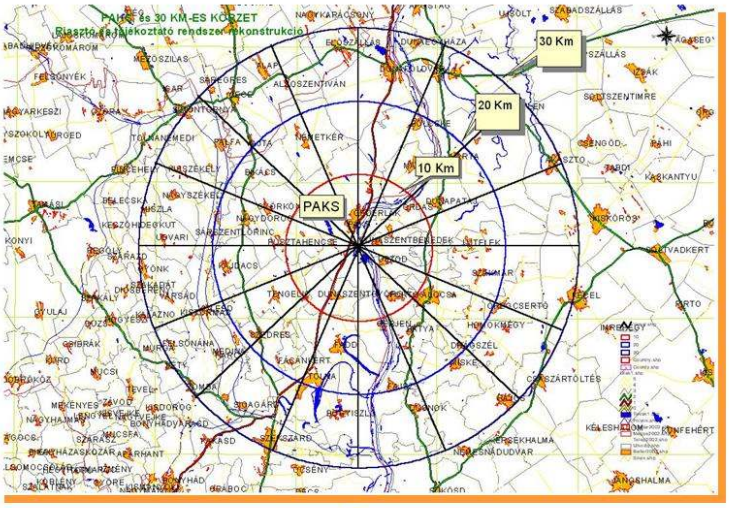
Mobil kivitelű tájékoztató-riasztó eszköz



Elektronikus sziréna

2007.10.01. 10

Paks és 30 km-es körzetében működő lakossági riasztó-tájékoztató rendszer



2007.10.01. 11

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.

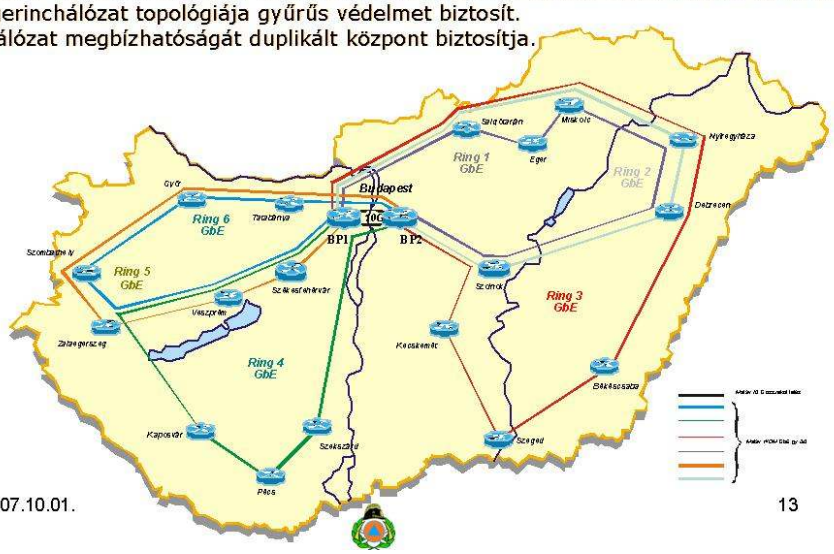
-A megvalósított infokommunikációs rendszer megfelelő hátteret biztosít a hatékony, kockázatelemzésre épülő, döntési alternatívákat adó, országos lakossági, települési adatokra épülő, osztott-egységes adatbázisú alkalmazások segítségével a helyi, regionális és országos kiterjedésű veszélyhelyzetek kezelésének informatikai támogatására.

-Jogosultság szerinti hozzáférést biztosít a katasztrófavédelem munkatársai részére a hatósági és veszélyhelyzet-kezelési szakterület által alkalmazott rendszerek adatállományához.

2007.10.01. 12

Az Egységes Kormányzati Gerinc

-A hálózat alapja DWDM technológia. **(nagysűrűségű hullámhossz multiplexálás)**
- Az országos gerinchálózat 6 db Gigabit Ethernet gyűrűvel került megvalósítására.
- Magyar Telecom és az EKG csomópontokat független optikai nyomvonalak kötik össz
- A gerinchálózat topológiája gyűrűs védelmet biztosít.
-A hálózat megbízhatóságát duplikált központ biztosítja.



Az OKF EKG-s VOIP hálózata

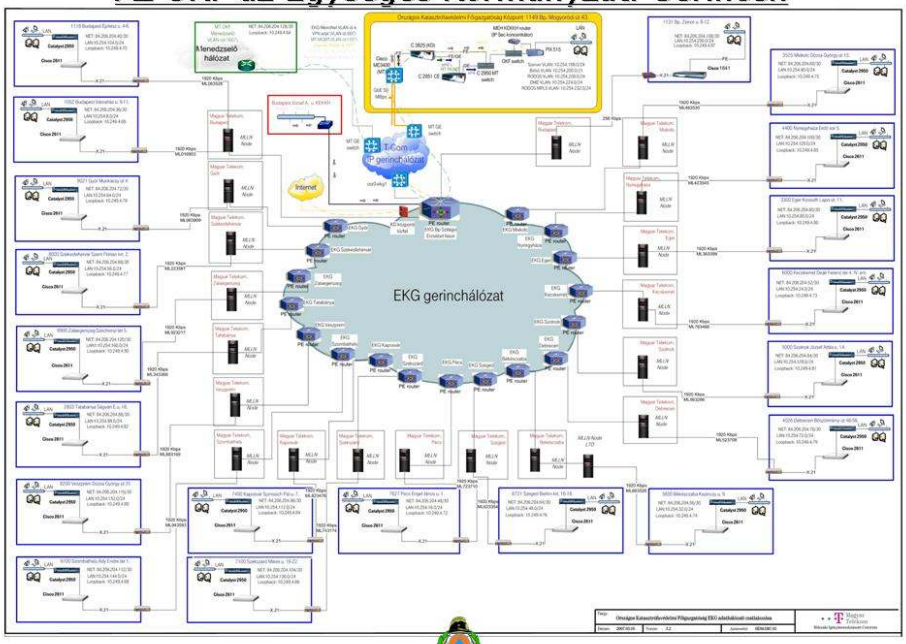
-Az OKF központban Siemens Hipath 4000 típusú központ 4 db ISDN 30-al (egyidejűleg 120 hangcsatorna).

- A központban és a végpontokon lévő Magyar Telekom fenntartású aktív eszközök távmenedzseltek.

-Az igazgatóságokon Siemens HiPath 3550 típusú IP alközpontok, melyek voice gateway nélkül biztosítják a hangforgalom IP gerinchálózaton történő kezelését.

-A telepítendő központok alapkiépítésben 8 fővonallal és 48-64 mellékkel kerültek leszállításra.

Az OKF az Egységes Kormányzati Gerincen



Központi Ügyeleti Információs Rendszer (IP / KÜIR) / Intranet Portál

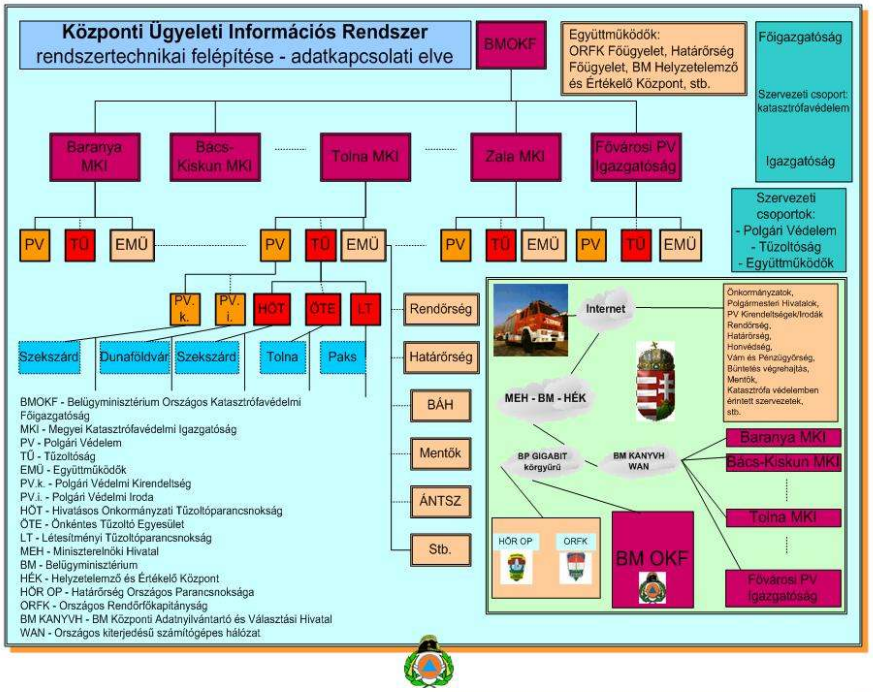
-olyan infokommunikációs rendszer, amely széles körben felöleli a katasztrófahelyzetben, veszélyhelyzet-kezelésben érintett szervezeteket,

- lehetőséget teremt az elektronikus kapcsolattartásra, csoportmunkára, adatátvitelre, központi Intranet Portál szolgáltatások biztosítására (Dokumentumtár, Hírlevél, Fórum, stb.),

- biztosítja az űrlapalapú adatszolgáltatást:

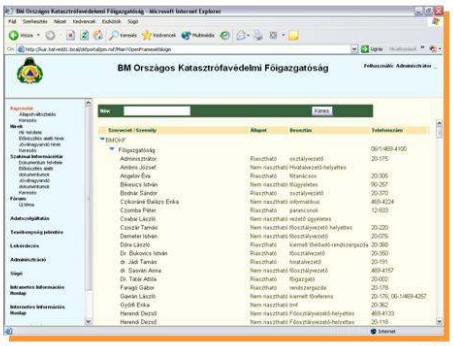
a. Létszám adatok (riasztható, nem riasztható, készenlétben, bevetésen)
b. Szerállapot nyilvántartás
c. KAP (Káreset Adatszolgáltatási Program)
d. RST (Riasztási és Segítségnyújtási Terv)
e. Rendkívüli időjárás (hóhelyzet) jelentés
f. Ár- és belvíz adatszolgáltatás

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.

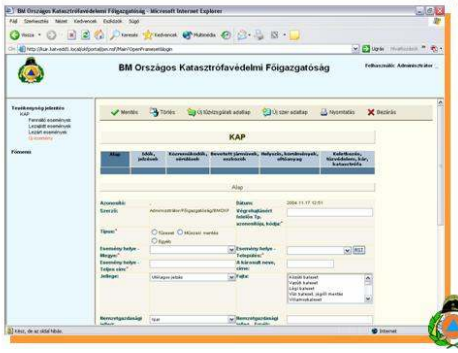


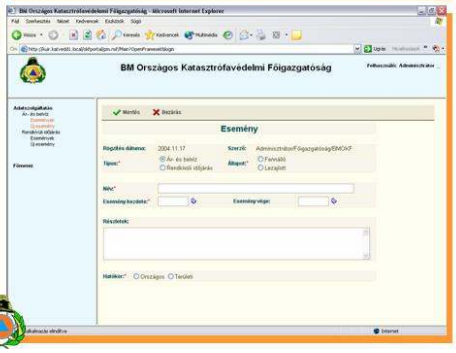
KÜIR:

- **Kapcsolatok**
- **Adatszolgáltatás**
- **Tevékenység jelentés**



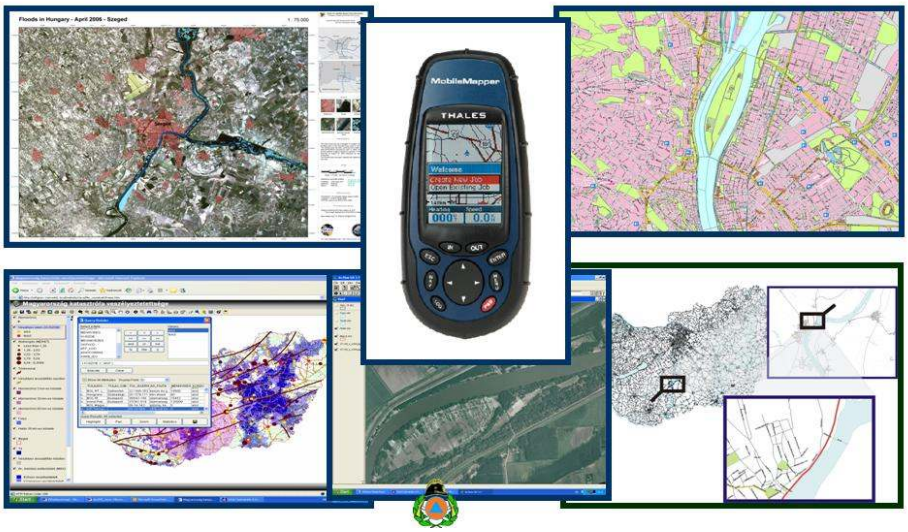
Regisztrált szervezetek: közel 400
Regisztrált felhasználó:2500 felett





A TÉRINFORMATIKA HELYE A KATASZTRÓFAVÉDELEMBEN

A katasztrófavédelem számára a térinformatika a veszélyhelyzet környezetének vizuális felderítésében, kiterjedésének megállapításában, a változások követésében, a mért adatok továbbításában hoz új minőséget.



