A ZRÍNYI MIKLÓS NEMZETVÉDELMI EGYETEM KIADVÁNYA

Kommunikáció 2008
Communications 2008

VIDEOTON
VT-Rendszertechnika Kft

AQAP-2110

ISO 9001 BUREAU VERITAS Certification No: 196340

ISO 14001 BUREAU VERITAS Certification No: 159610

MINŐSÍTETT NATO BESZÁLLÍTÁSRA ALKALMAS

8000 Székesfehérvár, Berényi út 72-100.
Tel: (22)533-790 Fax: (22)533-799
H-8002 Székesfehérvár, Pf. 284
E-mail:vtsys@rendszertech.videoton.hu
www.vtsys.videoton.hu
Bejegyezve: Fejér Megyei Cégbíróság
Cégjegyzékszám: 07- 09 002398

vtsys@rendszertech.videoton.hu

EGYSÉGES DIGITÁLIS RÁDIÓ-TÁVKÖZLŐ RENDSZER (EDR)

A Pro-M Professzionális Mobilrádió Zrt. (Pro-M Zrt.) feladata a rendkívül magas rendelkezésre állást biztosító **EGYSÉGES DIGITÁLIS RÁDIÓ-TÁVKÖZLŐ RENDSZER (EDR)** zavartalan üzemeltetése Magyarországon. A TETRA technológiájú zárt rádió-távközlő rendszer professzionális összeköttetést és együttműködést valósít meg a különféle készenléti és rendvédelmi szervek között, amely gyorsabbá, hatékonyabbá és biztonságosabbá teszi az egyes veszélyhelyzeti feladatok végrehajtását. A vállalat 2008 májusában az ISO 9001:2000-es és ISO/IEC 27001:2005-ös szabványoknak is sikeresen megfelelt, amellyel bizonyította felkészültségét és elkötelezettségét az EDR felhasználók, valamint a számukra elengedhetetlen információbiztonság iránt.

Bővebb tájékoztatásért látogasson el a www.pro-m.hu honlapra.

Pro-M Zrt.
A Magyar Telekom Csoport tagja

Zrínyi Miklós Nemzetvédelmi Egyetem
Budapest, 2008. október 7.

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. Szöllősi Sándor nyá. okl. mk. őrgy, egy. docens

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

Anyanyelvi lektor:
Dr. Fregan Beatrix

Felelős kiadó: Prof. Dr. Szabó János, a Zrínyi Miklós Nemzetvédelmi Egyetem rektora
Megjelent a Zrínyi Miklós Nemzetvédelmi Egyetemi Kiadó gondozásában
Készült a Zrínyi Miklós Nemzetvédelmi Egyetem nyomdájában, 100 példányban

ISBN 978-963-7060-57-1

TARTALOMJEGYZÉK

A nemzetközi szakmai tudományos konferencia kommunikációs partnere:

T-Systems

A tudományos konferencia támogatói:

Alcatel-Lucent	Alcatel-Lucent Magyarország Kft.
Elbit Systems Land and C4I - Tadiran	Elbit Systems
Fercom	Fercom Kommunikációs Kft.
HDT Hungaro DigiTel	Hungaro DigiTel Kft.
kapsch	Kapsch Telecom Kft.
mvm	Magyar Villamos Művek Zrt.
Pro-M Zrt.	Pro-M Zrt.
SCI-Network	SCI-Network Távközlési és Hálózatintegrációs ZRt.
SIEMENS	SIEMENS ZRt.
VT-Rendszertechnika Kft.	VIDEOTON VT-Rendszertechnika Kft.

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.
Elbit Systems
Fercom Kommunikációs Kft.
Hungaro DigiTel Kft.
Kapsch Telecom Kft.
Magyar Villamos Művek Zrt.
Pro-M Zrt.
SCI-Network Távközlési és Hálózatintegrációs Zrt.
SIEMENS Zrt.
VIDEOTON VT-Rendszertechnika Kft.

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
Dr. Szöllősi Sándor nyá. okl. mk. őrnagy

BEVEZETŐ

Ön a Kommunikáció 2008 (Communications 2008) tudományos kiadvány könyv változatát tartja kezében.

A Zrínyi Miklós Nemzetvédelmi Egyetem Híradó Tanszéke által szervezett rendezvény idén kilencedik alkalommal kerül megrendezésre. Nem titkolt szándékunk és célunk, hogy a honvédelmi, rendvédelmi, nemzetbiztonsági, illetőleg közigazgatási ágazat, a védelmi 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.

Az előző Konferenciától eltelt egy év gazdag volt változásokban. Mind a gyorsuló tudományos-technikai fejlődés, mind a makro és mikrogazdasági hatásokat megjelenítő közgazdasági háttér, mind a fejlődéssel együttjáró szervezeti változások arra késztetnek bennünket, hogy időről-időre megvizsgáljuk eddigi tevékenységünket, összevessük más akadémiai vagy ágazati kutatások eredményeit. Teszszük ezt azért, mert egyre inkább úgy tűnik, hogy a folyamatosan nehezedő gazdasági feltételek között tudatosan kell keresnünk a Win-win megoldásokat és a kooperatív együttműködés gyakorlati lehetőségeit. Ennek kiváló színpada a távközlési, az informatikai és a média ipar konvergenciája, mely eddig nem ismert, új lehetőségeket és megoldásokat kínál a professzionális és a magáncélú felhasználóknak.

A konferencián elhangzó előadások, illetőleg a kiadványban bemutatásra kerülő publikációk reményeink szerint elősegítik az állami- és a magánszektor közötti sikeres interakciót, melynek elmélyítését jelen könyvünk korlátozott példányszámú terjesztésével is szolgálni kívánjuk.

Egyúttal tisztelettel jelentjük a jelen sorok olvasóinak, hogy a szervező bizottság nagy örömmel és felelősséggel készül a 2009-ben megrendezésre kerülő 10. jubilleumi tudományos konferenciára, melyen való részvétel lehetőségére előzetesen is szeretnénk felhívni a figyelmet.

A szervező bizottság

VÖRÖS Béla[1]

SUSA ISTVÁN EMLÉKÉRE

Susa István ezredes egyetemünk halottja. 32 évig volt a hadsereg tagja.

1953. március l-étöl a Híradó Tiszti iskola parancsnoka, 1956-tól az összevont Híradó - Műszaki Tiszti iskola parancsnoka, 1957-töl az Egyesített Tiszti Iskola híradó tanszékének irányító vezetője, nyugállományba helyezéséig: 1980-ig.

Mint munkás kádert a kommunista párt küldte a hadseregbe. 1948. április 15-én vonult be Várpalotára, a lövész zászlóaljhoz. Fél évig részt vett az újonc kiképzésben, majd szeptemberben bevonult a Kossuth Akadémiára. 1949 januárjában válogatáson vett részt, ahol közölték vele, hogy híradóként fog tanulni a Szovjetunióban. Különleges tanfolyamon vett részt, ahol főként az orosz nyelvet tanulták. 1949. július 17-én alhadnagyi rendfokozatban avatták. A tanfolyam tovább folytatódott, matematika és fizikatanulással, majd annak befejezése után csak az orosz nyelvvel foglalkoztak. Szeptember 7-én megházasodott. 1949. november 25-én végre elindultak Kijevbe!

A felmérő decemberi vizsgán a tanfolyam idejét félévvel meghosszabbítva, másfél évben határozták meg. Az eredményes tanulás végén államvizsga volt. Szovjetunió Kommunista Pártjának történetéből, amit kiválóra tett le. Még 2 tantárgyból volt vizsgája, amire önéletrajzában nem emlékezik. A vizsga végén főhadnagy lett.

Hazajövetele után a híradó csoportfőnökségre került, a kiképzési osztályra. 1951. november 7-én századossá, 1952. november 7-én őrnaggyá léptették elő.

1953. március l-től kinevezték a Híradó Tiszti Iskola parancsnokává. Változások voltak a képzésben. Megszűnt a női tisztképzés, a tanulmányi időt pedig felemelték 3 évre. Bevezették a felvételi rendszert, a jelentkezést érettségihez kötötték. Az iskola parancsnokát beiskolázták a katonai akadémia levelező tagozatára. 1954 novemberében alezredessé léptették elő.

Személyi életében is változás történt. Megszületett második leánygyermeke. Rendkívül jó sportoló volt. Sport pisztolyban 1. osztályú versenyző, a tiszti röplabda csapatban tagként részt vett a csapatsportban.

1956-ban összevonták az iskolát a műszaki tiszti iskolával. Az iskola parancsnokává őt nevezték ki. Szentendrére költözés után röviddel kitört a forradalom. Kettős szerepe miatt több mint 10 évig nem léptették elő. Első feladatként 250 fővel védte a Magyar Dolgozók Pártja központját, más egységekkel együtt. A forradalom későbbi időszakában fegyverekkel látta el a megalakított Nemzetőrség

[1] Szerző: nyugállományú ezredes, Híradó tiszt.

csapatait.

1957. március l-i dátummal megalakult az összes tiszti iskolát összevonva az Egyesített Fegyvernemi Tiszti Iskola Budapesten (éppen ebben az évben, 50 év után szűnt meg az Üllői úton az elfoglalt épületekben a tisztképzés!).

Az iskolán kialakított Híradó Tagozaton ö lett a vezető, és itt maradt 1980-ig, nyugállományba helyezéséig.

Szolgálata közben a képzés többször átalakult, az iskola főiskola lett.

1957-ben befejezte a katonai akadémiát. 1969-ben egy évre ismét beiskolázták a Szovjetunióba, Leningrádba. 1974-ben megbízták a vietnami tiszti iskola technikai bővítésével. Tanszékén több olyan újítást vezetett be, ami később az egész iskola átvett (osztályfőnöki rendszer, a hallgatók tanszéki alárendeltségbe helyezése, a technikai szolgálatirányítása stb.). A Híradó tanszéken képeztek ki először külföldi hallgatókat.

1974-ben az ő vezetésével létrehozták a Híradó Múzeumot, ami leszűkítve, de még mindig létezik.

1969. április 4-én ezredes lett. Ezután még további munkával segítette a tisztképzést, melynek felsorolására már nem vállalkozom.

Meg kell még említeni a polgári életben végzett, több évtizedes tanácstagi munkáját a XI. kerületben. Mindkét leánya egyetemet végzett. Unokáit szerette, mindig mesélt róluk.

Nyugállományba helyezése után, amíg egészsége engedte, a Zalka, majd a Bolyai nyugdíjas klub vezetője volt.

Több évtizedig dolgoztunk együtt. Először, mint az alárendeltje, majd a nyugdíjas klubban a társa. Voltam vele Vietnamban, segítettem mindazon könyvek kiadásában melynek kiötlője volt. A többször áthelyezett Híradó Múzeum készítésében, majd áthelyezésében rész vettem. Nem volt könnyű ember, de élete végére megváltozott.

Most, hogy már nincs közöttünk, szívesen emlékezem Reá. Élete tanulságos lehet számomra is.

Dr. RÉVÉSZ Gyula

HÍRADÓ KIKÉPZÉS ANOMÁLIÁI

A híradóképzés története szorosan kapcsolódik a híradás és a katonai híradás kialakulásához és fejlődéséhez.

Az ókori görög drámaíró, Aiszkülosz Agamennon című drámájában részletesen leírja, hogyan tartotta a kapcsolatot a sereg vezére, Agamennon a feleségével a trójai háború alatt (jelzőtüzek, 800 km-re).

Korunkhoz közvetlenül kapcsolódó katonai távírásalegységek a XIX. század közepén jelentek meg, majd az ezredfordulón megkezdődött a rádióhíradás fokozatos bevezetése a hadseregekbe, melynek jelentősége az I. és a II. világháborúban teljesedett ki. Ma már a katonai telekommunikációs hálózatok lefedik bolygónk jelentős részét.

A híradó eszközök fejlődésével egyre jelentősebbé vált a híradócsapatok szerepe, melyek meghatározó eleme a tiszti-tiszthelyettesi állomány felkészültsége.

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 megváltoztatása, műveltségük gyarapítása; valamint a mai „rohanó" világ gyors ütemű fejlődésének – mind a számítástechnikai, a híradó és informatikai fejlődésének -, szinte azonos ütemben való követése.

Mindezek egy szakmailag jó felkészültségű oktatói, nevelői és pedagógiai módszerek összességét alkalmazva válnak megvalósíthatóvá. Egyrészt fokozódnak a személyi állomány kiképzésének követelményei, másrészt a társadalmi, a tudományos-technikai fejlődés, a harcászat minőségi változásai a pedagógia folyamatában, sok új elképzelést, lehetőséget hoztak felszínre. Így a szakkiképzésen áteső katonák időszakvégi, meghatározott követelmények teljesítési szintjének bizottságilag ellenőrzött felmérése, az osztályba sorolás is az a tevékenység, amely során megállapítható szintre ér a felkészített egyén.

Az oktatás szükségessége nem csak kötött iskolai intézmények keretein belül válik szükségessé, hanem változatos tanfolyamok megszervezése is hozzájárul a tudásszint gyarapításához. A permanens nevelés- művelődés eszméje, a személyiség egész életén át tartó formálásának- formálódásának gondolata természetesen nem valamiféle abszolút új, előzmények nélkül való, és nem is a XXI. század szülötte.

Valójában az oktatási rendszerben az jön létre, amivel az oktató és kiképzendő azonosulni képes, és aminek a végrehajtására kész. Így fog megvalósulni a kiképzés alkalmával a teljesítési szint produkálása.

A katonai híradás – mint a hadtudomány egyik ágazata – a fejődés során hosszú és bonyolult utat tett meg.

A híradás, illetve a híradó eszközök fejődése az emberi társadalom fejlődésével párhuzamos. Az első híradó eszközök – a harctevékenységekhez hasonlóan – rendkívül kezdetlegesek voltak.

A későbbiek folyamán a fegyveres erők létszámának növekedése, azok körszerűbb harci – technikai eszközökkel való ellátottsága, a harctevékenységek vezetési módszerének megváltoztatása a csapatok vezetését és irányítását is egyre bonyolultabbá tették. A híradással szemben fokozottabb követelményeket támasztottak, amelyek szükségessé tették új, korszerűbb híradó eszközök létesítését és a híradás megszervezése bonyolultabb módmódszereinek alkalmazását.

Ugyanakkor a híradó eszközök tökéletesedése rugalmasabbá tette a csapatok vezetésének megszervezését, ami befolyást gyakorolt a harctevékenységek vezetésének módszereire. Ilyen formában a katonai híradás fejlődése elválaszthatatlan a hadtudomány fejődésétől.

A híradás alapját a veszélyjelzések továbbítása képezte. Módszere: jelzőtüzek, fáklyák, különféle hang- és látjelek stb. voltak.

A különböző vezetési szervek kialakulásával a csapatok irányítására már látjeleket, hangjeleket, valamint a személyes példamutatást alkalmazták. Itt már alkalmazásra kerültek a különböző zászlójelek, kürtök, dobok stb. A harcoló felek létszámának növekedésével alkalmazást nyertek az őrszemláncok, gyalogos, lovas, majd kerékpáros hírvivők. Az összekötőt (megbízott személyek) napjainkban is alkalmazzák.

A XV-XVIII. Században a csapatok fegyverzetében és szervezésében, valamint a háború és harc vezetésének módszerében hatalmas változások történtek. A hadsereg számszerű változásával együtt új fegyverek is megjelentek. Növekedett a híradás jelentősége. Az egyszerű híradóeszközök mind kevésbé feleltek meg a háború és vezetés követelményeinek.

A technikai híradóeszközök fejlődésében az elektromosság felfedezése, alkalmazása, illetve az elektromos híradóeszközök feltalálása gyökeres fordulatot jelentett.

Modern haderőről a XIX. század vége és a XX. század elején végbement gyökeres technikai fejlődés után beszélhetünk. A híradás legfontosabb feladata a minden szintű vezetés megvalósítása. A haderő fejlődésével a csapatok vezetésének rendszere is egyre bonyolultabbá vált. A vezetés nagyobb igényű követelményeit ki kellett elégíteni a híradó technikai eszközöknek, ezzel együtt újabb és újabb technikai eszközök jelentek meg. A híradó kiképzést ezekhez az új megnövekedett követelményekhez kellet igazítani. A magyar haderő fejlődése és átalakulása során a híradó kiképzés is változott.

Megalakult a csak szerződéses és hivatásos katonákra épülő haderő. A szerződéses katonák képzésénél az elsődleges szempont a célirányos kiképzés, tehát konkrétan a beosztásával kapcsolatos feladatokat maximálisan ismerje, és ezeket folyamatosan fejlessze.

Előnye, hosszú időre lehet számolni viszonylag állandó állománnyal, követelményszint növelhető, takarékosabb kiképzés, ütőképesebb.

A híradócsapatok harckiképzésének céljánál, jellegénél, rendeltetésénél, feladatánál fogva, azoknak a céloknak és feladatoknak kell megfelelnie, amelyeket a direktívákban, parancsokban, intézkedésekben és szabályzatokban a Magyar Honvédség katonái, alegységei és egységei felkészítésére, összekovácsolására, az alaprendeltetésükből adódó feladataik teljesítésére való készenlét elérése érdekében meghatároznak.

A híradócsapatok harckiképzési rendszerének felépítése, alkotó elemei, követelményrendszere célirányosan, egységes keretbe foglalja mindazon elvárásokat és célokat, követelményeket és feladatokat, amelyeket a híradócsapatoknak teljesíteniük kell ahhoz, hogy meg tudjanak felelni azoknak az írott és íratlan feladatoknak, melyek a haza védelmének magasztos feladatából rájuk hárulnak.

A híradócsapatok harckiképzése tervezésének alapját a Honvéd Vezérkar főnökének, az MH szintű parancsnokok intézkedései, az előjáró parancsnok parancsa, a kiképzési és szakkiképzési programokban meghatározott feladatok, valamint az adott kiképzési időszakra tervezett kiemelt kiképzési feladatok képezik.

A tervezés általános követelményei olyan elvek, amelyeket a tervezéssel foglalkozóknak, így a parancsnoknak és törzseknek is figyelembe kell venniük a munkavégzés során. A legfontosabb alapelvek: az objektivitás, a komplexitás, a tudományosság, a rugalmasság és részletesség, a közérthetőség és az egységesség.

Az *objektivitás* azt fejezi ki, hogy a tervezésnek a létező valóságra, a szervezet működésére kell alapozódnia, kerülnie kell a szubjektív, az egyedi, vagy csak a szűk csoportérdekeket szolgáló tényezők figyelembe vételét.

A *komplexitás* arra utal, hogy a tervezés folyamatában mindig, minden esetben az egész szervezetet, annak minden folyamatát, tevékenységét összefüggéseiben kell látni ahhoz, hogy az elkészülő új terv illeszkedjen a korábbiakhoz, a korábban már megtervezett és beindított feladatok végrehajtásához.

A *tudományosság* megköveteli a vezetőtől – a meglévő gyakorlati tapasztalatai mellett, - hogy alkotó módon használja fel a tudományok által megteremtett, a gyakorlatban már bevált módszereket.

A *rugalmasság és részletesség* a tervezés során ellentétes követelményként állnak szemben egymással. A terv részletessége az, amely lehetővé teszi, hogy a szervezet különböző vezetési szintjein a tervet el lehessen készíteni. A különböző vezetési szintek nem igényelnek azonos részletességet. Az alsóbb vezetési szintektől a felsőbbek felé haladva nő a globalitás, az általánosság és a rugalmasság és csökken a részletesség igénye.

A *közérthetőség* biztosítja azt, hogy a terv tartalmilag és formailag úgy épüljön fel, hogy azt a szakterületen dolgozók kivétel nélkül értsék, mert ők fogják megvalósítani.

Az *egységesség* azt jelenti, hogy egyszerre egy, mindig csak egyfajta elgondolás lehet érvényben. (Ha több van az zavart okozhat!) Ugyanakkor arra is rávilágít, hogy minden tervnek követnie kell a szervezet specifikus (műszaki, gazdasági, pénzügyi stb.) cselekvési programjait, hiszen egymással kölcsönhatásban függnek egymástól.

Megtanítani és képessé tenni a katonákat szakbeosztásuk teljes értékű ellátására, kialakítani és megszilárdítani együttműködési készségüket az alegység előtt álló feladatok megoldásában.

Felkészíteni a katonákat a híradó és FRISZ eszközök (állomások) telepítésénél és bontásánál egy kezelői feladat irányítás mellett történő ellátására, megtanítani őket az ehhez szükséges alapvető szabályokra, valamint a tevékenységek során betartandó biztonsági rendszabályokra.

Felkészíteni a katonákat az eszközök szabályos üzemeltetésére és forgalmazási szakfeladataik ellátására.

Igen ma is ezen céloknak kell megfelelni, mikor a kibontakozó információs korszakban a globalizáció tendenciái és az informatika változatlan ütemű fejlődése minden szférában folyamatosan bővíti a különböző szereplők közötti együttműködés lehetőségét, ugyanakkor fokozatosan növeli szerepét. Ennek megfelelően növekszik a szereplők közötti interoperabilitás jelentősége is, amelynek megjelenése és előtérbe kerülése a technikai és ezen belül elsősorban az informatikai rendszerek és eszközök hálózatba kapcsolódásához köthető.

Bizony mikor annak idején az egyetemen, a híradótanszék vezetőjének felvetettem azt a problémát, hogy a tananyag, s az előadások jórészt ismeretlen híradó eszközökről és elvekről szólnak, nos Ő kifejtette, hogy e magas oktatási szinten előre kell tekinteni és a közeljövőben tért hódító, új eszközökre szükséges felkészíteni a hallgatókat. Meggyőződése volt (ahogy minden honvédelemre elkötelezett katonának), hogy hamarosan bekövetkezik az áttörés és felzárkózunk a világhoz híradótechnika és rendszerek terén.

Nos ábránd marad, vagy csak lassan haladunk!?

A II. Világháborút követően új magyar rádiókészülékeknél (R-10-től R-50-ig) a szovjet behatás érvényesül a Magyar Néphadseregben. A Varsói szerződés hatására a híradó eszközök cseréje beindul, és 1960-70 között ellátják az alakulatokat. Ezek a rádiók még a mai napig rendszerben vannak és használjuk őket. Ezek az R-130, R-111, R-123, R-140, R-137, R-107, R-159, R-1260, Troposzféra rádióállomás, Relék: R-1412, R-1406, Mikro: R-404, R-414.

A 80-as években kísérleti jelleggel műholdas híradást üzemeltettünk. A rácsrendszerű híradás gondolata már a 80-as években felvetődött, de szovjetek nem engedték mert az irány-tengely híradást alkalmazták.

Napjainkban még mindig az analóg rádiók vannak többségben, de már a rendszerváltás után megjelentek az új digitális eszközöket is. A digitális eszközök megjelenésével szükségessé vált a készülékekre történő kiképzés. (Digitális központok: HICOM 300E; Rádiók: Harris, MRR; Műholdas telefonok: Inmarsat, Iridium, Motorola) Ezeket központi tanfolyamokon valósították meg. Ezekre a tanfolyamokra a csapatoktól iskoláztak be az állományból, de a tiszti és tiszthelyettes képzésben is oktatták.

Rohamosan fejlődő kommunikációs igények a Magyar Honvédségnél is jelentkeztek. Az analóg kapcsolástechnika kiváltásának folyamata napjainkban is zajlik, a rendszer homogenitásáig még hosszú időnek kell eltelnie. A tervezett, a jövőben hadrendbe állítható katonai kommunikációs eszközök, hírhálózatok működése elkerülhetetlen az előzőekben említett kiválóan tréningezett katonák nélkül.

A hivatásos állománynak el kell sajátítania az új digitális rádiók, és más híradó eszközök rendszerben történő használatát, azok beillesztését a hálózatokba, azokkal történő szervezési, tervezési munkák elvégzését.

A tiszthelyettesi állomány a kivitelezés és megvalósítás legfontosabb rétege, számukra elsőrendű feladat az eszközök teljes mértékű ismerete, alkalmazása, illetve a beosztott állomány felkészítése.

A kiképzésen megfelelő mennyiségű, minőségű szemléltető eszközöket, segédeszközöket, trenazsőröket kell alkalmazni, illetve az éles gyakorlatok számát növelni kell a kiképzési tervekben.

A műholdas összeköttetés kiemelt jelentőségű az új kommunikációs rendszerben, ez az egyetlen átviteli út, amelyet a Magyar Honvédség nem használt a régi (analóg) eszközök alkalmazása során. Mára a külszolgálatok fontos összeköttetési vonala a műholdas kapcsolat.

A jelen és a jövő új technikai vívmányai közé tartozik az előző eszköz mellett a „digitális katona" által alkalmazott eszközök, video-konferencia összeköttetések, és számos újítások, melyeket a nyugati országok hadseregei már alkalmaznak.

Összegezve, a jövő katonáinak ismernie kell a számítástechnikai eszközöket, alkalmazásokat, a digitális rendszereket, magas szintű nyelvtudás birtokában kell lenniük.. A tiszt állománynak szervezői, tervezői, a tiszthelyettesi állománynak technikai és kiképzési ismeretekkel, a szerződéses legénységi állománynak pedig kezelői ismeretekkel kell rendelkeznie.

A híradótisztek képzése, akik katonai szakmai (villamosmérnöki) és az általános katonai (tiszti) tudás birtokában, rövid adaptációs időszak után képesek a híradó alegységparancsnoki, vagy javító alegységparancsnoki funkciók ellátására és a technikai, szervezeti változásokból adódó új feladatok végrehajtására.

A civil szférában a kommunikációs információs hálózatok és eszközök sokkal nagyobb ütemben fejlődnek, mint a katonai téren. Ennek oka egyértelműen a sokkal nagyobb piac a civil szférában. Kevés cég foglalkozik katonai alkalmazásra szolgáló berendezésekkel. Éppen ezért, hogy a hadsereg ne maradjon le technikailag, a kereskedelmi célokra gyártott rendszereket kénytelen alkalmazni. Ez persze nem minden esetben tesz eleget a NATO-irányelveknek. Napjainkban és a jövőben is a civil informatikai és a távközlési technológiák és eszközök fejlődési irányvonala határozza meg a Magyar Honvédségben alkalmazott eszközöket is.

A híradó ezred rendelkezik azon hagyományos technikai eszközparkkal, amely jelenleg még az MH hírrendszerének alapját képezi, valamint folyamatosan (bár lassan) egészül ki a technikai állomány korszerű eszközökkel.

Az eddigiekben leírtakból jól látszik, hogy mindenki ismeri-látja a híradó képzés (és egyéb területek fontosságát), támogatásának szükségességét. Noha sokat és meggyőzően beszélünk e tény fontosságáról, szinte semmi sem történik. Valószínűleg a politika, a pénzügy és hasonlók állnak a háttérben, de a lényeg nem változik.

Mivel nincs (szerencsére) közvetlen katonai veszély az országra, így a fontossági sorrend is összekuszálódik. A folyamatos létszámcsökkentések, átszervezések rettenetesen rányomták bélyegét a honvédségre. Gyakorlatilag missziós haderő lettünk és csak ezen illetve fenntartási és PR tevékenységek (falunap, bemutatók) feladatait hajtjuk végre.

A híradó tevékenység stabilan működik az objektumokban telepített hírközpontok által, valamint a mobil kisalegységek tevékenységein keresztül. Ez így igaz, de hogy ez milyen nehézségek árán teljesül, arról kevesen beszélnek.

Egyik fő probléma a létszámhiány, folyamatos a lemorzsolódás és egyre kevesebb a jelentkező. Ez egyértelműen anyagi és technológiai-ideológiai okokra vezethető vissza. A másik fő ok a kiképzés képzésrendszere. Míg a régi haderőben az iskolák komoly szervezésűek voltak, tele szakember gárdával, addig jelenleg talán már katonai iskola sincs. Amíg az alakulatokhoz megfelelően képzett híradó katonák érkeztek az iskolapadból és csak a tapasztalatszerzés, a gyakorlati ismeretek, valamint a rutin megszerzése volt a cél. Így hamar jó képességű szakemberek dolgoztak szerte az alakulatok híradó beosztásaiban. Jelenleg ez már csak a régmúlt idézése, mivel az utóbbi években megváltozott a képzési rendszer.

Híradó beosztásba érkezetteknél lehet kezdeni az átképzéseket, de ez a meglévő feladatokkal együtt roppant nehéz. Súlyosbító tényező a megfelelő szabályzatok, segédletek és legfőképpen a tantermek hiánya. A híradó szakág képzése technikai és tantermi segítség nélkül egy szélmalomharc. Mobil eszközökön hajtódnak végre a foglalkozások, megsokszorozva a hibalehetőségeket, a javítási feladatokat.

Missziós haderő, ugye korábban részleteztem, milyen nehéz kezelni a híradó eszközöket alapos felkészítés hiányában. Ugyanakkor halmozódik a probléma, hogy sok külszolgálaton olyan eszközöket kezelnek a katonák, ami itthon csak elvétve található meg, vagy még annyira sem. Korszerű műholdas képzés még ennél is nehezebb, mivel a használati díja kiemelkedő, így próbaüzemeket sem tanácsos végezni.

Fölösleges sorolni, mennyire szükséges lenne több és komolyabb technikai eszközökre, oktatási költségre, tantermekre, hiszen ezek magukért beszélnek. Nem lehet lebontani egy kiépített hírközpontot, hogy gyakorlás-képzés miatt újra felépüljön, vagy egy működő tábori hírrendszer híradó autóinál sem lehet gyakoroltatni az állományt újabb és újabb feladatokkal.

Megoldás a már említett felszereléseken múlik, de a legmodernebb technikai eszközök sem alkalmazhatók kezelőszemélyzet nélkül. Fentebb már utaltam az objektivitás fogalmára, de szembetűnő, mennyire nem valósul meg. Amikor az alegységek képzését sutba kell vágni, mert az elöljárónak éppen költözködési gondjai vannak.

A missziós leterheltség kettős megítélésű, hiszen komoly szakmai tapasztalatokkal jár, ugyanakkor a kiesett személyeket nehéz pótolni. Nagy idővallum a felkészítés- feladat-szabadság vonzata.

A megnövekedett díszelgési-kegyeleti feladatok épp úgy nyomják a híradók vállát, mint a frekvenciagazdálkodás. Régen tömkelegével állt rendelkezésre frekvencia, most a civil szféra elviszi a minőséget és csak a maradékból hámozgathatunk. Ez roppant felelőtlen és nagyon megnehezíti a gyakorlást. Sok esetben végrehajthatatlan feladatokat eredményez.

Összegezve megállapítható, hogy az új feladatok ellátására alkalmas modern haderő, csak a megfelelően kiképzett, eszközökkel felszerelt, felkészített és elegendő létszámú katonák segítségével állítható fel.

A fejlett, más hadseregek által már alkalmazott katonai kommunikációs hálózatokban digitális eszközöket alkalmaznak, melyek működéséből, kezeléséből adódóan új kiképzési rendszert kell kialakítani. Ennek biztosítására, előkészítésére elsődleges fontosságú a tiszti állomány kiképzése. Ezen állomány számára a sikeres feladat végrehajtás szempontjából legfontosabb a rendszerszemléletű gondolkodásmód, amely azt jelenti, hogy képes legyen az adott feladathoz kiválasztani a legmegfelelőbb kommunikációs rendszer felépítését, az alkalmazott módszereket, az összeköttetéseket, az alkalmazásra kerülő eszközöket.

Balázs PÁNDI– Erik PÁNDI2

KEY ISSUES REGARDING THE APPLICATION OF SOFTWARE TOOLS TO SUPPORT THE ORGANIZATION OF THE FIELD COMMUNICATIONS SYSTEM

Abstract: the article provides an overview of requirements - primarily from a NATO mission perspective - currently set out for the national military communications systems, then highlights the key issues regarding the application of software tools to support the organization of the Field Communications System for increased efficiency.

Keywords: CIS, C4, information, information technology, support.

1. Requirements set out for the national military communications systems

Since the era of the mass-armies has ended, both domestic and foreign military specialists have been forced to reconsider how to create such a new army that meets the challenges of our modern age, and is reconcilable with economic potential of a sustainable nation. In general it can be said that, due to the tightening of the military budget, focus has shifted to the solutions, which increase efficiency in the most economic way [1]. The extensive changes on the field of Information Technology in the previous decades, have expressed a strong demand for modernization of both the field and stationary communications systems. In the past few years many developments have focused on the creation of intelligent networks. The tendency has definitely shifted towards the smart, self-organizing, self-repairing networks [2]. The Hungarian Army is especially interested in the transformation of its' communications systems, as its' national and international responsibilities, and both personnel and financial capabilities, have fundamentally changed since joining NATO. Taking our current capabilities into account, these changes will definitely have to utilize the technological possibilities offered by the civilian sector [3].

An example of the changed circumstances is Hungary's active cooperation in the *International Security Assistance Forces* (ISAF) mission, where both civilian and military technical equipment and solutions can be found during the organization of the communications. The mission circumstances set out requirements on a wide scale for the applied technology. Key issues in terms of transferring information:

time needed for transferring information;
security of information;
invulnerability and integrity of information;
availability of information.

The realization of the above is assured by the communication and computer networks deployed for the Hungarian forces. *Communication networks* can be

[2] authors: Balázs Pándi, PhD-student, ZMNE BJKMK PhD Institute in Military Technology; asc. prof. Erik Pándi PhD, ZMNE BJKMK Department of Communications.

partly wired, or completely wireless, from which the communication between the individual campgrounds is always via satellite link, based on wireless communication, while the communication between campsites within the campgrounds is managed by UHF radio networks or satellite phones.

The organization of computer networks is done in a similar manner. The computer systems connected to the backbone network are connected via satellite link, while local intranet networks also exist, which have different levels of classification.

1.1 Communications networks

The communications network is based on an *Initial Voice Switched Network* (IVSN). It's also possible to make classified calls on this system. The backbone network is created by satellite link. *Inmarsat* and *Iridium* subsystems have been introduced for this system, the operational cost of these is however quite expensive. The Iridium system only provides a low level of data-security, while the Inmarsat system together with additional endpoint devices is capable of managing calls with a high level of information-security. In the UHF radio systems, the most commonly used device is the *Harris radio*, which is capable of both voice and data transmission. During NATO missions the systems of local GSM providers can also be used, but mainly for being in contact with the local authorities.

1.2 Computer networks

The campgrounds are connected using the NATO network based on the Microsoft Windows Active Directory System, which conforms to the highest level of security requirements (ISAF Secret Net). The main profile of the network is a mailing system using a modern addressing structure, and a Web portal (WISE page). The campgrounds and campsites also have local area intranet networks with different levels of classification. The networks are separated and the number of users with access to the system is also limited. The main concepts are:

users can only access data, which they have access to;

administrative access is kept on a minimal level;

the application of the "complete and satisfactory" concept when creating the system and the services;

the construction of a system/directory structure based upon special access rights for storing information, where the main point is that after a piece of information is entered into the live system, the user is unable to alter or delete it;

tape backups for protection against specific hardware faults [4].

It can be seen that communication of national military corps and sub-corps to be applied in an international environment is done by complex systems and solutions. So one of the crucial aspects of the new communications network based upon digital technology that the Hungarian Army would like to introduce, must be to conform to the requirements set out by NATO, in other words interoperability [5].

2. Key issues of software support

According to AAP-31 (NATO Glossary of Communication and Information Systems Terms and Definitions) the Command and Control Communications and

Computer system is inseparable. The C4 is an integrated system of doctrines, procedures, organizational structures, personnel, equipment, devices and communications, whichs' purpose, is to support commanders in command and control during military activities [6]. It can be seen that design and organization of the national field communications networks requires a new perspective. These processes today can no longer be carried out, according the traditional methods, in other words the everyday *write it on paper, send it, and finally the military organizations will try to execute it* process. The design and organization of the modern, digital communications system today can only be done by advanced hardware and software support [7]. Considering that the Hungarian Army in terms of the field communications system lacks modern solutions, in our opinion the military purpose design and organization software should implement the following functions:

selecting the deployment area on a digital map;
specifying the physical location of the nodes;
defining of the link between the individual nodes;
simulation;
necessary modifications after the simulation;
printing and visualization tasks;
data exchange with other users, and executive personnel;
network monitoring in the functioning system.

2.1. Selecting the deployment area

The software has to provide an option to select the deployment area on a digital terrain model (in the homeland, or primarily in the EU), where we would like to deploy the nodes of the grid.

2.2. Specifying the physical location of the nodes

The software has to provide an option to specify the exact (geographic) deployment location of the nodes and communications centres.

2.3. Defining the link between the individual nodes

After specifying the physical location of the communications centres, the software has to be able to calculate the connection-probability of the individual directions, and line-segments. At this point there has to be an option to create databases in which the tactical potential, the amount of technical equipment, the forces and equipment used and other additional data can be stored so that the executive personnel can access this when preparing the required outputs.

2.4. Simulation

This function can be considered the most important. After specifying the physical location of the nodes and defining the link between the communications centres, simulation of the network has to be done in order to find out the behaviour of the network under periods of load, the load characteristics during individual (attack, defence, non-combat) operations, and the problems which can arise.

2.5. Necessary modifications after the simulation

If during the simulation the system is unable to reach the requested performance, the software has to provide an option to modify the network by adding additional nodes, directions, or by modifying the connections of the communications centres. After the applying the modifications, the ability of the network to reach the requested performance can be verified by re-running the simulation.

2.6. Printing and visualization tasks

At this phase there has to be an option, to print the visualized results. It should be possible to display the incoming and outgoing channels from the individual nodes.

2.7. Data-exchange

The system has to ensure that the data is entered in a format that can be transferred, and converted to formats used by other planning software.

2.8. Continuous network monitoring

The purpose of this option is that high level network administration (e.g.: OHK) can also monitor the operation of the system and the individual nodes and through this, can increase the reliability of the system and its' the ability to react.

3. Summary

Our nation unfortunately only came to realize during cooperation in NATO operations, the necessity and the difficulties of introducing modern military communications networks. The Hungarian Army still does not have a modern field communications system, hence the modernization processes, in other words the equipment and system purchases, will have to consider the requirements also pointed out in this publication.

* * *

References

[1] Éber, László: A jövő hadseregének megteremtése (fejlesztés-modernizáció-hatékonyság és gazdasági kérdések), Nemzetvédelmi Egyetemi Közlemények, ZMNDU, Budapest, 2006, ISSN 1417-7323, pp 68-69, No 2, Vol 2006

[2] Takács, Péter – Rajnai, Zoltán: Gondolatok egy tábori hírhálózatról, Kard és Toll, MoD, Budapest, 2007, ISSN 1587-558X, pp 133, No 1, Vol 2007

[3] Takács, Péter: Possible wireless networks on the battlefield, „Kommunikáció 2007." National Science Conference, ZMNDU, Budapest, 2007, ISBN 978-963-7060-31-1, pp 263

[4] Rajnai, Zoltán – Takács, Péter: Az afganisztáni missziós híradás tapasztalatai, Kard és Toll, MoD, Budapest, 2006, ISSN 1587-558X, pp 28-31, No 3, Vol 2006

[5] Farkas, Tibor: A honvédség tervezett kommunikációs hálózata, Kard és Toll, MoD, Budapest, 2006, ISSN 1587-558X, pp 53, No 1, Vol 2006

[6] Sándor, Miklós – Farkas, Tibor: A honvédség állandó hírhálózata fejlesztésének kérdései, Kard és Toll, MoD, Budapest, 2006, ISSN 1587-558X, pp 159, No 2, Vol 2006

[7] Rajnai, Zoltán: A Kommunikációs rendszerek tervezését segítő szoftverek igényei, „Kommunikáció 2000." National Science Conference, ZMNDU, Budapest, 2000, pp 147-148

Dr. FREGAN Beatrix

CERTAINS ASPECTS SÉCURITAIRES DE L'IDÉE EUROPÉENNE

Pendant plus de 40 ans, le continent européen a été divisé en deux grandes entités politiques alors considérées immuables. Cet antagonisme a disparu de manière aussi brutale qu'imprévue, avec l'effondrement de l'URSS et la fin de sa domination sur les pays d'Europe centrale et orientale. Deux années auront suffi, de la chute du mur de Berlin en 1989 à la dissolution de l'URSS en 1991, pour que s'opère un renouvellement total du paysage politique, économique et militaire. On se trouvait désormais en présence d'une zone émancipée qui, exposée à une multitude de nouvelles menaces, principalement de nature économique et ethnique et aux contours encore flous, cherchait à rejoindre le camp occidental. En Europe centrale, orientale et balkanique, la chute du communisme s'est inscrite dans le cadre d'un retour en Europe qui s'est identifié entre autres à l'Union Européenne (UE). Ce thème a été repris par les principales forces politiques dans leurs campagnes lors des premières élections libres. Le principal atout de l'UE, outre le fait d'avoir combattu la domination soviétique, était simplement d'exister comme antidote ou alternative à l'intégration soviétique.

Pour l'UE, l'élargissement a nécessité une réforme profonde des politiques structurelles et un réexamen de l'ensemble des politiques communes, en gardant comme fil conducteur le principe de subsidiarité. Plusieurs motivations se mêlaient dans l'engouement des pays d'Europe centrale et orientale (PECO) pour l'UE. En premier lieu l'espoir de concrétiser le sentiment d'appartenance à une culture et à une civilisation commune: la " tendance à l'intégration volontaire " en cette fin de XXème siècle, " concerne les civilisations et pas les continents " (ancien Premier ministre hongrois József Antall). Pour la première fois depuis plus d'un demi-siècle, ces pays avaient le sentiment de pouvoir réconcilier leur géographie et leur histoire, leur culture et leur appartenance politique. Leur seconde motivation était éminemment politique : rendre la réussite de la transition à la démocratie irréversible. La question était de savoir si l'UE peut jouer vis à vis des PECO un rôle analogue à celui que la Communauté a joué dans la consolidation de la démocratie en Europe du sud. Essentielle, la troisième motivation éait économique. Pour les pays rompant avec un étatisme et un modèle d'intégration soviétique, l'UE représentait un modèle d'économie de marché et de prospérité qu'ils souhaitaient adopter au plus vite. Mais c'est aussi dans le domaine économique que les pays du centre-Est européen avaient le sentiment de rencontrer les obstacles les plus marqués à leurs objectifs d'intégration; leur désillusion se transformait souvent en critiques acerbes.

Le modèle d'intégration européenne ne se résume pas à la formule: le marché plus la démocratie. C'est aussi pour l'Est un antidote à la montée des

nationalismes. Paradoxalement, pour les pays de l'ex-bloc soviétique, le retour à la liberté s'identifie souvent au retour de la Nation, alors que le projet européen est perçu comme un dépassement de la Nation. L'Europe, dit François Furet, ne peut renier ses origines : la victoire de la société sur la Nation. A l'Est, le rêve européen a longtemps été l'apanage des intellectuels. Depuis 1989, il s'agit de le matérialiser sous la forme d'un projet politique et économique.

L'élargissement aux pays de l'Est a posé une série de problèmes qui tiennent à la fois à la nature des politiques communes et à l'état des mécanismes institutionnels. Assurer la sécurité nationale de son pays, se résume à préserver son indépendance et son intégrité territoriale, sa forme de gouvernement constitutionnelle et démocratique, et protéger ses habitants dans des circonstances critiques. Mais dans la pratique, tous les Etats membres de l'OTAN ont souscrit à des obligations de défense mutuelle et la plupart des Etats européens ont établi, depuis des décennies, des relations économiques toujours plus étroites. Cette structuration complexe de la sécurité européenne fait partie intégrante des relations occidentales et influence fortement les concepts de sécurité nationaux. C'est en revanche une nouveauté pour les PECO qui devaient abandonner leurs concepts de sécurité nationale pour en concevoir de radicalement différents.

Du temps de la guerre froide, les pays d'Europe centrale et orientale n'avaient pas de concept de sécurité nationale au sens occidental du terme. L'Union soviétique avait décidé de sa teneur, imposait son contrôle dans tous les pays du pacte de Varsovie. Pour définir un concept de sécurité, il ne suffit pas d'adapter un modèle européen existant et de le compléter d'une liste d'obligations spécifiques. Certes, l'Occident peut déterminer des principes et des lignes directrices, mais il n'existe pas de modèle universel adaptable aux pays post-socialistes. Ces nouvelles démocraties ne pouvaient s'appuyer sur une quelconque expérience, et le concept de sécurité nationale ne peut se résumer aux seuls plans militaires.

Pour adhérer à l'Alliance, les pays de l'Est devaient opérer des changements fondamentaux dans la conduite des affaires de sécurité et de défense. Il n'existe pas de formule ou de modèle unique du contrôle démocratique, ce qui rend difficile tout jugement sur sa qualité. Un cadre constitutionnel et juridique clair, un ministère civil de la défense et une véritable surveillance parlementaire représentent cependant le minimum nécessaire.

Enfin, le caractère défensif des alliances occidentales impose aux membres d'abandonner toute attitude menaçante à l'égard de leurs voisins. L'organisation, la préparation et l'instruction des forces armées doivent donc revêtir un caractère défensif, et les niveaux de forces doivent être réduits au minimum nécessaire.

Tout concept de sécurité expose en détail les préoccupations sécuritaires et l'attitude militaire d'un pays; sa politique de défense indique comment il réagira à ces questions. Le concept oriente donc la politique de défense, en privilégiant la posture défensive. Il reste alors les choix stratégiques, par exemple entre les

postures de dissuasion (adaptée à une grande puissance) et de refus (capacité pour un petit Etat d'interdire à tout agresseur l'invasion rapide de son pays). Cette stratégie s'accompagne d'un choix entre la défense du territoire, purement militaire, ou la défense globale, qui exige une action à long terme. La politique de défense détermine enfin la structure des forces (professionnelles, de conscription, ou panachées etc.) La réflexion sur la sécurité évoluant du concept vers la politique puis la planification, l'importance des relations entre le civil et le militaire s'affirment corrélativement. Les civils consultent les militaires pour arrêter le concept de sécurité. Leur coopération devient beaucoup plus étroite en matière de politique de défense. Enfin, les plans de défense, la préparation et le déploiement restent des prérogatives militaires.

Pour les nouvelles démocraties, l'élaboration de la politique de défense risque de soulever des difficultés dans les domaines civil et militaire. En effet, ni l'un ni l'autre ne possèdent une grande expérience en matière de répartition des responsabilités et de division des tâches.Une hiérarchie des priorités conflictuelles s'impose (défense nationale, participation à des activités de maintien de la paix, gestion des crises et situations d'urgence dans le domaine civil). Avec des budgets modestes, les PECO devaient entreprendre des réformes considérables (réduction de formats pléthoriques et reconstruction des industries de défense). La nouvelle définition de la sécurité met de plus en plus l'accent sur la réalisation d'un équilibre entre la prospérité, la démocratie au niveau national, l'égalité politique des minorités ethniques et la diplomatie préventive. L'équilibre des influences entre les deux partenaires transatlantiques s'est aussi modifié. L'intérêt évident des européens à maintenir un partenariat de sécurité n'a pas disparu; ils dépendent toujours fortement des capacités américaines. En revanche, avec la disparition des blocs, l'intérêt américain en Europe, sur le plan sécuritaire, a changé. Son intérêt géopolitique fondamental à maintenir la stabilité sur l'autre rive de l'Atlantique (son premier partenaire commercial) subsiste. Dès lors, le partage des responsabilités devra être en rapport avec les capacités et attentes de chacun.

CSUKA Antal3

INFORMÁCIÓVÉDELEM, MERRE TOVÁBB?

A korszerű műszer és méréstechnikán belüli fejlesztések információbiztonságra gyakorolt hatása még csak most körvonalazódik. Az összefüggések figyelemre méltóak.

Valós idejű spektrumanalízis. Új fogalom, ami ma már nem csak fogalom és elképzelés, hanem eljárás, módszer, ami mögött ott van több évtizedes fejlesztés eredményeként egy olyan eszköz, ami a még biztonságosnak hitt védelmi eljárásokról bebizonyíthatja, hogy a legalapvetőbb feladatuknak sem tesznek eleget. De attól kezdve akkor, hogyan és merre tovább információvédelem?

Bevezetés

A haderőfejlesztés és reform megvalósításának előfeltétele az elektronizálási programok keretében megvalósuló eszközfejlesztés és korszerűsítés.

Az eszközfejlesztés alatt a legkorszerűbb technológiák bevezetését, alkalmazását kell érteni, ami biztosítja a haderő megújulását, mindenkori hatékony működését és a biztonságot. A hatékonyság és biztonság összefüggését vizsgálva megállapítható, hogy egyiket és másikat is rendkívül sok tényező befolyásolja. Eszközszinten a képességeket döntően a bevezetett újszerű technológiák határozzák meg. Információ- és adatbiztonság nélkül elképzelhetetlen a hatékony működés, a haderő ütőképessége, ezért ennek kiemelt jelentősége van a fejlesztési koncepciókban.

„A XXI. századi haderő (FORCE XXI) a digitális hadszíntér, a digitális harcos, az információs harcos, az információs hadviselés koncepciói, és más korszerű kapcsolódó elektronizálási programok megvalósulását feltételezi, és egyben igényli is". [1] Örökérvényű igény, ami miatt ezek a programok soha sem tekinthetőek befejezettnek. Ugyanakkor figyelemre méltó a fejlesztés iránya. Egyfelől az igény, de főként az innováció határozza meg döntően, hogy milyen ütemben és milyen irányba halad a fejlesztés. Az elektronizálási programok eredményeire és irányára az eszközök műszaki jellemzői, tulajdonságai, fizikai méretei, az alkalmazott forradalmian új technológiák, bámulatos megoldások alapján viszonylag egyszerűen lehet következtetni. Sok részlet azonban még így is rejtve marad. Az „elektronizálási program" túlzottan széles fogalomkör ahhoz, hogy egy szűkebb szakterület eredményeit szemléletesen kifejezze. A technológiai fejlesztések mindemellett a műszaki terminológiára is hatást gyakorolnak. Olyan új szakkifejezések megjelenéséhez, bevezetéséhez járulnak hozzá, amelyek korábban ismeretlennek számítottak

[3] Zrínyi Miklós Nemzetvédelmi Egyetem Katonai Műszaki Doktori Iskola doktorandusz hallgató

Mobil híradástechnikai eszközök fejlődése

A katonai műveletek sikeréhez nagymértékben hozzájárulnak a kommunikációs, kapcsolattartást szolgáló eszközök. A kutatás és fejlesztés iránya is ezt tükrözi, gondoljunk a „digitális katona" felszerelésére. Ütemét a „mobil fegyveres küzdelem" megteremtésének törekvése diktálja. Mindez elképzelhetetlen a vezeték nélküli kapcsolat biztosítása nélkül. Óriási szerep jutott a mobil kommunikációs eszközöknek, amelyekkel ma korlátlan távolságok áthidalhatók. Ez csak úgy lehetséges, hogy hasonlóképpen gyors ütemben fejlődött a hálózat alapú kommunikáció. Új modulációs elvek teszik egyre bonyolultabbá ezeknek, az eszközöknek a működését.

Ha nagyléptékű és gyors fejlődésről esik szó, szinte kivétel nélkül a számítástechnika kerül előtérbe, holott a távközlés legalább ugyanolyan ütemben fejlődött az elmúlt néhány évtizedben. Az új alapokra helyezett fejlesztés a digitális nagysebességű műholdas kommunikáció irányába halad, mivel ez biztosítja a leghatékonyabb, és akadálymentes információtovábbítást.

Egy mai komplex híradó rendszerben elválaszthatatlanul egybefonódik a híradó egység és az informatikai rendszer. Nem csak a híradótechnikát reformálta meg az információtechnológia, hanem az informatika is egyre inkább a híradástechnika befolyása alá kerül. Utóbbira talán a legjobb példa a vezeték nélküli kommunikáció és annak nem minden esetben indokolt, erőszakos, megállíthatatlannak tűnő előretörése, napjainkban. Egyre szorosabb kapcsolat alakul ki az informatika és híradástechnika között, amire minden mai korszerű híradástechnikai eszköz példaként szolgálhat.

Az „elektronizálási programok" kissé idejemúlt és túlhaladott fogalmát felváltotta a digitalizálás, és ez a fogalomkör tovább bővül.

A töretlen fejlesztés nyomán újabb problémák kerülnek előtérbe, amelyek mind megoldásra várnak és komoly feladatok elé állítják a fejlesztést. Hiba lenne azonban a digitalizálásnak túlzott jelentőséget tulajdonítani. Itt ennél jóval többről van szó.

A digitális jelfeldolgozásnak magától értetődően szerepe van az információs technológiákban.

A mai híradástechnikát újszerű megoldások, és jelfeldolgozási technikák egész sora emeli ki az ismert megoldások közül. Ebben a digitalizálás, mint fogalom lassan és szinte észrevétlenül a háttérbe szorul. Vitathatatlanul mérföldkőnek számít a jelfeldolgozásban, viszont az eszközfejlesztés ma egy új irányt követ. Kényszerű fejlesztés öngerjesztő folyamata, ami a hidegháborús viszonyokra emlékeztető versenyben bontakozik ki. Ma főként az információ jelentősége kerül előtérbe és a figyelem az információbiztonságra összpontosul. Ez egyúttal meghatározza a fejlesztés irányát is. Kriptográfia, kriptoanalízis idejét múlt fogalmait felváltja valami új, amit ma még nehéz lenne megjósolni. Felfedés, megfejtés – talán-, ma mindinkább ezen van a hangsúly, és alapvetően ez jelenti a valódi kihívást, ha információs hadviselésről beszélünk.

„Az elektronikai ipar képességei meghaladják a szolgáltatások fogyasztóinak igényeit."[2]

Helytálló a nagy tömegek igényeit messze meghaladó komersz távközlési eszközök esetében. Egyes szakterületek mohón lesik az elektronikai és alkatrészipar

újabb eredményeit. A technológiai fejlődés újabb és újabb lendületet ad a miniatürizálásnak és az egyre magasabb fokú integráltságnak, ami által egyre komplexebb eszközök megalkotására nyílik lehetőség.

Információbiztonság

Az információ jelentőségét a szakirodalom kiemeli és hangsúlyozza.

Az információ a szervezetek – közöttük a katonai szervezetek – egyre növekvő jelentőségű erőforrása.[8] Más megfogalmazásban: „Az információnak hova tovább egyre nagyobb a jelentősége a hadügy területén". [3]

A kapcsolattartásra használt eszközök mindegyike, függetlenül attól, hogy vezetékes vagy vezeték nélküli információtovábbítást valósít meg, magukban hordozzák a továbbított bizalmas adatok illetéktelen személyek kezébe jutásának a kockázatát. Így, az információbiztonság központi kérdéssé, megvalósítása kiemelt feladattá vált a telekommunikáció fejlődése során. Az illetéktelen megismerés lehetősége fennáll, annak ellenére, hogy az igénybevett szolgáltató kötelessége biztosítani, különféle algoritmikus és rejtjelező módszerekkel, az adatforgalom biztonságát. Annak lehetősége, hogy az adatforgalom megfigyelhető és esetleg rögzíthető folyamatos kockázatot jelent, ennek ellenére. Eszerint a biztonságot mindenekelőtt az átviteli közeg és a vivő jellemzői határozzák meg.

Az információvédelem a megismerés veszélyét hangsúlyozza, kiemelten foglalkozik vele és az információs hadviselés körébe sorolja. A különféle védelmi megoldások ma még hatékonyan biztosítják a megismerés elleni védelmet, aminek következtében az elektronikai hadviselés nagyobb szerephez jutott. Nyilvánvaló az információs hadviselés fokozatos térvesztése, illetve átalakulása, ha a továbbított információ tartalmának a megismerése a cél. Sem a titkosítás, sem az „igénybevett utak" védelme nem biztosítja az adatok teljeskörű védelmét, ezért egészültek ki ezek a technikák különféle modulációs eljárásokkal. Nagy része ma egyre kevésbé csak a katonai rendszerek sajátossága. A hétköznapinak mondott, kommersz, vezeték nélküli eszközökben éppúgy megtalálhatók ezek a biztonságot szolgáló megoldások csakúgy, mint a kulcsfontosságú katonai híradó eszközökben.

Ilyenek a kiterjesztett spektrumú (LPI/LPD) adó-vevők, frekvenciaugratásos (hopping) rendszerek, kódosztásos (CDMA) rádió rendszerek, stb.

Alaposan összemosódott a katonai és „polgári" híradás, aminek veszélyei csak most kezdenek körvonalazódni. Ez további problémákat vet fel, ami az adatbiztonságot illeti. A hajdani egyszerű teljesítmény centrikus információ és adatátvitelt - az „erősebb győz", elnyomáson alapuló szemléletet-, mára felváltotta az „intelligens"- legalábbis annak tekinthető-, titkosított adatátvitel.

Eszköze a kis méretű, könnyű, alacsony fogyasztású, nagy komplexitású adó-vevő, amit különleges módon kell védeni. Növekvő „tudásához" nagyfokú sérülékenység társul fizikai értelemben.

Az eszközfejlesztéssel párhuzamosan fejlődtek az elektronikai hadviselés eszközei is, amelyek maguk is új fejlődési irányt képviselnek a technológiai fejlesztésben.

A kis valószínűséggel felderíthető és zavarható (LPD/LPI- Low Probality of Detection/Interception) adattovábbítási módok hosszú időn keresztül biztosították a szükséges biztonságot, olyan megoldásokkal, mint a spektrumkiterjesztés (FSS-

Frequency Spread Spectrum), frekvenciaugratás (FH- Freqvency Hopping), direkt szekvenciális zajmoduláció, stb. Mindezt kiegészítik az olyan eljárások, amelyek a WLAN, DVB-T, RFID, 3G, 2G jelekre jellemzőek [4]. Különösebben, eddig sem képezte vita tárgyát, hogy mindegyik adásmód sajátos módon felderíthető, a közvetített adatcsomag rögzíthető és kielemezhető, csupán a megfelelő eszköz még eddig nem állt rendelkezésre.

A legfőbb nehézséget az okozza, hogy a jel befogására és analízise (az értékes adatok kiszűréséhez) nem éppen kevés időre van szükség

A többszintű védelem, ami egyrészt a kommunikációs utak titkosításából, vivő manipulálásból, kombinált moduláció alkalmazásából, másrészt kiegészítő adatbiztonsági (COMSEC – Communication Security) eljárásokból tevődött össze, feltörhetetlen, megfejthetetlen és kellőképpen biztonságos adatátvitelt feltételezett és feltételez még ma is. Ez a feltételezés viszont meginogni látszik bizonyos új elvek szerint működő mérési eljárások és eszközök felbukkanásával. Részletekbe menő ismertetését megelőzően vizsgáljuk meg, hogy mi támasztja mindezt alá.

Az adatvédelem mind a mai napig két pillérre támaszkodik. Egyik az észlelés és befogás lehetetlenné tételét igyekszik a maga eszközeivel minél hatásosabban megoldani, a másik az adattitkosítást használja eszközeként.

Az adat titkosítás több évtizede kielégítően oldja meg a rá ruházott feladatot a titkosító algoritmusok és kriptográfiai eljárások által. Ne feledjük azonban, hogy ez egy múltbeli szemléletet hordoz magában, egyfajta ellenző, ami a szűk látókör fenntartását szolgálja hosszú ideje. Arra támaszkodik, hogy az algoritmusok megfejtése és az üzenet desifrírozása olyan időigényes művelet, ami alatt a tartalom érvényét veszti [5]. Hiba lenne azt hinni, hogy hosszútávon biztosítja az információ és adatbiztonságot.

„Így nem elég átgondoltak azok a nézetek, amelyek az elektronikus információvédelem egy területét helyezik előtérbe (pl. rejtjelezéssel mindent megoldottnak tekintenek)". [2] Amennyiben a technikai és műszaki fejlődés megragadt volna egy adott szinten, akkor kétségtelenül a titkosítás időtálló megoldás maradhatott volna. A számítástechnika rohamos fejlődése megállíthatatlan, ami miatt megdőlni látszik ez a nézet.

Vezeték nélküli információtovábbítás esetében a „megismerés" veszélye hangsúlyosabban merül fel, mint bármilyen más esetben, ahol a kisugárzás kisebb mértékű és a jelcsatorna védettsége valamilyen formában biztosítható. Sajátossága, mondhatni gyenge pontja, abban mutatkozik meg, hogy az információbiztonságba vetett hit érdekes megoldásokat szült. Gondolok itt arra, hogy az igénybevett utak nem mindig kellően biztonságosak, amint arra Papp György is rávilágít.

„Nem szabad elfelejteni azt a nyilvánvaló tényt, hogy az átviteli közeg egy pontján a vezérlő jelek és a közlemény adatait képező jelsorozat egyaránt megtalálható. Az információs blokkba olyan vezérlő adat rejthető, amely a vezérlő egység belső működési paramétereinek módosítására, felfedésére, megsemmisítésére ad lehetőséget." [6]

A másik pillér, mint említettem az adatbefogás megnehezítését szolgáló megoldásokra támaszkodik. Nem alaptalanul, mert a vezeték nélküli adatátvitel esetén az elsődleges védelemet (front door), éppen ez látja el. Ezek a megoldások sem nyújtanak viszont kellő védelmet, mert korszerű eszközök egész sora teszi lehetővé azt,

hogy az adatok minden nehézség nélkül befoghatók eltárolhatók és analizálhatók legyenek, méghozzá veszteségmentesen. A valós idejű spektrumanalizátor bizonyos szolgáltatásai alkalmassá teszi arra, hogy ellásson ezek közül néhány fontos feladatot. Ennek részleteit a továbbiakban szeretném ismertetni.

Az elektronikai ipar nem csupán a távközlés fejlődéséhez járult hozzá, hanem az eredményei minden téren fellelhetők. Mindössze egy példát kiragadva, az elektronikai és alkatrészipar hatásosan hozzájárul a távközlés mellett a műszertechnika rohamos fejlődéséhez is. Az analizátorokon belül olyan műszercsalád fejlődött ki az utóbbi néhány évben, amelyekre sajátos jelfeldolgozási technikájuk miatt illik és használható a valamikor csak félve kiejtett „a valós idejű spektrumanalízis" kifejezése.

Valós idejű spektrumanalizátorok

A digitális rendszerek előretörésével egyidejűleg az analóg technika méltánytalanul háttérbe szorult. Ez különösen igaz a távközlés esetében. A digitális híradás széleskörű elterjedése és megszilárdult egyeduralmának nyomán a nagy komplexitású titkosított információ továbbítására alkalmas híradó rendszerek, és eszközök kikerültek a felhasználók kezébe. Mérésük és vizsgálatukra alkalmas mérőeszközök és műszerek viszont visszaszorulnak a speciálisan felszerelt elektronikai műhelyek falai közé. Néhány évtized után a méréstechnika újra specializálódott, illetve kialakult egy olyan ága, aminek kezelése kiemelkedően magas szaktudást igényel. Rendeltetésüket tekintve az analizátorok ma nem a klasszikus értelemben vett, és ismert szerviz tevékenységet szolgálják. A nagy integráltságú, csak nagyító és mikroszkóp alatt vizsgálható SMD alkatrészekkel teli áramkörök esetében a szervízelés, ha nem lehetetlen, akkor egészen biztos, hogy gazdaságtalan tevékenységgé vált. A fejlesztő műhelyeknek ma nagy szüksége van az analizátorokra. Viszont:

Nem csak az eszközfejlesztés és gyártásban nélkülözhetetlenek a spektrumanalizátorok, hanem hatásos fegyverré is válhatnak az információszerzésért folytatott küzdelemben.

Magas áruk miatt a logikai és spektrumanalizátorok korábban is csak a fejlesztők és speciális szakszervizek valamint intézmények számára voltak elérhetőek.

A korszerű digitális eszközök nagyfokú komplexitása mára oda vezetett, hogy egyfelől garancia arra, hogy az avatatlan felhasználó elől rejtve maradnak bizonyos részletek, hardver és szoftver szinten egyaránt. Vizsgálata megköveteli az olyan bonyolult mérési eljárások és eszközök használatát, mint az analizátorok. Kisugárzott jelek analízise ma elképzelhetetlen a spektrumanalizátorok nélkül A bonyolult modulációs eljárások ellenére, megfelelő eszköz birtokában mindig van lehetőség a jelek vizsgálatára, aminek következtében a felderítés „kezében" egy valós idejű spektrumanalizátor nagyon hasznos eszköznek bizonyulhat.

Hajlamosak vagyunk megfeledkezni arról, hogy a műszer és méréstechnika milyen mértékben járult hozzá egykor a felderítéshez. Mi több, érdemben ezzel nagyon ritkán foglalkozik a katonai műszaki szakirodalom. Hajlamosak vagyunk egyben elhinni azt is, hogy a digitalizálással sok minden megoldottnak tekinthető, és a „hatékony" biztonsági megoldások alkalmazásával a méréstechnika következmények nélkül kikerülhet az információs és elektronikai hadviselés látóköréből.

A méréstechnika ígéretes megoldásaival, új elven működő eszközeivel, nagyobb fenyegetést jelent az örökérvényűnek hitt biztonsági megoldásokra, mint hinnénk.

Továbbiakban egy kicsit más szemszögből szeretném megközelíteni az adatbiztonság kérdését. Szeretném bemutatni a méréstechnika csúcstechnológiájú készülék csoportját, a Tektronix cég által forgalmazott RSA valósidejű spektrumanalizátorok néhány típusát és szolgáltatásaikat.

A műszaki részletek ismertetése mellett igyekszem feltárni és érzékeltetni, hogy milyen lehetőségeket kínál, az eddig abszolút biztonságosnak vélt jelek befogására és veszteségmentes tárolására alkalmas analizátor. A valós idejű analízis nem egyenértékű a feldolgozással! Ez utóbbi még várat magára, de úgy vélem ez is csak idő kérdése, mint ahogy néhány évvel ezelőtt is csak nagyon óvatosan fogalmazódott meg a valós idejű analizátor megszületésének a gondolata:

„Mivel az egyszerű sebességfölény nem biztosítható, ezért új mérési módszerek kutatásával, a meglévők hatékonyságának javításával, a felderítési adatok fúziójával számítógépes kiértékeléssel érhető el, hogy a „ vadászok „ utolérjék a „nyulakat". Ebben segítenek a nagy sebességű, közel valós idejű Real Time felderítő, iránymérő berendezések, az új elvű jelanalizátorok és jelanalizálási módszerek, az intelligens, gyors válaszzavaró berendezések és az ellenség és a saját elektronikai helyzetet követni, tervezni képes térinformatikai alapú vezetési rendszer".[7]

A „közel valós idejű ..." berendezések helyett ma valós idejű spektrumanalizátor –RTSA, azaz Real Time Spectrum Analyzer –ról beszélhetünk.

A mai eszközök segítségével az egykor megálmodott sebességfölény is biztosítható és nagy előnyre tehet szert az, aki előbb felismeri ennek jelentőségét, célirányosan alkalmazza, esetleg tovább is fejleszti, többek között olyan eszközzé, amelyik alkalmas lehet az értékes tartalom valós idejű kiszűrésére.

A továbbiakban bemutatott valós idejű analizátorok esetében mindössze azokat a legfontosabb jellemzőket szeretném kiemelni és bemutatni, amelyek a korábban említett cél megvalósulásához vezethetnek.

RSA analizátorok

A címben szereplő rövidítés egy műszercsaládot jelöl. Ezen belül én mindössze három készülék jellemzőit ismertetem röviden. Ezek a következők; RSA-3300B, RSA-3408B és RSA-6100A valós idejű spektrumanalizátorok.

A spektrumanalizátorok feladata, hogy egy adott jeltartományban (spektrumban) jelenlevő különböző frekvenciájú és amplitúdójú jel-összetevőket (komponenseket) egy frekvencia- amplitúdó kétdimenziós koordináta rendszerben megjelenítse.

Ez úgy valósul meg, hogy a befogott jelen egy úgynevezett gyors Fourier transzformációt hajt végre, kiszűrve az egyes összetevőket. Azonban bármennyire is gyors ez a frekvenciatartománybeli vizsgálat, mindig csak egy összetevő kiértékelését képes egyidejűleg elvégezni, aminek következtében a nem vizsgált tartományba eső összetevők amplitúdójának megváltozását az analizátor nem érzékeli. Ha az időt, mint dimenziót nem vesszük figyelembe, akkor irreális és hamis eredmény születhet.

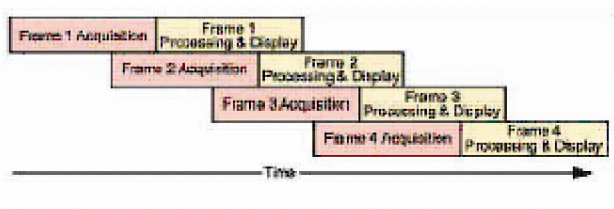
A szekvenciális, azaz sorrendi kiértékelés és megjelenítés következtében nem beszélhetünk valós idejű frekvenciatartománybeli analízisről, hiszen itt minden összetevőhöz eltérő időpillanat tartozik. Kiértékelése és rögzítése is eszerint történik. Reálisabb képet csak egy idő- frekvencia- amplitúdó, háromdimenziós megjelenítés adhat, ahol az egymás mögé helyezett időtengelyek mindegyikén csak egyetlen frekvencia-komponens van feltüntetve. Egy ilyen ábrázolás viszont nehezen kiértékelhető. Számunkra hasznos információt a frekvencia és a hozzá tartozó jel amplitúdója hordozza. Ilyen értelemben a többszörös időtényező nagyon zavaróan hathat. A háromdimenziós ábrázolás, mint módszer, nélkülözhetetlen a valós idejű spektrumanalízis esetében, de más összefüggésben lesz alkalmazva. Színskála szolgál a harmadik elképzelt „z" tengely menti jellemzők megjelenítésére, mint az 5, 6 és 8.ábrán látható a továbbiakban.

A mai híradó rendszerek bonyolult idő, frekvencia és kódtartománybeli modulációt alkalmaznak, aminek következtében a jel spektruma szét van terítve egy bizonyos frekvencia tartományban. Semmilyen olyan módszer nem alkalmas ezeknek a jeleknek a vizsgálatára, amely az egyes összetevőket eltérő időpillanatban képes „befogni" és feldolgozni, vagyis analizálni. Még a vektor jelanalizátorok (VSA- Vector Signal Analyzer) sem képesek a dinamikusan változó vizsgált jelek analízisére. A vektor analízis frekvencia és moduláció tartományban kellő információt ad azáltal, hogy pillanatfelvételt készítenek a vizsgált jelről, viszont időtartományban az eredmények nem kielégítőek.

1.ábra

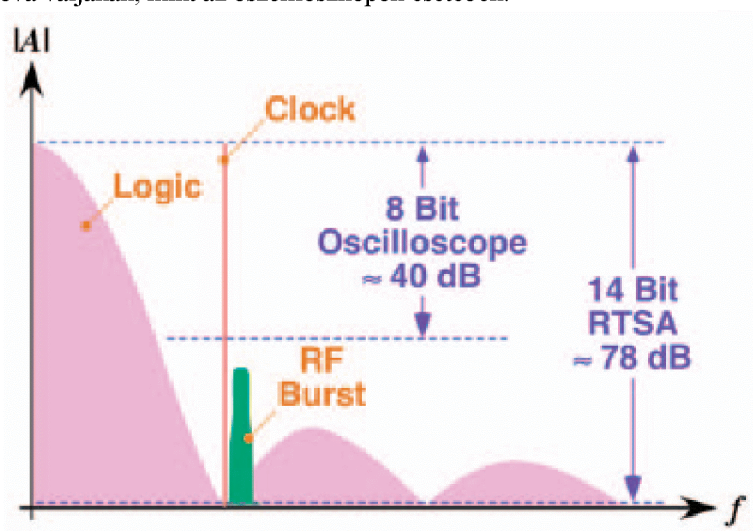
A Tektronix által kifejlesztett valós idejű spektrum analizátorok (RTSA- Real Time Spectrum Analyzer) (1. ábra) [11] a hagyományos analizátorokkal ellentétben nem a pásztázó technikát alkalmazza, hanem kellően gyors ahhoz, hogy pillanatfelvételt készítsen adott tartománybeli, bemenő jelből. Ezt keretekre bontva digitalizálja és gyors Fourier transzformációt (FFT) hajt végre rajta, majd eltárolja a további analízis céljából. Az egyes keretek befogása és feldolgozása olyan gyorsan történik, hogy átlapolódva „nincs kiesett idő", biztosítva a folyamatos jelbefogást és feldolgozást (2.ábra). Idötartománybeni vizsgálattal lehetővé teszi azt, hogy

akár az időtengelyen visszafelé haladva elemezzük a vizsgált tartományt. [5] Ez lehetővé teszi, hogy a valós idejű spektrumanalízissel megjeleníthető legyen minden olyan jel összetevő, ami adott időpillanatban előfordul a vizsgált tartományban. Az RTSA e „képessége" lehetővé teszi a frekvenciaugratásos rendszerek csatorna- frekvenciaváltásának a követését.



2. ábra

A pásztázó analizátorok teljesítménye a jelanalízis dinamizmusának van összefüggésben. Összehasonlítva a nagy sebességű digitális oszcilloszkópokkal az RSA 3408A [18] típusú analizátort a 3.ábrán látható, hogy egy 14 bites A/D átalakítóval rendelkező jelanalizátor hozzávetőleg 78dB „dinamika-tartománnyal" rendelkezik. Ez lehetővé teszi a felhasználó számára, hogy jóval kisebb amplitúdójú jelek is láthatóvá váljanak, mint az oszcilloszkópok esetében.

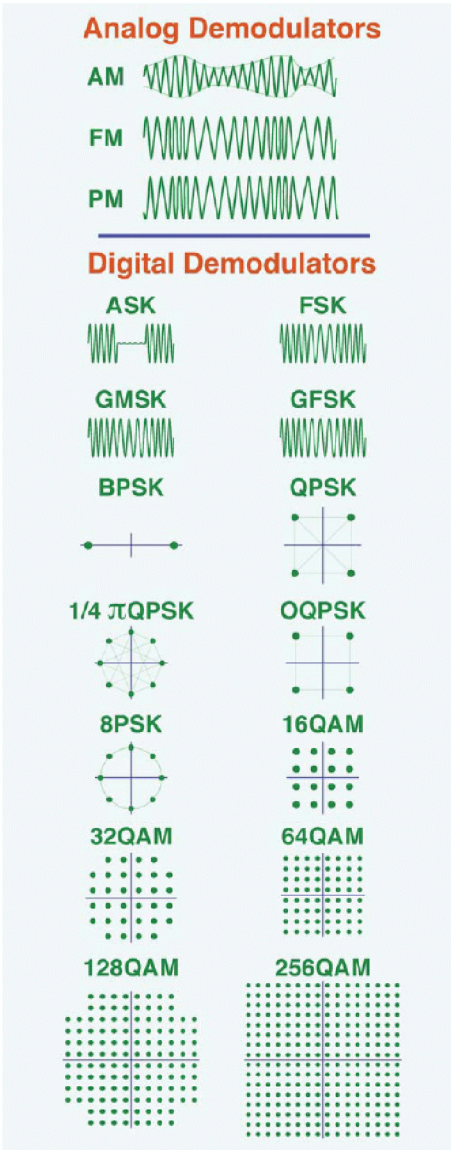


3. ábra

A mérés dinamikatartományának rendkívül nagy a jelentősége az interferenciák spektrális „lenyomatának" láthatóvá tételében és megértésében van. Az ábra egy méréstechnikai feladat- digitális áramkörök az órajelben előidézett interferenciájának- spektrum eloszlását mutatja be. [16)

Az interferenciavizsgálat módszereinek a felderítés szempontjából akkor van kiemelt jelentősége, amikor nagyon közeli és kis amplitúdójú jelek szétválasztása a

feladat. Ez mérési eljárás képezheti az információtartalom kiszűrésének az alapját a közeljövőben.