A KATIR KIALAKÍTÁSA

A katasztrófavédelem országos térinformatikai rendszerének kialakítását és formálását befolyásoló tényezők:

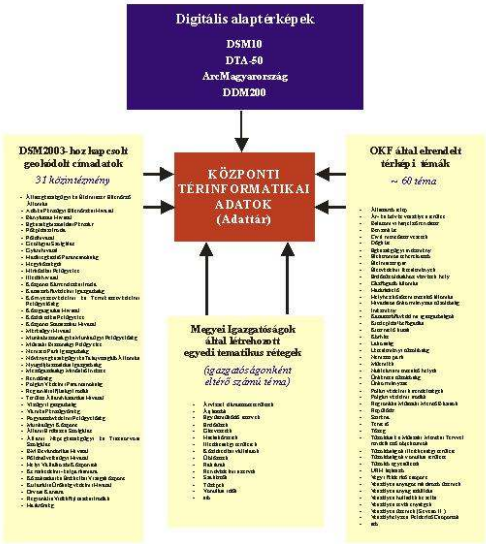
- **Stratégiák**
  (Pl.: A Magyar Információs Társadalom Stratégiája; Az Önkormányzati Is Területfejlesztési Minisztérium ágazati szintű informatikai stratégiája; A Katasztrófavédelem Országos Információs rendszere kialakításának stratégiája)
- **Jogszabályok és szabályozások**
  (Pl.: 1996. évi LXXIV. törvény a földmérési tevékenységről; DAT szabvány)
- **Térinformatikai eszközök piaci kínálata**
- **A katasztrófavédelem infokommunikációs háttere és annak fejlesztési elképzelései**
- **Pénzügyi források**
- **Humán erőforrás rendelkezésre állása, felkészültsége és befogadó készsége**
- **A „vizuális" megjelenítés igénye a vezetői és a szakterületi tájékoztatásban, valamint a lakosságtájékoztatás szerepének felértékelődése**

ADATOK

1996.évi. LXXIV. törvény 15.§-a alapján az állami és helyi önkormányzati térinformatikai rendszerek alapjául csak az állami térképeket és állami alapadatokat szolgálhatnak. E rendszerek térképi adatbázisaiban az egységes országos vetületi rendszerben és annak koordinátarendszerében meghatározott, vagy az abba átszámított koordinátákat kell használni.

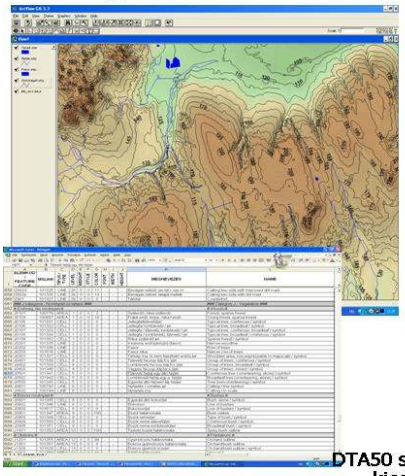
A katasztrófavédelem által használt térképek jellemzői:

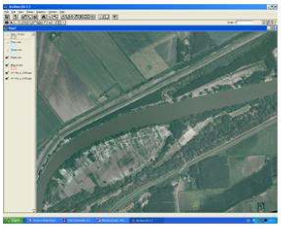
- Koordináta rendszer: 2D
- Vetület alapján: EOV
- Megvalósítás: döntően vektoros
- Méretarány: közepes (topográfiai)
  kis (tematikus)



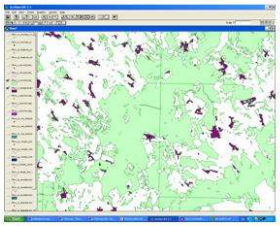
A KATIR GEOMETRIAI ALAPJA

DTA50 – interaktív felhasználásra hálózatban, egyszerre 20 felhasználóhoz



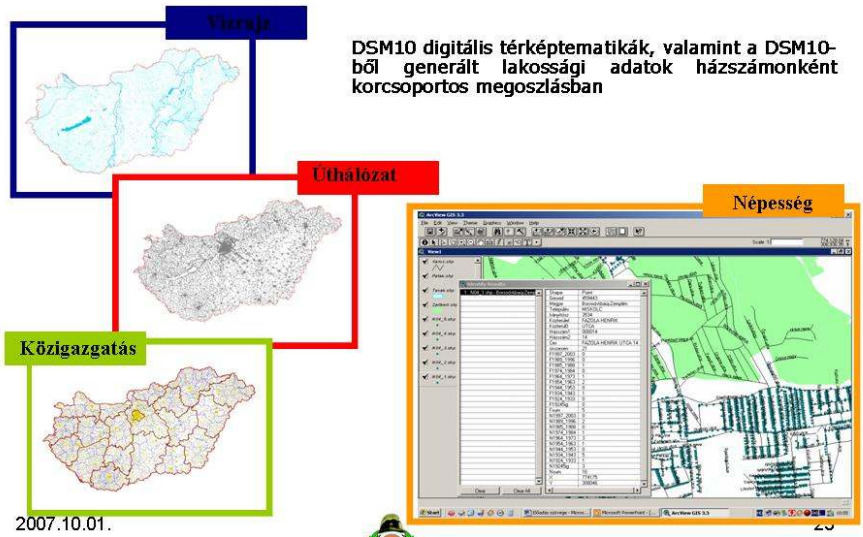


Digitális ortofoto kivágat a Tisza 1-1 km-es körzetében a partszakaszokra.



DTA50 szintvonalakat tartalmazó domborzati rétegének kiegészítése a magassági értékekat tartalmazó attribútum adatokkal

A KATIR TÉRKÉPI ALAPJAI

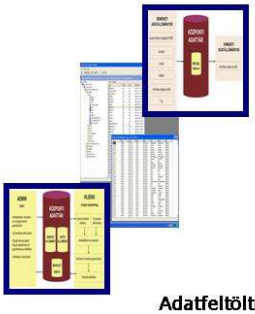


DSM10 digitális térképtematikák, valamint a DSM10-ből generált lakossági adatok házszámonként korcsoportos megoszlásban

2007.10.01. 23

KÖZPONTI ADATTÁR

Az adattár döntéstámogatási technikák gyűjteménye, mely adattárolási módszere és működése (adattisztítás, betöltés, frissítés stb.) segítségével a hagyományos tranzakció alapú rendszereknél jóval hatékonyabb elemzések elkészítését teszi lehetővé.



SQL alapú adatbáziskezelő

Metaadattár

Címinformációk egységesítése

Alaptérképek változásával a geokódok frissülnek

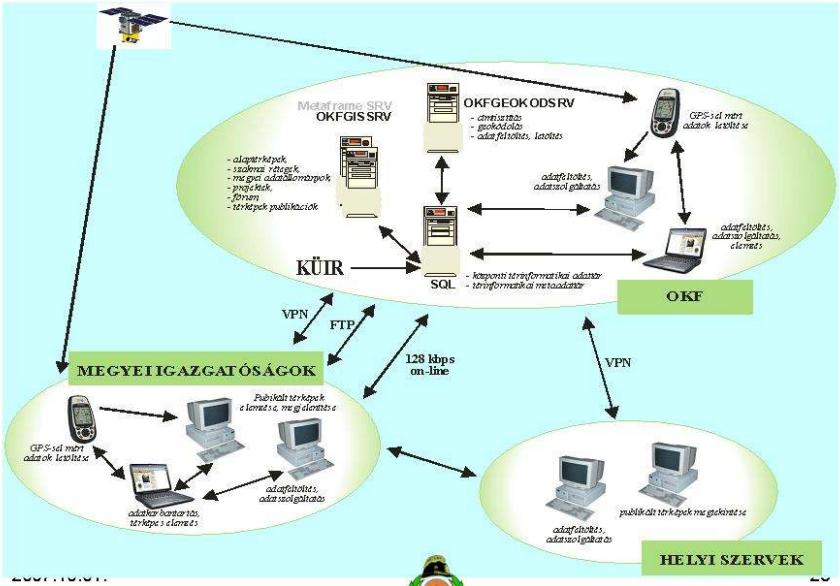
Adatfeltöltés és letöltés szigorú jogosultsági szabályok szerint

Tendencia számítási lehetőség

Egységes jelkulcs rendszer kialakítása

2007.10.01. 24

A KATIR FELÉPÍTÉSE – INFOKOMMUNIKÁCIÓS HÁTTÉR



RÖVIDTÁVÚ CÉLOK

- Tematikák címtisztítása és geokódolása
- Központi Adattárház feltöltése
- Térképpublikációk körének bővítése
- Webes felületen publikált térképek útvonaltervezésre alkalmassá tétele
- Szabadban keletkezett tüzek EU kötelezettségből adódó feladatainak térinformatikai biztosítása
- Az alkalmazott térinformatika hatékonyabbá tétele a felhasználói igények formálásával
- Szakember képzés és továbbképzés
- Információterjesztés a szakterületek felé
- Térképfrissítések finanszírozása
- Pályázati erőforrások bevonása a rendszerfejlesztésbe

26

KÖSZÖNÖM MEGTISZTELŐ FIGYELMÜKET!

jozsef.mate@katved.hu

MÉSZÁROS Árpád

TÁVKÖZLÉSI NEHÉZSÉGEKRŐL A MADÁRINFLUENZA ÜRÜGYÉN

Távközlési nehézségekről a madárinfluenza ürügyén

(A gazdaságmozgósítás egy különleges helyzete)

Mészáros Árpád
biztonsági szolgáltatási manager
Magyar Telekom Nyrt.