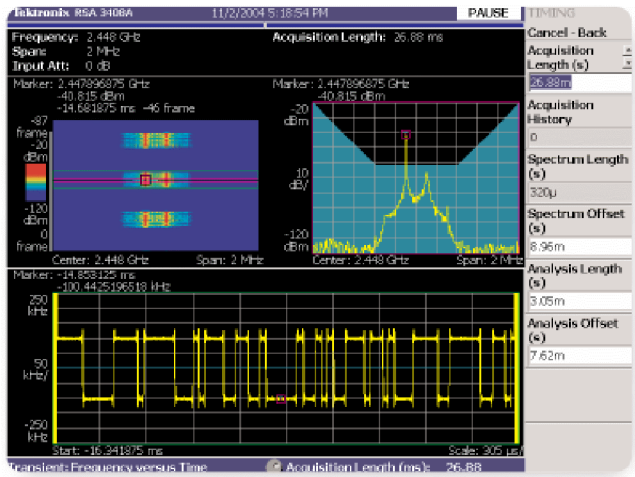
4. ábra

Az egyszerű folyamatos amplitúdó és frekvencia modulált jeleket alkalmazó vezeték nélküli kommunikációs berendezéseket mára felváltották a lényegesen kifinomultabb eljárások, úgymint az időben, frekvenciában és kódtartomány szerinti információ elosztás. A modulációs technológiák hova-tovább egyre bonyolultabb összefüggéseket tartalmaznak. A 4. ábrán láthatók mindazok a modulációs eljárások és formátumok, amelyek az RSA valós idejű spektrumanalizátorok szolgáltatásait oly mértékben kibővítik, hogy az lefedi a ma ismert összes modulációs módszereket és eljárásokat. [17] Ehhez tartozó szabványok a következők; Bluetooth, TETRA, P25, 802.15.4, RFID, ISO/IEC 1800, 14443, 18000-7,15693, stb.

Egyre gyakrabban alkalmazott az „intermitens", azaz szabálytalanul előforduló, több vivős vektor modulált digitális jelcsoport a híradó technikában. Minden ilyen megoldás lényege a jelanalízis megnehezítése, lehetőség szerint megakadályozása. Nem kifejezetten a szerviz tevékenység elleni „merényletről" van itt szó, hanem a továbbított adat biztonságát célzó intézkedésekről.

A korszerű modulációs formák, újszerű és különleges jelanalízis módszereket igényelnek. A vektor moduláció, szórt spektrumú és több vivős jelek vizsgálata alapvetően más szemléletmóddal közelíthető meg. Erre nem alkalmasak a hagyományosnak tekinthető vizsgálati eszközök és berendezések. Egyik oka, hogy a komplex jellemzők időtartománybeli egyidejű változása megnehezíti a jelfolyamban bekövetkező még nagyobb léptékű változások vizsgálatát. A korszerű mérési eljárások, más alapokra helyeződtek, az úgyne-

vezett tranziens analízis módszerét követik. Nem csak a zajszerű jelek vizsgálata igényli az új mérési eljárásokat, hanem minden aperiodikus jel. Az RF jelek analízisét a bennük előforduló intermitens4, aperiodikus jelek jelenléte nehezíti meg a leginkább.



5. ábra

A valós idejű analízis egyik rendkívül hasznos szolgáltatása a frekvencia tartománybeli maszkolt triggerelés, befogás, az „időkorrelált” több tartománybeli analízis és a komplex moduláció analízis. A frekvencia tartománybeli „trigger maszk” alkalmazására láthatunk példát a 5.ábrán. Az ábra jobb felső sarkában látható képrészlet halvány kék színnel jelölt területe a beállított maszkot jelöli.

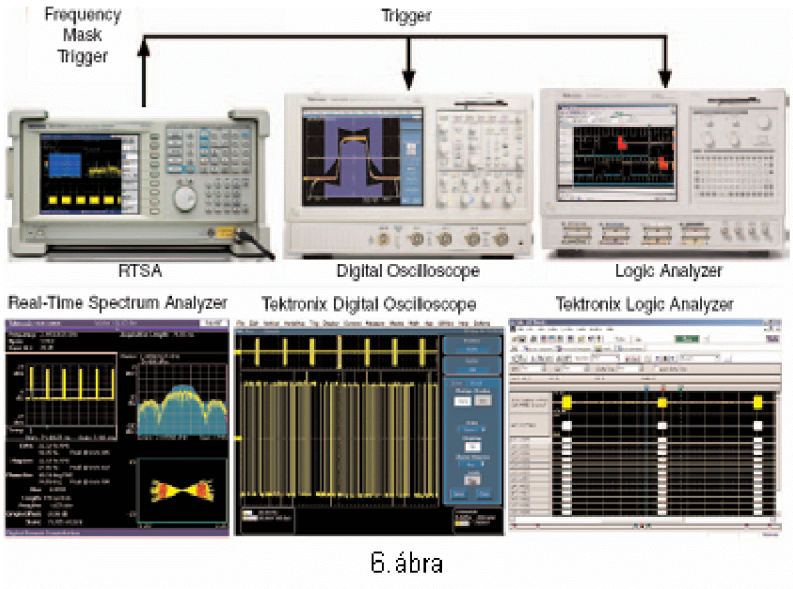
Ez alkalmassá teszi arra, hogy nagyon egyszerűen kiválasszon, és elkülönülten befogjon adott tartományban nagy valósszínűséggel előforduló bizonyos frekvenciájú jeleket vagy jelcsoportokat.

Az RTSA technológia egyedülálló módon biztosítja a tranziensek befogását, vagyis minden olyan összetevő vizsgálatát, ami nem szabályosan fordul elő a vizsgált spektrumban. Nagyon leegyszerűsítve lényegében ez a szolgáltatás biztosítja a frekvenciaugratásos és szórt spektrumú rendszerek által közvetített jelek befogását.

Az ábra alsó részén látható amint az FSK jelben előforduló tranziens detektálható és nyomon követhető. A valós idejű analízis nem csak a jel befogását teszi egyedülállóan egyszerűvé, hanem markerek elhelyezésével megállapítható, hogy ismétlődő „zavar” -jelekről van-e szó, egyszeri vagy szabálytalan időközönként (intermitens) fordul-e elő, stb. Ilyen szempontból az RTSA az egyedüli olyan mérőműszer, amelyik a vizsgált spektrumban előforduló tranziensekre is képes „triggerelni”.

Az 6. ábrán látható amint ez a trigger jel használható oszcilloszkóp vagy éppen logikai analizátor szinkronizálására a jel vizsgálata folyamán.

[4] Intermitent – szabálytalanul előforduló



6. ábra

A Tektronix az RTSA –t kifejezetten különféle modulációs eljárásokkal befolyásolt dinamikusan változó RF jelek és „burst”5 jellegű adatcsomagok vizsgálatára lett kifejlesztve.

Néhány fontosabb és figyelemre méltó jellemzője ennek a műszercsaládnak az 1. táblázatban látható. [11]

A valós idejű spektrumanalízis koncepciója azon a képességén alapul, hogy azonnal befogja a bemenetére adott jelet, elhelyezi a memóriájában és különféle tartománybeli analízist hajt végre rajta. Ez lehetővé teszi, hogy az időben változó RF jel minden jellemzője kielemezhetővé váljon.

A széles (több) tartománybeli moduláció analízis (Multi Domain Analysis) teszi lehetővé, hogy ismeretlen jelek is felderíthetők legyenek. Ehhez, a szakembernek rendelkezésére áll egy sor eszköz és szolgáltatás, aminek gyűjtő neve; „tools for signal analyzis”. A hardver jellegű kiegészítőktől eltekintve, ezek a következők;

teljesítmény- frekvencia, azaz spektrum analízis (spectrum),

spektrum- idő (spectrogram),

teljesítmény- idő, „szimbólum együttállás” „symbol constellations”(vector diagrams),

teljesítmény – kód „spreading code” (code domain power),

kód tartománybeli teljesítmény – idő (codogram).

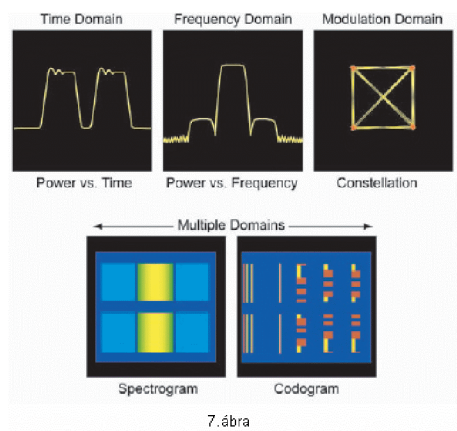
[5] burst- zaj

Specification or Feature	RSA3303/08B	RSA3408B	RSA6106/14A
Freq Range	DC to 3.0/8.0 GHz	DC to 8.0 GHz	9 kHz to 6.2/14.0 GHz
Max. Capture BW	15 MHz	36 MHz	40 MHz standard 110 MHz Option
Triggers, Standard	Level, Free Run, External	Level, Free Run, External	Level, Free Run, External(2), Line
Triggers, Optional	Frequency Mask, 15 MHz BW	Frequency Mask, 36 MHz BW	Frequency Mask, 40/110 MHz BW
Digital Phosphor (DPX) Spectrum Update Rate, Max Span and Min. Signal Duration	>48,000 Spectrums/sec, 15 MHz Max Span Min. Sig. Duration: 41 us	>48,000 Spectrums/sec, 36 MHz Max Span Min. Sig. Duration: 31 us	>48,000 Spectrums/sec, 40/110 MHz Max Span Min. Sig. Duration: 31/24 us
Memory	64 M/256 MB	64 M/256 MB	256 M/1 GB
Spurious-free Dynamic Range at Max. Capture BW	–70 dBc/15 MHz	–73 dBc/36 MHz	–73 dBc/110 MHz
DANL, 1 GHz	–150 dBm/Hz	–151 dBm/Hz	–149 dBm/Hz
ACLR (3GPP 1 DPCH)	66 dB	72 dB	79 dB
SSB Phase Noise at Specified Offsets at 1 GHz, dBc/Hz (Typical)	10 kHz: –108 1 MHz: –133 10 MHz: –136	10 kHz: –112 1 MHz: –135 10 MHz: –140	10 kHz: –110 1 MHz: –134 10 MHz: –142
Screen Size, User Interface	8.4 Inch Screen, Keyboard, Mouse, Front Panel	8.4 Inch Screen, Keyboard, Mouse, Front Panel	10.4 Inch Touch-Screen, Keyboard, Mouse, Front Panel
Interface Ports	GPIB, LAN, USB(2)	GPIB, LAN, USB(2)	GPIB, LAN, USB(4)
Storage Media	Internal HDD, FDD	Internal HDD, FDD Optional Removable HDD	Internal HDD, DVD ±RW Optional Removable HDD
IQ Inputs Option	20 MHz BW Differential Inputs	40 MHz BW Differential Inputs	Not Available
IF Outputs	Not Available	Standard, 421 MHz, 40 MHz BW	Option, 500 MHz, 120 MHz BW
Digital I and Q Output Option Bandwidth	Not Available	Up to 36 MHz BW	Up to 110 MHz BW, fully corrected amplitude and phase
Preamplifier	Option, External, 0.1 to 3 GHz 20 dB Gain nominal	Option, External, 0.1 to 3 GHz 20 dB Gain nominal	Option, Internal, 0.01 to 3 GHz 30 dB Gain nominal

1.táblázat

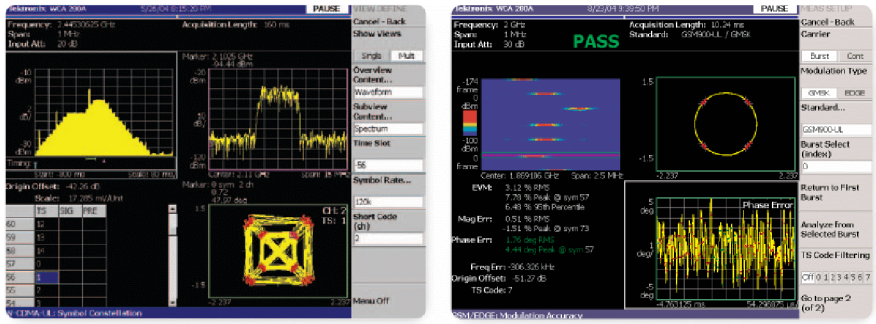
A lehetőségek sokasága az elemzést végző szakember munkáját segíti és egyben gyorsítja, azzal, hogy rendelkezésre áll mindig a célnak legmegfelelőbb vizsgálati módszer.

A 7. ábra néhány példát mutat az idő korrelált több tartománybeli analízisre. [10]



7.ábra

Ezt az analízist igénylik a cellarádiók a beállításuk folyamán. Különféle szabványok ellenőrzésére és vizsgálatára van lehetőség (GSM- EDGE, W-CDMA, HSDPA, cdma2000, 1xEV-DO és TD-SCDMA). Ezenkívül természetesen még számtalan példa akad, amikor az ábrán látható vizsgálati módszerek elengedhetetlenül szükségesek. Frekvenciaugratásos jel vizsgálata a 8.ábrán látható. Szemléletesen mutatja be egy ellenőrzés eredményét, amiben nagyvonalakban megtalálhatók mindazok a jellemzők, amelyek a jel előzetes vizsgálatához elegendőek.



8 ábra

A szokásos spektrumanalízissel szemben a Tektronix által kifejlesztett valós idejű spektrumanalizátor mérföldkőnek számít a méréstechnikában. „Digitális foszfor” DPX (Digital Phosphor Spectrum Analysis) elnevezéssel illetett eljárás szokatlanul hangzik. A foszfor jelen esetben egy kijelző technológiára utal, ami egy szabadalmaztatott és egyedülálló kijelző technológia. A szabadalmaztatott képmegjelenítési eljárás egy képtárolási metódust takar, aminek különlegessége abban rejlik, hogy a kép tárolási ideje szabályozható. Lehetővé teszi, hogy dinamikusan változó RF jelek megjeleníthetők legyenek a kisebb gyakoriságú és rövid időtartamú jelek mintájára. Nagy utóvilágítású foszfor kijelzők a korábbi mérőműszerekben is előfordultak, főként az analóg képtároló oszcilloszkópokban és a radarképernyők esetében. Az eltérés a korábbi kijelzőkhöz képest abban nyilvánul meg, hogy míg korábban az utóvilágítás a pásztázó elektronsugár „futásának” a gyakoriságától függött, addig a DPX technológia képes emulálni a változtatható időtartamú képtárolási folyamatot.

Az analizátor rendkívüli teljesítménye egyrészt a nagy utóvilágítású katódsugárcső emulációjának, másrészt a nagyságrendekkel nagyobb frekvencia átalakítási képességének tulajdonítható. A DPX feldolgozó egység statisztikai eljárások és függvények egész sorával biztosítja, hogy látható legyen a jelek teljes időbeni viselkedése. Nem csak periodikus, hanem véletlenszerűen előforduló és eltérő amplitúdójú, rövid és kis gyakorisággal előforduló jelek is láthatóvá tehetők.

A szabályozható utóvilágítás biztosítja a felhasználónak, hogy a képmegjelenítést a vizsgált jel jellemzőihez és tulajdonságaihoz igazítsa. Mindemellett a változó feltételekhez tudja igazítani nem csak a periodikus és dinamikusan változó RF jeleket, hanem az egyedi módon előforduló tranziens jelek megjelenítését is. Ennek köszönhetően olyan jelkomponensek megjelenítése is lehetséges, amelyek nem voltak kimutathatók a hagyományos spektrum analizátorokkal vagy vektor analizátorokkal. Egyedülálló képessége, hogy képes a vizsgált jel különböző jellemzőire triggerelni, befogja, eltárolja és utólag elemzi idő, frekvencia vagy modulációs tartományban.

A következő RF jeltovábbítás metódusok esetén is hatékonyan biztosítja a jelek vizsgálatát:

olyan kapcsolatok, amelyek csak nagyon rövid ideig aktívak és csak egységnyi adatok közvetítésének idejére lépnek működésbe, szabaddá téve a csatornát más

források számára. A legtöbb esetben az ilyen kapcsolatok időzítése véletlenszerű és ismeretlen,

olyan rendszerek, amelyek egy ugyanazon spektrumot időben m,egosztanak, mint például az ultra keskeny sávú (UWB- Ultra Wide Band) és kódosztásos (CDMA- Code Division Multiple Acces) technikák,

„intelligens", alkalmazkodó képességgel felruházott rádiórendszerek (CR – Cognitive Radios), amelyek a frekvenciájukat, modulációt és a teljesítményüket a környezethez képesek igazítani, [15]

Mindannyiszor nélkülözhetetlen a valós idejű spektrumanalizátor, amikor nagy sebességű adatkapcsolatok rezidens, 10-12 nagyságrendű bithibáit, vagy adatcsomag ütközéseket kell felderíteni és elkerülhetetlen a tranziens RF jelek analízisét lehetővé tevő berendezés használata.

Összegzés

Az információs hadviselés által célként megjelölt adat és információ megszerzésének vagy megsemmisítésének alternatív lehetősége a legtöbbször fennáll, és döntő módon befolyásolja a fegyveres összecsapás kimenetelét. Az információ értéke olykor felbecsülhetetlen, megszerzéséért folyó verseny kimenetelét többnyire a technikai fölény határozza meg.

A cikkem szűk keretein belül igyekeztem érintőlegesen bemutatni a „valós idejű spektrumanalizátor (RTSA- Real Time Spectrum Analyser) néhány szolgáltatását.

Szolgáltatásai olyan elemeket tartalmaznak, amelyek által potenciális fegyverré válhat a közeljövőben az információ megszerzéséért folytatott küzdelemben. Ehhez nem kell mást tenni, mint felismerni és kihasználni, és olyan irányban továbbfejleszteni, vagy kiegészíteni mindazon eszközökkel, amelyek további adatfeldolgozás által képesek kiszűrni a továbbított és titkosított jelből a hasznos információt.

Köszönetnyilvánítás

Ezúton szeretném megköszönni Földváry József ügyvezető igazgató úrnak (Foldertrade Kft.), hogy segített a cikk megírásához szükséges forrásanyag összegyűjtésében.

FELHASZNÁLT IRODALOM

[1] Dr. Várhegyi István- Dr. Makkay Imre- Dr. Ványa László: A felderítés korszerű eszköze, a minden adatforrást elemző rendszer (ASAS), Nemzetvédelmi Egyetemi Közlemények, 2. Évfolyam 2-3. Szám. 2. Kötet. A ZMNE tudományos lapja, 1998.

[2] Dr. Sándor Miklós- Rajnai Zoltán: Út a digitális kommunikációs rendszer felé? Nemzetvédelmi Egyetemi Közlemények, 1. Évfolyam 2. Szám. A ZMNE tudományos lapja, 1997.

[3] Dr. Haig Zsolt: Az információs hadviselés, vezetési hadviselés, mint a XXI. század új hadviselés formája, Nemzetvédelmi Egyetemi Közlemények, 2. Évfolyam 2-3. Szám. 2. Kötet. A ZMNE tudományos lapja, 1998.

[4] Földváry Botond: Valósidejű spektrumanalízis, www.foldertrade.hu (2008. június 26.)
[5] Simon Singht: Kódkönyv, Park Könyvkiadó, 2002
[6] Kassai Károly:A korszerű híradó és informatikai rendszer védelmi szempontú vizsgálatának egyes kérdései. Nemzetvédelmi Egyetemi Közlemények 2002. 6. évf. 2. szám, 163-171 pp.
[7] Dr. Makkay Imre: Az elektronika, távközlés és az elektronikai hadviselés a XXI. században. Nemzetvédelmi Egyetemi Közlemények, 1 Évfolyam 2. Szám. .A ZMNE tudományos lapja, 1997.
[8] Gorza Jenő: Az informatikai fejlesztési stratégia megvalósításának szervezeti keretei, Nemzetvédelmi Egyetemi Közlemények, 6. Évfolyam 2. Szám. .A ZMNE tudományos lapja, 2002.
[9] Modulation Analysis for Transient RF Signals, Tektronics- Technical Brief, (12p)
[10] RSA 3300B Series Real Time Spectrum Analizer , Tektronics – Technical Brief, (8p)
[11] RSA 6100A Series 6,2 GHz and 14 GHz Real Time Spectrum Analysers, Tektronics- Technical Brief, (15p)
[12] Quickly Identtify Intermitent and Interfering Signals with Real-Time Spectrum Analysis, Tektronics- Technical Brief, (7p)
[13] Fundamentals of Digital Phosphor Technology is Real -Time Spectrum Analyzers, Tektronics- Technical Brief, (14p)
[14] DPX Turns a Light On aDark Room, Tektronics- Technical Brief, (7p)
[15] Real-Time Spectrum Analysis for WLAN and Combo Devices, Tektronics-Technical Brief, (20p)
[16] Flexibile Modulation Analysis with the Real- Time Spectrum Analyser, Tektronics- Technical Brief, (19p)
[17] RSA 3408B Real-Time Spectrum Analyser, Tektronics-Technical Brief, (7p)

KERTI András – PÁNDI Erik:[6]

AZ INFORMÁCIÓTECHNOLÓGIAI ÁGAZAT SAJÁTOSSÁGAI

Absztrakt: A jelenlegi Rendőrség gazdasági szakszolgálat IT ágazat a Magyar Köztársaság Rendőrsége és a Magyar Köztársaság Határőrsége szakállományának összevonása révén jött létre folyó év január 1-jével. Az eddigi működési tapasztalatok az idő rövidsége miatt még nem engedik meg közép- és hosszútávú következtetések levonását, azonban a korábbi nyilvánvaló működési problémák, illetőleg a jelenlegi szervezeti struktúra kialakításának gyakorlata felvet néhány olyan kérdést, amelyek átgondolás nélkül történő elvetése – megítélésünk szerint – nem segítheti elő a homogén, „egy nyelven beszélő", stabil szakmai alapokon álló IT ágazat tényleges kialakítását. Jelen publikációban áttekintjük a Rendőrség szakterületének és szakállományának jelenlegi helyzetét, sajátosságait.

Kulcsszavak: Határőrség, információtechnológia, Rendőrség.

1. A Rendőrség egykori IT ágazata

Az IT ágazat egykori felépítése elveinek tisztázására néhány korábbi szakmai anyag összességében korrekt felvilágosítást adhat [1], [2]. Az integráció során bekövetkezett szervezeti változásokig a rendőrségi IT ágazat elvi felépítése többékevésbé a hetvenes évekre kialakult szervezeti struktúrát (szervezési koncepciót) őrizte meg. Ennek lényege a központosított szakirányítás, amely egyrészt a központi, valamint a területi és helyi rendőri szervek kommunikációs igényeit kiszolgáló szervezeti egységek tekintetében valósult meg. Az 1990-es éveket megelőzően a szakirányító szerv a Belügyminisztérium egyik osztálya[7] volt, amelynek funkcióját a későbbiekben az ORFK-n megalakuló osztály, majd főosztály[8] látta el. A központi szervek kiszolgálását kezdetekben a szakirányító szerv végezte, majd a kilencvenes évek első harmadától a korábbi szakirányító szervből alakult üzemviteli szervezet[9] látta el. A területi és helyi rendőri szervek ellátását a megyei (fővárosi) rendőr-főkapitányságokon, valamint a különleges rendőri szerveknél[10] létre-

[6] Szerzők: Kerti András, adjunktus, ZMNE BJKMK Híradó Tanszék, PhD-hallgató, ZMNE KLHK Hadtudományi Doktori Iskola, Dr. Pándi Erik, egyetemi docens, ZMNE BJKMK Híradó Tanszék

[7] BM Anyagi-Pénzügyi-Technikai Főcsoportfőnökség Híradástechnikai Osztály

[8] néhány megnevezés: ORFK Híradástechnikai Iroda, ORFK GIF Anyagi-Technikai és Informatikai Főosztály, ORFK GF Információtechnológiai és Műszaki Főosztály, stb.

[9] ORFK GIF Híradástechnikai Szolgálat, illetőleg ORFK GF Híradástechnikai Szolgálat

[10] például: Köztársasági Őrezred, Készenléti Rendőrség, stb.

hozott szervezeti egységek[11] végezték. A központi szervek ellátási gyakorlatában – *lényegében* – 2003-tól újabb változások mentek végbe, amikor a Rendőrség legnagyobb üzemviteli szervezete a felügyeletet ellátó minisztérium háttérintézményeként működött, majd az integrációt megelőző egy évvel közigazgatási szervvé került átalakításra.[12] A szervezeti változások ellenére elmondható, hogy a legfőbb irányítási alapelvek több mint három évtizeden keresztül nem változtak, vélhetően többé-kevésbé sikeresen töltötték be funkcióikat, amelynek lényegét egy szakértő a következőképpen fogalmazza meg: [az] *„…irányítás célját legáltalánosabban a […] jogszerű működésnek átfogó és teljes körű biztosítása, továbbá a működéshez szükséges feltételekről való gondoskodás adja. Az irányítás lényege tehát az […] akaratérvényesítés a […] működés fölött."* [3].

A megfogalmazottakkal ellentétben, az IT ágazat tekintetében, a kilencvenes évektől kezdődően az akaratérvényesítés – *a korábbiakban megszokott gyakorlattól eltérően* – meggyengült, aminek egyenes következménye egy olyan – *napjainkra is jellemző* – vákuum, amelyre jellemző a teljes szabályozatlanság,[13] valamint az anyagi-pénzügyi erőforrások szükségesnél nagyobb mértékű dekoncentráltsága.[14] E két fő probléma lényegében az ágazat átlátható és a tervszerűségen alapuló célszerű működését teszi nehézkessé. A kialakult – *és napjainkra akuttá vált* – helyzet ok-okozati összefüggéseinek feltárása komplex és mélyreható vizsgálatokat igényelne, amelyre jelen tanulmány keretei nem adnak lehetőséget, azonban néhány, a felszín közvetlen közelében rejtőzködő – *a felkészítéssel, a rendfokozati és beosztási rendszerrel is összefüggő* – problémára ezúton szeretnénk röviden rávilágítani. Elöljáróként le kell szögezni, hogy a kialakult problémák egy része nem vezethető vissza a személyi és vezetői állomány szakmai tevékenységére, azok tőlük független okok miatt alakultak ki és mélyültek el.

A kilencvenes évektől kezdődően hazánkban is megjelentek a korszerű távközlési és informatikai technológiák, illetőleg szolgáltatásaik, amelyek az idő előrehaladtával egyre inkább beépültek a rendőri tevékenységekbe oly módon, hogy azok eredményes végrehajtása napjainkban már elképzelhetetlen nélkülük, amely tényt a szakirodalom is megfelelően alátámaszt [4]. A korszerű eszközök és szolgáltatások térhódítása, a technológiai konvergencia ténye a globális gazdasági és társadalmi térség kialakulásával egyértelművé vált, e folyamatot az ezredfordulótól – *mint az előzőekben azt már láthattuk* – a magyar kormányzat sajátos jogi-szervezeti és anyagi-pénzügyi megoldásokkal erőteljesen támogatja. A szakmai vezetés e kihívásra szervezetileg jól reagált, hiszen a hagyományos *„híradó"* kultúrára építkezve megalakította a *„híradó és informatikai"* szervezeti elemeket,

[11] a kilencvenes éveket megelőzően a főkapitány alárendeltségében működő alosztályokként, majd az elmúlt évtizedekben a gazdasági igazgató alárendeltségében működő osztályokként

[12] 2002. december 1-jén a BM Távközlési Főosztály és az ORFK GF Híradástechnikai Szolgálat bázisán, kettős (belügyi ágazati szakirányító és központi üzemeltető) funkcióval megalakult a BM Távközlési Szolgálat (BM TÁSz). A BM TÁSz a 276/2006. (XII.23.) Korm. rendelet révén, 2007. január 1-jén szűnt meg. Jogutódja a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala

[13] a jogszerű működés átfogó és teljeskörű biztosítása

[14] a működéshez szükséges feltételekről való gondoskodás

amelynek keretében megindult a helyi szervekhez történő szakállomány kihelyezése is. Ugyanakkor, egyfajta elhibázott lépésként értékelhető, hogy a szakmai szervezetek belső tartalmának súlypontjaival kapcsolatos gyorsütemű átszervezések szükségességét viszonylag későn ismerte fel, szinte csak akkor, amikor a technológiai konvergencia beteljesedése már nyilvánvaló ténnyé vált. Ennek egyik oka talán az is lehet, hogy a változások időszaka során túlsúlyban voltak az átalakítások önálló kezdeményezéséért és végrehajtásáért felelős azon személyek, akiknek szakmai gyökerei, valamint szakmai szocializálódásuk környezete egyértelműen a hagyományos távközlésben voltak megtalálhatók. A Rendőrség jelenleg is tapasztalható, hosszú évtizedekre visszanyúló sajátja, hogy a funkcionális tevékenységek ellátására tervszerű, egységes közép- és felsőfokú szak-, illetve felsőoktatási képzést nem szervez, utánpótlását a szervezetek önállóan, a fellépő lokális igényekhez és az adott időszakban, adott területen fennálló belső és külső körülményekhez igazítva hajtják végre. A helyzet a szakterületi tovább- és átképzések, illetőleg felsőoktatási beiskolázások terén is hasonló. Úgy tűnik, a Rendőrség hosszú évtizedek óta kimondatlan szabálynak tekinti azon eljárást, amely szerint a szakma kívánalmainak megfelelő iskolarendszerű képzés révén szakképzettséget szerzett szakállománynak a szakterületi jártasságot, majd készséget mindenekelőtt a beosztási helyen kell tudnia megszerezni. Ténykérdés azonban az, hogy az IT területe tekintetében, a gyakori technológiaváltás a tudásszint igen gyors elévüléséhez vezet, tehát ezen hallgatólagos gyakorlat fenntartása az ágazat eredményes működése szempontjából nem lehet előremutató.

Visszatérve korábbi fejtegetésünkhöz, mindenképpen elgondolkodtató, hogy a kilencvenes évek előtt minőségét és szervezettségét tekintve magasabb színvonalon álló „híradó szolgálat" utódja, a szervezetileg megújuló „híradó és informatikai szolgálat", vagyis az IT ágazat jelenünkben is működési problémákkal küszködik. Fentiek révén úgy gondoljuk, hogy a közel két évtizede tapasztalható hullámzó, de ugyanakkor a korábbiakhoz mérten nagyarányúnak tekinthető – *és talán folyamatosnak tekinthető* – fluktuáció a többségében hagyományos elveken és eljárásokon nevelkedett vezetői állományt arra sarkalta, hogy a hiányzó, a megváltozó szakmai környezetbe eredményesen beilleszkedő humán erőforrásokat elsősorban a szervezeten kívülről pótolja. Ez a lépés egyúttal egyre sürgetőbb feladattá vált, hiszen az IT ágazat belső, időben történő, mélyebb strukturális átalakítása korábban elmaradt, vagy vontatottan haladt, azonban a rendőrszakmai és ezeken keresztül egyes közigazgatási feladatok korszerű informatikai és kommunikációs szolgáltatásokkal való támogatása tekintetében a rendőri felsővezetés egyre nyomasztóbb követelményeket támasztott az ágazati vezetőkkel szemben. A humán erőforrások pótlására több lehetőség adódott, egyrészt a társszervek állományából,[15] másrészt a polgári társadalomból, azonban mindenképpen elmondható, hogy e létszámkonjunktúra révén a korábban egységes elvek mentén szocializálódott „híradó szolgálat" – *a fogalom jó- és rossz értelmében egyaránt* – felhígult. Ennek egyik pozitív jele, hogy sok olyan új gondolat, gyakorlati tapasztalat és eljárás került a rendszerbe, amelyet alkotó módon lehetett felhasználni a mindennapi munkában, ugyanakkor

[15] itt lehetőség nyílt a Magyar Honvédség, valamint a Határőrség állományából történő átvételre egyaránt

negatívumként értékelhető, hogy a hagyományos és a szervezet egészének működése szempontjából is bevált gyakorlatok elsajátítására és átörökítésére sem elegendő idő, sem megfelelő kvalitású mentorállomány – *az idő haladtával* – már nem állt rendelkezésre.

Mindenképpen szükséges néhány szót ejteni a szervezeten kívülről érkezett szakemberállományról és motivációiról, mivel e kérdéskör felveti az állománytáblával kapcsolatosan kialakult problémákat is. Köztudomásúak azon tények, amelyek egyrészről alátámasztják, hogy a polgári IT ágazat tekintetében napjainkban is inkább a munkaerő-kereslet a jellemző, másodrészről bizonyítják a vidéki és ezen belül a keleti megyék magas munkanélküliségi rátáit, harmadrészről nyilvánvalóvá teszik ezen ágazatban elérhető rendőri és polgári illetmények különbségét. Ezekből kiindulva elmondható, hogy a polgári életből érkezők Rendőrséggel szembeni elkötelezettsége és szakmai kvalitása – *vélhetően* – alacsonyabb, mint azon társaiknak, akiket a hazai, illetőleg nemzetközi üzleti szféra természetes úton „választott" ki. Számunkra ezen állománycsoportba sorolható munkavállalók jelentik azt a kategóriát, amelyek tudatos „szocializáció" nélkül – *még ha hivatásos állományba is kerülnek* – soha nem fognak azonosulni[16] sem az IT ágazattal, sem magával a szervezettel, amelynek egyik hosszútávú következménye lehet a szakmai diszkvalifikálódás. Ezzel ellentétben, a társszervektől érkező – *elsősorban hivatásos állományú* – munkavállalók szervezettel kapcsolatos – *karrierközpontú* – motiváltsága mindig is jóval magasabb volt, így esetükben, korábbi pályafutásuk révén mesterséges „szocializációs" folyamatra általában nincs szükség. E kategóriába tartozó munkavállalók szempontjából, sok esetben a karrierközpontúság jóval meghatározóbb, mint a szakmai motivációs tényezők, ami tudatos beavatkozás nélkül szintén egyfajta szakmai diszkvalifikálódáshoz vezethet akár anélkül, hogy az egyén ezt érzékelhetné.

Az egykori „híradó szolgálatra" is jellemző volt, hogy állománytábla szempontjából vegyes szervezeteket[17] hoztak létre, amelynek egyik fő szempontja volt, hogy a munkakörök egy elég széles rétegében a magasabb szintű kötődés[18] útján a szervezettel szembeni elkötelezettséget és ezzel a végrehajtás minőségét növeljék az érintett állományban. Általánosságban elmondható, hogy a kilencvenes éveket megelőzően az ágazatban az állománytáblák kialakítására az egységesség volt jellemző. Megítélésünk szerint, az integrációt megelőzően a Rendőrség IT ágazatában alkalmazott állománytábla az ágazat feladatával, tevékenységével, szervezetével, állományával és hatáskörével kapcsolatos részletes szabályozás hiánya miatt a múlt szokásjogára támaszkodva, a személyzeti hatáskört gyakorló illetékes vezető belátása és meggyőzése, valamint a rendelkezésre álló bérkeret, mint kényszer által kialakított helyzetet tükrözte vissza. A kialakult gyakorlat tehát a vonatkozó jogszabály, a fegyveres szervek hivatásos állományú tagjainak szolgálati viszonyá-

[16] megítélésünk szerint az azonosulás nem más, mint megismerni és elfogadni a szervezet erősségeit és gyengeségeit, az általa nyújtott előnyöket és okozott hátrányokat, megtanulni ezekkel pozitív módon együttélni és ennek tudatában együttműködni az egyént körbevevő szűk közösséggel a szervezet pozitív irányú fejlődése érdekében

[17] alapvetően: főtiszt, tiszt, zászlós, tiszthelyettes és kinevezett polgári alkalmazott

[18] és ezzel szélesebb kedvezmények, valamint magasabb illetmények

ról szóló 1996. évi XLIII. törvény preambulumában foglaltakkal sem volt összhangban, hiszen lényegében nem volt tisztázott, hogy az IT ágazat mely tagjával kapcsolatosan várt *„az állam tántoríthatatlan hűséget, bátor helytállást […] a törvények és más jogszabályok, valamint a nemzetközi jog előírásainak megfelelően, a fegyveres szervek feladataihoz igazodó szakmai ismeretek birtokában…”* [5]. Ez különösen akkor lehetett gond, amikor – *hosszú évekre visszavezethetően, a gyakorlatban is bizonyítható módon* – két ugyanolyan felelősséggel és kötelezettséggel bíró munkakört két különböző besorolással, de azonos szakmai végzettséggel rendelkező munkavállaló látott el. A legszembetűnőbb kontrasztok vidéken alakulhattak ki, ahol példaként véve két különböző rendőrkapitányság állományában dolgozó rendszergazdát, az egyik már elvégzett egy főiskolát, így a megyei- és országos rendőrfőkapitány támogatásával a miniszter kinevezte tisztté, amíg a másik ugyanazon főiskola egy évvel fiatalabb hallgatójaként csak középfokú végzettsége szerinti közalkalmazotti besorolásban (és bérrel) látta el hasonló típusú és felelősségi körű feladatát.

A kilencvenes évek közepétől további nehézségeket jelentett a tiszthelyettesi állomány megszervezése, mivel az állományba való felvétel alapkövetelménye az egységes rendészeti tiszthelyettes-képzés rendszerében való szakképzettség megszerzése lett, amelyet az állományilletékes vezetők többnyire nem támogattak. A tiszthelyettesi beosztásokat többnyire a már rendészeti képesítést szerzett állomány átképzése révén töltötték fel, de összességében elmondható, hogy a problémakör kezelése a gordiuszi csomó mintája alapján történt, vagyis a státuszok általában átminősítésre[19] kerültek. A tiszti állományba való felvétel különleges problémákat nem vetett fel, hiszen mind a társszervektől áthelyezéssel érkezők, mind a megfelelő főiskolai-, vagy egyetemi végzettséggel rendelkező, alkalmasság szempontjából megfelelő[20] köztisztviselők és közalkalmazottak az előírt szaktanfolyam elvégzését követően „képzett” rendőrtiszteknek minősültek. A hivatásos, köztisztviselői és közalkalmazotti státuszok kapcsán fennálló ellentmondások mellett sok esetben nem lehetett egységesnek tekinteni a középfokú és felsőfokú, valamint főiskolai és egyetemi végzettséghez kötött státuszok kialakításának gyakorlatát sem, amely egyes esetekben a fentiekben ismertetett problémákat vetette fel.

Mindezeket összefogva úgy ítéljük meg, hogy a Rendőrség IT ágazata az integrációt megelőzően, személyi állományának jogviszonyát, azok felkészültségét és végzettségét, valamint korábbi szakmai pályafutását illetően heterogénnek, a korfa a dinamizmus kívánalmai szempontjából kedvezőnek tekinthető. Az állományt pozitív értelemben vett kozmopolitizmus, vagyis retrográd korlátok nélküli szakmai sokszínűség jellemzi. Az ágazat hátránya, hogy az elődök által felhalmozódott szakmai tapasztalat, ismeretanyag – *különböző okok miatt* – gyengén örökítődött át, ezért a szervezet által korábban már érdemben hasznosított és bevált gyakorlati eljárások újbóli alkalmazása nehézkesen, továbbfejlesztésük szinte alig realizálódik. Ennek okán az ágazat tevékenysége kevéssé tekinthető átláthatónak, koordináltnak és tervezhetőnek, vagyis amely probléma leginkább a szabályozás és az ehhez szervesen kapcsolódó szakirányítás kérdésköreiben jelentkezik.

[19] többnyire közalkalmazotti státuszra
[20] fizikálisan és mentálisan egyaránt

2. A Határőrség egykori IT ágazata

Az egykori IT ágazat szemléltetésre néhány egykori szakmai anyag összességében megfelelő szintű felvilágosítást adhat [6], [7]. A Magyar Köztársaság Alkotmányáról szóló 1949. évi XX. törvény módosításai révén visszavezetve, a Határőrség státuszában 2005. január 1-jén következett be – *a korábbiakhoz képest* – az első jelentősebb változás, amikor is megszűnt a fegyveres erőkben[21] betöltött státusza. Ettől kezdődően a szervezet alapvető feladata az államhatár őrzése és rendjének fenntartása lett [8]. Az integrációig fennmaradt három esztendőben a szervezet – *a Rendőrséghez hasonlóan* – hármas tagozódásban[22] működött. Az IT ágazat szervezetének átalakítására jóval korábban, már a kilencvenes évek közepén megtörtént, amikor a hagyományos „híradó szolgálat" „informatikai szolgálattá" való szervezése ténylegesen végrehajtásra került. Az IT szakirányítás problematikája és érdemi megvalósítása a Határőrség tekintetében különösebb kérdéseket nem vetett fel, hiszen a teljes szervezet korábbi múltja[23] inkább volt militáns és így erőteljesen centralizált, mintsem kissé liberálisabb, közigazgatási vénájú. A szakállomány a három vezetési szint mindegyikén jelen volt.[24] Hasonlatosan a rendőri szervekhez, az IT állomány feletti munkáltató illetékesség gyakorlásában az ágazati vezetők nem vettek részt. A kilencvenes éveket követően az IT ágazat szabályozottsága – *ellentétben a Rendőrséggel* – továbbra is kimunkáltnak és begyakoroltnak volt tekinthető, amellyel párhuzamosan az anyagi-pénzügyi erőforrások alsóbb fokú szerveknél történő dekoncentrálása kisebb mértékben történt meg. Ezek alapján úgy ítéljük meg, hogy a Határőrség IT ágazatának működése a szabályozottabb és kiegyensúlyozottabb jelzővel illethető, amely természetesen elgondolkodtató kijelentés is egyúttal. Tekintettel arra, hogy mind a Rendőrség, mind a Határőrség alapfeladata a legmagasabb szintű törvénytől kezdve – *a jog hierarchiáján keresztül* – a legalsóbb fokú normákig szabályozott volt, ezért a szakszolgálatok tevékenységei között tapasztalható minőségi különbségek véleményünk szerint egyértelműen a személyi állomány felkészültségében és tevékenységének minőségében keresendők.

A Határőrség korábbi „híradó szolgálata" és „informatikai szolgálata" személyi állományának összetételét vizsgálva megállapíthatjuk, hogy a kilencvenes éveket megelőző időszakokban, a szervezet különleges helyzete miatt az arányok inkább voltak hasonlatosak a hadseregben alkalmazott megoldásokhoz, vagyis döntően hivatásos tiszti és tiszthelyettesi státuszok kerültek kialakításra, amelyek mellett, viszonylag szűk keretben – *többségében a kisegítő tevékenységek*[25] *körében* –

[21] fegyveres erők: a Magyar Honvédség és a Magyar Köztársaság Határőrsége

[22] központi, területi és helyi szervek összessége. Az integráció során lényegében csak a helyi szervek, vagyis a határrendészeti kirendeltségek maradtak fenn változatlan szervezetben. E szervek Rendőrségbe való konkrét betagozására a Rendőrség szerveiről és a Rendőrség szerveinek feladat- és hatásköréről szóló 329/2007. (XII.13.) Korm. rendelet alapján történt

[23] lényegében: 1947-től

[24] központi szinten: Informatikai Főosztály, területi (igazgatósági) szinten: Informatikai Osztály, helyi szinten: kirendeltségvezető-helyettes, vagy referens

[25] ennek keretében jellemzően anyagi-technikai-pénzügyi segédtevékenységekről van szó

megtalálhatók voltak a polgári státuszok is. A személyi állomány utánpótlása a tiszti állomány körében nem jelentett problémát, mivel azokat a katonai felsőoktatás rendszere – *az előre tervezett létszám szerint* – rendelkezésre bocsátotta [9]. A tiszthelyettesi állomány utánpótlása jellemzően a sorállományból történt. Az „informatikai szolgálattá" történő átszervezés időszakában a Határőrségnél már megindultak azon folyamatok, amely a rendészeti szervvé történő átalakuláshoz vezettek. Ennek keretében a sorállományú határőrök létszáma folyamatosan csökkent, majd megszűnt, így a testület gerincét egyre inkább alkotó tiszthelyettesi állomány szerepe felértékelődött. A belügyi ágazatban egységesülő tiszthelyettes szakképzés[26] révén a kilencvenes évek második felétől ezen állománykategóriába már csak a rendészeti szakközépiskolák elvégzését követően lehetett kerülni. A rendészeti szakközépiskolákban a szervezetek alaptevékenységi körén túlmutató feladatokra, vagyis szakszolgálati feladatokra szakképzés nem folyt és nem folyik, vagyis az „informatikai szolgálat" ezirányú szükségleteit e forrásból megoldani nem volt képes. A probléma megoldását jelentette egyrészt az erre alkalmas, képesített (kiképzett) határőr tiszthelyettes Határőrségen kívüli tanfolyami átképzése, másodrészt a polgári státuszra felvett közalkalmazott, köztisztviselő rendészeti szakközépiskolában, munka mellett megvalósuló szakképzése, majd tiszthelyettessé való kinevezése. A középfokú végzettséghez kötött munkakörök betöltését az „informatikai szolgálat" fentieken túl, egyre bővülő létszámban oldotta meg köztisztviselői és közalkalmazotti státuszra, polgári életből való, megfelelő szakképzettséggel rendelkező állomány felvételével.

Az „informatikai szolgálat" megszervezésével és az IT, mint szakma előretörésével a tiszti állomány utánpótlásának gyakorlata kétség kívül megváltozott. A katonai felsőoktatásból érkezők[27] aránya csökkent, amíg nőtt azoknak tiszthelyetteseknek, közalkalmazottaknak és köztisztviselőknek a száma, akik a megfelelő szakképzettség megszerzését és a tiszti kinevezéshez szükséges rendészeti szaktanfolyam elvégzését követően hivatásos tiszti állományba lehetett venni. A Határőrség esetében is érzékelhető, hogy a szakma belső tartalmának megváltozása az IT ágazat vezetői számára elég komoly kihívásokat jelentett, hiszen a különböző információs és kommunikációs rendszerek modernizálása[28] nem elsősorban belülről fakadó szervezeti igényként jelentkezett, így e terület a nemzetközi érintettség okán mind szakmailag, mind politikailag exponálttá vált [10]. A szakmai vezetés a vele szemben támasztott követelményeknek lényegében sikeresen megfelelt, ezért felmerül a kérdés, hogy a Határőrség „informatikai szolgálata" látszólag miért tűnt sikeresebbnek?

A kérdésre egyrészről már válaszoltunk, hiszen utaltunk arra, hogy a múltból fakadó gyökerek okán a szakirányítási eljárás gyakorlatban való megvalósulása,

[26] a kezdetben különálló határrendészeti és rendészeti szakközépiskolák évtizedünk közepén folyamatosan összevonásra (integrálásra) kerültek, amellyel párhuzamosan számuk is redukálódott

[27] míg korábban a beiskolázásra kerülők a hagyományos híradó szakokon folytatták tanulmányaikat, addig a kilencvenes évek végétől mindinkább az igényeket jobban kielégítő informatikai szakokon történt a képzés

[28] legismertebb: a SIS rendszerhez való csatlakozás hazai műszaki-technikai és szervezeti hátterének kialakítása

valamint az anyagi-pénzügyi források központosítottabb felhasználása eredményesebb volt. A szakállomány ugyancsak „felhígult", hiszen a korábban rendelkezésre álló iskolarendszerből a szakmai igények kielégítése nem volt megoldható, így hasonlóan a rendőrségi gyakorlathoz az IT ágazat vezetői merítettek a polgári élet kínálta lehetőségekből. Ténykérdés egyrészről, hogy a szakirányítás elemeinek konzekvens alkalmazása révén a szakmai vezetők az állományilletékes parancsnokoknál érvényre tudták juttatni az általuk kialakított és széles körben elfogadott szakmai elveket, amelynek egyik része volt az egységes elvekre épülő, homogén állományszervezés. Másrészről szintén ténykérdés, hogy a Határőrség szervezete folyamatosan csökkent, az integráció előtt létszáma már csak alig volt egyharmada a Rendőrség létszámának, amely egyebek iránt megmutatkozott a feladatkörök szélességében is. E körülmények között nyilvánvaló, hogy időben több lehetőség adódott egyrészt az egyéni szakképzések támogatására, valamint a teljes IT ágazat szakmai közösségének rendszeres és együttes továbbképzésére, amely egyúttal jó táptalaja volt az állomány szervezeti érdekeknek megfelelő „szocializálására" is. Felmerül a képzési és átképzési költségek problematikája, azonban a Határőrségnél általánosan elfogadott elv volt, hogy a szakmai jártasságok kialakítását és a készségek elsajátítását nem csak a beosztási helyen eltöltött szakmai gyakorlat révén kell végrehajtani, hanem azt mind közösségi, mind egyéni formában segíteni szükséges, így a költségtervezés mindenképpen tudatos és előrelátó tevékenységként jelentkezett. Mindezeket összefoglalva elmondható, hogy az IT ágazatot illetően kódexszerű, belső norma a Határőrség esetében sem létezett. Az egyéb működési okmányokban rögzített, a szervezetben íratlanul elfogadott magatartási formákra (hagyományokra) épülő egységes gyakorlat, valamint a tudatos és kevésbé tudatos „szocializációs" eljárások a más rendészeti szervek szakállományától képességek szempontjából gyökeresen nem eltérő személyi állományt azonban a szervezettel azonosulni tudó közösséggé formálták. Talán kijelenthető, hogy a Határőrség „informatikai szolgálatát" képezők nagy többsége – *akarva, akaratlanul* – elsajátította az **egy nyelven való beszéd, beszélgetés** képességét.

3. A jelenlegi, integrált IT ágazat

Az Alkotmány, illetőleg a Rendőrségről szóló 1994. évi XXXIV. törvény módosítása révén 2008. január 1-jén megszűnt a Magyar Köztársaság Határőrsége. A szervezet jogutódjaként a Magyar Köztársaság Rendőrsége került kijelölésre, amelynek belső struktúrája módosításra került oly módon, hogy a határvédelmi és -rendészeti funkciók továbbra is zökkenőmentesen legyenek elláthatók. Ennek egyik folyományaként a Rendőrség gazdasági szakszolgálatában és ezen belül az IT ágazatban is szervezeti rekonstrukciók kerültek végrehajtásra. Ahogyan azt az előző fejezetben már érintettük, az IT ágazat a gazdasági szakszolgálatba tagozódik. A szakállomány továbbra is mindhárom szinten jelen van. A szakirányítás és a végrehajtás struktúrájában – *tekintettel a gazdasági szakszolgálat átalakítására* – a területi szinteken következtek be jelentősebb változások. A megyei rendőrfőkapitányságokon szervezett híradó és informatikai osztályok, valamint a határőr igazgatóságokon funkcionált informatikai osztályok a régiós illetékességi körökre kialakított gazdasági ellátó igazgatóságok hatáskörébe kerültek. Az igazgatóságok keretében regionális IT osztályok alakultak, amelyek azonban közvetlenül nem

vezetik a megyei rendőr-főkapitányságok gazdasági osztályain[29] létrehozott IT csoportokat, azok szempontjából csak szakirányítást gyakorolnak.[30] E szervezési megoldás alól többek között a Köztársasági Őrezred, a Budapesti Rendőr-főkapitányság, a Pest Megyei Rendőr-főkapitányság, a Készenléti Rendőrség,[31] Repülőtéri Rendőr Igazgatóság is mentesült, amely szerveknél a korábbi szakmai struktúra[32] fennmaradt, egyúttal esetükben a Központi Gazdasági Ellátó Igazgatóság IT szerve szakirányítást nem gyakorol. Központi szinten, az ORFK Gazdasági Főigazgatóság szervezetében IT főosztály került kialakításra, amelynek keretében szakterületi osztályok kezdték meg működésüket.[33] Az IT főosztály egyúttal ellátja a Rendőrség központi szerveit, valamint működteti és menedzseli a központi IT szolgáltatásokat.[34]

Az állománytábla kialakításánál a központi IT főosztály, valamint a regionális gazdasági ellátó igazgatóságok esetében a köztisztviselői és közalkalmazotti státuszok kerültek jelentős túlsúlyba,[35] vagyis mind a Rendőrségtől, mind a Határőrségtől érkezett hivatásos szakállomány eltérő státuszon kerül alkalmazásra. A helyi szervek esetében a korábbi gyakorlat fennmaradt. Ténykérdésnek kell azonban tekinteni egyrészt azt, hogy az integráció során a személyi állomány egy része kihasználta a nyugállományba vonulás kedvező lehetőségét, másrészt a hivatásos jogviszony rövid- és hosszútávú féltése miatt az állomány egy másik része szakmaváltást[36] hajtott végre, harmadrészt, saját elhatározása révén távozott a szolgálatból. Az integráció során többnyire befogadásról lehet beszélni, ugyanakkor mind a Rendőrség, mind a Határőrség területi IT szerveinél hivatásos szolgálatot teljesítők számára az alkalmazott szervezeti megoldások és az alkalmazási feltételek egyaránt újszerűen hatottak, a korábbi körülményeikhez, elképzeléseikhez képest merőben más jövőképet vázolnak fel. Összességében véve, a Rendőrség IT ágazatának személyi állománya, valamint szervezési megoldásai jelenleg heterogénnek tekinthetők. Az ágazatban megvalósult szervezeti rekonstrukciók újszerűen hatnak, elsősorban a területi szerveknél szolgálatot teljesítők körében. A kialakított struktúra alapvetően alkalmas a szakfeladatok ellátására, azonban az eltelt rövid időszak

[29] a megyei rendőr-főkapitányságok gazdasági osztályai szintén a regionális gazdasági ellátó igazgatóságok szervezetében kerültek megszervezésre

[30] a mostani szervezési helyzet némi bizonytalanságot okoz a helyi szervek számára, hiszen néhány esetben nem tisztázott kellőképpen, hogy a megyei IT csoport, vagy a regionális IT osztály gyakorol-e szakirányítást

[31] a Készenléti Rendőrség esetében az IT szervezet nem a gazdasági igazgatóság szervezetébe, hanem a fő szakmai tevékenységet jelentő bevetési ágazatba került integrálásra

[32] mindegyik szervezet esetében speciális megoldásokat alkalmaztak korábban is

[33] az osztályok mennyisége növekedett, a szakterületi beosztás a szakmai elveknek megfelelően került meghatározásra

[34] elsősorban: adatbázisok

[35] az alkalmazott megoldás megfelel az úgynevezett „civilesítés" követelményeinek, amelynek lényege, hogy a nem alapfeladatot ellátó, vagyis funkcionális területen szolgálatot teljesítő állomány nem sorolható be az 1996. évi XLIII. tv. hatálya alá. Besorolásukra vagy közalkalmazottként, vagy köztisztviselőként kerülhet sor

[36] amelyet a tiszti, vagy tiszthelyettesi kinevezéshez szükséges szakmai végzettség tett lehetővé

miatt jelenleg még nincs lehetőség sem az előnyök, sem a hátrányok korrekt, meszszemenő eredményeket felvonultató értékelésére, elemzésére.

4. Összegzés, következtetések

Áttekintve mind a Rendőrség, mind a Határőrség korábbi IT ágazatát **megállapítottuk**, hogy a kilencvenes évektől kezdődően mindkettő szervezet esetében generális, a megváltozó körülményekhez igazodó változások mentek végbe. Az eltérő hagyományok és szervezeti kultúra miatt a két szervezet működési hatékonyságában eltérések voltak megfigyelhetők, amelyek okai nem az egyéni képességek területén jelentkeztek. **Vizsgálataink** alapján **úgy ítéljük meg**, hogy a jogszerű működés átfogó és teljeskörű biztosítása, valamint a működéshez szükséges feltételekről való gondoskodás az elmúlt években a Határőrség IT ágazatában valósulhatott meg sikeresebben vélhetően azért, mert a személyi állomány direkt és indirekt „szocializációja" eredményesebb volt. **Kijelenthető**, hogy a szervezet IT ágazatában szolgálatot teljesítők nagy többsége – *akarva, akaratlanul* – elsajátította az **egy nyelven való beszéd, beszélgetés képességét**. A Rendőrség és Határőrség integrációja és ezzel az IT ágazatok összevonása két szakmai kultúra mentén került végrehajtásra, azonban mind a befogadó, mind a befogadott állomány szempontjából a jelenleg alkalmazott szervezési és működési megoldások újszerűnek hatnak.

Felhasznált irodalom:

[1] Pándi Erik – Vörös Szabolcs: A belügyminisztériumi ágazati távközlés fejlesztésének néhány kérdése (tanulmány), Tudomány Napja 2000. pályázat, fődíjnyertes pályamű, 22-55. oldal, Zrínyi Miklós Nemzetvédelmi Egyetem, Egyetemi Könyvtár, Budapest, 2000.;

[2] Pintér Sándor: A magyar rendőrség átvilágításának fő tapasztalatai, azok hasznosításának lehetőségei a rendőrség korszerűsítésében, A magyar rendőrség és a határőrség a közvéleményben és a valóságban, A Belügyminisztérium és a Hanns-Seidel Alapítvány konferenciája, 15-19. oldal, Hans-Seidel Alapítvány – Batthyány Lajos Alapítvány – HM – BM, ISBN 963 7703 80 2 16, Budapest, 1993. február 23.;

[3] Mráz István: A haderő vezetése békétől eltérő (minősített) időszakokban, „Kommunikáció 2003." nemzetközi szakmai tudományos konferencia, 222. oldal, Zrínyi Miklós Nemzetvédelmi Egyetem, ISBN 963 86229 6 2, Budapest, 2003. október 15.;

[4] Mráz István: A vezetés információs támogatásának vezetői követelményei, „Kommunikáció 2001." nemzetközi szakmai tudományos konferencia, 153-154. oldal, Zrínyi Miklós Nemzetvédelmi Egyetem, ISBN 963 00 8819 3, 179-191. oldal, Budapest, 2001. november 28.;

[5] A fegyveres szervek hivatásos állományú tagjainak szolgálati viszonyáról szóló 1996. évi XLIII. törvény, DVD jogtár 2007/12. szám, Complex Kiadó Jogi és Üzleti Tartalomszolgáltató Kft., ISSN 1788-5027, Budapest, 2007.;

[6] Egri Gábor: Projektek a Belügyminisztériumban, „Kommunikáció 2001." nemzetközi szakmai tudományos konferencia, 243-246. oldal, Zrínyi Miklós Nemzetvédelmi Egyetem, ISBN 963 00 8819 3, Budapest, 2001. november 28.;

[7] Határőrség Országos Parancsnokság: A Határőrség középtávú informatikai stratégiája az 1999-2001. évekre, 1-21. oldal, ORFK ITF irattár, Iktatási szám: 1/2-5/1999., Budapest, 1999.;
[8] A Magyar Köztársaság Alkotmányáról szóló 1949. évi XX. törvény, DVD jogtár 2007/12. szám, Complex Kiadó Jogi és Üzleti Tartalomszolgáltató Kft., ISSN 1788-5027, Budapest, 2007.;
[9] Koczka Ferenc: Az alapfokú híradótiszt-képzés elemzése, javaslatok a fejlesztés fő irányaira, „Kommunikáció 2001." nemzetközi szakmai tudományos konferencia, 86-89. oldal, Zrínyi Miklós Nemzetvédelmi Egyetem, ISBN 963 00 8819 3, 180. oldal, Budapest, 2001. november 28.;
[10] Egri, Gábor: Integration of the Schengen Information System in Hungary, „Kommunikáció 2007." nemzetközi szakmai tudományos konferencia, 403-416. oldal, Zrínyi Miklós Nemzetvédelmi Egyetem, ISBN 978 963 7060 31 1, Budapest, 2007. október 16.;

KORONCZAI Tibor

INFOKOMMUNIKÁCIÓS MEGOLDÁSOK A NATO-BAN

Az elmúlt években több doktori értekezés, tanulmány és publikáció jelent meg mind a hazai, mind a nemzetközi tudományos életben a távközlés, informatika, híradás és infokommunikáció területéről. A távközlés az informatikával és médiával konvergálva infokommunikációvá szélesedik, a technológiák, a szolgáltatások, a jogi és gazdasági környezet, a vezetési módszerek és a szervezeti szerkezetek dinamikusan változnak.

A távközlési és informatikai hálózatok technikai konvergenciájának hatása fokozatosan kimutatható, a lejátszódott folyamatok az infokommunikációs technikai eszközök egész világon végbement korszerűsödésével kapcsolatosak. Az infokommunikációs eszközök különböző teljesítmény paraméterei (sebesség, tárolókapacitás, sávszélesség, stb.) a vonatkozó tapasztalati törvényeknek (Moore, stb.) megfelelően tovább növekednek.

Az infokommunikációs rendszereknek az élet minden területén való széleskörű elterjedése jelentős veszélyforrásokat jelenthet a

- a működés megbízhatóságának hiányosságai,
- a tárolt illetve átvitt adatok integritásának és titkosságának sérelme,
- valamint a személyiségi és egyéb jogok esetleges megsértése vonatkozásában,
- ami a rendszerek iránti bizalom csökkentésével az informatikai szolgáltatások elterjedését gátló tényezővé válhat.

Ezért a technológiák fejlesztésével párhuzamosan fokozott gondot fordítanak a fenti problémák technikai és/vagy szabályozási eszközökkel való megoldására, úgy, hogy ez a rendszerek „alkalmazhatóságát" minnél kisebb mértékben csökkentse.

A NATO ajánlásokat fogalmaz meg. A kommunikációs rendszerek egymással összekapcsolhatóságát elvben a különböző STANAG-ek (lefektetett szabványok) biztosítják. A gyakorlati tapasztalatok másak, több alkalommal voltak problémák a nemzetközi gyakorlatokon, valamint a „missziók" híradásával. Az általunk tervezendő hálózatoknak mindenféleképpen csatlakozniuk kell a szövetségi rendszerünkben szerepet vállaló többi ország fegyveres szervezeteinek hálózataihoz, illetve a NATO C4ISR rendszeréhez, ez viszont csak akkor valósítható meg, ha tisztában vagyunk a követelményekkel.

A távközlés reformja, a globális infokommunikációs verseny kialakulása. Távközlés fejlődési trendek, infokommunikációs konvergenciák, a NATO integráció hatása. A hírközlésről, az elektronikus aláírásról és a médiáról szóló törvények. Nemzetközi szabványok, szabályozások, egyezmények, szervezetek. Infokommunikációs stratégia nem más, mint válasz a környezet kihívásaira. A stratégia meghatározása, célja. A stratégia tervezésének és megvalósításának folyamata. Változtatás-menedzsment. Hálózatfejlesztési és informatikai stratégiák. Az infokommunikációs terület szabályozása. A távközlési versenypiac kialakításának és az infokommunikációs konvergencia kibontakoztatásának feladatai. Szol-

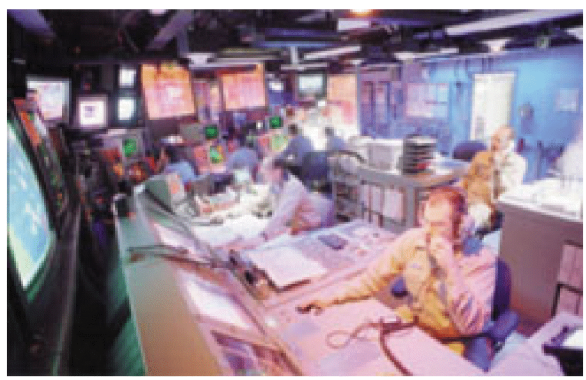
gáltatások engedélyezése, hálózatok integritása, összekapcsolása, átengedése, minőségfelügyelet, egyetemes szolgáltatások. Frekvenciagazdálkodás, szám- és címgazdálkodás. Alkalmazások biztonság- és tartalomszabályozása.

Az infokommunikációs eszközök katonai alkalmazása

Az elmúlt egy évtizedben teret nyert az infokommunikációs eszközök katonai alkalmazása. Legismertebb és széles körben terjedt el a mobiltelefon. A vezeték nélküli kommunikációs eszközök elterjedése a mobilizálhatóságuk miatt, a '90-es évek sláger infrastruktúráját jelentő vezetékes telekommunikációs eszközökkel (telefon, telefax, telex) szemben teret nyert, napjainkban pedig szinte kivétel nélkül mindenki ezeket használja.

Az elmúlt tíz évben a számítógépek alkalmazása és az internet, intranet használata fokozatosan terjedt el a katonai alkalmazások terén. A hálózatok fejlesztésével szélessávú kapcsolatok kialakításával, azaz az infokommunikációs infrastruktúra állapotának javulásával megteremtődött az információs hadviselés alapja.

Információs hadviselési szempontból, különösen igaz ez azon országok esetében, amelyek a fejlett országok körébe tartoznak. Ezek az országok rá vannak utalva az infokommunikáció használatára, így maguk is a legsebezhetőbbek közé tartoznak.



1. ábra: Infokommunikációs alkalmazás a vezetési ponton
(Forrás: The Information Warfare Site)

A parancsnokság és a harcoló alakulatok közötti, illetve az egyes egységek közötti modern kommunikációs hálózat blokkolása igen súlyos következményekhez vezet. Nem véletlen, hogy manapság már nem a hadvezérek elfogása az ellenség célja, hanem a parancsnoki központok bemérése, megsemmisítése, hiszen onnan irányítják a harcot. Azt a sebezhetőséget használja ki, hogy az elektronikus kommunikáció megjelenésével és annak katonai alkalmazásba való vételével az ellenség kommunikációjának zavarása, blokkolása révén az ellenség megbénítható, összezavarható, végső soron csaták, háborúk nyerhetők.

A telekommunikáció, az informatika megjelenése tehát minden előnye mellett egyúttal új, sebezhető pontot jelent a hadviselés során. Ez ahhoz hasonlítható, amikor a haderők gépesítését megkezdték, megjelent azok sebezhetősége is. Jó példa

erre a II. világháború, ahol elsősorban üzemanyag-utánpótlási problémák jelentkeztek, a repülő csapatoknál, valamint a harckocsiknál és szállító járműveknél.

2. ábra: Harcjármű IT berendezéssel (Forrás: www.bundeswehr.de)

Az információs hadviselés egyik kiemelt területe a hírszerzés alapú hadviselés (Intelligence Based Warfare). Az elnevezés alapján a klasszikus kémkedésre gondolunk általában a hírszerzés kapcsán. Itt azonban a katonai értelemben vett felderítés, célmeghatározás infokommunikációs eszközökkel való kiváltásáról van szó, és ezúton az emberi életet veszélyeztető, emberi felderítés helyettesítéséről.

A hírszerzés alapú felderítés alapvetően tehát infokommunikációs eszközökkel manipulál, amelyek négy fő csoportba oszthatók az érzékelés távolsága alapján:

nagy távolságú (tipikusan az űrbe telepített),

közeli helyen (például ember nélküli légi járműveken),

helyszíni (akusztikus, gravitációs, optikai),

illetve fegyverekre szerelt érzékelők (infravörös érzékelők, reflexiós radarok).

Az infokommunikációs eszközök alkalmazása mindamellett, hogy az emberi élet veszélyeztetését kiváltja, sokkal pontosabb, feldolgozhatóbb, nagyobb mennyiségű információt szolgáltat a hadvezetésnek és a harcoló alakulatoknak. Ugyanakkor ezen érzékelő eszközök zavarhatók, megtéveszthetők, kommunikációjuk blokkolható, összezavarható, illetve maguk az érzékelők fizikailag megsemmisíthetők. Az információs hadviselés korában mindenki meg tud figyelni mindenkit, és sokszor eredetileg nem háborús célokra kifejlesztett eszközöket tud bevetni a megfigyelés érdekében.

Szoftverrádiók

A szoftvervezérlésű rádiók a fejlett szolgáltatásaikat a stabilan működő üzemelési környezetben képesek maximálisan a felhasználók részére biztosítani. A működéshez elengedhetetlen feltétel a vezetés és az együttműködés megvalósulása a kommunikáció minden szintjén. Az automatikus azonosítás, szinkronizálás, az illetéktelenek kizárása a hálóból. Integrált hálózatmenedzselés, tervezés, konfigurálás, rugalmas és gyors beavatkozás lehetősége, szoftver támogatásával. Az alkalmazott szoftverektől függően a híradó és elektronikai felderítés, a navigációs és azonosító rendszerek, az információs műveletek, az elektronikai hadviselés, irányzás, vezérlés, elhárítás kiemelten fontos területek. A szoftvervezérlésű, illetve szoftverrádiók rugalmas rendszerkialakítási lehetősége előnyösen használható ki a feladatorientált szervezeti felépítés esetén, felhasználói igények változásai, a szol-

gáltatások paraméterei rugalmasabban és egyszerűbben köthetőek egyes szervezeti szintekhez, beosztásokhoz.

Harcászati internet

Elsőként az amerikai haderő alkalmazta az afganisztáni, majd az iraki műveletekben. A német haderő a FAUST vezetési-irányítási rendszert használja fel harcászati internetként, Afganisztánban kiválóak az alkalmazói tapasztalatok. A francia haderő a SICF vezetési-irányítási rendszert alkalmazza. A megosztott információ, jobban informált katonákat jelent, mely befolyásolja a kezdeményező készségüket.

A harcászati internet alkalmas a felderített adatok gyors, pontos és megbízható továbbítására és tárolására. A kommunikációs felderítés kiemelten fontos a katonai és nem katonai műveletek végrehajtása során. A technikai, és hírszerzési információkat, a külföldi kommunikációs forrásokból, valamint szükséges egyéb forrásokból gyűjti össze.

3. ábra: „Digitális vezetési pont" (Forrás: www.bundeswehr.de)

A COMINT (Communication Intelligence – Kommunikációs Felderítés) nem más, mint az elektromágneses energiát kisugárzó aktív kommunikációs hírközlő eszközök, rendszerek passzív eszközökkel történő felderítése, figyelése, ellenőrzése, technikai analizálása, és fizikai helyzetének meghatározására irányuló komplex tevékenység.

A SIGINT (Signal Intelligence – Jelfelderítés/ rádiótechnikai felderítés/) kommunikációs felderítés a jelfelderítés egyik fő összetevője, amely magába foglalja a COMINT-en kívül a nem kommunikációs típusú jelek, pl. radarjelek összegyűjtését.

A COMINT alkalmazásának célterületei igen szerteágazóak. A XXI. század kihívásának megfelelően a kábítószer kereskedelem, pénzmosás, nemzetközi terrorizmus is a célterületei.

Műholdas távközlés

A STANAG 5048 így utal a műholdak alkalmazására: „A szárazföldi erők részére, hadtesttől felfelé a követelményeknek megfelelően további kapcsolatok biztosíthatók a NATO vagy nemzeti harcászati műholdas (TACSATCOM) híradórendszeren keresztül. NATO beszédrejtjelző berendezések, NATO és nemzeti

digitális faxok, valamint NATO vezetés irányítás információs rendszerének (C2IS) termináljai kerülnek alkalmazásra."

A műholdas távközlési berendezések (SATCOM) térszegmensből és földszegmensből épülnek fel. A térszegmens egy vagy több távközlési műholdból áll össze. A földszegmenst egyrészről a térszegmens irányítása és felügyelete céljából létesített földi állomások, másrészről a távközlési kommunikáció megvalósítása céljából felépített földi állomások alkotják.

Egyes üzemeltetőknél a térszegmens 6 műholdból áll és két egységre tagozódik, amelyekből az űrben egyszerre csak két operatív és egy tartalék műhold található. A földszegmens kategóriában a következő típusok találhatók:

- nagy, közepes és kis földi állomás
- hordozható földi állomás
- mozgás közben üzemelő földi állomás
- tengerre telepített „földi" állomás (a tengerészet rendelkezik előjogokkal).

A potenciális bevetési terület lefedéséhez, amennyiben nincs lehetőség katonai SATCOM alkalmazására civil távközlési, kereskedelmi műholdakat üzemeltető társaságokat kell igénybe venni. (Például a Bundeswehr a német IFOR-csapatokkal való távolsági kommunikáció fenntartását az INTELSAT, EUTELSAT, DFS-Kopernikus és INMARSAT kereskedelmi műholdak távátviteli kapacitásának bérlésével oldotta meg.) A műholdak pozicionálásánál a szomszédos műholdakkal való kölcsönös zavarással kell számolni. Elvileg a kereskedelmi és katonai átvitel között nincsen különbség, de katonai SATCOM esetében a zavaró befolyás alatti kommunikáció téves intézkedéseket eredményezhet. Katonai távközlési műholdak esetében nem kizárt a szándékos zavarás lehetősége. Ezek kiszűrésére a földi állomásokon speciális modemeket alkalmaznak.

A nemzeti és NATO-érdekeltségű területen a katonai SATCOM-rendszer részére az átviteli csatornák használhatóságával kapcsolatban különösképpen magas követelményeket állítanak, tekintettel a SATCOM-mal kapcsolatos katonai vezetési eszközök használhatóságára. A távátvitel technikai funkciói és a szolgáltatások szabványosítása jelentékeny erőfeszítéseket követelt. A szabványosítás célja egy közös térszegmens, az EUMILSAT (Europäisches, Militärisches Satellitenkommunikationsystem) európai katonai távközlési műholdrendszer kialakítása. A cél egy közös (francia, brit, német, olasz, belga, spanyol) szabványosított közös katonai űrszegmens, amelynek az összes részt vevő nemzet kommunikációs követelményeit biztosítania kell.

Összegzés

A Magyar Honvédség vezetési feladatainak ellátásához elengedhetetlen az infokommunikációs eszközök, rendszerek alkalmazása. A teljesség igénye nélkül emeltem ki néhány elemet a más NATO tagországok által már alkalmazott infokommunikációs alkalmazási lehetőségek közül. Az eltérő rendszerek közötti kommunikáció szükségessé teszi az alkalmazott elektronikus védelmi megoldások összehangolását, rugalmasságuk és hatékonyságuk növelését. Fontos és kiemelt figyelmet kell szentelni az információ megosztására, meg kell akadályozni a jogosulatlan hozzáférést, megismerést. Akarjuk vagy sem, de az infokommunikációs hálózatok szerepe a távközlési és informatikai hálózatok technikai konvergenciájá-

nak hatására fokozatosan növekedni fog. A kialakításra kerülő (tábori) híradó és informatikai hálózatot valamilyen formában csatlakoztatni kell ehhez, ezért ez nagymértékben befolyásolja lehetőségeinket, és messzemenően figyelembe kell vennünk mindenféle tervezési és szervezési feladatnál.

Felhasznált irodalom

[1] Fekete Károly: A Magyar Honvédség állandó telepítésű kommunikációs rendszere továbbfejlesztésének technikai lehetőségei, Doktori (PhD) értekezés, Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, 2003.

[2] Hóka Miklós: A Magyar Honvédség harcászati rádiórendszerének kialakítási lehetőségei egyes NATO-tagországok rádiórendszereinek vizsgálata tükrében, Doktori (PhD) értekezés, Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, 2005.

[3] Rajnai Zoltán: A tábori alaphírhálózat vizsgálata és digitalizálásának lehetőségei egyes NATO tagországok kommunikációs rendszereinek tükrében, Doktori (PhD) értekezés, Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, 2001.

[4] NATO STANAG 5048

[5] FAUST Digital Command and Control, CD-ROM kiadvány, EADS Dornier GmbH System & Defence Electrinics (www.sysde.eads.net)

[6] Koronczai Tibor: A távközlési és informatikai rendszer konvergenciájának lehetőségei tábori hálózatokban, tanulmány, Székesfehérvár, 2005

[7] Koronczai Tibor: A digitális alapú tábori hálózatokban alkalmazható távközlési, informatikai és média technológiai rendszerekben rejlő lehetőségek az összhaderőnemi vezetés érdekében.

PÁNDI Balázs – PÁNDI Erik37

A JÖVŐ VÁRHATÓ HÁBORÚINAK ÉS KATONAI KONFLIKTUSAINAK HATÁSA A HAZAI TÁBORI KOMMUNIKÁCIÓS RENDSZER MEGÚJÍTÁSÁNAK FOLYAMATÁRA

Absztrakt: jelen közlemény a mérvadó szakirodalomra támaszkodva összegzi a jövőben várható katonai jellegű konfliktusok jellemzőit, illetőleg a Magyar Honvédség kötelékeinek nemzetközi tapasztalatait, amelyeken keresztül választ próbál adni a tábori hírrendszer megújításának egyes kérdéseire.

Kulcsszavak: információtechnológia, fegyveres konfliktus, háború, tábori hírrendszer, válságkezelés.

1. A jövő háborúinak és fegyveres konfliktusainak jellemzői

A jövő háborúi az azokat jellemzően meghatározó haditechnikai eszközök alapján az alábbiak szerint csoportosíthatók [1]:

a) a hagyományos háborúk lehetnek:

- tömegpusztító fegyverekkel való zsarolással, vagy az azok alkalmazása körülményei között vívottak;
- nagypontosságú fegyverek kiterjedt alkalmazásán alapuló, továbbá a legkorszerűbb felderítési-, vezetési- és irányítási rendszerek segítségével vívott multihaderőnemi precíziósak;
- hagyományos tűz- és csapásmérő eszközökkel vívottak;

b) kiterjedésük szerint:

- világháború;
- regionális háború;
- helyi háború;

c) időtartamuk szerint:

- villámháború;
- hagyományos háború;
- elhúzódó háború.

Fenti csoportosításon túlmenően, a fegyveres konfliktusokat vizsgálva a jövőben a következő fajták jelenhetnek meg:

a) szimmetrikus konfliktus;

b) aszimmetrikus konfliktus:

[37] Szerzők: Pándi Balázs, PhD-hallgató, ZMNE BJKMK Katonai Műszaki Doktori Iskola; Dr. Pándi Erik, egyetemi docens, ZMNE BJKMK Híradó Tanszék

- hagyományos;
- tömegpusztító fegyverek általi zsaroláson, vagy azok alkalmazása viszonyai között lefolytatott.

A konfliktusok aszimmetrikus jellege egyrészt az abban résztvevő egyik fél nem állami, nem legitim státusát jelöli, másrészt pedig az alkalmazott haditechnikai eszközök minőségének és mennyiségének összevethetetlenségével függ össze. Ha a jövő háborúját említjük, akkor lényegében két jól elkülöníthető háborúról lehet beszélni, egyrészt a közeljövőé, amelyet még éppen nem vívtunk meg. Másodrészt a távolabbi jövő háborúja, ami egyfajta vizionált, előrejelzett háború, amely a jövő fenyegetéseire adandó várható fegyveres válasz sajátosságait körvonalazza és normális esetben a nemzeti és koalíciós haderők hosszútávú fejlesztésének, katonai potenciálja kialakításának alapjául szolgál. A jelenkor modern háborúja és a jövőkor kettő típusú háborújának alapvető összefüggései:

a) mindegyikben megtalálható a jelen háborújának ismérvei és az alkalmazott haditechnikai eszközök, de a jövőbeniben egyre több és több új sajátosság és modernebb haditechnika épül be;
b) közös vonásuk, hogy a jelenkor fenyegetései, úgymint a globális világban meglevő instabilitás, a tömegpusztító fegyverek elterjedésének veszélye, valamint az egyre globalizálódó terrorizmus, lényegükből adódóan a jövőben sem szűnnek meg, legfeljebb egyes régiókban azok tovább terjednek, így egyúttal a jövőnek is fenyegetései maradnak.

A fenyegetések a következők lehetnek:

a) aszimmetrikus fenyegetések;
b) a hadászati tömegpusztító fegyverek elterjedése;
c) regionális hatalmak fenyegetései.

E fenyegetésekre adandó válasz, azaz a jövő háborújának általános célja a győzelem kivívása, vagy egy kedvezőbb békeállapot feltételrendszerének megteremtése lesz. Jellemző vonása pedig a nagypontosságú fegyverekkel és hálózatközpontú, felderítő, vezetési- és irányítási rendszerek segítségével vívott hadviselés mellett a hadászati űrfegyverek és a robotok alkalmazása lesz. A háború alapvető elvei a jövőben sem változnak. Alapelvnek tekinthető továbbra is egyrészt a hadászati kezdeményezés megragadása és fenntartása. Másodsorban a siker és a katonai győzelem eléréséhez szükséges döntő tevékenységek, műveletek komplexitásával és végrehajtásának képességével, a nagyfokú manőverező képességgel, a katonai feladatok pontos végrehajtásával, a csapatok teljeskörű védelmével és az összpontosított logisztikai támogatás képességével, beleértve a logisztikai rendszerek interoperabilitását is [2]. A jövő háborúja az információk háborúja is lesz egyúttal, ahol jellemző az információs fölényért vívott kíméletlenül gyors és dinamikus küzdelem. Amely fél ezen a területen fölénybe kerül, az fog rendelkezni az első, sőt a megelőző csapás lehetőségével, amely döntő lehet a háború megnyerése szempontjából. Vélhetően nem csökken a szárazföldi csapatok szerepe, hiszen a

háborúk zömében – kivétel lehet a megtorlás vagy a békekikényszerítés céljából folytatott háború – továbbra is fontos szerepe lesz a területek elfoglalásának, megtartásának és ellenőrzésének. Amennyiben a háború koalíciós méreteket ölt, a szárazföldi csapatoknál koncentrálódik majd leginkább a többnemzetiségű jelleg is [3].

A jövő fegyveres konfliktusának egyre gyakoribb formája lesz az aszimmetrikus, ezen belül is a terrorista fegyveres konfliktus. Ennek jellemzője, hogy egy adott államon belül, vagy néhány államban, illetve egy adott, vagy több hadszíntéren egyidőben, hirtelen, szinte a semmiből tör ki és rendszerint nem a hadsereg a célpontja. Mire ellentevékenységre kerülhetne sor, addigra be is fejeződik, illetőleg tartósan szünetel. Ennek okán a terrorizmus elleni harcra kijelölt erőknek folyamatosan készenlétben kell állniuk. A konfliktusok időtartama bizonytalan, de valószínűleg elhúzódó lesz. A nemzeti vagy koalíciós haderőnek a saját hatékony önvédelméről is szüntelenül gondoskodnia kell. A jövő fegyveres konfliktusai a válság fokozódásával háborúba nőhet át, de annak csillapodásával átmehet a válságkezelés különböző, békésebb fokozataiba. A válságreagáló műveletek terén a NATO, EU és az ENSz napjainkban eltérő módon értelmezi a műveletek típusait, azonban a végrehajtásban és a fegyverek szerinti felosztásban történő osztályozás azonos [4]:

a) végrehajtás szerint:
- nemzeti területen önállóan;
- nemzetközi területen szövetségi kötelékben;

b) fegyverek alkalmazása szerint:
- nem fegyveres tevékenységek (katasztrófák elhárítása, felszámolása, humanitárius segítségnyújtás, stb.);
- fegyveres tevékenységek (terrorizmus, szervezett bűnözés elleni fellépés, stb.);
- kombinált tevékenységek (nem várt, kikényszerített fegyverhasználat).

2. A külföldön tevékenykedő magyar kötelékek híradó és informatikai támogatása

Az információk és az ezekhez kapcsolódó tevékenységek valamennyi katonai szervezet számára a célkitűzések elérésének, a rendeltetésszerű tevékenység megvalósításának egyik legfontosabb feltételeit, erőforrásait képezik. Napjaink katonai műveleteiben a felek eredményes tevékenységének alapvető feltétele a döntési fölény és az ezt megalapozó információs fölény és egyeztetett közös helyzetismeret kialakítása és fenntartása. Mindez gyakorlatilag már megvalósíthatatlan a korszerű információtechnológia eszközrendszerének széleskörű, tervszerű és szervezett alkalmazása nélkül [5].

A Magyar Köztársaság és ezen belül a Magyar Honvédség külföldi szerepvállalása a délszláv válság rendezésében elsőként az IFOR feladat kapcsán jelentkezett. A katonai szervezet akkor a meglevő híradóeszközökkel került vezénylésre, vagyis R-142, R-145 rádióállomásokkal, illetőleg R-1340 RH, MT-300 és R-159 rádióké-

szülékekkel. A szolgálati távbeszélő viszonylatok ALCATEL digitális központban végződtek. A szolgálatot teljesítő kötelékek több, egymástól független műholdas átviteli eszköztípussal kerültek ellátásra, amelyek biztosították a mindenidejű, megbízható kapcsolatot hazánkkal [6]. Napjainkban, az ISAF misszióban a híradás megszervezése során a rendszerben polgári és katonai technikai eszközök és megoldások egyaránt megtalálhatók. Előzőek megvalósulását a magyar erők részére telepített távbeszélő és informatikai hálózatok biztosítják. A távbeszélő hálózatok lehetnek részben vezetékeken alapuló, valamint teljes egészében vezeték nélküli hálózatok, amelyek közül az egyes táborhelyek közötti kommunikáció mindig műholdas, tehát vezeték nélküli technikán alapul, míg léteznek a táborhelyen belüli telephelyek közötti kommunikációt biztosító URH rádióhálózatok, vagy műholdas telefonok. Az informatikai hálózatok szervezése hasonlóan történik. A gerinchálózatra csatlakozó informatikai rendszerek műholdas kapcsolatban vannak a hálózattal, míg léteznek helyi intranet hálózatok, amelyek különböző szintű minősítésűek. Látható, hogy a nemzetközi környezetben alkalmazásra kerülő hazai katonai egységek, alegységek kommunikációjának biztosítása komplex rendszerekkel és megoldásokkal történik [7]. Hasonló megoldások találhatók az EUFOR missziók esetében is, hiszen napjainkban a videokonferencia szolgáltatást a híradó és informatikai rendszerek egyik alapszolgáltatásaként kell tekinteni (STANAG 5048). A misszió keretében működő járőrszolgálati egységek számára biztosítani kell a mobil távbeszélő és adatátviteli (többnyire: valósidejű) szolgáltatásokat is [8]. A nemzetközi együttműködési kényszer egyik pozitív hatásaként tekinthető, hogy a hazai mértékadó katonai körök ténylegesen készek elismerni, hogy napjainkban az információs és vezetési rendszerrel szemben a következő alapvető követelmények fogalmazódnak meg [9]:

a) az állandó telepítésű, a mobil és mesterséges holdas kommunikációs eszközök együttes jelenléte;

b) a valósidejű és szélessávú adatátvitel;

c) az információs rendszer megbízható és folyamatos működőképessége a csapatok alkalmazása során.

3. A megújítási folyamatot érintő hatások

A hazai tábori hírrendszer megújítására több terv is készült egy évtizeddel ezelőtt. A végrehajtás meghiúsulásának több oka lehetett, egyes korábbi vélemények szerint az átalakítási ciklust túl hosszú időben szabták meg a tervezők, másrészt nem állt rendelkezésre megfelelő szakállomány, harmadrészt koncepcionális tévedések voltak a tervben [10]. A modernizáció nem valósult meg, így mára végrehajtása lényegében már nem halogatható tovább. Ezt támasztják alá a jövő háborúival és fegyveres konfliktusaival kapcsolatos kutatások, illetőleg a nemzetközi környezetben szolgálatot teljesítő magyar katonák személyes tapasztalatai is. Az Egyesült Államok már az elmúlt évtizedben megfogalmazta a teljes harcászati kép kialakítására szolgáló Harcászati Internet elnevezésű integrált kommunikációs hálózat kialakításának szükségességét [11], amely mellett a nemzetközi szakmai események tanulmányozása során egyértelműen megfigyelhető azon tendencia is, amely szerint a fejlettebb európai NATO tagországok többségében, mind a harcászati, mind a hadműveleti szintű kommunikációs rendszerek tekintetében komoly fejlesztések

kezdődtek meg. Ezek egyértelműen előrevetítik az IP alapú, szélessávú mobil adatátviteli lehetőségek kiterjesztését célozzák meg [12]. Kísérletek hazánkban is folynak, hiszen 2007-ben a Combined Endeavor gyakorlat keretében IMS architektúra alkalmazásával magyar katonák kommunikációs céljaikra felhasználták a VoIP kapcsolat révén megvalósított valósidejű videó és audio szolgáltatásokat is [13].

A Magyar Honvédség jelenlegi harcoló, harci támogató és támogató szervezeteinek nagysága, illetőleg létszámának mennyisége a politikai és katonai felsővezetés megítélése szerint napjainkban már arányban áll az ország teherbíró képességével, így megítélésünk szerint – *a prognosztizálható jövőre is tekintettel* – célszerű lenne komplex, a nyugat-európai NATO tagországokban is már alkalmazott tábori C2, vagy fejlettebb rendszerek beszerzését komoly megfontolás tárgyává tenni. Úgy ítéljük meg azonban, hogy a modernizáció érdemi megvalósulásáig a tábori hírrendszer tekintetében jelentkező egyes szakfeladatok automatizálása érdekében célszoftverek megalkotása válhat szükségessé (pl.: híradás vázlata, stb.), amelyek elősegíthetik a hírrendszerrel kapcsolatos manőverek időtartamának redukcióját, a reagálóképesség szintjének emelését.

4. Összegzés, következtetések

A nemzetközi és hazai katonai kutatások továbbra is prognosztizálják a háborúkat és a katonai konfliktusokat. Hazánk szövetségi tagságából adódóan nemzetközi léptékekben is ellát katonai feladatokat, amelynek megfelelő támogatásához azonban tábori kommunikációs rendszere elavultnak tekinthető. Mind a kutatási, mind a személyes tapasztalatok alátámasztják, hogy a tábori rendszer megújítása elkerülhetetlen, azonban mindaddig, amíg a modernizációs folyamat meg nem kezdődnek célszerűnek mutatkozik egyes munkafolyamatok automatizálása.

Felhasznált irodalom:

[1] Molnár István: A jövő háborúinak és fegyveres konfliktusainak jellemzőiről, Kard és Toll, Honvédelmi Minisztérium, Budapest, 2005., ISSN 1587-558X, 7-14. oldal, 2005/3. szám;

[2] Kőszegvári Tibor – Szternák György – Magyar István: A XXI. századi hadviselés, egyetemi jegyzet, Budapest, 2000., 35-42. oldal;

[3] Scales, Robert H. Jr.: Certain Victory: The U.S. Army int he Golf War. Brassey's. Washington London, 380-382. oldal, 1994.;

[4] Farkas Tibor: Válságkezelés, válságreagáló műveletek, Hadtudományi Szemle, ZMNE KLHK, Budapest, 2008., 2. oldal, 2008/1. szám;

[5] Munk Sándor: Az informatikai támogatás alapjai, Nemzetvédelmi Közlemények, ZMNE, Budapest, 2005., ISSN 1417-7323, 188. oldal, 2005/2. szám;

[6] Hóka Miklós – Horváth Attila: A béketámogató és válságreagáló műveletek híradása – itthoni szemmel, „Kommunikáció 2005." nemzetközi szakmai-tudományos konferencia kiadványa, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2005, ISBN 963-7060-11-1, 147-148. oldal;

[7] Rajnai Zoltán – Takács Péter: Az afganisztáni missziós híradás tapasztalatai, Kard és Toll, Honvédelmi Minisztérium, Budapest, 2006, ISSN 1587-558X, 28-31. oldal, 2006/3. szám;

[8] Fekete, Károly: Modelling the videoconference in mission, „Kommunikáció 2007.” nemzetközi szakmai-tudományos konferencia kiadványa, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2007, ISBN 978-963-7060-31-1, 126-127. oldal;
[9] Czank László: A NATO távközlési- és információs rendszere a XXI. század küszöbén, Nemzetvédelmi Közlemények, ZMNE, Budapest, 2003., ISSN 1417-7323, 168. oldal, 2003/3. szám;
[10] Szöllősi Sándor: A Magyar Honvédség állandó és tábori hírhálózatának átalakításával kapcsolatos problémák, „Kommunikáció 2001.” nemzetközi szakmai-tudományos konferencia kiadványa, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2001, ISBN 963-00 8819 3, 228-229. oldal;
[11] Hóka Miklós: A harctéri kommunikáció egyik lehetséges jövőképe: a harcászati internet, „Kommunikáció 2003.” nemzetközi szakmai-tudományos konferencia kiadványa, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2003, ISBN 963-86229-6-2, 103. oldal;
[12] Kenyon, Henry S.: France reboots its networking capabilities, Signal, AFCEA's international journal, Fair Lakes Court, Fairfax, Virginia, U.S., ISSN 0037-4938, 39. oldal;
[13] Boland, Rita: Standards place everything over the internet, Signal, AFCEA's international journal, Fair Lakes Court, Fairfax, Virginia, U.S., ISSN 0037-4938, 57. oldal.

Károly FEKETE PhD

COMPARISON OF BROADBAND WIRELESS TECHNOLOGIES

This Paper was supported by the János Bolyai research Scholarship of the Hungarian Academy of Sciences

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

Abstract

The growth of wireless broadband wireless networks in the past few years can be attributed to rising demand for wireless services such as data, voice, video, and the development of new wireless standards even in military and governmental environment. Mobile broadband wireless access is needed to provide advanced telecommunications services effectively and affordably to consumers around the world. This paper evaluates the current commercial alternative, mobile (3G and 4G) and fixed wireless (Wi-Fi and WiMAX) technologies.

Introduction

The growth of wireless broadband networks is expected to gradually outpace landline communications as advancements in these technologies enable broadband speeds. This growth can be attributed to an increase in demand for wireless services such as data, voice, video, and the development of new wireless standards.

Broadband wireless networks fall into two general categories: fixed, and mobile. This is followed thereafter by a discussion on fixed broadband wireless networking technologies; Wi-Fi and WiMAX (802.16). The goal is to examine the key drivers for both fixed and mobile broadband wireless networks in military and governmental environment by exploring currently deployed and anticipated technologies. Within each of these technologies, standards, protocols, data transport, strengths, weaknesses, and security will be discussed.

Fixed broadband access has already become an urban commodity in the world an in Hungary from the beginning of 2000 (Fig. 1.), but so far there have been few means of delivering these bandwidth-consuming services effectively and affordably to the significant number of rural and mobile users. However, recent advances in e.g. signal processing, radio protocols, and mobile network

infrastructure are now enabling the concept of mobile broadband for consumers around the world.

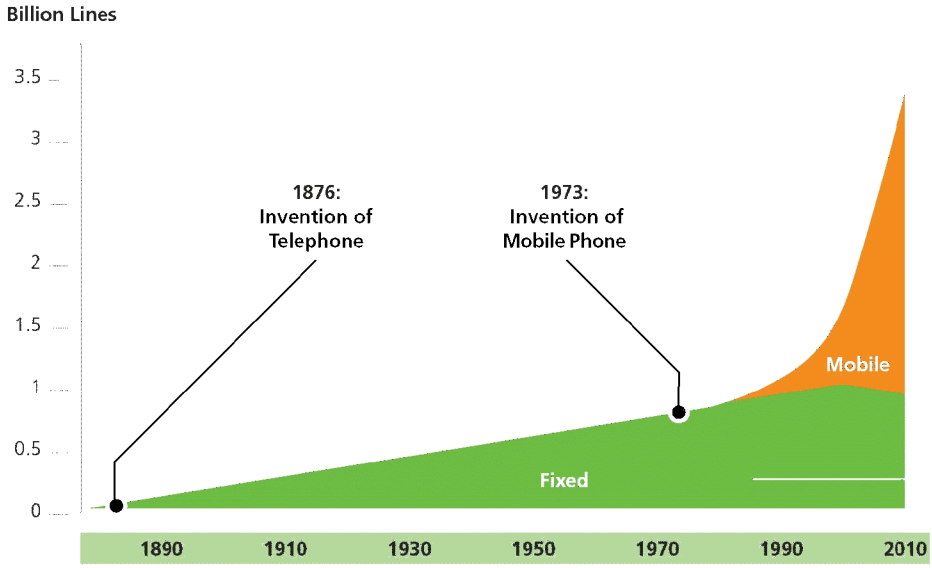


Fig. 1. Growth of Voice Services

Generations of Mobile Broadband Technologies

Currently there are a number of different technologies for broadband wireless access for both fixed and mobile applications. Historically, the era of mobile broadband wireless networks evolved through several generations of cellular mobile networking systems. The first generation (1G) systems were analog FDMA systems which primarily were designed for voice only communication. These 1G systems were replaced by the 2G systems which although digital were also capable of voice communications. The transition from 2G to 3G involved a brief phase called CDMA2000 phase I (2.5G) which introduced technologies such as; General Packet Radio Service (GPRS), and Enhanced Data Rates for Global Evolution (EDGE).

While some 2G and 2.5G systems are still available, third generation (3G) mobile networking systems are replacing them gradually (UMTS-HSDPA-HSUPA). Governed by International Telecommunications Union (ITU), 3G wireless broadband networks can deliver high data transmission rates, greater system capacity, and improved spectrum efficiency. Some of them are completely proprietary, based on vendor-specific solutions that are noninteroperable, while others are based on open standards developed by industry working groups.

Third generation (3G)

Commercial deployments of 3G technologies started in 2000. The CDMA2000 and WCDMA (Wideband Code-Division Multiple-Access) technologies account for more than 50% of all the subscribers to 3G services. This number is expected to grow as the technology improves and the market becomes competitive. The main driving force behind the growth of 3G is its ability to deliver data, voice, and video telephony. However all 3G technologies do not posses the same performance capabilities.

Generally 3G technologies can be split into the following:

- UMTS (Universal Mobile Telephone System);
- HSDPA-HSUPA (High Speed Downlink-Uplink Packet Access);
- CDMA2000;
- EV-DO.

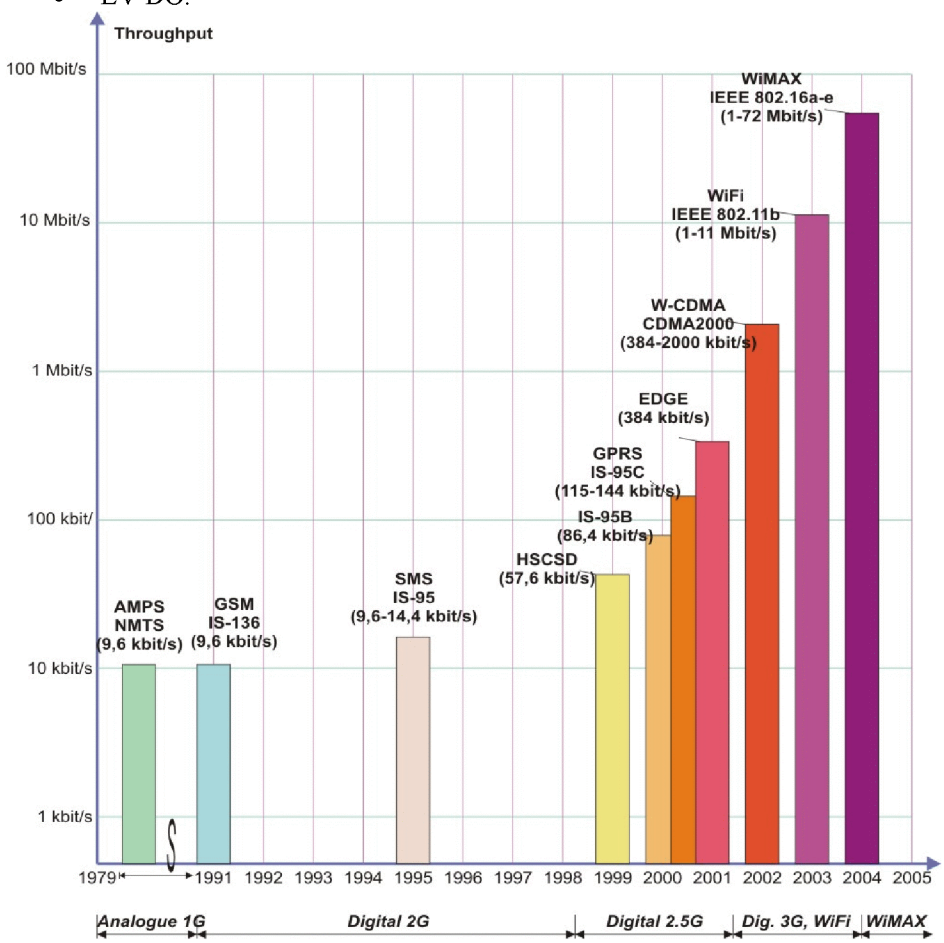


Fig. 2. Evolution of Broadband Wireless Networks

3G cellular systems, most notably UMTS, are currently the most widely deployed mobile broadband technology with a huge established presence in terms of operators, customer base, brand, deployed base station sites, and backhaul capacity. Standardized by 3GPP in its Release 5, HSDPA is a tremendous performance upgrade for UMTS packet data, enabling peak data rates up to 14,4 Mbit/s, although the initial limit is 1,8 Mbit/s. Latency is also reduced, and spectral efficiency is improved as well. These improvements are achieved through improved modulation and coding, and implementing fast scheduling and retransmissions at base station level.

The UMTS (also known as W-CDMA) is based on the W-CDMA technology that is favored by countries that use GSM which are primarily located in Europe. WCDMA supports speeds between 64 and 384Kb [1]. WCDMA has evolved into HSDPA (HSUPA) which supports a converged packet network that allows support for end-to-end IP services. HSDPA data transfer rates range between 400Kbps and 3,2Mbps. CDMA2000 is an outgrowth of the 2G CDMA standard or IS-95. There are several transmission technologies that fall under the CDMA2000. These include: 1xRTT, CDMA2000 and 1xEV-DO (EV-DO)/1xEV-DV (EV-DV). Figure 2 provides a good overview of the evolution of the mobile wireless broadband networks.

High-Speed Uplink Packet Access (HSUPA) is included in 3GPP Release 6. The combination of HSDPA and HSUPA is often called simply HSPA. It will deliver uplink data rates of up to 5,76 Mbit/s and further decrease the network RTT to a level of 50 ms. HSUPA trials are expected to begin gradually and the technology is bound to hit the market in 2007. Although most WCDMA/HSDPA deployments are based on FDD where different radio bands are used to separate downlink and uplink transmission, 3GPP specifications also include a TDD version of UMTS where both transmit and receive functions alternate in time on the same radio channel. This can be beneficial for the many asymmetric data applications that consume more bandwidth in the downlink than in the uplink. A TDD radio interface can dynamically adjust the downlink to uplink ratio accordingly, and thus can balance both forward link and reverse link capacity. Spectral allocation is also more straightforward, as TDD requires only one band instead of two bands and a further guard band in FDD.

More fundamental 3G developments proceed under the umbrella name of UMTS Long Term Evolution (LTE). Key elements are currently being standardized for 3GPP Release 8 and LTE aims for peak data rates of 200 Mbit/s for downlink and 100 Mbit/s for uplink.

Evolution Data Only (EV-DO)

EV-DO is a high performance technology based on IP network architecture. EV-DO end user data rates range between 400Kbps and 700Kbps where the com-

mercial EV-DO system can provide data transfer rates of 2.4Mbps downlink. This service is available throughout the country with the most availability concentrated in metropolitan areas. The convention is whenever users move away from these EV-DO coverage areas, the service drops to the underlying 1x RTT network.

Fourth generation (4G)

Fourth Generation (4G) broadband wireless networks are expected to replace the current 3G wireless network deployments. These 4G networks are expected to transfer data at speeds of 20Mbps for uplinks and 100Mbps for downlinks. The key drivers for adopting 4G are; its support for multimedia services, wider bandwidths, global mobility, service portability, low cost, and scalability.

Architecturally, the 4G networks unlike the 3G networks packets are switched. In addition, 4G network elements possess the ability to connect to other wireless technologies such as WCDMA, EDGE, and WIFI seamlessly. This pervasiveness will employ smart-radio technology that is capable of managing the spectrum use and power transmission efficiently. Finally 4G will provide the ability to use mesh routing protocols to create ad hoc mesh networks.

Advantages and challenges

The high bandwidth that 4G supports provides an ideal mode for data transport. It is expected that users who demand high quality video and audio will benefit because of the Orthogonal Frequency Division Multiplexing (OFDM) and Orthogonal Frequency Division Multiple Access (OFDMA) which are used extensively in 4G networks. Both these technologies allocate network resources effectively to multiple users. Additionally, 4G provides high bandwidth, better security, and low latency data transmission.

Fixed broadband wireless networks

Fixed broadband wireless technologies can be defined as high speed wireless networks that connect to stationary locations and are intended to serve nomadic users. This report will examine two of these technologies; wireless fidelity (Wi-Fi) and Worldwide Interoperability for Microwave Access (WiMAX). Both these technologies are governed by IEEE 802.X standards.

Technology Standard Throughput Range Frequency:

- Wi-Fi 802.11a Up to 54Mbps Up to 100m 5Ghz
- Wi-Fi 802.11b Up to 11Mbps Up to 100m 2.4Ghz
- Wi-Fi 802.11g Up to 54Mbps Up to 100m 2.4Ghz
- WiMAX 802.16a Up to 70Mbps 5-8 km 11Ghz
- WiMAX 802.16d Up to 75Mbps(20Mhz) 6-10 km 11Ghz
- WiMAX 802.16e Up to 30Mbps(10Mhz) 1,5-5 km 2.6Ghz

Wireless fidelity (Wi-Fi)

Wi-Fi is considered to be one of the first widely deployed fixed broadband wireless networks. As a result there are many Wi-Fi compatible products on the market today. Wi-Fi is a set of technologies that are based on the following IEEE 802.11a, b, and g standards. Each of these Wi-Fi technologies can be found at hotspots located in homes, libraries, university campuses, military bases, and airports. As long as the user remains within 100m of the fixed wireless access point, they will maintain broadband wireless connectivity.

The Wi-Fi architecture consists of a base station that wireless hosts connect to in order to access network resources. The base station is responsible for sending and receiving data to and from the wireless host that is associated with the base station. The connection between the host and the base station is the wireless communication link. This communication link is responsible for the data transport between the base station and the hosts. The base station relays the data between the host and the larger network (defense network, corporate, internet, home etc). Various mobile service providers (e.g. T-Mobile) operate hotspot base stations located in public phone booths, airports that can be used for internet access.

From point of view of military users the main strength of Wi-Fi is its simplicity and ease of deployment given that it uses unlicensed radio spectrum which does not require regulatory approval. Secondly, the cost for rolling out this wireless solution is low because of no expensive wiring is required. This makes Wi-Fi a perfect solution, for places that are hard to wire (metropolitan buildings and land area). Thirdly, Wi-Fi allows military users to be mobile for up to 100 m from the base station and still have access to the network. Fourthly, there are many Wi-Fi compatible products that are available at a low cost and can interoperate with other network technologies in the market today (COTS). For example most laptops and mobile devices come with build in Wi-Fi connectivity thus making it easy to use after a simple configuration. Finally, Wi-Fi standards are interoperable globally thus Wi-Fi military clients can work seamlessly in other military users of different countries with minimal configuration.

As a fixed broadband access technology, Wi-Fi has its weaknesses. First the military user can only use the technology within the confines of a 100 m radius thus limiting the level of mobility. Secondly, the fact that this technology operates in the 2.4GHz band and does not require any licensing, thus rendering them susceptible to interference from other devices such as Bluetooth, cordless phones, and microwave ovens. Finally security is a concern because most of this wireless access remains unsecured because the encryption standard used such as Wired Equivalent Privacy (WEP) which has been shown to be easily breakable [2], [3].

Worldwide Interoperability For Microwave Access (WiMAX)

WiMAX is an emerging fixed broadband wireless technology that has garnered a lot of attention and enthusiasm in the wireless industry.

WiMAX is short for Worldwide Interoperability for Microwave Access and it is defined by the IEEE 802.16 Working Group. Although first intended for fixed applications, the initial WiMAX standards have evolved to form the basis for mobile WiMAX as well. The current version of the fixed WiMAX standard is 802.16-2004, sometimes also referred to as 802.16d [6]. It is essentially frequency independent, allowing also nonline- of-sight (NLoS) operation in the lower end of the frequency range what is essential for military applications. The radio access interface is based on orthogonal frequency division multiplexing (OFDM) with 256 subcarriers[38]. OFDM allows good resistance to interference and multipath fading. Channel bandwidth ranges from 1,25 to 20 MHz, and either FDD or TDD may be used for duplexing. WiMAX cell size is dependent on the used frequency band, but coverage radiuses of 1 to 2 km for NLoS and 10 to 16 km for LoS are typical with standard base station equipment. With some optional enhancements, however, the figures are 4 to 9 km (NLoS) and 30 to 50 km (LoS). Actual data rates are also highly variable and depend on a number of factors. Although rates as high as 75 Mbit/s have been advertised, 2 Mbit/s over a range of roughly 5 to 10 km is closer to reality according to the experiments of COMMIT 2007 Communications Training in Budapest.

Fixed WiMAX, as defined in 802.16-2004, does not support handovers or any other basic mobility mechanisms. Deployed in phases, WiMAX uses the IEEE 802.16 standard specifications (802.16 d, and e). The IEEE 802.16d specification is primarily tailored to wireless wide area networks (WLANs). The recently approved IEEE 802.16e specification on the other hand is primarily used for mobile wireless metropolitan networks (WMANs). These two specifications render WiMAX architecturally ideal for the connection to the last km military networks, the backhaul, internet service providers, cellular base stations that bypass PSTN-s, hotspots, and enterprise networks.

Abilities such as a high bandwidth frequencies between 2 GHz and 11GHz, makes WiMAX ideal for data transport. WiMAX has a range of up to 50 km. This ability is enhanced by WiMAX-s cell radius of 7-10 km. Lastly, WiMAX also has the ability to support various data transmitting rates of up to 75Mbps.

Mobile WiMAX (IEEE 802.16e-2005)

According the Military requirements on tactical level the biggest shortcoming of 802.16-2004 is the lack of support for mobility. IEEE addressed this issue by developing specifications for a separate version of the standard, the 802.16e, which was approved on December 7, 2005 (IEEE 2005). Also known as mobile WiMAX, the standard is seen to be in competition with 3G cellular technologies. Its radio access method is even more sophisticated than that of fixed WiMAX. The tradeoff

[38] OFDMA2048 and single carrier access modes are included in the 802.16-2004 standard as alternatives.

is increased complexity in physical layer processing. Fast handover signaling is supported, e.g., to allow users in moving vehicles to seamlessly switch between base stations. Mobile WiMAX operates in the 2 to 6 GHz range that mainly consists of licensed bands. Mobile applications are likely to operate in frequencies below 3 GHz, while even some fixed applications are expected to use 802.16e due to its better characteristics.

However, it should be noted that there is no backward compatibility with fixed WiMAX. Cell radiuses are expected to be typically 2 to 5 km, and user data rates up to 30 Mbit/s are achievable in theory with full 10 MHz channels. The first certified 802.16e products are expected to be available by late 2006, though wide scale commercial deployments are expected not earlier than 2009.

IEEE 802.20

The IEEE 802.20 (or Mobile Broadband Wireless Access - MBWA) Working Group was established on December 11, 2002 with the aim to develop a specification for an efficient packet based air interface that is optimized for the transport of IP based services. The goal is to enable worldwide deployment of affordable, always-on, and interoperable networks based on IEEE 802.20 for both business and residential end user markets. The group will specify the lower layers of the air interface, operating in licensed bands below 3.5 GHz and enabling peak user data rates exceeding 1 Mbit/s at speeds of up to 250 km/h. The goals of 802.20 and 802.16e are similar [5].

Advantages of WiMAX from the point of view of military applications

There are several advantages to the deployment of WiMAX. Foremost, it supports high throughput rates, data speed rates, and multitudes of military users via a single channel. Therefore the deployment of this technology can be done quickly in bad or enemy terrain areas or in environments with limited wired infrastructure. Secondly, WiMAX supports and integrates easily to other wired and wireless technologies such as Ethernet, IPv4-6, ATM, SDH, VLANs, and Wi-Fi in the NATO OSE.

Consequently existing Wireless Service Providers can use this technology to scale and expand their numbers cost effectively. Thirdly, WiMAX also provides network connectivity using multi-path signals and without the requirement of a direct line of sight from Headquarters or between deployed elements of military communications infrastructure. Fourthly, WiMAX provides a great Quality of Service by taking advantage of smart antenna technology that utilizes the spectrum more efficiently reducing the EMR and support EMC. Lastly, WiMAX provides a more robust security that employs encryption.

Disadvantages of WiMAX

The main drawback to the deployment of WiMAX is complicated equipment. WiMAX equipment must be able to utilize power efficiently in order to deliver optimum functionality. For WiMAX, the output power usage is based on a ranging process that determines the correct timing offset and power settings. This ensures that the transmissions for each military subscriber station arrive at the base station at the proper time and at the same power level. Consequently stations must have a quite big 50 dB transmit dynamic range in order to allow for stations that are close to the base station to back off their transmit power so that the far away ones can transmit. Secondly, WiMAX when deployed outdoors, in non-line of sight (NLoS) environments may encounter delay spreads of 5 to 10 s[39].

Comparison of mobile and fixed broadband

Both mobile and fixed broadband wireless networks are meeting the growing needs and demand for broadband services globally. The mobile wireless networks cater to mobile military users that need access to the network with a large operational area. The fixed wireless networks on the other hand can help meet the need for broadband services at the last km where traditional wired infrastructure does not suffice or is not cost effective but it is not acceptable within dynamic environment of military operations.

Conclusion

In conclusion, this paper provided a short overview of current and anticipated mobile and fixed broadband wireless networks from the main expectations of military applications. There is a strong growth in demand globally for mobility, data services, and ubiquitous computing within the military communicatios sytem. Mobile wireless solutions provided by the 3G and 4G networks enable wireless network access for highly mobile military users with handsets, laptops, and other wireless devices. Whereas, Wi-Fi and soon to be deployed WiMAX are helping military users meet the growing need for broadband wireless access at hotspots and beyond. However, there are issues such as standards, protocols, strengths and weaknesses of each technology and security that must be considered.

[39] Which can cause potential intersymbol interference over 50 or more data symbol intervals.

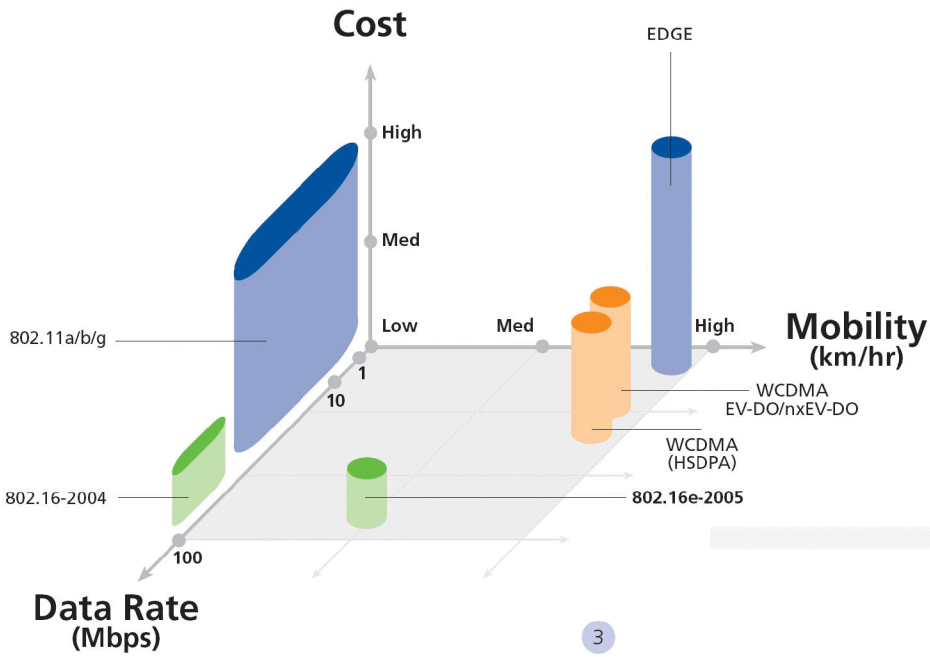


Fig. 3. Cost, Data Rate and Mobility comparison of Wireless Technologies [4]

It is seeming clear that the current years 2006-2009 will mark the true beginning of widespread deployment for mobile broadband. 3G/HSDPA-HSUPA and mobile WiMAX are seen as the main contenders in military applications. In the meanwhile, military user experiences and pilot systems continues to improve with upcoming enhancements on several levels. While the current 3G network architecture is well suited to handle voice applications and mobility, it is quite heavy for most data services. WiMAX-like flat network architecture would be more cost effective in many cases (Fig. 3.).

References

[1] Károly FEKETE: The benefits of high performance WIMAX solutions in multinational missions, Kommunikáció 2005 (Communications 2005) tudományos kiadvány, Budapest, 2005, ISBN 963 7060 11 1

[2] Károly FEKETE: Secure based wireless IP protocols with regard to closed networks, Kommunikáció 2005 (Communications 2005) tudományos kiadvány, Budapest, 2005, ISBN 963 7060 11 1

[3] TAKÁCS Péter: A WiFi hálózatok esetleges katonai felhasználásának lehetőségei, Kommunikáció 2007 (Communications 2007) tudományos kiadvány, Budapest, 2007, ISBN 978-963-7060-31-1

[4] Mobile WiMAX: Personal Broadband Services For Enhancing Lifestyles and Productivity, Alvarion Ltd., 2006, Ref No: 214424 rev.a, www.alvarion.com, pp. 1-12

[5] Samiseppo Aarnikoivu, Juha Winter: Mobile Broadband Wireless Access, Helsinki University of Technology, Telecommunications Software and Multimedia Laboratory

[6] Alcatel. 2005. WiMAX: From Fixed Wireless Access to Internet in the Pocket. White paper, http://www.alcatel.com/com/en/appcontent/apl/T0506-Wimax-EN_tcm172-262111635.pdf, referenced on April 13, 2006.

KERTI András

A POLGÁRI ÉLET ÉS A KATONAI INFORMÁCIÓBIZTONSÁG VISZONYA

Korunknak, az információs társadalomnak az egyik nagy, ha nem a legnagyobb kihívása az információk biztonságának megőrzése, az információ biztonságot meghatározó információ védelem megfelelő működtetése.

A különböző írott és elektronikus szaksajtóban naponta megjelennek az információbiztonsággal, annak megsértésével, kapcsolatos cikkek, adatok, incidensek leírásai. Azok az információbiztonsági incidensek, amelyek nagyobb mennyiségű adatokat, vagy a lakosságot jobban foglalkoztató információkat is érintenek pl.: banki csalások, adó adatok a napvilágra kerülése, stb… a napilapokban is szerepet kapnak.

A fentiek alapján nem véletlen, hogy az információbiztonság az egyik legdinamikusabban fejlődő szakterület. Majdnem mindegyik információbiztonsági szabvány, ajánlás megemlíti, hogy teljes biztonság nem létezik és nincs egy mindenek felett álló biztos módszer, de nem találni olyan szakcikket, amelyik a polgári élet és katonai információbiztonság kapcsolatát vizsgálná. Kell-e, lehet-e különbséget tenni a kettő közt? Az alábbi írásomban erre keresem a választ.

Az alapok

Az információvédelem legfontosabb alapelve a „Need to Know" elv vagyis minden információt az ismerhessen meg, akinek szüksége van rá; másik nézőpontból viszont ez azt is jelenti, hogy akinek jogosan szüksége van rá, az megismerhesse és ebben a jogában ne legyen korlátozva.

Az információvédelmi rendszabályoknak a célja, hogy statikus esetben, vagyis amikor az információt csak tároljuk, feldolgozzuk, de azt nem továbbítjuk, nem adjuk közre, egy közös munkához a jól ismert CIA tulajdonságok megőrzésére korlátozódik. Ezek:

Bizalmasság: olyan tulajdonság amely biztosítja, hogy az információt jogosulatlan személyek, vagy folyamatok számára nem teszik hozzáférhetővé, és nem hozzák azok tudomására.

Sértetlenség: Az információk pontosságának és teljességének védelmét biztosító tulajdonság.

Rendelkezésre állás: az információnak az a tulajdonsága, hogy a feljogosított személyek számára, amikor szükséges hozzáférhető és igénybe vehető legyen.

Az információ feldolgozás dinamikus esetében amikor, az információinkat, egy szélesebb körben, áramoltatjuk, esetleg egy közös platformon közös feldolgozásnak, szerkesztésnek vetjük alá, biztosítani kell még ezen felül a:

- Hiteleséget, a hitelesítést, amely egyrészt lehet az információ hitelesítése, vagy akár az információt szolgáltató, feldolgozó hitelesítése is. A hitelesítés az a folyamat. amely során kétséget kizáróan megállapítjuk, hogy az információt szol-

gáltató személy, szervezet, vagy eszköz kétséget kizáró módon az akinek, vagy aminek mondja (azonosítja) magát

- Az elszámoltathatóságot, ami azt jelenti, hogy a személy, vagy rendszer, mindig tudja hogy az információinkat mikor ki, ismerte meg és használta.
- Letagadhatatlanságot, amit a rendszer akkor biztosít, ha bizonyítékot szolgáltat arról, hogy a másik fél az általunk átadott információkat, bizonyítható módon megkapta.
- Megbízhatóságot, ami a rendszernek azon tulajdonsága, hogy folyamatosan a tőle elvárt módon üzemelnek.

Amennyiben elolvassuk az információbiztonsággal foglalkozó szabványokat, az Európa Tanács biztonsági szabályzatát, illetve az információ biztonsággal foglalkozó jogszabályokat, és összehasonlítjuk azokat megállapíthatjuk, hogy a biztonsági alapelvek mindegyikben azonosak.

Miért kell védenünk az információkat?

Az üzleti életben az információk kiszivárgása, sérülése az üzleti eredményt, a profitot csökkentheti, rosszabb esetben tönkre is mehet a vállalkozás. A katonai életben egy feladat kudarcához vezethet és ez a katonák életét is veszélyeztetheti. A mindkét fajta szervezetnél tehát alapvető érdek az információk védelme.

Minden bevezetett információbiztonsági előírás betartása azonban egyrészt gát az információ áramlás útjában, másrészt pénz kiadás is. Azért, hogy a megfelelő szintű védelmet biztosítsuk a rendszereinknek, de ne essünk túlzásokba, alapos kockázat elemzést kell végrehajtani mindkét szektorban. A kockázat elemzés során azonosítani kell a vagyontárgyakat, amelyek az információ feldolgozó rendszer elemei és a kezelt információk, meg kell határozni a fenyegetéseket, fel kell tárni a sebezhetőségeket, és meg kell állapítani az elfogadható kockázat szintjét. A kockázat elemzés után meg kell határozni az információbiztonság érdekében foganatosítandó cselekvéseket.

A fenyegetések szinte teljesen azonosak mindkét esetben, a különbség véleményem szerint annyi, hogy a katonai szektor információira nagyobb veszélyt jelentenek egy másik állam által támogatott titkos szolgálatok, és hogy a katonai akciók, mint például a missziók, sokkal ellenségesebb környezetben folynak.

A vagyontárgyak esetében gyakorlatilag nincs különbség az informatikai eszközökben, viszont az információk osztályozási szempontja szerint igen. Az üzleti életben az információk osztályozásának elve a vállalkozás számára kifejezhető előny, illetve elvesztésük esetén okozott kár nagysága, ennek érték, ha nem is egyszerűen, de kifejezhető pénzben.

A katonai információk esetében, sokkal nehezebb meghatározni az értéket, pénzben még nehezebben lehet kifejezni az esetleges kárt, és az osztályozás elsődleges szempontja az információk minősítése. A kockázat elemzést végző szervezetnek nem áll módjában az információ minősítésének, a minősítéssel kifejezett

értékének, megváltoztatása, kibocsátó beleegyezése nélkül. A sebezhetőségek megállapításánál az üzleti életben, sokkal nagyobb szerepet kaphat az informatikai információs rendszer leállása, mint az információk szivárgása, ugyanis az informatikai rendszer leállása az egész termelési folyamat leállását is jelentheti. A katonai életben, kifejezetten a „hadműveleti" területen, pont fordított lehet a helyzet. A kiszivárgott információk okozhatnak nagy veszteségeket. A polgári életben teljesen nyílt információ, mint például, hogy hol helyezkedik el egy leányvállalat, a hadszíntéri információra átfordítva, hogy helyezkednek el a különböző katonai egységek, akár titkosak is lehetnek. Kitudódásuk, az egész művelet egészét veszélyeztethetik. A katonai informatikai rendszer leállása szintén nagy problémát okozhat, de csapatok vezetése más módszerekkel is megoldható. Elvileg.

Szintén különbözik a két szektor abban, hogy milyen előírásokat vesz figyelembe az információ biztonsági rendszerének kialakításakor. Az üzleti élet szereplői választhatnak, a meglévő ajánlások és szabványok bevezetése között, a katonai szervezetek, bár figyelembe vehetik ezeket a szabványokat és ajánlásokat, a jogszabályokban leírtak a mérvadók számukra. Ez a tény, az ellenintézkedések megválasztásakor kap fontos szerepet, ugyanis egy vállalat a kockázat elemzésből kiindulva, annak eredményére támaszkodva saját maga alkothatja meg a minimális követelményeket és az elfogadható kockázat mértékét. Ebből fakadóan két ugyan olyan cég fizikai biztonságának a kialakítása teljesen más lehet a különböző földrajzi körülmények között. A katonai esetben, az azonos minősítési szintű információk fizikai biztonságát meghatározó jogszabálytól[40], csak nagyobb biztonságot jelentő intézkedések bevezetésével lehet, függetlenül attól, hogy mennyire biztonságos is az adott terület.

Az információs rendszerek összehasonlítása

Ahhoz, hogy a bevezetésben feltett kérdést meg tudjuk válaszolni, meg kell vizsgálnunk, magát az információs rendszert is. A polgári életben a vállalatok információs rendszerét két komponensre tudjuk bontani:

Valamilyen, az élőszóban közölt információk átvitelére alkalmas telefonhálózat, amelynek lehetnek külső és belső kapcsolatai is. A külső kapcsolatok lebonyolítására egyre inkább a mobil telefonok jönnek szóba.

Valamint a digitális információk feldolgozására, továbbítására alkalmas számítógépes hálózatok. Természetesen a két fajta rendszer között egyre kevesebb az eltérés, gondoljunk csak a VoIP telefonokra.

Megítélésem szerintem nagyon lényeges, hogy nagyon kevés olyan vállalat van, amely a két, vagy több telephelye közötti kapcsolatait, a saját hálózatán keresztül bonyolítja. Erre egy külső szolgáltató céget, telefontársaságot, internet szolgáltatót vesznek igénybe.

A katonai információs rendszer is nagyon hasonló képet mutat, a különbség csak az, hogy a katonai információs rendszerek rendelkezhetnek olyan külső, vagy

[40] Pl.: 179/2003 sz. kormány rendelet.

nagyobb távolságot áthidaló kapcsolatokkal, amelyek létesítésért, fenntartásáért a katonai alakulat felel. Ilyen közvetlen összeköttetések lehetnek vezetékes, és kisugárzó eszközökkel megvalósított összeköttetések. Számítógép-hálózatok esetében a módszerek szinte teljesen megegyeznek. A lényeges különbséget csak abban látom, hogy azon katonai rendszerekben, amelyekben minősített információkat kezelnek, csak olyan eszközök, hardware és software alkalmazhatók, amelyeket valamelyik hivatalos biztonsági szervezet (Pl: NSA) akkreditált. Ez igazából nem azt jelenti, hogy ezek jobbak mint a nem akkreditált társaik, hanem, hogy a gyártóik vállalják a számukra előírt biztonsági szabályok bevezetését, fenntartását és ellenőrzését.

Visszatérve a közvetlen összekötetésekhez, amelyeket különösen akkor használnak, ha valamely feladatot –*gyakorlatot, missziót stb.* – hajtanak végre a csapatok, elmondhatjuk, hogy az ezekhez az összeköttetésekhez tartozó információ védelmi feladatok ismeretlenek a legtöbb polgári cég számára. Milyen plusz feladatot róhat a közvetlen összeköttetések megléte az információbiztonságra? Az információk biztonságát, a sértetlenséget, a rendelkezésre állást, a bizalmasságot az átviteli út során is biztosítani kell. Szintén biztosítani kell ebben az esetben, az információk hitelességét, valamint a letagadhatatlanságot. Ezek a feladatok csak akkor hajthatók végre maradéktalanul, ha tervező állomány tisztában van az összeköttetések tervezésének követelményeivel, az elektromágneses hullámok terjedési sajátosságaival, az elektromágneses kompatibilitás rendszabályaival.

Az információk hitelesítését mindkét információs rendszerben meg kell oldani, távoli információforrás esetében. A civil életben egyre inkább erre az aszimmetrikus rejtjelzésen alapuló digitális aláírással valósítják meg. Természetesen a nyílt kulcsú infrastruktúra szintén rohamosan fejlődik a katonai rendszerekben, de kifejezetten a közvetlen összeköttetések eseteiben alkalmazásban vannak még a szimmetrikus megoldások is. Ilyen szimmetrikus megoldások lehetnek az azonos forgalmi adatok, ismertetőjel kérés-adás, azonos szimmetrikus rejtjel kulcsok.

Összegzés

Mind a civil, mind a katonai életben, egyre nagyobb szerepet kap az információ biztonság. Teljes biztonság nincs csak tudatosan elfogadott szintű kockázatvállalás. Szintén nincsen kizárólagosan kijelölhető a többinél jobb információbiztonsági módszer. Hogy mik a különbségek a polgári cégek és a katonai információ biztonság között a cikkemben meg vázlatosan megvizsgáltam. A következtetéseimet az alábbi táblázatban foglalom össze:

Az információbiztonsági területek:	Polgári információbiztonság	Katonai információbiztonság
Az információbiztonsági alapelvek	Megegyeznek nincs eltérés	
Átviteli út biztonság	A szolgáltató felelőssége	A saját kiépítésű rendszerekben külön intézkedéseket kíván.
Kockázatkezelés	A kockázat elemzés alapján.	Az előírásoktól csak a szigorúbb rendszabályok felé lehet eltérni.
A szabályzók rendszere	Ajánlások szabványok, nem kötelező őket alkalmazni.	Jogszabályok, és más kötelező érvényű előírások
Hitelesítés	Alapvetően aszimmetrikus módszerekkel	Szimmetrikus, és aszimmetrikus módszerek is lehetnek.
Információk minősítése	Üzleti titok	Szolgálati és államtitok
Hálózatbiztonság	Alapvetően ugyan az	A minősített információkat feldolgozó rendszerekben csak hatóságilag engedélyezett eszközök használata lehetséges.

Felhasznált irodalom:

[1] MSZ ISO/IEC 27001:2005 Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények.

[2] MSZ ISO/IEC 13335 Informatika. Az informatikai biztonság menedzselésének irányelvei.

[3] Az Európai Tanács Határozata (2001. március 19.) a Tanács biztonsági szabályzatának elfogadásáról (2001/264/EK)

[4] 179/2003. (XI. 5.) kormány rendelet, a nemzetközi szerződés alapján átvett, vagy nemzetközi kötelezettségvállalás alapján készült minősített adat védelmének eljárási szabályairól

BLEIER Attila

MAGYAR HONVÉDSÉG ELVÁRÁSAI ÉS A XXI SZÁZAD KIHÍVÁSAI

Bevezetés

A hadviselés 90-es évektől kezdődően komoly változáson megy keresztül. A második hullámú anyagközpontú hadviselésből folyik az áttérés a harmadik hullámú (negyedik generációs) információs hadviselésre. Erre a váltásra a NATO komoly hangsúlyt fektet, és ez megjelenik a Magyar Honvédség Összhaderőnemi doktrínában is mint hangsúlyos kérdés, valamint a 2007-2016 közötti hosszú távú fejlesztési tervekben is.

Az alábbi anyagban arra keressem a választ, melyek azok a kihívások amiknek a Magyar Honvédség hírrendszere – azon belül is kiemelten az állandó hírrendszere – meg kell , hogy feleljen, mert ezek határozzák meg azokat az irányvonalakat amelyek mentén a kutatásomat végeznem kell. Ezen belül kiemelten kezelem (a harmadik fejezetben) a Magyar Honvédség Összhaderőnemi Doktrínáját. Az utolsó fejezetben egy összegzésben foglalom össze az anyagban szereplő fontosabb észrevételeimet.

XXI sz. kihívásai

Az ezredfordulóra a NATO a világ legnagyobb katonai szövetségi rendszerévé vált, ezzel együtt felvállalva azt is , hogy adekvát választ ad az ezredforduló katonai-politikai jellegű kihívásaira is. Ezen kihívások között a legfontosabbak a terrorizmusra adott megfelelő válasz, illetve az infokommunikációs technológiák fejlődésével a hadviselés, és a hadseregek átalakítása mily módon történjen. Az előbbi kérdésre (terrorizmust illetően) ez az anyag nem tér ki, az anyag elsősorban az utóbbi kérdés magyar vonatkozásaival foglalkozik.

A negyedik generációs hadviselés

A XX-sz. végén megjelent az Öböl-háborúkkal a hadviselés egy új formája (az ún. negyedik generációs hadviselés) , ahol a kulcsponti kérdés, az információs fölény megszerzése lett. Az információs fölény megszerzése azért fontos, mert amennyiben az információs fölényben van az adott hadviselő fél, az előnyt jelent a döntéshozóknál – és döntési fölényben jelentkezik. A megfelelő információ birtokában, jobb döntéseket lehet hozni, és ez meghatározó kimenetelű lehet az ütközet kifejletére.

Ezért elsődleges fontosságú az információs fölény megszerzése és fenntartása a jelen és a jövő háborúiban/válsághelyzeteiben. A kérdés az, hogy milyen módszerekkel, és eszközökkel tudjuk az információs fölényt kialakítani és fenntartani. Ez a kérdéskör, az információs hadviselés témaköre, amelynek egyik súlyponti oldala, a híradó / kommunikációs célú információs fölény kiépítése és fenntartása napjaink egyik hadtudományi/katonai műszaki oldalról leginkább kutatott területe.

A katonai alkalmazások követelményei a hírrendszerrel kapcsolatban

A NATO Network Enabled Capabilities doktrínájával hangsúlyossá válik a katonai informatikai és információs rendszerek alkalmazása. Ilyen rendszerek például az amerikai hadseregben a WWMCCS, GCCS, NMCS – vezetés irányítási rendszerek, ill. JOPES Összhaderőnemi hadművelet-tervező rendszer; a brit hadseregben az IARCCIS és THISTLE, a német haderőnél a HEROS vezetésirányítási rendszer, az ADLER tüzérségi informatikai rendszer és az EIFEL a német légierő informatikai rendszere, a francia haderőnél a SGEA és STRIDA. [Munk pp.131-164]

Ezek a rendszerek megkövetelik a híradó infrastruktúra felülvizsgálatát. A korábbi „hang-központú" megközelítés az új informatikai és vezetésirányítási rendszerek igényeit nem elégítik ki, hiszen ezek nagy mennyiségű adatforgalmat generálnak. Új információ központú, megközelítés szükséges, és a híradó rendszereket is ebben a felfogásban szükséges felújítani, modernizálni. Ez természetes nem jelenti, nem jelentheti azt, hogy a hagyományos rendszereket egyik napról a másikra szüntessük meg, hanem egy migrációs út szükséges a jelenlegi állapotból az elérendő végcél irányába.

A katonai információs rendszerben végbenő változások másik fontos irányvonala a különböző jellegű adatok és információs rendszerek integrációja – amely az egyes rendszerek között szorosabb együttműködést követel meg. Ezek természetesen együttműködési (szakszóval interoperabilitási) problémákat hoznak magukkal, amiket le kell küzdeni. Ez is abba az irányba mutat, hogy a különféle szolgáltatást biztosító rendszereket, így a hangátviteli rendszereket ill. informatikai rendszereket ne különálló rendszerekként kezeljük, hanem olyan rendszerelemekként, amelyek az erőforrások egy bizonyos halmazát képesek nyújtani. Ez egy új megközelítést igényel (ahol erőforrások adottak) és a híradórendszer (kommunikációs rendszer) szolgáltatásokat nyújt a (hálózati) erőforrásokon keresztül. Ez összhangban van a NATO Network Enabled Capabilities doktrínájában megfogalmazott elvekkel. [Munk pp. 96-99]

További kihívást jelent a hosszabb távon a Network Centric Warfare (Hálózatközpontú hadviselés) elterjedése – ami szintén része a NATO doktrínának. Itt megjelenik az a koncepció, hogy a katonai hálózatban egészen a végrehajtó egységekig minden egység, egy (IP alapú) kommunikációs hálózatba szervezett, így a különböző szintű döntéshozók, gyakorlatilag ugyanazokkal az információkkal rendelkeznek, mint a végrehajtó egységek. Ez komoly követelményeket ró, mind a harctéri, mind a tábori , mind pedig az állandó hírrendszerre.

A harctéri hírrendszer alkalmazása sokkal szélesebb körű kell, hogy legyen mint a jelenlegi helyzetben, hiszen nagyon sokféle és különböző jellegű információkkal segítheti ez a csapatvezetést. Pl. a különböző életfunkciókat figyelő szenzorok, folyamatos jelentést küldhetnek a katona állapotáról a döntéshozó, ill. az egészségügyi támogató csapatoknak, vagy a páncélozott járműveknél a különböző szenzorok küldhetnek állapotjelzéseket a a jármű műszaki állapotáról a műszaki támogató csapatoknak. Megjelenhet, az élő képi jelek küldése közvetlenül a végrehajtó csapatoktól. Ezek természetes mind, mind megfelelő minőségi követelményeket rónak a hálózatra, a különböző adatokat, különböző prioritással , különböző jellemzőkkel szükséges kezelni, mind a harctéri, mind a tábori, illetve az állandó

hírrendszerben. Pl. ezen aggregált forgalmak, az állandó hírrendszerben a jelenleg használatos sávszélességek, és technológiák többszörösét, és új kezelését igénylik.

A mobilitás növelése is fontos, elsősorban a tábori, és a harctéri hírrendszer esetében, ahol az új technológiák mint pl. Wimax elterjedése várható, de az is várható , hogy bizonyos esetekben az EDR [PÁNDI2007] ill. civil mobil technológiák veszélyhelyzeti alkalmazása [MAROS2005, MAROS2006], így pl. a civil GSM hálózatok minősített helyzetben való alkalmazása kívánatos. Ezen technológiák közös előnye, hogy gyorsan, a helyzetnek megfelelően bevethetőek, hátrányuk, hogy – elsősorban az optikai szálas vezetékes technológiákkal szemben – nagyságrendekkel kisebb sávszélességet biztosítanak.

További fontos követelmény a megbízhatóság, a rendelkezésre álló sávszélesség, mind a stacioner mind a tábori hálózatban, illetve a hálózat tűrőképességének növelése.

A Magyar Honvédség Összhaderőnemi Doktrínája és a kutatási terület kapcsolata

A Magyar Honvédség követendő irányvonalát az érvényben lévő Összhaderőnemi Doktrína határozza meg, 2003-ban lett elfogadva, jelenleg a felülvizsgálata folyik, a változások az év végére jövő év elejére várhatóak. Az új doktrínában várhatóan hangsúlyosabb szerep jut a híradó és informatikai résznek, azonban ebben a fejezetben a várható módosítások még nem szerepelnek. Ebben a fejezetben azt fogom tárgyalni, hogy mik azok az elvárások, ill. mi az az irányvonal, amelyet az érvényben lévő Összhaderőnemi Doktrína a kutatási területemre (a Magyar Honvédség állandó hírrendszerének modernizálására) vonatkozólag meghatároz.

Az Összhaderőnemi Doktrína definiálja, hogy melyek azok a feladatok amire a Magyar Köztársaság fegyveres erőinek fel kell készülniük: „Az MK fegyveres erőinek készen kell állniuk mind a hagyományos katonai védelemi feladatokra, mind pedig azoknak a konfliktusoknak a megoldására, amelyek közvetetten érintik országunk és szövetségeseink biztonságát és veszélyeztetik szűkebb vagy tágabb környezetünk stabilitását." [ÖHD pp.11] Ennek fényében kell vizsgálnunk a továbbiakban MH híradó és informatikai rendszerét, amely tehát két feladatra kell, hogy felkészüljön: „védelmi feladatokra" (elsősorban stacioner hálózat), ill. válságkezelő feladatokra (elsősorban tábori hálózat).

Az Összhaderőnemi Doktrina, azt is meghatározza, hogy mik azok fenyegetések, ill. konfliktusok, amikre fel kell készülnünk. A doktrína elsődleges fenyegetésként nevezi meg a nemzetközi terrorizmus megerősödését, így mind a stacioner, mind a tábori hálózatot úgy kell kialakítani, hogy erre a fenyegetésre megfelelő választ tudjon adni.[ÖHD pp.11] .

A doktrína a híradó és informatikai rendszert, a harci támogató erők közé sorolja. [ÖHD pp. 17], ennek kapcsán két fogalmat kell tisztáznunk: a harci támogatás fogalmát, ill. a támogatott és támogatói viszonyt. Az előbbit így definiálja: „A harci támogatás tartalma a harci erő támogatása, ami a támogatott harci egység feladata végrehajtásának felderítési adatokkal illetve tűzzel való támogatását, manővere végrehajtásának szabadságát és az ellenség mozgásának korlátozását, a szárazföldi erő légvédelmét, a tömegpusztító fegyverek elleni védelmet, az elekt-

ronikai-, információs-, a vezetési-irányítási-, lélektani hadviselést, valamint a polgári-katonai együttműködést, és a tömegtájékoztatást foglalja magában"[ÖHD pp 27]. Mint láthatjuk az adattal való támogatást a doktrína, kulcsfontosságúan kezeli közvetlenül is, és közvetetten is az elektronikai- információs-,vezetés-irányítási- ill. lélektani hadviselés kapcsán is (amelyekben az infokommunikációs rendszerek szintén fontos szerepet kapnak. Az adattal való támogatás szerepének felértékelődése, valamint az elektronikai-, információs- hadviselés megjelenése a korábbiakban megjelent információs fölény kialakításához szükséges. Ez a feladat komoly szerepet ró a Magyar Honvédség híradó és informatikai rendszerére.

A másik fontos dolog amiről a harci támogatás kapcsán az Összhaderőnemi Doktrína említést tesz, az a Támogatott és támogatói viszony [ÖHD pp. 28-29]. Tehát az Összhaderőnemi Doktrína, meghatározza az irányelveket – az „ún." támogatási szolgáltatásra vonatkozóan. Ennek a továbbgondolása lehet az a támogatási vagy szolgáltatási szintet definiáló megállapodás, amelyekre a további fejezetekben részletesen ki fogok térni.

Az Összhaderőnemi Doktrínában több helyen hangsúlyos szerepet kap a híradó és informatikai rendszert. Pl. A vezetési pont definíciójában is (értelemszerűen) fontos szerepet kap, amely szintén mutatja azt a kiemelt szerepet, amit a döntéshozatali folyamatban, a döntési fölény kialakításakor játszik[ÖHD pp.46], ill. felderítő információgyűjtő,feldolgozó és tájékoztató központ kapcsán is jelentős szerepet kap az információ továbbítása, amely elsősorban a híradó infrastruktúrán kell, hogy megtörténjen.

Az ÖHD 11.fejezete foglalkozik kiemelten a híradó és informatikai rendszerrel, amelyet az ÖHD így határoz meg: „a különböző vezetési szintek tevékenységéhez szükséges, rugalmasan változtatható, egységes elvek, módszerek és tervek alapján létrehozott; feladat, hely és idő szerint koordinált híradó és informatikai eszközök, eljárások, valamint az információs tevékenységeket végrehajtó szakállomány összessége." [ÖHD pp.87] Az ÖHD a híradó és informatikai rendszert, mint egységes egészet definiálja, összhangban a NATO elfogadott doktrínájával – ez egységes szervezeti felépítést sugall. Fontos észrevenni, hogy az információs tevékenységeket (tágabb értelemben az információs műveleteket) végrehajtó személyeket az híradó és informatikai rendszer részének tekinti.

A híradó és informatikai rendszerrel szemben az Összhaderőnemi Doktrínában az alábbi követelmények fogalmazódnak meg amelyet három fő csoportban ismertetek:

Működtetés, a fejlesztést, a meglévő rendszerekkel való integrációt támogató követelmények: szabványosság, kompatibilitás, interoperabilitás, felcserélhetőség, azonosság. Ezen követelmények azért fontosak, hogy a Magyar Honvédség rendszere egységes legyen, amely üzemeltetési és fejlesztési előnyökkel jár. (Üzemeltetési előnyök pl. : kisebb tartalékot kell képezni, kisebb az rendszerbeillesztés, a betanítás/oktatás költsége, könnyebb megoldani a támogató személyzet helyettesítését és a személyeknek is kevesebb gyártófüggő szabványt, kell megtanulniuk, a rendszerek egymással való helyettesítése is könnyebb, a rendszerek cseréje, és fejlesztése szempontjából is ezek előremutató szempontok)

A speciális katonai alkalmazásból eredő, nagy rendelkezésreállást és gyors bevethetőséget segítő követelmények: Reagáló képesség, Megbízhatóság, szilárdság,

időbeniség, rugalmasság, mobilitás. Ezen követelmények a katonai alkalmazás speciális igényei. Ehhez hasonló rendszerkövetelményeket a polgári infokommunikációs rendszerekben a távközlési szolgáltatóknál is találunk, ezért is fontos, hogy a polgári életben az infokommunikációs szolgáltatóknál használt elvek, megjelenjenek a Magyar Honvédségnél is.

Információbiztonsággal összefüggő követelmények:hitelesség, biztonság, rejtettség, elektronikai információvédelem. Ez a kormányzati ill. katonai szférában speciális követelmény, amelyre kiemelt figyelmet kell fordítani (és a Magyar Honvédség jelenleg is kiemelt figyelmet fordít).

Az Összhaderőnemi Doktrína meghatározza békében, minősített időszakban ill. háborúban a híradó és informatikai rendszerét. Békében alapvetően békeállománnyal, a MH állandó jellegű hálózatain üzemeltetett rendszer, amelynek képessége elégséges a békevezetés, irányítás, kiképzés és fenntartás teljesítéséhez. A rendszernek képesnek kell lennie, minősített időszak, válságreagáló és katasztrófa helyzetek megoldására, ill. a készenlét fokozásával a tábori híradó és informatikai rendszerek csatlakoztatására. A válságreagáló műveletek, és NATO kötelezettségeink kapcsán felmerülő fontos szempont a nemzetközi rendszerekhez való csatlakozásnak képessége. Háborúban, ugyanezen a bázison képesnek kell lennie az összhaderőnemi tervezés, vezetés támogatására, ill. a NATO védelmi erők támogatására. [ÖHD pp. 87-92]

Az Összhaderőnemi doktrína legfontosabb vezérelvként említi, hogy az a felhasználó tevékenységének támogatására legyen megtervezve: polgári szóval élve, legyen felhasználóbarát, alkalmazási képesség szempontjából pedig az a legfontosabb irányelv, hogy háborús alkalmazásra legyen megtervezve.[ÖHD pp. 87-92]

Korábban már említettük, hogy a Magyar Honvédség Összhaderőnemi Doktrínája az információs műveleteket végző személyeket a híradó és informatikai rendszer részének tekinti, így az információs műveletekként definiált feladatok a híradó és információs rendszer részét kell, hogy képezzék, az információs műveletekkel a Doktrína 12. fejezete foglalkozik. [ÖHD 93-97]

Az infokommunikációs rendszer megjelenik (v. távközlési v. híradó és informatikai rendszerként) megjelenik az információs műveletek, a védelmi és támadó információs műveletek fogalmának definíciójánál is. Ez az a területe a hadviselésnek amely dinamikusan fejlődik, és a NATO haderőknél egyre hangsúlyosabb szerepet kap. Az információs műveletek katonai tevékenységei és képességei meghatározásánál kiemelt rész foglalkozik a távközlési (híradó) és információs rendszerekkel, és hangsúlyozza a doktrína, hogy a vezetési és irányítási hadviselés alapelvei nagy mértékben függnek az időbeni és pontos információktól, kritikusak a hadműveletek sikeres végrehajtásánál. A híradó központokat a doktrína kritikus csomópontként definiálja, melynek elvesztése azonnal csökkentheti a vezetési irányítási képességet. [ÖHD pp. 97]. Ennek megfelelően az állandó jellegű és tábori hírközpontok mindennemű támadástól való védelme elsődleges fontosságú.

A híradó és informatikai rendszerrel összefüggő az Összhaderőnemi Doktrínában definiált Elektronikai hadviselés is. [ÖHD 109-112] Az elektronikai hadviselés kiemelt célpontjai a híradó és informatikai rendszerek, ezért az elektronikai hadviseléssel szembeni védelem, kiemelt fontosságú a híradó és informatikai rendszerek

kialakításakor. A híradó és informatikai rendszer megjelenik még több más vonatkozásban is az Összhaderőnemi Doktrínában, erre azonban itt most nem térek ki.

Mint láthatjuk, az előző fejezetben vázolt alapelveket: a rendszerintegráció képességét, az információs műveleteket, a mobilitást a Magyar Honvédség érvényben lévő Összhaderőnemi Doktrínája is súlyponti kérdésekként kezeli. Ugyanakkor látnunk kell, hogy a NATO vezető katonai hatalmai, a fontosabb szerepet szánnak a híradó és informatikai rendszernek pl. az információs műveletek, vagy a stacioner, tábori és harctéri kommunikáció terén. Ezen változások remélhetőleg az új, átdolgozott doktrínába be fognak kerülni.

Összegzés

Az új évezred, új kihívásokat hozott mind a nemzetközi mind a hazai katonai infokommunikációs rendszerek számára. Ezen legfontosabb kihívások között az áttérést harmadik generációs, információ-központú hadviselésre történő áttérést, az egyre szélesebb körben használt katonai információs és kommunikációs rendszerek megfelelő kiszolgálását, ill. az új katonai infokommunikációs koncepciók támogatását emeltem ki a bevezetést követő első fő fejezetében (második fejezet).

A harmadik fejezetben arra kerestem a választ, hogy az Összhaderőnemi Doktrína milyen követelményeket, milyen elvárásokat támaszt a szűkebb kutatási területem - Magyar Honvédség híradó és informatikai rendszerével kapcsolatban, ill. mennyire felel meg, tartalmazza a választ azon kihívásokra, amelyet az első fejezetben megfogalmaztam.

A fejezetben, kiemeltem, hogy az Összhaderőnemi doktrína a Magyar Honvédség híradó és informatikai rendszerét, mint egy harci támogató rendszert fogalmazza meg, és új megközelítés lehetőségét vetettem fel a támogató-támogatott viszonyt illetően – mellyel részletesebben a következő fejezetben foglalkoztam. Meghatároztam a főbb irányvonalakat (rendszerintegrációs, katonai műszaki, és biztonsági, információvédelmi) irányvonalakat amelynek mentén a híradó és informatikai rendszerrel szemben elvárt követelményeket meghatározták. Az Összhaderőnemi Doktrína alapján meghatároztam azon irányelveket, amelyek mentén a híradó és informatikai rendszert ki kell, kellett alakítani. Felhívtam a figyelmet, hogy a doktrína az információs műveleteket is a híradó és informatikai rendszer feladataként jellemzi.

Az Összhaderőnemi doktrína meghatározta azon irányelveket, amelyek mentén a Magyar Honvédség híradó és informatikai rendszerét tervezni, kivitelezni és üzemeltetni szükséges. Ezen irányelvek lehetővé teszik polgári életben használt nagy rendelkezésre állású hálózatok tervezéséhez, kivitelezéséhez és üzemeltetéséhez használt módszerek és eszközök használatát, amennyiben a katonai alkalmazásból adódó speciális követelményeket figyelembe vesszük.