A 131/2003. (VIII. 22.) Korm. rendelet (A) a nemzetgazdaság védelmi felkészülése és mozgósítása feladatai végrehajtásának szabályozásáról

- **Jogi alapja a hatályon kívül helyezett 1993. évi CX. tv., vagyis a régi honvédelmi törvény.** (Erre vonatkoznak a hivatkozások.)
- **Jelenleg a 2004. évi CV tv. van életben: új honvédelmi tv.** (Ezzel nincs írott kapcsolata.)
- **A távközlés a 7. § (1) és (2) szerint stratégiai értékű kapacitásnak tekintendő.**

A 131/2003. (VIII. 22.) Korm. rendelet (B)

- **A távközlés a 12. § (2) b) szerint a gazdaságfelkészítési tervezés alá tartozik**
- Fentiek miatt gazdaságfelkészítési és – mozgósítási, szolgáltatási, védelmi és helyreállítási tevékenységekhez - **ÁC készletekkel kell rendelkezni.** (Minisztériumi feladat)
- Követelménytámasztó és felelős teljesítő szervek:
  - **ÁNTSZ a népegészségügyért, stb.**
  - GKM ~~IHM~~ **az informatikai és távközlési szolgáltatásokért**
- **Az érintett szolgáltatók közé tartozik a távközlési szolgáltatók egy köre a 6. § szerint**

A 131/2003. (VIII. 22.) Korm. rendelet (C)

A gazdaságfelkészítési tervezésről:

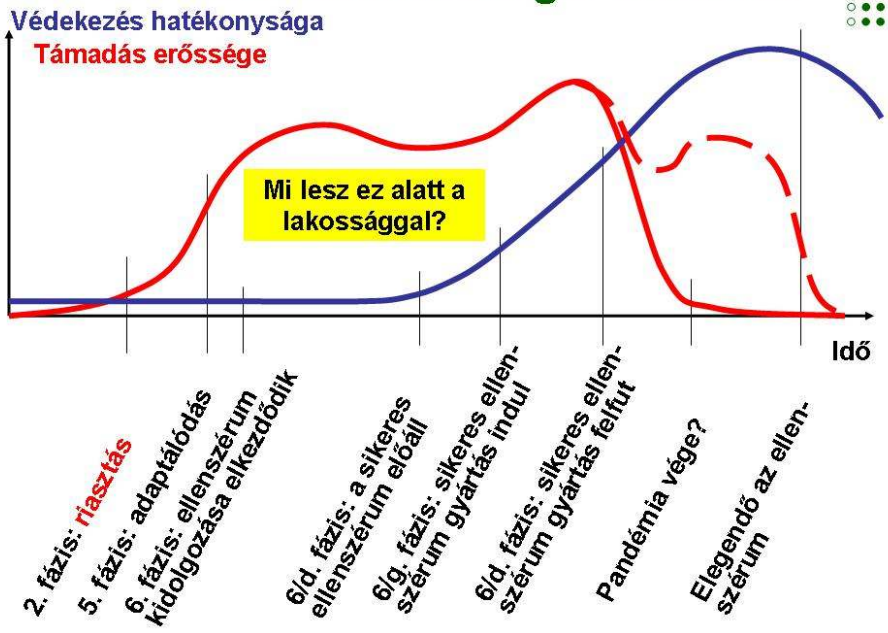
- **Az alapterveket készítik:**
  - Központi tervező: **GKM**
  - Ágazati tervezőszervek: **minisztériumok, stb.**
  - Területi tervezők: **megyei véd. bizottságok, stb.**
  - Helyi tervezők: **helyi védelmi bizottságok és a polgármesterek**

Honnan van/lesz megbízható alapadatuk?

Szemelvények a NIPT-ből

- A Kormányzat a katasztrófák kezelése szerint járjon el – (minősített helyzet)
- A kórházakat a lehető legteljesebb mértékben ki kell üríteni az influenzás betegek fogadása érdekében.
- Az oltóanyagok korlátozottan hatékonyak és csak lassú ütemben szerezhetők be (prioritás)
- Az alapellátás a lakáson történjen (távközlés kell)
- A kórházi látogatási tilalom miatt fokozódhat a távközlési igény a hozzátartozók részéről
- A járvány leküzdésében dolgozók távközlési igénye felerősödik

A védekezés lehetőségei és az idő



A távközlés és a pandémia

A pandémia a távközlést érintheti:

- Mint a járvány szenvedő alanya
  - Csökkenő dolgozói aktív létszám
  - Csökkenő fenntartói tevékenység
  - Szolgáltatások esetleges felfüggesztése
- Mint a pandémia ellen harcoló szervezetet
  - Promt szolgáltatási megrendelések teljesítése
  - Frekventált összeköttetések működtetése

A távközlés működőképessége

A távközlés működőképessége csak bizonyos feltételek teljesülése esetén oldható meg:

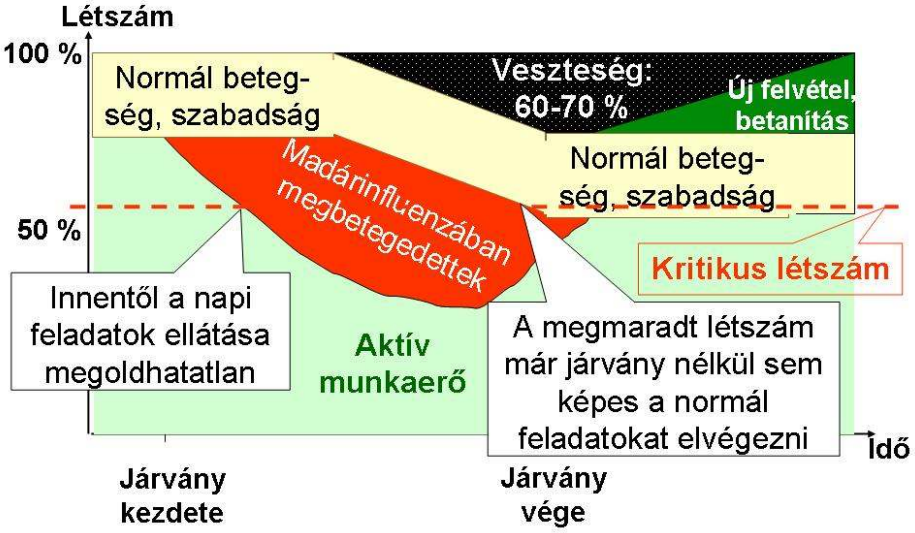
- Villamos energia
- Pénzügyi források
- Emberi erőforrások
- Gazdasági környezet
- Közlekedési lehetőségek
- Jogi rendezettség
- stb.

A pandémia támadása erősen veszélyezteti!

Lehetnek érintettek!

A kritikus létszám alatt a normál szolgáltatási szint már nem oldató meg…

Hogy jelentkezhet a távközlésben?
Humán erőforrás alakulása



Mi is az a kritikus létszám?

- **Alaphelyzetben:** az a dolgozói létszám, amely még képes a szolgáltatási rendszer folyamatos üzemeltetését fenntartani.
- **Konkrétan:**
  - napszakonként, hetente és havonta változik,
  - feladatfüggő,
  - gyakorlott, több ismerettel bíró dolgozóból általában kevesebb is elegendő egy feladathoz
  - a helyismeret szükségessége időnként csak nehezen (vagy nem) pótolható
  - láncszerű feladatoknál a statisztikai számok érvénytelenek

Munkahelyi létszám alakulása pandémia esetén

Nem képes a munkáját ellátni, aki:

- **Megbetegedett**
- **Kisgyermekére kell vigyáznia**
- **Beteg hozzátartozóját kell ápolnia**
  - NIPT szerint a kórházakat ki kell üríteni
  - Családtagok is megbetegedhetnek
- **Karantén miatt nem tud bejárni**
- **Akit PV munkára berendelnek** (helyi polgármester)

De itt segíthet a távmunka

A szabadságolás értelem szerűen szünetel.

Kritikus létszám alatt vagyunk!?

- **Átcsoportosítások:**
  - **Földrajzilag**
  - **Szervezetileg**
  - **Más munkakörből**

Helyismeret, kapcsolati rendszerek, közlekedés, elhelyezés, pihenési lehetőségek, család, vállalás, stb.

- **Kölcsön-munkaerő**
- **Nyugdíjasok bevonása**
- **Polgári védelmi egységek**
- **Honvédelmi munkakötelezettség**

Helyismeret, szaktudás, stb.?

A távközlés elsődleges feladatai

A szolgáltatások fenntartása és a bevétel folyamatossága érdekében:

- **A dolgozókat minél jobban védeni kell!**
  - **Csökkenjen a fertőzési esély!**
  - **Növekedjen az immunitásuk!**
  - **Többlet feladatokra fel kell készülni!**
- **A kieső-elvesző dolgozókat pótolni kell!**
  - **Helyettesíteni a betegállományosokat!**
  - **Az elhunyt dolgozókat pótolni kell!**

Veszélyhelyzetet csökkenteni! (1)

Csökkenjen a fertőzési esély!

1. **A személyes ügyfélkapcsolatot a minimumra kell csökkenteni, de szerelni csak a helyszínen lehet.**
2. **A halasztható értekezleteket, megbeszéléseket, oktatásokat el kell halasztani!**
3. **Tömegközlekedés helyett vállalati és magángépkocsi használat.**
4. **Nagy légterű irodákból távmunkára küldeni a dolgozókat, mert a légkondi terjeszt(het)i a vírusokat.**

Veszélyhelyzetet csökkenteni! (2)

Csökkenjen a fertőzési esély!

5. Fel kell készülni az eszközök és járművek tömeges és sűrű fertőtlenítésére.
6. Műszakok széthúzása a találkozási esélyek csökkentése miatt.
7. A „csak kicsit vagyok beteg, de bejöttem dolgozni" gyakorlatot meg kell szüntetni.
8. Szükség van a mindennapos létszám-jelentésekre a reggeli órákban, s információt kell szerezni a hiányzások okairól, a betegek állapotáról.
9. A bejárást naponta frissített adatokból rendszeresen újra kell szervezni.

Belső erőforrások átcsoportosítása

Többletfeladatokra felkészülés!

- **A hálózatbővítés előkészítése, tervezés:**
  - A létszám optimalizálása miatt már alig van hozzáértő!
  - Minden gépesítve lett, de azt embernek kell kezelnie!
- **Szerelői kapacitás**
  - Struktúra átszervezés miatt zömében <u>külsős vállalkozók</u>
  - Újak szerződéses bevonása <u>közbeszerzési kérdés</u>
  - <u>Helyismeret</u> nélkül az újak mozdulni sem tudnak (kulcsok, tápfejek helye, kollégákkal kapcsolat, betanulás, stb.)
  - <u>Biztonsági kockázat</u> (sok helyen még az erkölcsi bizonyítvány is kevés lehet, hiszen nemzetbiztonsági vizsgálathoz kötődnek egyes feladatok: **IDŐ!!!**)

Egy újabb mentsvár: a távmunka

Csökkenjen a fertőzési esély!

- **Nincs közösségtől eredő fertőzésveszély**
  - Sem a bejáráskor, sem a munkavégzéskor
  - Mellette az otthoni feladatok jobban szervezhetők (pl. hozzátartozó ápolása)
- **Hátrányok, feltételek:**
  - Végezhető-e a feladat odahaza?
  - Hajlandóság a távmunkára (főnök közelsége)?
  - Otthoni fogadókészség (szoba, család, stb.) ?
  - Technikai feltételek (átviteli út, eszközök, stb.)?

A tömegközlekedés kiiktatása

Csökkenjen a fertőzési esély!

Minél nagyobb arányban kall saját és vállalati a járvány idején bejárni:

- **Jogi háttér rendezése** (szerződések, APEH, belső szabályozások, stb.)
- **Parkolási gondok** (különösen a fővárosban, és nagyobb városokban)
  - Ahol ma helyet látunk, ott más cégek is parkolni akarnak
  - Ha sokat kell gyalogolni, gyorsabb gyalog bejárni
- „**Telekocsi" szervezés** (költséghatékonyság és parkolási gondok miatt)
  - Állandóan újraszervezni a kiesések és a túlórák miatt
  - A fertőzésveszély itt is fennáll

Dolgozók megelőző védőoltása

Növekedjen az immunitásuk!

- **A járvány kezdetén:** várhatóan kevés lesz az oltóanyag (s az sem véd azonnal, és nem is tökéletesen)
  - Immunerősítő kiosztása
  - Valószínű a távközlés a harmadik–sokadik körben kap néhány %-nyi dolgozóra oltóanyagot (PRIORITÁS???)
  - Ki kötelezhető beoltásra?
  - Milyen gyorsan lehet beoltani a legfontosabb dolgozókat?
- **A járvány második hullámánál:**
  - Lesz elég oltóanyag (?) (Outszourcinges és szerződéses beszállítók beoltása?)

Várható többletfeladatok

Többletfeladatokra felkészülés!

- **A járvány kitörésének hírére:**
  - A cégek távmunka-feltétel kialakítási rohama eli
  - Átviteli eszközkészlet csökken (a világ m gaiban is – beszerzési gondok várhatók)
  - A szerelőkapacitás ma az átl retezett – kevés lesz
- **A pandémia támad :**
  - A szerelők m korlátos lehet, egy részük kieshet
  - Szám szerelési igény merülhet fel
  - rtási munkák csökkenése miatt egyre több galmi zavar lehetséges
  - Egyes szolgáltatások felfüggesztése felmerülhet

Karantén területére kit és hogyan lehet beküldeni?

Gazdálkodás a humán erőforrással

Többletfeladatokra felkészülés!