Rövidítésjegyzék

WWMCCS – World-Wide Military Command and Control System (Világméretű katonai vezetési rendszer)

GCCS – Global Command and Control System (Globális vezetési és irányítási rendszer)

NMCS – National Military Command System (Nemzeti katonai vezetési rendszer)

JOPES – Joint Operation Planning and Execution System (Összhaderőnemi hadművelet-tervező és végrahajtó rendszer)

IARCCIS – Interim ACE Rapid Reaction Corps Information System (ACE Gyorsreagálású hadtest átmeneti informatikai rendszere)

HEROS – Heeres Führunginformations System (für die rechnerunterstützte) Operationsführung in Staeben (Csapatvezetési információs rendszer, hadműveleti vezetés a törzsekben)

ADLER – Artillerie-, Daten-, Lage- und Einsatz-Rechner (Tüzérségi, adat, helyzet és bevetési számítógép hálózat

SGEA - Systéme de Guerre Électronique de l'Avant (Elektronikai hadviselési rendszer)

STRIDA – Systéme de Traitment et de Représentation des Informations de Défense Aérienne (Légvédelmi információk kezelésének és megjelenítésének rendszere)

TDM – Time Division Multiplex (Időmultiplexált)

IP – Internet Protocol (Internet Protokoll)

QoS - Quality of Service (Szolgáltatásminőségi paraméterek)

SLA – Service Level Agreement (szolgáltatási szint szerződés)

BER – Bit Error Rate (Bithibaarány)

round trip delay – az a késleltetési idő amíg egy IP csomag egy útvonalat oda – vissza megjár

MPLS – Multiprotocol Label Switching – többprotokollos címkekapcsolás

ZMNE – Zrínyi Miklós Nemzetvédelmi Egyetem

IETF – Internet Engineering Task Force – szabványügyi szervezet

IEEE - Institute of Electrical and Electronics Engineers, Inc – szabványügyi szervezet

ITU – International Telecommunication Union – szabványügyi szervezet

ETSI – European Telecommunication Standard Institute

Wimax - Worldwide Interoperability for Microwave Access – Vezetéknélküli adatátviteli szabvány

UMTS – Universal Mobile Telecommunication System – 3-dik generációs mobiltelefonia szabványrendszere

STANAG - Standardization Agreement – NATO szabvány

NATO – North Atlantic Treaty Organization - Nemzetközi védelmi szövetség

AARMS - Academic and Applied Research in Military Science – ZMNE nemzetközi folyóirata

Felhasznált Irodalom

[1] Kommunikáció 2005 I.-II., Communications 2005 I.-II., 2005/10 Zrínyi Miklós Nemzetvédelmi Egyetem, Zrínyi Miklós kiadó, Budapest, p. 601 ISBN 963 7060 11 1

[2] Kommunikáció - 2006, Communications - 2006, 2006/10 Zrínyi Miklós Nemzetvédelmi Egyetem, Zrínyi Miklós kiadó, Budapest, p. 391, ISBN 978-963-7060-18-2

[3] Kommunikáció 2007 I.-II., Communications 2007 I.-II., 2007/10 Zrínyi Miklós Nemzetvédelmi Egyetem, Zrínyi Miklós kiadó, Budapest, p. 511, ISBN 978-963-7060-31-1

[4] Dr. Munk Sándor: Katonai informatika a XXI. század elején, 2007, Zrínyi Kiadó, p. …ISBN: 978 963 327 419 4

[5] dr. Rajnai Zoltán, dr. Fekete Károly: Tanulmány a Wimax használhatóságáról a Magyar Honvédség hírrendszerében, 2007

[6] dr. Haig Zsolt: Információs műveletek I-II jegyzet, 2008

[7] dr. Haig Zsolt, dr. Vass Sándor, dr. Ványa László: Elektronikai Hadviselés, 2008

[8] dr. Haig Zsolt: Integrált felderítés és elektronikai hadviselés, jegyzet, 2008,

[9] http://www.wikipedia.org

[10] [MAROS2005] Maros Dóra, Mészáros Árpád, Kommunikáció 2005 I.-II., Communications 2005 I.-II., 2005/10 Zrínyi Miklós Nemzetvédelmi Egyetem, Zrínyi Miklós kiadó, Budapest, p. 601 ISBN 963 7060 11 1,pp.203-209

[11] [MAROS2006] Maros Dóra, Kommunikáció - 2006, Communications - 2006, 2006/10 Zrínyi Miklós Nemzetvédelmi Egyetem, Zrínyi Miklós kiadó, Budapest, p. 391, ISBN 978-963-7060-18-2 , pp. 154-168

[12] [PÁNDI2007] Pándi, Erik, Pándi , Balázs, Kommunikáció 2007 I.-II., Communications 2007 I.-II., 2007/10 Zrínyi Miklós Nemzetvédelmi Egyetem, Zrínyi Miklós kiadó, Budapest, p. 511, ISBN 978-963-7060-31-1, pp.254-260.

[13] [ÖHD] A Magyar Honvédség Összhaderőnemi Doktrínája, 2003-as kiadás

[14] [Munk] Dr. Munk Sándor: Katonai informatika a XXI. század elején, 2007, Zrínyi Kiadó, p.264,ISBN: 978 963 327 419 4

PÁNDI Balázs – PÁNDI Erik41

AZ ÉSZAK-ATLANTI SZERVEZETET KISZOLGÁLÓ KOMMUNIKÁCIÓS RENDSZEREK JELLEMZŐI

Absztrakt: a publikációban a szerzők áttekintik az Észak-Atlanti Szerződés Szervezete távközlési és információs rendszerének (NCIS) lényegi elemeit a NATO Hálózat Nyújtotta Képességek (NNEC) tükrében, célul tűzve ki a hazai tábori hírrendszer sikeres átalakításához való hozzájárulást.

Kulcsszavak: C4I, hálózatközpontú hadviselés, műholdas távközlés, NATO, NCIS, NNEC, tábori hírrendszer.

1. Az NCIS

Az NCIS nem más, mint a NATO vezethetősége biztosításának érdekében létrehozott és működtetett távközlési és információs rendszer. A NATO hozzávetőleg negyven évvel ezelőtt fejlesztette ki e széles körben alkalmazott infrastruktúráját. Működésének lényege, hogy a telepített elemek segítségével kapcsolatot teremt a hadászati szint és a magasabb egységek harcászati mélysége között. A rendszer egyes elemei alapvetően a következőképpen csoportosíthatók [1]:

a) távközlési műholdak;
[15] b) mobil rendszerű távközlési műholdak;
[16] c) nemzetközi haditengerészeti távközlési műholdak;
UHF – harcászati távközlési műholdak;
MAXIMA;
automatikus üzenettovábbító rendszer;
hangátvitelre alkalmas kapcsolt távbeszélő hálózat;
adatátviteli alapszolgáltatás;
integrált digitális hálózati kapcsolóközpont;
PROMINA;
[17] k) videókommunikációs rendszer;
egyéb adatátviteli rendszerek.

1.1. Távközlési műholdak

Az alrendszer (SATCOM) geostacioner pályán keringő műholdakból, valamint fix telepítésű földi terminálból (SGT) áll. Az alrendszer célja a katonapolitikai konzultációs folyamatok biztosítása a tagországok között.

1.2. Mobil rendszerű távközlési műholdak

A NATO rendelkezik távközlési műholdakat szállító földi terminállal (TSGT). Ezen alrendszer jelentősége és használhatósága az IFOR/SFOR missziók kezdete óta bizonyított. Az alrendszer továbbfejlesztése révén 40 db TSGT modul kerül

[41] szerzők: Pándi Balázs, PhD-hallgató, ZMNE BJKMK Katonai Műszaki Doktori Iskola; Dr. Pándi Erik, egyetemi docens, ZMNE BJKMK Híradó Tanszék

rendszeresítésre, amelyből minden második az NCIS rendszer telepíthető modulja (DCM) lehet.

1.3. Nemzetközi haditengerészeti távközlési műholdak

Az alrendszert összefoglaló neve INMARSAT. Az önálló alrendszert veszélyhelyzetben alkalmazzák, ezek nem tartoznak az NCIS rendszeréhez, így a hálózatba való integrálásuk is elmaradt. Jelenleg a különböző katonai és egyéb műveletek során mintegy közel háromtucat műhold kerül felhasználásra.

1.4. UHF – harcászati távközlési műholdak

Ezen hálózatot alkalmazza a műveleti területen tevékenykedő haderő. Az alrendszer révén lehetőség nyílik információvédett, mobil, vagy állandó telepítésű kommunikációs lehetőségek kialakítására.

1.5. MAXIMA

Az alrendszer egy intelligens, digitális multiplex rendszer, amely csomópontok kialakításán alapul. Az alrendszer bevezetésére a SATCOM rendszer optimalizálásának céljából került sor az IFOR műveletek kezdetén.

1.6. Automatikus üzenettovábbító rendszer

Az alrendszer (TARE) egy számítógép által ellenőrzött rendszer, amely szabványszövegek automatikus továbbítását végzi. A hálózat közel kéttucat csomópontból áll (TARE MDC). Az alrendszer tárolja az adatokat, és amint szabad kapacitás van, továbbítja azokat.

1.7. Hangátvitelre alkalmas kapcsolt távbeszélő hálózat

A NATO információvédett és nyílt hangalapú forgalmát az IVSN alrendszer biztosította, amelyet az ISDN alapú NATO törzshálózat vette át.

1.8. Adatátviteli alapszolgáltatás

Az új technikai generáció első alrendszere (NIDTS). Egy tucat csomópontból álló WAN, amellyel az NCIS teljesítménye megsokszorozódott.

1.9. Integrált digitális hálózati kapcsolóközpont

Az IDNX egy intelligens multiplex átviteli alrendszer, amely lehetővé teszi a digitális átviteli rendszer hatékony működését önellenőrző képesség mellett. Alapvetően az IFOR/SFOR harcászati követelmények kiszolgálására készült.

1.10. PROMINA

Az alrendszer az IDNX működésének támogatására létrehozott digitális rendszer, amely a MAXIMA-val együtt lehetővé teszi az NCIS digitális elemeinek optimális hasznosítását.

1.11. Videókommunikációs rendszer

A VTC alrendszer első alkalmazására 1996-ban került sor. A VTC alkalmas harcászati információvédett hangátviteli szolgáltatás nyújtására is, amely lehetővé teszi a bevetések közben végrehajtandó konferencia lehetőségét.

1.12. Egyéb adatátviteli rendszerek

A NATO által alkalmazott alrendszer a válságkezelő műveletek nyitott információs rendszere (CRONOS), amely gondoskodik a felhasználók számára zárt e-

mail lehetőség, professzionális irodarendszer, valamint a SHAPE számára WWW működtetéséről a felhasználók, a SHAPE törzs, más NATO törzsek, valamint nem NATO tagállamok számára, amelyek egy alacsony szintű, túlnyomórészt intelligens, multiplex eszközökön keresztül kerültek hálózatba kötésre. A felhasználók számának bővülésével, nemzeti modulok alkalmazásával a hálózat folyamatosan bővíthető. A CRONOS NATO és IP szabványok szerint működnek, egyúttal rendelkeznek információvédelmi képességekkel is.

Az automatizált üzenetfeldolgozó alrendszer (AMPS) lehetővé teszi a CRONOS munkahelyeken, hogy a TARE információkat elküldjék, illetve fogadják.

A haditengerészeti vezetési és irányítási tájékoztató alrendszer (MCCIS) elemei a szárazföldi erők parancsnoki központjában, valamint a hadihajók fedélzetén kerültek telepítésre. Ezt az alrendszert a hadászati parancsnoki szinttől lefelé a vegyes összetételű összhaderőnemi alkalmi kötelékek törzséig bezárólag alkalmazzák.

Fentiek alapján jól érzékelhető az észak-atlanti szervezetet kiszolgáló CIS összetettsége és bonyolultsága. Napjainkban az információhoz való mindenidejű hozzáférés elengedhetetlen, amely követelmény megvalósításához modern, nagyteljesítményű információ feldolgozó és továbbító rendszerekre van szükség.

2. Az NNEC elmélete

Az információtechnológia tehát jelentős szerepet játszik a NATO követelményeiben, terveiben és jövőképeiben. A Védelmi Képességek Kezdeményezés szerint a vezetési és informatikai rendszereknek jobban kell illeszkedniük a NATO jövőbeni katonai műveleti követelményeihez, amelyek egyúttal maguk után vonják a korábbiaknál sokkal több információ cseréjét, és egyúttal kiterjednek az alacsonyabb vezetési szintekre is. A NATO hadászati parancsnokok egyeztetett jövőképében a hatásalapú hadműveletek egyik alapvető feltételét képező döntési fölény a hiteles és időszerű információktól, illetve védett cseréjüket és egyeztetett módon történő értelmezésüket biztosító eszközökön múlik [2]. Az információs színtér szereplőivel történő információcserének, illetve a rendelkezésre álló információs szolgáltatások felhasználásának tehát konfliktusos és versengő helyzetben az információs fölény (előny), illetve ennek révén a műveleti főlény (előny) kialakításában és fenntartásában, semleges környezetben pedig a működési hatékonyság növelésében van jelentős szerepe. Egy adott szereplő műveleti képességeit, működési hatékonyságát ugyanis többek között információs képességeinek növelésével fejlesztheti, amelynek lehetséges módjai: az egyedi (belső) információs képességek hatékonyságának növelése, illetve az együttműködő, semleges és szembenálló környezettel történő információs kapcsolatok hatékonyságának növelése [3].

Az NNEC megvalósíthatóságának vizsgálata során a NATO megállapította, hogy az NNEC egy a kulcsfontosságú koncepciók közül, amely a NATO átalakítás középpontjában áll. Sokkal inkább emberekről, szervezetekről és új, sokkal dinamikusabb, rugalmasabb, hatékonyabb módon együttműködésre képessé tett nemzetekről szól, mint technológiáról. Mégis technológia, amely az információt nagy sebességgel, a szükséges bőséggel biztosítja, amely lehetővé teszi, hogy az átalakulás megtörténjen. Alapvető természete folytán az NNEC és az átalakítás sokkal inkább egy utazásról szól, mintsem egy végállomásról. Egy olyan utazásról, ahol a

szervezeti és technológiai innovációnak és változásnak az átalakulás érdekében kéz a kézben kell együttműködnie [4]. Az NNEC révén a jövőbeni katonai műveletek egyes jellemzői is megváltoznak. A hadseregekben jelenleg alkalmazott hadviselési forma szerint például az érzékelő és a csapásmérő képesség egységet alkot. A hálózatközpontú hadviselés jelzőjével aposztrofált hadviselési formában az érzékelő és a végrehajtó erők közé beiktatásra kerül a teljes vezetési-döntéshozó rendszer. Így a felderítési adatoknak el kell jutnia a döntéshozókig, majd onnan a feladatoknak a végrehajtó erőkig. Ez a hierarchia a következő követelményeket támasztja [5]:

a) valós idejű és biztonságos kommunikáció az érzékelők és a döntéshozók között;

[18] b) az adatok valósidejű továbbítása, feldolgozása, megjelenítése, és hatékony felhasználása;

[19] c) decentralizált adatstruktúra, amely minden döntéshozó számára biztosítja az adatokhoz való hozzáférést és azok kiértékelését.

A hálózatközpontú hadviselés metodikájának megfelelő komplex vezetési rendszereknek a C4I rendszerek (command – vezetés, control – irányítás, communication – híradás, computer – computer, intelligence – felderítés, hírszerzés) tekinthetők. Ezek egységbe foglalják az információgyűjtést, tárolást, feldolgozást, kommunikációt, a csapatok vezetését. Biztosítják, hogy a szükséges adatok mindig a megfelelő helyen és időben rendelkezésre álljanak. A C4I rendszerek feladatai a következők [6]:

a) a harctevékenység támogatása a harc minden időszakában;

[20] b) biztosítani a csapatok felkészítését, a gördülékeny átmenetet a béke helyzetből a háborús helyzetbe;

[21] c) folyamatosan figyelemmel kísérni és értékelni a saját csapatok és az ellenség helyzetét;

biztosítani az adatok és információk gyűjtését, feldolgozását, továbbítását és elosztását;

biztosítani a riasztást és a csapatok kiértesítését;

biztosítani a csapatok követését, irányítását és a tőlük érkező jelentések fogadását;

támogatni a háborús helyzetből a békehelyzetbe való átmenetet;

védelmi tevékenységekkel biztosítani az információs rendszer hatékony működését.

Az NNEC elérése viszonylag hosszú folyamat, amelynek eredményei várhatóan a következő évtizedben realizálódnak. A megvalósulást az Egyesült Államok Hadserege 2020-ra prognosztizálja. A fejlesztés több területen párhuzamosan is megvalósítható. A felcsatlakozás szabványos felületeinek kialakítása, az adatátviteli rendszer architektúrájának és átviteli csatornáinak megtervezése, a rendszer alapszolgáltatásainak és alkalmazási körének meghatározása, az adatrendszer és adatbázisok struktúrájának kialakítása egymással párhuzamosan, de nem egymástól függetlenül folyhat. Fontos kérdés, hogy a jelenleg is fejlesztés alatt álló NCIS megfelelő alapot nyújt-e a rendszer kialakítására. Az NNEC koncepció alapvetően önállóan is megállja a helyét, azaz a C2 képességek megfogalmazását követően a vezetési rendszer részletes ismerete nélkül is kialakítható a CIS, amely moduláris felépítéséből és rugalmas alakíthatóságából adódóan, paraméterezhető szoftvermegoldá-

sokra támaszkodva gyakorlatilag minden vezetői információs igényt ki tud elégíteni, egyszerűen adaptálható a vezetés rendjéhez, az alkalmazási környezetekhez és a végrehajtandó feladatokhoz. Az NNEC koncepció legfontosabb elve, hogy az információk igény és szükség szerint legyenek biztosíthatók és az információs (kommunikációs) rendszer képességei azt a lehető legkisebb mértékben korlátozzák [7].

3. Összegzés, következtetések

Az információtechnológia területének elmúlt évtizedekben történt lendületes fejlődése lehetővé tette a kommunikációs és információs rendszerek modernizációját. Ennek megfelelően az NCIS komplex, de ugyanakkor folyamatosan modernizálódó rendszer. Napjaink, illetőleg a közelmúlt konfliktusai több esetben kisebb-nagyobb mértékű háborús, illetőleg nemháborús katonai műveletek végrehajtását eredményezte, egyúttal új kihívásokkal szembesítve mind a NATO-t, mind az EU-t. A kihívásokra való megfelelő válaszok kialakítása csak egy átalakuló NATO-val lehetséges, ezzel párhuzamosan, a technológia fejlődésével megalapozható a hálózatközpontú hadviselés, amelynek csapásmérő ereje a szemben álló felek aszimmetrikus helyzetéből fog adódni.

Hazánknak, mint NATO tagországnak katonai kommunikációs rendszereit – *és ezen belül a tábori hírrendszert* – mindenképpen alkalmassá kell tenni az NNEC megvalósítására. Miután a C2 képességek megfogalmazását követően a vezetési rendszer részletes ismerete nélkül is kialakítható a modernizált nemzeti CIS, ezért a jelenlegi analóg tábori hírrendszer kiváltását célszerű napirendre tűzni.

Felhasznált irodalom:

[1] Czank László: A NATO távközlési- és információs rendszere a XXI. század küszöbén, Nemzetvédelmi Közlemények, ZMNE, Budapest, 2003., ISSN 1417-7323, 169-176. oldal, 2003/3. szám;

[2] Munk Sándor: Az informatikai támogatás alapjai, Nemzetvédelmi Közlemények, ZMNE, Budapest, 2005., ISSN 1417-7323, 178. oldal, 2005/2. szám;

[3] Munk Sándor: Interoperabilitási problémák és elképzelések a katonai alkalmazásban a XX. század végéig, Hadmérnök, ZMNE BJKMK, Budapest, 2006., ISSN 1788-1919, 25. oldal, 2006/2. szám;

[4] Szép József: A NATO új kezdeményezése a hálózat nyújtotta képesség, „Kommunikáció 2004." nemzetközi szakmai-tudományos konferencia kiadványa, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2004, ISBN 963-86441 5 X, 297. oldal;

[5] Haig Zsolt – Várhegyi István: Információs műveletek, egyetemi jegyzet, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2004., 37. oldal;

[6] Előházi János: Védelmi célú informatikai rendszerek feladatai és fenyegetettségei a hálózatközpontú hadviselésében, Hadmérnök, ZMNE BJKMK, Budapest, 2007., ISSN 1788-1919, 71-72. oldal, 2007/3. szám;

[7] [7] „Kommunikáció 2004." nemzetközi szakmai-tudományos konferencia kiadványa, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2004, ISBN 963-86441 5 X, 126. oldal.

TAKÁCS Attila:42

„112" EGYSÉGES SEGÉLYHÍVÓ RENDSZER (ESR) MAGYARORSZÁGI KIALAKÍTÁSA

Absztrakt: A szerző – szakmai tapasztalataira építve – áttekinti az Egységes Segélyhívó Rendszer továbbfejlesztésének mibenlétét, illetőleg rendszerezi a megvalósítással kapcsolatos feladatokat.

Kulcsszavak: 112 segélyhívó-szám, Egységes Segélyhívó Rendszer (ESR).

1. A segélyhívás rendszerének jelenlegi működési struktúrája

A 112-es hívószám 1999 óta ingyenesen hívható a magyarországi vezetékes- és mobil hálózatból. A koordinációs feladatokat a zártcélú hálózatokat érintő nagyarányú átszervezéseket követően, 2007-től a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala vette át [1]. A segélyhívásokat a Budapesti Rendőr-főkapitányság és a megyei rendőr-főkapitányságok fogadják. Az ún. „nemzeti hívószámok" (104, 105, 107) párhuzamosan működnek. Az Országos Mentőszolgálat a 104-es hívások fogadására 26 központot alakított ki. A 107-es hívások fogadása a rendőrkapitányságokon és rendőr-főkapitányságokon, a 105-ös hívások fogadása az önkormányzati és köztestületi tűzoltóságokon történik, mindkét feladat esetében országosan több mint 150 helyen. Az ESR rendszer – *mint minden rendszer* – egymással kölcsönhatásban levő komponensek jól körülhatárolható halmazából áll. A „komponens", vagy „összetevő" szavakat itt klasszikus rendszerelméleti értelemben használjuk, vagyis bármilyen élő, élettelen vagy absztrakt komponenstípus alkalmazható (pl. ember). Az ESR rendszer alatt azon komponensek összességét értjük, amelyek összehangolt működtetése lehetővé teszi az alábbi alapvető célkitűzések elérését:

- a segélyhívásokra vonatkozó reagálási idő rövidül, különösen a készenléti szervezetek együttműködését igénylő események tekintetében (párhuzamos riasztás),
- az intézkedő egységek gyorsan és pontos információt kapnak az intézkedések hatékonyabb és eredményesebb végrehajtása érdekében,
- az érintett szervezetek segélyhívással kapcsolatos tevékenységirányítási folyamatainak egységes keretbe foglalása, ezen belül a riasztások, vonulások és intézkedések összhangjának megalapozása az információs rendszer segítségével,
- az Egységes Segélyhívó Rendszer jogszabályi környezet szempontjából megalapozott szervezeti-irányítási struktúrában, azon belül folyamatszemlélettel működik.

[42] Szerző: Takács Attila PhD-hallgató, ZMNE Hadtudományi Doktori Iskola

2. Az ESR tervezett működése

Az ESR működésének lényegi eleme, hogy a segélyhívások előfeldolgozása egy elkülönült szervezetnél történik, de a végrehajtás továbbra is az önálló szakmai felelősséget hordozó készenléti szervezetek feladata marad. A napi 60-65 ezer hívás eredményes intézéséhez három hívásfogadó központot célszerű létrehozni, „államigazgatási" tulajdonú épületekben. Egyet Budapesten, egyet az ország keleti-, egyet a nyugati felében. A központokat úgy kell kialakítani, hogy szükség esetén egymást is tudják helyettesíteni. Az összehasonlító számítások alapján legfeljebb 120 hívásfogadó munkahely kialakítására van szükség a beérkező hívások megfelelő színvonalú elintézéséhez.

2.1. Kapcsolódás más rendszerekhez

A rendszer eredményes működéséhez szükség van külső kapcsolatokból származó információra. A megvalósítás során a kapcsolódási felületek (interfészek) kialakításánál figyelembe kell venni, hogy:

- a bejövő információ struktúráját a rendszeren belül kell definiálni, és elő kell írni a külső rendszerek felé,
- a kimenő információ struktúráját más rendszerek határozzák meg, amihez a megvalósítás során igazodni kell.

Bejövő információs kapcsolatok:

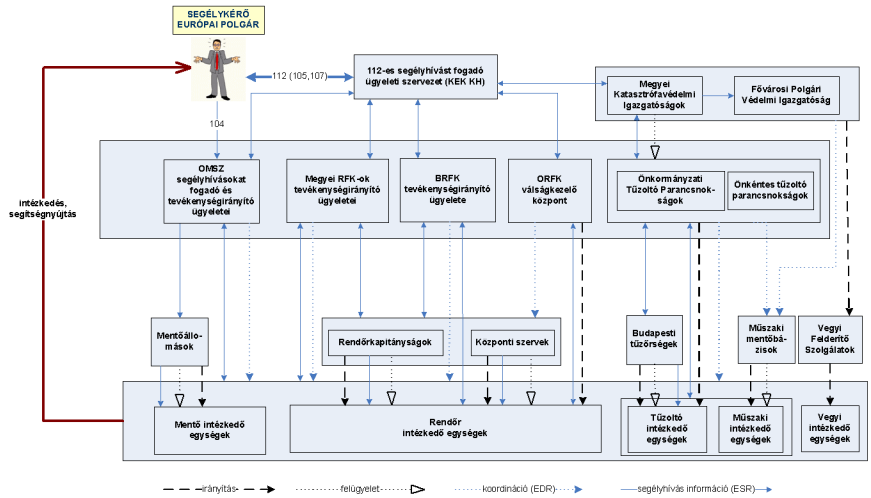
- központi nyilvántartások,
- személy- és lakcímnyilvántartó,
- körözési nyilvántartás,
- gépjármű nyilvántartás,
- címregiszter (objektum adatbázis),
- Monitoring Lakossági Riasztórendszer (MoLaRi),
- a távközlési szolgáltatók által nyújtott hívó fél hívás- és helyszín azonosító adatai.

Kimenő információs kapcsolatok:

- az érintett szervezetek adatszolgáltatási / statisztikai igényeit kiszolgáló információs utak.

Bejövő és Kimenő információs kapcsolatok:

- EDR és az AVL (Automatikus járműkövető) alrendszer,
- Robotzsaru.



1. ábra. A segélyhívások tervezett szervezeti- és irányítási struktúrája (forrás: Miniszterelnöki Hivatal)

2.2. Számítástechnikai architektúra

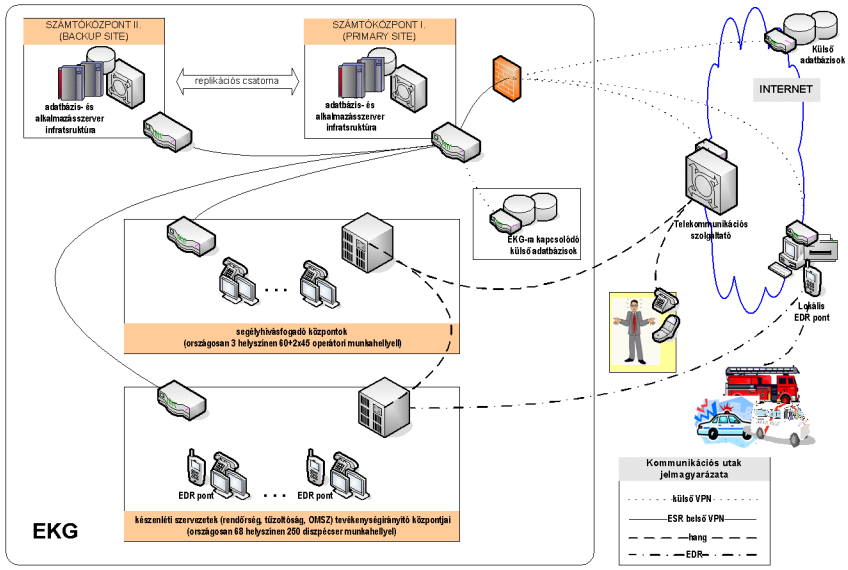
A számítástechnikai architektúra – *mint infrastrukturális háttér-keretrendszer* – az ESR automatizált folyamat-elemeinek (főbb folyamatok: hívásfogadás, -kezelés és minősítés, tevékenységirányítás, térképi információs) támogatását látja el.

Az architektúra az alábbi funkcionális területekre osztható:

- számítóközpont (2 db),
- hívásfogadó központok (3 db),
- tevékenységirányító központok:

[8] rendőrség (20 db),
[9] katasztrófavédelem, tűzoltóság (29 db),
[10] OMSZ (26 db),

- külső helyszínek.



2. ábra. Az ESR tervezett rendszer architektúra vázlata, (forrás: Miniszterelnöki Hivatal)

A 112, 105 és 107 hívások minden esetben a hívásfogadó központok kezelése alá esnek, a 104-es hívások kezelése ettől eltérő. Abban az esetben, ha a telekommunikációs szolgáltatók által átadott híváshoz kapcsolódó helymeghatározási adatok helyesek és az SLA által meghatározott időtartamon (határidő) belül érkeznek a rendszerbe, a hívások kezelését az Országos Mentőszolgálat operátorai/diszpécserei végzik. Hibás vagy határidőn belül nem elérhető adatok esetén a 104-es hívásokat is a hívásfogadó központok operátorai kezelik. Országosan három hívásfogadó központ áll rendelkezésre az állampolgárok segélyhívásainak fogadására:

- Budapest és Közép-Magyarország (60 hívásfogadó operátor),
- Kelet-Magyarország (45 hívásfogadó operátor),
- Nyugat-Magyarország (45 hívásfogadó operátor).

A hívásfogadó központok az EKG-n keresztül, zárt VPN-en át érik el a számítóközpontot. A segélyhívások kezelését végző hívásfogadó központokat úgy kell kialakítani, hogy azok szükség esetén magas szolgáltatási szinten tudják egymást helyettesíteni. Egy központ telítődése esetén a hívásokat automatikusan továbbítani kell más, kevésbé terhelt központok felé. A hívásfogadó központok operátorai a központi alkalmazás használatával látják el feladatukat. Az állampolgárok segélyhívásai a telekommunikációs szolgáltatók hálózatán keresztül a hívásfogadó központok telefonközpontjaiba jutnak, a hívásokhoz kapcsolódó érvényes adat kiértékelése a számítóközpont feladata csakúgy, mint a határidőn belüli hívásvezérlések kiadása, és a térképi információk megjelenítése. Az intézkedést igénylő segélyhí-

vások esetében az operátor a megfelelő készenléti szervek tevékenységirányító központjainak adja át a feladatot.

3. Hazai szabályozás

Az elmúlt három évben különböző, a Miniszterelnöki Hivatal által koordinált [2] projekt-munkálatok kezdődtek Magyarországnak az ESR-hez való csatlakozásával kapcsolatban, azonban a jogi szabályozás elvi kidolgozásának, a műszaki-technikai feltételek kialakításának nem volt egyetlen centruma. Ezek a munkálatok az elektronikus hírközlésről szóló 2003. évi C. törvény (Eht.) megalkotásával leálltak. Az Európai Bizottság 2006. április 6-ai kötelességszegési eljárásának eredménye kapcsán megállapítható, hogy az Eht.-ban lefektetett általános szabályok kialakítása megfelelő kezdet volt, azonban nem követték az ESR kialakításával összefüggő részletes és pontos működési kereteket meghatározó jogi részletszabályok, így Magyarország jelenleg mulasztásos helyzetben van. A 112-es segélyhívó kérdéskörét a kormányprogram kiemelten kezeli, azonban konkrét intézkedések csupán az 1066/2006. (VI.29.) Korm. határozat [3] kapcsán kezdődtek meg, melyben a Kormány a közigazgatási informatikáért felelős kormánybiztos feladatává tette az ESR szabályozás közösségi előírásoknak megfelelő megvalósítás feladatainak előkészítését. A „112-es" Európai Segélyhívó Rendszer kialakításával kapcsolatos feladatokról szóló 2031/2007. (III.7.) Korm. határozatban [4] pedig már konkrétan megjelölésre kerültek az egyes feladatok – *az ESR szervezeti felállítása, a Rendszerirányító Központ és regionális alközpontjainak tevékenységének jogi, hatásköri, illetékességi kérdéseinek meghatározása* – elvégzéséért felelős miniszterek, illetve feladatok elvégzésére meghatározott határidők. Jelenleg a tervezett jogszabályok, módosítások közül csupán az egységes európai segélyhívószámra irányuló segélyhívások támogatása érdekében a nyilvános telefonhálózatra vonatkozó műszaki követelményekről szóló 23/2007. (II.23.) GKM rendelet [5] valósult meg, illetve az egységes digitális rádió-távközlő rendszerről szóló 109/2007. (V.15.) Korm. rendeletben [6] került kialakításra a készenléti szervek által használt EDR rendszer. Az ESR megvalósításával kapcsolatos Kormány részére szóló előterjesztés 2007. július 26-án készült el.

4. A segélyhívás folyamata

A 112-es segélyhívószámon a hívások az önálló szervezeti egységként működő fogadó ügyelethez fut be, de a nemzeti hívószámok megmaradása esetén – *átmenetileg* – direkt módon is eljuthat a készenléti szervezetek tevékenységet irányító ügyeleteire. Egy összetett esemény esetében a koordinációt a tevékenységirányító felügyeletek végzik. Az egyszerűbb esetekben erre nincs szükség, itt az intézkedő egységet kiküldő lokális szerv végzi az irányítást és koordinálást. A koordinációt jelentő információ lényegi része az EDR-en keresztül jut el az intézkedő egységekhez. A tevékenységirányítást végző szervezeteknek egyedi szervezeti - és működési szabályzatuk van, ezek a saját szakmaiságuk biztosítékai is egyben, amelyet az ESR rendszernek támogatnia kell.

5. A projekt megvalósítása, jövőbeni feladatok

A jövőbeni feladatok körébe sorolható a szervezetfejlesztés, amely során az ESR rendszer működtetéséhez szükséges szervezeti folyamatok meghatározását, a szervezeti működésbe történő integrációt és az auditálást kell végrehajtani. Ezt követően a segélyhívásokat fogadó ügyeleti személyzet toborzását és kiválasztását szükséges lebonyolítani. A kiválasztott személyzet oktatása során a 112-es operátorok, a tevékenységirányító diszpécserek és az ESR rendszer üzemeltető személyzetének kiképzését kell megoldani. Minden alkalmazottat ki kell képezni a az alkalmazások használatára, amely során az együttműködő szervek ügyeleti személyzetének szakmai kiképzését is tervezni kell. Ennek becsült létszáma: 1400 fő+ 6 fő HelpDesk személyzet.

6. Összegzés, következtetések

Hazánk az EU-hoz való csatlakozással kapcsolatos egykori feltételek sorában kialakította az európai Egységes Segélyhívó Rendszert. A jogi szabályozás területén Magyarország nem teljesítette az ESR kialakításával összefüggő részletes és pontos működési kereteket meghatározó jogi részletszabályozás megalkotását, így bekövetkezett az EU által is megállapított mulasztásos helyzet. A probléma feloldása érdekében a Kormány a vonatkozó kormányhatározat alapján megkezdte a szükséges feladatok végrehajtását.

Felhasznált irodalom:

[1] Pándi Erik: A hazai zártcélú hálózatok szerepének átalakulása az elektronikus közigazgatási szolgáltatások bevezetése és kiterjesztése folyamatában, Hadmérnök, ZMNE BJKMK, Budapest, 2007., ISSN 1788-1919, 101-102. oldal;

[2] Nagy Lajos – Pándi Erik: A katasztrófavédelmi kommunikációs rendszer jellemzői II., Védelem, BM Duna Palota és Kiadó, Budapest, 2006., ISSN 1218-2958, 17. oldal, 2006/4. szám;

[3] A közigazgatási informatikáért felelős kormánybiztos kinevezéséről és feladatairól szóló 1066/2006. (VI.29.) Korm. határozat, Complex DVD-jogtár, Budapest, 2008., ISSN 1788-5027, 2008. június 30.;

[4] A „112-es" Európai Segélyhívó Rendszer kialakításával kapcsolatos feladatokról szóló 2031/2007. (III.7.) Korm. határozat, Complex DVD-jogtár, Budapest, 2008., ISSN 1788-5027, 2008. június 30.;

[5] A nyilvános telefonhálózatra vonatkozó műszaki követelményekről szóló 23/2007. (II.23.) GKM rendelet, Complex DVD-jogtár, Budapest, 2008., ISSN 1788-5027, 2008. június 30.;

[6] Az egységes digitális rádió-távközlő rendszerről szóló 109/2007. (V.15.) Korm. rendelet, Complex DVD-jogtár, Budapest, 2008., ISSN 1788-5027, 2008. június 30.

PÁNDI Erik:43

AZ ELEKTRONIKUS KÖZIGAZGATÁSI KERETRENDSZER KIALAKÍTÁSA

Absztrakt: Hazánk az E-kormányzat 2005 Stratégiában kiemelt figyelmet fordított az elektronikus kormányzati szolgáltatások megvalósítására. A középpontban az Európai Unió (EU) által meghatározott húsz leggyakrabban igénybevett szolgáltatás állt. A szolgáltatások magas színvonalon megvalósultak, amelynek eredményeként Magyarország az EU országok rangsorában a korábbi sereghajtó helyről 2005 végére a középmezőny élére került, és az Egyesült Nemzetek Szervezete Gazdasági Együttműködési és Fejlesztési Szervezet (UN OECD) 2006. évi országjelentése alapján is jelentőset lépett előre a világ országai között [1]. A 2005 végéig kialakított, önállóan működő szolgáltató rendszerek további jelentős fejlődést már nem tettek lehetővé. Az elmúlt két évben a szolgáltatások száma némileg nőtt, és a korábban indított elektronikus szolgáltatások minősége is javult, azonban ezek az eredmények az indikátorokra csak minimális mértékben hatottak. Ennek eredményeként Magyarország az EU-országok középmezőnyének végére csúszott vissza. Jelen közlemény a Miniszterelnöki Hivatal Infokommunikációért és E-közigazgatásért Felelős Szakállamtitkárság által közrebocsátott szakmai anyag alapján összegzi az okokat, egyúttal egybefogva a lemaradás megszűntetésére tett intézkedések lényegét [2].

Kulcsszavak: E-közigazgatás, e-közszolgáltatások, információtechnológia (IT), interoperabilitás, OECD.

1. A lemaradás vélelmezett okai

Az okokat elemezve a Miniszterelnöki Hivatal Infokommunikációért és E-közigazgatásért Felelős Szakállamtitkárság (továbbiakban: MeH) arra a következtetésre jutott, hogy a fejlődés legfőbb gátja az egyes ágazati rendszerek közötti interoperabilitás hiánya. A közigazgatási reformmal párhuzamosan (2006 második felétől) a Kormány elsődleges célként fogalmazta meg, hogy minőségileg új alapokra kell helyezni az elektronikus közszolgáltatások fejlesztését. Az eddig egymástól függetlenül működő ügyintézéshez kapcsolódó szolgáltatásokat fel kell váltani az élethelyzethez kapcsolódó szolgáltatásokkal. Az ilyen típusú szolgáltatások alapvető feltétele, hogy az eddig önállóan – *szigetszerűen* – működő elektronikus szolgáltatások között olyan kapcsolat jöjjön létre, amelyek biztosítják a különböző szervezetekhez köthető adatok elérését, és emberi beavatkozás nélküli feldolgozását. Az elképzelés megvalósítása csak a technikai és a szemantikai interoperabilitás feltételeinek megteremtése útján lehetséges. Előzőeket figyelembe

[43] Szerző: Dr. Pándi Erik, egyetemi docens, ZMNE BJKMK Híradó Tanszék

véve a magyar E-közigazgatás i2010 Stratégia az interoperabilitás megteremtésével összefüggő feladatokat kiemelten kezeli. Alapvető feltétel, hogy az elektronikus közszolgáltatások fejlesztése során olyan szabványok, követelmények és eljárásrendek kerüljenek meghatározásra, amelyek egységesen használhatók, és biztosítják a különböző rendszerek között szükséges adatcsere megvalósítását. Ennek érdekében első lépésként a Magyar Nemzeti Interoperabilitási Keretrendszer (MNIK) létrehozása valósul meg, és ennek eredményeire építve alakíthatók ki az interoperábilisan működő közigazgatási szolgáltató rendszerek.

2. Az MNIK célja

A létrehozás elsődleges célja azoknak a szabványoknak, követelményeknek és előírásoknak a meghatározása, amelyek biztosítják az elektronikus közigazgatás teljes fejlesztéséhez és üzemeltetéséhez az egységes technikai, szemantikai, IT biztonsági, alkalmazásfejlesztés-módszertani, valamint projektmenedzselési és monitoring platformot. Ennek a célkitűzésnek a megvalósulása és következetes érvényesítésének biztosítása megfelelő garanciát jelent ahhoz, hogy az önállóan megvalósuló szakágazati, illetve önkormányzati alrendszerek fejlesztése, továbbfejlesztése eredményeként interoperábilis, biztonságos és korszerű elektronikus közigazgatási rendszer jöjjön létre. Az MNIK célja továbbá, hogy megteremtődjenek a pán-európai szolgáltatások feltételei.

3. Az MNIK tartalma

Az egyes részek együttesen biztosítják azt a szakmai, technológiai, módszertani tudáshátteret és kompetenciát, amely az e-közigazgatási szolgáltatások egységes platformjának létrehozásához, valamint az egységes platform előírásainak, szabványainak és követelményeinek a központi, szakágazati és önkormányzati alrendszerekben történő érvényre juttatásához szükséges. Ennek érdekében az MNIK az alábbi főbb fejezeteket tartalmazza:

a) folyamatleíró módszertan és eszközrendszer kidolgozása;
[7] b) technikai és szemantikai interoperabilitási követelmények meghatározása;
[8] c) alkalmazásfüggő IT biztonsági követelmények meghatározása;
fejlesztési módszertan és alkalmazásfejlesztési keretrendszer;
szabványtár működtetési és gondozási rendszerének kialakítása;
projektmenedzsment módszertan és szakmai monitoring kialakítása.

3.1. Folyamatleíró módszertan és eszközrendszer kidolgozása

Cél a folyamatok korszerűsítését segítő módszertan és a folyamatok formális leírását támogató eszközkészlet kidolgozása, kiválasztása. A közigazgatás ügyintézési folyamatainak elektronizálása nem jelenti automatikusan sem a közigazgatás belső hatékonyságának, sem az ügyfelek elégedettségének növekedését. Az elektronikus közigazgatás kiépítésének, amely mind az EU, mind a hazai fejlesztési stratégiák egyik kiemelt prioritása [3], az állampolgárok, és a vállalkozások igényei alapján kell megtörténnie, annak érdekében, hogy megvalósuljon a szolgáltató

állam modellje, illetve, hogy megtakarításokat lehessen elérni a többszörözések kiszűrése és a folyamatok egyszerűsítése által. A szolgáltatási folyamatok egyszerűsítésének fő célja a folyamatok integrálási lehetőségeinek (interoperabilitás) feltárása, és az esetleges átfedések, ellentmondások megszüntetése. Kiemelt cél az ügyféligények által vezérelt folyamatok kialakítása, az ügyféloldali adatszolgáltatás és az ügyfél részvételének minimalizálása az ügyintézési folyamatokban, valamint az ügyintézési folyamatok élethelyzethez, a megoldandó problémához való igazítása. Ezen a területen nagy előrelépés lehetséges, ha a leggyakrabban keresett szolgáltatások elektronizálásának továbbfejlesztése abban az egységes szemléletben történik, amely előrevetíti a kialakítandó szolgáltatások minél egyszerűbb, a felhasználók számára minél kevesebb ráfordítással járó folyamatokra való épülését.

Mindezekre tekintettel a fő cél olyan eszközrendszer és módszer kidolgozása, amely támogatja a közigazgatás és a közigazgatási szolgáltatások folyamatainak megújítását, szükség szerint újraszabályozását, és az egyes folyamatok egységes keretrendszerben történő formalizált leírását. Csak formalizált leírás segítségével biztosítható az egyértelműség, a dokumentáltság, a módosíthatóság és a követhetőség. Megfelelő formális leírásból nemcsak kód generálható automatikusan, hanem a folyamatok konzisztenciája, vagy esetleg magasabb összefüggések is ellenőrizhetők.

Az egységes keretrendszerben elkészülő követelményspecifikációk egységes struktúrát és kiszolgálási, illetve mérési keretrendszer létrehozását teszik lehetővé, amelyek megalapozzák a jogszabályi változások rugalmas, gyors követését. A szabványosításban, egyszerűsítésben és megosztásban rejlő hatékonyság az intézmények összekapcsolása révén, a központi infrastruktúra, a szolgáltatási portfolió és a tudásbázis lehető legszélesebb körű kihasználásával erősíthető.

3.2. Technikai és szemantikai interoperabilitási követelmények meghatározása

Hosszútávon életképes és hatékony e-közigazgatási rendszer csak úgy képzelhető el, ha a rendszerfejlesztés minden résztvevője magáévá teszi az interoperabilitás elvéből eredő követelményeket. Mindennek előfeltétele az interoperabilitás követelményrendszerének meghatározása, publikálása, valamint megfelelő módszertani útmutatók elkészítése.

A technikai interoperabilitási szint az egyes alrendszerek közötti kommunikáció megteremtése. Ide tartoznak a különböző kommunikációs protokollokat, biztonsági megoldásokat és alapvető adatformátumokat leíró szabványok, ajánlások és egyéb tájékoztatóanyagok. A szemantikai interoperabilitási szint az egyes kommunikáló alrendszerek között átvitt adatok azonos értelmezését írja elő, és ezt az előírást kell megvalósítani. A feladatok megvalósítása során:

a) elkészül az interoperabilitási követelményrendszer specifikációja és előírása;

[9] b) a bevizsgálási és tanúsítási módszertan és eljárás;

[10] c) módszertani útmutató az interoperabilitásra történő tervezés és fejlesztés segítéséhez;

szabványok és előírások gyűjteménye a technikai interoperabilitási szinthez, a központi, szakrendszeri és önkormányzati rendszerekhez;

szabványok és előírások gyűjteménye a szemantikai interoperabilitási szinthez, a központi, szakrendszeri és önkormányzati rendszerekhez.

3.3. Alkalmazásfüggő IT biztonsági követelmények meghatározása

A közigazgatásban alkalmazott rendszerekkel szemben támasztott követelmény, hogy informatikai biztonsági szempontból megfelelőek legyenek [4]. Az IT biztonság önmagában nem értelmezhető, figyelembe kell venni a konkrét környezetet. Fontos, hogy a biztonságnak tudatosan kell megjelennie a tervezési, fejlesztési, üzemeltetési folyamat minden fázisában, nem lehet utólag vagy külön megvalósítani. Ebből következik, hogy a fejlesztési projektekben meg kell jelennie az IT biztonsági lépéseknek és követelményeknek, valamint ezek ellenőrzésének és betartatásának. A jogszabályi környezettel összhangban ki kell dolgozni azokat a kötelezően betartandó előírásokat, módszereket, amelyekre a fejlesztési projektekben figyelemmel kell lenni. A követelményrendszer alapján a fejlesztési projektekben kötelezően erőforrást kell allokálni az IT biztonsággal kapcsolatos tervezési, kivitelezési és üzemeltetési lépésekre.

A követelményrendszernek:

a) figyelembe kell vennie a jogszabályi környezetet;

[11] b) a legjobb gyakorlatból kell kiindulnia, a nemzetközi és hazai szabványok alapján;

[12] c) figyelembe kell vennie a működési környezetet, valamint a terület műszaki és üzemeltetési sajátosságait;

ki kell terjednie a pályáztatás és a működés teljes életciklusára, úgymint tervezés,

fejlesztés, megvalósítás, tesztelés, működtetés, fenntartás, valamint ellenőrzés, monitoring és audit;

struktúráltnak kell lennie;

kockázati alapú megközelítést kell megkövetelnie;

ki kell terjednie az üzletmenet folytonosság kérdéseire, valamint

saját életciklusára és menedzsmentjére.

3.4. Fejlesztési módszertan és alkalmazásfejlesztési keretrendszer

A fő cél olyan alkalmazás-fejlesztési keretrendszer és ezen belül megfelelő fejlesztési eszközrendszer és módszertan kifejlesztése, amely igazodik a szolgáltatásorientált működési módhoz és rendszerarchitektúrához. Az e-közigazgatási rendszer fejlesztésének körülményei és követelményei komplexek. Az e-közigazgatás fejlesztése folyamatos feladat, amelyet a kormányzat rendszeresen karbantartott stratégia mentén, koordináltan hajt végre. Az aktuális feladatok az e-közigazgatásban meglévő alrendszerek (szakrendszerek) integrációját igénylik, hiszen számos, a szakrendszereken átívelő szolgáltatás szerepel az elérendő célok között. Párhuzamosan több, az alrendszerekre vonatkozó fejlesztési projekt indul, az integrációt tehát menetközben, fokozatosan és folyamatosan lehet és kell végrehajtani.

Az integrációban résztvevő alrendszerek különböző szervezetek felügyelete alátartoznak [5], célszerű ezért az integráció során a lazán csatolt alrendszerekre törekedni, azaz megtartani az alrendszerek függetlenségét, de megszabni a csatlakozási felületeket. Az integrált rendszernek nyitottnak kell lennie, hiszen egyrészt egyre több új hazai szereplő bekapcsolódása várható (pl.: önkormányzatok, illetve regionális központok), másrészt a páneurópai szolgáltatásokhoz való csatlakozás igénye a határon túlnyúló kapcsolódási lehetőséget is megköveteli. Az integráció során csak olyan megoldásokat szabad alkalmazni, amelyek garantálják a biztonságot és a személyes adatok védelmét.

3.5. A szabványtár működtetési és gondozási rendszerének kialakítása

Nagyon fontos szempont, hogy a nemzeti interoperabilitási keretrendszer elemeit az érintettek, a közigazgatási szervezetek munkatársai és a potenciális fejlesztő cégek is megismerjék. Ennek érdekében a fejlesztéshez és üzemeltetéshez szükséges szabványok, követelmények, előírások, ajánlások és egyéb információs anyagok publikálására a keretrendszer kialakításával egyidejűleg szabványtár kerül létrehozásra, meghatározva az ezt működtető szervet felépítését és feladatait, valamint a szükséges infrastruktúrát. A szabványtár az e-közigazgatási keretrendszer számára lényeges dokumentumokat tárolja, elsősorban a következő területekre koncentrálva: architektúra, technikai és szemantikai interoperabilitás, folyamatleírás és folyamat-modellezés, valamint IT biztonság. A keretrendszer szempontjából minden műszaki és egyéb előírás jól meghatározható életciklussal rendelkezik. A cél egy olyan szervezet és háttér-infrastruktúra létrehozása, amely megvalósítja a szabványtárban tárolt információk és dokumentumok életciklusának menedzselését, és megfelelő minőségű publikálását.

3.6. Projektmenedzsment módszertan és szakmai monitoring kialakítása

A sokszereplős, komplex közigazgatási folyamatok egységes szemléletű elektronizációja és ennek központi koordinációja és felügyelete jól szervezett projektet, tervszerű működést igényel [6]. A szakágazati fejlesztési projektek összefogása megköveteli az egységes közigazgatási standard projekt-karta kialakítását és karbantartását. A közigazgatás, a közszolgáltatások korszerű elveken alapuló, hatékony és állampolgárbarát működésének biztosítása érdekében jelentősen fejleszteni kell az elektronikus közigazgatást, amelynek során közigazgatási szinten az ügyfolyam egységesítésének, szabványosításának irányába kell haladni, a szolgáltatásokat pedig közelebb kell vinni a társadalomhoz.

A technológia korszerűsítése többek között jelenti a termékek és/vagy szolgáltatások kialakítására, fejlesztésére, karbantartására (együttesen: létrehozására) irányuló módszertanok egységesítését, továbbfejlesztését is. A módszertan magába foglalja egy termék vagy szolgáltatás létrehozásával kapcsolatos tevékenységek leírását, azok sorrendjét, az alkalmazott technikákat, módszereket és eszközöket, valamint a felhasznált, illetve létrehozott munkaanyagokat. A termék/szolgáltatás létrehozása projekt keretében zajlik le. A projekt magába foglalja mindazon erőfeszítéseket, szervezeteket, erőforrásokat, amelyek az adott termék/szolgáltatás létre-

hozása céljából szükségesek. A módszertan tartalmazza a projektlétrehozásával és végrehajtásával kapcsolatos technikákat és módszereket.

4. Az e-közigazgatási szakágazati projektek folyamatos informatikai szakmai koordinációja, felügyelete

Az e-közigazgatás céljai akkor valósulnak meg, ha a központi közigazgatási, illetve a regionális és helyi fejlesztések meghatározott, az érintettek által megismerhető szakmai alapokon állnak, és így az alrendszerek interoperabilitása és IT biztonsága biztosítható, és a fejlesztés korszerű módszertanok alapján, rugalmas architektúra kialakításával, hatékonytechnológiai eszközökkel történik. A legfőbb problémát az okozhatja, hogy az egyes kiemelt fejlesztési projektek csak a saját feladataikkal foglalkoznak, mintha nem egy összefüggő, komplex rendszer alrendszerei lennének. Ezért elengedhetetlen egy program szintű irányító, koordináló és felügyelő központi szervezet, mert az e-közigazgatási és önkormányzati rendszerek megvalósítása csak a résztvevők szoros kooperációja és koordinációja esetén lesz sikeres. Azoknál az összetett és elosztott információs rendszer fejlesztéseknél, ahol a kialakítandó rendszer több alrendszerből áll, fejlesztését több, önálló közigazgatási szervezet irányítja és szerteágazó körnek nyújt szolgáltatást, ezeknél a rendszerfejlesztéseknél a fejlesztéseknek szigorú és következetes szakmai kritériumrendszerét kell létrehozni, és be kell tartani a fejlesztés logikai menetét.

Az e-közigazgatási és önkormányzati szolgáltatás-fejlesztések esetében ez a kritériumrendszer azt jelenti, hogy a szolgáltatási folyamatokat, valamint az olyan követelményeket – *mint az interoperabilitás, az IT biztonság, a fejlesztés-módszertan* – kell először meghatározni, és csak ezt követően kezdődhet az egyes központi és ágazati szakrendszerek és önkormányzati rendszerek tervezése és megvalósítása. A kiemelt projektgazdákkal együttműködve célszerű kialakítani azoknak a szabványoknak, előírásoknak, követelményeknek az ún. minimálisan szükséges körét, amelynek megvalósításával biztosítható az interoperábilis és biztonságos e-közigazgatás létrejötte.

Az e-közigazgatási fejlesztések sikerességének biztosításához nem elégséges összehangolt és egységes szempontokat követő informatikai fejlesztési módszertanokat és technológiákat alkalmazni. Ehhez szükség van a kifejlesztett rendszerek megfelelő üzemeltetésének biztosítására is. Ehhez már a fejlesztést megelőző projekt kezdeményezési, szállító-kiválasztási szakaszban meg kell határozni a rendszer későbbi üzemeltetésének követelményeit, feltételrendszerét. A rendszerek fejlesztésével párhuzamosan az előírt üzemeltetési követelményeknek megfelelően részletesen ki kell dolgozni a fejlesztett rendszerüzemeltetésre történő átadási és üzemeltetési feladatait, a támogatandó üzemeltetési folyamatokat, a szállító és megrendelő üzemeltetési időszakra vonatkozó felelősségi körét és feladatait, valamint biztosítani kell a jelzett feladatokhoz szükséges erőforrásokat.

5. Összegzés, következtetések

Az MNIK kialakítása az előzőekben ismertetett elvek és tartalmi elemek alapján jelenleg is folyik. Dokumentumai várhatóan ez év végig készülnek el. A MNIK az EU vonatkozó követelményeivel összhangban, ahhoz igazítva, de a nemzeti sajátosságok figyelembe vételével kerül kialakításra.

A MeH célja tehát azon feltételek megteremtése, amelyek biztosítják, hogy a magyar közigazgatás minden szervezete egységes elvekre és szabványokra épülő, hatékonyan és biztonságosan működő, ugyanakkor az elektronikus közszolgáltatásokat igénybe vevők érdekeit maximális mértékben figyelembe vevő rendszereket fejlesszen ki, és üzemeltessen. Fontos szempont, hogy ezek a rendszerek és elektronikus szolgáltatások képesek legyenek együttműködni a kapcsolódó európai rendszerekkel és szolgáltatásokkal, biztosítva ezzel a pán-európai szintű elektronikus szolgáltatások kialakítását.

Felhasznált irodalom:

[1] Pándi Balázs – Takács Attila – Pándi Erik: A közigazgatás elektronizálásának gyakorlata Magyarországon, Hadmérnök, Zrínyi Miklós Nemzetvédelmi Egyetem BJKMK, Budapest, 2008., ISSN 1788-1919, 101-102. oldal, 2008/1. szám;

[2] Baja Ferenc: Háttéranyag „E-közigazgatás keretrendszer kialakítása" projekt, Miniszterelnöki Hivatal, Budapest, 2008. június 13., 1-8. oldal, http://www.ekk.gov.hu/;

[3] Takács Attila – Pándi Erik: A hazai közigazgatás elektronizálásának helyzete, Hadtudományi Szemle, Zrínyi Miklós Nemzetvédelmi Egyetem KLHK, Budapest, 2008., 80. oldal, 2008/1. szám;

[4] Pándi Erik – Pándi Balázs: Az elektronikus közszolgáltatások nemzeti szabályozó hatóság részéről történő támogatottságának kérdései, Hadtudományi Szemle, Zrínyi Miklós Nemzetvédelmi Egyetem KLHK, Budapest, 2008., 108-109. oldal, 2008/1. szám;

[5] Pándi, Erik – Pándi, Balázs: Structural changes among domestic closed-purpose networks, „Kommunikáció 2007." nemzetközi szakmai-tudományos konferencia kiadványa, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2007., ISBN 978-963-7060-31-1, 254-256. oldal;

[6] Pándi, Erik: Modernisation process of public administration services, „Kommunikáció 2007." nemzetközi szakmai-tudományos konferencia kiadványa, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2007., ISBN 978-963-7060-31-1, 92-93. oldal;

SEBESTYÉN Attila[44]

AZ INTERNET A TUDOMÁNYMETRIA SZOLGÁLATÁBAN

*Absztrakt: Jelen közlemény vállalkozik, hogy **igazoljon egy hipotézist, amely szerint az Internet** jószolgálati **viszonyban van a tudománymetriával**, hova tovább a tudományos kommunikáció és publikálás eszközévé is válik. E téma öncélúan is érdeklődésem középpontjába került, hiszen kutatási témám szerint az Internetet - mint információs halmazt -, egy adott témában meghatározható tudás bázisaként kívánom bemutatni. Példát, megoldási módszert kívánok nyújtani szekunder kutatási célomhoz, a Rendőrségnél alkalmazott informatikai megoldásokban tárolt adatok feltérképezéséhez és tudástárba helyezéséhez.*

Kulcsszavak: Internet, IPv6, TCP/IP.

1. Áttekintés

Az Internet, a „világ információs sztrádája" mindössze 36 éves múltra tekint vissza. Az elosztott számítógépes hálozat a hidegháború következményeként is felfogható, az USA válaszlépéseként a Szputnyikra, a Szovjetunió 1957-ben felbocsátott műholdjára, illetve a szovjetek világkörüli űrutazásaira. Az USA Hadügyminisztériumán belül (Department of Defense) létrehozták a Fejlett Kutatási Projektek Ügynökségét (Advanced Research Projects Agency - ARPA), amelynek feladata volt olyan osztott számítógépes hálózat létrehozása, amely alapot teremt a katonai célú tudományos és technikai kutatásokra, és az ezekben a projektekben dolgozó szakemberek együttműködésére. Három, egymástól elszigetelt, párhuzamosan futó kutatás is folyt számítógépek hálózatba kötésének, a számítógépek erőforrás megosztásának, műszaki-technikai megvalósítására. A Massachusetts Institute of Technology (MIT) számítógép-hálózati projektje (1961-1967), a Rand Corporation védelmi célú kutatása (1962-1965), valamint a brit National Phisycal Laboratory számítógép-hálózati projektje (1964-1967). Az áttörés 1967. októberében történt meg a Tennesee állambeli Gatlinburgban tartott szakmai szimpóziumon, ahol mindhárom szakmai csoport képviselte magát. Larry Roberts nyilvánosságra hozta az első ARPANET tervet [1]. Egy csapásra megváltozott az addigi műhelymunkák folyamata olyannyira, hogy 1969-ben már működött négy csomóponton az elosztott hálózat:

a) UCLA (University of California at Los Angeles);
b) SRI (Stanford Research Institute);
c) UCSB (University of California at Santa Barbara);
d) University of Utah.

[44] szerző: Sebestyén Attila r. alezredes, PhD-hallgató, ZMNE KLHK Hadtudományi Doktori Iskola, Védelmi Vezetéstechnikai Rendszerszervező MSc. szak másodéves hallgató, ZMNE BJKMK Híradó Tanszék, ORFK osztályvezető

Az 1971-es évben már 15 csomóponton 23 számítógép működik, 1973-ban pedig megvalósul az első nemzetközi kapcsolat Norvégia és Anglia között. A katonai fejlesztésként finanszírozott, majd az egyetemeket, tudományos kutató műhelyeket összekötő hálózat 1990-re túlnőtte az ARPANET kereteit[2]. A TCP/IP alapú hálózat – a mai Internet – világhódító útjára indult, sorra fedezte fel magának az oktatás, a kereskedelem, az államigazgatás, a szórakoztató ipar, és az egyén is. Ma, mintegy 542 millió Host található az Interneten [3]. Kína Internetes forradalma miatt napi problémává vált az évtizednyire jósolt IP szám válsága. A mai négy tagú IP címmel közel 4,3 milliárd számítógépet lehetne megcímezni, de a számtartomány rossz felosztása miatt (20 éve az USA-ban alakultak ki a mai címmegosztási arányok), ténylegesen néhány százmillió számítógép címezhető csak meg. Ez pedig a globalizálodó világban kevés, elég ha csak a Host-ok számára hivatkozom. A holnap Internetje az IPv6-ra készül [4].

2. Problémafelvetés

A tudományos kutatómunka szempontjából az Interneten tárolt és elérhető információ halmaz több problémát vet fel. Ezek, az információ:

a) rendezetlensége;
b) hitelessége;
c) bibliográfiai hivatkozásra való alkalmassága;
ca) a forrás hivatkozásának lehetősége;
cb) a forráshivatkozás elérhetősége.

2.1. A rendezetlenség

Az Interneten való tartalomszolgáltatás határok nélküli, az egyén exibicionizmusától kezdődően, az egyes érdekcsoportokon keresztül, az állami köztájékoztatáson át az emberi élet minden területét felöleli. Ezek az információk, éppen az Internet lényegéből fakadóan, nem strukturáltak, a szolgáltatott adatok kapcsolatai, összefüggései, témaazonosságuk nem rögzített. Hogyan válhatott mégis az Internet a tudás megszerzésének elsődleges eszközévé?

Elsősorban természetesen a kereső alkalmazások, un. kereső szerverek segítségével. Ilyenek például a Yahoo, Altavista, Lycos, vagy Heuréka. A Google korábban kezdő oldalán hirdette magáról, hány Web lapon keres, ez akkor (2005. június 25-én) meghaladta a 8 milliárd oldalt [5]. Egyes felmérések szerint a kereső szerverek az Internet tartalmának mindössze 1/500-ad részét ismerik [6]. A számadatok alapján nyugodt szívvel kijelenthetjük, az Internet is rendelkezik a rendelkezésre álló tudás megismerhetetlenségének korlátjával, mint ahogy az összes nyelven valaha megjelent publikációk tudását sem birtokolhatjuk. Mindemellett a releváns szakirodalom eszenciáját, a specifikus mag által publikált műveket az Internetes forrásból is megismerhetjük [7]. Másodsorban a tematikus tartalomszolgáltató oldalak, portálok segítségével. A tematikus oldalak, valamilyen adott témához (fejezetcímhez) tartozó és annak megfelelő oldalakat tartalmaznak, illetve ilyen tartalomszolgáltatói oldalakat gyűjtenek össze. A Google „tematikus oldalak" kulcsra korábban (2005) még 483 oldalt sorolt fel, ez ma (2008. szeptember) már 151 ezer találatra bővült. Az ismeretbővülés nagyságrendbeli.

2.2. Hitelesség:

„Az Interneten szükséges és érdemes is megkülönböztetni a kereskedelemmel, illetve a puszta információcserével összefüggő kínálatot és szolgáltatásokat. Ez utóbbi alapvetően kétféle lehet …: a hagyományos kommunikációs folyamatban is részt vevő, ismert és a köztudatban már minősített, valamint az ismeretlen, azonosítatlan, lenyomozhatatlan forrásból való."[8]. Sajnos az azonosítatlan forrás kategóriájába kell sorolnunk minden, a lenyomozhatatlan forrás kategóriájába tartozó oldalt is. Nem elegendő az oldalon való szerzői hivatkozást tényként elfogadni, hiszen éppen a véleménynyilvánítás szabadságából, így a cenzúrázatlan megjelenésből fakadóan gyakran a szerző is „szerzői álnév" mögé rejtőzik. Az Interneten megjelenő tartalom szolgáltatások között hitelesnek tekinthető minden olyan államigazgatási, közfeladatot ellátó vagy hírközlő oldal, amely az oldalán impresszumát megjelenteti [9]. Természetesen a publikált adatok tekintetében hiteles oldalak nagyságrendekkel nagyobb számban vannak jelen az Interneten, mint az itt megfogalmazott kör - gondoljunk csak a saját magunkról, tevékenységünkről készíthető ingyenes oldalakra -, véleményem szerint azonban tudományos kutatás forrásaként az e körön kívüli oldalak, fenntartással alkalmazhatóak. Elsősorban nem a hitelesség okán, hanem a forrás rendelkezésre állásának, a publikáció állandóságának okai miatt. És itt el is jutottunk a következő mérlegelési szemponthoz.

2.3. A bibliográfiai hivatkozásra való alkalmasság:

Sajnálatos tény, hogy még abban az esetben is, ha a keresett témát, vagy adatot meg is találtuk az Interneten, és azt olyan helyen találtuk is meg, amelyet – valamilyen ok miatt – hitelesnek tekintünk, még így sem biztosított egyértelműen, hogy tudományos publikációnkban, mint forrást, azt egzakt bibliográfiai hivatkozással megjeleníthetjük [10]. Az Internetes oldalnak bár van egyedi, ún. URL címe, és az adott lapon többnyire szabatos hivatkozással, egzakt módon meghatározható a felhasznált adat – pl.: negyedik francia bekezdés 6. oldal -, mind emellett az egyéb, az írott publikációkra vonatkozó adatok (úgy, mint szerző, cím, kiadó, kiadás száma, éve, oldal stb.), hiányosan adhatók meg, vagy teljesen hiányoznak a forrásból. Tapasztalataim szerint a másik alkalmatlansági tényező, az oldalak elérhetősége, pontosabban elérhetetlensége, ugyanis amilyein szabados a publikálás lehetősége, legalább annyira változó az oldalak fennmaradása és törlése is. Jómagam több tucat mára elérhetetlen URL címmel rendelkezem, amelyeket korábbi tanulmányaim során rögzítettem. E szempontok szerint az Internet és a tudománymetria viszonyának vizsgálatára olyan, a kereső szerverekkel megtalálható, magyar nyelvű oldalakat tekintettem forrásnak, amelyek hitelességét az oldalak impresszioma szerint általánosan elfogadottnak ítéltem. Külön fontosnak tartom megjegyezni a hitelesnek talált dokumentumok esetében az ISBN szám megjelölését, illetve azt a tényt, hogy az Interneten egyre növekvő számban megjelenő elektronikus publikációk következtében 2007. január 01-től Magyarország is áttért a korábbi 10 jegyű ISBN számról az EAN-13 kód adaptálását lehetővé tevő 13 jegyű ISBN számra [11]. A témám szerinti kulcsszavak keresések során (Internet tudásbázis, tudás alapú rendszer) örömmel vettem tudomásul, hogy a levéltárak mód-

szeresen felépített tartalomszolgáltatói oldalakkal vannak jelen, ahol nemcsak az írott publikációk reprint példányai, de elektronikus irodalmi alkotások is megjelennek. Például a Magyar Elektronikus Könyvtár oldalán hadtudomány és katonapolitika témakörben már 15 tematikus területre felosztott keresési lehetőség áll rendelkezésre [12]. Mondhatni természetesen, a Magyar Tudományos Akadémia is jelen van az Interneten, mind on-line adatbázisával, mind e-folyóirataival [13]. Az Internet és a tudomány kapcsolatában az Internet „ősidejétől fogva" a legjelentősebb szolgáltatásnak az elektronikus levelezést és később az erre alapuló levelezőlistát tartom. A tudományos kutatás két publikáció közötti tevékenységében, „válaszút előtt", az informális kapcsolatokkal támogatott döntés, vagy ennek előkészítése, pótolhatatlan lehetőség. És ez így volt a tudomány „ősidejében" is. Azonban más, kézzel írottan, egy-egy példányban, lassú postai úton közvetítve terjeszteni eredményeinket, és más elektronikus levélként egy példányban megírva és számos címzettnek percek alatt eljutatva tenni ugyanezt. Más dolog tudományos folyóiratban megjelentetni 2-7 év időtartam alatt, ahogy ez az Academia Royale des Sciences: Histoire et Memoires –ben történt [14], és megint más „pillanatok alatt" az érdeklődők elé tárni, akár interaktív módon is azt. Ez a tudományban is felgyorsult Internetes Világ. Ne feledjük azonban Manten szavait: „a tudományos infromáció publikálása nem azonos a nyilvános terjesztéssel"[15] és gondolataim itt találkoznak az Internettel kapcsolatos előzményeimmel.

3. Tudománymetria az Interneten

Ebben a viszonyban két markáns megközelítés különíthető el. Egyik a tudománymetriának, mint témának (a tudománymetriáról szóló oldalak, és tudománymetriát, mint módszert alkalmazó publikációk), másik az Internetnek, mint a tudománymetria eszközének témája. A tudománymetria (scientometric - 36000) az Interneten 2620 alkalommal fordul elő (2008. szeptember). Együtt az Internet kifejezéssel ez a szám 526 (scientometric and Internet – 10100). Tovább szűkítve a találati arányt az eszköz kifejezéssel összesen 188 találatot kaptam (scientometric and Internet and tool - 14400). Ténylegesen az Internettel, mint a tudománymetria egy lehetséges eszközével 1 oldal foglalkozott [16]. A Magyar Elektronikus Könyvtár könyvkeresés oldalán 9 on-line kereső rutin található, amelyek – az ismétlődésektől eltekintve - összesen 44. könyv ajánlat szerepelt. A listából Bujdosó Ernő: Bibliometria és tudománymetria című művét választottam ki, amelyet Budapesten az OSZK-KMK az MTA Könyvtára gondozásában 1986-ban jelentetett meg. ISBN száma 963 201 263 1, lelőhelye a Semmelweis Egyetem Központi Könyvtára. Az oldalról kérőlap karton is nyomtatható.

A következőkben a publikáció Internetes változatának megkeresését céloztam meg. Két oldalon, mint forráshivatkozást találtam, magát a könyvet elektronikus formában nem sikerült sem tematikus oldalon, sem e-könyvtár, sem más tartalomszolgáltatói oldalon megtalálnom. Több helyütt, regisztrációhoz volt kötve az adatbázisban való keresés, illetve az e-könyv letöltése és olvasása – ilyen például az UHU.hu oldal – ezeken természetesen hozzáférés hiányában nem sikerült keresnem. Sikertelenségem miatt, az MTA oldalához fordultam, de sajnos a publikációk csak 1992-től kereshetők a www.mtatpa.hu oldalon. Természetesen eredeti kutatási

témámat érintően is keresést indítottam (ezek a tudásbázis, tudásmenedzsment, adatbányászat, adattárház), abban bízva, hogy az általam kutatott tudományterület fiatal, kialakulóban lévő, így az 1992-es korlátot nem haladja meg, és szerencsésen 171 találatot kaptam is a tudás* -hoz kapcsolódóan. Sajnos a publikációkhoz felhasználói jogosultság hiányában nem férhetem hozzá. Maradt a „nyilvános" keresőszerverek szerinti forráskutatás, tudásmenedzsment címszó alatt (2008. szeptember) 93300 találatot kaptam, ISBN –nel kiegészítve 943-et. Az adatbányászattal kiegészítve a keresés 87 találatot adott, amelyek közül 4 elektronikus reprint publikáció, illetve 5 linken további forrásjegyzék található.

Hipotézisem, a magam által meghatározott korlátok között, csak részben talált igazolást. Az Internet a tudományos kommunikáció és publikálás eszközévé vált, elsősorban az elektronikus levelezés és az arra alapuló levelezőlista miatt. A cenzúrázatlan, szabados, talán szélsőségesen liberalizált publikálási lehetőségként nem igazolta a hozzá fűzött reményeimet az elektronikus dokumentumok terén, mert olvasható szakanyagokat nagyobb részt hozzáférési korláttal, vagy időintervallum korláttal találtam. Az Internetes forráskutatást, mind emellett hasznos kiegészítőjeként értékelem a levéltárban, vagy a könyvtárban végzett katalogizált keresésnek, hiszen témára, szerzőre, sőt un. szabad szöveges keresésre is meggyőző sokasággal adott találatot. A tematikus és elektronikus könyvtári oldalak (ez alatt értve a könyvtárak on-line szolgáltatását, minimálisan a kartoték elektronikus elérhetőségét), rövid befektetett idő alatt megfelelő számú, és minőségű, a hozzáférést kielégítően biztosító megoldást adott – akkor is, ha az a papíralapú publikáció elérhetőségi adatainak biztosítását jelentette. Fontosnak tartom megjegyezni azt is, hogy Hazánkban jelenleg folyik az Internet forradalma, a szélessávú Internet elérés infrastruktúrájának megteremtése, a szolgáltatások számítástechnikai alapokra helyezése (utalva itt például az e-kormányzati törekvésekre) [17]. Jól mutatja az Internet alkalmazásának, mint technikai eszköz rendszer alkalmazásának, különbözőségét a magyarországi és egyéb találatok közötti különbség. A tudománymetria és scientometric találati számának viszonya alig több 7% -nál. Az információs technológia térnyerését legalább ilyen módon igazolja, hogy újszerűnek, és önön magának való témában, mint például a tudásmenedzsment és a knowledge basis közel azonos számú találatot ad (2008. szeptember - tudásmenedzsment 958000, knowledge basis 101000).