- Mire fordítsuk a **megcsappant erőforrást?** (ha van lehetőség az átcsoportosításra)
  - Kinek vannak megfelelő **speciális ismeretei?**
  - Kinek van rendben a **biztonsági kockázata?**
- **Nincs sem jogi, sem állami** irányításból származó **állásfoglalás,** hogy a csökkenő lehetőségek esetén **mely távközlési szolgáltatást kell, vagy lehet** az adott **kényszerhelyzetben egy másik rovására előtérbe helyezni.**

Vitatható helyzet a kiemelt feladatokra

Többletfeladatokra felkészülés!

Mit kell/lehet kritikus működési területnek tekinteni:

- **A pillanatnyi pénzügyi bevételek** döntsenek?!
- A 2003. évi C. törvény, vagyis az **Egységes hírközlési törvény** szerinti egyetemes szolgáltatói kötelezettségek lehetnek a kritikus működési területek, de ezt ez **a törvény nem rögzíti!**
- **A távközlési szolgáltatást igénybe vevők száma szerint** a mobil távközlést kellene kiemelni?!
- Az **internet** legyen a legkritikusabb távközlési szolgáltatás?!
- **A kormány-hírközlésében elsőbbséget élvező beszédátvitelt** kellene privilegizálni?!

Minősített helyzetben csak kissé más a helyzet…

Outszourcing és a beszállítók

A pandémia nem válogat: a külsőseinket is megtámadhatja, ám tőlük függünk, pl.:

- Számítógépes háttérrendszer
- Erősáramú ellátás
- Ingatlanok üzemeltetése
- Objektumok őrzése
- Járműveink üzemeltetése
- Hálózat üzemeltetés
- Hálózat bővítése, stb.

Kapnak-e időben és elegendő védőoltást?

Van-e elegendő erőforrás tartalékuk?

Ők milyen prioritásokat alkalmaznak?

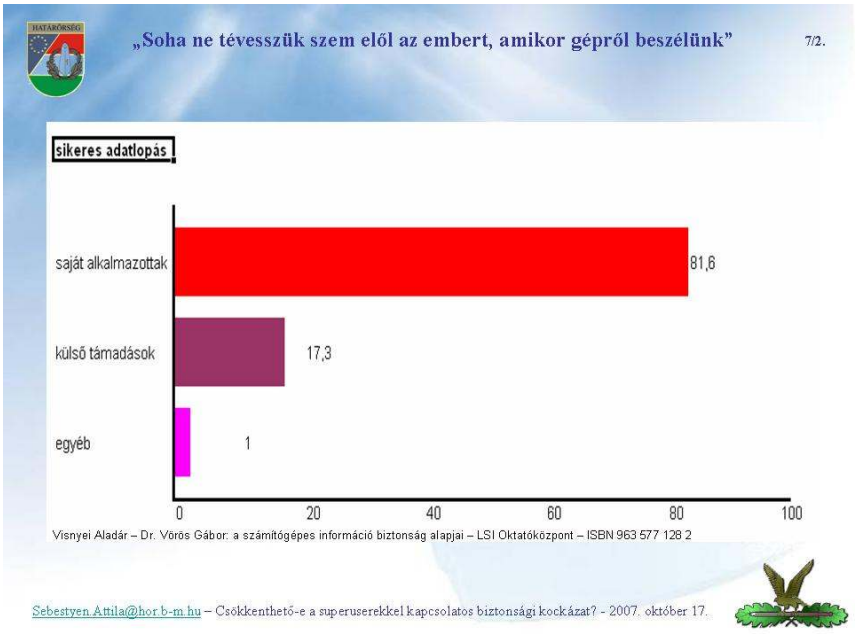
Mennyit érnek a szerződéseik?

Köszönöm a figyelmet, és várom a kérdéseket!

Mészáros Árpád
meszaros.arpad1@telekom.hu

SEBESTYÉN Attila

CSÖKKENTHETŐ-E A SZUPERUSEREKKEL KAPCSOLATOS BIZTONSÁGI KOCKÁZAT?



„Soha ne tévesszük szem elől az embert, amikor gépről beszélünk” 7/3.

A szuperuserek kivételezett helyzete:

- ✓erősen hierarchizált, tudás alapú tevékenység
- ✓az informatikai biztonsági szabályok kívánatos felhasználói magatartást írnak le
- ✓a megfogalmazott szabályok csak általánosságuk okán vonatkoztathatóak rájuk
- ✓általánosságban kerülik a szabályok az „önkorlátozást” kiváltó normákat
- ✓letéteményesei inkább a „rendnek”, mint kockázati tényezők
- ✓a szervezeti hatalom tényezőinek együttállása a „Thompson modell” szerint:
  - o a tevékenység centralitása – központi szerepe, fontossága
  - o a tevékenység ellenőrizhetősége – bizonytalansági elemek
  - o a személy, vagy csoport lecserélhetősége, pótolhatatlanság

„Soha ne tévesszük szem elől az embert, amikor gépről beszélünk” 7/4.

Általános védelmi intézkedési struktúra:

- ✓a szervezethez-,
- ✓az infrastruktúrához-,
- ✓az eszközökhöz (hardverekhez)-,
- ✓az alkalmazásokhoz (szoftverekhez)-,
- ✓a dokumentációkhoz-,
- ✓az adatokhoz-,
- ✓az adathordozókhoz-,
- ✓a kommunikációhoz-,
- ✓az eljárási rendhez-,
- ✓a személyekhez kapcsolódó.

„Soha ne tévesszük szem elől az embert, amikor gépről beszélünk” 7/5.

Adatbiztonsággal kapcsolatos emberi motívumok, a 7E*:

- ✓Ego - hiúság
- ✓Embezzlement - sikkasztás
- ✓Eavesdropping - lehallgatás
- ✓Enmity - ellenségeskedés
- ✓Espionage - kémkedés
- ✓Extortion - zsarolás
- ✓Error - hibás döntés

* Virrasztó Tamás: titkosítás és adatrejtés – NetAcadémia oktatóköztont – http://www.cryptox.hu/crypto02.php

Sebestyen.Attila@hor.b-m.hu – Csökkenthető-e a superuserekkel kapcsolatos biztonsági kockázat? - 2007. október 17.

„Soha ne tévesszük szem elől az embert, amikor gépről beszélünk” 7/6.

Módszerek a szuperuser adatsértési kockázatának csökkentésére:

- ✓Adatkörök szétválasztása* - alkalmazás és infrastruktúra rendszergazdaság
- ✓Munkakörök rotálása* - pótolhatóság, ellenőrizhetőség, állományképzés
- ✓Kötelező szabadság* - váratlan, legalább 10 munkanapos „eltávolítás”
- ✓Dokumentálás* - műszaki, rezsim, működés adminisztráció
- ✓Hozzáférés szabályozás* - szükséges és még elégséges a feladat végrehajtásához
- ✓„Üres íróasztal” politika* - csak aktuálisan végzett feladat anyagai kezelhetők
- ✓Hulladék megsemmisítése - adathordozó anyagától független megsemmisítés
- ✓Szükséges mérték - funkciókhoz definiált jogosultság, NEM kiváltság
- ✓Megszemélyesítés - általános szuperuser név használatának tiltása
- ✓Napló és monitoring - szuperusertől függetlenített funkció – biztonsági mb.
- ✓Egyszemélyű vezetés - szakfelügyeleti nem végrehajtási jogosultság

*Kő Andrea: információrendszerek auditálása – Budapesti Közgazdaságtudományi- és Államigazgatási Egyetem – 2003.

Sebestyen.Attila@hor.b-m.hu – Csökkenthető-e a superuserekkel kapcsolatos biztonsági kockázat? - 2007. október 17.

Csökkenthető a szuperuserekkel kapcsolatos biztonsági kockázat!!!
- 2007. október 17. –
Sebestyén Attila határőr alezredes
Köszönöm a megtisztelő figyelmet!
Sebestyen.Attila@hor.b-m.hu – Csökkenthető-e a superuserekkel kapcsolatos adatbiztonsági kockázat? - 2007. október 17.

SÍK Zoltán Nándor

AZ INFORMÁCIÓS HADVISELÉS ÉS A KRITIKUS INFRASTRUKTÚRÁK VÉDELME

Az információs hadviselés és a kritikus infrastruktúrák védelme
(Vitaindító: Társadalmi feladat vagy üzleti lehetőség?)

Sik Zoltán Nándor, ENO Advisory Kft.

STRATÉGIAI TANÁCSADÁS

Tartalom

- Röviden az információs hadviselésről (IW, InfoOps)
- Nemzetközi jogi megfontolások (IHL, LOAC)
- Kormányzati feladatok
- A létfontosságú infrastruktúrák védelme (CIP/CIIP)
- Hogyan tovább?

STRATÉGIAI TANÁCSADÁS

Az IW fogalma

- Nehéz meghatározni, körülírni…
- Túl bő, túl szűk definíciók
- Első def: Thomas Rona (1972)
- Ma használatos (IWS, Google, Wikipedia, stb.):

  „Az információs hadviselés a hadviselés egy új formája, amikor is az információ, illetve támadások az információ, illetve az információs rendszerek ellen a hadviselés eszközeivé válnak."

IW és ICT (1)

- ICT-re támaszkodik
- Technológia vezérelt
- Elnevezések változása: Signals warfare, C2W, IW, ma már: Info Ops

- Németország vezette konzorcium (ma 20 partnerrel): MNIOE – Multinational Information Operations Experiment
- MNIOE definíció:
  - *„Az információs rendszereket – beleértve a rendszerek viselkedését és lehetőségeit – érintő, olyan katonai tevékenységekre való javaslattétel, illetve ezek koordinálása, amelyekkel a kívánt hatások elérhetők"*

C2W (1)

- Definíció:
  - a kommunikáció vezérelt hadviselés **az információs hadviselés hadszíntéren történő implementálásának katonai stratégiája**, beleértve a fizikai megsemmisítést. Célja **az ellenség hadvezetési struktúrájának haderőktől történő elválasztása** (DoD Directive TS-3600.1, 21 December, 1992, „Information Warfare")

- Területei:
  - A parancsnoki központ elválasztása a harcoló alakulatoktól
  - A harcoló alakulatok egymástól való elválasztása

IBW (1)

- Definíció:
  - Amikor **a hírszerzés közvetlenül az operatív tevékenységek (katonai műveletek) kivitelezését szolgálja**, nem pl. a kommunikáció alapú hadviselés (C2W) általános bemeneti információit adja (IBW pl. a **célpont meghatározás** („targetálás"), **károk felbecslése)**

- Területei:
  - Helyzetértékelés
  - Harcmező áttekintése

- Érzékelői (real-time, near-real-time):
  - Nagy távolságú (űr, szeizmikus, akusztikus, stb.)
  - Közeli helyű (robotrepülőgép, UAV, SAR, elint, stb.)
  - Helyszíni (akusztikus, gravitációs, biokémiai, földi optikai, stb.)
  - Fegyverre szerelt (infra, radar, lidar, stb.)

EW (1)

- Def:
  - Amikor **a rádiótechnikát, az elektronikát és a rejtjelezést (kriptográfiát) használják a hadviselés eszközeként**. Az elektronikus hadviselés célja az információ átvitel elektronikus alapjainak hatástalanná tétele, illetve a kriptográfiai eszközök alkalmazásával az információ oly módon történő átvitele a védetlen csatornán, hogy az az ellenség birtokába ne, vagy csak aránytalanul nagy gazdasági befektetések árán, és az információ elavulása után jusson.