4. Összegzés, következtetések

Véleményem szerint az Internet, mint eszköz, helyénvaló kutatási segédeszköz a XXI. században már Magyarországon is. De kiegészítője, és nem helyettesítője a papíralapú, levéltári és könyvtári forráskutatásnak. És végezetül had ajánljam figyelmébe annak az elvetemült olvasónak, aki az Internetet a kutatómunka eszközeként kívánja felhasználni Barry Schwartz: A választás paradoxona. (Miért a kevesebb a több?) című könyvét [18]. Az Internet világában, ahol manapság (2008. szeptember) már több mint 542 millió Host, több mint 8 milliárd indexelt oldalt kezelő kereső motor, címszavakra könnyen 10, 100 ezer, nemegyszer milliós találati lista, fizikai képtelenség minden forrást megismerni, nem hogy „érdemi" isme-

retet szerezni. Igazi kihívás, zsonglőri ügyességet igénylő kulcsszavas mágia, de ez már egy messze vezető új gondolat sor …

Felhasznált irodalom:

[1] http://izzo.inf.elte.hu/~hehe/ve2002/halozat/tori.htm (2.bekezdés)
[2] http://www.inf.unideb.hu/~bodai/internet/internet_tortenete.html#Feladatok (3. bekezdés)
[3] http://www.isc.org/index.pl?/ops/ds/
[4] http://www.csatolna.hu/hu/erdekes/Grin/erdekesg1.html
[5] http://wikipedia.org/wiki/Google
[6] http://www.sg.hu/cikkek/12227
[7] Tudományos kutatás elmélete II. – szemelvények a tudománymetria témaköreiből (szöveggyűjtemény a doktori képzésben résztvevők részére) ZMNE Budapest 2003. – összeállította Dr. Szilágyi Tivadar, Dr. bujdosó Ernő: Bibliometria és tudománymetria című könyve alapján (Budapest, 1986 ISBN 963 201 260 1) 33. oldal 3. bekezdés
[8] http://www.piacesprofit.hu/?s=32&n=4&mr=154
[9] Pándi Erik: Trendek és kihívások – zártcélú hálózatok a globális térben (tanulmány), ZMNE, Egyetemi Könyvtár, Budapest, 85-89. oldal, 2007.
[10] Dr. Gőcze István: A tudományos kutatás elmélete és módszertana – előadás vázlat doktorandusz hallgatóknak, ZMNE Filozófia és kultúrtörténeti tanszék 2003. – A bibliográfiai hivatkozások fontosabb előírásai 3. oldal
[11] http://wikipedia.org/wiki/ISBN
[12] http://mek.oszk.hu/html/vgi/kereses/keresesuj.phtml?tip=temak&fotema=tarsad
[13] http://www.mtak.hu/hun.html
[14] Tudományos kutatás elmélete II. – szemelvények a tudománymetria témaköreiből (szöveggyűjtemény a doktori képzésben résztvevők részére) ZMNE Budapest 2003. – összeállította Dr. Szilágyi Tivadar, Dr. bujdosó Ernő: Bibliometria és tudománymetria című könyve alapján (Budapest, 1986 ISBN 963 201 260 1) – 44. oldal
[15] ua. mint 13., - 16. oldal
[16] http://zrinyi.zmne.hu/kulso/mhtt/hadtudomany/2004/3_4/2004_3_4_8.html - Hangya Gábor és Kende György: Az informatikai forradalom hatása a forráskutatás rendszerére – Hadtudomány XIV. évfolyam 2004. november 3-4. szám vezetés-kiképzés
[17] Pándi Balázs – Takács Attila – Pándi Erik: A közigazgatás elektronizálásának gyakorlata Magyarországon, Hadmérnök, ZMNE BJKMK, Budapest, 2008., ISSN 1788-1919-101. oldal, 2008/1. szám
[18] Barry Schwartz: A választás paradoxona (Miért a kevesebb a több?) – Lexecon Kiadó Győr 2006. – ISBN: 963-06-1222-4 – ISBN-13: 978-963-06-1222-7

PÖLCZ Péter:[45]

A TÁBORI VEZETÉSI ÉS IRÁNYÍTÁSI INFORMATIKAI RENDSZER KIALAKÍTÁSA

Absztrakt: A tábori vezetési és irányítási informatikai rendszer a vezetői információs ellátás és döntéstámogatás szerepét tölti be oly módon, hogy a döntések automatizáltan és irányítottan jutnak tovább a végrehajtó egységek felé, míg ellentétes irányból a döntések előkészítéséhez, helyzetelemzéséhez és meghozatalához szükséges (felderítési, visszajelzési) információk áramlanak. A rendszernek illeszkednie kell a NATO elvárásaihoz (interoperabilitás) és információs segítséget kell nyújtania a harcoló vagy békefenntartó erőknek. Megvalósíthatóságának követelményei a fizikai rendszer kívül a döntéshozatali rendszerbe történő beépülésen keresztül zajlik. Jelen közleményben a szerző megvalósítási a korszerű követelményeknek megfelelő javaslatokat tesz.

Kulcsszavak: C2, CIS, HW, SW, tábori híradó és informatikai rendszer, vezetés-irányítás.

1. A tábori vezetési és irányítási informatikai rendszer szerepe és feladatai

A XXI. század hadviselését és hadvezetési stratégiáját erőteljesen átformálta az ellenségkép megváltozása, valamint az alkalmazott és újonnan megjelent technikák és rendszerek komoly együtthatásai. A világban folyó változások, melynek fő irányvonala a globalizáció, új „típusú ellenség (terrorizmus)" megjelenését hozta létre. Az változások dinamikájából adódóan a globális rendszerek legrugalmatlanabb részei úgymint a vallás, ideológia, etnikai hovatartozás stb. egy új „belső" ellenséget, a terroristákat hozták létre. A honvédségek és hadseregek egységes szövetségbe való tömörülése komoly kihívásokat jelent a katonai rendszerek együttműködése, és irányítása számára. A közös kommunikációs és műveletvégző platformot a már világméretű elterjedésű informatikai rendszerek adják, illetve adhatják (a nagy létszámú hadseregek irányítása már csak egy információs hálózaton keresztül valósítható meg). A Magyar Honvédség szerepét és feladatait a katonai stratégák a szövetséges erőkkel (NATO) együttműködve határozzák meg.

Mivel az együttműködő hadseregek különböző országokból, különböző hagyományokból és struktúrákból állnak össze lassan globális rendszerré így komoly felülvizsgálatot igényel a rendszer elemeinek funkcionális, informális és feladatvégző elemzése. A Magyar Honvédség működő döntéshozó, valamint együttműködő képességét a szövetséges erőkkel, komolyan befolyásolja az infokommunikációs, információgyűjtő, feldolgozó és döntés előkészítő rendszer, amely gyorsan, címzetten, azonosíthatóan vezérelhető és irányítható. Mindezt oly módon, hogy az információáramlás valós kétirányú mozgása miatt azonnali infor-

[45] Szerző: Pölcz Péter, Védelmi Vezetéstechnikai Rendszerszervező MSc. szak másodéves hallgató, ZMNE BJKMK Híradó Tanszék

máció gyűjtő és válasz (reagáló) rendszerek és szoftverek képezik. Előzőek alapján a Magyar Honvédség jelen és jövőbeli feladatait csak egy átfogó infokommunikációs rendszer (hardver, szoftver) kialakításával láthatja el, amely a kisebb, de hatékony egységek vezetésétől és irányításától kiindulva egészen a felső szintű vezetési parancsnokságig terjedve lefedi a felderítő, elemző, integrált adat-hang és kép kommunikációs, beavatkozó, irányítási rendszerét. Mindezt lehetővé téve oly módon, hogy bekapcsolódási pontokat biztosít a baráti, illetve együttműködő (EU, NATO) informatikai és infokommunikációs vezetésirányítási rendszere felé. A Magyar Honvédség feladatköreinek változása (terrorista ellenes egységek, rendvédelmi, katasztrófa védelmi, békefenntartó, támogató egységek stb.) szükségessé teszi, hogy rendszereinek és egységeinek elérése, vezetése és információval való kétirányú ellátása, a szélsőséges időjárási viszonyok mellett országos és leválasztott rendszerben is működőképes maradjon. Vagyis a rendszer legkisebb eleme is önálló működésre képes legyen mind eszköz, mind szoftver, mint kommunikációs szinten, betartva az ilyen jellegű hálózatokkal és rendszerekkel szembeni műszaki, technikai követelményeket. A közlemény kidolgozásakor a jelenleg elfogadott és NATO rendszerekben is alkalmazott szerver-terminál rendszerű kialakítást implementáltam a hazai elérhető informatikai struktúrák figyelembevételével a Magyar Honvédség számára.

2. A rendszer alkalmassága az informatikai hadműveleti vezetés számára

A kialakítandó informatikai rendszer alkalmas kell, hogy legyen a hadsereg vezetésére és irányítására mindazon körülmények feladatok között melyre a Magyar Honvédség önállóan és a nemzetközi partneri viszonyaiból származóan, számíthat és elláthat. A rendszernek minden olyan információt és döntéstámogatói adatot össze kell gyűjtenie és rendszerezett formában a döntéshozók felé megjeleníteni, döntésre előkészíteni, ami a katonai vezetési és irányítási rendszerekben a legkisebb egységtől a vezetés legfelső szintjeiig szükséges. A rendszer feladatai közé tartozik, a kétirányú kommunikáció (jelentés és irányítás), információgyűjtés (elektronikus tevékenység, adat, kép, hang, környezeti változók, ellenséges tevékenység), adat és információtovábbítás, tárolás, feldolgozás, elemzés, döntés előkészítés, döntési javaslat, hatáseredmény szimuláció, irányított parancstovábbítás és hatás visszajelezés (hatékonysággal, eredményességgel kiegészítve). A rendszernek biztosítania kell a redundanciát, kieső egységek (elveszett, megsemmisült, illetéktelen vagy ellenséges kezekbe került), leválaszthatóságát, helyettesíthetőségét a kapcsolatok és adatok védelmét és biztonságát, az újonnan belépő egységek gyors beilleszthetőségét. A rendszer hardver és szoftver elemeinek síkonként tagozódnia kell, oly módon hogy a legkisebb egységtől felfelé haladva a hierarchikus létrán a rendszer és a síkok eszközeinek képességei és kapcsolódási pontjai növekednek mindkét irányban. Természetesen az egyes síkok tagozódása és kapcsolódása egy bonyolult de modellezhető hálót ad ki, amely kiterjedésük szerint is csoportosíthatóak és rétegezhetők. Műszaki, logikai megközelítésben a a rendszer leginkább fa struktúrát képez, de egyes moduljai ezen belül csillag architektúrát igényel.

Az informatikai rendszert fontos hogy infokommunikációs rendszernek tekintsük, mivel az információk begyűjtése, célba juttatása, felhasználása és a képződött eredményből való cselekvés végrehajtatása a kétirányú információ és adatáramlást, az információt közvetítő közeget, a megszerzett és mozgatott információk biztonságát együtt jelenti. Röviden tehát információról csak akkor van értelme beszélni, ha azt el is tudjuk juttatni a feldolgozó vagy végrehajtó egységhez. Tehát információ csak a biztonságos kommunikációs csatornák kiépítésével és célbejuttatásával válik használhatóvá. Mivel az informatikai rendszerek fejlettsége lehetővé teszi, hogy az adatok (melyek bármilyen adatgyűjtőből, személytől vagy eszköztől is érkeznek),mellet képi, hang , állapot , folyamat információt is továbbítsunk. Ha az infokommunikációs rendszerünket a fentek alapján elemezzük, úgy rá kell, hogy jöjjünk, hogy strukturált rendszerben a beszéd, a képi és az adatcsatornákat is azonos módon kezelhetjük. Így létrehozhatjuk az adatok (legyen az informatikai, képi, vagy akár hang) egységes védett, vagy titkosított rendszerét és ennek alkalmazására a nyílt vagy védett csatornájú megbízható, többirányú és síkú infokommunikációs hálózatot, melynek alapja az informatika, az IT hálózati eszközök, az elektronikus vagy optikai telekommunikációs rendszerek, valamint a működtető és kommunikációs, felderítő és védelmi programok. A Magyar Honvédség és védelmi szféra számára kiépítendő informatikai irányítási rendszernek alkalmasnak kell lennie a különböző események felderítésére, továbbítására, ábrázolására, gyors megjelenítésére, a döntéstámogatásból adódóan automatikus döntési javaslat elkészítésére, szimulációk azonnali futtatására.

3. A kialakítandó rendszerek hardware és SW követelményei

3.1. A HARDVERREL szemben támasztott követelmények

Az alkalmazott eszközöknek teljesíteniük kell a megfelelő katonai szabványokat és elvárásokat. (pl.. rázásállóság, hideg és meleg állóság, adatbiztonság, hozzáférési és behatolás vagy bontás biztonság, ellenőrizhetőség, szoftver biztonság, szoftver követhetőség,). A hardver eszközökkel szemben támasztott követelmények:

Sor szám	TEMPEST	RUGGED
1	Asztali, Állványos kat. 1 (Tempest Level 1)	Irodai kivitelű eszközök Homogenitás, csereszabatosság
2	Asztali, Állványos kat. 2 (Tempest Level 2)	Konténerbe építhető Keskenyebb környezeti feltételekkel bíró Rázásállóság
3	Notebook (Tempest Level 1)	Vezetési buszba, sátorba telepíthető Szélesebb környezeti feltételek Gyorsabb mobilitás Nagy megjelenítők
4	Vezetési pontok konténereibe építendő (Tempest Level 1)	Harcjárműbe telepíthető Szélesebb környezeti feltételek Komoly ütés és rázásállóság Egységvezérlő és mérőeszköz interface Víz és por állóság

5		Szabadba telepíthetők Nagyon széles működési spektrum Gyors áttelepíthetőség Kommunikációs csatorna biztosítás Por és vízállóság (IP 65)
6		Kézi adatgyűjtők A legszélesebb spektrumú környezetállóság Legkomolyabb rázás vibráció állóság Folyóvíz és por állóság Helyzetmeghatározó rendszer Kommunikációs rendszer kapcsolat

A **hardver követelmények** kialakításában komoly szerepet játszik a redundancia mind a kapcsolati módokban, mint a megbízható működésben. A szabványoknak való megfelelőségen kívül a rendszer egyes elemeinek kapcsolódásakor komoly szerepet kell, hogy betöltsön az behatolás védelem (informatikai, hírszerzési)és azonosíthatóság. A rendszert úgy kell kialakítani, hogy a megfelelő adatszintekhez csak a megfelelő személyek juthassanak hozzá. A feladatokat a többlépcsős azonosító rendszerrel lehet megoldani. A centralizált rendszert tökéletesen lefedi, ha a harcálláspontok rendszerei egymásnak tükrözött képei. A centralizált és szétosztott rendszer (könnyen kialakíthatóan) rendelkezik a biztonsághoz hozzáféréssel (központi ellenőrizhetőség), az egyszerűbben megoldható fizikai védelemmel, és mindezeket ötvözendően a redundanciából adódó adatvédelemmel és csereszabatossággal. A biztonságot tekintve a meg lévő információk minősége és szintje miatt a zászlóalj alacsonyabb besorolású információvédelmet igényel, de itt is a központi rendszerek védelme (itt alakul ki az információs bázis első komolyabb hálópontja) kiemelt figyelmet érdemel. Az egységek gyors reagálását és bizonyos fokú szabadságát (lásd: NATO rendszerek) az első „információs csomópont" vezetési döntései határozzák meg. A hardver megjelenésének másik fontos szerepe a fix IP cím használata a rendszerben. Ennek oka a hardver eszközök gyors azonosítása, szükség esetén letiltása és ellenőrizhetősége. Katonai fogalmak szerint az ellenség barát felismerés fontos részeleme. (Az egész honvédségi rendszerben csoportonként csak egy adott IP című hardver egység szerepelhet. Minden az engedélyezett IP címtől és azonosítótól való megjelenés illetéktelen és ellenséges hozzáférésnek minősül, melyet a központi hardver és szoftver letilt, illetve azonnal riasztja az adminisztrátor személyzetet.)

3.2. A SZOFTVERREL szemben támasztott követelmények

A szoftver rendszerében a megvalósítandó rendszer kell, hogy rendelkezzék a hozzáférési védelem különböző szintjeivel (NATO ajánlások szerint MS NT, MS Win 2000, MS Win XP operációs rendszerek biztosítják ezt, de gondolatként megjegyezném, hogy az új elképzelések szerint a nyílt forráskódú rendszerek az adatkiszivárogtatás elleni védelmet is jelenthetik, lásd: Microsoft és az információgyűjtő és jelentő rendszerei-bár ezek zárt rendszerben életképtelenné válnak.). A szoftver alrendszereknek alkalmasnak kell lenniük különböző platformok futtatására, mégpedig olyan módon, hogy a felsőbb kapcsolat felé a nyelvi eltérések nem akadályozhatják a kommunikációt, a térgrafikai rendszerek futását nem lassítja, és nem

okoz rendszerleállásokat. A szoftver felépítésnek a következő piramis elvet kell követnie.

1. számú ábra: a szoftverfelépítés (forrás: szerző)

A szoftver rendszernek olyan szerkezetűnek kell lennie (modularitás), hogy a rendszer egyes elemeinek kiválásakor azok önálló életre, és működésre legyenek képesek. A rendszernek alkalmasnak kell lennie békeidőkben bekapcsolódni és támogatni a Magyar Honvédség országos béke hálózatát és üzenetküldő rendszerét, valamint egyes egységek leválásakor (békefenntartás, katasztrófa, terrorcselekmény stb.) önállóan alkalmasnak kell lenni az adott egység off-line vagy standalone működésére. **Fontos,** hogy a szoftver feleljen meg annak a követelménynek, hogy a rendszert, mint egységet és egészet tudja kezelni, illetve védve legyen az informatikai támadásokkal szemben. A tábori informatikai rendszer mind zászlóalj szintig bezárólag mind ez felett fix IP című kommunikációval és azonosítóval rendelkező komplett SW ellenőrzést valósítson meg. A rendszer kialakítására javasolt a terminál szoftveres megoldás, amely lehetővé teszi a gyors ellenőrzést, így a rendszerben egyidejűleg csak egy azonos IP címmel rendelkező számítógép lehet. Továbbá megoldja a centralizált adatkezelést és biztonságos adathozzáférés kérdését oly módon, hogy bármely eszköz illetéktelen kezekbe jutásakor az információ nyilvánosságra kerülése szinte lehetetlen. A tábori vezetés informatikai rendszere alkalmas legyen, tehát legyen is kapcsolódási felülete a Magyar Honvédség által használt többi program felé. A rendszerben alkalmazott SW és programok feladata, hogy a megfelelő szintű interoperábilis kapcsolatok mellett a hazai igényeket és elvárásokat kielégítve megfelelő adatbiztonsággal a katonai vezetés számára átlátható eszköztárral a döntés és információ előkészítést és feldolgozást, hatás szimulációt biztosítson. Fontos szempont az adatvédelem a megbízható kapcsolatok és kommunikációs vonalak kiépítése és megléte a szükséges a titkosítás és rendszer redundancia. A Magyar Honvédség számára kialakítandó rendszer HW követelményeiben fontos szerepet kell betöltenie a felhasznált eszközök „alkalmazkodó" képességének.

A hardver elemek tekintetében a környezeti igény szerint két csoportot (TEMPEST, RUGGED), illetve csoportonként 3-6 különböző „teherbírású" infokommunikációs eszközcsaládot kell, hogy különböztessünk. Fontos, hogy a rendszerek modulárisan bővíthetők legyenek (rendszer homogenitás), illetve legyenek is a bővítésükhöz szükséges moduljaik. A magyar fejlesztőkapacitások, és

gyártások előny kell hogy élvezzenek, mivel a források, és a fejlesztési illetve gyártási lehetőségek a magyar ipar támogatottsága mellet nemzetbiztonsági és SECOP érdek.

4. A rendszer fizikai elhelyezése (járművön, konténerben, terepen), valamint bázis körülmények között

A rendszer elhelyezés szempontjából lehetséges eszközök úgy, mint konténer (hordozójárművön, vagy letelepítve), sátorban illetve törzsbuszban, terepi körülmények között (szabadban). A fix telepítésű rendszerekben ugyanazok a fizikai követelmények vannak, mint a kommersz eszközök esetében. A rendszer adatbiztonsága miatt kialakított rezsim intézkedések azok, amelyek a környezeti feltételeket megváltoztatják. A konténeres kialakítás szempontjai:

- A konténer rázkódása miatt az eszközöket vibrációelnyelő alapzattal rendelkező állványokba kell szerelni (amortizáció);
- A központi gép (szerver) konfigurációját úgy kell specifikálni, hogy mind a feldolgozó egység (központ) és mind a háttértár redundánsan és két különböző állványban kerüljön elhelyezésre (oka az esetleges állványzat vagy „rack" meghibásodása vagy extrém körülmények közti sérülése ne okozza mind két egység kiesését;
- A központi rendszer mellé helyezhető elemek a konténeren belül kialakított adminisztrátori munkahely kliens gépei;
- A hálózati illetve kommunikációs eszközök a kábelrendező egységgel együtt kell, hogy beépítésre kerüljenek;
- A konténeren belüli adatkommunikáció gerinc interfésze gigabites hálózat, amely a réz alapon is kapcsolódhat egymáshoz, de lényeges hogy ebben az esetben a konténer maga egy zárt megfelelően földelt Faraday ketrecet képezzen, a kompromittáló kisugárzások elkerülésére;
- A kifele irányuló kommunikációs lehetőségek miatt a kilépő adatvonalak árnyékolt kábelen történő kiléptetése szükséges;
- A beépített adminisztrátori munkaállomások monitorai a külső betekintés elkerülése végett a bejárattal ellentétes irányban kell, hogy legyenek. (Az adminisztrátor rálát a bejáratra);
- A konténeres rendszer két fajta kivitelben szerepelhet, úgymint ablakkal ellátott és ablaktalan felépítményben (a központ rendszer, ahol az adatok összesítődnek ajánlott, hogy ablaktalan felépítmény legyen az EMC kisugárzás biztonságos leárnyékolására. A törzsbusz, vagy konténeres feldolgozó lehet ablakos kivitelű, de a behatolás védelmet (rács) és kisugárzás védelmet itt is meg kell oldani.

Fontos paraméterek a központi rendszer kialakításakor:

- Az alkalmazott rendszer hőmérséklet tűrése a kommersz eszközökével azonos (a konténert klimatizálni kell belülről);
- A informatikai rendszernek amortizálásakor figyelembe kell venni, a hogy a rendszer legkényesebb pontja a RAID diszkes háttértároló alrendszer;

- A szünetmentes tápegységek kialakításakor a méretezési időt az áramforrás (aggregátor) cseréjének vagy üzemanyaggal való feltöltésének maximum ideje adja;
- A szünetmentes egységekkel való ellátást lehet központi egységgel is biztosítani, de ebben az esetben ennek fizikai mérete kérdéses lehet;
- A szünetmentesre való átálláskor a nyomtatási feladatok várakozó sorba kerülnek, mivel a nyomtató nagy energiaigénye jelentősen csökkentené az áthidalási időt;
- A nyomtatás formája illetve minősége a központi konténerben az információ minősége szerinti módon vagy betekintéssel történhet;
- Az adatbeviteli egyéb eszközök elhelyezése a központi számítógép környezetében lévő LAN hálózaton csatlakozó konténerben vagy buszban lehetséges (plotter, szkenner, stb. Fontos hogy ilyenkor a feladatot végző számítógép megfelelő hozzáférési és adat, mentési hellyel illetve jogosultsággal rendelkezzen);
- Mivel a központ a rendszer egyik legkényesebb eleme fontos a konténerbe való be és kilépés rögzítése és ellenőrzése (ezért szól a javaslatban a kettős belépő ajtó használata).

Az adatfeldolgozó kialakításának szempontjai a konténerben:
- A központi szerver bázishoz közel (2-4 km sugarú körben) kerülhet elhelyezésre az adatfeldolgozó konténer(k);
- Az adatfeldolgozó alegység a kezdetben vázolt koncepció alapján csak terminál üzemmódokat láthatna el;
- Az adatfeldolgozó szerepénél fogva korlátozott kialakítású de rázásálló rendszerkialakítást igényelne;
- Az adatfeldolgozó konténer infokommunikációs útvonala minimum két redundancia szinttel kell, hogy rendelkezzen;
- A vezetési csúcs felé haladva az információk miniségének formája miatt a kapcsolata a központtal optikai kábelen és titkosított mikrohullámú (Wireless) LAN hálózaton lehetséges;
- Az adatfeldolgozóba való belépés központ ellenőrzését meg kell oldani;
- Az adatfeldolgozó konténerben kerülne elhelyezésre a plotter, a színes nyomtató, a szkenner.

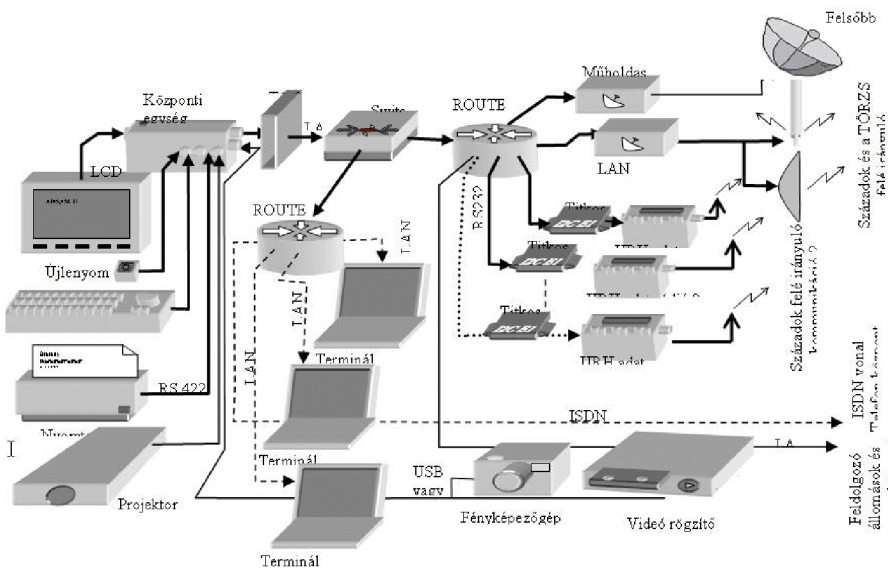
Fontos elvárások az adatfeldolgozóval szemben:
- A az adathozzáférés terminálomként és személyenként változhat (dedikált IP címek);
- Az adatfeldolgozó ablakát belátás és kisugárzás elleni védőfóliával kell ellátni;
- Az infokommunikációs rendszert zárhatóvá kell tenni;
- Az eszközös adatbevitel (szkenner) hozzáférését személyre szólóvá kell tenni;
- Javasolt az azonosító (beléptető kártyák) használata az információs rendszerhez is;

- Más eszköz csatlakoztatását lehetetlenné kel tenni (nincs kiépített szabad csatlakozás);

5. Mobil vezetési rendszer kialakítása

A mobil vezetési rendszer kialakításakor a szóba jöhető hordozó jármű, pl. konténer, BTR speciális kialakítási igényeket és elvárásokat támaszt, úgymint:

- Nagy rázásállóság;
- Komoly hőmérsékleti ingadozás;
- Por, vízállóság;
- 24 V-s energiaellátás;
- Kis beépíthető méret;
- Speciális csatlakozási felületek;
- Viszonylag kis hatótávolságú folyamatos adatkapcsolat;
- Redundáns kommunikáció.

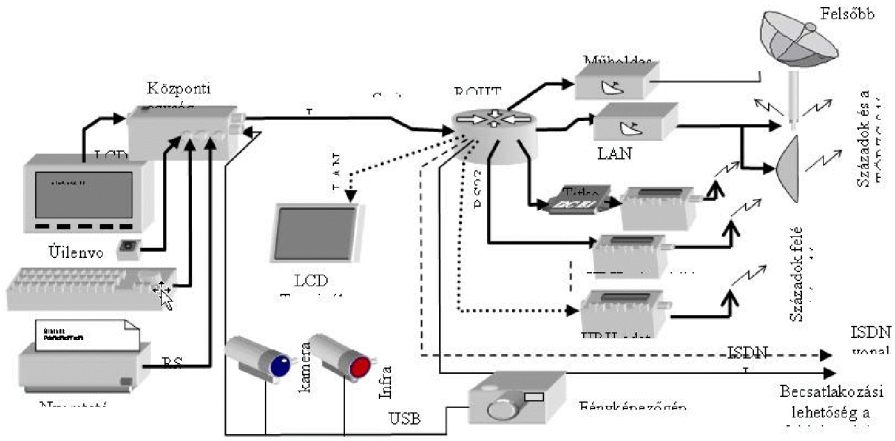


2. számú ábra: A mobil konténeres vezetési pont kialakítása (forrás: szerző)

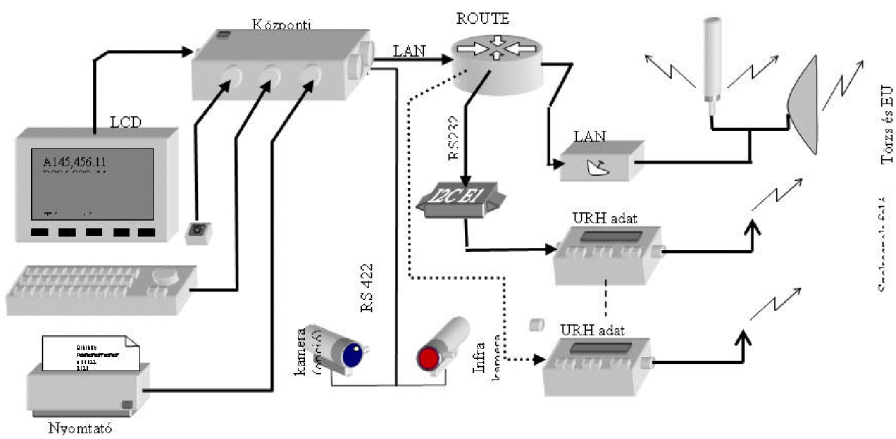
Az előzőekben említett kialakításokból származó hátrányok:

- Kisseb adatmennyiség tárolható;
- Kevesebb feldolgozó egység (alkalmanként csak maga a vezetési pont gépe);
- Kisebb megjelenítő panel (a beépíthetőség miatt 12-15" max.);
- Korlátozott térgeometriai megoldások (a futtatásához szükséges plusz erőforrásokat az adatfeldolgozás rendszere emészti fel);
- A központ gép (szerver) szerepét átvéve el kell látnia a terminál szerver feladatokat is;

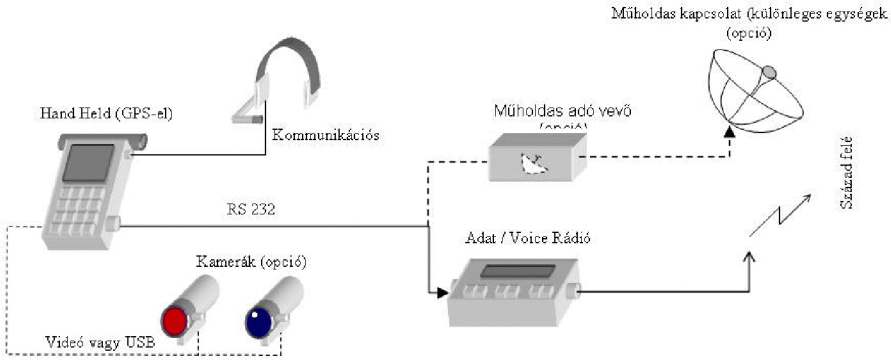
- Az infokommunikáció főleg sugárzott módon valósítható meg (URH és mikrohullámú adatkapcsolat);
- Korlátozott a rácsatlakoztatható egységek száma (8-16 egység, a csatlakozás típusától függően);
- Kis belső mobilitás.



3. számú ábra: BTR-ben telepített vezetési pont (forrás: szerző)



4. számú ábra: század vezetési pont elrendezése (forrás: szerző)



5. számú ábra: szakasz-rendszer (forrás: szerző)

6. Összegzés, következtetések:

Napjaink megváltozott hadviselési és infokommunikációs körülményei közepette a Magyar Honvédség tábori informatikai, valamint komplex informatikai rendszere is átalakításra szorul. Jelen közleményben a rendszer kialakításának megtervezésére és kivitelezésére a Honvédelmi Törvény ajánlásainak a figyelembe vételével tettem javaslatot.

Felhasznált irodalom:

[1] Pölcz Péter: A tábori vezetési és irányítási informatikai rendszer hardwer renszer kialakítása (tanulmány), Videoton, Székesfehérvár, 2008.;
[2] Pándi Erik: Trendek és kihívások – zártcélú hálózatok a globális térben (tanulmány), ZMNE, Egyetemi Könyvtár, Budapest, 2007.;
[3] Pándi, Erik: Unification of the Hungarian governmental communications systems, „Kommunikáció 2005" nemzetközi szakmai tudományos konferencia, ZMNE, Budapest, ISBN 963 7060 11 1, 371-376. oldal, 2005. X. 27.

Zoltan RAJNAI

LES ELEMENTS ET LA PHILOSOPHIE DU RESEAU TACTIQUE

Nous avons une grande ambition à satisfaire l'objectif des Forces Armées Hongroises de disposer de moyens de commandement et de communications opérationnels et conformes avec l'OTAN.

Voyons d'abord les moyens de transmissions qui constituent l'architecture des communications tactiques d'une grande unité opérationnelle:

- au niveau des sections, des compagnies et jusqu'au bataillon les moyens de transmissions sont essentiellement des radios tactiques HF et VHF dont les dernières générations sont capables de transmettre des données IP entre les systèmes C2 des différents niveaux de commandement:

[4] à partir du niveau bataillon les postes de commandement sont connectés au réseau maillé soit par Radio de Combat (RFP) soit par Faisceaux Hertziens

[5] les Postes de Commandement disposent d'une station et de moyens LAN associés pour offrir des services multimédia aux usagers

[6] le système peut bien sûr être connecté au réseau d'infrastructure fixe ainsi qu'aux réseaux de l'OTAN.

Parmi les besoins opérationnels prioritaires, exprimés par les Forces Armées, l'un des plus importants a été certainement de donner aux moyens de Transmissions une véritable capacité de déploiement et de mise en oeuvre rapide des équipements avec le minimum de personnels. - Les systèmes de communications tactiques de la génération précédente, et encore en service dans la grande majorité des armées, sont organisés en noeuds de Transmissions de la taille d'une section. Il faut une trentaine d'hommes et une dizaine de véhicules pour assurer la fonction de Centre de Transmissions. Le volume et le poids de ces moyens, les personnels nécessaires à leur mise en oeuvre, sont peu compatibles avec les impératifs de déploiement rapide.

- L'élément de base autonome a été réduit à un seul véhicule de transmissions et un véhicule cargo pour les antennes et accessoires, servis normalemant par un groupe de 6 personnels: 1 officier - 2 Sous Officiers et 3 opérateurs et conducteurs.

- Sur le plan économique l'architecture réduit fortement le coût d'acquisition et d'exploitation du réseau tactique

- en terme de nombre de véhicules et de stations de transmissions,
- et pour le nombre de personnels qualifiés nécessaires à sa mise en oeuvre.

Voyons les briques du système de télécommunication tactique.

Le réseau est un réseau de zone maillé, dont la finalité est de couvrir très rapidement une zone opérationnelle d'artères de communication sécurisées. Il est d'abord constitué de stations de Transit et d'intégration radio. Ces stations seront

raccordées entre elles par des Faisceaux Hertziens. Le réseau de Transit permet de raccorder les Stations d'Accès:

[7] des Postes de Commandement de Division et de Brigade installés en shelters ou dans des batiments suivant le cas

[8] et des Postes de Commandement de Bataillon installés dans des véhicules de commandement blindés à roue.

Le réseau de Transit permet aussi de raccorder d'une manière totalement automatique les usagers mobiles dotés de postes radio VHF.

Le déploiement sur un site d'une station est grandement facilité par la possibilité d'installer les mâts d'antenne des faisceaux hertziens jusqu'à 600 mètres de la station et raccordés par des cables à fibres optiques. Ainsi en terrain difficile la station peut être camouflée en toute sécurité en bas d'un point haut, alors que les mâts d'antenne seront installés sur la crête militaire autour de ce point haut.

Les liaisons de maillage sont réalisées en Bande 4 OTAN, c'est à dire de 4.4 à 5 GHz, avec un débit de 8 Mb/s. Deux antennes peuvent être installées sur un même mât. Les liaisons de raccordement vers les postes de commandement peuvent être effectuées soit en Bande 4 OTAN avec un débit de 8 Mb/s, soit en bande 5 OTAN avec un débit plus important de 34 Mb/s. La station est opérationnelle avec une première liaison hertzienne en fonctionnement dans les 30 minutes après l'arrivée sur le site.

Sur le même principe qu'une station satellite le PC est constitué d'une partie intérieure et d'une partie extérieure, les deux étant reliés par une fibre optique de 600 mètres.

- l'équipement extérieur comprenant l'antenne et la partie Radio Fréquence (RF) émission et réception intégrée
- en version Bande 4 (bande des 5 GHz) le PC est constitué d'une antenne électronique de type patch. Le faisceau est formé par la combinaison des multiples patchs émetteurs.
- en version Bande 5 (15 GHz), le PC comprend une antenne parabolique classique
- l'équipement intérieur dit « Bande de Base » (BBE) est commun quelque soit la bande utilisée pour la liaison. Il se trouve dans la station technique, un même équipement BBE peut être connecté à trois PC et donc permettre trois liaisons. Cette solution comme nous l'avons vu permet d'éloigner les antennes hertziennes de la station et facilite l'installation et le camouflage sur le site.
- Un combiné d'exploitation permet d'assurer d'une part la fonction de chargement des parametres radio de la liaison et d'autre part la fonction de Voie de service entre les opérateurs.

La mise en oeuvre typique d'une station de nouvelle génération avec un

Faisceau Hertzien en version Bande 4:

- l'antenne électronique sur son mât en fibre de carbone

[9] un touret d'alimentation électrique et de télécommande contenant un UPS (batterie) pour la réalisation immédiate d'une jonction

- le combiné d'exploitation
- l'équipement Bande de Base situé dans la station technique
- un touret de Fibre optique d'une longueur de 600 mètres
- si la distance avec la station est importante on utilise un petit groupe électrogène pour alimenter l'équipement.

Le détail de l'antenne électronique, qui est dotée d'un système d'alignement automatique de pointage vers la station correspondante.

Le FH en Bande 4 permet un débit de 8 Mb/s pour des liaisons d'une portée moyenne radio de 30 à 40 km. Une version en bande 4 offrant un débit de 34 Mb/s est en cours de réalisation pour satisfaire au besoin de plus en plus pressant d'augmentation de débit exprimé par de nombreuses armées.

Typiquement la station en camionnette tactique permet de desservir un poste de commandement d'environ 80 usagers et de raccorder 5 LAN pour les Systèmes d'information Opérationnels et la bureautique.

La station du réseau en Véhicule de l'Avant Blindé permet quant à elle de desservir un poste de commandement tactique jusqu'à 40 usagers et de raccorder aussi 5 LAN.

Les usagers mobiles dotés de postes de radio de combat disposent d'un service automatique et sécurisé de radio-téléphone avec des fonctions phonie et transmissions de données. Les radios mobiles peuvent appeler d'autres mobiles ou des usagers fixes du réseau sans l'intermédiaire d'aucun opérateur. D'autre part à travers le réseau tactique i1s peuvent joindre les usagers des réseaux d'infrastructure ou des réseaux alliés connectés au réseau.

En cours de déplacement les radios mobiles disposent d'une fonction automatique de changement de balise radio camme dans un réseau cellulaire.

Les fonctions d'administration et de commandement sont assurés par le système de gestion du réseau. Ce système NMS est constitué de deux ensembles, d'une part les stations qui assurent l'administration complète du réseau, et d'autre part les terminaux de gestion locale présents à chaque station du réseau. Une station peut assurer à elle seule le management d'un réseau déployé en opération. Mais dans le cas d'un réseau important les fonctions de planification et de commandement du réseau, de gestion de l'annuaire des usagers, de logistique des noeuds de transmissions peuvent être réparties entre plusieurs stations. Les stations sont alors au nombre de deux ou trois pour un réseau de grande unité, elles sont normalement localisées dans les Postes de Commandement importants.

Les stations constituent un système de gestion et d'administration distribué, où chaque station met à jour en temps réel les autres stations du réseau. Les stations NMC et les FC des stations du réseau échangent entre elles des flux d'information:

- des messages opérationnels pour la manoeuvre du réseau, les liaisons à réaliser, les déplacements de stations, les ordres logistiques et les comptes-rendus d'exécution
- et des messages techniques pour le transfert des données de configuration du réseau, et la connaissance en temps réel de l'état des liaisons et des équipements.

En conclusion, le réseau tactique de nouvelle génération comprend un certain nombre de fonctions :

- Des Services Internet Tactique offerts aux usagers
- Une fonction Switching et Routing
- Des équipements Faisceaux Hertziens
- Des équipements de chiffrement des liaisons COMSEC et de sécurité IPSEC
- Des Radios de Combat qui peuvent s'intégrer comme usagers mobiles
- Des outils d'administration et de gestion du réseau.

Károly FEKETE PhD

PROTOCOL BASED CONSIDERATIONS OF WIMAX IN MILITARY COMMUNICATIONS NETWORKS

This Paper was supported by the János Bolyai research Scholarship of the Hungarian Academy of Sciences

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

Abstract

The communications industry is heading towards wireless data transfer with great speed and several competing technologies are emerging to replace the old ones. The traditional Wireless Local Area Network (WLAN) has gained a place in the military environment and is definitely the leader for short distance wireless networks. However, the coverage and mobility are adequate for indoor usage only. The Mobile WiMAX is planned to be independent or to extend the mobile access when a military user exits the WLAN hotspot coverage area.

Introduction

Mobile devices such as cell phones, digital assistants or laptops are increasingly used to transfer data over cellular wireless networks such as GPRS/EDGE, 3G and 4G networks [1]. These commercial wireless networks carry data traffic for a variety of applications such as multi-media messaging (MMS), web browsing, and advanced applications like video-streaming or push-to-talk. Since in the military applications radio resource remains the critical resource, operators need to manage military communications networks in a way that provides both a comfortable QoE (Quality of Experience) for military subscribers and an efficient bandwidth usage. For these purposes there is a QoS differentiation between real time and non-real time application flows and service continuity within modern WLANs. In this context, it is of primary importance for network engineers to have a radio link dimensioning tool that allows predicting the impact of traffic growth within and between classes. Many works study the problem of performance analysis in WiMAX networks either by simulation or analytical modeling. Both have advantages and drawbacks. On the one hand, the accuracy of simulation results is obtained at the expense of long processing time (prohibitive to be involved in a dimensioning optimization process) and the analysis of the performance results for dimensioning the system inputs is often a difficult task. On the other hand, analytical modeling

gives faster results and a better understanding of the intrinsic system behavior, but relies on strong and non-realistic assumptions. Many works propose analytical models assuming a single type of data traffic with classical circuit-based assumptions that are not adapted to wireless data networks.

WiMAX highlights

WiMAX (Worldwide Interoperability for Microwave Access)—or IEE 802.16 or Wireless MAN—provides such broadband wireless access over larger areas than 802.11 (Wireless LAN), and it does so at broadband speeds.

There are four key defining elements that differentiate WiMAX and other wireless technologies:

- WiMAX is a broadband wireless access (BWA) technique, offering fast broadband connections over long distances;
- The technology underlying the standard is often referred to as "Wireless MAN wireless local loop" or "WiMAX";
- A key aspect of WiMAX is the interoperability between products from different vendors;
- WiMAX uses different modulation schemes between the consumer and the base station along different distances.

WiMAX architecture

The IEEE Working Group 16 defined two access options for a WiMAX network: fixed (IEEE 802.16TM- 2004) and portable (IEEE 802.16eTM). In the fixed option, access is provided through a fixed antenna as in a satellite television subscriber station. In portable option, the subscriber stations are very similar to IEEE 802.11 Wi-Fi stations.

WiMAX point-to-point backhaul can be used to interconnect Wi-Fi mesh networks through dual mode Wi-Fi and WiMAX cells [5]. It can also be used to offer access to fixed WiMAX point- to-point backhaul, interconnecting Wi-Fi mesh networks through a dual mode Wi-Fi and WiMAX cells.

Furthermore, it can be used to offer access to fixed Military Subscriber Stations (MSS) through a Point to Multi Point (PMP) topology. Mesh topology can be used to reach users, who cannot otherwise be reached without a new Base Station (BS). Portable SS's will be supported in the near future.

The WiMAX architecture depends on: topology and Wi-Fi interconnection. With the emergence of WiMAX in near future, deployments that combine the two technologies can be constructed to take advantage of the strengths of both Wi-Fi and WiMAX. The WiMAX cells will interoperate seamlessly with existing Wi-Fi cells always selecting the best path for delivering maximum user throughput end-to-end.

The scenario will become increasingly complicated with the introduction of five other factors:

- PHY air interface;
- Duplexing technique (FDD—Frequency Division Duplexing/TDD—Time Division Duplexing);
- Transmission mode (half-duplex/full-duplex);

- Operation (licensed/unlicensed);
- Adaptive burst profiles.

Protocol stack

The IEEE 802.16 protocol reference model has three planes: User, control and management, as is shown in Figure 3. The IEEE standard 802.16TM-2004 deals with user and control planes. It defines two layers in these planes: Medium Access Control layer (MAC) and Physical layer (PHY). The MAC layer has three sub-layers: Service-Specific Convergence Sublayer (CS), Common Part Sub-layer (MAC CPS) and Security Sub-layer. CS provides the required adaptation for the up-layer incoming traffic while MAC CPS makes available key link layer functions for solving several broadband wireless communication issues.

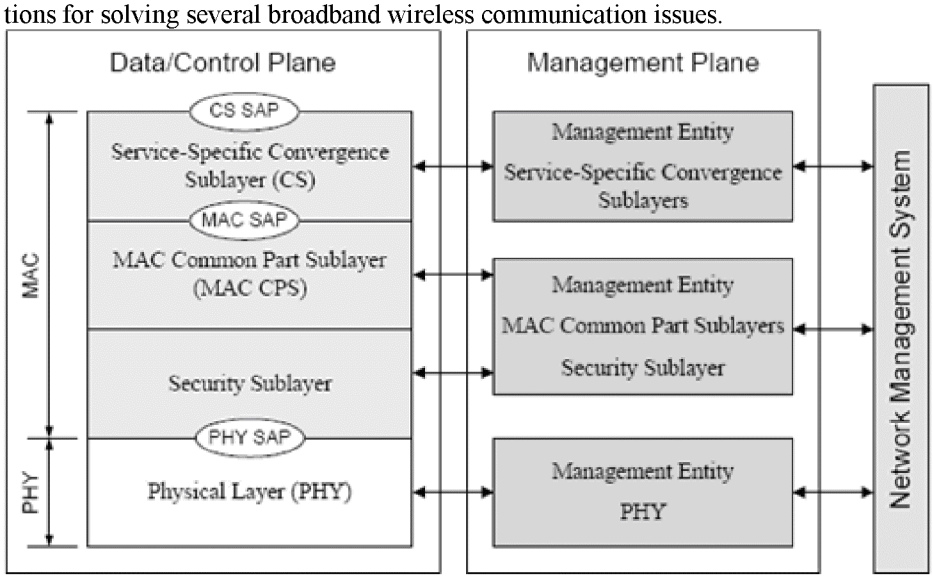


Fig. 3. Protocol stacks as per IEEE 802.16 MAC.

Mobile WiMAX Physical (PHY) Layer

The 802.16-2004 specification and the 802.16e-2005 amendment define five PHY alternatives:

- WirelessMAN-SC (Wireless Metropolitan Area Network using Single Carrier Modulation for use in the 10-66 GHz bandwidth region);
- WirelessMAN-SCa (Wireless Metropolitan Area Network using Single Carrier Modulation for use on bandwidths below 11 GHz);
- WirelessMAN-OFDM (Wireless Metropolitan Area Network using OFDM);
- WirelessMAN-OFDMA (Wireless Metropolitan Area Network using OFDMA);
- WirelessHUMAN (Wireless High-Speed Unlicensed Metropolitan Area Network);

Orthogonal Frequency Division Multiple Access (OFDMA)

OFDMA is a multi-user version of the OFDM digital modulation scheme. Subsets of subcarriers are assigned to individual users to provide simultaneous low data rate transmission from several users.

In practice, the base station (BS) receives packets from the higher layer to be broadcasted to multiple mobile stations (MS), and performs channel coding separately for each packet that will be broadcasted to different mobile stations. After separating channel coding, all packets for the broadcast service sent to mobile station. The base station independently interleaves and modulates the encoded broadcast service packets.

On completion of modulation, the base station segments each broadcast service packets into 'X' transmission units. In doing so, the number of transmission units is segmented to change the subject. After segmentation, the base station performs multiplexing operation. Multiplexing is performed such that segmented broadcast service signal is transmitted sequentially or in predetermined time intervals.

If broadcast services required by different mobile stations are different, increasing the number of transmission units can help meet the increased data amount and broadcast service signal transmission. Since all packets are multiplexed, the individual mobile station requires only a part of that multiplex signal. When a time-multiplexed broadcast signal is transmitted, a mobile station selectively receives only its desired transmission unit frame. After selecting the desired signal, the mobile station combines the entire selected signal to form a required packet.

The OFDMA has several advantages over traditional Code Division Multiple Access (CDMA)-versions used in post-GSM 3G technologies. The spectral efficiency is higher and the fading can be tolerated better. In OFDMA data streams from different users are combined to sub-channels in both Downlink (DL) and Uplink (UL). However, there are some drawbacks as well. Since the manufacturing of OFDMA electronics is rather complex, the expenses rise at the same time. Additionally, the Co-Channel Interference (CCI) from neighboring cells is less disturbing in CDMA than in OFDM. A mobile station (receiving a particular frame) receives physical layer transmission information of the corresponding frame, and determines a CID corresponding to its desired broadcast services. The mobile station can receive the desired broadcast service symbol.

OFDM Basic Principle

With OFDM the used bandwidth is divided into several frequency sub-carriers so that they are orthogonal to each other. The stream of input data is separated into multiple, parallel sub- streams with reduced data rate. Then the sub-streams are modulated individually and sent on separate sub-carriers. Consequence of this is the increase in symbol duration. Since the long signal duration decreases Inter Symbol Interference (ISI) caused by multipath propagation, it is efficient to transmit the low-rate streams in parallel, instead of one high-rate stream. The signal duration is long, so by using a proper guard interval, the ISI can be avoided totally, assuming the guard interval is longer than the difference between the first and last

multipath echo. The Figure 2 below illustrates the principle of several sub-streams combined at the transmitter and separated again at the receiver.

As seen in the Figure 2 the information is coded and modulated across the sub-carriers before performing an Inverse Fast Fourier Transform (IFFT). The IFFT takes advantage of the frequency diversity of the multipath channel. Finally, before transmitting the data, the streams are combined to a single signal and sent to the air interface. At the receiver end the procedure is the same, but in reversed order. The 802.16e specification defines the Fast Fourier Transform (FFT) size to be 128, 512, 1024, or 2048 with respective channel bandwidths 1.25, 5, 10, and 20 MHz. However, the Mobile WiMAX allows other bandwidth profiles to be used as well.

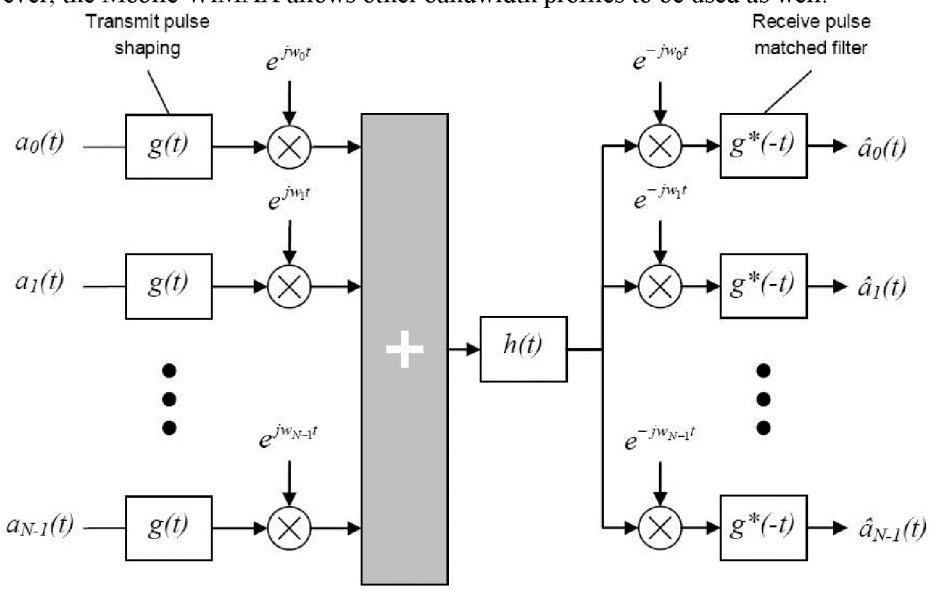


Fig. 2 - Basic Architecture of an OFDM System [4]

The available resources of OFDM can be divided into time and frequency domains. In the time domain OFDM symbols can be used and frequency domain has sub-carriers. Both of these can be utilized for individual users by using sub-channels [4].

OFDMA Symbol Structure and Sub-Channelization

The OFDMA symbol structure is shown in Figure 3. As can be pointed, three types of sub- carriers are used in OFDMA symbols. Data sub-carriers handle the transmission of data, pilot sub-carriers are for the estimation and synchronization use, and null sub-carriers have no transmission, but they are intended for guard bands and Direct Current (DC) carriers.

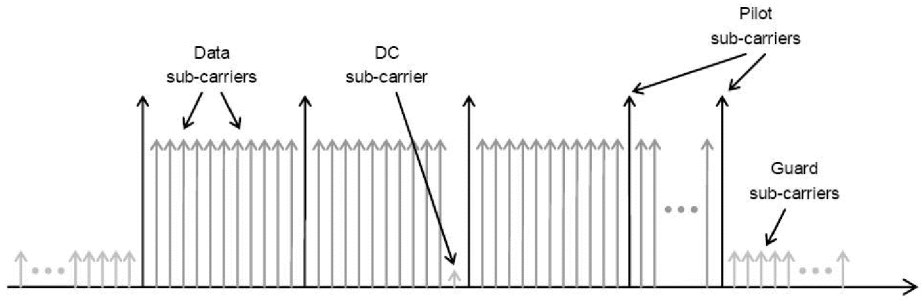


Fig. 3. - OFDMA Sub-carrier Structure [4]

The definitions sub-carrier and sub-channel may be confusing, but they can be clarified in the following way: a subset of data or pilot sub-carriers is a sub-channel and the OFDM symbol consists of several sub-channels [3]. Sub-channelization defines the smallest time-frequency resource unit to be a slot. One slot is the same as 48 data tones, in other words sub-carriers.

Time Division Duplex Frame Structure

The Mobile WiMAX used to support only Time Division Duplex (TDD) but recently full and half-duplex Frequency Division Duplex (FDD) support has been added too. This is mainly because of local restrictions in some areas. A drawback for TDD is that it needs to be synchronized over the whole system, but however, there are several reasons for preferring the use of TDD. The ratio of DL/UL data rates can be adjusted freely while with the FDD the ratio is always constant, and in most cases symmetric. Figure 4. demonstrates the structure of an OFDMA TDD frame. There are additional and optional fields as well that can be used in the sub-frames.

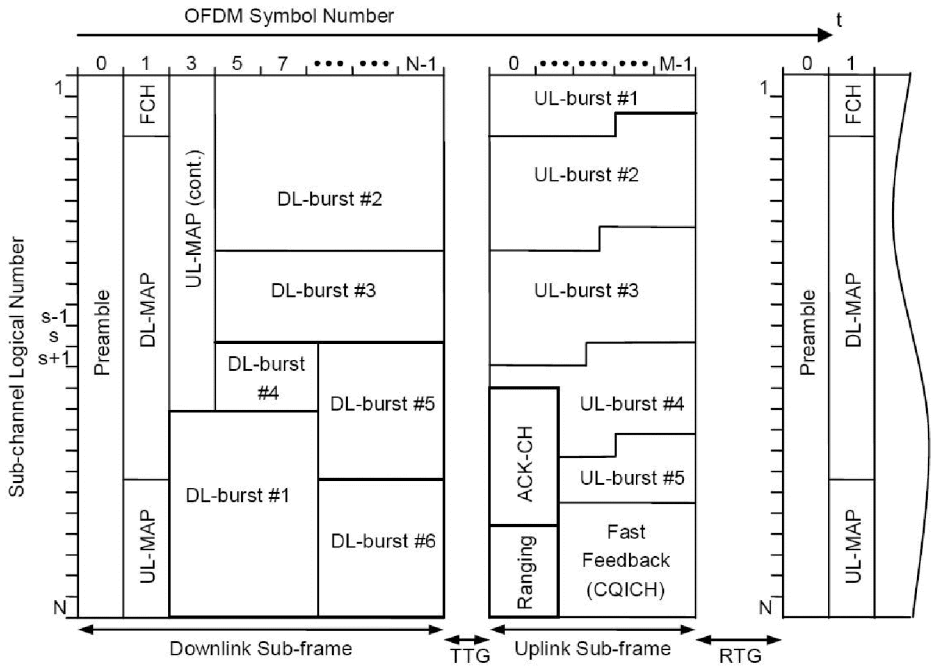


Fig. 4. - OFDMA Frame Structure in TDD [5]

The development of Mobile WiMAX was considered to fulfill requirements for all major traffic types. This means that it will have to support voice, data and video, even simultaneously. The normal voice calls are very sensitive to latency and on the other hand video-streams demand capacity for transmission. Data traffic requires also a high-speed connection, but the bandwidth usage comes in bursts. The allocated resource can vary from a single time slot to the entire frame. Variations can be made frame-by-frame. The WiMAX introduces two sharing mechanisms for the air interface. The Point-to- Multipoint (PMP) networking and Mesh networking.

The Mesh network has a station, with a direct connection to the backhaul services outside the Mesh network, named as Mesh BS while all other stations are called Mesh SSs. Nodes with direct links (one hop distance) to each other are called neighbors and neighbors of a node create a neighborhood. The extended neighborhood includes the neighbors of neighborhood (two-hop distance).

Quality of Service (QoS) Support

Mobile WiMAX is suited for supplying various QoS methods for different types of data services and applications. This is achieved with the sufficient data rates, adjustable capacities in both DL and UL, the fine resource granularity, and flexible mechanism for resource allocation. To provide QoS in Mobile WiMAX, so called service flows are designed. These flows are unidirectional packets with certain QoS parameters and Figure 5 is demonstrating the principle. When some type of data service (voice, data, etc.) is wanted to be offered, a connection has to be

created between the BS and the MS. The packets at the MAC interface are attached with information of a service flow to be delivered over the connection. Since the QoS is connection-oriented, it can be effectively controlled during the transmission. Additionally, this enables an end-to-end QoS even over the air interface, which usually is the main problem in wireless communications.

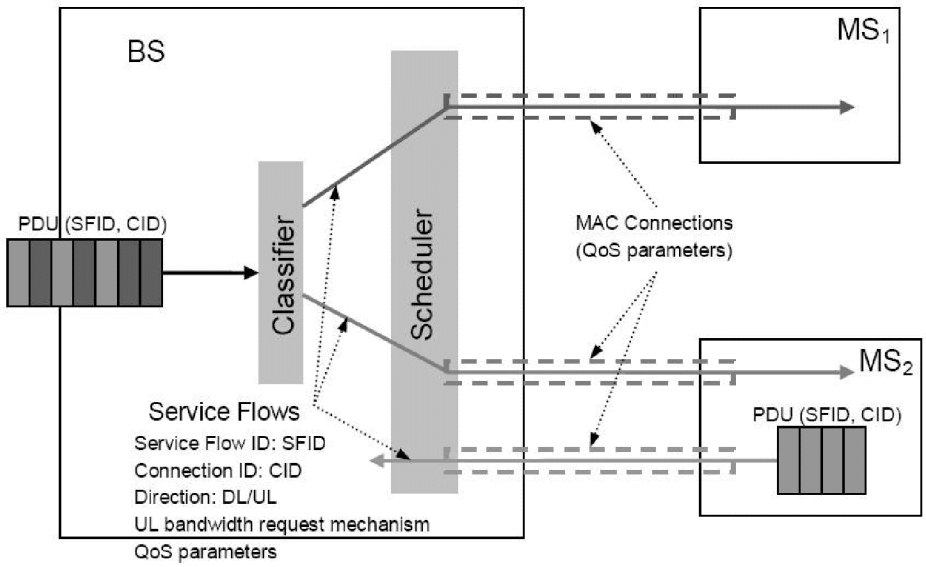


Fig. 5 - Mobile WiMAX QoS Support [4]

End-to-End WiMAX Architecture

The IEEE only defined the Physical (PHY) and Media Access Control (MAC) layers in 802.16. This approach has worked well for technologies such as Ethernet and WiFi, which rely on other bodies such as the IETF (Internet Engineering Task Force) to set the standards for higher layer protocols such as TCP/IP, SIP, VoIP and IPSec.

The Mobile WiMAX End-to-End Network Architecture is based on an All-IP platform, all packet technology with no legacy circuit telephony (Figure 6.). It offers the advantage of reduced total cost of ownership during the lifecycle of a WiMAX network deployment. The use of All-IP means that a common network core can be used, without the need to maintain both packet and circuit core networks, with all the overhead that goes with it. A further benefit of All-IP is that it places the network on the performance growth curve of general purpose processors and computing devices, often termed "Moore's Law". The end result is a network that continually performs at ever higher capital and operational efficiency. This results in lower cost, high scalability, and rapid deployment. In order to deploy successful and operational commercial systems, there is need for support beyond 802.16 (PHY/MAC) air interface specifications.

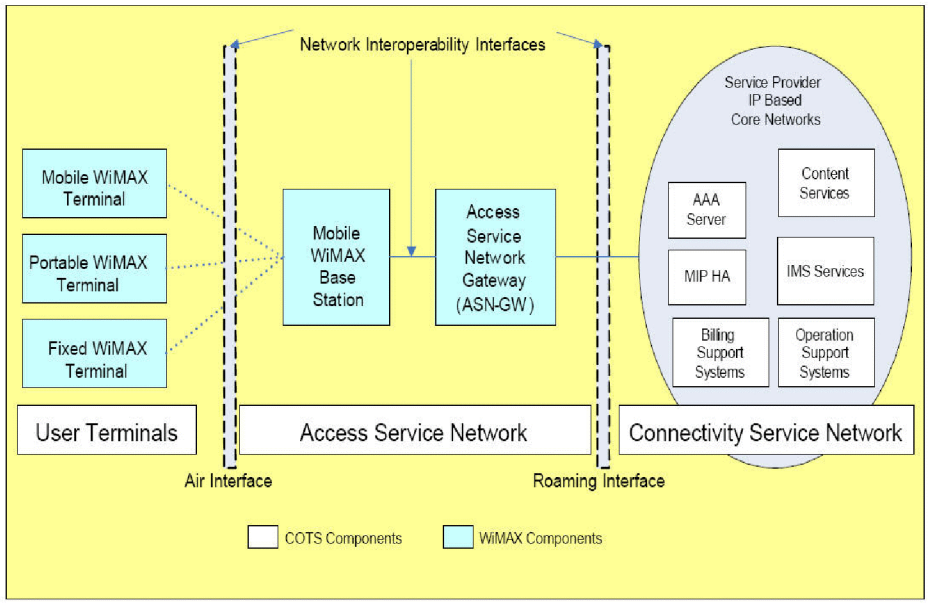


Fig. 6. WiMAX Network IP-Based Architecture

Conclusion

In the military applications there is soaring demand for wireless broadband access, and wide range of applications which are today require mobile data access as fixed and mobile voice services, and content streaming on strategic, operational and tactical level (Figure 7.) [2]. WiMAX is committed to meeting the requirements of all these applications.

The main advances of WiMAX in the military network are:

- Cost effective COTS based hardware and software sets;
- Excellent level of interoperability and technical compatibility with different military networks;
- All IP based network able to integrate all kind of TCP/IP, SIP, VoIP and IPSec applications;
- Good QoS support of different kind of information such as data streaming, video, voice and database access;
- The WiMAX network has high scalability, and rapid deployment;
- The WiMAX network is future proof due to the continuously increasing of the computing power of its components.

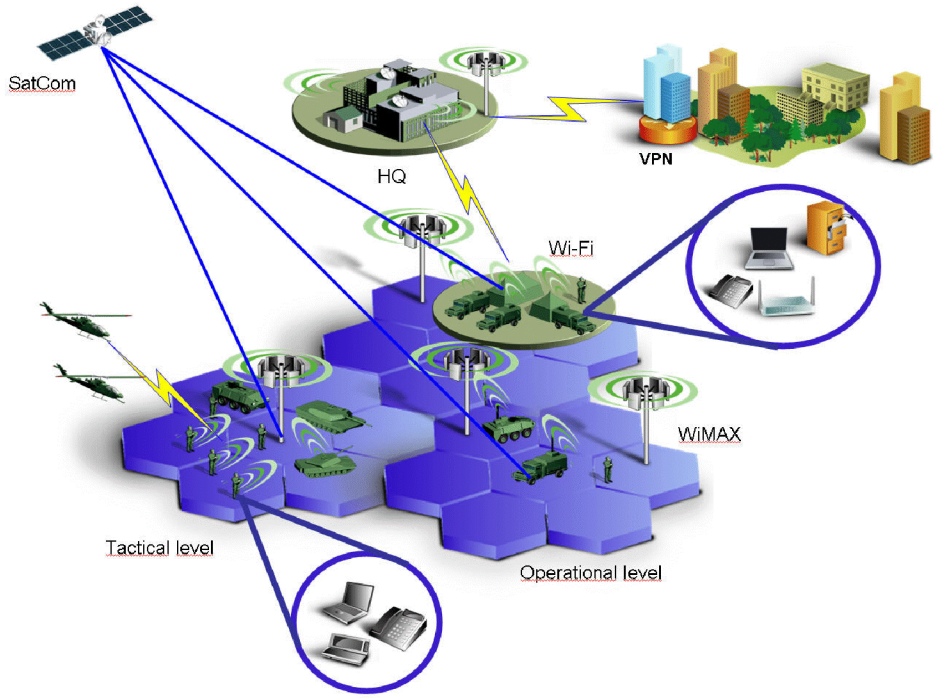


Fig. 7. WiMAX in Military Communications Network

References

[1] Károly FEKETE: The benefits of high performance WIMAX solutions in multinational missions, Kommunikáció 2005 (Communications 2005) tudományos kiadvány, Budapest, 2005, ISBN 963 7060 11 1

[2] Károly FEKETE: New possibilities in the field of WAN-WLAN military communications, Kommunikáció 2004 (Communications 2004) tudományos kiadvány, Budapest, 2004, ISBN 963 86441 5 X

[3] Dr. DÁRDAI Árpád: Az OFDM eljárások a védelmi célú mobil távközlésben, Kommunikáció 2005 (Communications 2005) tudományos kiadvány, Budapest, 2005, ISBN 963 7060 11 1

[4] WiMAX Forum: Mobile WiMAX – Part I: A Technical Overview and Performance Evaluation, http://www.wimaxforum.org/news/downloads/Mobile_WiMAX_Part1_Overview_and_Performance.pdf (August, 2006)

[5] Szöllősi Sándor: Konvergáló hálózatok fejlődési trendjei, a technikai alkalmazhatóság kérdései a Magyar Honvédség infokommunikációs rendszerében, Doktori (PhD) értekezés, Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, 2007.

DORKÓ Zsolt – PÁNDI Erik:[46]

AZ IT ÁGAZAT SZERVEZETI ÉS IGAZGATÁSI FEJLESZTÉSÉNEK EGYES KÉRDÉSEI

Absztrakt: A Rendőrség IT szolgálata jelenlegi formájában folyó hó január 1-jén alakult meg. A szerzők jelen közleményükben – támaszkodva korábbi szakmai tapasztalataikra – javaslatokat fogalmaznak meg az ágazat egyes szervezési és humánfejlesztési területeit illetően.

Kulcsszavak: humán erőforrások, IT szolgálat, Rendőrség.

1. Bevezetés

A Rendőrség integrált IT ágazatának – az alaptevékenységek eredményes támogatása érdekében – a jövőben oly formában lenne célszerű működtetni, hogy az egyrészt a gyakorlatban megoldja az információ gyűjtését, tárolását, visszakeresését, terjesztését és biztonságos továbbítását, másrészt tervező, előkészítő, szervező, rendelkező és adminisztrációs tevékenységgel hatékonyan segítse mindezen funkciók megvalósítását szolgáló optimális módszerek, eszközök és rendszerek kialakítását, kifejlesztését. Látszik, hogy az elmélet komplex probléma elé állítja az ágazat vezetését, hiszen ezen feladatoknak (elvárásoknak) való magas szintű megfelelés elérésének és fenntartásának gyakorlati kivitelezése igen bonyolult és egyúttal jól átgondolt megoldásokat igényel. Nem tudjuk elég sokszor hangoztatni azon elvet, amely szerint [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." [1]. Úgy ítéljük meg, hogy az integrált Rendőrség kialakítása rendkívül jó lehetőség arra, hogy a korábbi erősségekből és gyengeségekből, valamint az elméleti megalapozásból kiindulva, illetőleg más pozitív gyakorlati tapasztalatra építve jelen fejezetben – kizárólag vitaindítás gyanánt – néhány lehetséges, esetlegesen célszerűnek mutatkozó fejlesztési irányra felhívjuk a figyelmet. Mindezt tesszük annak érdekében, hogy elősegítsük az IT ágazatra nehezedő és egyre fokozódó belső és külső elvárásoknak – az objektív korlátok által behatárolt mozgástér keretein belül – történő minél magasabb szintű megfelelést.

2. A szabályozottság kérdéskörei

Az ágazat által végzett tevékenységeket többé már nem lehet lokális jelzővel és lokális módon kezelni. A Rendőrség életében napjainkra globális szinten vált meg-

[46] Szerzők: Dorkó Zsolt r. alezredes, Védelmi Vezetéstechnikai Rendszerszervező MSc. szak másodéves hallgató, ZMNE BJKMK Híradó Tanszék; Dr. Pándi Erik egyetemi docens, ZMNE BJKMK Híradó Tanszék

határozóvá47 az IT, amely szerepkört maga a kormányzat is folyamatosan erősít mind az egyén, mind a szervezetek szintjén. A lokálisból a globális minőség felé való egyértelmű haladás miatt megítélésünk szerint hosszútávon már nehezen tartható fenn az a gyakorlat, amely mind az üzemviteli,48 mind az irányítói (szakirányító)49 tevékenység során előnyt, illetve igen tág teret biztosít a tapasztalati úton való és egyéni megítélés szerint történő végrehajtásnak. Természetesen megkövetelhető a személyi állománytól, hogy szakmája tekintetében ismerje a vonatkozó előírásokat,50 azonban az ágazatban a konzekvens szabályozás, mind állami, mind szervezeti szinten hiányosnak tekinthető. A hiányosság mellett elmondható, a meglevő előírások sok esetben az érintett, vagy érintetté váló személyi állomány számára nem elérhetők.51 Miután az IT-nek az alaptevékenység szempontjából egyrészről támogató, illetőleg kiszolgáló funkciói is vannak, ezért a területet interdiszciplinárisnak is tekinthetjük, ami ugyancsak problémaforrásokat generál [2]. Sok esetben52 az alaptevékenységet szabályozó normatív háttér olyan széleskörű, hogy egyszerűen nem várható el a személyi állomány egyes tagjától a mélyebb összefüggések önálló felismerése, illetőleg a levont konzekvenciák alapján az elvek gyakorlatba való beépítése, holott több esetben ezen ismeretek hiánya szakmai tevékenységének minőségét, illetőleg megítélését jelentősen befolyásolja. E témakörökben további konfliktusokat lehet előidézni azzal, ha egy problémára – az egymás információitól való elszigeteltség miatt – több, esetlegesen rossz megoldás születik és épül be a gyakorlatba. Természetesen nem azt kívánjuk ezzel sugallni, hogy nincs helye egyéni, önálló kezdeményezésnek és kreatív tevékenységnek, hanem inkább arra kívánunk rámutatni, hogy a helyes megoldások intézményesítése, bevált gyakorlattá alakítása jelentheti az IT ágazat és ezzel a szervezet elsőszámú érdekét. Mindezek alapján javasoljuk egy olyan keretszabályozás, avagy kódex kidolgozását, amely moduláris felépítése révén, a változó igényeknek megfelelően rugalmasan változtatható, azaz szűkíthető, bővíthető, átdolgozható. E kódex általános célja tehát egy olyan átfogó, komplex ismeretanyag és ehhez köthető részszabályozások összefoglalása és közreadása, amelynek kiadmányozásával többek között:

- megteremthető az IT ágazat identitástudata;
- megismerhetők az ágazat aktuális stratégiai céljai;
- iránymutatás adható a követendő szakmai alapelvekről;
- rögzíthetők az ágazat szervezeti és működési alapelvei;

[47] példának okáért gondolhatunk itt a „Robotzsaru”-ra, vagy a határregisztrációs rendszerekre

[48] információ gyűjtése, tárolása, visszakeresése, terjesztése, biztonságos továbbítása

[49] tervező, előkészítő, szervező, rendelkező, adminisztratív

[50] szabványok, jogi normák és jogszabályok

[51] példának okáért egyes szabványokhoz való hozzáférés néhány esetben csak anyagi ellentételezés mellett lehetséges, vagy megemlíthető, hogy egy területi szerv kiadmányozásra jogosult vezetője által kiadott normatív szabályozás más illetékességi területen működő területi vagy helyi szerv, de akár a központi szerv számára nem válik automatikusan ismertté. Ilyenek lehetnek: ügyrendek, szervezeti és működési szabályzatok, intézkedések, utasítások

[52] például: adatvédelem, információbiztonság, stb.

- meghatározhatók az ágazati párbeszéd formái, keretei;
- lefektethetők az egyénre és szervezetre vonatkozó minőségbiztosítási alapelvek;
- kialakíthatók az egyén szakmai és beosztásban történő előmenetelének alapelvei;
- áttekinthetők az érdekvédelem alapkérdései;
- egybefoghatók a vonatkozó szabályozások, alkalmazásuk alapelveinek magyarázatai.

Kétségtelen ugyanakkor, hogy a kódex összeállítása egyrészről hosszabb időt igényel, másrészről az ágazat részéről széles támogatottságot. A fentiekben felvázolt témakörök részletes kifejtése jelen publikáció kereteit sajnálatosan mindenképpen meghaladja, ezért – a kódexhez szervesen kapcsolódva – néhány, általunk relevánsnak tartott kérdéskörre kívánunk a továbbiakban kitérni.

3. Részterületek

Kiragadva az ismertetett részterületek közül a szakmai alapelvek, valamint a szervezeti és működési alapelvek kérdéskörét az alábbiakban szeretnénk néhány problémára rávilágítani, illetőleg azok megoldására egyfajta javaslatokat adni.