Hacker Warfare (1)

- **Winn Schwartau**: a számítógépes hálózatok elleni támadásokat tekinthetjük úgy, mint maga az információs hadviselés

  - Hacker warfare: „Informatikai" hadviselés
  - A hálózatok biztonsági réseinek kihasználása
  - Nem tényleges, hagyományos értelemben vett harc
  - Céljai: lehallgatás, megszemélyesítés, beavatkozás

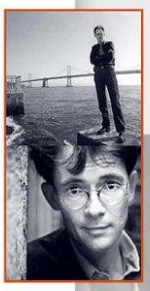
EIW (1)

- Def:
  - **a gazdasági hadviselés és az információs hadviselés közös metszete**
- Területei:
  - Információs blokád
  - Információs dominancia (információs imperializmus)
- Információs blokád
  - Fejlettebb országok élnek vele (pl. USA)
  - Ellenkezője is lehetséges (pl. Észak-Korea)
  - Nehéz kivitelezni:
    - Fejlett államok sokkal inkább információ függő
    - Infrastruktúrák kevéssé ellenőrizhetők
    - Szándékoltan redundánsak

Cyberwarfare (1)

- Def:
  - A kibernetikai hadviselés a **kibertérben zajlik**, és mint olyan eléggé megfoghatatlan, **utópisztikus**. Itt egyes területeken csak **trendekről, kibontakozó irányokról beszélhetünk**, más oldalon viszont van **tényleges hadviselési gyakorlat is.**
- Területei:
  - Információs terrorizmus
  - Szemantikai támadások
  - Szimulált háborúk
  - Gibson hadviselés – 4GW (5GW)

  (ld. William Gibson: Neuromancer)



IW és IT biztonság

Információs hadviselés

- Fókusz: információ
- Offenzív/defenzív terület
- Állami hatáskör a szektoriális hatáskör mellett
- Teljes társadalomra, kultúrára, gazdaságra hatással van

IT biztonság

- Fókusz: technika, ICT
- Defenzív terület
- Az adott cég, intézmény adott szektor hatásköre
- Szektoriális érdekek

IW és nemzetközi jog (1)

- Kérdések - a Nemzetközi Humanitárius Jog, ill. a Háborús Jog nem ad választ pl. a következőkre:
  - Vitatott, hogy egyáltalán hadviselés-e?
  - Erőszakos, ill. fegyveres támadás-e?
  - Mi jelenti a „károkat”?
  - Mi számít békeidőnek?
  - Létezhet-e „semleges” fél? (Értelmezhetők-e egyezményes jelek?)
  - Válasz hagyományos eszközökkel agresszió-e?
- További kérdések:
  - Hogyan azonosítható a támadás?
  - Hogyan azonosítható a támadó?
  - Polgári és katonai célpontok megkülönböztetése? – lehetséges?
  - Kik harcolnak kikkel? – ma már nem nemzetek közti harc

IW és nemzetközi jog (6)

- IW nemzetközi jogi megítélése nem kiforrott
- Bármely állam sebezhető!
- Megfontolások:
  - Hiányosságok, kétségek tisztázása szükséges
  - Nemzetközi összefogás kell (ilyen pl. a Cybercrime Egyezmény, Budapest, 2001)
  - **Kritikus infrastruktúrák védelme (CIP)**
  - Nemzetek közti együttműködés és nemzetközi szervezetekkel való együttműködés (ENSZ, OECD, ITU,stb.)
  - Korlátozhatók-e az IW eszközök?
  - Tartózkodás az offenzív IW alkalmazás

STRATÉGIAI TANÁCSADÁS

IW esetek

- Eddig nyilvánosságra került esetek
  - 1999, Moonlight Maze – USA ellen irányu Oroszországnak tulajdonítják
  - 2003, Titan Rain – USA ellen irányult, Kínának tulajdonítják
    - érintettek: Lockhead-Martin, Sandia National Labs, Redstone Arsenal, NASA
    - **Shawn Carpenter** (haditengerészet veteránja) 2005-re „felgöngyölítette"
  - 2007, Észtország elleni, Oroszországnak tulajdonított DDoS akció
    - elsősorban Hacker Warfare, EIW, Cyberwarfare területeket érint
    - Botnet bérlés, nem követhető vissza (KGB?, Nashi ifjúsági szervezet?)

STRATÉGIAI TANÁCSADÁS

Kormányzati kihívások (1)

- **Érintett minden állami szerv**, amely az információval kapcsolatos tevékenységet fejt ki
- Az állam kellő figyelmet kell fordítson a területre, **a védekezésre, a megelőzésre, illetve a megadott struktúrák védelmére**
- Csak partikuláris területeken léteznek **nemzetközi együttműködések** (hatásossága és hatékonysága sokszor vitatott)
- Sürgető a feladatok részletezése és a megfelelő **stratégiák megalkotása, operatív intézkedések kidolgozása**

Kormányzati kihívások (2)

- Elsősorban a **védelemre kell összpontosítani**
- **Célok: a gazdaság működőképességének fenntartása, a társadalom, a kultúra védelme és fejlődési ütemének biztosítása**
- **Állami szinten védeni a kritikus (információs) infrastruktúrákat (CIP/CIIP)**
- Minősített időszakban pl.:
  - Tömegtájékoztatás
  - Információk biztosítása
  - Hírközlési szolgáltatások fenntartása (koordináció!)
  - EKG, EDR/TETRA, stb.

Kormányzati kihívások (3)

- Állami feladatvállalás területei:
  - A térség, ezen belül **az ország helyzetének, lehetőségeinek, veszélyeztetettségének felmérése**
  - Nemzetközi erőfeszítésekben való részvétel, **nemzetközi együttműködések** kialakítása
  - **Feladatok felvázolása**, meghatározása
  - **Védelmi stratégiaalkotás**, részstratégiák egyeztetése, stratégia lebontása és végrehajtása

Kormányzati kihívások (4)

- Állami feladatvállalás területei(folytatás):
  - **Szervezetek kijelölése, kialakítása**
  - **Költségvetés készítése**, és a **források biztosítása**
  - **Szabályozási lépések** (nemzetközi jogi és hazai bázison)
  - **Felelősségek, feladatok telepítése, kötelezettségek előírása**
  - **Operatív intézkedések**, állami közvetlen beavatkozások
  - **Együttműködések** a gazdaság szereplőivel, társadalmi szervekkel

Kormányzati kihívások (5)

- Mi történik most?
  - EU jogszabály készül (CIP direktíva)
  - CIP/CIIP hazai koordináció
    - Kormányzati Koordinációs Bizottság (KKB)
    - Ágazati CI-k felmérése- szaktárcák
    - IRM kijelölt jogszabály-előkészítési felelősséggel
    - Jogszabály előkészítés – december 31-ig
    - Adaptálni kellene az EU direktívát eddig, de kész lesz?
  - Védelmi és biztonsági ipar stratégiájának előkészítése
    - Védelmi és Biztonsági Együttműködési Fórum (VBEF)
    - GKM projektet alapított rá, több főosztály bevonásával
    - IVSZ is involvált
  - Továbbiak…

STRATÉGIAI TANÁCSADÁS

CIP/CIIP (1)

- Nem elsősorban az IW-hez, hanem a terrorizmus elleni harchoz kötődik
- USA: 2001/09/11 után létrehozza a Department of Homeland Security-t
- EU: 2004-es madridi és 2005-ös londoni metró robbantások után 2006-ban EPCIP és CIWIN
  - EPCIP Green Paper (COM (2005) 576 final)
  - EPCIP –European Program for Critical Infrastructure Protection (COM(2006) 786 final – 2006/12/12)
  - EPCIP része a CIWIN - Critical Infrastructure Warning Information Network

STRATÉGIAI TANÁCSADÁS

CIP/CIIP (2)

- EPCIP dimenziói:
  - NCI – létfontosságú nemzeti infrastruktúrák
  - ECI – EU szempontból is fontos infrastruktúrák
- Az EPCIP által kijelölt területek:
  - Energia
  - Nukleáris ipar
  - Infokommunikációs technológiai (ICT) ipar
  - Vízügy
  - Élelmiszeripar
  - Egészségügy

STRATÉGIAI TANÁCSADÁS

CIP/CIIP (3)

- EPCIP által kijelölt területek (folytatás):
  - Pénzügy
  - Szállítás
  - Kémiai ipar
  - Űrkutatás, űrtechnológia
  - Kutatás-fejlesztés

- EU koordinatív szerepet kíván játszani
- ICT területen – ENISA - European Network and Information Security Agency (2004-től létezik)

STRATÉGIAI TANÁCSADÁS

Hogyan tovább? (1)

- A CI minden területen tartalmaz CII-t is:
  - Funkcionális ICT (pl.: IT, távközlés, műsorszórás, távérzékelés, navigáció, irányítás, vezetési és vezérlési rendszerek, stb.)
  - Támogató ICT (pl. energetika, logisztika, bankok, K+F, stb.)
- ITU ajánlás a CIIP struktúrára
  - A CIIP pillérei, funkciói:
    - Megelőzés, figyelmeztetés
    - Detektálás
    - Reagálás
    - Krízis kezelés, „utógondozás"
  - **CIIP szervezet:**
    - **Állami koordináló szerv – Stratégia és felügyelet**
    - **Szituáció kezelő központ – Adatgyűjtés és analízis**
    - **Nemzeti CERT – Információ biztonsági technikai kérdések**

STRATÉGIAI TANÁCSADÁS

Hogyan tovább?(2)

- EPCIP Pilot Project (Decision C/2006/5025 – 2006/10/26):
  - 2007 Call for Proposal – 3m Euro
  - EU a megfelelő költségekhez 70%-ban járul hozzá
  - A kritikus infrastruktúrára (CI) vonatkozó területek:
    - A CIP fejlesztése érdekében tett lépések
    - A CI sebezhetősége, rugalmassága, fejlesztési metódusok
    - CI kockázat mérséklési stratégiák, veszélyek megbecslése
    - Üzemben tartási tervek készítése
    - Közös védelmi szabványok fejlesztése, CIP innovatív technológiák
    - Nemzetek közti projektek, amelyek min két tagállamot, illetve egy tagállamot és egy jelentkező államot vonnak be

STRATÉGIAI TANÁCSADÁS

Hogyan tovább?(3)

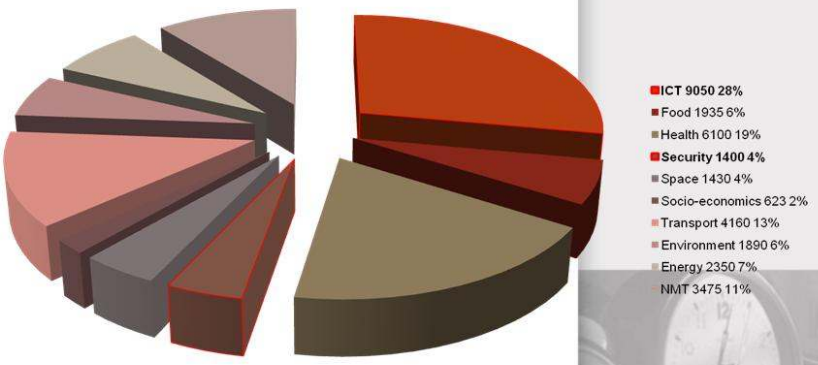
- Futó EU-s projektek (még FP6 alapján):
  - Specific Targeted Research Projects (STREP)
    - **CRUTIAL** - Critical utility infrastructural resilience – http://crutial.cesiricerca.it
  - Integrated Projects (IP)
    - **IRRIIS** – Integrated Risk Reduction of Information-based Infrastructure Systems - http://www.irriis.org
  - Coordination Actions (CA):
    - **GRID** - A coordination action on ICT vulnerabilities of power systems and the relevant defence methodologies – http://grid.jrc.it
    - **CIR2CO** - Critical information infrastructure research coordination – http://www.cir2co.org
- **FP7**
  - **ICT-SEC-2007.1.7** Critical Infrastructure Protection
  - A felhívás 2007. augusztus 3-án jelent meg (FP7-ICT-SEC-2007-1)
  - **Beadási határidő: 2007 október 29, 17:00** (brüsszeli idő)
  - Az ICT és a Security programok közös pályázata
  - **40mEuro keretösszeg**
  - Info: http://cordis.europa.eu/fp7/dc/index.cfm?fuseaction=UserSite.CooperationDetailsCallPage&call_id=70
    http://cordis.europa.eu/fp7/ict/critinfpro/home_en.html

Hogyan tovább?(4)

- ICT prioritások: CI-k összekapcsolása biztonságos, ellenálló és mindig rendelkezésre álló információs infrastruktúrákkal
- SEC prioritások: biztonságos, ellenálló és mindig rendelkezésre álló energia- és közlekedési infrastruktúrák
- További info:
  - NKTH EU IST Promóciós csoport : http://www.eu-ist.hu
  - FP7 ICT - Security: http://cordis.europa.eu/ist/trust-security/index.html
  - ICT Work Programme 2007-08: ftp://ftp.cordis.europa.eu/pub/fp7/ict/docs/ict-wp-2007-08_en.pdf
  - Angelo Marino (DG INFSO, F5): http://www.ci2rco.org/workshops/cf2/presentations/CI2RCO_2nd_CIIP_Conference-CIIP_R&D_FP7.pdf

Hogyan tovább?(5)

FP7 kooperációs programok keretösszege összesen: 32413 mEuro!