3.1. Szakmai alapelvek köre

A Rendőrség alapfeladata igen sokrétűvé vált, így a polgári jellegű közigazgatási feladatoktól kezdődően a félkatonai jellegű csapaterős feladatokig bezárólag a rendészeti tevékenységi körök széles palettájával és ezek megoldására létrehozott szervekkel találkozhatunk az integrált szervezetben. Mint azt már korábban megállapítottuk, a központi szervektől a helyi szervekig mindenhol megtalálható az IT szakállománya, vagy szakszerve. A szakmai alapelvek felvázolása során, megítélésünk szerint szükséges lenne pontosan felmérni és kategorizálni az egyes rendőri szerveknél megjelenő IT feladatokat, meghatározni az ellátáshoz szükséges szakállomány kvantitatív és kvalitatív mutatóit. A kvalitatív mutatók esetében egzakt módon meg kell határozni a szakmai felkészültség elégséges színvonalát, vagyis azt, hogy az állomány milyen konkrét végzettséggel rendelkezzen. Ennek kidolgozását elsősorban azért ítéljük fontosnak, mert – szintén hivatkozva a korábbiakra – az ágazat tekintetében nem beszélhetünk egységes alapelveket magába foglaló felkészítési rendszerről.53 A mennyiségi és minőségi felmérést követően vizsgálni kell a rendőri szerv alaptevékenységének jellegét, hiszen csak ennek ismeretében lehetséges meghatározni az alkalmazandó állományviszonyt. Nézőpontunk szerint nagyon durva megközelítés azon elvnek az alkalmazása, amely szerint a funkcionális tevékenységet ellátók nem lehetnek a Rendőrség hivatásos állományú tagjai.54

Ezen információk birtokában az IT ágazatra jellemző beosztások már kategorizálhatókká válnak. Célszerű csoportosításnak tűnik a közép- és felsőfokú végzettségű, valamint a főiskolai és egyetemi végzettségű halmazok kialakítása, amelye-

[53] sem középfokú, sem felsőfokú, sem főiskolai, illetve egyetemi szintű

[54] a legeklatánsabb példája ennek a Készenléti Rendőrség, ahol a szakállomány a rendőri műveletek során az irányító törzzsel együtt, azt kiszolgálva tevékenykedik

ken belül műszaki-üzemviteli és adminisztratív-irányítói részhalmazokat érdemes alakítani. Az egy nyelven való beszélgetés képességének kialakítása érdekében a négy alapkategória számára kompetenciaszinteket kell kidolgozni, amelyeket értelemszerűen a fejlődéssel párhuzamosan alakítani, módosítani kell. Természetesen a kategóriák száma bővíthető, ugyanakkor látni kell, hogy kezdetben a megfelelő kompetenciák tartalmának kidolgozása is igen időigényes tevékenység. A kompetenciaszintek és kompetenciák meghatározását követően átgondolhatóvá válnak a teljesítésükre irányuló megoldások is. A szakmai kompetenciák kidolgozására megítélésünk szerint az IT ágazat tagjaiból álló testület hivatott, amelynek munkáját külső szakértők55 is segíthetik. Az irányvonalak56 kialakítását és az aktualizálási feladatok végrehajtását is e grémium látná el. A kompetenciákat kezdetben úgy célszerű meghatározni, illetőleg felvázolni, hogy azok teljesítése elméleti felkészülést igényeljen [3]. A következő, a kompetenciák teljesítésére szolgáló szükségszerű lépés a differenciált ismeretanyag összeállítása és annak eldöntése, hogy milyen módon, módszerrel sajátítható el, illetve ellenőrizhető vissza a teljesülés a leghatékonyabban. Alkalmazható a klasszikus módszer, vagyis az ismeretanyag mennyiségének és bonyolultsági fokának függvényében, elsősorban kislétszámú, csoportos foglalkozás keretében megismertetni a tananyagot, majd meghatározott időtartamú egyéni felkészülést követően írásbeli és/vagy szóbeli visszaellenőrzést végrehajtani. Modernebb megoldásnak tekinthető a multifunkcionális, multimédia elemeket tartalmazó mobil elérésű távoktatási tananyag egyéni elsajátíttatása, majd visszaellenőrzése [4]. Ez esetben az ellenőrzés szintén történhet korszerűen, vagyis az elektronikus rendszeren keresztül, de ez esetben a vizsgáztatóknak le kell mondaniuk az orális számonkérés lehetőségéről. A távoktatás alkalmazása költségkímélőbb megoldás, de ugyanakkor a személyes kontaktus hiánya miatt az állomány ágazat kívánalmainak megfelelő „szocializációja", mint egyik elérendő fő célt nem szolgálja kellőképpen. Az ismeretanyag kidolgozásában, az oktatási módszer eldöntésében, illetőleg a végrehajtásban természetesen igénybe vehető az Igazságügyi és Rendészeti Minisztérium felügyelete alatt működő oktatási intézményrendszer, mint szakmai bázis.

Külön kérdéskörként kell kezelni az iskolarendszerű szakképzést, valamint a főiskolai és egyetemi képzést. Megítélésünk szerint minden esetben meg kell ismertetni az IT ágazat által preferált intézményeket és programokat az e képzési formába belépni57 kívánó állománykategóriával annak érdekében, hogy a szakmai egyenszilárdság hosszútávon is biztosítható legyen. Az ajánlások összeállításánál tekintettel kell lenni a lokális, valamint a támogatási lehetőségekre egyaránt.

Mindezen feladatok hatékony koordinálása és irányítása érdekében, az IT ágazat központi szervének kezelésében, a személyiségi jogokkal összhangban levő

[55] külső szakértők lehetnek a katonai- és rendvédelmi felsőoktatásban, a rendészeti szakközépiskolákban, illetőleg közigazgatási, tudományos, társadalmi, vagy vállalatok elismert szakértői, munkatársai

[56] fontos annak eldöntése és rögzítése, hogy az egyéni kompetenciák felülvizsgálata milyen időközönként történjen, hiszen az egyes beosztási kategóriák esetében az ismeretanyag megújítására és aktualizálására eltérő időben van szükség éppen jellegük miatt

[57] ebben az esetben többnyire a saját elhatározás alapján, államilag elismert, magasabb szakmai végzettség megszerzésére irányuló tevékenységről van szó

személyügyi adatbázist kell felállítani. Ugyanakkor konszenzus révén dolgozandók ki az IT ágazatban bevezetendő kompetenciarendszerrel kapcsolatosan alkalmazható ösztönző, illetve szankcionáló elvek. Egy megoldásként alkalmazható lehet olyan szabályozás bevezetése, amely lehetővé teszi, hogy a szakállomány minősítésére jogosult illetékes vezető számára legyen kötelező figyelembe venni a kompetencia teljesítését, avagy sikertelen megfelelést igazoló IT testületi határozatot. A szakmai alapelvek körénél szükségszerűnek tartjuk megemlíteni, hogy az IT ágazatban megindult a hivatásos állománykategória visszaszorítására, illetőleg megszüntetésére irányuló törekvések, amelyek egyúttal azt is jelentik, hogy az ágazat – az érintett állomány megszűnése révén – véglegesen kiszorulhat mind a rendészeti szakvizsga, mind a rendészeti vezető- és mestervezető-képzés rendszeréből, amely jelenleg az egyetlen intézményesített, továbbképzésre irányuló szisztéma. Ennek okán mindenképpen megfontolandónak tartjuk a kompetenciaalapú rendszer ágazati működési rendbe történő beillesztését és elterjesztését.

Az ismertetett elképzelés megvalósításához, azaz a részterület kialakításához belső szabályozás, vélhetően miniszteri, vagy ORFK vezetői utasítás kiadmányozására van szükség. Ezen norma természetesen részét képezné az IT ágazat szakmai kódexének.

3.2. Szervezeti és működési alapelvek köre

Az ágazat sajátja, hogy a mindhárom szinten, egyes, illetve szervezetben működő szakállomány állományilletékes vezetője nem IT szakmai vezető, vagyis közvetlen szakmai vezetés megvalósulásáról lényegében nem beszélhetünk. Ez a gyakorlat más rendvédelmi szervnél is hasonló, tehát a szakmai munka minőségét elvi síkon nem befolyásolja. Mint azt a korábbiakban, a szakmai irányítás (szakirányítás) kapcsán azonban már rögzítettük, úgy tűnik, hogy normatív szabályozás híján e terület a Rendőrség esetében lényegében „szokásjog" alapján működik, minden félreérthetetlen előnyével és hátrányával. A szakmai irányítás témakörének újragondolása, illetve rendezése egyúttal elősegítheti az előző alfejezetben felvázolt modell megvalósítását és működtetését. Nézőpontunk szerint a szakmai elvek mind szélesebb körű érvényre juttatása érdekében lehetőséget kell biztosítani az IT ágazat vezetése számára, hogy az egyes rendőri szervek esetében véleményezési és egyetértési jogot szerezhessen az alábbi területeken:

- az IT szakfeladatok beazonosítása;
- az IT szakfeladatokkal kapcsolatos szabályozás;
- a szükséges szakállomány létszámának meghatározása;
- a szakállomány képzettségi követelményének meghatározása;
- az egyes szakközeg kinevezése, elbocsátása;
- az állományviszony beazonosítása;
- az IT szakterülethez kötődő, de nem az ágazat által szervezett szakmai közép- és felsőfokú szakképzés, főiskolai és egyetemi képzés;
- az egyes szakközeg teljesítményértékelése, minősítése.

Fenti feladatok helyi és egyes területi szerveknél történő végrehajtása az IT ágazat központi, illetve területi (regionális) szintjén működő irányító szervek között természetesen megoszthatók, azonban az előző alfejezetben említettek okán célszerű, hogy a végrehajtással kapcsolatosan keletkező adatok és információk

tárolása a központi szinten létesített adatbázisokban történjen. Az IT ágazat személyi állománya kapcsán fentiek szerint kialakítható szorosabb kötődés, illetve felügyelet (irányítás) mellett megítélésünk szerint célszerű javítani a technikai működés egységét és egységességét biztosító témakörökkel összefüggő működési gyakorlatot. Erre elsősorban a rendszerszemléletű gondolkodás erősítése okán van szükség, hiszen e tevékenység „…nem csak (nem is elsősorban) a meglevő rendszerek részekre (végső soron elemekre) bontásához, az elemek rendszerezéséhez, a rendszer belső és külső kapcsolatainak feltárásához, a sokféle vizsgálati szempont (tudományközi együttműködés) lehetőségeinek és szükségességének felismeréséhez szükséges, hanem ahhoz, hogy meglevő elemekből az új igényeknek megfelelő és a környezettel összhangban levő rendszereket tudjunk összeállítani. […] A meglevő rendszerek működtetése – valamilyen meghatározott szempont szerint – optimális üzemviszonyok között szükségessé teszi egyes részek megújítását, esetleges cseréjét. […] A társadalom fejlődése miatt nemcsak a rendszer működésével szembeni követelményértékek, hanem még a – már többször említett – biztonsági tartomány is változik. A „változatlan" technikai rendszer általában – a környezet szakadatlan változása miatt – elavul, használhatatlanná válik, tehát: relative visszafejlődik. […] A rendszerelemzés következtetései – mindezek miatt – nem egyszeriek, örökérvényűek, hanem olyanok, amelyeket időszakonként felülvizsgálni, a környezeti feltételek változása és a rendszer egyes részeinek (erkölcsi és anyagi) kopása miatt módosítani kell." [5]. Ez összességében azt jelenti, hogy még a meglevő rendszerek működtetése is szükségessé teszi az állandó megújítást, a részek cseréjét, a használati mód fejlesztését, illetve új rendszerek létrehozását, amely országos rendszerek esetében mindenképpen szabályozott üzemviteli tevékenységet feltételez. Javasoljuk tehát olyan, az előzőekben ismertetett műszaki jellegű tevékenységekhez köthető szabályozási keretrendszer kidolgozásának megindítását, amely révén az ország bármely rendőri szervezete részére egyértelmű viszonyokat teremthet a működtetés és fejlesztés terén.

Az ismertetett elképzelések megvalósításához, azaz az újabb részterület kialakításához belső szabályozás, vélhetően szintén miniszteri, vagy ORFK vezetői utasítások kiadmányozására van szükség. A kidolgozásra kerülő normák – hasonlatosan az előzőekhez – részét képeznék az IT ágazat szakmai kódexének.

4. Összegzés, következtetések

Jelen közleményben – áttekintettük a lehetséges fejlesztési irányokat. Ennek keretében úgy ítéltük meg, hogy az integrált Rendőrség folyó év elején történt kialakítása egyes szakterületek működési gyakorlatának módosítására rendkívül jó lehetőséget nyújt. Az IT ágazat identitástudatának kialakítása, az aktuális ágazati stratégiák, a szakmai, a szervezeti és működési, a minőségbiztosítási, valamint előmeneteli alapelvek, illetőleg a vonatkozó szabályozások összefoglalása és közreadása érdekében olyan keretszabályozás, avagy kódex kidolgozására tettünk javaslatot, amely elősegítheti az egy nyelven történő beszélgetés, beszéd érdemi megvalósítását. Miután jelen tanulmány keretei erősen behatároltak, ezért csak néhány részterület kapcsán tettünk – véleményünk szerint – alkotó jellegű megállapításokat. Az egységes szemléletmód meghonosítása érdekében kidolgoztuk a beosztások kategorizálásának elvét és főbb jellemzőit, amelyek mentén a beosztá-

sokhoz szükséges kompetenciaszintek és kompetenciák megfogalmazhatók. A kompetenciák által meghatározottak teljesítésének elősegítése érdekében áttekintettük a felkészítés lehetséges megoldásait, azok előnyeit és hátrányait. Összességében úgy ítéltük meg, hogy a kompetenciaalapú rendszer ágazati működési rendbe történő beillesztését és elterjesztését mindenképpen megfontolás tárgyává kell tenni. A szervezeti és működési alapelvek körével összefüggő vizsgálódásaink során tett megállapításunk szerint, a szakmai elvek mind szélesebb körű érvényre juttatása érdekében lehetőséget kell biztosítani az IT ágazat vezetése számára, hogy az egyes rendőri szervek esetében véleményezési és egyetértési jogot szerezhessen meghatározott területeken. Ennek keretében nyolc részterületre tettünk javaslatot. Utolsóként, a rendszerszemléletű gondolkodás erősítése okán, a műszaki jellegű tevékenységekhez köthető szabályozási keretrendszer kidolgozását láttuk megvalósítandónak, amely révén az ország bármely rendőri szervezete részére egyértelmű viszonyok teremthetők a működés és fejlesztés területén.

Az elképzelések megvalósítását miniszteri, vagy ORFK vezetői utasítások kiadmányozása révén tartottuk biztosítottnak.

Hivatkozások

[1] Sebestyén Attila: Csökkenthető-e a „Superuser"-el kapcsolatos biztonsági kockázat?, „Kommunikáció 2007." nemzetközi szakmai tudományos konferencia, 220. oldal, Zrínyi Miklós Nemzetvédelmi Egyetem, ISBN 978 963 7060 31 1, Budapest, 2007. október 16.;

[2] Kassai Károly: Az elektronikus adatkezeléssel kapcsolatos kockázatok kezelésének egyes kérdései, „Kommunikáció 2007." nemzetközi szakmai tudományos konferencia, 78-79. oldal, Zrínyi Miklós Nemzetvédelmi Egyetem, ISBN 978 963 7060 31 1, Budapest, 2007. október 16.;

[3] Rajnai Zoltán – Kerti András: Az információvédelmi szakállomány továbbképzési rendszere, „Kommunikáció 2007." nemzetközi szakmai tudományos konferencia, 86-89. oldal, Zrínyi Miklós Nemzetvédelmi Egyetem, ISBN 978 963 7060 31 1, Budapest, 2007. október 16.;

[4] Busznyák János: Multifunkcionális, multimédia elemeket tartalmazó mobil elérésű távoktatási anyag összeállítása és tesztelése, X. Multimédia az Oktatásban Konferencia, 35-42. oldal, Szegedi Tudományegyetem, ISBN 963 7179 88 7, Szeged, 2004.;

[5] Szücs Ervin: Rendszer és modell I., Egységes Jegyzet (ELTE TTK), Kézirat, Tankönyvkiadó, Budapest, 99-100. oldal, 1987.;

Dr. NÉMETH András

MRR RÁDIÓK ADATHÁLÓZATI KÉPESSÉGEINEK KIAKNÁZÁSA

Bevezetés

A Magyar Honvédség (MH) haditechnikai fejlesztésének keretében beszerzésre került Kongsberg MRR58 URH rádiócsalád tagjai jelentős előrelépést jelentenek technikailag, technológiailag és szolgáltatások tekintetében egyaránt a hagyományos analóg (R-107, R-111, R-123, R-159, R-173 stb.) eszközökhöz képest. A rendszeresítéssel egyidejűleg kiemelt feladattá vált a rádiók csapatvezetés rendszerébe történő integrációja, a hatékony alkalmazás körülményeinek megteremtése, a szükséges járműkomplexumok kialakítása (PK-1, PK-2, PK-3, PK-4, ERIP). A biztosított szolgáltatások, valamint az ezekre épülő alkalmazások széles köre merőben új szemléletet követel a híradó szakemberektől, parancsnokoktól és kezelőktől egyaránt annak érdekében, hogy a rádiók képességeit a lehető legnagyobb mértékben, hatékonyan tudjuk kihasználni. Ennek keretében a jelenlegi csonka képzési rendszer kiegészítése mellett, ki kell dolgozni azokat a megoldásokat, amelyek lehetővé teszik, hogy a harcvezetési rendszer egyes elemeit illeszteni tudjuk a rádióhullámok által biztosított vezetéknélküli információs csatornákhoz. Cikkemben igyekszem összefoglalni a rádiót, mint adatátviteli eszközt jellemző alapvető tulajdonságokat, paramétereket és szolgáltatásokat, felhívván a figyelmet néhány jelenleg is folyó fejlesztésre.

MRR rádiók általános jellemzői

Az MRR rádiók olyan digitális, többfunkciós, az URH tartományban üzemelő (30.000 – 87.975MHz) vezetéknélküli kommunikációs eszközök, melyek a klasszikus értelemben vett beszédátvitel mellet számos kiegészítő szolgáltatást, és adatátviteli megoldást kínálnak a felhasználók számára. Digitális adásmódokban biztosított a rejtjelezett információtovábbítás lehetősége. A család három tagja az MV300 járműfedélzeti, az MP-300 hordozható, valamint az MH300 kézirádió, amelyek CNR59 üzemmódban a klasszikus rádióháló szervezésű híradás keretein belül (beszéd, adat) teljeskörűen képesek együttműködni egymással. Az MP300 és MV300 ezen felül alkalmas APR60 módban szelektív beszéd és adathívások lebonyolítására, megfelelő konfigurációban reléként működni, illetve a rádióvezérlő terminál (RCT61) segítségével távvezérlésük is biztosított.

CNR módban a rádiók FM modulációra is képesek, ami biztosítja a régi analóg eszközökkel való forgalmazást. (Vészhíváson és rádiócsenden kívül más szolgáltatás nem vehető igénybe.) Digitális fix frekvenciás (FF) és frekvenciaugratásos

[58] Multi Role Radio
[59] Combat Net Radio
[60] Autonomous Packet Radio
[61] Radio Control Terminal

(FH) adásmód esetén a spektrumszórásnak (NBDSSS62) és GMSK63 modulációnak köszönhető hatótávolság növekményen felül lehetőség van az elektronikai harc és rádióelektronikai felderítés eredményességét csökkentő szolgáltatások (interferencia védelem, automatikus frekvenciaválasztás) alkalmazására, valamint rövid szöveges üzenetek (SMS64) küldésére is.

MRR rádiók adatátviteli szolgáltatásai, tulajdonságai

Az alapvető műszaki paraméterek közül az adóteljesítmény65 és a minimális jel/zaj viszony (-3dB) mellett, az adatátvitelre jellemző vevőérzékenység határozza meg az adott átviteli sebességhez tartozó maximális hatótávolságot. Míg beszédösszeköttetés létrehozásához a vevő bemenetén FM esetben legalább -112dBm, digitális modulációval pedig -114dBm teljesítményre van szükség, SMS küldéséhez -122dBm, alacsonysebességű (2,4kbit/s) adatok továbbítására pedig már -123dBm is elegendő. Azaz a legnagyobb hatótávolság alacsonysebességű adatátvitel során valósítható meg. Az átviteli sebesség növelésével az áthidalható távolság csökken66.

Transzparens átvitel esetén az RS232 soros többvezetékes adatátviteli szabványon keresztül illesztett terminál által szolgáltatott adatok módosítás nélkül kerülnek kisugárzásra a titkosítást, valamint a rádiófrekvenciás jelfeldolgozást követően. A hatótávolságon belüli, azonos hálóparamétereket, rejtjelező kulcsot és interfészkonfigurációt használó rádiók ezeket a jeleket veszik, visszaalakítják és kicsatolják a megfelelő portjukra, azaz broadcast jellegű információtovábbításról, adatszórásról beszélhetünk (körözvény hívás). Szinkron átvitel megvalósításához az órajel továbbítására is szükség van, hogy a megfelelő információs bitek a számukra kijelölt időrésekben kerüljenek átvitelre vezérlőbitek alkalmazása nélkül. Aszinkron esetben a csatornára adott információs bitsorozatokat vezérlőbitek (start, stop) határolják, amelyek alapján a vevő rádió tudja, mikor kell fogadásra kapcsolnia és mikor leállnia.

Típus	Üzemmód	Protokoll	Sebesség (bit/s)	Interfész
MV300/ MP300	CNR/ CNR relé	transzparens szinkron	FF – 2400/4800/9600/16000 FH–300/600/1200/2400/4800/9600/16000	2-vezetékes többvezetékes
		transzparens aszinkron	FF – 2400/4800/9600/19200 FH – 300/600/1200/2400/4800/9600/19200	2-vezetékes többvezetékes
		X.25 protokoll (szinkron)	2400/9600/16000	2-vezetékes többvezetékes
	CNR APR	X.25 protokoll (szinkron)	2400/9600/16000	2-vezetékes többvezetékes
MH300	CNR	transzparens szinkron	300/600/1200/2400/4800/9600/16000	többvezetékes
		transzparens aszinkron	300/600/1200/2400/4800/9600/19200	többvezetékes

[62] Narrow Band Direct Sequence Spread Spectrum

[63] Gauss Minimal Shift Keying

[64] Short Message Service

[65] MV300: 10mW/500mW/5W/50W, MP300: 10mW/500mW/5W, MH300: 16mW/1W

[66] pl. 16kbit/s esetén a vevőérzékenység már csak -110dBm, tehát 2dB-el még az FM hangátvitelénél is kisebb lesz a hatótávolság.

A rádiócsalád minden tagja a különböző típusú adatterminálok fizikai csatlakoztatására tartalmaz egy multipólusú interfészt, míg a hordozható és járműfedélzeti eszközök RCT-i még egy érintkezőpárral is el lettek látva kétvezetékes kapcsolat létrehozása érdekében. Az MV300 és MP300 rádiók két interfészéből egyszerre csak egy aktiválható, ugyanakkor mindkettőhöz hozzárendelhető a három adatátviteli protokoll bármelyike. A transzparens szinkron és aszinkron átviteli mód az MH300-as többvezetékes interfészén keresztül is hozzáférhető, míg az X.25 szabvány szerinti kommunikáció csak a másik két típus esetén biztosított. CNR APR üzemmódban csak ez utóbbi protokoll alkalmazható. A különböző üzemmódokban, interfészeken és protokollokkal elérhető adatsebességeket a következő táblázat tartalmazza67

Az X.25 protokoll specifikációja szerint egy csomagkapcsolt hálózati szabvány, ami a fizikai csatornától függetlenül szabályozza az adatterminálok közti forgalmazást. Az X.25 már nem számít korszerű megoldásnak, pláne az IP68 alapú kommunikáció világában, így a számítógépek és operációs rendszerek nem támogatják közvetlenül használatát. Az anomália feloldása csomagképző (PAD69) alkalmazásával lehetséges, ami interfészt biztosít az adatterminál (DTE70) és az adathálózati eszköz (DCE71) között. Tehát egy számítógép MRR rádióhoz X.25-ön való illesztéséhez modem alkalmazására van szükség, ami lehetőséget biztosít egy adatháló tagjai között a címzett, közvetlen információtovábbítás megvalósítására (pont-pont, pont-multipont).

A rádiók hardvere és szoftvere által biztosítottak a specifikációban szereplő adatkommunikációs lehetőségek, gyakorlati alkalmazásuk azonban további feltételek teljesülése esetén válhat csak lehetségessé. Mind a transzparens szinkron, mind az X.25-ös protokoll alkalmazásához megfelelő csatlakozó kábelekre és egyes alkalmazásokhoz számítógépes kártyákra lenne szükség. A MH rádiókészleteihez rendszeresített kiegészítő anyagokkal jelenleg csak transzparens aszinkron adatátvitel valósítható meg, ami azonban a fentiek alapján adathálózati protokoll hiányában megbízhatóan csak pont-pont viszonylatban alkalmazható. Ha egy adathálózatban növeljük a tagállomások számát, az adatátvitel során alkalmazott paritásra épülő „küldés-nyugta, vagy küldés-újraküldés„ metódus felborul, hiszen semmi nem vezérli a tagállomások forgalmazását. A nyugták ennek következtében gyakran ütköznek, így az adórádió nem kapja meg azokat és újraküldi a hibásan átvittnek hitt adatokat. Ez rövid időn belül kaotikus forgalmazáshoz, majd az összeköttetés megszakadásához vezet. (Hogy ez bekövetkezik-e és mikor, az függ a tagállomások számától, az alkalmazott adóteljesítményektől és a hálózati topológiától, azaz a rádiók egymáshoz képesti elhelyezkedésétől.) Ezáltal a harcászati igényként fölmerülő adatgyűjtés (pl. felderítési adatok), valamint adatszétosztás (pl. célkoordináták) a jelenlegi feltételek mellett nem valósítható meg megbízhatóan.

[67] A fenti paraméterek az MH alakulatainál rendszeresített eszközök jelenlegi szoftververzióira érvényesek.

[68] Internet Protocol

[69] Packet Assembler/Disassembler

[70] Data Terminal Equipment

[71] Data Circuit Terminating Equipment

Az adatkommunikációra épülő egyéb szolgáltatások tekintetében a fönti anomália további nehézségeket is okozhat, ugyanakkor számos egyéb alkalmazás problémamentesen vehető igénybe. Az SMS minden digitális üzem- és adásmódban hozzáférhető, amelynek segítségével tetszőleges tartalmú, vagy formázott, nyílt, vagy minősítetett információkat tartalmazó szöveges üzenetek küldhetők közvetlenül egyes tagállomásoknak, tagállomások egy csoportjának, vagy broadcast jelleggel minden hatótávolságon belüli tagállomásnak nyugtával, illetve nyugta nélkül egyaránt. A jelenlegi szoftververzióval nem elérhető, ugyanakkor rendelhető szolgáltatás, hogy a rádióhoz csatlakoztatott számítógép vegye át az üzenetkezeléssel kapcsolatos funkciókat, ami megkönnyítené a vezetési pontokon szolgálatot teljesítők munkáját a nagyszámú beérkező jelentés gyors feldolgozásának lehetőségével.

Automatizált vezetési rendszerek kialakításához szükséges szoftvermódosítás szintén rendelhető szolgáltatás. Ennek segítségével a rádiók teljes vezérlését, vagy vezérlési funkcióinak egy részét az RCT átadhatja a csatlakoztatott számítógépen futó alkalmazásoknak, így gyorsítva az adatforgalmazás rádióhálóban történő szervezését, illetve a harcvezetési rendszerek működését, a kezelői beavatkozás szükségességének minimálisra csökkentésén keresztül.

Az RCT-hez közvetlenül illeszthető hálózat- és teljesítményválasztó egység (NPS72), harcászati nyomtató alkalmazásának akadálya kizárólag azok hiánya, rádióink semmilyen módosítását nem igényelné.

A reléként való működés két rádió (MV300, vagy MP300) kétvezetékes interfészen keresztül történő összekapcsolásával jelenleg is biztosított.

Megoldások az MRR rádiók adathálózati képességeinek növelésére

A rádiók felépítése, műszaki paraméterei és interfészei által biztosított adatátviteli szolgáltatások gyakorlati alkalmazások számára való hozzáférhetővé tétele egyre sürgetőbb feladattá válik, az egyre növekvő számú és eltérő jellegű adatkommunikációs igények miatt. A korábban felvázolt anomália feloldására több lehetőség is kínálkozik.

A legköltségesebb, ugyanakkor leghatékonyabb megoldás, ha az adathálók létrehozásához IP platformon működő hálózati (szoftver) rádiókkal váltjuk ki MRR eszközeinket, ezzel lehetőséget teremtve az adatterminálok közvetlen, problémamentes illesztésére, informatikai alapú hálózatba szervezésére, valamint a jövőben fölmerülő adatkommunikációs igények gyors és rugalmas kielégítésére.

Kevésbé költséges és rugalmas megoldás, ha a meglévő rádióink jelenlegi adatkommunikációs képességeinek maximális kihasználtságát lehetővé tevő kiegészítő eszközöket beszerezzük, illetve az adatátviteli sebességek növeléséhez (64kbit/s) szükséges szoftverfrissítéseket megrendeljük.

Minimális anyagi ráfordítással a fent említett problémák jelentős része saját fejlesztésű számítógépes alkalmazásokkal, illetve illesztő egységekkel is áthidalhatóvá válik. Ennek létjogosultságát alátámasztandó, szeretném felhívni a figyelmet néhány olyan jelenleg is folyó fejlesztésre, ami a fennálló feltételek mellet igyekszik maximalizálni az MRR rádiók adatátviteli képességének kihasználását.

[72] Network & Power Selector

A Zrínyi Miklós Nemzetvédelmi Egyetem Kossuth Lajos Hadtudományi Kar Műveleti Támogató Tanszékén hosszú évek óta zajlik a TOPCIS tábori számítógépes harcvezetési rendszer fejlesztése. Felmerült az igény, hogy az alkalmazás mobilitásának növelésére a rendszer termináljait ne csak vezetékes informatikai hálózaton, hanem MRR rádiókból felépülő rádióhálón is össze lehessen kapcsolni. A probléma megoldásához a ZMNE Bolyai János Katonai Műszaki Kar Híradó Tanszékétől kértek segítséget. Az újjászerveződő tudományos diákköri mozgalom keretében Németh Szabolcs végzős híradó hallgató (ma mk. hdgy.) vállalta fel, hogy készít egy a TOPCIS rendszer igényihez optimalizált kísérleti programmodult, ami képes – a fent említett korlátozások miatt kizárólagosan rendelkezésre álló – transzparens aszinkron csatornán hierarchikus adatkommunikáció megvalósítására. Munkáját siker koronázta, az alkalmazás elkészült, rendeltetésének megfelelően működött. Eredményeiből pályázatot készített, amellyel indult a ZMNE 2007/2008. évi tavaszi Intézményi Tudományos Diákköri Konferencián, valamint egy csehországi nemzetközi tudományos diákköri konferencián, és számos különdíj mellett elnyerte – mindkét helyszínen – szekciójának első díját.

Mivel a szoftver bevált, szükségessé vált egy hasonló, de komplex szolgáltatásokat biztosító, általánosabb felhasználású program készítése is, melynek fejlesztése Salamon Dániel mk. hdgy. által jelenleg is zajlik.

Az eddig szerzett tapasztalatok, illetve elért eredmények segítséget jelentenek és jelenthetnek a továbbiakban is a MH 12. Arrabona Légvédelmi Rakétaezrednél kialakítás alatt álló tűzvezetési rendszer, valamnMH Görgei Artúr Vegyivédelmi Információs Központnál fejlesztés alatt álló légi vegyisugár-felderítő konténer MRR rádiókra épülő adatkommunikációs csatornáinak kialakításához.

Konklúzió kicsit másként

A MH különböző szervezeteinél, alakulatainál szolgáló híradó és informatikai tisztek rendelkeznek megfelelő mérnöki alapokkal, általános szakmai-, valamint saját területükön specifikus ismeretekkel és tapasztalattal, ami lehetőséget biztosítana egy állandó szakmai fórum létrehozására. Ennek feladata a felmerülő technikai és szervezési kérdések, problémák megvitatása lenne, lehetőséget teremtve optimális, hatékony megoldások kidolgozására, illetve a döntéshozók felé egységes álláspont kialakítására a híradó és informatikai tervezési, szervezési, fejlesztési és beszerzési területen egyaránt.

Felhasznált irodalom

[1] Németh Szabolcs: Hierarchikus adatátvitel megvalósítása a TOPCIS harcvezetési rendszerben MRR rádióhálók transzparens aszinkron adatkommunikációs csatornáin, ZMNE, 2008 (szakdolgozat)

[2] Konsberg MRR rádiócsalád dokumentációja [Konsberg Defense Communication AS]

PÁNDI Balázs – PÁNDI Erik[73]

A TÉRINFORMATIKA TÁBORI HÍRRENDSZERBEN TÖRTÉNŐ ALKALMAZÁSÁNAK KÉRDÉSEI

Absztrakt: cikkünkben a hazai szakmai-tudományos közélet által közreadott véleményekre támaszkodva, azokat értékelve áttekintjük a térinformatikai alkalmazások jelenlegi hazai tábori kommunikációs rendszerben való felhasználásának feltételeit és lehetőségeit.

Kulcsszavak: MHÁTKR, MHKR, MHTKR, MHTTKR, tábori hírrendszer, térinformatika, vezetés-irányítás.

1. Alapvetés

A harc eredményes megvívását nagymértékben befolyásolja a vezetés-irányítás támogatási rendszere. A kommunikáció megfelelő biztosításának hiányában az egységek, alegységek képtelenek feladataik sikeres végrehajtására. A különböző vezetési szinteken napjainkban markánsan fogalmazódik meg azon követelmény, amely szerint a lehető legtöbb, strukturált adatnak, információnak kell rendelkezésre állnia ahhoz, hogy a döntés-előkészítés és -hozatal korrekt lehessen [1]. A jelenleg meglevő, a gépesített harcászati-hadműveleti magasabbegységek infrastruktúráját biztosító hálózat a kor követelményeinek megfelelő, a kor színvonalán álló rendszer biztosítására nem képes. Kis csatornaszámmal rendelkezik, manőverező képessége alacsony szintű, technikai eszközei mind erkölcsi, mind fizikai szempontból amortizáltnak tekinthetők. A rendszer túlnyomó többségében analóg felépítésű, hálózati szolgáltatásokkal nem rendelkező szisztéma, amely a szükséges hírközpont sűrűséggel nem képes a hadműveleti terület lefedésére, híradó csatlakozás biztosítására. A hálózat telepítése mellett külön üzemel még a közvetlen összeköttetések vonalain belül a személyhez kötött rádióállomások rendszere, ami jelentősen növeli a híradó eszközök és személyzet létszámát. A hálózat távfelügyelettel, informatikai eszközökkel támogatott hálózattervezéssel, elektronikus csatornaállapot vizsgálattal nem rendelkezik. Tartalékai a rendszernek szinte nincsenek, csatornamanőverek, kerülő irányok létesítése a katonai műveletek időszakában óriási feladatot jelent, magas szakmai felkészültséget igényel. A korszerű hadviselés alapelvei alapján a rendszer nem képes követni a helyzetek gyors és éles változását, alaphírközpontjai nem képesek lépést tartani az összfegyvernemi tevékenységek ritmusával. A tábori alaphírhálózat korszerű híradó eszközöket nem tartalmaz, a katonai műveleti vezetés részére multimédia szolgáltatások biztosítására nem alkalmas. Más NATO tagországokkal rendszerszintű együttműködésre lehetőség nincs, multinacionális alkalmazás esetén képtelen más tagországok rendszereinek fogadására [2].

[73] szerzők: Pándi Balázs, PhD-hallgató, ZMNE BJKMK Katonai Műszaki Doktori Iskola; Dr. Pándi Erik, egyetemi docens, ZMNE BJKMK Híradó Tanszék

Ezzel ellentétben, a NATO hasonló kommunikációs rendszerei esetében a műveleti területen egy rácsrendszerű, területlefedő hálózat kialakítására törekednek, megfelelő hírközpontsűrűséggel. Ez azt jelenti, hogy a domborzat és a kommunikációs igények figyelembe vételével a csomópontokat a műveleti területen egymástól néhány tíz km-re helyezik el, majd azokat a szomszédos csomópontokkal összekötik, így alakítva ki egy komplex kommunikációs hálózatot. Ezen megoldás nem feltételez tengelyeket, mint a hazai tábori alaphírhálózat, mert a műveleti területen telepített csomópontok azonos szolgáltatásokat képesek nyújtani. A csomópontok tehát azonos képességekkel rendelkeznek, így a rendszer minden pontján képes fogadni a különböző vezetési pontok hírközpontjainak csatlakozását a harcászati kötelékektől egészen a legfelső katonai parancsnokságig. A területlefedő rácsrendszerek közös jellemzője az automatikus útvonal keresési rendszer. A kommunikációs hálózatok a hívott fél keresését, az összeköttetés felépítését és létesítését automatikusan valósítják meg az előre meghatározott fizikai, vagy logikai útvonal kiválasztásának megfelelően [3]. A tábori hírrendszer kapcsán fennálló generációváltás szükségességére a madridi, illetve londoni terrorcselekmények ismételten rámutattak, hiszen a terrorizmus elleni küzdelemben a megfigyelő, különösen a mobil képátvitelt biztosító rendszereknek napjainkban már kiemelkedő szerep jut. Ezzel párhuzamosan, a hadseregben, a nemkatonai műveletek (pl.: terrorizmus elleni harc) sikere egyre inkább igényli a valósidejű adatátviteli képességek kialakítását [4].

A Magyar Honvédség Kommunikációs Rendszerét (MHKR) alkotó MH Állandó Telepítésű Kommunikációs Rendszer (MHÁTKR), illetőleg MH Tábori Kommunikációs Rendszer (MHTKR) közül az MHTKR és ezen belül az MH Tábori Területi Kommunikációs Rendszer (MHTTKR) kimondottan elavultnak tekinthető. Az MH híradása fejlesztésének alapelvei és célkitűzései nem mások, mint [5]:

a) egységes, közös híradó és informatikai infrastruktúra kialakítása;
b) integrált szolgáltatású digitális hálózat felépítése;
c) állandó és tábori körülmények között is azonos szolgáltatások biztosítása;
d) NATO követelmények kielégíthetősége;
e) a kormányzati, a közcélú és a szövetségi rendszerekhez való csatlakozás képességével rendelkező integrált rendszer kialakítása;
f) biztonsági feltételek biztosítása;
g) a továbbfejlesztés biztosítása.

2. A térinformatika alkalmazási lehetőségei

A NATO tagországokban a térinformatikai alkalmazásoknak különösen a tervezés, szervezés időszakában, de a végrehajtási fázisokban is fajsúlyos jelentőséget tulajdonítanak. A célszoftverek alkalmazási területei a következők lehetnek [6]:

a) a hadműveleti terület értékelése;
b) elhatározás kialakítása;
c) vezetési pontok települési helyeinek kiválasztása;

d) hírközpontok, csomópontok települési helyeinek kiválasztása;
e) összeköttetés tervezése;
f) tűzvezetés;
g) logisztikai támogatás, utánpótlás;
h) közlekedés, szállítás;
i) kommunikációs infrastruktúra, stb.

Amennyiben szűkebb területre, a kommunikációs rendszerek tervezésére, szervezésére korlátozzuk a térinformatikai alkalmazások lehetőségeit, megállapítható, hogy a kommunikációs rendszerek tervezése időszakában a híradófőnök kiemelt feladata már a feladattisztázás során a terep értékelése, hiszen a hírközpontok települési helyeit, a köztük levő összeköttetések megvalósulásának valószínűségét már a tervezés során vizsgálnia kell. Elemeznie szükséges a terep magassági adatait a láthatóság (URH, mikrohullám) vizsgálatához. Természetesen ezek csak a legfontosabb elemi területei a híradófőnökök munkájának, ahol a térinformatikai alkalmazások felhasználásra kerülhetnek.

Az összfegyvernemi törzs felhasználási lehetőségei ennél sokkal szélesebb körűek, nemcsak az adatbázisok, rétegek felhasználásával (újabb rétegek létrehozásával), hanem adatok továbbításával is alkalmazhatja a térinformatikát. Amennyiben egy híradófőnök hírközpontot kíván telepíteni az adott műveleti területen, lehívhatja a *csapatok elhelyezkedése* réteget, amely megmutatja számára az adott területen diszlokált alegységeket, egységeket, így eldöntheti a pontos települési helyet. Ha tehát meg akarjuk határozni azokat a rétegeket, amelyekkel egy adott térinformatikai szoftvernek rendelkeznie kell, a következőket célszerű például követelményként támasztani:

a) békediszlokáció;
b) határszakaszok;
c) út- és közúthálózat;
d) vízrajz;
e) domborzati adatok;
f) növényzet;
g) hidak;
h) térképi objektumok (háromszögelési pontok, azok jellemzői);
i) lakott települések;
j) kommunikációs (távközlési) infrastruktúra.

Mindezek mellett néhány réteg még biztosítható egyes speciális feladat támogatására, mint például:

a) műveleti felépítés (csapatok helyzete a műveleti területen);
b) vezetési pontok és hírközpontok elhelyezkedése;
c) fegyvernemek, szakcsapatok saját rétegei.

Megállapítható tehát, hogy a katonai térinformatikai rendszereknek támaszkodnia, illeszkednie kell polgári, hagyományos tevékenységekkel folytatott tervezési rendszerekhez, így biztosítható, hogy a katonai térinformatikai rendszerrel szembeni elvárások nem lesznek irreálisak.

Természetesen a rendszernek nem minden pontján van szükség ugyanazon szolgáltatásokra, másra lesz szükség egy szárazföldi, vagy egy légi műveletben. Ezeket a sajátosságokat már a kidolgozás fázisában figyelembe kell venni. A kato-

nai térinformációs rendszereknek tehát olyan digitális térképi állományokat és azok objektumleírásait kell kezelnie, amelyek az adott szintű tervezési feladatok információs igényeit a lehető legszélesebb spektrumban és a legnagyobb mélységben kielégítik. Ez azonban nem jelenti azt, hogy a különböző vezetési szintek csak a térképmunkánál használatos digitális térképen kell, hogy dolgozzon. Adott esetben a magasabbegység részére is szükséges lehet M 1:50000 léptékű nagyítás a terület egy-egy részéről, hogy a lehetséges alternatívákat a szükséges mélységig képes legyen a törzs kidolgozni a parancsnokok döntésének támogatására. A digitális térképészeti adatok mellett ezen alkalmazások képesek az adott objektumról szöveges információt is adni.

A nyugat-európai példák jól mutatják, az informatikai eszközök nem helyettesítik, hanem csak támogatják a hagyományos törzsmunkát. A jelenlegi tervezési folyamat jellegzetességét, főbb munkafázisait nem szabad figyelmen kívül hagyni, e tevékenység továbbra is a tervezés gerincét alkotja, a számítógépes alkalmazások bevezetése ezt a folyamatot meggyorsítja, egyes részeit automatizálja, az értékelés folyamán olyan eseményekre hívja fel a figyelmet, amelyek hagyományos technikákkal fel sem mérhetők, valamint lehetőséget adnak bizonyos események modellezésére.

Egy vezetést támogató, döntést előkészítő rendszert a vezetési hierarchiának megfelelően, fentről lefelé célszerű kiépíteni, ami a műveleti tervezés folyamatában azt jelenti, hogy először a magasabbegység, majd egység és végül az alegység szintű rendszereket kell kiépíteni. A fegyvernemek rendszereinek egymással rugalmasan együttműködő, illeszkedő modelljének megalkotása lehet az egyik fő feladat. A térinformatikai rendszerek kialakításánál célszerű a rendszert úgy felépíteni, hogy az támaszkodjon az MH már meglevő és fejlesztés alatt álló informatikai rendszeréhez, és mind a béke, mind a műveleti feladatokat egyaránt támogassa. Ezeknek az alkalmazásoknak olyan digitális térképi állományokat és azokat leíró attribútumait kell kezelniük, amelyek az adott tervezési feladatok információs igényeit kielégítik. A kialakítandó rendszernek biztosítania kell a hadrendi elemek földrajzi elhelyezkedésének nyilvántartását, digitális térkép fölötti megjelenítését, a hadrendi elemek mozgatását, egyezményes jelkészlet kialakításával ezen jelek, szimbólumok térképre történő felvitelét. Ehhez jó alapot szolgálnak a NATO egyezményes jelek, amelyek a számítógépes feldolgozásra is kiválóan alkalmasak. Szükséges továbbá, hogy az objektumleíró funkciókat egyesítve a rendszer biztosítani tudja az egyezményes jelek, tereptárgyak, objektumok jelei mellett az azokhoz köthető szöveges (karakteres) jellemzők megjelenítését is a már kiválasztott 3D ábrázolás mellett.

Fentiek alapján látható, hogy bármilyen térinformatikai rendszer csak akkor alkalmazható műveleti területen, amennyiben rendelkezésre áll az adatok továbbításának lehetősége. Ehhez két feltételt kell biztosítani. Egyrészről egy korszerű hálózatra van szükség, másrészről a rendszernek biztosítania kell az adatátvitelhez szükséges szabványformátumokat. Az adatcsere másik feltétele a szabványoknak való megfelelés, hiszen az adatcserét nemcsak a saját csapatok között, hanem multinacionális környezetben is meg kell valósítani. A térbeli adatátvitelben több szabvány is létezik, amelyeket az alkalmazások rendszerbe állítása előtt célszerű figyelembe venni.

3. Összegzés, következtetések

A térinformatikai alkalmazások felhasználása nélkül napjainkban a vezető-irányító, valamint a végrehajtó állomány lényegében kevéssé tud megfelelni a XXI. század új hadviselési formája által támasztott követelményeknek. Az MHTTKR jelenlegi formájában alkalmatlan a korszerű információtechnológiai alkalmazások támogatására, ezért a külföldi műveleti területeken kötelékben szolgálatot teljesítő magyar katonák kénytelenek ad-hoc összeállított, valamint a NATO által rendelkezésre bocsátott kommunikációs eszközökkel és megoldásokkal élni.

Természetesen az MHTTKR rendszerében önállóan, esetleg hírközponton belül lokálisan működő alkalmazások felhasználására mód nyílhat, azonban az adatcsere követelménye a korábban már több helyen jelzett okoknál fogva csak a tábori rendszeren belül nem oldódhat meg. A probléma látens kezelésére felhasználható az MHÁTKR, azonban e pótmegoldás nem elégíti ki a mobilitási igényeket.

Összességében a *NATO Hálózat Nyújtotta Képességek (NNEC)* programja keretében kialakítandó képességek befogadása érdekében az MHTTKR gyorsütemű, első fejezetben jelzett elvek szerinti modernizációja nem maradhat el.

Felhasznált irodalom:

[1] Farkas Tibor: A honvédség tervezett kommunikációs hálózata, Kard és Toll, Honvédelmi Minisztérium, Budapest, 2006., ISSN 1587-558X, 54. oldal, 2006/1. szám;

[2] Rajnai Zoltán: A tábori alaphírhálózat korszerűsítésének lehetőségei, „Kommunikáció 2000." nemzetközi szakmai-tudományos konferencia kiadványa, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2000, 95-96. oldal;

[3] Kerti András: A vezetés és a hírrendszer kapcsolata, „Kommunikáció 2006." nemzetközi szakmai-tudományos konferencia kiadványa, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2006, ISBN 978-963-7060-18-2, 295. oldal;

[4] Bleier Attila – Rajnai Zoltán: Vezeték nélküli képátviteli rendszer, Kard és Toll, Honvédelmi Minisztérium, Budapest, 2007., ISSN 1587-558X, 118-119. oldal, 2007/1. szám;

[5] Sándor Miklós – Farkas Tibor: A honvédség állandó hírhálózata fejlesztésének kérdései, Kard és Toll, Honvédelmi Minisztérium, Budapest, 2006., ISSN 1587-558X, 160-163. oldal, 2006/2. szám;

[6] Rajnai Zoltán: A csapatvezetésben alkalmazott térinformatikai rendszerek szabványosítási törekvései, Nemzetvédelmi Közlemények, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2002., ISSN 1417-7323, 120-123. oldal, 2002/1. szám.

TAKÁCS Péter

KATONAI INFORMÁCIÓS RENDSZEREK ALKALMAZÁSI LEHETŐSÉGEI A MAGYAR HONVÉDSÉG TÁBORI HÍRADÁSÁBAN

Absztrakt

A 21. században az információ, az ahhoz való hozzáférés felértékelődésével összhangban változás állt be a hadviselésben is. Az új technikai vívmányokon alapulva új információs rendszerek jelentek meg, amik a régi rendszerekkel összeolvadva egy integrált rendszert hoztak létre, kialakítva ezzel a hálózatközpontú hadviselést.

In the 21. century the information, the ability of accessing this information become the leading part of modern warfare. Based on the new technical solutions new information systems shown up. Integrating these new sytems with the old ones, the network centric warfare spread all over the world.

Kulcsszavak: hálózat központú hadviselés, katonai információs rendszer, taktikai internet

Nemzetközi helyzet

A 21. század hadviselése, katonai műveletei az új technikai vívmányok hatására jelentősen megváltoztak. Előtérbe került a csapatok mobilitása, és a harchelyzetek esetenként éles változásának ellenére a csapatok folyamatos vezetésének, a harchelyzet figyelemmel kisérésének igénye. Ezek az új követelmények az információ nagy tömegben történő gyors átvitelét, a hatalmas mennyiségű információk gyors kiértékelését, megjeleníthetőségét teszi szükségessé. Az 1990-es évek elejétől a világ (de főleg Európa) vezető országai felismerték, hogy hadseregeik vezetésirányítási rendszereit meg kell reformálniuk. Megjelent és előtérbe került a hálózat központú hadviselés, mely lehetővé teszi, hogy az információ a kellő időben rendelkezésére álljon a vezetés minden szintjén az optimális döntések meghozatalának érdekében. Ez a harctér digitalizációját, új katonai információs rendszerek kialakítását, ezekbe a régi rendszerek teljes integrációját vonták maguk után. Ilyen változások történtek például az USA-val az élen a német, a francia, a kanadai és a brit hadseregekben is.

Fontos kiemelni, hogy ezek a hálózatok a nagy hadsereggel rendelkező országokra különösen jellemzőek, melyek a szárazföldi, a légierő és a haditengerészet erőinél is képviseltetik magukat. Jellemző ezekre a hadseregekre, hogy komplett, nagyméretű hadműveletek végrehajtására képesek, ahol fontos az összehangolt művelet, a bonyolult szituációk egyszerű felvázolása az események valós idejű követése és az összhaderőnemi együttműködés szükségessége.

Hazai helyzet

A Magyar Honvédség egyre nagyobb szerepet vállal a világ több pontján békefenntartó, multinacionális missziókban, ami égetően szükségessé teszi az előző részben említett, átfogó digitalizációt a harctéren, illetve a haderőben. Ezzel ma-

gyarázható a szövetségi elkötelezettségekből adódó feladatok során más nemzetekkel történő együttműködés szükségessége is, ahol hatékonyan ki lehet használni a korszerű vezetés-irányítási rendszerek által nyújtott ilyen jellegű szolgáltatások alkalmazása. Gondolok itt egy kisebb, zászlóalj erejű alegység felszerelésre tábori C2 vezetés-irányítási rendszerrel, mely kellő műszaki követelmények és kompatibilitási feladatok realizálása mellett szövetségi műveletek kereteiben is hatékonyabban és biztonságosan képes a vezetés részére szükséges elengedhetetlen információk biztosítására [1]. Ezek a rendszerek lehetővé teszik a mindenkori valósidejű helyzetkép kialakítását, éppúgy, mint a műveletek sikerét, annak biztonságos végrehajtását támogatását.

Egy zászlóalj erejű alegységnek a jövőben a hatékony nemzetközi szerepvállalás érdekében minimum a következő katonai információs rendszerek integrációjával, alrendszerekkel kell rendelkeznie:

- Harcászati Internet
- Helymeghatározó rendszer
- Harctéri azonosító rendszer
- Vezetési pont informatikai rendszere
- A hálózat elemeit összekötő kommunikációs hálózat

Harcászati Internet

A Harcászati Internet a modern háborús hadviselés egy új fogalma, a hadszíntér digitalizálásának egyik legfontosabb eleme. Lényegében ez egy integrált kommunikációs rendszer mely összeköti a harctér minden résztvevőjét, az első sorban harcoló katonától kezdve a vezetési ponton levő parancsnokig. A hálózat egyik legfontosabb jellemzője, hogy minden felhasználójának a kellő időben, a felhasználó szintjének megfelelő mennyiségű információt biztosít, ez által segíti a döntéseiben a parancsnokot, megbízható kommunikációt biztosít a hálózat szereplői között így a parancsnok döntései időben eljutnak az alárendeltekhez.

Eszközrendszerét tekintve gyakorlatilag rendszerbe integrált harcászati rádiókat jelent, melyek a hangátvitel mellett több más szolgáltatást nyújtanak, mint például álló vagy mozgókép átvitel.

Helymeghatározó rendszerek

Idegen, ellenséges környezetben létfontosságú, hogy a saját erők mindig megbízhatóan tisztában legyenek elhelyezkedésükkel a harctéren. A helymeghatározásra az elmúlt években több technikai megoldás is született (Pl.: GSM alapú, stb.). Főleg igaz ez a technikailag fejlett térségekre. A békeműveletek és más katonai műveletek helyszínei ellenben technikailag jóval elmaradottabbak, ezekben a régiókban ma az egyetlen jól alkalmazható eljárás a GPS alapú pozícionálás, segítségével mára méteres pontossággal meghatározható a helyzetünk. Saját missziós tapasztalataim alapján itt tartom fontosnak megemlíteni, hogy a pozíció lekérésének többirányúnak kell lennie. A mai fejlett katonai információs rendszerekben ez mára már így működik. Gondolok itt a lekérdezés forrására. Tehát a rendszer nem csak a katonát tájékoztatja a saját pozíciójáról, hanem a parancsnokát is, más együttműködő információs rendszereknek is átadja a koordinátáját.

Fontosnak tartom megemlíteni, hogy a GPS rendszerek nagyban zavarhatóak, a tájékozódása az egyes katonának nem függhet egyoldalúan az ilyen rendszerektől. Képzésükben meg kell tartanai a régi, hagyományos tájékozódási, helymeghatározási eljárásokat is, ezzel növelve túlélőképességüket.

Harctéri azonosító rendszerek

NATO tagságunk kezdete óta egyre nagyobb szerepet vállalunk a világ stabilitásának visszaállításában, fenntartásában, a világ több színterén képviseltetjük magunkat békemissziókban. Ezekben egyelőre a járőrözésen és táborvédelmen kívül közvetlen harci tevékenységet nem folytatunk, de történhet úgy, hogy többnemzetiségű kontingensekkel közös műveleteket kell végrehajtani. Mára ennek a közös munkának egyik feltétele a harctéri azonosító rendszer megléte. Több technikai megoldás létezik, pl.: a GPS pozíciókkal feltöltött adatbázis alapú, vagy a lekérdező modellen alapuló.

Ennek a rendszernek a tervezésekor alaposan figyelembe kell venni, hogy az képes legyen együttműködni a többi nemzet ilyen rendszereivel, hiszen ezek alkalmazása nem öncélú.

Vezetési pont informatikai rendszer

A harctér összes elemének tervezésekor fontos szem előtt tartani, hogy azok nem öncélú rendszerek, képesnek kell lenniük összedolgozni, egymásnak adatot szolgáltatni. Ez a vezetési ponton csúcsosodik ki, ide kell befutnia minden szálnak, hogy a parancsnok a harctéri szituációt egyetlen képként tudja értelmezni, kellő mennyiségű és pontos információval rendelkezzen, hogy megalapozott döntést tudjon hozni minden helyzetben.

Kommunikációs hálózat

A harctéri rendszerek működése szempontjából kulcsfontosságú tényező az őket összekötő hálózat technikai paraméterei. Ezeknek a hálózatoknak legfontosabb jellemzői a mobilitás, a gyors helyváltoztatás, melyek vezeték nélküli eszközöket feltételeznek. A legnagyobb technikai kihívást ezen a téren nem a rádiók, mint eszközök, hanem az általuk használt úgynevezett „routing protokollok" jelentették. A hálózat elemeinek a harctéren egymáshoz viszonyított elhelyezkedése gyorsan változhat, eszközök semmisülhetnek meg, eshetnek ki. Ezekre a szituációkra a hálózatnak önállóan reagálnia kell, a fennálló helyzet függvényében a rendszernek az adatok útját folyamatosan és rugalmasan tudnia kell megváltoztatni.

Másik fontos tényező az ellenség támadó jellegű elektronikai tevékenysége, melyek kivédése speciális rádiókat követel meg. Mára már teljesen elfogadott és elterjedt eszközei a harctérnek a különböző szórt spektrumú, frekvenciaugratásos elven működő eszközök.

Amennyiben ezeket a rendszereket áttekintjük nemzetközi téren, néhány tipikus és általános jellemzőt is meg kell említenünk. Ezek értelmezését néhány példán keresztül kívánom bemutatni.

USA

Az előző részben említett ilyen területű kutatások egyik legfontosabb képviselője a DARPA[74], mely neve alatt több, vezeték nélküli hálózatok kialakítására törekvő, nyílt és zárt projekt folyik napjainkban is. Ilyen említésre méltó fejlesztések voltak a következőek, melyek a DARPA STO[75] közvetlen irányítása alatt álltak az elmúlt 1-2 évben:

- Next Generation Wireless Networking
- Wireless Network after Next
- Wireless Adaptable Network Node
- DARPA Interference Multiple Access (DIMA)
- Mobile Network MIMO programok

Ezeknek a kutatásoknak általános célja egy több száz, vagy akár ezer csomópontból álló, kognitív rádiókat felhasználó, decentralizált, vezeték nélküli hálózat kifejlesztése volt. Ezek tapasztalatai alapján alakította ki az USA jelenlegi harctéri hálózatait. [2]

Kanada

Hasonlóan széles kutatásokat hajtott végre a General Dynamics Canada, aki 1991 óta a kanadai hadsereg egyik legnagyobb beszállítója, a TCCCS[76], vagy Iris névre hallgató taktikai kommunikációs és vezetés-irányítási rendszer kifejlesztője, melynek továbbfejlesztése a BOWMAN rendszer. A rendszer ma is jelen van Afganisztánban, alkalmazhatóságát ezt megelőzően már Boszniában is bizonyította. A rendszer nyílt forrású technológiákra épít, azt erősíti katonai eszközökkel, mint például speciális VHF rádiók.

A hálózat alapvetően IP alapú, jórészt a polgári életben megtalálható protokollokat használ, mint például: SNMP-t hálózat managementre, de az UDP protokoll egy speciális fajtája, az RUDP is megjelenik az üzenetek továbbításánál. Az előző fejezetekben említett routolási[77] problémát az OSFP[78] technológia felhasználásával oldották meg, mely szintén megtalálható a polgári életben. [3]

Franciaország

A francia hadsereg Harcászati Internet kutatója és a haderő igényeinek adaptálója, megvalósítója a Thales cég. Idevágó egyik fő produktuma a RITA[79] 2000 néven futó rendszer, mely mára már teljes egészében rendszeresítésre került. A rendszer minőségi szintjét mutatja a francia haderő megelégedettsége, melynek bizonyítéka, hogy 2003-ban 78 millió eurós szerződés keretében a francia hadsereg és a Thales további rendszerbővítésekre egyezett meg.[4]

A hálózat kerete alapvetően ATM alapokon nyugszik, erre csatlakoznak fel a különböző hálózati eszközök, mint például a PR4G rádiócsalád tagjai. [5]

---

[74] DARPA: Defense Advanced Research Projects Agency (http://www.darpa.mil)
[75] Strategic Technology Office
[76] Tactical Command, Control, Communication System
[77] útvonalválasztás
78 Open Shortest Path First
79 Réseau Integré des Transmissions Automatique

Széleskörű szolgáltatásokat nyújt hang, adat, video átvitel terén, valamint a harctéri levelező és üzenetküldő szolgáltatások területén.[6]

Emberi tényezők

Mindezen technikai újítások bevezetésnek megfontolásakor célszerű más tényezőket is megvizsgálni. Mint minden rendszerben itt is az emberi tényező lehet a leggyengébb láncszem. Az ilyen „digitális" jellegű hadviselés a régi hagyományos követelményektől egészen eltérőeket támaszt mind a harctéren harcoló katonával, mind a vezetési ponton lévő parancsnokkal, törzsekkel szemben. Teljesen más parancsnoki- és törzsmunkát feltételez az ilyen jellegű eszközök és rendszerek alkalmazása a vezetésben, és a katonák tevékenysége is jelentős hatást gyakorol. Hasznos idevágó tapasztalatokat lehet és érdemes gyűjteni külszolgálatokon, közös nemzetközi gyakorlatokon résztvevőktől, mint például a ZMNE Híradó tanszékétől a nemzetközi COMMIT gyakorlatsorozat résztvevőitől, ahol ennek a rendszernek az adaptálási, alkalmazhatósági vizsgálatait is végzik oktatók és hallgatók közös keretben.

Összegzés

A világban zajló folyamatok, az információ felértékelődése a hadviselésre is kihatással van. A világ fejlett haderőiben belátták ezt és váltottak: hadseregeiket, azok vezetését a kornak megfelelő elvek szerint szervezték át korszerű vezetés-irányítási rendszerek alkalmazásával. Ahhoz, hogy a Magyar Honvédség a jövőben is képes legyen megfelelni a kor követelményeinek, szintén váltás szükséges mind technikai eszközök, és rendszerek, mind szemléletmód, alkalmazás területén. A közeljövőben meg kell honosítani a hálózat alapú hadviselés elveit és eszközeit, melyeknek vezetés-irányítási rendszerünkben is tükröződnie kell. Erre irányulva a Magyar Honvédség 2007 decemberében közbeszerzési eljárás indított a tábori C2 szoftverrendszer beszerzésére zászlóalj szintre, melyet az elkövetkezendő években tovább fejlesztve és kiterjesztve több zászlóaljra és dandár szintre is ki kívánja terjeszteni.

Felhasznált Irodalom

[1] Rajnai Zoltán: A kommunikációs rendszerek tervezését segítő szoftverek igényei, Kommunikáció-2000 Nemzetközi szakmai tudományos konferencia Különkiadás, ZMNE, Budapest, 2000. pp. 147-150

[2] http://darpa.mil

[3] http://www.gdcanada.com/documents/Battlespace%20Networking%20MA%203.pdf

[4] http://www.janes.com/extracts/extract/jc4i/jc4i1354.html

[5] http://www.defense-update.com/products/r/rita.htm

[6] Rajnai Zoltán: A hadszíntér digitalizálása, Kommunikáció-2001 Nemzetközi szakmai tudományos konferencia Különkiadás, ZMNE, Budapest, 2001 ISBN 963 00 8819 3-2001. pp. 171-179.

Dr. DÁRDAI Árpád

MOBIL TÁVKÖZLŐ- ÉS -MULTIMÉDIÁS RENDSZEREK KÖZÉP ÉS HOSSZÚ TÁVÚ FEJLŐDÉSI TENDENCIÁI, ÉS VÁRHATÓAN MEGJELENŐ RENDSZEREI ÉS SZOLGÁLTATÁSAI

Dr. Dárdai Árpád, távközlési szakértő
06 1 322-1575, 06 20 9322-143, dardai.arpad@t-online.hu

Absztrakt

Az előadás a mobil távközlés közép, ill., hosszú távú fejlesztési koncepcióit ismerteti. Ilyenek az FMC, az UMA-GAN, a Femtocell, az UMB, az NGN, az UWB, NFC, az LTE-SAE, az OFDM-MIMO, a HSOPA és hasonló, ill., más fejlett koncepciók és elképzelések, törekvések, ill., rendszerek, amelyek a PSTN-PLMN/ISDN/IN, az IMS, az Internet-Intranet, a VoIP, a VoLAN-VoWLAN, VoD, továbbá a többszolgálatú (triple/guad-play) rendszerek és teljesen IP alapú alkalmazások egyre fejlettebb megvalósulásait szolgálják és eredményezik, egyre gazdaságosabban, egyre jobb rendszer- és készülék-, és szolgáltatás technikával.

Rövid összefoglaló

Az elmúlt években számos fejlett, új mobil távközlési, -informatikai és multimédiás mobil távközlő rendszer jelent meg, mind a megvalósítás terén, mind a közép és hosszú távú tervek, célkitűzések és fejlesztések tekintetében.

A teljesség igénye nélkül, a jelenlegi megvalósítások között említhetők a sokoldalú képességekkel rendelkező 3G-UMTS mobil távközlő rendszerek, továbbá az ezekhez csatlakozó, ezeket kiegészítő, ill., az ezeknek a platformján létesülő, és a korábbiaknál fejlettebb adatátviteli-informatikai képességekkel rendelkező újabb Bluetooth-verziók, az IEEE 802.11/b,g szabvány családba tartozó WiFi, a IEEE 802.16 szabványú fix és mobil WiMAX, ill., a megfelelő több módusú, több sávú mobil készülékek, a PDA-k, a laptop- és notesz PC gépek és a 3G-UMTS rendszerre alapuló HSPA (HSDPA, HSUPA) nagy sebességű gyomagkapcsolt adatátviteli eljárás, továbbá a szintén a 3G-UMTS rendszerekre és fejlett, nagy integráltságú mobil készüléktechnikákra alapuló DVB-H eljárások és szolgáltatások.

A folyamatos fejlődés eredményeképpen – a 3GPP és más nemzetközi távközlési szabványosító testületek munkája keretében – újabb és további koncepciók, irányzatok és rendszerek is megjelentek és megjelennek a mobil távközlés, -informatika és -multimédia folyamatosan bővülő területein. Ilyenek az FMC, az UMA-GAN, a Femtocell, az UWB, az LTE-SAE (az előfizetői rádiós szakaszok és a maghálózatok architektúrájának párhuzamos fejlesztései), az OFDM-MIMO, a HSOPA és hasonló, ill., más fejlett koncepciók és elképzelések, törekvések, ill., rendszerek, amelyek végül is a PSTN-PLMN/ISDN/IN, az IMS, az Internet-Intranet, a VoIP, a VoLAN-VoWLAN, VoD, továbbá a „háromszoros-négyszeres játszást" (triple/guad-play), vagyis a többszolgáltatású rendszereket lehetővé tevő, és a teljesen IP alapú alkalmazások egyre fejlettebb megvalósulásait szolgálják és

eredményezik, egyre gazdaságosabban, egyre jobb rendszer- és készüléktechnikával, így például a szoftverrádiók egyre szélesebb körű alkalmazásával, valamint egyre teljesebb területi és felhasználói lefedéssel. Az előadásban a fentiek áttekintése történik.

1. Bevezetés

A vezetékes beszéd célú távközlés jelentős fejlődést jelentett a 20. század elején, sok-sok változást hozva a gazdasági életben és a mindennapokban. A 20. század utolsó évtizedeiben megjelenő és egyre inkább elterjedő vezetéknélküli és mobil távközlés a változásokat tovább gyorsította és számos további újszerű lehetőséget teremtett meg a gazdaság, a közigazgatás, a veszélyhelyzeti készenléti szervek és a mindennapok embere számára egyaránt.

A vezetékes- és vezetéknélküli távközlés fejlődésével párhuzamosan, a 20. század utolsó évtizedeiben, szinte versengően, megjelent az Internet, amely egyre nagyobb hangsúlyt és fontosságot kapott és a távközlés egyre nagyobb és nagyobb részein kezdték alkalmazni. Az Internet egyre nagyobb arányú alkalmazásában élenjártak a mobil rendszerek. Az Internet, ill., az Internet Protokoll, a fix- és mobil távközlési, a számítástechnikai, informatikai és multimédiás felhasználások mellett egyre jobban alkalmazást nyert a mindennapokban is, és az utóbbi években egyre inkább megváltoztatta a mindennapokat, sőt, sok esetben akár az emberek életstílusát is.

A 20-21. század fordulóján, ill., az azt követő években a vezetékes és a vezetéknélküli távközlésben megjelentek és egyre jobban elterjedtek a szélessávú megoldások. Az elmúlt években számos fejlett, új mobil távközlési, -informatikai és multimédiás mobil távközlő rendszer jelent meg, mind a megvalósítás terén, mind a közép és hosszú távú tervek, célkitűzések és fejlesztések tekintetében.

A – teljesség igénye nélkül – jelenlegi megvalósítások között említhetők a sokoldalú képességekkel rendelkező (FDD, TDD) 2G-GSM, ill., a 3G-UMTS mobil távközlő rendszerek, továbbá az ezekhez csatlakozó, ezeket kiegészítő, ill., az ezeknek a platformján létesülő, és a korábbiaknál fejlettebb adatátviteli-informatikai képességekkel rendelkező újabb Bluetooth-verziók, az IEEE 802.11/b,g szabvány családba tartozó WLAN, ill., WiFi, (UMA az ISM sávokban), az IEEE 802.16d szabványú fix WiMAX (FDD), az IEEE 802.16e szabványú mobil WiMAX (a TDD 2,5, ill., 3,5 GHz-es sávokban), ill., a megfelelő több módusú, több sávú mobil készülékek, a PDA-k, a laptop- és notesz PC gépek és a 3G-UMTS rendszerre alapuló kezdeti (örökség) EDGE, ill., a tovább fejlesztett EDGE-E (Evolution), a 3GPP HSPA (HSDPA, HSUPA) nagy sebességű gyomagkapcsolt adatátviteli eljárás, továbbá a szintén a 3G-UMTS rendszerekre és fejlett, nagy integráltságú mobil készüléktechnikákra alapuló DVB-H eljárások és szolgáltatások.

A folyamatos fejlődés eredményeképpen – a 3GPP és más nemzetközi távközlési szabványosító testületek munkája keretében – újabb és további koncepciók, irányzatok és rendszerek is megjelentek és megjelennek a mobil távközlés, -informatika és -multimédia folyamatosan bővülő területein.

2. Közép és hosszú távú fejlődési tendenciák és megjelenő hatékony mobil távközlő rendszerek áttekintése

Vezetéknélküli távközlési tendenciák és technológiák. A mobil és a vezetéknélküli távközlő rendszerek és szolgáltatások nemzetközi távközlési és szabványosítási szervezetek irányítása és szervezése keretében fejlődik. Ilyen testületek a 3GPP, az ITU, és az ETSI. A 3GPP (3rd Generation Partnership Project - 3GPP), maga is együttműködő távközlési szabványszervezetekből és a távközlési piac jelentős képviselőiből, mint tagokból áll. A szervezet tagjai az ARIB, CCSA, ETSI, ATIS, TTA, TTC. A 3GPP célja, hogy a 3G (4G) mobil távközlő rendszerek műszaki és szolgáltatási specifikációit kidolgozzák, karbantartsák, fejlesszék, összhangban az ITU IMT-2000 (International Mobile Telecommunications-2000) rendszerrel. A 3GPP előírások és specifikációk a GSM (Global System for Mobile Communications) előírásokat és szabványokat messzemenően figyelembe veszik a későbbi szabványok kidolgozásánál.

A 3GPP és az említett nemzetközi szabványosító szervezetek több évtizedes összehangolt munka keretében közép, ill., hosszú távú fejlesztési koncepciókat és vezetéknélküli technológiákat határoztak meg, amelyek elősegítik a megfelelő távközlési tendenciákat és a fejlett távközlési technológiák kialakulását, bevezetését és elterjedését. Ilyenek az FMC, az UMA-GAN, a Femtocell, az UWB, az NFC, az LTE-SAE, az OFDM-MIMO, a HSOPA és hasonló, ill., más fejlett koncepciók és elképzelések, törekvések, ill., rendszerek, amelyek végül is a PSTN-PLMN/ISDN/IN, az IMS, az Internet-Intranet, a VoIP, a VoLAN-VoWLAN, VoD, továbbá a „háromszoros-négyszeres játszást" (triple/guad-play) lehetővé tevő, vagyis a többszolgáltatású rendszerek egyre fejlettebb változatait és megvalósulásait szolgálják. A többszolgáltatású (triple/guad-play) rendszerek a hagyományos beszéd célú távközlést, az adatszolgáltatásokat és a nagysebességű internet hozzáférést, valamint a különféle fejlett alkalmazásokat és a multimédiás szórakoztató szolgáltatásokat teszik egyidejűleg lehetővé.

Mindezek a teljesen IP alapú alkalmazások bevezetését is feltételezik és segítik, egyben eredményezik, és egyre gazdaságosabb, és egyre jobb rendszer- és készüléktechnikát is magukkal hoznak. Ezt segítik és szolgálják például a szoftverrádiók egyre szélesebb körű alkalmazása, valamint távközlő- és multimédiás rendszerek és -szolgáltatások iránti igények egyre teljesebb területi és felhasználói lefedése.

Előfizetői megoldások. A sokoldalú képességekkel rendelkező, engedélyköteles frekvenciasávokban működő (FDMA/TDMA, FDD/TDD technikákat használó) 2G-GSM, 3G-UMTS mobil távközlő rendszerek, továbbá az ezekhez csatlakozó, ezeket kiegészítő, ill., az ezeknek a platformján létesülő és a korábbiaknál fejlettebb adatátviteli-informatikai képességekkel rendelkező további távközlő rendszerek alakultak ki az elmúlt évtizedekben. Ilyenek a nem frekvencia engedély köteles WLAN rendszerek és alkalmazások, vagyis az UMA (Unlicenced Mobile Acess), aminek igen elterjedt példája az IEEE 802.11/b,g szabvány családba tartozó WiFi (2,4 GHz-es ISM sáv), tovbbá az egyre fejlettebb Bluetooth-verziók és az egyre inkább elterjedő NFC (Near Field Communication), az UWB (Ultra Wide Band), ill., a Femtocell (mikro-, pico-, femtocellás) kategóriájú és hatókörzetű távközlés.

A frekvenciaengedély köteles megoldások is tovább fejlődtek, ilyen az IEEE 802.16e szabványú mobil WiMAX (TDD technika a 2,5 GHz-es és a 3,5 GHz-es

sávokban), ill., a megfelelő több módusú, több sávú multimédiás szolgáltatásokra képes mobil telefonkészülékek, továbbá a mobil telefonálásra is alkalmas PDA-k. Egyre szélesebb körben bevezetésre került, mind az asztali, a laptop- és notesz PC gépekhez, mind a 3G-UMTS rendszerre és készülék technikára alapuló és ezekhez is csatlakoztatható, ill., ezekbe is beépített HSPA (HSDPA, HSUPA) nagy sebességű csomagkapcsolt adatátviteli eljárás és modemek is. Szintén a 3G-UMTS rendszerekre és fejlett, nagy integráltságú mobil készüléktechnikákra alapulóan egyre több országban és szolgáltatónál alkalmazzák és bevezették, ill., bevezetik a DVB-H szabványokat és eljárásokat, valamint más, a mobil rendszerekre alkalmazható szélessávú multimédiás rendszereket, így a MBS (Mobile Broadband Services) megoldásokat és szolgáltatásokat is.

Az előfizetői szintű és a mobil vagy állandóhelyű (fix) előfizetői végfelhasználói készülékeket a maghálózathoz és a tartalom, ill., alkalmazói kiszolgálókhoz kapcsoló hozzáférési hálózatok megoldásai sorában számos megoldást említhetünk: rádiós előfizetői szakaszok, különféle rézvezetős (xDSL technikák) és üvegszálas (FTTx) előfizetői megoldások (first mile), forgalom- és szolgáltatás koncentráló és elosztó technikák (second mile) és csomópontok (DSLAM egységek, bázisállomások (rádió interfész), nyalábolók, koncentrátorok), amelyek biztosítják a kívánt sávszélességet és forgalmi minőséget, továbbá a szétosztják és hozzáférhetővé teszik a kívánt szolgáltatásokat és alkalmazásokat az előfizetői szakaszok és az egyes előfizetők számára.

A hozzáférési hálózatok magukba foglalják az előfizetői szakaszok számos hozzáférési csomópontjait, amelyeket forgalmilag, csatlakozásilag egyesítenek, nyalábolnak és a maghálózathoz kapcsolják. A hozzáférési csomópontok egyesítése, nyalábolása, csatlakoztatása különféle technikákkal oldható meg. A korszerű megoldások Ethernet-protokoll segítségével működnek és üvegszálas átviteli eszközöket használnak, amíg a hagyományos nyaláboló és elosztó megoldások ATM technikát és TDM alapú SDH átvitelt, és többszolgáltatású rendszereket kiszolgálni képes hálózatokat, valamint vezetéknélküli mikrohullámú rádiós technikákat használnak. A koncentráló-nyaláboló hálózatoknak teljesíteni kell a szolgáltatások szintjeire vonatkozó nemzeti és nemzetközi szabványokat és előírásokat (megbízhatóság, rendelkezésre állóság), és támogatniuk kell a különféle szolgáltatás minőségszinteket és -osztályokat (QoS, GoS).

A szolgálatok és szolgáltatások fejlődésével, gazdagodásával párhuzamosan nőtt a sávszélesség igény és nőttek az átviteli minőséggel szemben támasztott elvárások. Megjelentek és elterjedőben vannak a HDTV eljárások, a minőségi videó távközlés, és az új szórakoztató szolgáltatások, mint a „távolsági" játékok, a virtuális világ-játékok, virtuális partnerekkel. Az üzleti előfizetők számára fejlett VPN szolgáltatások váltak hozzáférhetővé megállapodásos differenciált szolgáltatás szintekkel, videokonferencia szolgáltatásokkal, és a vállalati, társasági helyi hálózatok (LAN) szervereinek, a közöttük lévő kapcsolatok támogatásával.