STRATÉGIAI TANÁCSADÁS

Sik Zoltán Nándor
sikzoltan@enoadvisory.com
ENO Advisory Kft.
www.enoadvisory.com

STRATÉGIAI TANÁCSADÁS

VESZÉLYHELYZETI KOMMUNIKÁCIÓ

ADATSZOLGÁLTATÁS AZ ADATVÉDELEM
ÉS TÖRVÉNYI KÖTELEZETTSÉGEK
EGYENSÚLYÁBAN

Jogszabályi háttér

- 2003 évi C. tv. (EHT),
- 1992 évi LXIII. Tv. (AVTV),
- 100/2004. (IV 27) kor. r. (elektronikus hírközlési szolgáltatók minősített időszaki feladatairól…)
- 27/2004. (X.6.) IHM rendelet (Ügyeleti rend)
- 24/2004. (VIII. 16.) IHM rendelet
- Nemzetközi kötelezettségvállalásaink

Veszély helyzeti kérdéskör a távbeszélő szolgáltatók esetében

- Kettős feladatrendszer:
  - Veszélyhelyzet esetén nyújtandó támogatási feladatok:
    - Technikai rendszer támogatás (pl. árvíz esetén, stb.),
    - Forgalmazási adatokból történő támogatás (pl. cella inf.),
    - Egyéb lehetőségek jogszabályi korlátokon belül,
  - A szolgáltató, mint veszélyeztetett:
    - Tudatos támadás,
    - Természeti katasztrófák, váratlan műszaki kiesésesek (adatvesztés akár veszélyhelyzet idején is)

A támogatás kérdései

- A szolgáltatónál keletkezett adatok kezelésének lehetőségei és korlátai:
  - jogszabályi elvárások és korlátok;
    - Ki a forgalmazás során generálódott adatok tulajdonosa(?), jogai és az adatkezelés korlátai, (lehetőségek, állásfoglalások, visszaélések). Az adat tulajdonos a saját adatával történő rendelkezést törvényi feltételek határozzák meg. Adatai felett nem rendelkezhet korlátlanul, u.a. adatainak kezelése szigorúan törvényhez kötött.
  - technikai lehetőségek és korlátok:
    - Azonos időben történő mozgás követés,
    - GSM rendszer időjárási, forgalmazási és domborzati viszonyaiból adódó korlátok (személy, gépjármű, repülő felkutatásába való bekapcsolódás)
  - Adatbázisba rögzített forgalmazási adatok veszélyhelyzeti esetekben történő alkalmazása (az adatbázisban tárolt adatok tartalma és a szolgáltatás anomáliája.

A támogatás kérdései

- Következtetés:
  - A forgalmazási adatokat megkülönböztethetjük:
    - dinamikus, műszaki segítség nyújtás azonnali esetleges követéssel,
    - statikus adatállomány kezelés
  - A szolgáltatóknál őrzött és kezelt adatbázisokat egységesen egy központi rendszerben kellene kezelni. A koncentrált adatbázis kezelés figyelembeveendő elvei:
    - Technikai kommunikációs rendszer kiépítése, működtetése,
    - Költségviselés,
    - Kiépítési elvek projekt menedzsmentje.

Szolgáltatót érő veszélyhelyzeti kockázati tényezők

- A szolgáltatót érő tudatos külső támadás:
  - Célja a kommunikáció korlátozása vagy teljes megsemmisítése,de ide tartozik a szolgáltató piaci érdekeinek tudatos csorbítása (visszaélések, csalások)
  - A külső támadások célpontjait és annak védelmét a ma már jól ismert információ biztonsági szabványok leírják (az objektum és technikai védelemtől a személyi és rezsim intézkedésig)
    - MS 17799,
    - COBIT,
    - CC,
    - Stb.
  - A szabványi alapon való működtetés alapproblémája a biztonsági tudatosság. Alapot képez a törvény a szabvány és a biztonsági tudatosság, amire épül a megvalósítási eljárás és a annak folyamatos visszaellenőrzése, illetve annak mindenkori a változó helyzethez való korrigálása

Szolgáltatót érő veszélyhelyzeti kockázati tényezők

- Természeti katasztrófák, váratlan műszaki technikai kiesések
  - Külső irányba történő reagálási intézkedések
    - Azonnali jelentési kötelezettség a főügyelet felé, jogszabályi és rendeleti előírások,
    - Társszolgáltatókkal kapcsolatfelvétel (ezen szinten nem a piaci célok a meghatározóak)
  - A szolgáltató saját preventív intézkedései:
    - rendszeres vizsgálatok, tesztelések, személyes koordinációk
      - Az ellenőrzések kiterjedhetnek:
        - » Előírások betartására,
        - » Rendszeres karbantartásokra,
        - » A szigorú dokumentáció kezelésre,
        - » Rendszeres továbbképzésre.

Összefoglalás és következtetések

- A szolgáltatók veszélyhelyzeti vagy egyéb rendkívüli helyzetekben történő feladatai és érintettsége rendszerezhető. A rendszerzés elvei:
  - Alapelemek
    - Szabályozó rendelkezések,
    - Alkalmazható szabványok és ajánlások,
    - Személyi elfogadottság, értelmezés, tudatosulás (veszély- és egyéb rendkívüli helyzetek tudatos értelmezése, a problémával való azonosulása),
    - A szolgáltató, mint piaci szereplő és a hatósági szervek közötti kölcsönös belátóképesség:
      - Kötelezettségek (jogszabályok) azonos értelmezése,
      - Társadalmi funkciók és szereplők közötti kölcsönös ismeret,
      - Költségek közös vállalása, stb.

Összefoglalás és következtetések

- Gyakorlati megvalósulás:
  - Jogszabályi harmonizáció (üzleti szabadságfok vs. biztonsági és veszélyhelyzeti kockázatok kezelése),
  - Szabványok alkalmazása és a folyamatokban résztvevők teljes azonosulása (minden szabvány alkalmazása annyit ér, amennyit az annak megvalósításában résztvevők motiváltak az alkalmazásban)
  - Személyi feltételek (természetes és jogi személyek) gyakorlatai viszonyai:
    - Szoros, folyamatos szakmai kapcsolat
    - A kapcsolati szintek közös értelmezése (feladatok, kötelezettségek, elvárások)
    - Emberi kapcsolatok.

Összefoglalás és következtetések

Fentieknek megfelelően a veszélyhelyzeti és rendkívüli események kezelését egyben a biztonságos (kezelt kockázati) kommunikáció feltételeit is az alábbi már kiemelt tényezők határozzák meg:

- Törvényi feltételek,
- Információ és informatikai szabványok alkalmazása,
- Személyi feltétele.

Köszönöm a figyelmüket!

SPRINGEL János

DIGITÁLIS ALÁÍRÁS ÉS HITELES ARCHIVÁLÁS EGYES KÉRDÉSEI

Tartalomjegyzék

- Elektronikus aláírás bevezetése
- e-Számla > Jogi háttér
- Archiválás > Jogi háttér

T Systems 1. oldal

Internet és informatikai biztonság

Jelen helyzet: Nyílt hálózatokon a legnagyobb gondot az adat- és szolgáltatásvédelem és a hitelesség jelenti

Igény üzleti és kormányzati alapú alkalmazásnál: az információk védelme és a hiteles adat- dokumentumcsere megvalósítása

Megoldás: PKI alapú megoldások alkalmazása

- titkosított,védett adatcsatorna a kommunikációra
- digitális aláírás

T Systems

2. oldal

Az e-business és az e-kormányzat alapvető kérdése a biztonság

Miért fontos a biztonság:

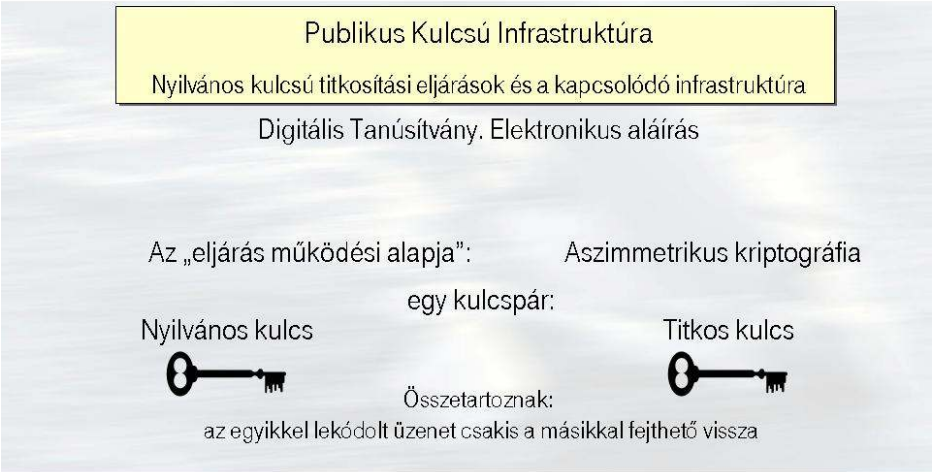
- Adat / információ érték !
- Szerződések érvényre juttathatósága
- rendszer-betörések és DoS támadások
- önrendelkezés jogának védelme
- egyéb szempontok

Ma már nem technikai kérdés alapvetően!

T Systems

3. oldal

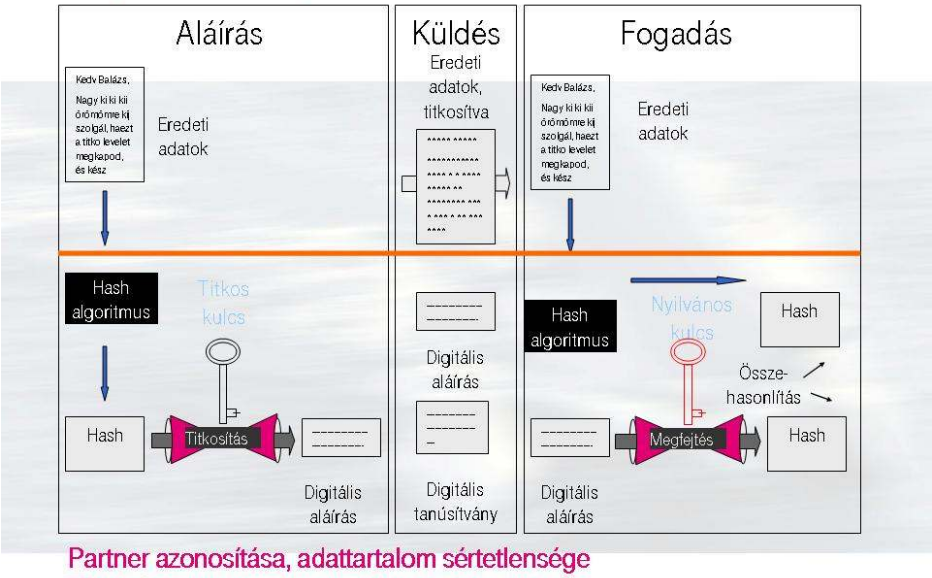
A válasz...



T Systems

4. oldal

A digitális aláírás folyamata:

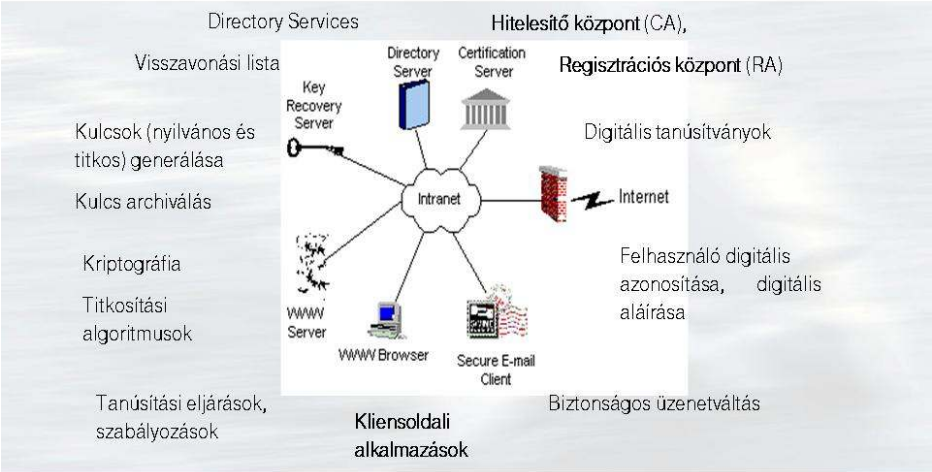


Partner azonosítása, adattartalom sértetlensége

T Systems

5. oldal

Mit ért(s)ünk PKI alatt?



T Systems

6. oldal

Előzmények – az elektronikus aláírás bevezetése

- 1997: Előterjesztés a Kormány részére az elektronikus okiratok jogi hatályáról
- 1999-től a jogszabály-előkészítés a Közlekedési, Hírközlési és Vízügyi Minisztérium koordinációjában folyik
- a kormányzat átalakításával az informatikával kapcsolatos kérdések a Miniszterelnöki Hivatalhoz kerültek
- 2001. május 28: a Parlament elfogadja az elektronikus aláírásról szóló 2001. évi XXXV. törvényt (EAT) > 2001. szeptember 1-el lépett hatályba
- 2004. évi LV. törvény: az EAT átfogó módosítása: az EU követelményeihez igazítás, harmonizáció, új szolgáltatástípusok elismerése, önkéntes akkreditáció, adatvédelem

T Systems

7. oldal

Hiteles elektronikus dokumentumok és e-Számla > Jogi háttér

Törvények – rendeletek az e-számlázáshoz, és megőrzéshez

- XXXV. Tv. Elektronikus Aláírás törvény - 2001. év
- 20/2004 (IV.21.) PM rendelet!!!
- 3/2005. (III.18) IHM rendelet
- 7/2005. (VII.18) IHM rendelet!!!
- 13/2005. (X.27) IHM rendelet
- + magyar(!) számviteli szabályok + APEH ajánlások (2006)
- 2007 – követelményrendszer archiválási szolgáltatókra

Ezek a szabályozások kötelezőek a külföldi „megőrzés" esetében is!!!

NHH (HIF) előírások, GKM workshop

T Systems

8. oldal

Az EAT szerkezete, szabályozási tartalma

- Az elektronikus aláírás fogalmi alapjai, alkalmazása és joghatásai, jogkövetkezményei
- Az elektronikus aláírással kapcsolatos szolgáltatásokra vonatkozó közös és különös szabályai
- Aláírás-létrehozó eszköz, az aláírás-létrehozó adat elhelyezése
- Az időbélyegzés szolgáltatás
- Az elektronikus archiválási szolgáltatás különös szabályai
- Az állami felügyelet szabályai

T Systems

9. oldal

Elektronikus számlázás

A számviteli törvény 2002 január 1-től hatályos módosítása alapján, az elektronikus aláírásról szóló törvény értelmében minősített elektronikus aláírással és időbélyegzővel ellátott elektronikus számla érvényes számviteli bizonylatnak tekintendő

T Systems

10. oldal

De miért?!

A jogalkotó megalkotta a jogszabályt, de azt alkalmazásba is kell venni!

Pl.:

- Ellenőrizni kell > olvashatóság
- Fel kell dolgozni > szabványosság
- Meg kell őrizni > archiválás > archiválási szolgáltató! Külön rendelet! De hol van? Hol szabályozták? Mik a követelmények?

T Systems

11. oldal

20/2004. (IV. 21.) PM rendelet az elektronikus számláról

Az elektronikus számla megfelelősége

1. § (2) Az elektronikus számla az áfa-törvény 43. §-ának (7) bekezdésében meghatározott feltételek szerint adóigazgatási azonosításra akkor felel meg, ha az adóalany az elektronikus számla

- *a)* eredetének hitelességét,
- *b)* tartalmának teljességét, megváltoztathatatlanságát, sértetlenségét,
- *c)* értelmezhetőségét (olvashatóságát > APEH!)
- *d)* a jogosultak általi hozzáférhetőségét, valamint
- *e)* a jogosulatlan hozzáférés, módosítás, törlés vagy megsemmisítés elleni védelmét

a kibocsátáskor és a számla megőrzésére külön jogszabály által előírt időtartam alatt is biztosítja.

T Systems

12. oldal

20/2004. (IV. 21.) PM rendelet az elektronikus számláról

Mi az elektronikus számla

2. § (1) Elektronikus számla

- *a)* legalább fokozott biztonságú elektronikus aláírással és időbélyegzővel ellátott elektronikus adat formájában, vagy
- *b)* elektronikus adatcsere rendszer alkalmazásával létrehozott elektronikus adat formájában

bocsátható ki.

T Systems

13. oldal

20/2004. (IV. 21.) PM rendelet az elektronikus számláról

Egyéb előírások

4. § (1) Az elektronikus számlát és az összesítő dokumentumot a kiállítása szerinti eredeti formában, az áfa-törvény 13. § (1) bekezdésének 26. pontjában meghatározott Közösség területén kell megőrizni.

(2) Az adóalany az adóhatóság felhívására az elektronikus számlát és az összesítő dokumentumot ellenőrzés céljából 3 munkanapon belül bemutatja.

(3) A helyszíni ellenőrzés során az adóalany az adóhatóság részére a számlák olvashatóságához szükséges számítástechnikai eszközöket, az eszközök használatához szükséges dokumentációt biztosítja, a szükséges felvilágosítást megadja. Az adóalany az általa megőrzött számlák másolatát az adóhatóság felhívásában meghatározott csoportosításban és az adóhatóság által közzétett formátumban is köteles az adóhatóság rendelkezésére bocsátani.

T Systems

14. oldal

20/2004. (IV. 21.) PM rendelet az elektronikus számláról

Egyéb előírások

5. § (1) Elektronikus számlák jogszabály által előírt megőrzési kötelezettsége esetén a megőrzési kötelezettséget a kötelezett maga is elláthatja vagy annak ellátásával külön törvény szerinti archiválási szolgáltatót bízhat meg.

6. § Az elektronikus adatcsere rendszer alkalmazásával létrehozott elektronikus számla megőrzése során a számla megőrzője köteles az 1. § (2) bekezdésében foglalt feltételeket a számla őrzése alatt folyamatosan biztosítani.

T Systems

15. oldal

Mit értünk archiválása alatt?

- Adatok megőrzése ➔ adatok tárolása ➔ adatok archiválása
- Műszaki értelemben beszélhetünk archiválásról
- Cél hogy jogi értelemben is megfelelő archiválási szolgáltatást nyújtsunk
  - Eat. 2001. évi XXXV. törvény
  - 7/2005 IHM rendelet
- Jogszabály szerint kétféle módon lehet dokumentumokat hitelesen archiválni:
  - Saját számlák archiválása, saját zárt rendszerrel
  - Archiválási szolgáltató megbízása

T Systems

16. oldal

7/2005. (VII. 18.) IHM rendelet

a digitális archiválás szabályairól, valamint az információs társadalommal összefüggő szolgáltatásokkal kapcsolatos elektronikus archiválás szabályairól

3. § (1) Az elektronikus dokumentumokat oly módon kell megőrizni, amely kizárja az utólagos módosítás lehetőségét, a megőrzési kötelezettség lejártáig folyamatosan biztosítja a jogosultak részére a hozzáférést, a dokumentum létrehozójának és archiválójának egyértelmű azonosíthatóságát, valamint az elektronikus dokumentumok értelmezhetőségét (olvashatóságát). Az elektronikus dokumentumokat védeni kell a jogosulatlan hozzáférés, módosítás, törlés vagy megsemmisítés ellen.

T Systems

17. oldal

7/2005. (VII. 18.) IHM rendelet

Ennek eleget lehet tenni:

- zárt rendszer alkalmazásával,
- zárt megőrzéssel,
- elektronikus adatcsererendszer (EDI) igénybevételével
- fokozott biztonságú vagy minősített elektronikus aláírás alkalmazásával.

T Systems

18. oldal

7/2005. (VII. 18.) IHM rendelet

Saját megőrzés!

6. § Amennyiben a megőrzési kötelezettséget a kötelezett személy maga látja el, a kötelezett:

a) biztosítja a jogszabályoknak és szabályzatoknak megfelelő és naprakész belső irányítási és ellenőrzési eljárásrend és a kapcsolódó felelősségi rendszer folyamatos működtetését; a rendszer megfelelő működését a belső ellenőrzés tevékenysége biztosítja;

b) biztosítja, hogy az elektronikus archiválással kapcsolatos munkakört csak olyan személyek tölthetnek be, akiknek a munkakör betöltéséhez szükséges befolyásmentességét és szakértelmét a minősített szolgáltató hatósági erkölcsi bizonyítványnyal, szakmai gyakorlattal, végzettséggel és szakképesítéssel igazolni tudja;

c) biztosítja azt, hogy a belső ellenőrzéssel és az archiválással kapcsolatos munkaköröket betöltő személyek egymástól függetlenek;

d) biztosítja az archivált adatok tárolására szolgáló helyiségek fizikai védelmét a jogosulatlan hozzáféréstől, a jogosulatlan személyek bejutását kizárva; a belépésre jogosultak belépésének időpontját, időtartamát, kilépésének időpontját naplóban kell rögzíteni;

T Systems

19. oldal

7/2005. (VII. 18.) IHM rendelet

Saját megőrzés!

e) biztosítja a fizikai és környezeti biztonság komplex kezelését, amely magába foglalja az élet- és vagyonvédelem alábbi területeit is: tűz, árvíz, elárasztás, fizikai behatolás, sugárzás, áramellátás-kimaradás elleni megfelelő szintű védelem;

f) köteles az üzemmenet folytonossága és az adatvesztés elkerülése végett mentéseket végezni, és biztosítani, hogy szükség esetén az informatikai rendszer egésze helyreállítható legyen; a mentéseket védenie kell különösen a jogosulatlan hozzáférés, megváltoztatás, törlés vagy megsemmisítés ellen;

g) köteles biztosítani az adatvédelem és az adatbiztonság területén a jogszabályoknak megfelelő működést, a jogok, kötelezettségek, felelősségi körök meghatározását.

T Systems

20. oldal

7/2005. (VII. 18.) IHM rendelet és NHH követelmény rendszer

szolgáltató!

Kötelező szolgáltatások:

- Sértetlenség fenntartása
- Létezés bizonyítása
- Bizalmasság garantálása
- Értelmezhetőség garantálása:

  Jelezni kell, ha az értelmezendő dokumentum olyan rejtett vagy aktív kódot tartalmaz, amely a dokumentum megjelenítésében változást okozhat,
- Egyéb szolgáltatások

T Systems

21. oldal

Mi hiányzott még?

Könyvelési és a valós számlázási folyamatokhoz igazítás.

Ellenőrizhetőség – APEH! – kialakítása:

- Milyen formátumokban?
- Az ajánlott formátumokra ajánlott tartalmi előírások.
- Megjeleníthetőség biztosítása!
- De!!! Apeh ellenőr!!!

T Systems

22. oldal

Végkövetkeztetés?

Nem elég törvényt alkotni – vagy elérni, hogy azt a törvényhozás elfogadja – azt működésbe is kell hozni!

Az egész folyamatot, minden szereplőjével együtt kell szemlélni és tesztelni.