A felhasználók és előfizetők egyre nagyobb hányada, egyre nagyobb arányban kívánja használni a mobil technikákat, és azt is elvárják, hogy az eddig a vezetékes technikákkal használt szolgáltatások a mobil rendszerekkel is hozzáférhetők legyenek. A szolgáltatók számára egyre fontosabb az előfizetők megtartása, a beruházási és üzemeltetési költségeik optimalizálása, amiket rendszerük minél jobb, költség-

hatékonyabb kihasználásával, ugyanakkor rendszerük, hálózatuk és távközlési, valamint tartalom szolgáltatásaik állandó fejlesztésével érhetnek el. Mobilitás és sávszélesség egyre fontosabb kulcskérdésekké váltak. Egyre jelentősebbé, fontosabbá vált az előfizetők és a maghálózat közötti szakasz, a rádiós hozzáférési szakasz, a rádiós interfész.

A mobil technika és a mobil rendszerek hálózati, valamint előfizetői és hozzáférési szakaszai termékenyen, gyümölcsözően, sokoldalúan és meglehetősen gyorsan - nem egyszer újító és újszerű módon - magukba integrálták távközlési (IN/ISDN) hálózati tulajdonságokat és szolgáltatásokat, és a különböző vezetéknélküli szélessávú előfizetői szintű és a hozzáférési megoldásokat, amelyeknek hozzáférési rendszereit gyűjtő néven vezetéknélküli szélessávú hozzáférési (WBA – Wireless Broadband Access) megoldásoknak, hálózatoknak nevezhetjük.

3. A fejlődési tendenciák és a kialakult rendszerek, szabványok áttekintése

Vezetéknélküli technológiák. A távközlési szolgáltatók számára igen nagy értéket képviselnek az engedélyezett frekvenciák és frekvenciasávok. Mind az alacsonyabb, mind a magasabb frekvenciasávok értékesek. Az alacsonyabb sávok ellátási körzetei nagyobbak (nagyobb cellák), ugyanakkor a kapacitásuk kisebb, a magasabb sávok ellátási körzetei kisebbek (kisebb cellák), de az átvitel sávszélessége és így kapacitásuk nagyobb. Értéknek számít, ha egy szolgáltatónak minél szélesebb sávok állnak rendelkezésére.

A frekvencia párokból álló készletet rendszerint az FDD üzemmódhoz használják, ami a jelenlegi frekvencia készletek és használatok tetemes részét képezi. A TDD frekvenciahasználat a 2,5 és a 3,5 GHz-es sávokban szokásos, ami azt jelenti, hogy a bázisállomás felé (uplink) és az onnan érkező (downlink) jelek azonos sávban vannak.

A GSM-UMTS mobil szolgáltatók számára szükséges egy olyan szélessávú technika is, ami az FDD sávokban is használható és ott is működik. Ilyen a HSDPA, ill., HSUPA, gyűjtő nevükön HSPA, és ennek az LTE (Long Term Evolution) irányába fejlődő változata, továbbá a fix WiMAX (IEEE 802,16d), amely szintén az egyik lehetséges FDD technika a 3,5 GHz-es frekvenciasávokban, ill., a TDD mobil WiMAX a 2,5, ill., a 3,5 GHz-es sávokban.

Igen fontos a vezetéknélküli technikáknál – az alkalmazott frekvenciasávtól függően - az ellátási körzet nagysága, mert ez alapvetően befolyásolja a szükséges bázisállomások számát és ez által a hálózat létesítési-, és nagyban az üzemeltetési költségeit (CAPEX, OPEX) is. A költségek mellett azonban a mindez kihatással van az épületen belüli ellátottság minőségére is, ami a mobil szolgáltatók és az előfizetők számára egyaránt alapvetően fontos. Az épületen belüli ellátottság alapvetően függ az épületcsillapítástól és az alkalmazott frekvenciasávtól. E tekintetben az alacsonyabb sávok kedvezőbbek, ugyanakkor az alacsonyabb sávok átviteli kapacitása kisebb. Célszerű ezért egyazon területen az alacsonyabb és a magasabb sávok alkalmazását kombinálni, ami a mobil szolgáltatók egyre inkább gyakori módszere is.

3GPP szélessávú vezetéknélküli hozzáférési technikák. Ezek sorában az EDGE-E, a HSPA és variánsai, valamint az LTE technológiák a legfontosabbak. A HSDPA technológia rádióinterfésze valódi szélessávú hozzáférést tesz lehetővé

előfizetőnként 1 Mbit/s-os sebességnél nagyobb átviteli sebességgel, és előfizetőnként legalább 1 GByte/hónap letölthető adatmennyiséget, ami mind az előfizetők, mind a szolgáltatók számára elfogadható mennyiségek. Az UMTS szolgáltatók legtöbbje hálózatát fejlesztette, alkalmassá tette arra, hogy 3,6 Mbit/s és 7,2 Mbit/s közötti letöltési (downlink) átviteli sebességekkel hálózatát üzemeltethesse. A feltöltési átviteli adatsebesség (uplink) 2 Mbit/s-os értékét a HSUPA (High Speed Upload Packet Access) szabvány biztosítja. Ez az átviteli sebesség érték 2007-től vált hozzáférhetővé.

A HSDPA eljárás kedvező mind a beszédátvitel, mind a jelzésátvitel tekintetében. A technikai fejlődés lehetővé tette, hogy a HSDPA eljárás 14,4 Mbit/s-os (3GPP Szabvány Release 5, röviden 3GPP R5), és a HSUPA eljárás pedig 5,76 Mbit/s-os (3GPP R6) átviteli sebességekre is alkalmas legyen. További fejlesztéseket is kitűztek és megvalósítanak a HSPA eljárásokban (3GPP R7), amelyek keretében javították a rádiótechnikai jellemzőket, így javultak a válaszidők (látencia), tovább nőttek az adatátviteli sebességek, javult a spektrum hatékonyság, és csökkent a készülékek teljesítmény igénye, ill., javult a felvett teljesítmény felhasználása, továbbá a felhasználók számára tovább javult a HSPA szolgáltatás teljesítőképessége.

Ezeket a javításokat, amelyeket az R7 irányozott elő, gyűjtő néven HSPA+ névvel is jelölik, amelyek keretében a HSPDA esetére 28,8 Mbit/s-os, HSUPA esetére 11,5 Mbit/s-os (R7), ill., a 43,2 Mbit/s-os (R8) adatátviteli sebességet, és a legfeljebb 30 ms-os válaszidőt (látenciát) irányoztak elő és értek el, ugyanakkor, az R7 keretében a technológiát alkalmassá tették arra, ill., a szükséges fejlesztési lépéseket megtették abba az irányba, hogy a HSPA eljárás tulajdonságai a 3GPP LTE (Long Term Evolution) végfelhasználói szabvány követelményei szerint alakuljanak. Ezt nagyrészt költséghatékony szoftverek kifejlesztésével célszerű elérni, és így is tervezik kialakítani.

Az LTE keretében egyébként 160 Mbit/s-os csúcs adatátviteli letöltési sebességet tűztek ki célul (3GPP R8), 10 ms-nál kisebb látenciával. Az LTE technológiát az R8 keretében tovább fejlesztik. Fontosabb célok: rugalmas frekvencia spektrum használat, a frekvenciák és a sávszélességek variálása, kombinálása a felhasználók alkalmazásai függvényében, hatékony teljesítmény szabályozás kezelés a felhasználói rádiós terminálóknál, az ellátott területek kialakításánál, lefedésénél az egyidejű nagy- és a kiscellás szerkezetű működés és hálózat szerkezet kombinálása, az adatátviteli igények szerinti választása, kiscellás eljárásokkal kombinált hatékony antenna nyaláb formálás adaptív eljárásokkal, amelyekkel javul a spektrum hatékonyság, csökkennek az interferenciális zavartatások és javul a hálózat rádiótechnikai tervezhetősége. Ezekkel a módszerekkel az egyes antenna szektorokban akár 40 Mbit/s-os adatátviteli sebesség is elérhető, ami, pl., 20 MHz-es szolgáltatói sávszélességgel, 1-2 bit/s/Hz értéket képviselhet antenna nyalábonként.

Fontos törekvésként jelenik meg az is, hogy az adatátviteli sebességek jelentős növekedése mellett, a versenyképesség érdekében az előfizetői adatátviteli költségek csökkenjenek, továbbá, hogy a hálózat kialakítása a későbbi követelményekkel kompatibilis, és üzemeltetése minél gazdaságosabb legyen, valamint a tarifálás legyen egyszerűbb. Az R7 szerinti hálózat architektúra olyan, amilyen az LTE

számára is szükséges, de az LTE rendszerrel kompatibilis kialakítású volt már az R5 szerinti HSDPA hálózat architektúra is.

Megemlítendők még az EDGE (Enhanced Data Rates for GSM Evolution) eljárásra vonatkozó fejlesztési törekvések (EDGE-E, EDGE Evolution, 3GPP R7) is. Ezek szerint az EDGE átviteli sebességét 1,4 Mbit/s-os értékre növelik. Az EDGE alkalmazások szerepe hasznos azokban az esetekben, amelyeknél mobil hálózatot a HSPA, ill., a WiMAX megoldásosokkal még nem egészítették ki. A hagyományos, GSM alapú EDGE hálózatrészek könnyen kiegészíthetők és tovább fejleszthetők az EDGE-E megoldással. Az EDGE, mint megfelelő, globális roamingra képes megoldás, jól támogatja és elősegíti az adatátviteli sebességek növelését, az adatátviteli ellátottság javítását, az adatátviteli alkalmazások fejlesztését, bővítését, és a HSPA technológia felé történő fejlődést. A meglévő GSM BSS egységeken megfelelő szoftver cserékkel az EDGE-E megoldások eredményesen használhatók.

WiMAX, az IEEE 802.16 szabvány szerinti szélessávú hozzáférés. A WiMAX (Wordwide Interoperability for Microwave Access) rendszernek a fejlődés során, célszerűen két változata alakult ki: a fix WiMAX, a 802.16d szabvány szerinti, és mobil WiMAX, a 802.16e szerinti.

A fix WiMAX (802.16d) hozzáférési megoldás a vezetékes ADSL alternatívája vezetéknélküli technikával. A fix WiMAX FDD üzemmóddal működik, a 3,5 GHz-es frekvenciasávban.

A mobil WiMAX (802.16e) TDD üzemmódot használ, és állandóhelyű, változóhelyű és mobil állomások számára nyújthat hozzáférési megoldást, és a 2,3, a 2,5 és a 3,5 GHz-es sávokban működhet. Az RF vivők sávszélessége (csatornaosztás) 5-10 MHz közötti lehet, amit később 20 MHz-re terjeszthetnek ki. A mobil WiMAX csúcs adatátviteli sebessége 10 MHz-es csatorna osztás esetén 40 Mbit/s, és 20 MHz-es csatorna osztás esetén max. 80 Mbit/s lehet. A mobil WiMAX egy perspektivikus, szabványos szélessávú átviteli eljárás, széles nemzetközi szabványosítási és gyártói támogatottsággal mobil szélessávú célokra, gazdaságos műszaki megoldással. A fix WiMAX-ból kialakult mobil WiMAX gazdaságossági és célszerűségi okok miatt gyakran fix célokra is alkalmazásra kerül.

A WiMAX technológia szabványos kialakítása következtében az egyes gyártók szabványokat követő termékei egymással jól együttműködnek.

Egyéb vezetéknélküli szélessávú hozzáférési technikák. A HSPA és a kapcsolódó, valamint a WiMAX technológiák mellett egyéb vezetéknélküli hozzáférési megoldások is kialakultak. Ilyenek a 3GPP R4-ben definiált TDD TD-SCDMA és az FDD Flash-OFDM. A TD-SCDMA alacsony chip-sebességgel és keskenysávú TDD üzemmóddal működik, amíg a Flash-OFDM megoldás szélessávú célokra nagycellás frekvencia használattal és FDD üzemmóddal üzemel, gazdaságos kialakítással. Egyik alkalmazási területe a WiFi forrópontok (hotspots) hozzáférési hálózataként szokásos, buszokon, vonatokon, pályaudvarokon való WiFi alkalmazásokhoz.

A WiFi alkalmazás egyre jobban megtalálható az asztali-, a hordozható-, ill., a notesz PC számítógépeken, valamint a PDA készülékeken és a mobil telefonokon is. Napjaink WiFi eszközei a 802.11b,g szabványait követik (10, ill., 54 Mbit/s-ig), de a fejlesztések nyomán várható a 802.11n szabvány szerinti (200 Mbit/s-ig vagy még nagyobb adatátviteli sebességre alkalmas) eszközök megjelenése is.

A WiFi gyakori beltéri, épületen belüli alkalmazása mellett, alkalmazható kültéri helyeken, mint például forgalmas városi körzetekben (éttermek, szállodák, repülőterek, pályaudvarok, stb.) is. A WiFi rendszerekkel javítható a rádiós ellátottság, segítségükkel cellás lefedések is megvalósíthatók. A WiFi rendszerekhez a csatlakozó hozzáférési hálózatok és azok csatlakozása a kívánt gyűjtő, ill., magasabb szintű hálózatrészekhez gazdaságosan megvalósíthatók.

A WiFi a nem engedélyköteles 2,4 GHz-es és az 5,4 GHz-es ISM frekvenciasávokban működik, ezért zavartatások más készülékektől előfordulhatnak, azonban ezek a WiFi használhatóságát, előnyeit általában nem kisebbítik.

Mobil és hordozható rádiós terminálok. A vezetéknélküli technika rohamos fejlődése következtében egyre teljesebb, komplettebb és kompaktabb megoldásokat, sokoldalú készülék és szolgáltatás csomagok széles választékát kínálják a gyártók a vég-vég felhasználók, ill., felhasználások számára, egyre kedvezőbb árviszonyok mellett. A mobil készülékek és a hordozható készülékek (PDA-k, PNA-k, laptop-, notebook-, tablet PC-k) által kínált megoldások egyre inkább magukba foglalják a WiFi, a HSPA, és várhatóan hamarosan a WiMAX, majd az LTE technológiákat is. A megoldásokat fejlett antenna- és vevőtechnikák is segítik, ilyenek pl., a különféle adaptív antennák, antenna rendszerek és a MIMO vételtechnikai megoldások, amelyek az OFDM alapú WiMAX, HSPA és az LTE technológiák és fejlesztéseik fontos részei.

A hozzáférési hálózatok kapcsolódásának fejlesztése vezetéknélküli technikákkal. A rádiós rendszerek bázisállomásainak kapcsolódását a hálózhoz az 1G és a 2G rádiótelefon hálózatoknál TDM E1/T1 összeköttetésekkel oldották meg. Ezek adatátviteli sebessége azonban már lassú a 2,5G és különösen lassú, és ezért nem megfelelő a 3G, 4G hálózatokban. Ezért mind a letöltési, mind a feltöltési (downlink/uplink) irányokban nagyobb átviteli sebességű, nagyobb kapacitású megoldásokat kellett keresni.

A céloknak és a feladatoknak megfelelő megoldásokra mind vezetékes, mind vezetéknélküli technikák találhatók. A növekvő átviteli sebességek sorrendjében felsorolt vezetéknélküli eljárások: EDGE, EDGE-E (evolution), HSPA, WiMAX, LTE (160 Mbit/s-ig). A szintén a növekvő átviteli sebességek sorrendjében felsorolt vezetékes technikák, áttekintő jelleggel: ADSL, E1/T1, ADSL2, VDSL2, PON/GPON, Ethernet (8-9 Gbit/s-ig). A vezetékes és a vezetéknélküli megoldások az adott esetek és körülmények szerint kombinálhatók.

A hozzáférési hálózatrészek adatátviteli igényei gazdaságosan jól kiszolgálhatók mikrohullámú összeköttetésekkel is olyan esetekben, amelyeknél a vezetékes megoldások nincsenek kiépítve, vagy létesítésük gazdaságtalan lenne, vagy a földrajzi viszonyok miatt az összeköttetések létesítése rádiós (mikrohullámú) megoldással előnyösebb, kivitelezhetőbb.

A vezetékes megoldásokhoz megjegyezhető, hogy jelenleg még nagyabb átviteli sebességeket nyújthatnak, mint a rádiós megoldások, a jelenlegi (és a várható) vezetéknélküli technikák nagyfokú fejlődése mellett is. Így a vezetékes (üvegszálas) technikákkal jól kiszolgálhatók az IPTV, a HDTV, a szélessávú csomagkapcsolt hálózatok és az utóbbira alapozott, üzleti célú VPN (VPN, MPLS …) hálózatok, valamint a különféle fájlmegosztó szolgáltatások.

A szolgáltatók törekednek arra, hogy a meglévő rézvezetékeket, különösebb beruházások nélkül, a különféle xDSL technikákkal minél tovább és minél jobban hasznosítsák, bár az optikai megoldások gazdaságosabbá válásával, a rézvezetők alkalmazásának előbb-utóbb egyre erősebb versenytársai lesznek a különféle üvegszálas FTTx megoldások, a rezet és használatukat mindinkább visszaszorítva, alkalmazási területüket csökkentve. Másrészt, a rézvezetők xDSL jellegű felhasználásának egyre erősebb versenytársát jelentik a különféle rádiós megoldások is (WiFi, HSPA, WiMAX, LTE), amelyek adatátviteli sebessége az utóbbi években a fejlett rádiós technikáknak (OFDM változatai és kombinációi) köszönhetően jelentősen nőtt és tovább nő.

FMC - Fix Mobil Konvergencia. A mobil és az állandóhelyű (fix) távközlés, ill., távközlési ágazatok és szakterületek fejlődése a kezdeti években egymástól, legalábbis látszólag, sok tekintetben, közel függetlenül történt. A két szakterület az elmúlt évtizedekben az adott kor és fejlődési szakasz igényei és sajátosságai szerint alakult. Jellemzően, az ágazatok, ill., a szakterületek és az alkalmazott technikák látszólagos függetlensége miatt csak viszonylag kevéssé hatottak egymásra. A távközlés fejlődése során, kezdetben, ill., a most tekintett időszakban (1950-1990-es években), a vezetékes távközlés és előírásai, szabványai voltak az inkább mérvadók, és a jobban, alaposabban kidolgozottabbak. Bár a vezetéknélküli távközlés megjelenésétől és egyre nagyobb arányú elterjedésétől (1950-es évektől) kezdve alapvetően fontos volt a mindennapok számos területén, a polgári és a nem polgári alkalmazásokban, miközben a vezetéknélküli távközlés rohamosan fejlődött, legalábbis az előfizetők szempontjából, egyre vonzóbb és jobb megoldások alakultak ki. Elegendő az IN/ISDN jellegű és tulajdonságú GSM rendszerek, hálózatok és szolgáltatások sikerére gondolni.

Az időközben egyre fontosabbá és általánosabbá váló IP technikát is, a mobil technika példamutatóan egyre jobban alkalmazta. Kialakult a teljesen IP alapú (all IP) hálózat koncepciója, és ez a 3G, 4G rendszerekben egyre inkább megvalósul. Kialakultak a szélessávú képességekkel rendelkező hálózatok, amelyek IP alapon továbbították az adatokat. A fejlődési tendenciák szerint, mind a hozzáférési szakaszon, mint a gyűjtő, továbbító szakaszon, mind a gerinchálózati szakaszon egyre inkább az IP alapú átvitel használatos, ill., egyre inkább ennek alkalmazása várható (all IP). Kialakult az IMS (IP Multimedia Subsystem), IP alapú multimédiás alrendszer elgondolása és szabványa, amely a multimédiás szolgáltatások egységes IP alapú működtetését teszi lehetővé. Megjelentek olyan törekvések és megoldások, amelyeknél a beszéd, az adatátvitel és hozzáférés, valamint a multimédia, sőt, bizonyos játékok és hozzáférésük, egyazon hálózat keretében kerülnek átvitelre, szolgáltatásra, és hozzáférésre (triple/quad play, többszolgáltatású hálózatok).

A szabványosító testületek (3GPP) kialakították az NGN (Next Generation Network), a következő generációs hálózatok koncepcióját és szabványi előírásait, amelyek keretében az addigi elkülönült fix vezetékes és a mobil hálózatok felépítése, szerkezete, megoldásai, szolgáltatásai, működése és működtetése hasonlók, ill., azonosak, vagyis kialakult a FMC (Fixed-Mobile Convergence).

A felhasználó szempontjából az FMC azt eredményezi, hogy az előfizetői készülékek és a készülékekkel, ill., a hálózatokkal hozzáférhető szolgáltatások azonosak, ill., igen hasonlóak a fix és a mobil hálózatokban egyaránt. Akár egy mobil

hálózat, akár egy fix hálózat, vagy akár egy WLAN hálózat előfizetői készülékével, ill., egy mobil (ill., fix) hálózat WLAN képes mobil (fix) előfizetői készülékével, vagyis bármilyen hálózat bármilyen készülékével azonos, IP alapú szolgáltatásokat (VoIP) lehet, ill., lehessen elérni.

A WLAN hálózaton a WLAN képes mobil készülékekkel hozzáférhető VoIP beszédszolgáltatás az UMA (Unlicensed Mobile Access, hozzáférés az ISM sávokban) elgondolás és szabvány, és az IMS alapú VCC (Voice Call Continuity) segítségével valósul meg.

Az FMC koncepció keretében egyre jobban elterjed az asztali, a laptop és a notesz PC számítógépek és más személyi informatikai, ill., multimédiás (mobil készülékek, PDA, PNA, stb.) készülékek beszédcélú, szélessávú és multimédiás alkalmazása is a hivatalokban és az otthonokban, amit a megfelelő beltéri, ill., épületen belüli rádiós ellátás tesz lehetővé. A kívánt ellátottságot épületen belüli femtocellás eszközökkel lehet biztosítani. A személyi eszközök alkalmazását tovább segít az, hogy ezekben a készülékekben (PDA, Laptop, stb.), vagyis a mobil terminálokban, egyre nagyobb arányban helyeznek el 3G-s, később 3,5G-s, 4G-s adóvevőket, RF modemeket. Mindezek az alkalmazásfejlesztések, bővítések, a kültéri 3G, 4G ellátottságot, a szolgáltatások hozzáférhetőségét, minőségét nem csökkentik, ugyanakkor a felhasználók számára a szolgáltatás hozzáférési lehetőségeket lényegesen bővítik.

4. A 3GPP együttműködés LTE szabványa.

A 3G-UMTS rendszerhez kapcsolódó HSPA, WiMAX, ill., más nagy adatátviteli sebességű eljárás a 3GPP (amely a távközlési szabványosítási szervezetek és vezető piaci tényezők együttműködése) és fejlesztési koncepciója keretében az LTE irányába fejlődik.

Mi is az LTE? Az LTE (Long Term Evolution) koncepciót és szabványt a 3GPP dolgozta ki a versengő technológiák és szabványok nyomán és hatására. Az LTE egy a meglévő mobil eljárásoknál és szabványoknál, mint a GSM, EDGE, HSPA, W-CDMA, fejlettebb, hatékonyabb technológia lesz. Az LTE szintén különböző fejlődési szinteket és fázisokat képvisel.

A hosszú távú fejlődés szempontjából a 3GPP fejlesztési tevékenységével szemben követelményként merült fel az, hogy a mobil rendszerek fejlesztésénél a nagyobb adatátviteli sebességekre és az új multimédiás szolgáltatások támogatására vonatkozó végfelhasználói követelményeket fokozottan vegyék figyelembe, valamint a kifejlesztésre kerülő új koncepció és új rendszer a már kialakuló és versengő, más nagy adatátviteli sebességet teljesíteni képes technológiáknál (WiMAX, HSPA) még jobb legyen. A folyamatosan növekvő végfelhasználói követelmények kiszolgálására, és a 3G rendszer versenyképességének megtartása érdekében, a 3GPP testület 2004. novemberében fogalmazta meg és kezdeményezte a 3G mobil rendszerek hosszú távú fejlesztésének (LTE - Long Term Evolution) koncepcióját.

2008. áprilisában a 3GPP újabb tervet fogadott el az LTE kidolgozásának jövőbeni munkáira vonatkozóan, amelyet az ITU tevékenysége keretében is figyelembe vesznek. Ennek a tervnek az LTE-Advanced nevet adták, amelynek követelményeit a 3GPP által kiadott TR 36.913 Műszaki Jelentés (Requirements for LTE-

Advanced, TR Technical Report) tartalmaz. A 3GPP célja az LTE szabványrendszerrel és továbbfejlesztésével, a 3G-4G rendszerek versenyképességét továbbra is megtartani. Az eredeti célkitűzések szerint az LTE szabvány befejezését 2007-re tervezték, ez lényegében teljesült is, azonban, a fentiek szerint, továbbfejlesztések az LTE területén is történnek. Szabványtestületek, gyártók, piaci tényezők széles köre támogatja az LTE termékek kifejlesztését és gyártását.

Az LTE felé történő fejlődés néhány főbb tulajdonsága:

- megnövelt hálózatkapacitás és átvitt adatmennyiség,
- 3GPP Release 6 HSPA átvitelhez képest 3-4-szer hatékonyabb spektrum felhasználás,
- lényegesen nagyobb adatátviteli sebesség,
- kisebb működési késleltetési- és 20 msec-nál kisebb válaszidők (látencia),
- javított végfelhasználói tapasztalat és hatás elérése (kiváló hang/video konferencia szolgáltatások, sokszereplős játékok).

Az ellátottság növelése és a spektrum hatékonyság további javítása az LTE keretében igen fontos. Az RF csatorna sávszélesség 1-20 MHz lehet, az LTE elhelyezésére rendelkezésre álló frekvenciasávoktól függően. A nagyobb csatorna szélesség kedvezőbb az LTE szolgáltatásainak minél teljesebb kiaknázásához. Az LTE kezdeti rendszereihez elképzelhetők a 2012-2015 körül kezdődően kifutó GSM rendszerek sávjaiban történő elhelyezés, kisebb csatorna sávszélességekkel, majd a későbbi rendszerek erre kijelölt és alkalmas sávokban 20 MHz-es csatorna sávszélességeket is kaphatnak. Az itt elérhető adatátviteli sebesség letöltéskor (downlink) 144 Mbit/s, feltöltéskor (uplink) 50 Mbit/s, de 20 MHz-es csatorna sávszélességnél a fejlesztési célkitűzések rendre a 300 Mbit/s-os, ill., a 70 Mbit/s-os értékeket jelölnek meg.

A látencia javítása szintén igen fontos a VoIP és az interaktív Internet-játékalkalmazásokhoz. Mindezeket a célokat és feladatokat az LTE optimalizált hálózatszerkezettel és az üzemeltetők-szolgáltatók számára költséghatékony megoldásokkal éri el.

A 3GPP a 3G LTE fejlesztése számára tehát a következő magas szintű követelményeket fogalmazta meg:

- az átvitt adatmennyiség egy bitjére eső költségek csökkentése,
- megnövelt szolgáltatás mennyiség ellátásának képessége, több javított szolgáltatás ellátása alacsonyabb költségek és a végfelhasználók növekvő megelégedettsége mellett,
- a korábban rendelkezésre álló és az új frekvenciasávok rugalmas, hatékony felhasználása,
- egyszerűbb hálózati és rendszertechnikai felépítés, és szabványos nyílt interfészek használata,
- a végfelhasználói terminál készülékek teljesítmény igény csökkentése
- rugalmas, hatékony rádiós tervezési megoldások az LTE követelményeihez.

Maga az LTE az OFDM (Orthogonal Frequency Division Multiplex) modulációs eljárás és a MIMO (Multiple Input/Multiple Output) antennatechnika alkalmazásán alapul. Az eljárást többantennás megoldások egészítik ki a bázis és az előfizetői terminál oldalán, valamint antenna nyaláb formáló megoldások.

Az OFDM modulációs eljárás elmélete és rendszertechnikája szerint, az OFDM szomszédos keskenysávú vivők (alvivők) nyalábja. Az OFDM adó ezeket a külön-

böző frekvenciákat párhuzamosan továbbítja, sugározza ki az OFDM vevő számára. Az OFDM átvitel alvivőinek nagy száma és keskenysávú természete következtében, az OFDM nagyfokú állóságot mutat a többutas interferenciákkal szemben, amelyek más modulációs eljárásokhoz képest magas interferenciatűrést, kiváló hibavédelmet, és ennek következtében járulékosan jelentősen megnövekedett továbbítandó adatmennyiséget eredményez. Természetesen, az OFDM is tartalmaz kifinomult hibavédelmet (FEC) és az alvivők hatékony sokszintű modulációját (64QAM).

A 3GPP által képviselt mobil és cellás közösség számára mutatkozó, LTE névvel fémjelzett vezetéknélküli jövő, amit tehát a 3GPP keretében az utóbbi években fogalmaztak meg, a maghálózatok párhuzamos fejlesztését is megkívánta. A magházatok a teljesen IP alapú (all IP) hálózatok irányába fejlődnek. E fejlődés és koncepció neve SAE (System Architecture Evolution), ill., EPC (Evolved Packet Core, TCP/IP alapú). Ezek a koncepciók javítják a szolgáltatások ellátását és megkönnyítik a különféle fix és nem 3GPP mobil hálózat együttműködését.

Megemlíthető még, hogy a 3GPP LTE koncepciója és előírás rendszere az évek során más neveket is kapott. Ilyenek: Super 3G, 3G+, 3.9G és más hasonló elnevezések. Ebben az anyagban a 3GPP Long Term Evolution előírás együttesét 3GPP LTE elnevezésként jelöljük.

Szintén utalunk néhány szóval még, a CDMA távközlési közösségre. Addig, amíg a 3GPP a GSM-UMTS közösséget képviseli, a CDMA (cdma-2000) világot a 3GPP2 társulás fogja össze. A 3GPP2 keretében, az LTE-hez hasonlóan, kidolgozták a hasonló célú EVDO (Evolution Data Only) technológiát és ennek fejlesztési és bevezetési koncepcióját. Az EVDO technológiával az LTE-hez hasonló adatátviteli sebességek érhetők el. Várható, hogy a fejlődéses folyamatok eredményeként a nem 3GPP technológiák is az LTE szabványokat fogják követni.

5. Összefoglalás

A rádiófrekvenciás spektrum egyre zsúfoltabbá vált az utóbbi években, használata egyre összetettebb, és maga a frekvencia spektrum, ill., sávjainak megszerzése, használata, egyre fontosabb területe a versenynek. Ismeretes, hogy a rádiófrekvenciás spektrum véges természeti erőforrás, ezért az előadásban ismétlődő szempont és sokoldalúan megfogalmazott követelmény a rádióspektrum minél hatékonyabb felhasználása. Ez annál is inkább fontos, mert a mai és a jövő távközlése, a távközlési szolgáltatók, az előfizetők megszerzése és megtartása érdekében, az erre irányuló versenyben, egyre nagyobb mértékben fogja használni az újabb és újabb vezetéknélküli távközlési megoldásokat, különösen a hozzáférési szakaszokon és az előfizetői készülékek közelében használható különféle alkalmazásokhoz (NFC, UWB).

Az előadás másik fontos témaköre a maghálózatok és az ezeket támogató IP protokoll és az IT információs technológiák minél szélesebb körű alkalmazása. A lényegesen hatékonyabban használható, perspektivikus IP alapú hálózat infrastruktúra kialakítása csak több lépésben megvalósítható nagy feladat, ami jelentős beruházásokkal jár, de ami jelentős bevételekkel és ígéretes nyereséggel kecsegtet.

Utalunk arra, hogy a 3G, ill., a 4G távközlési technológiák egy sor fejlődő, versengő technikát tartalmaznak, beleértve, a létező és kialakuló cellás mobil távközlő

rendszereket, valamint a különféle rádiós hozzáférési technikákat, mint a WiFi, WiMAX, WiBRO, LTE. A verseny mind a szolgáltatók, mind a gyártók számára jelentős kihívásokat képvisel, de ezek alapvetően hozzájárulnak a felhasználók szokásainak, a szolgáltatás igénybevételek módjának alakításához, fejlődéséhez is. E rendszerek és alkalmazásuk egyre fontosabb, mind az üzleti, mind a magán célú távközlési felhasználásokhoz. A felhasználók a hálózatokat, különösen a mobil hálózatokat, a hagyományos beszéd célú és üzenet szolgálatok mellett, a DSL, ill., a WiFi alapú szélessávú világ igénybevételével, egyre inkább használni kívánják a mindennapi életben, munkában, tanulásban, továbbképzésben, az emberi kapcsolatokban, valamint a kikapcsolódásban és szórakozásban egyaránt.

Végül hivatkozunk mind a hozzáférési, mind a gyűjtő-koncentráló, mind a maghálózat létesítése, fejlesztése, üzemeltetése során érvényes gazdaságossági (CAPEX, OPEX, ARPU) szempontokra és a piac, a piaci körülmények és követelmények alakulására, fejlődésére. Ezek lényegesen befolyásolhatják az egyes ismertetett innovatív távközlési megoldások elterjedését, az elterjedés időbeli lefutását. Biztató, hogy a mobil rendszerek előfizetőinek száma egyre nő.

6. Fontosabb rövidítések jegyzéke

ARPU Average Revenue Per User	IMS Internet Multimedia Subsystem
ATM Asynchronous Transfer Mode	LTE Long Term Evolution (UMB Ultra Mobile Broadband)
BPON Broadband PON	LTE-A LTE Advanced (3GPP R9)
CAPEX Capital Expenditure	MIMO Multiple Input Multiple Output
DSLAMDigital Subscriber Line Access Multiplexer	NGPON Next Generation PON
EDGE Enhanced Data rate for GSM Evolution	OFDM Orthogonal Frequency Division Multiplexing
EDGE-E (EDGE Evolution)	OFDMA Orthogonal Frequency Division Multiple Access
EPC Evolved Packet Core	OPEX Operation Expenditure
EVDO Evolution Data Only (3GPP2, cdma2000)	PDA Personal Digital Assistant
FDD Frequency Division Duplex	PNA Personal Navigation Assistant
Femtocell Small Cellular Base Station	SAE System Architecture Evolution
Flash OFDM Fast Low-latency Access with seamless Handoff OFDM	TDD Time Division Duplex
FMC Fixed Mobile Convergence	UMA Unlicensed Mobile Access
GAN Generic Access Network	UMB Ultra Mobile Broadband
GE-PON Gigabit Ethernet PON	UMTS Universal Mobile Telecommunication System
GPON Gigabit-capable PON	VoIP, VoLAN, VoWLAN Voice over …
GSA Global mobile Suppliers Association	WiBRO Wireless Broadband (Internet Technology, Mobile WiMAX)
HSOPA High Speed OFDM Packet Access	WiFi Wireless Fidelity
HSPA (HSDPA, HSUPA)	WiMAX Worldwide Interoperability for Microwave Access
I-HSPA Internet HSPA	

SEBESTYÉN Attila – PÁNDI Erik[80]

A KÖZIGAZGATÁS ÁLTALÁNOS ÉS IT RENDSZEREINEK MODERNIZÁCIÓJA

Absztrakt: Jelen közlemény a témakörrel foglalkozó szakemberek véleményének széles bázisára építve betekintést ad a hazai kormányzati reformoknak és a közigazgatási rendszerek modernizációjának helyzetére, amelynek során a félreértések, problémák és dilemmák feltérképezése mellett megoldási alternatívákat is felvázol a napjaink közérdeklődésének egyik középpontjában levő terület átalakításának folytatását illető kérdésekben.

Kulcsszavak: elektronikus kormányzás, elektronikus közigazgatás, információtechnológia, információs társadalom.

1. Dilemmák, szemléletek

Hazánkban a kormányzat és a közszféra tervezési és operatív tevékenységének minősége az információs társadalom megfelelő ütemű fejlesztésében rejlik. A közigazgatási rendszerek modernizációja (reformja) nem elsősorban technológiai, hanem szemléleti és szervezeti feladatokat jelent. Nem az informatizálás a fő cél, hanem a rendszer működési folyamatainak racionalizálása. Az Európai Unió által meghatározott elvárások (ajánlások) teljesítése elvileg kedvez a felsőbb döntési szintekről kiinduló átalakításnak, de Magyarország – nehézkes az átalakítási folyamatok tekintetében. A kormányváltás óta úgy tűnik hiába alakult ki az új kormányzati struktúra, hiába jelentek meg az információs társadalommal kapcsolatos magyar stratégiák, a jelenleginél nagyságrendekkel átfogóbb és tudatosabb gyakorlat kialakítása nélkül nem remélhető előrelépés. Az e-kormányzat valós kialakítása tekintetében hazánknál sikeresebb országokban az építkezés megkezdésekor három alapvető kiinduló szempont került rögzítésre, így magával a kormányzattal kapcsolatosan a következő fő feladatok fogalmazódtak meg:

a) az informatikai megoldásokon messze túlmutató, korszerű információ- és tudásmenedzsment megoldások bevezetése és folyamatos fejlesztése;

b) a megfelelő nemzetközi interoperabilitás biztosítása;

c) a „vállalkozó állam" (government enterpreneurship) szerepkörének betöltése, különböző vagyonelemek céltudatos és ésszerű alkalmazásával, forgatásával;

d) a közhivatalokban való állampolgári bizalom erősítése ügyfélközpontú szolgáltatási szemlélet kialakításával, ahol hatványozottabb szerepet tölt be a helyi ügyintézési központ és a személyre szabott szolgáltatások;

[80] Szerzők: Sebestyén Attila r. alezredes, PhD-hallgató, ZMNE KLHK, Hadtudományi Doktori Iskola, Védelmi Vezetéstechnikai Rendszerszervező MSc. szak másodéves hallgató, ZMNE BJKMK Híradó Tanszék, ORFK osztályvezető; Dr. Pándi Erik egyetemi docens, ZMNE BJKMK Híradó Tanszék

e) a nyilvánosság új típusú megközelítése és kezelése.

Fentiek tükrében a hazai közigazgatási rendszerek modernizációja során a szervezeteket és folyamatokat tehát úgy kell alakítani, hogy a gazdaság általános élénkítése mellett a különböző versenyszabályokat nem sértő módon hozzon létre új formákat egyrészt a jelen és jövő domináns ágazatához, az információs- és tudásszektorhoz tartozó magyar termelő és szolgáltató vállalatok nemzetközi versenyképességének megerősítésére. Másrészt a közoktatás, a felsőoktatás, a kutatásfejlesztés és a kultúra területének stratégiai erőforrásaként és befektetési célpontként való felfogásához és ennek megfelelő prioritások biztosításához. Az információs kor kihívásai az intézményrendszerek mélyreható átalakítását követelik meg a tudásvagyon gazdálkodás kialakításával, a fenntarthatóság követelményének a tervezés és végrehajtás minden szintjére való beépítésével, valamint a társadalmi igazságosság és az esélyegyenlőség növelésének az információs kor igényeihez alkalmazkodó formáival.

2. Az elektronikus közigazgatás kialakításának kényszere

Az ügyfélkapcsolati rendszerek kiterjesztése, a szolgáltatások gyors és egyszerű eljuttatása az állampolgárokhoz, a szolgáltató oldali kommunikáció, valamint az adatok tárolása, továbbítása és feldolgozása ma már csakis a modern információs és kommunikációs technológiai eszközök segítségével oldható meg. A közigazgatási rendszerek modernizációja két egymástól elválaszthatatlan, szorosan összefonódó területet ölel fel:

a) a szolgáltató oldali, vagyis a közigazgatáson belüli folyamatok modernizációját;

b) a felhasználó oldali, vagyis az ügyfél és a közigazgatási szervek kapcsolatában megjelenő szolgáltatások fejlesztését.

Magyarországon a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény (Ket.) értelmében 2005 novemberétől az ügyfeleknek nem kell a hivatalok között ingázniuk különböző adatokért. Ha azok valahol már szerepelnek az állami, illetve önkormányzati adatbázisokban, az állampolgár ismételten nem kötelezhető a beszerzésükre. Sürgető feladat tehát a sok helyen használt szolgáltatások, valamint a minden intézmény működésében szerepet játszó és azonos funkciót betöltő belső folyamatok közös platformjának, felületeinek és szabványos megoldásainak kidolgozása. Folytatni kell az egységes ügyiratkezelés kialakításának szabályozását és standardizálását, elsősorban az önkormányzatok tekintetében. A szolgáltató oldali modernizáció nélkül reménytelen lesz betartani a Ket. előírásait, reménytelen lesz ügyfélorientált felhasználó oldali szolgáltatásokat várni a közigazgatástól. Az Európai Unióban jelentős erőfeszítések történnek arra, hogy a közigazgatás elektronizációját célzó projektek társadalmi-gazdasági hatásainak azonnali mérhetősége megvalósuljon. Az elektronizált közigazgatás révén megtakarítható a költségek több mint 5%-a, így az e-szolgáltatások elterjedtsége valóban fontos kérdésként vetődik fel. A felhasználói oldalon az állampolgárok és üzleti szereplők számára legfontosabb előnyként a gyorsaság és a minőségi, rugalmas szolgáltatás követelménye jelenik meg az e-közigazgatási szolgáltatásokkal kapcsolatban, amit papírlapon, egyetlen mamutszervezettel nem lehet megvalósítani. Magyarországon az APEH jár élen az e-adózás bevezetése

terén, ezzel nincs is gond. A gondot elsősorban az egyéb (önkormányzati, társadalombiztosítási) rendszerek okozzák, ezek elektronizációja jótékony kényszerrel hatna az állampolgárokra az on-line szolgáltatások igénybevételének használatára, azok elsajátítására.

3. Akadályozó tényezők

A közigazgatási rendszerek modernizációt hazánkban alapvetően a következő tényezők gátolják:

a) a közigazgatás és a politika csekély előrelátása;
b) az állampolgári tudatosság hiánya;
c) a köztisztviselők ellenállása;
d) az állampolgári igények megismerésének hiánya;
e) alacsony szintű tudásmenedzsment és humánerőforrás fejlesztés, képzés a közigazgatásban;
f) a szélessávú hozzáférés hiánya;
g) a back-office és a front-offic folyamtok koordinálatlan fejlesztése, az interoperabilitás hiánya;
h) a középkorú, illetve a kistelepüléseken élő állampolgárok érdeklődésének, igényének kielégítetlensége;
i) gyenge digitális írástudás;
j) ismeretlen az elektronikus aláírás.

A **közigazgatás és a politika csekély előrelátása** elsősorban abban nyilvánul meg, hogy a közigazgatási rendszerek modernizációja nem kötődik össze az elektronikus közigazgatási szolgáltatások eszközeinek és lehetőségeinek hangsúlyozásával, tudatosításával, holott az említett célok eléréséhez minden fejlett országban segítségül hívják az információs és kommunikációs eszközöket (ICT). Hazánkban még azokban az esetekben is jelentős lemaradás figyelhető meg, amelyekben egyébként az Országgyűlés példamutató előrelátással hoz meg törvényeket. Ilyen az elektronikus információszabadságról szóló törvény, amelynek végrehajtását kevés minisztérium alkalmaz a valóságban. A feladat egyszerűnek tűnik, a közigazgatásnak csak be kell tartania a vonatkozó jogszabályokat, tehát. Az **állampolgári tudatosság hiánya** abban jelentkezik, hogy hazánkban a felnőtt lakosság több mint a fele úgy gondolja, hogy a digitális világ nem nyújt számára semmi lényeges, általa igényelt lehetőséget. Évek óta alig csökkent azok aránya, akiknek igen kevés közvetlen kapcsolata van az információs társadalom jellegadó technológiai alaprendszerével, az internettel. A világhálót jelenleg egyáltalán nem használók több mint a fele lakik olyan háztartásban, ahol sem internet, sem számítógép, sem internetező személy nincs. Az internetet nem használók nagyobbik részét soha senki nem akarta eddig személyesen meggyőzni arról, hogy az hasznos lehet számára. Az igényteremtést kell segíteni, ezt pedig a – *lehetőleg* – ingyenes, vagy kedvezményes oktatással és az információs társadalom humán infrastruktúrájának fejlesztésével lehet elérni. A **köztisztviselők ellenállása** gyakorlatilag minden tagállamban megfigyelhető, ugyanakkor az más-más intenzitással jelentkezik. Hazánkban a közszolgálatban ma 200 ezer fővel kevesebben dolgoznak, mint 1988-ban. A közintézményi szféra dolgozói létszáma mintegy 300 ezerrel csökkent, ugyanakkor a közhatalmi ágazatban dolgozók létszáma 150 ezer fővel növekedett. Ebből követ-

kezik, hogy a megszaporodott feladatok ellátását elsősorban létszámnöveléssel, nem pedig a szolgáltató oldali folyamatok racionalizálásával oldották meg. Kevés figyelem összpontosul arra, hogy a közigazgatás informatizációja elsősorban a szervezeti folyamatok modernizálását, ésszerűsítését jelenti, ami nagyon sok esetben inkább attitűdbeli, kulturális és munkaszervezési változtatásokat igényel. Ez a folyamat pedig jóval hosszabb, mint egy informatikai rendszer felállítása, így erre a területre sokkal jobban érdemes koncentrálni. Az **állampolgári igények megismerésének hiánya** egyértelmű, hiszen hiányoznak az erre irányuló kutatások felmérések. Az ország viszonylag jól teljesíti az Európai Unióban pillanatnyilag előírt 20 minimális közigazgatási szolgáltatás elektronikus úton való elérhetőségének biztosítását. Jelenleg hazánkban nem ismertek azok az állampolgári felhasználói igények és elvárások, amelyekre támaszkodva meg lehetne kezdeni a fejlesztési programok kidolgozását, meghatározva fő irányukat és prioritásukat. Ugyanakkor az Európai Unióban máris kiemelt prioritást kapott a befogadó e-közigazgatás koncepciója, ami mögött az a cél húzódik meg, hogy az eddigieknél sokkal jobban vegyék figyelembe a felhasználók igényeit. Hazánkban jelenleg **alacsony szintű tudásmenedzsment és humánerőforrás fejlesztés, képzés jellemzi a közigazgatást**. Az utóbbi évtizedekben mind a fejlett, mind a fejlődő országokban jelentős hangsúlyt kapnak az átfogó közigazgatási reformtörekvések (New Public Management). A közigazgatási és kormányzati munka újragondolása és gyakorlati átszervezés lehetővé teszi, sőt egyenesen sürgeti a civil szektorban a tudásmenedzsment terén szerzett tapasztalatok (szemlélet, modellek, eljárások) adaptációját. A kormányzati tevékenységek korszerűsítése és az ezt támogató új szervezeti kultúra a technológiai fejlesztési programok, az új menedzsmentmódszerek, illetve a kezelendő tárgykörök komplexitása miatt csakis egy tudásközpontú fordulat révén születhet meg. Az állampolgároknak nyújtott szolgáltatások tartalmi menedzselése, valamint az egykapus e-kormányzati szolgáltatások kialakítása hatékony adat-, információ- és tudásmegosztást, illetve együttműködést igényel a különböző intézmények között és az egyes szereplők között. A közigazgatási munka racionalizálását és a működési költségek csökkentését célzó reformok sürgetik az intézmények tevékenységi körében meglevő átfedések és a redundancia kiszűrését, illetve kiküszöbölését. A fenti célok megvalósításához nélkülözhetetlen az egységes, de legalább kompatibilis technológiai platform kialakítása és a központi koordináció. A közérdekű adatok olyan üzletileg is hasznosítható adatvagyonként állnak elő a közszféra szervezeteinél, amelynek a hasznosítása mind a piaci szereplőknek, mind közszférának fontos lehet. Az előző hármas kihívásnak való megfelelést a kormányzati információ- és tudásmenedzsment jelenlegi helyzetképének alapos átvilágítás alapján történő felrajzolása segíthetné a legjobban, melynek alapján kidolgozható a kormányzati tudásmenedzsment stratégia. A **szélessávú hozzáférés hiánya** jelenti talán a modernizáció egyik jelentős akadályát. Az Európai Bizottság direktívái évek óta világosak, hiszen mind az eEurope2005, mind az i2010 az elsők között emelik ki a szélessávú internet eléréséhez szükséges infrastruktúra fejlesztését és az e-közszolgáltatások elterjedését alapvetően befolyásoló szolgáltatási árak letörését. A végfelhasználók szintjén az internetszolgáltatók, valamint a hozzáférést biztosító egyéb technológiai lehetőségek versenye hazánk településeinek döntő többségében nem valósult meg. A kistelepülések esetében a

helyzetet rontja, hogy az elmúlt években nem történt áttörés az olcsóbb, alternatív[81] technológiák megjelenésében, bármennyire ez felelne is meg leginkább az Európai Unió direktíváinak. Már-már erőszakos módon kell tehát támogatni a szabályozás eszközeivel a Wi-Fi, az üvegszálas és egyéb alternatív technológiák elterjedését. Hamarosan jelentős fejlődésnek indul például a digitális televíziózás is, amit az önkormányzatok nagyon hatékonyan felhasználhatnának az állampolgárokkal való kommunikációban. Erre már lényegében napjainkban is fel lehetne készülni a megfelelő szolgáltatások kialakításánál. Hazánk örökös problémája az egyeztetés nélküli cselekvés. A **back-office és a front-office folyamtok koordinálatlan fejlesztése, az interoperabilitás hiánya** ennek csak egy területe. A jövőt tekintve össze kell hangolni a mesterségesen szétválasztott központi és önkormányzati közigazgatás sok esetben párhuzamos elektronizációját is. A fejlesztési politika koordinálatlansága különösen az európai uniós források szétosztásával történő fejlesztési programok esetében mutatkozik meg, így az egymással kommunikálni nem képes rendszerek itt is problémákat fognak szülni. Ugyanez a helyzet a koordináció nélküli nagy rendszerek párhuzamos fejlesztésénél is. Több mint 40 e-önkormányzati fejlesztési program indult az országban, összesen több milliárd forint ráfordítással, a közszolgáltatások on-line elérhetősége az önkormányzatok esetében mégis még mindig gyerekcipőben jár. Óriási gondot jelent, hogy a helyi szinten kialakított informatikai rendszerek egy része nem lesz képes összekapcsolódni sem az Ügyfélkapuval, sem egymással, sőt a nagy államigazgatási rendszerekkel sem. Ezek a fejlesztéseket nem tartoztak a központi államigazgatás felügyeleti körébe. A **középkorú, illetve a kistelepüléseken élő állampolgárok érdeklődésének, igényének kielégítetlensége** azért okoz gondot, mivel az internet alacsony elterjedtségi mutatói ellenére az e-közigazgatási szolgáltatások nagyobb mértékű igénybevétele lehetne az a húzóágazat, amely a korszerű infokommunikációs eszközök használatára, esetleg az ilyen eszközökbe való beruházás felé terelné az érintett társadalmi csoportot. A lakosságnak majdnem fele pozitívan viszonyul az elektronikus ügyintézéshez, az elektronikus kormányzati és önkormányzati szolgáltatások meglétével tisztában levő állampolgárok 40 %-a tervezi, hogy a jövőben ki is próbálja azokat. Előrelépést ezen a téren az olyan on-line közigazgatási szolgáltatások támogatása, ösztönzése lehet,[82] amelyek iránt a középkorú vagy idősebb potenciális felhasználók között nagy az érdeklődés. Hazánk **gyenge digitális írástudása** megmutatkozik abban, hogy Magyarország az Európai Unió egyik negatív listavezetője e téren. A lakosság 57 %-a soha nem használt még számítástechnikai eszközt, illetve kétharmada nem tekinthető internetezőnek sem. A munkahelyi eszközhasználat esetében sem jobb a helyzet. Hazánkban csak a munkavállalók mintegy 30 %-a alkalmaz számítógépet munkája során. A helyzet alapvetően kezelhető, mivel a foglalkoztatáson keresztüli képzéssel az állampolgárok jelentős része elérhető. **Ismeretlen az elektronikus aláírás** a lakosság több mint kétharmada számára, de a fennmaradó mintegy 30 % többsége sincs tisztában annak mivoltával. A szolgáltatást az összlakosság 2 %-ánál többen még nem használták. Az elektronikus aláírást még nem használó vállaltok döntő többsége, mintegy kilenctizede állította azt, hohy

[81] elsősorban száloptikás, illetve vezetéknélküli
[82] pl.: adókedvezmény

náluk eddig még nem merült fel igény a szolgáltatás iránt. A digitális hitelestést már alkalmazó vállalkozások csaknem 65 %-a a hatóságokkal tartja a kapcsolatot az e-aláírás segítségével. Egyes kiemelt célcsoportok[83] számára adható ingyenes digitális aláírás nagy lökést jelenthetne az új szolgáltatás tömeges bevezetésében.

4. Modernizáció a közszférán kívül

Az ICT alkalmazásának terén konzervatív magyar társadalomban számos lehetőség mutatkozik arra, hogy a modernizáció kihasználja a pozitív külső hatásokat, illetőleg kisugárzó erejét tudatosan érvényesítse a közszférán kívül is. Ilyen lehet például úttörő alkalmazások bevezetése vagy új eszközök használatában való példamutatás. Ezt hatékonyan egészíti ki az ICT-eszközök széles körű használhatóságának népszerűsítése, az előretekintő tudatosság (awareness raising) növelése. Ennek sikere az új környezet iránti társadalmi bizalom növekedését, az ICT-vonatkozású biztonságérzet javulását és ezen keresztül közvetve az e-gazdaság térnyerését is elősegíti. A közigazgatás és általában a közszolgálat és a közvetlen előnyöket nyújtó elektronikus szolgáltatások kiterjesztése, segítheti a digitálisan írástudatlanok felzárkózását, ezen keresztül pedig a társadalmi részvétel erősödését és a felelősségvállalás növekedését is. A közigazgatási rendszerek modernizációjának ez különösen fontos, de jelenleg jellemzően háttérbe szoruló feladata.

5. Összegzés, következtetések

Az elmúlt évek gazdaságpolitikai döntései révén – *akár tetszik, akár nem* – hazánk a globális gazdasági térség egyik nem minden mutatójában jól prosperáló szereplőjévé vált, ezért kénytelen kellett *„beszállni”* a földrajzi környezetünkben a befektetések megszerzéséért folyó éles, időnként öldöklő, permanens versenybe. A globális térben a tőkét mozgatók bizonyos szempontból tekintve *„törvényen felüliek”*, ezért a *„szükséget szenvedőknek”* a kényszerűség okán is törekedniük kell olyan belső környezet kialakítására, amely kielégítő közszolgáltatásokat feltételez. Az ICT alkalmazása azonban önmagában nem javítja a kormányzati munkát, eredményességhez arra van szükség, hogy az új eszközök bevezetése szerves részévé váljon a közigazgatás modernizációjának és ez a kormányzat valamennyi intézményének és szintjének összehangolt erőfeszítését igényli. Hazánk Európai Uniós csatlakozása óta sokat fejlődött e téren, azonban a kezdeti biztató és dicséretes technológiai fejlesztéseken túl újabb próbatétel előtt áll.

Felhasznált irodalom:

[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.,

[3] http://europa.eu.int/information_society/activities/egovernment_research/doc/scenario_session_report.pdf

[83] pl.: vállalkozók, munkavállalók, felsőoktatási hallgatók

[4] Szittner Károly: Az elektronikus közigazgatás kezdetei Magyarországon, Magyar Közigazgatás LVI. évf. 3-4. szám, Budapest, ISSN 0865 736 X, 193-195. oldal, 2006.
[5] Dr. Várnay Ernő – Dr. Papp Mónika: Az Európai Unió joga, Budapest, ISBN 963-224-746-9, KJK-KERSZÖV Jogi és Üzleti Kiadó, 2005.
[6] 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
[7] 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.

Dr. HÓKA Miklós

TECHNIKATÖRTÉNET II.
NÉMET RÁDIÓK A II. VILÁGHÁBORÚBAN

A legrégebbi gyár, amely fontos szerepet játszott a német katonai rádiók kialakításában a híres Telefunken cég volt. Az I. Világháború alatt ez a cég látta el a német hadsereget tábori rádiókészülékekkel. Az akkori technológiai háttér eltűnt a Versaille-i békeszerződés után, de újjáéledt az 1930-as évek elején, amikor Hitler magához ragadta a hatalmat.

A gazdasági válságból kivezető utat Németország vezetői a fegyverkezésben látták, így a rádiógyártás vonatkozásában ismét a Telefunken cég került vezető pozícióba. Egy másik német cég, a Lorenz, amely *az amerikai ITT konszern* német vállalata volt, - együtt a Telefunkennel - megkezdte a német harcászati rádiók gyártását 1935-ben. Más nagy német cégek, mint a Siemens ugyancsak résztvettek az együttműködésben.

Korabeli források szerint, mintegy 40 000 munkás dolgozott a rádiógyártó hadiüzemekben és a háború végéig csak a harckocsirádióból, az un. "Bogegerat"-ból mintegy 180000 db.-ot gyártottak.

Vessünk egy pillantást a német katonai rádiók technológiai hátterére!

Meghatározó volt a kevés típusváltozatú vákuumcsövek alkalmazása: a legtöbb rádiókészülékben ugyanazokat az elektroncsöveket használták. Ennek előnye egyértelműen az esetleges javításoknál jelentkezett. A csöveket kifejezetten katonai alkalmazásra fejlesztették ki, a speciális foglalatú miniatűr csövek azokban az időkben nagyon strapabíró eszközök voltak, és szabványként szolgáltak a kis számú civil rádiókészülékek gyártásánál is. A rádiók belső kialakításánál a modulrendszer volt az alap, egyszerűen és könnyen kapcsolták össze az egyes paneleket, funkciójuknak megfelelően.

Rádiókezelő egy motorkerékpárra szerelt Torn.fu.b1 rádiót üzemeltet

Német rádiósraj egy Torn. Fu. d2-t használ a Franciaországi csata alatt

A modulok kialakításánál külön szempont volt, hogy mind mechanikailag, mind elektronikai szempontból önálló egységet képezzenek. (Hasonlítsuk össze ezt a gyártási szemléletet napjaink elvárásaival a modern rádióeszközök kialakításában!)

A modulegységek elektronikai csatlakozásai sokérintkezős, „tűs"csatlakozókkal történtek, a különösen erős konstrukciójú rádiókészülékek ennek is köszönhették hibamentes működésüket, de az egyszerű szervízelési lehetőségeiket is.

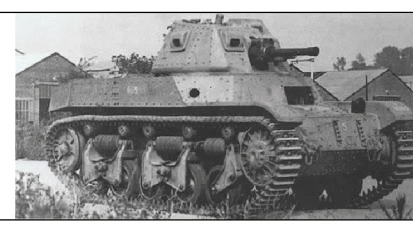
Hatvan évvel a háború után ezek a készülékek olyanok, mintha tegnap kerültek volna ki a gyárból (a tankokba épített készülékek külseje speciális lakkal lett kezelve a gyártásnál). A német II. Világháborús kondenzátorok ma is működnek, az ellenállások szintén, az egyetlen probléma a csövek állapota, amelyek fűtőszála már nem tökéletes.

Német harckocsirádiók

Német páncélos a háború elején

A II. Világháború alatt a német hadsereget az erőteljes rádióhasználat (is) jellemezte. A villámháborús (Blitzkrieg) tervek a páncélos csapatok, a légierő, a tüzérség és a gyalogság összehangolt tevékenységén alapultak, mely koordináció a rádióeszközökkel valósult meg. Lengyelország villámgyors lerohanása 1939-ben jól illusztrálja a földi és légi egységek együttműködésének fontosságát, de ez döntő jelentőségű volt a későbbi franciaországi és oroszországi páncélos műveletekben is. Guderian nézetei igazolást kaptak.

Az 1940-es francia haderőben a vezetők igencsak híján voltak a kor követelte vezetési technikáknak. Annak ellenére, hogy a francia haderő nagyszámú, korszerű harckocsival rendelkezett, a franciák sohasem tudták koncentrálni a védelmüket, vagy jelentős ellentámadást kialakítani.



Francia páncélos

A harci tervek futárok útján, szóban kerültek továbbításra a csapatokhoz, így a harci erők átcsoportosítása, mozgatása elég nehézkesen ment. Harc közben a parancsok kiadása zászlójelekkel történt, így a füstben, a sötétségben vagy a harcme-

zőn összekeveredett csapatok között sohasem érték el azt a hatásfokot, amit egy rádióháló biztosíthatott volna. Egy jelentés szerint nem egy francia harccsoportnál éppen a tényleges harc előtt merültek le a rádiók akkumulátorai, így azok rögtön elvesztették híradási – és ezzel együtt vezetési - képességüket.

Német Tigris harckocsi

Orosz T-34 harckocsi

Az 1941-es oroszországi invázió alatt a németek ismét bizonyságát adták vezetési képességeiknek. Bár a T-34-es szovjet harckocsik a szemtől-szembeni harcban gyakran sikeresebbek voltak a Wehrmacht tankoknál, előnyüket nem tudták kihasználni a friss harcparancsok vételében, vagy a más fegyvernemekkel való együttműködésben. A német nehéztüzérség vagy a 88 mm-es légelhárító ágyúk tüzének koncentrálása, az oldalról való támadásba való átmenet manőverezése kiegyenlítette a Párduc és Tigris harckocsik kezdeti gyengeségeit. A harci tapasztalatok azt mutatták, hogy legalább 88mm-es ágyúkkal kell felszerelni a német felsővezetés által kért új páncélosokat, kiegyensúlyozni az oroszok lényeges számbeli fölényét, illetve nagyobb páncélvédettségét. (A T-34 harckocsiból mintegy 90 ezer darabot gyártottak a háború végéig, és ez messze felülmúlta a német lehetőségeket.) A másik probléma, hogy a harckocsik nem több ezer km-es távolságok megtételére készültek, különösen nem az orosz időjárási és „útviszonyokra". A poros, sáros utakon a légszűrők gyakran eltömődtek, jelentősen növelve az üzemanyagfogyasztást, és nehezítve az előrejutást. A 3200 km-re nyúlt utánpótlási vonalakon a partizántevékenységek akadályozták az alkatrészellátást, a kegyetlen orosz tél pedig már Napoleon seregeit is legyőzte. Az oroszok ugyan sohasem ismerték el a külső körülmények negatívumait a németek számára, és pusztán saját hősiességüknek tudták be a háború fordulatát, de gondoljunk csak a rádiókkal lényegesen gyengébben ellátott orosz harckocsik kommunikációs képességeire, vagy akár a rádiós kiképzettség hiányára.

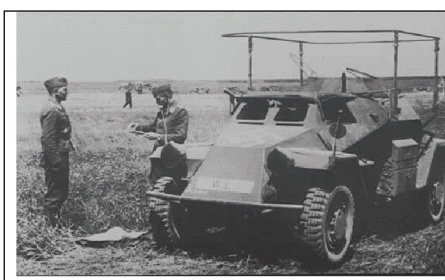
A németek javára billentette a mérleget a kiképzettségük, és az, hogy rendelkezésükre álltak azok a minőségi rádiók, amelyek megfeleltek a páncélos csapatok harci követelményeinek. A kiképzéshez tartozott például: ha egy német páncélos harcjármű lerobbant és fennállt a veszélye, hogy a felszerelés az ellenség kezére jut, a rádiókezelőnek kötelessége volt a rádióeszközöket elrejteni vagy megsemmisíteni. Majdnem mindegyik páncélosban volt rádióvevő, de ezen túl még speciális páncélos járművek is egy koordinációs rádióhálóba voltak szervezve, amelyekben szerepeltek a vezetési pontok, a légierő, a páncélosok, a tüzérség és a gyalogság

parancsnokai. Ezek a járművek szét voltak osztva a páncélos alegységek között és ugyanúgy részt vettek a harcban, mint a nehézharckocsik.

A páncélosok vezetésében a legmeghatározóbb jármű a parancsnoki páncélos volt (Panzerbefehlwagen PZB fwg): ebbe több rádióeszköz került beépítésre, amelyek széles frekvenciasávban voltak képesek kommunikálni, és elérték a vezetési pontokon a magasabb parancsnokokat. Külsőleg csak egy járulékos antenna különböztette meg a többi páncélozott harcjárműtől: a „csillag"antenna, amely esernyőszerűen beborította a jármű tetejét.

PZB fwg (SDkfz-263)

A négy, hat vagy nyolckerekű, páncélozott harcjárművekbe épített rádióeszközök különböző teljesítményűek voltak (20, 50, 80W), a jármű tetején méretezett keretantenna biztosította a számos variációban beépített rádiók üzemét.



SD.kfz.-223 híradó páncélos

SD.kfz.-232 városban

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

A harckocsikba szerelt rádiók külön adóegységből, vevőegységből, motoros dinamóból, a csatlakozó kábelekből és a belső beszélgető rendszerből álltak.

Típus	*Frekvencia*	*Alkalmazás*

10 W.S c Transmitter	27.2 - 33.3 MHz	Minden páncéloson
10 W.S. h Transmitter	23-24.95 MHz	Koordinációs rádióháló
20 W.S. Transmitter	27.2 - 33,300 MHz	Szdpk. és zpk. harckocsik
30 W.S. Transmitter	1,110 – 3,010 MHz	Ezred és hadosztály szinten
100 W.S. Transmitter	200kHz - 1,200 MHz	Nagy távolságokra
Ukw (URH) Ea rádióvevő		Együtt a fenti rádióadókkal
Kw (RH) Ea rádióvevő	980 kHz - 10,200 MHz	Koordinációs rádióháló
Mw (KH) Ec vevő	830 -3000 kHz	Koordinációs rádióháló

A 10 W.S. típusú rádióadó

A 20 W.S. típusú rádióadó

A 30 W.S. típusú rádióadó

URH vevő, 1940-es tervezés

URH vevő, későbbi tervezés

Német hátirádiók

A legtöbb harci egységnél a Torn E b készüléket használták, amely a háború korai szakaszában két különálló egységből állt, a rádióból és a tartozék egységekből. Ezeknek az egységeknek a tápellátása szárazelemről történt, de rendszeresítve voltak a vibrátoros áramfejlesztők a készülékekhez.

Típus	*Frekvencia*	*Alkalmazás*
Feldfu.a1	120-156 MHz	Lövészek
Feldfu b	90-110 MHz	Lövészek
Feldfu b1		Hegyivadászok
Feldfu b2		Páncélgránátosok
Fedlfu c	130 - 160 MHz	Lövészek
Feldfu .f	28. 0 - 33.0 MHz	Páncélgránátosok
Feldfu .h	23.1 - 25.0 MHz	Védelemben és együttműködésre
Kl.Fuspr.d „Dorette”	32.0 -38.0 MHz	Tüzérségi megfigyelőpont
Torn Fu g	830 kHz-3MHz	Széleskörű

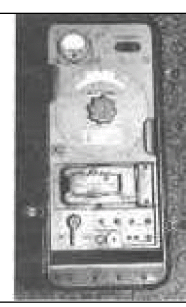
Híradóraj egy Torn. E b rádióvevőt üzemeltet

A földi állomások adóból, vevőből és néhány esetben 2 ütemű dízeles generátorból álltak. Létezett egy kerékpárhajtású generátor is, de ez viszonylag ritkán került ki a harcolókhoz.

A harcászati hátirádiók áramellátása ugyancsak vibrátoros tápegységgel történt, szárazelem táplálással. A hátirádiók a háború korai szakaszában két dobozba kerültek beépítésre, amit később egyesítettek, az egyszerűbb hordozhatóság végett.

Feld Fu

A „Szárazföldi Beszédadó" (Feld fu) egy valódi hátirádió volt, 2,4 V-os, Ni-Cad akkumulátorról üzemelt és 1940/41-től került rendszeresítésre. A II. Világháború alatt a németek nagyon magas minőségre fejlesztették az akkumulátorokat, még különleges kézitöltőket is kifejlesztettek hozzájuk. A szabványosítást olyan megfontolásból is végezték, hogy a kellően begyakorolt mozdulatok alapján sötétben is lehetett akkumulátort cserélni a készülékekben, a tetejükön kialakított fémkampók letapogatása alapján, de Braille írással is feltüntették a készülékek kezelőszervein a beállítási értékeket, hogy akár vakok is tudják kezelni, hangolni a rádiókat.

			
Feld Fu hátirádió	Feld Fu hátirádió, előlap	Torn Fu g rádió	Kleinfunksprecher d (KlFuSpr.d) "Dorette"

Torn Fu g

A Torn Fu g egy középhullámú, valódi szuperheterodin vevő volt. Sokszor használták harckocsikban is (Párduc és Tigris tankokban) a páncélgránátosokkal való együttműködésre. A háború későbbi szakaszában már hátirádióként is funkcionált.

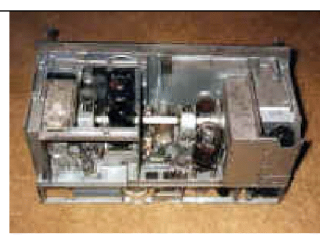
Kleinfunksprecher d (KlFuSpr.d) "Dorette"

A „Kis Beszédadó" - Kleinfunksprecher d (KlFuSpr.d) - a "Dorette" , 1944 októberétől került a harcolókhoz, ez volt a legkisebb német harcászati rádió, eredetileg tüzérségi megfigyelő és tűzvezetési pontokra tervezték. A Dorette szolgált alapul számos, háború utáni orosz rádió kialakításánál, illetve a cseh RF-11 készülék szinte ennek a készüléknek a közvetlen másolata.

KiFuSPR.d Dorette

Cseh gyártású RF-11 mkII.

A II. Világháborúban használt német rádiókészülékek több szakíró véleménye szerint is világszínvonalat képviseltek az 1930-as évektől kezdve. A rádiók üzemképességéről csak annyit, hogy még 60 évvel a II. Világháború után is jelentős hányaduk működőképes (már az a néhány száz darab, ami elkerülte a szétszerelést[84]).



A 20WS rádióadó belseje

A Dorette belseje

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

KORONCZAI Tibor

A MAGYAR HONVÉDSÉG KATONAI KOMMUNIKÁCIÓS RENDSZERÉNEK VIZSGÁLATA

A rendszerváltást követően néhány év alatt gyökeresen átalakult a távközlés, a kommunikációs szolgáltatók megteremtették a kínálati piacot. A polgári távközlés és informatika a hálózatok kiépítésével, valamint a fogyasztók részéről jelentkező igényekkel rohamosan fejlődni kezdett, megelőzve a katonai híradást. A katonai kommunikáció terén változás következett be a NATO-hoz történő csatlakozás előkészítése folyamán. A csatlakozási feltételek, az országgal szemben támasztott elvárások, a katonai költségvetés növekedése eredményeként az állandó telepítésű kommunikáció korszerűsítésének a feltételei, lehetőségei is megteremtődtek. A NATO ajánlások, szabványok a szervezési módok meghatározták, a fejlesztés lehetőségét, irányait. Az alapgondolat, hogy a Magyar Köztársaság területét lefedő „nagysebességű" információ átvitelt biztosító, szövevényes hálózatot hozzanak létre, a csomópontokban korszerű digitális kapcsoló berendezések alkalmazásával, lehetővé tette a Magyar Honvédség számára a civil szférában már alkalmazott korszerű szolgáltatások elérését.

A Magyar Honvédség létszámának, struktúrájának meghatározó szerepe van mind az állandó telepítésű, mind a tábori híradó eszközök, rendszerek, infrastruktúrák korszerűsítése és fejlesztése tekintetében. A meglévő tábori alap-hírhálózat korszerűsítése tekintetében Dr. Rajnai Zoltán megállapításai megfontolandók a döntés előkészítők és döntéshozók számára is: *„... az új digitális rendszert a NATO tagországokban alkalmazott és széles körben elterjedt rácsrendszerű, területlefedő hálózatként kell kialakítani, ahol a kommunikációs eszközök, végberendezések, és a hálózat magában foglalja a hírközlő- és informatikai hálózatokat is, és egységes rendszert képezve biztosítja az információk széles skálájának továbbítását a felhasználók részére."*

A Magyar Honvédség kommunikációs rendszere véleményem szerint, a Magyar Köztársaság területén, vagy területén kívül (pl. ideiglenes katonai szervezetek hírrendszere, a „missziók" hírrendszere) a Magyar Honvédség érdekében állandó, vagy ideiglenes jelleggel üzemelő komplex információtovábbító rendszer, mely magába foglalja az átviteli utakat, a kapcsoló elemeket, a hálózati infrastruktúrát, a végberendezéseket. A kommunikációs rendszert üzemeltető személyzet kulcsfontosságú a rendszer tekintetében!

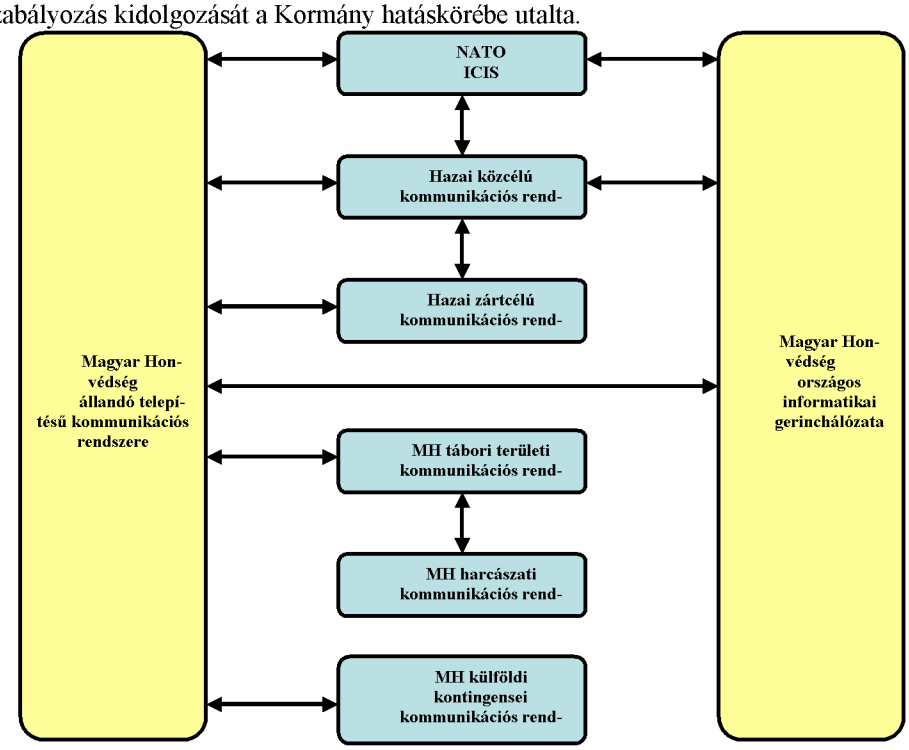
A MH kommunikációs rendszerének békeidőszakban, veszélyhelyzetben, fegyveres vagy fegyvernélküli katonai alkalmazáskor a katonai szervezetek közötti vezetési, együttműködési tevékenység során biztosítania kell az igényeknek megfelelő információcsere lehetőségét kettő vagy több vezetési szint részére.

A távközlési és informatikai rendszerek folyamatos fejlődése eredményeként előtérbe kerülnek a nagyobb sebességet igénylőalkalmazások. A multimédiás eszközök nemcsak a polgári életben, hanem a katonai alkalmazásokban is teret nyertek. Ma már a Magyar Honvédség is csökkenti a papír alapú nyilvántartásokat, melynek helyét a digitális adatbázisok veszik át. Az adatállományok mérete, sokasága meg-

követeli a kommunikációs hálózatok fejlesztését. Gyorsabb, jobb minőségű, a sávszélességeket jobban kihasználó hálózat létrehozása a cél.
A kommunikációs hálózatok fejlesztése többnyire magas költségű beruházásokkal valósítható meg. A fejlesztés során figyelembe kell venni a meglévő hálózati elemek optimális felhasználási és kihasználási lehetőségeit, mind az állandó telepítésű, mind a kommunikációs rendszerek tekintetében. A hálózatok szervezése, irányítása, felügyelete kiemelten fontos terület melyet nem hanyagolhatunk el. A hálózat fejlesztés részeként kell kezelni a hálózat-felügyeletet, valamint az üzemeltető állomány kiválasztását, felkészítését.

A Magyar Honvédség Katonai Kommunikációs rendszere

A Magyar Honvédség Katonai Kommunikációs rendszere nem vizsgálható az alapvető jogi környezet vizsgálata nélkül. A távközlésről szóló 1992. évi LXXII. törvényben jelenik meg a „zártcélú hálózat" fogalma, melynek egyik fajtája a „kormányzati hálózat." A távközlési törvény a zártcélú hálózatokra vonatkozó szabályozás kidolgozását a Kormány hatáskörébe utalta.