Jelen esetben – számlázás:

- Számla előállítás, továbbítás, feldolgozás (könyvelés, kontírozás, reklamáció, módosítás), megőrzés és ellenőrzés.
- Számla kibocsátó, befogadó, könyvelő, könyvvizsgáló és adóellenőr (szolgáltatók: VAN, HSz, Archiválás)

T Systems

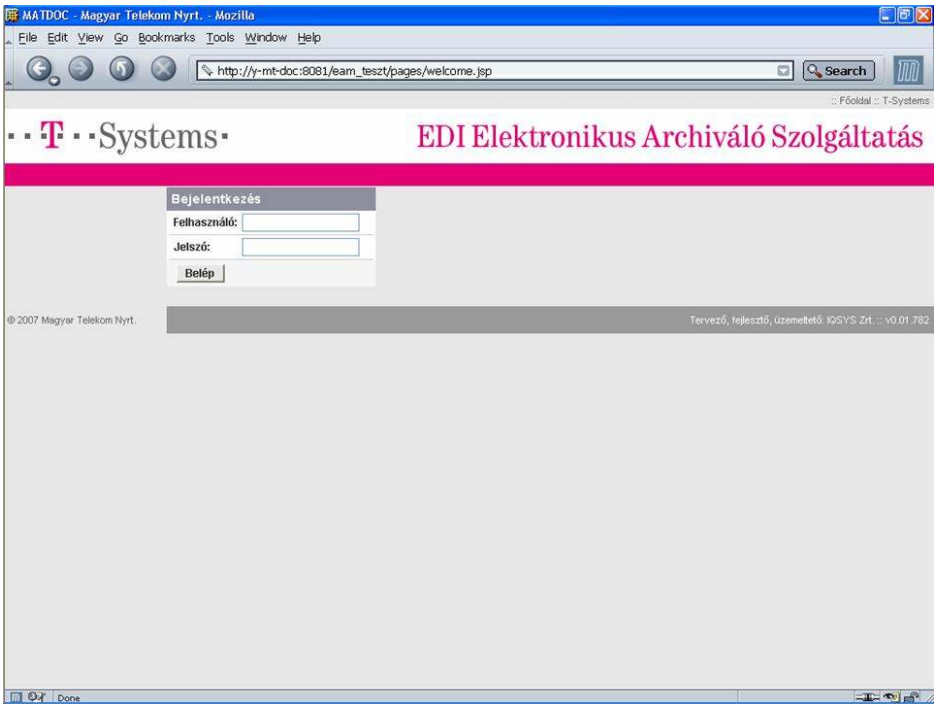
23. oldal

Archiválás – megőrzés
Funkciók

- Archiválási szabályok beállítása:
  - Megőrzési idők
  - Partnerek
  - Dokumentum típusok
- Keresési feltételek:
  - Időpontra vagy időtartamra
  - Partnerre
  - Dokumentum típusra
  - Egyedi azonosítóra
- Dokumentum kiadása
  - Az eredeti EDI számla és/vagy
  - az APEH által megkövetelt XML formátumú számla.

T Systems

24. oldal



MATDOC - Magyar Telekom Nyrt. - Mozilla

File Edit View Go Bookmarks Tools Window Help

http://y-mt-doc:8081/eam_teszt/ff002/main.do

Search

:: Főoldal :: T-Systems

T Systems

EDI Elektronikus Archiváló Szolgáltatás

Bejelentkezett felhasználó: ADMIN Kilépés

:: Szerződések
:: Üzenettípusok
:: Üzenetek keresése
:: Eseménynapló
:: Kérések állapota
:: EDI azonosítók betöltése
:: Számlázási riport
:: Konfiguráció frissítése
:: Archiválás indítása
:: Értesítés lejáró üz.
:: Felhasználói riport
:: Rendszeres selejtezés
:: Arch. szab. felt. sFTP-re

Archiválási szabályok listája (FF010)

Mégsem | Keres | Kiürít

Szerződés adatai

ICCM/Siebel azonosító: 102225

Ügyfél neve: Praktiker Magyarország Kft.

Kezdődátum: 2007.05.01.

Keresési feltételek

Üzenettípus:

Forgalom iránya:

Érvényes: -tól -ig

Szabályok listája

Új | Töröl | EDI azonosító váltás

	Üzenettípus	Üzenet iránya	Saját EDI azonosító	Partner EDI azonosítója	Érv. kezdete	Érv. vége	Leírás
☐	ORDERS - megrendelés	küldött	PRAKTIKER , Praktiker Magyarország Kft.	mind	2007.04.12. 00:00:00	-	
☐	INVOIC - számla	fogadott	PRAKTIKER , Praktiker Magyarország Kft.	mind	2007.05.01. 00:00:00	-	Praktiker minden bejövo számla

© 2007 Magyar Telekom Nyrt.

Tervező, fejlesztő, üzemeltető: IQSYS Zrt. :: v0.01.782

MATDOC - Magyar Telekom Nyrt. - Mozilla

File Edit View Go Bookmarks Tools Window Help

http://y-mt-doc:8081/eam_teszt/ff010/main.do

Search

:: Főoldal :: T-Systems

T Systems

EDI Elektronikus Archiváló Szolgáltatás

Bejelentkezett felhasználó: ADMIN Kilépés

:: Szerződések
:: Üzenettípusok
:: Üzenetek keresése
:: Eseménynapló
:: Kérések állapota
:: EDI azonosítók betöltése
:: Számlázási riport
:: Konfiguráció frissítése
:: Archiválás indítása
:: Értesítés lejáró üz.
:: Felhasználói riport
:: Rendszeres selejtezés
:: Arch. szab. felt. sFTP-re

Archiválási szabály létrehozása (FF011)

Mégsem | Mentés

Szerződés adatai

ICCM/Siebel azonosító: 102225

Ügyfél neve: Praktiker Magyarország Kft.

Kezdődátum: 2007.05.01.

Arciválási szabály adatai

Üzenettípus:* INVOIC - számla

Forgalom iránya:* küldött

Saját EDI azonosító:* azonosító: PRAKTIKER név: Praktiker Magyarorsz

Partner EDI azonosítója: azonosító: Kiválaszt név: bármely postaláda

Leírás:

© 2007 Magyar Telekom Nyrt.

Tervező, fejlesztő, üzemeltető: IQSYS Zrt. :: v0.01.782

Done

MATDOC - Magyar Telekom Nyrt. - Mozilla

File Edit View Go Bookmarks Tools Window Help

http://y-mt-doc:8081/eam_teszt/ff012/main.do

Search

:: Szerződések
:: Üzenettípusok
:: Üzenetek keresése
:: Eseménynapló
:: Kérések állapota
:: EDI azonosítók betöltése
:: Számlázási riport
:: Konfiguráció frissítése
:: Archiválás indítása
:: Értesítés lejáró üz.
:: Felhasználói riport
:: Rendszeres selejtezés
:: Arch. szab. felt. sFTP-re

Üzenetek keresése (FF012)

Mégsem | Keres | Kiürít

Keresési feltételek

ICCM/Siebel azonosító:

Ügyfél neve:

Lejárati dátum: -tól -ig

Küldés dátuma: -tól -ig

Üzenettípus: mind

Küldő EDI azonosítója: azonosító: Kiválaszt név:

Fogadó EDI azonosítója: azonosító: Kiválaszt név:

Üzenet egyedi azonosítója:

Találatok száma: Találatok lapozása: Megjelenítendő sorok száma: 5

Találati lista 1. oldal

Megtekint | << | < | > | >> | Összes kijelölése | Összes kijelölés visszavonása | Letöltés EDI | Letöltés XML | Megőrzés módosítása | Selejtezés

	Üzenettípus	Üzenet egyedi azonosítója (SNRF)	Küldés dátuma	Küldő EDI azonosítója	Fogadó EDI azonosítója	Archiválás dátuma	Lejárat dátuma	Ügyfél neve
☐	megrendelés	5136#547	2007.05.11.	PRAKTIKER , Praktiker Magyarország Kft.	FISKARS , Fiskars Rt.		2016.04.06.	Fiskars Rt.
☑	számla	5132#543	2007.06.07.	ZALAFA , Zalafa Rt.	PRAKTIKER , Praktiker Magyarország Kft.		2019.04.06.	Praktiker Magyarország Kft.
☐	számla	5133#541	2007.12.08.	FISKARS , Fiskars Rt.	PRAKTIKER , Praktiker Magyarország Kft.		2019.04.06.	Praktiker Magyarország Kft.
☐	számla	5134#545	2007.05.09.	KISSFERI , Kiss Feri és Társa Bt.	PRAKTIKER , Praktiker Magyarország Kft.		2019.04.06.	Praktiker Magyarország Kft.

MATDOC - Magyar Telekom Nyrt. - Mozilla

File Edit View Go Bookmarks Tools Window Help

http://y-mt-doc:8081/eam_teszt/ff020/main.do

Search

:: Főoldal :: T-Systems

T Systems

EDI Elektronikus Archiváló Szolgáltatás

Bejelentkezett felhasználó: ADMIN Kilépés

:: Szerződések
:: Üzenettípusok
:: Üzenetek keresése
:: Eseménynapló
:: Kérések állapota
:: EDI azonosítók betöltése
:: Számlázási riport
:: Konfiguráció frissítése
:: Archiválás indítása
:: Értesítés lejáró üz.
:: Felhasználói riport
:: Rendszeres selejtezés
:: Arch. szab. felt. sFTP-re

Üzenet megtekintése (FF014)

Mégsem

Üzenet tartalma

SZÁMLA

Eladó adatai	Vevő adatai	Számla adatai
Neve: Henkel Magyarország Kft. Címe: Budapest1113Dávid Ferenc 6.utca6 Adószáma: 10783050-2-44	Neve: BICSKE RAKTÁR Címe: Bicske2060Spar útutca	Sorszám: 5710438134 Kiállítás dátuma: 2007-01-04+01:00 Teljesítés dátuma: 2007-01-03+01:00 Fizetési határidő: 2007-01-03+01:00 Fizetés módja: átutalás Számla típusa: kereskedelmi számla/eredeti Pénznem: HUF

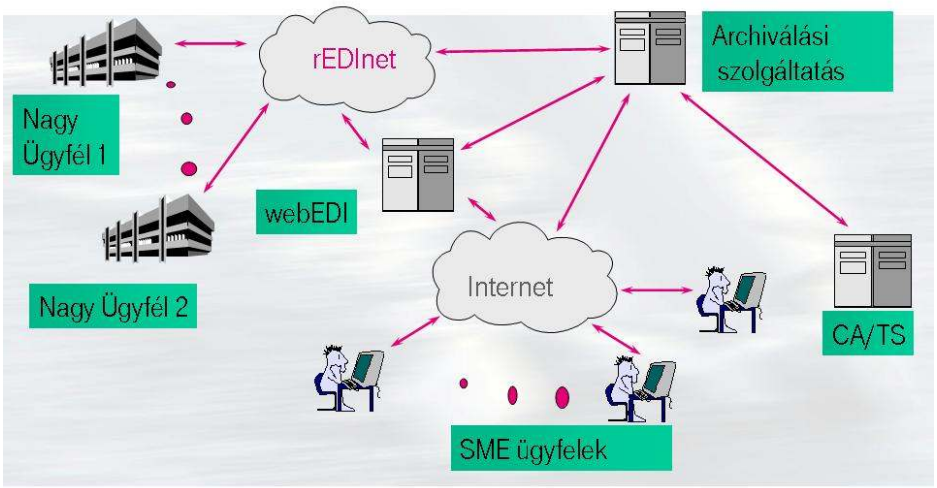
Termék neve	Besorolási száma	M.e.	Menny.	Nettó egységár	Nettó ár	Áfa kulcs	Áfa	Bruttó ár
Clin ablakt.750ml utántöltő	3402209000	PCE	750.0	222.22	10101.0	20.0	11111.0	20202.0
Opti 500ml bútorápoló	3405200000	PCE	768.0	300.0	222222.05	20.0	55555.0	333333.06
Clorox 1 lt virág	28289000	PCE	540.0	100.01	22222.4	20.0	12222.0	8111112.0
1. ÁFA rovat:								
Összesen:					6666666.0		1222223.0	8888888.0

© 2007 Magyar Telekom Nyrt.

Tervező, fejlesztő, üzemeltető: IQSYS Zrt. :: v0.01.782

Done

T-Systems - komplex EDI megoldások



T Systems

30. oldal