2. ábra: a MH Hálózatának kapcsolata más kommunikációs rendszerekkel (forrás: Dr. Fekete Károly)

Az 50/1998. (III.27.) Kormány rendelet a zártcélú távközlő hálózatokról hat különböző hálózatgazdát nevesít meg, a honvédelmi miniszter, mint hálózatgazda felügyelete alatt a Magyar Honvédség és a katonai nemzetbiztonsági szolgálatok

tartoznak. Ugyanakkor a Kormány a hírközléspolitika függelékében célként határozza meg az egységes kormányzati felügyelet alatt lévő, integrált, költségtakarékos kommunikációs rendszer kialakítását, deklarálva a zártcélú kormányzati távközlő hálózatok létesítése és működtetése terén indokolatlan párhuzamosságok megszüntetését.
Az 1126/2003. (XII.12.) a Magyar Információs Társadalom Stratégiáról és annak végrehajtásáról szóló Kormány határozat többek között előirányozza a kormányzati szervek csatlakozását az Elektronikus Kormányzati Gerinchálózathoz (EKG), valamint a kormányzati elektronikus aláírás rendszer (PKI), és az egységes kormányzati címtár és levelező rendszer kialakítását.
Az EKG kialakításával kapcsolatosan a 1122/2001. (XII.22.) Kormányhatározat tartalmazza a kormányzati és közigazgatási adatbázisok és informatikai rendszerek összekapcsolását, melynek célja a közigazgatási szervek közötti nagysebességű kapcsolatok megteremtése, valamint ez által az elektronikus szolgáltatások elérhetősége.
Az EKG-hoz köteles csatlakozni a Honvédelmi Minisztériumot és az általa működtetett zártcélú távközlő hálózat.
A polgári távközlési és informatikai hálózatok technikai konvergenciája eredményeként az országgyűlés 2007 őszén megalkotta és elfogadta a LXXIV. törvényt a műsorterjesztés és a digitális átállás szabályairól. A technikai konvergencia megvalósulását tükrözi, hogy a magyarországi szolgáltatok (távközlési, informatikai, médiatechnológiai, infokommunikációs) egy szolgáltatásként, vezetékes vagy vezeték nélküli átviteli úton különböző csomagokban kínálják a felhasználók részére, a hang, adat és képátvitelét (telefon, Internet, televízió).
A polgári technikai konvergencia a NATO-ban is elindított egy útkeresést, melynek várható következménye, hogy a jövő alapvető információ továbbító katonai hálózata (főként az állandó jellegű hálózatok) IP alapú lesz.
A Magyar Honvédség és a Honvédelmi Minisztérium állandó jellegű és tábori híradó és informatikai rendszere a jelenlegi állapotában nem alkalmas a követelményeknek a kielégítésére. Mégpedig azért, mert szolgáltatásaiban szűk körű, tábori eszközein csak kézi kapcsolt beszéd kapcsolatok létesítésére alkalmas. A különböző hazai távközlő hálózatokhoz csak jelentős nehézségekkel, vagy már úgy sem tudjuk csatlakoztatni. Technikailag elavult, fenntartása erő- és eszközigényes, a kezelők kiképzése pedig időigényes.
A korszerű infokommunikáció követelményei, a multimédia funkciók analóg rendszerben nem, vagy csak rendkívül korlátozott mértékben elégíthetők ki. A NATO csak a hadtestek szintjéig rendelkezik szabványos rendszerrel. A tagállamok többségének saját, nemzeti tábori digitális rendszerei, harcászati rádiói egymással csak csatornaszinten, a rádiók esetében pedig a legegyszerűbb üzemmódokban képesek együttműködni. Az interoperabilitás elérése egymás között is feladat, nem csak a partnerországokkal. Ez a digitális technológia egyik velejárója. Nincs olyan kész megoldás, szabvány, amely átvehető, amelynek alkalmazásával saját nemzeti rendszerünk kialakítható.
Több alkalommal halottam már a különböző „workshop"-ról, nemzetközi gyakorlatról, külföldi tanfolyamról hazaérkezők beszámolóit a „fantasztikus" berendezésekről, mert látták, hogy az a kicsi, mobilhoz hasonlító rádió mindent tud, nem

lehallgatható, könnyű, nem törik stb., nem tudva, hogy a mögötte lévő kommunikációs infrastruktúra nélkül annyit ér, mint a saját mobilja a Káli-medencében, ahol köztudottan nincs térerő.
A Magyar Köztársaság távközlési infrastruktúrája dinamikusan fejlődik, a legkorszerűbb szolgáltatások is igénybe vehetők. Amennyiben a nemzetközi polgári szabványok mellett kötelezzük el magunkat, akkor igénybe vehetjük, és rendszer szinten integrálhatunk szolgáltatásokat, alkalmazhatunk polgári berendezéseket.

Összegzés

Azt gondolom, hogy a kialakítandó IP alapú digitális rendszert, amely kielégíti a Honvédelmi Minisztérium és a Magyar Honvédség korszerű vezetési, irányítási, informatikai és felderítési rendszerei támasztotta információcsere és információvédelem követelményeit, képes a Magyar Köztársaság köz- és zártcélú hálózataival, a NATO rendszereivel együttműködni. Ez a rendszer természetesen sokba kerül, országunk teherbíró képessége pedig véges. Ez a szakemberek számára azt jelenti, hogy a leggazdaságosabb megoldásokra tegyenek javaslatot, kerüljék a párhuzamosságokat, olyan mértékben egységesítsék a rendszert, amilyen mértékben lehetséges.

Felhasznált irodalom

[1] Rajnai Zoltán: A tábori alaphírhálózat vizsgálata és digitalizálásának lehetőségei egyes NATO tagországok kommunikációs rendszereinek tükrében, Doktori (PhD) értekezés, Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, 2001.

[2] Fekete Károly: A Magyar Honvédség állandó telepítésű kommunikációs rendszere továbbfejlesztésének technikai lehetőségei, Doktori (PhD) értekezés, Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, 2003.

[3] Pándi Erik: A magyar kormányzati távközlés egységesítésének hatása a rendvédelmi-, katonai-, és közigazgatási kommunikációs rendszerek megszervezése és irányítása, Doktori (PhD) értekezés, Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, 2005.

[4] Az 1992. évi LXXII. Törvény a távközlésről.

[5] Az 50/1998. (III.27.) Kormány rendelet a zártcélú távközlő hálózatokról

FARKAS Tibor – PÁNDI Erik[85]

AZ IT SZAKTERÜLET MEGKÖZELÍTÉSE, BEHATÁROLÁSA

Absztrakt: Az információtechnológia (IT) kifejezéssel lényegében napról napra találkozhatunk különböző általános, illetőleg speciális médiumokban anélkül, hogy annak jelentését, fogalmát pontosan definiálnák magunk számára. E jelenség ugyancsak megfigyelhető a rendészeti szervek esetében is, hiszen a szervezetek működését, mindennapi életét meghatározó jogszabályok, normák e területe nem bővelkedik részletes és korrekt magyarázatokkal. Jelen közleményben a szerzők megkísérlik feloldani e problémát.

Kulcsszavak: informatika, információtechnológia, távközlés.

1. A szakterület jogi-igazgatási megközelítése

A Rendőrség Szolgálati Szabályzatáról szóló – *jelenleg már nem hatályos* – 3/1995. (III.1.) BM rendelet szövegezésében a 4. § (4) bek. b) pont *információ technikai (tájékoztatási) szakszolgálatként* nevesítette az IT ágazatot [1]. A Határőrség Szolgálati Szabályzatáról szóló 40/2001. (XII.23.) BM rendelet 4. § a) pontjában a gazdasági szakszolgálat keretében került rögzítésre az *informatika*, mint funkcionális terület [2]. A szervezetek összevonását követően hatályba lépő, a Rendőrség Szolgálati Szabályzatáról szóló 62/2007. (XII.23.) IRM rendelet 2. § (5) bek. a) pontja szerint az *információ technológia* területe a gazdasági szakszolgálathoz kerül besorolásra [3]. Látszólag tehát az IT ágazat „jogszabályi" alapjai mindkét korábbi rendészeti szervnél lényegében rendezettnek volt tekinthető, míg napjaink Rendőrsége esetében e probléma fel sem merül. Másik szempontból vizsgálódva azonban le kell szögezni, hogy a Szolgálati Szabályzat az *információ technológia* fogalmára, konkrét területére kielégítő magyarázatot nem ad. Harmadrészről, a rendészeti szakvizsgáról, a rendészeti vezetővé képzésről és a rendészeti mestervezető képzésről szóló 14/2006. (BK 7.) BM utasítás 8. § (1) bek. h) pontja a Rendészeti Szakvizsga Bizottság egyik albizottságaként nevesíti a Műszaki-Technikai-Informatikai Albizottságot (a továbbiakban: MTIAB), amely testület – *többek között* – a *„Rendvédelmi szervek informatikai igazgatása"* c. tárgykörben képzi tovább, illetve vizsgáztatja napjainkban is a legmagasabb beosztott tiszti (I/VI.) besorolású hivatásos rendőri szakállományt [4]. Az IT szakterület besorolását és meghatározást körülvevő ellentmondások ténye tehát nyilvánvaló, a kérdés ezzel kapcsolatosan az, hogy a korábbi szabályzatok alapjaira építkező jelenlegi szabályozás hogyan értelmezhető az integrált szervezet részéről?

[85] szerzők: Farkas Tibor, tanársegéd, ZMNE BJKMK Híradó Tanszék, PhD-hallgató, ZMNE KLHK Hadtudományi Doktori Iskola, Dr. Pándi Erik, egyetemi docens, ZMNE BJKMK Híradó Tanszék

Az *informatikai igazgatás* tárgykörének meghatározása még a napjainkban hatályos tankönyv egykori szerzői számára is nehézségekbe ütközött, ezért az évek folyamán a probléma feloldására egy sajátos megoldás került kialakításra. Ezek során, ragaszkodva az utasítás normatív szövegezéséhez megtörtént az **informatika**, mint fogalom behatárolása, ami a Magyar Tudományos Akadémiától kölcsönzött klasszikus definíció szerint nem más, mint: *„Az információs rendszerek létrehozásával, struktúrájának és működésének elemzésével foglalkozó tudomány. Az informatika ezért a tudományos információs tevékenység elméletét, módszereit, szervezetét, hatékonyságát, technológiáját, valamint történetét tanulmányozza azzal a céllal, hogy optimális módszereket és eszközöket fejlesszen ki az információ gyűjtésére, tárolására, visszakeresésére és terjesztésére. Az alkalmazott informatika a megvalósítási kérdésekkel foglalkozik."* [5]. Az **igazgatás** fogalmára a nagylexikon a következő magyarázatot adja: *„…valamely adott feladat megvalósítását szolgáló végrehajtó tevékenység. Az igazgatás olyan szervezeti funkció, amely az alapvető célok és feladatok realizálását segíti tervező, előkészítő, szervező, rendelkező és adminisztrációs tevékenységgel."* [6]. E két alapdefiníció felhasználásával az **informatikai igazgatás** MTIAB által elfogadott meghatározása a következőként került rögzítésre: **Az információ gyűjtését, tárolását, visszakeresését, és terjesztését szolgáló optimális módszerek és eszközök kifejlesztésének (megvalósításának) hatékony elősegítése tervező, előkészítő, szervező, rendelkező és adminisztrációs tevékenységgel.** A képzésben és szakvizsgáztatásban alkalmazott definíció tehát rendelkezésünkre áll, de a két korábbi, valamint a jelenlegi szolgálati szabályzat szövegezéseit áttekintve még mindig zavarok tapasztalhatók, vagyis nincs kielégítő magyarázat az *információ technológia* fogalmára, illetőleg arra, hogy az *információ technológia*, mint szakszolgálat, miért vesztette el önálló státuszát, miért került a gazdasági szakszolgálat egyik ágazataként besorolásra?

2. Behatárolás

Visszatérve a „kályhához", vagyis a jelenünket erősen befolyásoló technológiai konvergenciához és kiteljesedésének kérdésköréhez, továbbá a hatályos Szolgálati Szabályzathoz, megítélésünk szerint az informatikai igazgatás Rendőrségnél jelenleg alkalmazott tantárgyi meghatározásának, definíciójának átgondolását, újraértékelését teszi szükségessé. E gondolat már nem tekinthető újszerűnek, hiszen mind a hazai, mind a közösségi államigazgatási gyakorlatban – *a szolgáltató állam, az elektronikus kormányzás és az elektronikus közigazgatás témakörén keresztül* – konkrét, kézzelfogható törekvések figyelhetők meg a szektor további fejlesztését illetően, amelyek egyúttal kényszerűséget is jelentenek a hazai rendvédelem számára. Röviden és plasztikusan áttekintve a technológiai helyzetet megállapítható, hogy a hagyományos hazai távközlő hálózatok kilencvenes években megkezdett digitalizálási folyamataival párhuzamosan az informatikai eszközök és hálózati megoldások kvantitatív és kvalitatív mutatói is emelkedtek [7]. Ezen folyamatok már csírájában magukban hordozták a csak távbeszélő funkciót (szolgáltatást) biztosító struktúrák leépülését, kihalását. A digitális távközlő hálózatokban minden területen kommunikációs célszámítógépek jelentek meg, amelyek a formai kiviteltől eltekintve ténylegesen csak az alkalmazott perifériák és futtatott kommunikációs célú operációs rendszer tekintetében térnek el egy általános számítógéptől. A

korábban elszigetelt *„informatikai szigetek”* összekötésére megnőtt a felhasználói igény, egyre nagyobb és szövevényesebb vállalati (hivatali) intranet hálózatok megjelenése bizonyította a gyors információáramlás előnyeit, majd a digitális (fő funkció tekintetében eredetileg távbeszélő) kapcsolóközpontok rendszerére ráépülve – *több lépcsőben* – teret hódított az internet. A civil (polgári) felhasználásban egyre jobban elterjedtek a különféle, személyi számítógépeken is futtatható beszédcélú szoftverek (pl.: Skype, Messenger, stb.), amelyekkel – *bár minőségi kompromisszumok árán* – kikerülhetővé tették a vezetékes telefonvonalakhoz való *„röghöz kötöttséget”*. Megjelentek olyan távbeszélésre specializált telefonok is, amelyek digitális központra való csatlakozás nélkül, mint a számítógépes hálózat egyik célszámítógépeként kerülhettek alkalmazásra [8].

Más megközelítésből nézve azt lehet mondani, hogy a korábbiak mellett megjelent egy másik konvergenciahatás is, nevezetesen a vezetékes technikai megoldások mobil átviteli rendszerek felé történő elmozdulása, illetve a vezetékes megoldások kiváltása. Ez korábban a mobiltelefon-rendszerek gyors elterjedésében volt megfigyelhető, de napjainkban már a mobil adatátviteli megoldások egyértelmű előretörése érzékelhető. Míg régebben a vezetékes megoldások rovására törtek előre a mobil rádiótelefon-szolgáltatások, addig ma a mobil szolgáltatásokra épülő nagysebességű adatátviteli és informatikai alapú vezetéknélküli, nagysebességű rendszerek közötti evolúciós harc figyelhető meg. A tendenciák minden területen az internet protokoll irányába való elmozdulást mutatják, maguk a távközlési szolgáltatók is ennek megfelelően kénytelenek folytatni fejlesztéseiket. Az Európai Unió (EU) információs társadalom és médiaügyekért felelős biztosának[86] véleménye szerint az információs társadalom megteremtésének egyetlen útja az információs technológiák előretörésében, valamint a távközlési szolgáltatók monopolhelyzetének megtörésében, vagyis a **szolgáltatások**, illetve a **hálózatüzemeltetési feladatok** szétválasztásában rejlik [9]. Ez gyakorlatilag azt jelenti, hogy a már rendelkezésre álló, döntően optikai távközlő hálózatokra – *mint hordozó struktúrára* – építve lehetségessé válhat a szélessávú információs technológiák távközlési szolgáltatók korlátozó hatása nélküli szabadabb fejlesztése.

Összességében véve, technológiai szempontból megállapítható, hogy a távközlő és informatikai hálózatokban megtalálható eszközök napjainkban lényegében már minden területen informatikai alapra épülnek. Rövid időn belül, mértékadó szakértői vélemények szerint tíz évnél nem hosszabb időn belül várható a jelenlegi, hagyományosnak tekinthető **távközlő rendszerek teljes átalakulása**, amelyből valójában csak az optikai gerinchálózatok rendszere lesz túlélőképes, mint hordozószolgálat. A gazdasági fejlettség élvonalában járó térségek – *közöttük az EU* – további fejlődését a technológiai konvergencia jelenségek és azok hatásai kedvezően befolyásolták a kilencvenes években, hiszen a telekommunikációs és informatikai ágazatok olyan gazdasági húzóágazattá alakultak át, amelyek egyúttal előrevetítették az információs társadalom érdemi kialakítását. Az új társadalmi modell egyik szegmense a szolgáltató állam és ennek alrendszere az elektronikus kormányzás (e-kormányzás), avagy elektronikus közigazgatás (e-közigazgatás), amelyek kiépítésére a bővülő EU igen nagy hangsúlyt fektet napjainkban is. Az EU e-

[86] 2006-ban, a publikáció közlésekor a biztos Viviane Reding volt

kormányzati törekvései 1995-ben indultak el, az IDA[87] program keretében. Az IDA felelős a legfontosabb e-kormányzati folyamatokért, ez koordinálja a legmagasabb, európai szinten a szolgáltató-oldali folyamatokat, a szabványosítást és a páneurópai szolgáltatásokat. A program két szakaszra tagolódott: a) 1995-1999, b) 1999-től napjainkig. Az e-kormányzat és e-közigazgatás politikai tervezésének új irányvonala már a Barroso-bizottság működéséhez köthető, amelynek alapjai a következők [10]:

a) közigazgatás modernizációja: cél egy nyitott és transzparens közigazgatás megteremtése, amely széles körben, demokratikus alapokon vehető igénybe;

b) innovatív kormányzati szolgáltatások: személyre szabott, a társadalmi bevonást elősegítő és költségkímélő online szolgáltatások kialakítása;

c) pán-európai közigazgatási alkalmazások elterjesztése: közigazgatási hálózatok közötti kölcsönös együttműködés és működőképes integrált rendszerek megteremtése feltételezi a pán-európai viszonylatban kialakított e-kormányzati folyamatokat.

Mindezeken belül, a 2006-2010 közötti időszak prioritásaiban a jellemzően pán-európai célok mellett a következők is megfogalmazódnak:

a) elektronikus azonosítás és hitelesítés a közszolgáltatásokban;

b) európai digitális állampolgárság;

c) e-közigazgatás társadalmi hatásainak vizsgálata, mérési keretek meghatározása;

d) a többszintű e-közigazgatási szolgáltatások közötti mélyebb integráció megteremtése;

e) közösségi interoperabilitási előírások;

f) PPP-modell[88] erősítése;

g) e-közigazgatás társadalmi hatásainak vizsgálata, mérési keretek meghatározása;

h) a többszintű e-közigazgatási szolgáltatások közötti mélyebb integráció megteremtése.

Az általános iránymutatáson túl, az azonos e-kormányzati fejlettség elérése érdekében az EU a stratégiai irányvonal meghatározása mellett konkrét projekteket és egységes politikai állásfoglalásokat is igyekszik megfogalmazni. A korábban elfogadott EU-javaslatok[89] az alábbi célokat fogalmazzák meg:

a) 25 %-kal kell csökkenteni az állampolgárokkal és az üzleti élet szereplőivel szembeni adminisztratív korlátokat;

b) 2010-ig ki kell alakítani a felhatalmazás és azonosítás módszereit a pán-európai szolgáltatások használata során;

c) valóra kell váltani a papírnélküli közigazgatást;

d) ösztönözni kell az e-közigazgatási szolgáltatások használatát.

[87] Interchange of Data between Administrations. Közigazgatási szervek (adminisztráció) közötti adatcserét koordináló EU-program

[88] PPP-modell: public/private partnership

[89] CoBrA recommendations

A CoBrA-javaslatok alapján elkészített, 2010-ig érvényes szupranacionális[90] szintű akcióterv a legfontosabb mérföldköveket a következők szerint határozta meg, amely irányelvek tagállami alkalmazását egyúttal az EU kötelezővé is tette:

a) valamennyi közösségi állampolgár, vállalkozás és közigazgatási rendszer számára lehetővé válik az elektronikus azonosítás és hitelesítés rendszerének használata;

b) a tagállamok részéről az elektronikus dokumentumok egységes használatát lehetővé tevő hivatkozási és hitelesítési keretrendszer kidolgozása;

c) az ICT eszközök révén valamennyi állampolgár társadalmi befogadását el kell érni;

d) minden nyilvános, közérdekű információ és szolgáltatás könnyített hozzáférését biztosítani kell;

e) a hozzáférés előtt álló korlátok azonosítása, a szükséges helyzetelemzés elvégzése minden tagállamban;

f) az állampolgárokra és üzleti vállalkozásokra háruló adminisztrációs terhek csökkentése, a transzparencia[91] és a számonkérhetőség jegyében hatékonyabb közszolgáltatási rendszerek kiépítése;

g) széleskörű hatással bíró szupranacionális szintű szolgáltatások megvalósítása;

h) a kormányzatok közötti adatcsere és interoperabilitás megvalósítása nyílt szabványok bevezetése révén.

A magyar kormányzat – *amely a közigazgatás elektronizálása területén az EU-27-ek rangsorában kedvező helyet foglal el* – 2007. január 1-jével a zártcélú hálózatok – *és így a belügyi igazgatás hatókörébe tartozó szerveket korábban kiszolgáló kommunikációs rendszerek és szervezetek* – tekintetében jelentős átalakításokra szánta el magát,[92] amelyek egyértelműen tükrözik a hazai kormányzati (közigazgatási) informatika és így az uniós e-kormányzati és e-közigazgatási irányelvek továbbfejlesztése melletti álláspont erőteljes képviseletét. Fenti határidőtől az Igazságügyi és Rendészeti Minisztériumot (IRM), illetőleg az Önkormányzati és Területfejlesztési Minisztériumot (ÖTM) irányító miniszter[93] elvesztette hálózatgazda jogosultságát, amellyel egyidejűleg az irányítása alá tartozó Rendészeti Hálózat (RH)[94] és üzemeltető szervezet az Elektronikus Kormányzati Gerinchálózat (EKG)

[90] szupranacionális: nemzetek feletti

[91] transzparencia: átláthatóság

[92] az akkor hatályos, következőkben felsorolt jogszabályok és normatív eszközök mentén: 2006. évi LV. törvény, 2006. évi CXXI. törvény, 2006. évi CXXVII. törvény, 44/2005. (III.11.) Korm. rendelet, 144/2006. (VI.29.) Korm. rendelet, 160/2006. (VII.28.) Korm. rendelet, 276/2006. (XII. 23.) Korm. rendelet, 7/2006. (XII.20.) ME rendelet, 1054/2006. (V.26.) Korm. határozat, 1066/2006. (VI.29.) Korm. határozat, 2118/2006. (VI.30.) Korm. határozat, illetve a 1026/2007. (IV.11.) Korm. határozat

[93] e megállapítás természetesen érvényes a jelenlegi Önkormányzati Minisztériumra, illetőleg a Nemzeti Fejlesztési és Gazdasági Minisztériumra is

[94] korábban: Egységes Belügyi Digitális Hálózat (EBDH)

alhálózataként került besorolásra. Az EKG jelenlegi hálózatgazdája a Miniszterelnöki Hivatalt vezető miniszter. Ezen intézkedések paradigmaváltást[95] jelentenek, amelyekkel végérvényesen lezárulni látszik egy a kormányzati és közigazgatási szereplők, ágazatok közötti szakmai-pénzügyi vitáktól erősen terhelt, szervezeti és irányítási szempontból decentralizált időszak [11]. A konvergencia- és EU-s folyamatok tárgyalását lezárva, azokkal párhuzamokat vonva, **összességében véve** megállapíthatjuk, hogy napjainkra a rendészeti szervek esetében lényegében megvalósult az informatikai és távközlési szolgáltatások és hálózatüzemeltetési feladatok adminisztratív szétválasztása.

Visszatérve az alapkérdéshez, vagyis hogyan értelmezhető az *információ technológia*, úgy ítéljük meg, hogy a jelenleg elfogadott **informatikai igazgatás** megnevezését és definícióját kell mindenképpen olyan irányba szélesíteni, amely mindkét eredeti meghatározáson túl magába foglalja a hagyományos telekommunikációs tevékenységrendszereket az azokat kiszolgáló hálózatok üzemeltetési funkcióinak kivételével.

3. Definiálás

A jövőt illetően, a Rendőrség tekintetében az informatikai igazgatást mindenképpen **információtechnológiai igazgatásnak** kell tekinteni, amely általunk elfogadott definíciója a következő lehet: **Az információ gyűjtését, tárolását, visszakeresését, terjesztését és biztonságos továbbítását szolgáló optimális módszerek, eszközök és rendszerek kifejlesztésének (megvalósításának) hatékony elősegítése tervező, előkészítő, szervező, rendelkező és adminisztrációs tevékenységgel.**

Az **IT igazgatás** integrált rendőri szerveknél való megjelenésének főbb tulajdonságai lehetnek:

- az IT alkalmazott „tudományágként" jelentkezik;
- célja az alaptevékenység támogatása;
- fentiek okán az IT igazgatás funkcionális tevékenységként azonosítható be;
- szervezeti keretei elsősorban a funkcionális (gazdasági) szerveknél kerül kialakításra;
- előző megállapításból kifolyólag, a funkcionális szerveket magába foglaló gazdasági szakszolgálat ágazataként a sajátos feladatok ellátására, a tevékenységi körök végrehajtására létrehozott szervezeti egységek összessége alkotja a Rendőrség gazdasági szakszolgálatának IT ágazatát.

4. Összegzés, következtetések

A Magyar Köztársaság Rendőrsége szabályzataiban az információtechnológia, mint a mindennapokban használatos kifejezés definiálása nem történt meg. Szélesköru szakirodalomra alapozva – *sajátos eszközrendszerünk révén* – e hiánypótlást jelen közleményben elvégeztük.

[95] paradigma: egy adott történeti időszakban uralkodó elméleti modellvariáns

Felhasznált irodalom:

[1] A Rendőrség Szolgálati Szabályzatáról szóló 3/1995. (III.1.) BM rendelet, DVD jogtár 2007/12. szám, Complex Kiadó Jogi és Üzleti Tartalomszolgáltató Kft., ISSN 1788-5027, Budapest, 2007.;

[2] A Határőrség Szolgálati Szabályzatáról szóló 40/2001. (XII.23.) BM rendelet, DVD jogtár 2007/12. szám, Complex Kiadó Jogi és Üzleti Tartalomszolgáltató Kft., ISSN 1788-5027, Budapest, 2007.;

[3] A Rendőrség Szolgálati Szabályzatáról szóló 62/2007. (XII.23.) IRM rendelet, Igazságügyi Közlöny CXVI. évf. 1. szám, 337. oldal, ISSN 0133 7645, Budapest, 2008.;

[4] A rendészeti szakvizsgáról, a rendészeti vezetővé képzésről és a rendészeti mestervezető képzésről szóló 14/2006. (BK 7.) BM utasítás, DVD jogtár 2007/12. szám, Complex Kiadó Jogi és Üzleti Tartalomszolgáltató Kft., ISSN 1788-5027, Budapest, 2007.;

[5] Magyar Nagylexikon kilencedik kötet, 870-871. oldal, Magyar Nagylexikon Kiadó, ISBN 963 9257 00 1, Budapest, 1999.;

[6] Magyar Nagylexikon kilencedik kötet, 768. oldal, Magyar Nagylexikon Kiadó, ISBN 963 9257 00 1, Budapest, 1999.;

[7] Pándi Erik: Trendek és kihívások – zártcélú hálózatok a globális térben (tanulmány), 19. oldal, Zrínyi Miklós Nemzetvédelmi Egyetem, Egyetemi Könyvtár, Budapest, 2007.;

[8] Szöllősi Sándor: Konvergáló hálózatok fejlődési trendjei, a technikai alkalmazhatóság kérdései a Magyar Honvédség infokommunikációs rendszerében (PhD-értekezés), 18-29. oldal, Zrínyi Miklós Nemzetvédelmi Egyetem, Egyetemi Könyvtár, Budapest, 2007.;

[9] Berta Sándor: Viviane Reding szétzúzná a távközlési konszerneket, SG.hu Kiadói Kft. honlapja, http://www.sg.hu/cikkek/48697, 2006. november 22.;

[10] Takács, Attila: New challenges in the are of European electronic government, Kommunikáció 2006. nemzetközi szakmai-tudományos konferencia, Zrínyi Miklós Nemzetvédelmi Egyetem, 223-226. oldal, ISBN 978 963 7060 18 2, Budapest, 2006. október;

[11] Pándi Erik: A hazai zártcélú hálózatok szerepének átalakulása az elektronikus közigazgatási szolgáltatások bevezetése és kiterjesztése folyamatában, Hadmérnök, II. évf. 2. szám, 92-97. oldal, ISSN 1788 1919, Budapest, 2007.

Gábor EGRI

THE SCHENGEN INFORMATION SYSTEM AS A SPECIAL RESOURCE FOR POLICE OPERATION

THE HUNGARIAN NATIONAL SUBSYSTEM

Introduction

Hungary acceded to the European Union at 1st of May 2004 with other new member states from Eastern and Southern Europe96. After a strong and hard preparation Hungary together with other 8 new countries97 joined the Schengen Agreement98 [SchAgr] and the Schengen Convention99 [SchConv], as well.

One of the main conditions of the so called Schengen requirements was to create and introduce into operation the Hungarian national subsystem of the Schengen Information System, the NHU.SIS, and to start the cooperation with the whole system, with its SISone4ALL version100.

The process of the creation of NHU.SIS

Information are significant and very important resources for the police work, so information-technology as the science dealing with the creating, processing, transmission and evaluation of information has a huge relevance in the professional work. The IT and telecom activity is used widely in every-day police work as the state-of-the-art computer technology and other possibilities are widely used nowadays in public administration. For instance the electronic mails, the telephone and fax connections have decreased the volume of the conventional mails and flowing of documents.

Nowadays the fight against cross-border crime need in incredible level the international interoperation of the police organisations and it is effectively and at this moment irreplaceably served by special European information system, by the Schengen Information System (SIS). The first generation of the Schengen Information System started its operation in March 1995 after thorough-going analysis of technical, legal, economical, and financial aspects of development.

96 The new member states are Czech Republic, Cyprus, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Slovakia, and Slovenia. Since that time other two states have acceded to the EU, Bulgaria and Romania.

97 The new „Schengen" countries are the tens except Cyprus who will join only to the SIS II system together with UK and Ireland.

98 Agreement between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders. 14th of June 1985

99 Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders. 19th of June 1990

100 The SISone4ALL version was initiated by Portuguese partners and fulfilled by the cooperation between all member states and the European Commission.

The creation process of NHU.SIS had had a long preparing period of time near from the beginning of the decade till the acceding action. During this time we used the resources given by the European Union (e.g. PHARE project) and from own budget.

After 2004 the resources of Schengen Found were open for special purposes, to prepare the country to the joining the SchAgr and the SchConv.

We had opportunity to use a huge amount of budget to create a brand new system for border guarding near to the external101 borders of the country. We made investment into the whole infrastructure including rooms, IT, telecommunications, vehicles, etc., as well.

The role of the information technology

The investments mentioned above were made to help the policing and border policing activities in the country. The new IT system as the part of the operational SIS 1+ gives huge and very good resource for police personal. The information which is necessary for officers at the border and at in-depth control is done at the right place and just in time. So Hungary can fulfil the requirements of SchAgr and SchConv to protect not only the own country but the whole EU.

The use of the system is in very close connection with the IT and the police or border police activity including the whole operating territory of the interested parties. The most spectacular application of the system is the border control as it is the best known adoption for the public. This opportunity can be divided into several parts depending on where the operation is in use, at external or internal102 borders or at in-depth control.

The SISone4ALL is in use at external border as an IT support to border police and customs. Just such detailed control, based on all the data of the Schengen countries can guarantee the high level of the internal safety and security of the European Union. The officer of the public administration in the external border protects not only his/her own country but the whole Schengen area.

This total control at the external border gives possibility to eliminate the border control at the internal borders. In such cases the open frontier is realised without any stopping and difficulties, the border crossing is known only by seeing the foreign language text.

Other applications of the SIS are the cases when the police make the so called in-depth control, the supervision made in the internal part of the country by border police. This police activity has rising importance due to the problems of migration, smuggling and organised crime. In this case the officer makes his/her duty in the whole territory of his/her region using necessarily the IT resources of SIS, as in the case of a real border control.

---

101 External border means a border between countries where one country is the member of the EU but the other is not. So in every case an international airport or harbour is external border even if its traffic is moving not only within the EU. The external borders of Hungary are the frontiers to Ukraine, Romania, Serbia and Croatia.

102 Internal borders are the common borders of the states that signed the Schengen Agreement. Hungary has internal borders nowadays with Austria, Slovakia and Slovenia.

Development of the system

The SchAgr and the SchConv was signed more than 15 years ago and the SIS has begun its running for more than ten years. The development of the technical level of IT was increased significantly and the political environment changed a lot during this period of time so the Commission of the EU decided to fundamentally reconstruct the present system, to create the second generation Schengen Information System, the SIS II.

The necessity of SIS II

During the development process the European Commission started to set up a brand new system. The necessity of it is based on the following aspects:

- The present so called SIS 1+ system was ready to serve only 18 countries. This figure was counted as the total number of former and old member states (15) and the number of potential parties, Norway, Iceland and Switzerland. The accession protocol of ten new countries contains that it is obligatory them to use the Schengen Acquis and to accede to the Schengen Area. To fulfil this obligation the EU as the admitting organisation has to prepare its technical system itself for this task.
- Since starting the operation of SIS the information technology itself has been developed very much the digital technology has spread in general use in computer science. Mentioning only the main aspects of these developments nowadays the mobile communications reached incredible high level, together with other elements serving the mobility, the capacity of memories and computers increased rapidly, the speed of data communication grew up several times as before, etc.
- It is necessary to enlarge the connecting capacity not only because the number of member states increased but new international organisations, as Europol, or Eurojust appeared as potential end-users of the information system. The enlargement of EU made in 2004 and the number of new member states and other organisations will resume even more than 30 connecting parties instead of the present 18. This procedure of course is not only a technical task but has a lot of legal problems to solve in the near future, too.
- The SISone4ALL version is only a temporary resolution for new member states to use the SIS and join the Schengen Area.

Main features of SIS II

The present services of the SIS suffered larger and smaller developments several times during its operation. These new implementations meant the enlargement of services and more powerful applications but the architecture of the system is the same as was before. The result of the new development will be the SIS II and it will fulfil a lot of new services respectively to new requirements. The Commission is responsible for the whole process of renewal of SIS.

- The process of the development is based on brand new platform of architecture. It means a modified conception with new elements of the system e. g. in the question of national copy.

- A really new function is the more detailed data in the registers. So they content not only alphanumeric characters but pictures, images, biometrics etc. ensuring more complex data processing possibilities.
- SIS II is in principle the newest IT system with much more power and robustness for serving better the end-user's requirements.
- The SIS II made a big step forward to enlarge the basis of information (e. g. biometrics) and using this platform to process data and support new European legal tasks as EAW (European Arrest Warrant).
- The possibility of interconnections between the SIS and VIS systems enables more efficient way to fulfil the interests of the member states.
- The new system brings closer to the optimum the use of national and communal resources. To compare to the present operation the network management, the operation and maintenance, testing of the system, change management will be simpler and so it will increase cost efficiency. The up-to-date positions, the scalability, the easier management will lead to use a more resilient system ensuring the maximum capacity and effectiveness.

The structure of SIS II

In the new system the national copy is not used in every member state. It is typical that the old member states having the national copy now will preserve for themselves the possibility of own copy on the basis of the present storages. This opportunity is unnecessary and results needless additional charges by the Commission. Hungary does not plan to create national copy. In consequence of absence of a national copy the reliability, redundancy and back up of the central system shall be realised in much higher level than the present one. The working centre of CS is in Strasbourg, France and the back up system will be located in Austria.

Another significant difference is the speed of data transmission in the network. Nowadays the technical possibilities are much greater than at the beginning of the operation were, so the new network will able to serve the higher requirements in the field of security, safety and the strong volume of information.

Setting up the SIS II system

The time schedule of the creation of the SIS II system is a very important political issue in the EU. In the beginning of development process the deadline for the going into operation was decided the beginning of 2007. The call for tender was issued in August 2003 but the legal procedure followed by the evaluation has stopped the process for several months. After the consensus the development could continue but the official deadline was modified only much later. The documents of EU contain the end of September 2009 for switch-over the new system.103

103 Provisional high-level schedule for the SIS II project State of Play. 20080226194340268.pdf

The development of the second generation Schengen Information System (SIS II) has been entrusted to the Commission pursuant to Council Regulation (EC) No 2424/2001 and Council Decision 2001/886 JHA on the development of the second generation Schen-

Enlargement of the Schengen Area as a success story

The enlargement of the Schengen Area with the 9 new member states to SISone4ALL was a very successful story. It is clearly proved by the fact as the original deadline of 31st of December 2007 was fulfilled some days earlier at 21st of December.

This border lifting became possible on the continuous operation of the technical system. A line of technical staff, engineers, IT experts etc. were working to achieve this goal during the all year. The technical system itself was ready to operation at the end of May, 2007 but we had to run a lot of tests and data loading processing, as well.

After a detailed control and supervision got the countries (all the 9) the opportunity for the lifting of border control at internal borders.

Hungary joined the Schengen Area in December 2007 under the governmental decision 2328/2004 (XII. 21.).[104]

All the old and new member states (all the staff of them) were working in perfect way doing everything to help each other giving a good example of the EU's mind. We try to use this forum to say again thank you to all partners at home and abroad in this long and very important project.

gen Information System. The network requirements for SIS II development are established by Commission Decision 2007/170/EC and by Commission Decision 2007/171/EC. The second generation Schengen Information System has been established by Regulation (EC) No 1987/2006 of the European Parliament and of the Council and by Council Decision 2007/533/JHA on the establishment, operation and use of the second generation Schengen Information System.

104 Considering the practices of former accessions the real opening of the borders were realised after several months following the readiness of the technical systems, as in Hungary as well. E.g. the situation with Italy was the following: Signing the Agreement on the Accession of the Italian Republic to the Convention implementing the Schengen Agreement were done on 27th November 1990; the technical system was ready to use in 26 October 1997 and the opening of border were done at the beginning of next year.

KARSAY Gábor

ALCATEL-LUCENT NONSTOP LAPTOP GUARDIAN

Az IT menedzserek a vállalati laptopok terjedésével új kérdéssel szembesülnek a „mobile blindspot"al. (láthatatlanság).

Amikor egy felhasználó teljes lelki nyugalommal kikapcsolja a laptopját és elhagyja vele a vállalatot, az IT menedzsmentnek a kockázatok megnövekedését jelenti, hiszen egészen addig amíg a felhasználó egy VPN kapcsolaton keresztül be nem jelentkezik semmit nem tudunk a laptopról.

- Hol van éppen a laptop?
- Ki használja?
- Védettek vajon a rajta tárolt adatok?
- A felhasználó vajon tudatában van a kockázatoknak?
- Ha kiküldünk egy biztonsági update-et akkor azt mikor tölti le a felhasználó? És vajon a fontos adatokat minden változtatáskor back-up mentéssel a központi szerveren is lementi?

A laptop elvesztése/ellopása pedig az igazi rémálom kategória nemcsak a felhasználónak, hanem a vállalatvezetésnek is, különösen ha a laptopon harmadik féllel kapcsolatos bizalmas adatok is vannak.

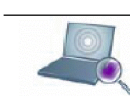
A kérdés tehát: mobilitás vagy biztonság?

Részmegoldások eddig is léteztek. A Bell Laboratórium fejlesztésével az Alcatel-Lucent Omniaccess 3500 kártyával azonban mobilitás és biztonság többé nem egymást kizáró fogalmak és sem a vállalati kommunikáció szabadságában sem biztonságban nem kell kompromisszumot kötni.

Képzeljünk el egy olyan PCMCIA kártyát, amely beépített moduljai (3G modem, VPN, személyes tűzfal, titkosító megoldás, GPS, beépített akkumulátor, Linux alapú saját op rendszer, API interfész) segítségével

- megvalósítja a laptop 7x24 órás adatbiztonságát, hozzáférését és menedzsmentjét;
- a végfelhasználónak növekvő teljesítményt és könnyű használhatóságot,
- az IT menedzsereknek láthatóságot és kontrollt;
- a vállalatnak drámaian csökkenő kockázatot és felelősséget nyújt;
- hatékonyan véd a laptopok elvesztésével és ellopásával szemben;
- biztosítja az üzletfolytonosságot;
- védelmet nyújt a zero day támadások ellen;
- kikényszeríti az IT policy teljes betartását mindig és mindenhol;
- lehetővé teszi az elvesztett vagy korrupt adatok gyors helyreállítását
- valamint a patcheknek holtidőben a laptopra installálását.

Az alábbi táblázatban egy bővebb funkcionális áttekintést kaphat, a bővebb információért azonban kérjük hallgassa meg munkatársunk előadását a ZMNE konferencián!

	IT probléma	Alcatel-Lucent Omniaccess 3500 Nonstop Laptop Guardian
	Ellopott vagy elveszt-ett laptop	Egyedi helymeghatározási és távoli adattörlő képességek: • Az IT ismeri a laptop helyét • Az IT biztonságosan menti a kulcsfontosságú adatokat a laptop-ról • Az IT eltávolítja a titkosító kulcsokat és törli az adatokat a lap-topról • Az IT visszajelzést kap, hogy az adatok biztonságban vannak
	Trójaival fertőzött laptop	Egyedülálló hálózati hozzáférés ellenőrzés. Az NLG: • Észleli, ha a laptop védelmét kikapcsolták • Blokkolja az IP hálózati hozzáférést és ellenőrzi a titkosítást • Riadóztatja a vállalatot a történtekről • Az IT megkezdi a helyreállítást a távolból
	Hitelesítés	A kártya egy integrált kulcsot nyújt a laptopnak: • Az IT bárhol és bármikor meg tudja vonni a hozzáférést a lap-tophoz • Policy alapú
	Adatvédelem	Beágyazott titkosító kulcsok: • Kulcsfontosságú adatok védelme a laptopon • A kulcsok a vállalati szabályok és a fenyegetettség alapján töröl-hetőek, újra generálhatók és cserélhetők • Teljes merevlemez titkosítás
	Mentés és visszaállítás	3G hálozaton keresztül történő mentés és visszaállítás képességek: • A titkosított adatok kártyára mentése • Mentési adatok automatikus továbbítása - akkor is, ha a laptop éppen ki van kapcsolva
	VPN használat	Automatikus VPN csatlakozás: • A felhasználó beavatkozása nélkül, mindig felépül a VPN kap-csolat, függetlenül a használt hozzáférési hálózattól (3G, WiFi, LAN)
	Patchek az idő 100%-ában	Minden patch installálása a laptopon: • A patch-ek tárolása a kártyán, bootoláskor azok azonnali telepíté-se
	Hamisítás védelem	Egyedülálló technológia: • Futó alkalmazások távolról megvizsgálhatók a laptopon • Az IT riadóztatása és a szükséges lépések megtétele, ha az Alcatel-Lucent Omniaccess 3500 Nonstop Laptop Guardian-ban vagy a laptop biztonsági beállításaban változás történik
	Laptop helyzete	GPS képesség: • Az IT és a felhasználó is hozzáférhet a hely alapú szolgáltatások-hoz
	3rd party integráció	Egy nyitott platform: • Egyszerű és nyitott API-k lehetővé teszik a 3rd party alkalmazá-sok számára a folyamatosan elérhető, helyfüggő és megbízható szolgáltatásokat • A vállalatok folytatólagosan használhatják a jól bevált alkalma-zásokat az Alcatel-Lucent Omniaccess 3500 Nonstop Laptop Guardian minden előnyével együtt

PÖLCZ Péter[105]

IP ALAPÚ REJTJELZŐ ESZKÖZ KÖRNYEZETI ÉS VÉDELMI RENDSZERÉNEK KIALAKÍTÁSA

Absztrakt: Jelen közleményben a szerző egy hazai viszonylatban korszerűnek tekinthető, IP alapú rejtjelző eszközfejlesztésével kapcsolatos műszaki-technikai kérdéseket világítja meg.

Kulcsszavak: IP, rejtjelzés, TCP/IP, védelmi rendszer.

1. Az eszköz rendeltetése

A IP rejtjelző eszköz a biztonságos és védett kommunikációt teszi lehetővé. Ennek elérésére a felhasznált algoritmus szerint 64-2048 bit mélységű titkosítást használ. Működése IP alapú hálózatokon keresztül történhet általában 100-1000 Mbps sebességgel (de vannak rendszerek amelyeknél már 5-10 Gbps sebességgel zajló átvitelről beszélhetünk). Az rejtjelzett adatátvitel számára közömbös, hogy az adatok számítógépes információk, vagy IP alapú telefonbeszélgetések, vagy videokonferenciák, esetleg rendszervezérlés, adat le- és feltöltés (megfelelő sávszélességek és módok megválasztása esetében).

2. A működtetéshez és elhelyezéshez szükséges tényezők

A rejtjelző eszköz elhelyezéséhez a következő információkat és adatokat kell figyelembe venni:

- A tápellátás: 110-230V, 50-60 Hz váltóáram;
- A rejtjelző eszköz felvett teljesítménye kisebb, mint 60VA;
- A rejtjelző eszköz a rátöltött algoritmusok és kulcsok nélkül, mint csupasz hardware nem képez adatvédelmi kockázatot;
- A rejtjelző eszköz elhelyezésére a környezet (telephely) elhelyezkedése és védelme alapján EUR 3-4 vagy BOVAS páncélszekrényben javasolt. Javasolt hogy a páncélszekrény belső zárható fiókkal rendelkezzen, melyben az eszköz és a médiakonverter kerül elhelyezésre;
- A rejtjelző eszközt befoglaló páncélszekrény az előző pontban leírtak mellet megfelelő zárszerkezettel kell, hogy ellátott legyen. (javasolt a mechanikus tárcsás kombinációs zár);
- Mivel a rendszer önvédő, a jelen leírásban később szereplő elektronikával kiegészítve így az önvédelmi funkciói azonnal reagálnak, ezért magára a páncélra a megfelelő minőség és zár mellett nem szükséges nyitási időzítés.(Ez lehetővé teszi, hogy a megfelelő jogosultsággal rendelkező személy rövid időn belül az eszközt használja, és azon forgalmazzon. Tehát nem szükséges a nyitási késleltetést kivárni, és ezzel esetleg az információ elévülését kockáztatni);

[105] Szerző: Pölcz Péter Attila, Védelmi Vezetéstechnikai Rendszerszervező MSc. szak másodéves hallgató, ZMNE BJKMK Híradó Tanszék, Codel Kft.

- A rendszerterv kialakításakor, figyelembe vettük, hogy magát a berendezést és védelmi rendszerét autonóm módon magára lehet hagyni, oly módon hogy az behatoláskor, illetéktelen hozzáférési kísérletekor, külső áramforrás megszüntetésekor önállóan és visszaállíthatatlanul törli a kulcsokat és rejtjelző algoritmusokat;
- A rendszer összeállításakor javasoljuk (de nem feltétlen szükséges, mivel a kommunikáció a rejtjelző és a számítógép között optikai kábelen megy, így az lehallgathatatlan), hogy az adatforrásként szereplő számítógépeket (lehetőleg TEMPEST minősítésűeket) ugyanazon páncélszekrényben kerüljenek elhelyezésre, mint a rejtjelző eszköz. (lásd javasolt összeállítás);

3. Az eszköz minősítése

A rejtjelző eszköz jelen algoritmussal és kulcsokkal (Triple DES és Rijndael AES), max 2048 bit kulcsmélységgel alkalmas a BIZALMAS információk védett küldésére, fogadására, illetve védett / rejtjelzett beszéd és videó csatorna kiépítésére. A rendszer hardverének módosítása nélkül, a berendezés alkalmassá tehető nemzeti TITKOS, SZIGORÚAN TITKOS, ÁLLAMTITOK minősítésű anyagok forgalmazására, az eszközt működtető szoftver (algoritmus) és kulcs cseréjével. (Jövőbeli funkciók).

4. A rejtjelző eszköz önvédelmi funkciói

A jelen rejtjelző eszköz logikai védelmét autonóm belső és fizikai külső részre osztjuk.

Az autonóm funkciók:

- A beállított szabályok szerint KEK, DEC kódok önálló cseréje, mely lehetővé teszi, hogy a kulcscserék automatikusan lezajlódjanak, és így a nyílt vonalon lévő adatok beavatatlannak keveredjenek;
- A hardverre csak feltölteni lehet a kódot és algoritmus, letölteni nem lehetséges, így az illetéktelen kezekbe kerülés esetén sem kell új algoritmus készíteni;
- A beépített önvédelmi funkcióknak megfelelően a mesterkulcs (fizikai kulcs) beállítása szerint a rejtjelző eszköz törli minden tartalmát, ha megmozdítják, illetve az operátora azonnali gombnyomással törlést kezdeményez;
- A rendszer rugalmasan kezelhető, és központilag a védett csatornán keresztül ellenőrizhető illetve menedzselhető;
- Kiegészítő elektronikával (5.sz ábra Zöld egység) külső behatolás védelmi rendszerrel (elektronikus biztonsági rendszer) összekötve behatolás, illetéktelen belépés esetén önműködően kulcs- és algoritmustörlés.

A fizikai funkciók:

- Az eszköz a fizikai kulcs beállításától függően, kerülhet önvédelmi, szállítási és törlési állapotba.
- Az önvédelmi állapot esetén (4. sz. Ábra) Függőleges kulcsállásban „B" állása kulcs kivételével a rendszer törli minden tartalmát, ha megmozdítják, vagy a törlési gombját megnyomják.(még áramtalanított esetben is).
- A törlési állapotba kapcsolás esetén (4. sz. Ábra), a „C" állásba fordítva a kulcsot a törlési gomb megnyomásával azonnali kulcs és algoritmustörlést hajt végre a rendszer. .(még áramtalanított esetben is).

- A szállítási (tansport) állapotba a rendszer önvédelme deaktiválásra kerül. Ilyen állapotba célszerű kulcs és algoritmus feltöltése nélkül szállítani.
- Az eszköz felnyitás ellen védett. Kinyitás és ennek kísérlete esetén a rendszer mind kikapcsolt (áramtalan esetben is) törli és megsemmisíti belső fizikai tartalmát.

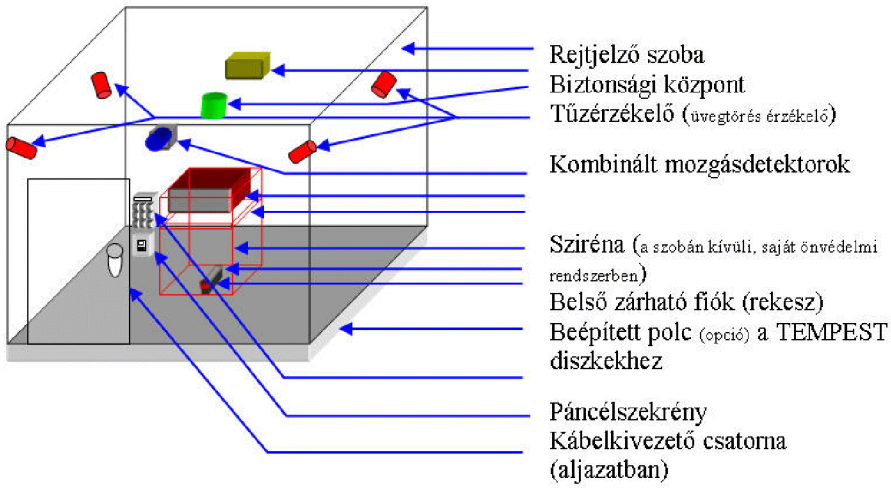
Az eszköz alkalmas arra, hogy minimális helyszíni felügyelettel a menedzselő központból új algoritmus és kulcsokat töltsön le és kezdjen használni. Az eszköz a fizikai kinyitási kísérletre helyreállíthatatlan állapotba kerül, így csak cserével javítható.

5. A rejtjelző eszköz környezeti kialakítása

A rejtjelző eszközt magába foglaló páncélszekrénnyel és szobával szemben támasztott követelmények kialakításánál figyelembe veendő tények:

- A szobának és az ajtajának kialakításakor legalább 20 perces ellenállási képességgel kell rendelkeznie;
- A páncélszekrénynek legalább 20 perces behatolási ellenálló képességet kell tudnia;
- Az alkalmazott mozgásérzékelő rendszer detektorainak kombinált (infra és radar) típusúaknak kell lennie;
- Az üvegtörés érzékelőt ugyanazon védelmi rendszerbe kell bekötni min a mozgásérzékelőket;
- A füst és tűzdetektorokat (az épület központi védelmén kívülieket) szintén a szoba védelmi rendszerének központjába kell bekötni;
- Az ajtóknak nyitásérzékelővel kell rendelkeznie, melynek a szobán belül és befúrt típusnak kell lenni és a szoba védelmi elektronikai központjába, kell bekötni. Lsd 1.sz lábjegyzet;
- Az ajtónak a külső és belső nyitását proximity kártya és a hozzá tartózó PIN kód megadásával a központi védelmi rendszer végzi (mágneszáras megoldással, javasoltak a síkmágneses zárak). Belülre lehetséges a vésznyitó gomb felszerelése;
- Az ajtó nem rendelkezhet kilinccsel, nyitását és zárását csak az elektronika végezheti;
- A szoba ajtajára mechanikus behúzó rendszert kell szerelni;
- Amennyiben a szoba ablakkal is rendelkezik, úgy az ablakokat is saját nyitásérzékelővel kell ellátni. (javasolt a biztonsági szabályzatokban előírt ablak magasság függvényében a rács használata, amennyiben nem lehetséges, úgy biztonsági fólia használata javasolt.);
- A szoba belátásvédelmét (ha van belátás) úgy függönnyel meg kell oldani;
- A rejtjelző eszközt (és a javasolt TEMPEST számítógép adathordozójának) tárolását végző páncélszekrény védelmét a mechanikus, kombinációs forgótárcsás számzárral kell ellátni;
- A páncélszekrényre nyitására időzítőt nem javaslunk egyéb megfontolások (gyors információközlés, még az információ elévülése előtt) miatt, valamint a védelmet a beépített elektronika látja el, a megfelelő időzítésekkel és a hozzájuk tartózó jogosultságokkal;

- A páncélszekrénynek rendelkeznie kell egy belső zárható fiókkal, melynek mérete legalább magas: 22 cm; széles: 50 cm; mély: 46 cm.



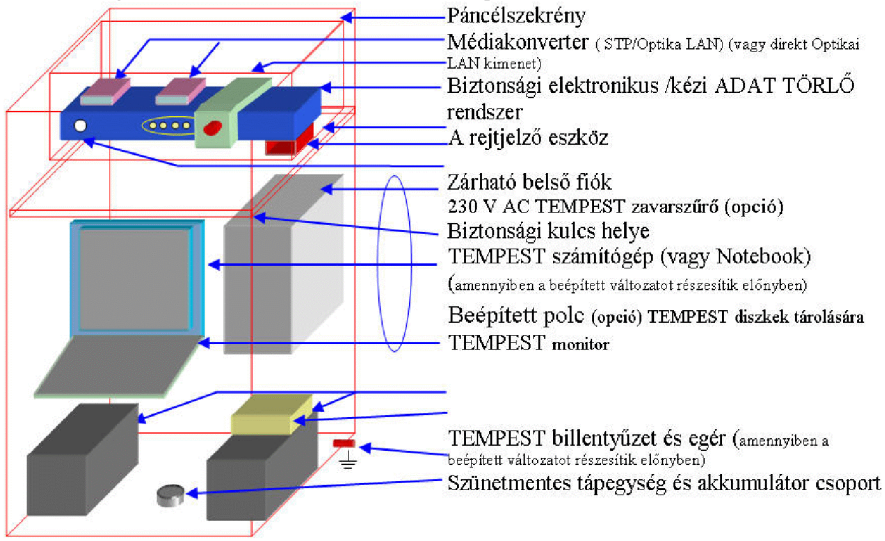
1. sz. ábra: kialakítás (forrás: szerző)

4. A páncélszekrény belső elrendezése

A páncélszekrény belső kialakításánál a következőket vettük figyelembe:

- A páncélszekrénynek az önvédelmi funkciók miatt nem szükséges extrém erős kivitelűnek lennie;
- A belső elrendezésnél a belső zárható fiók esetében a rendszer alkalmas a rejtjelző eszköz TEMPEST követelményeinek kialakítására;
- A kommunikációs, rejtjelző rendszer be- és kimenete optikai kábelen keresztül történik a lehallgathatóság kivédésére;
- A rejtjel eszköz fiókjára célszerű felszerelni egy 230V-os hálózati kapcsolót mellyel a fiók kinyitása nélkül a hálózat kikapcsolható;
- A rendszerrel lehetséges dolgozni zárt és nyitott nagyajtó esetében (mivel a kompromittáló kisugárzást jelentő eszközök a bezárt fiókban vannak.);
- A rendszer alkalmas arra, hogy a TEMPEST számítógépet, vagy notebookot is befogadja.
- A kialakításból adódóan, amennyiben TEMPEST számítógépet használunk, úgy lehetőség van (mindkét optikai szál –be és kimenet- kivezetésére) a teljesen zárt szekrény használatára;
- A szekrényben elhelyezett polc lehetővé teszi, hogy külső TEMPEST minősítésű számítógép adathordozóját a szekrényen belül elhelyezzük. (Figyelem: a szekrény önvédelmi rendszere csak a titkosítót és a hozzá tartozó sw-t védi, illetve illetéktelen hozzáférés esetén törli. Tehát az elhelyezett adathordozón lévő adatoknak rejtjelzetteknek kell lenniük és a hozzá tartozó kulcsok, és kártyát máshol kell tárolni.);

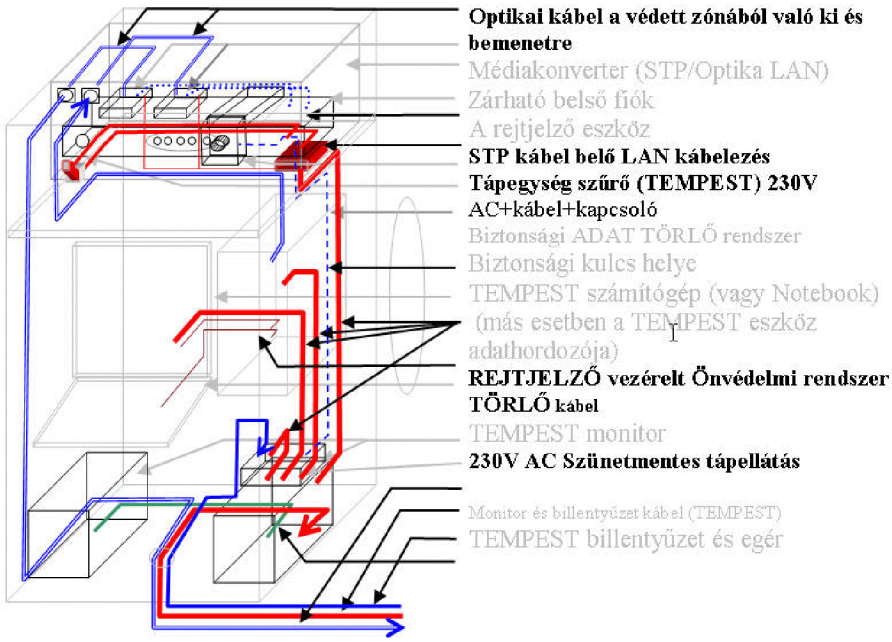
- Az önvédelmi rendszer központja saját akkumulátorral van ellátva így a rejtjelző eszköz védelmét ellátó akkumulátor csoporttól független rendszert alkot;
- Az akkumulátor csoport lehetővé teszi, hogy áramkimaradásos veszély esetén személyes beavatkozással a hálózatra még üzenetet lehessen küldeni.



2. sz. ábra: Páncélszekrény belső elrendezése (forrás: szerző)

5. A páncélszekrény belső kábelezése

A páncélszekrény és az abban elhelyezett eszközök védelmét maga a szekrény a benne és a környezetében elhelyezett elektronikai rendszerek és érzékelők közösen látják el. A páncélszekrényen belüli kábelezés nem kíván extra megoldásokat. Az egyetlen kiemelt védelmi pont a belső fiókban lévő rejtjelkészülék és média konverter melynek tápellátására TEMPEST tápszűrő alkalmazását javasoljuk. A kimenő adatvédelmet az optikai kábel megoldás biztosítja. A rendszer működőképességének és áthidalási időinek biztosítására használjuk a belső szünetmentes energiaforrást. Az energiaforrás kalkulációja és az áthidalási időit az energetikai kalkuláció adatlapja tartalmazza. A kivezető kábelek a páncélszekrény alján kialakított átvezető csatornán mehetnek. A biztonsági és vagyonvédelmi rendszer tápellátása a központból történik, mivel ez saját akkumulátorcsomaggal van ellátva a folyamatos működés és a szabotázsvédelem biztosítása miatt.



3. sz. ábra: Páncélszekrény belső kábelezése (forrás: szerző)

6. A rejtjelző eszköz kulcsbeállításai és biztonsági funkciók

Kulcsbeállítások, biztonsági funkciók:

- A rejtjelző eszköz helyes kulcskezelése elengedhetetlen feltétele a rendszer és önvédelmi funkciók szabályos működtetéséhez;
- A rejtjelző eszköz kiegészítésre került egy külső védelmi elektronikával, amely a szoba elektronikus védelmi rendszerével van összeköttetésben, illetve a külső védelmi rendszer jelzésére a eszközön a kulcs- és algoritmustörléshez szükséges gombot az elektronika megnyomja. Ugyanezen blokkon foglal helyet az azonnali kézi kulcs és algoritmus törlés gomb;
- A rejtjelző eszközön lévő kulcs mindig egyedi és géphez kötött.

Az egyes rejtjelző eszközökhöz tartozó egyedi kulcsot három y pozícióba lehet (A;B;C) elfordítani illetve kivenni (B). Az „**A" pozícióba** Fordított kulcs esetén a rejtjelző önvédelmi funkciói kikapcsolásra kerülnek. Ez a transzport vagy szállítási állapot. Mivel ezen esetben a rendszer szállítási állapotban van, így nem célszerű hogy ezen állapotában az „éles" kulcsokat és algoritmusokat a rendszer tartalmazza. A **„B" pozícióba f**ordított kulcs esetében mind a kulcs kivehető állapotba került. A kulcs kivételével így élesítjük a mozgásérzékelő és a biztonsági törlő rendszert. A szekrényben élesített állapotban így kell tárolni a berendezést. (A kulcsot másik szekrényben, más helyen kell tárolni a biztonsági okokból). A rendszer ez esetben is működőképes (rejtjelfunkciói mennek) csak az önvédelmi áramkörei is bekapcsolt állapotban vannak. Ebben az esetben, ha a kiegészítő áramkör és a hozzá tartozó mágnes a külső védelmi rendszer hatására, ha megnyomja a törlő gom-

bot úgy minden adatot, kulcsot és algoritmus azonnal kitöröl a rejtjelző készülékből. A rejtjelző ezen állapotában, ha manuálisan megnyomjuk a törlő gombot úgy az előzőhöz hasonlóan a rendszer teljes, és azonnali törlését végezzük el. A **„C" pozícióban a** rendszer a behelyezett kulcs esetén a törlőgomb megnyomásával azonnal kitöröl minden információt a rejtjelző eszközből. (Ebben az állásban a rejtjelző mozgásérzékelője nincs aktiválva.

7. A szünetmentes áramforrás kialakítása és ebből adódó védelmi funkciók

Energetikai Kalkuláció						
Sor	**Eszköz megnevezése (1)**	**Db (2)**	**Áramforrás (Volt / AC) (3)**	**Energia igény (Watt/db) (4)**	**Energiaellátás típusa (5)**	**Elvárt szünetmentes futás idő (percben / órában) (6)**
1	Rejtjelző	1	230	120	Szünetmentes APC	1020 / 17
2	Média konverter	2	230	15	Szünetmentes APC	30 / 0,5
3	TEMPEST tápszűrő	1	230	0,1	Transzparens APC	1020 / 17
4	Védelmi elektronika	1	230	20	Saját szünetmentes	5760 / 96
5	TEMPEST számítógép	1	230	250		
6	TEMPEST monitor	1	230	80		
7						
8	Összesítve APC		230	151 (1+2+3)	Szünetmentes APC	1020 / 17
9	Számolva APC verzió 1		230	180	APC Smart-UPS XL 750VA USB & Serial 230V + (1)UXBP24 Battery Unit	1177 / 19,6 max: 54,9 óra
10	Számolva APC verzió 2		230	180	APC Smart-UPS XL 750VA USB & Serial 230V + (2)UXBP24 Battery Unit	2390 / 39,8 max 111,5 óra

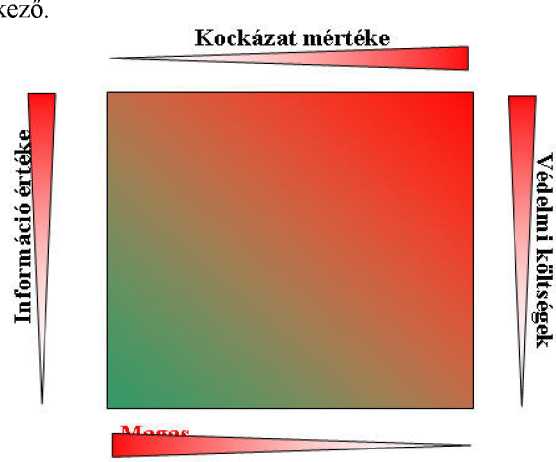
8. Reakció analízis

Reakció Analízis						
Sor	**Biztonsági szint (1)**	**Információ Minősítés (2)**	**Őrzés - Védelem formája (3)**	**Rendszer saját ellenálló képessége** (leggyengébb láncszem elvén) **Percben / Órában** (minimum) (4)	**Esemény (5)**	**Elvárható beavatkozás, Intézkedés típusa (6)**
1	Alacsony	Nyílt	Nincs	nincs	Nincs	Nincs
2	Alacsony	Bizalmas	Nincs	60 perc / 1 óra	Nincs	Analízis
3	Közepes		Elektronika	600 perc / 10 óra	Behatolás, Hozzáférés	Analízis, ha kell fejlesztés
4	Magas		Személy és Elektronika	2 880perc / 48 óra	Szabotázs, Behatolás, Hozzáférés	Azonnali személyes intézkedés, Analízis, Módosítás, Kulcs csere
5	Közepes	Titkos	Elektronika	3 000 perc / 50 óra	Szabotázs, Behatolás, Hozzáférés	Analízis, módosítás, Kulcs csere
6	Magas		Személy és	4 800 perc /	Konfrontáció	Azonnali

			Elektronika	80 óra	Szabotázs, Behatolás, Hozzáférés	személyes intézkedés, Analízis, Módosítás, Kulcs csere, Átkonfigurálás, Személycsere
7	Magas	Szigorúan titkos	Személy és Elektronika	10 080 perc / 168 óra	Konfrontáció Szabotázs, Behatolás, Hozzáférés	Azonnali személyes intézkedés, Analízis, Módosítás, Kulcs csere, Átkonfigurálás, Személycsere, Hatásanalízis
8	Extrém magas		Személy és Elektronika és Objektum	30 240 perc / 504 óra	Konfrontáció Szabotázs, Behatolás, Hozzáférés	Azonnali személyes intézkedés, Analízis, Módosítás, Kulcs csere, Átkonfigurálás, Személycsere, Hatásanalízis

9. Kockázati mátrix

A rendszer kiépítésének, valamint az adatvédelmi kockázatok összesítő mátrixa a következő.



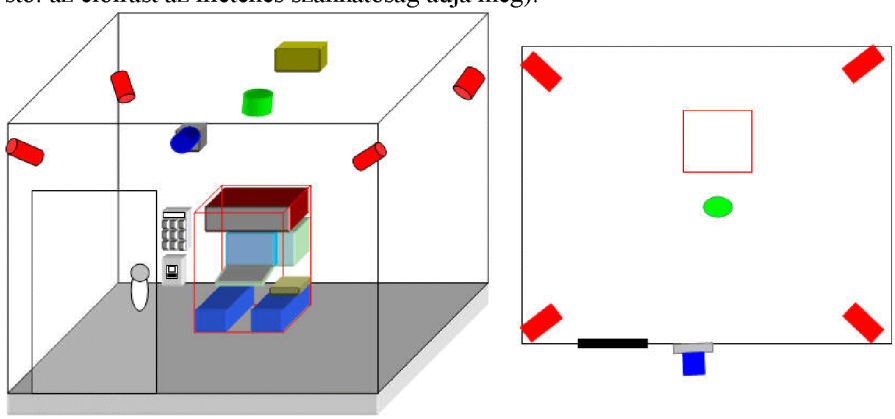
4. sz. ábra: kockázati mátrix (forrás: szerző)

A megfelelően pozícionált biztonság, védelem, költség és információ érték alapján tervezhető és számítható a szükséges anyagi emberi és technikai erőforrások mértéke. Az optimumra való védelmi törekvés, kockázatokat jelenthet egy „fontosabb" információ közvetítés és tárolás esetén. Ezen esetekben vizsgálandó az eltérés gyakorisága, és a kockáztatott információ(k) értéke, ezért a cselekvési és biztonsági szabályok és ráfordítások időszakos ellenőrzése szükséges. (Ezen tevé-

kenységes az illetékes hivatal illetve szakszolgálat kell, hogy ellássa). Az információvédelmi ellenőrzések gyakoriságát a hatályos törvények és jogszabályok határozzák meg. Az ellenőrzések és átminősítések időszakos gyakoriságba az adatminőség változásai a magukkal hordozott kockázati értékük szerint beleszólnak.

10. Az eszköz és a páncélszekrény a rejtjelszobában

Az eszköz elhelyezését a rejtjelző szobában javasoljuk. Nem javasoljuk a páncélszekrényt közvetlenül a fal mellé elhelyezni, ha a fal túloldalán lévő helyiség növeli a kockázatot, pl. ha a fal nem tömör és nem beton fal, ha a szomszédban nem saját terület van. (amennyiben a védendő szoba környezetében idegen személyek is tevékenykedhetnek, valamint a fal ellenálló képessége alacsony, pl. gipszkarton, akkor javasolt a radaros-mozgásdetektoros érzékelők kiegészítése falbontás érzékelő fejekkel-legalább a páncél háta mögötti rész esetében., a fal megerősítése stb. az előírást az illetékes szakhatóság adja meg).



5. sz. ábra: A rendszer elhelyezése térbeli és felülnézet (forrás: szerző)

A szobába való belépést a minősítés szintjének megfelelően lehet, illetve kell módosítani (ezen ajánlást és előírást a szakhatóság javaslatára kell elvégezi), javasolt a biometrikus azonosítás, pl. újlenyomat, írisz vagy tenyér érhálózati azonosítás. A védelmi rendszer élesítése csak a szobán belülről, míg deaktiválása csak a szobán kívülről (belépés előtt) lehetséges. Ezen eljárással megakadályozható, a „véletlen" belépés, riasztás és az elektronikai rendszer szükségtelen beavatkozása (kulcs, és algoritmus törlés). Az esetlegesen „mégis" bekövetkező jogosult belépés esetén a beriasztott és védett területre az illetőnek lehetősége van az elektronikus rendszer késleltetése idején a kulcs és kód ismételt megadására a beléptetési ponton. (Az eljárást és módszereket a szakhatóság határozza meg és ellenőrzi). A páncélszekrényen belüli önvédelmi rendszer ÉS kapcsolatban van a riasztó, és elektronikus és/vagy személyi védelmi rendszerrel, olyan módon, hogy amennyiben a területre történő illetéktelen behatolás történt ÉS az engedélyezett időn belül nem történik személyi vagy védelmi válaszlépés akkor a védelmi elektronika parancsot ad a rejtjelző eszköz kiegészítő áramkörének a kulcs és algoritmus azonnali törlésére. A mozgásdetektorok, falfúrás érzékelő detektorok, üvegtörés érzékelő detektorok jelzése valamint a páncélszekrény mozdítás érzékelőjének együttes hatására a

rendszer azonnali kód- és kulcstörlést kezdeményez. Mivel a szoba önvédelmi rendszerrel bír, ezért ezt menhelyként, menedékként, vagy menekülési helyként CSAK a rejtjel kulcsok és algoritmusok törlése után lehetséges. (mivel ezen esetekben a rendszer nem tudja az önvédelmi funkcióit ellátni (A kikapcsolt mozgás, behatolás érzékelők, és önvédelmi rendszerek miatt. Esetleges kábító gáz használat esetén a rendszer védtelenné válik, és a központ sem értesül időben az eseményről). Javasolt, a védelmi rendszer önálló figyelmeztető SMS küldése mellett, a riasztás tényének jelzése az épület biztonsági szolgálata, valamint a helyszínen tartózkodó saját erők számára, illetve lehetőség esetén akár a védett csatornán történő üzenetküldésre az eseményről.

11. Nem várt esemény bekövetkezése esetén az eljárási módok

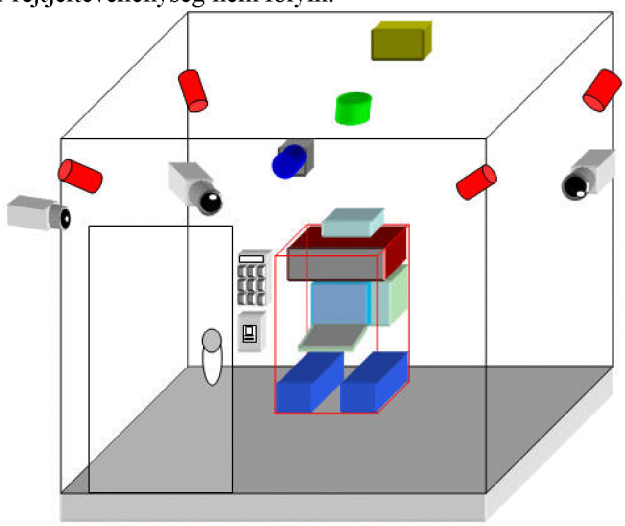
A nem vár események illetve a védett információk kiszivárgása, esetén a rendszer üzemeltetésétől és felügyeletétől elvárt cselekvéseket a következőkben foglalnám össze:

- **Azonnali személyes intézkedés:**
- Azonnali helyzetjelentés a központ felé;
- A további folyamatos személyi védelem megerősítése;
- Szükség esetén az információk kimentése illetve kijuttatása a mentési helyre;
- Szükség esetén azonnali információ és adat törlés, megsemmisítés (melyet a helyi jogosult vezető rendel el);
- A megbízott személyek, védelmi szakemberek azonnali beavatkozása, a központ azonnali értesítése a kiszivárgott információk felderítése illetve érzékenysége fokáról;
- A védett körzetbe történő belépési jogosultságok leszűkítése (maximum 3 főre);
- Az elektronikus védelem rendszer és a rejtjel eszköz azonnali kulcs cseréje;
- Az elektronikus védelem ellenőrzése, és újra aktiválása;
- A további információ- és adatkiszivárgás megszüntetése;
- Helyzetjelentés a megoldásokról és intézkedésekről a központ felé;
- Kommunikációs útvonalak cseréje (helyi biztonsági vetető elrendelése alapján);
- Más védett csatornák aktiválása.
- **Kulcs csere:**
- A rejtjelkulcsok azonnali cseréje;
- A rejtjel eszközön küldött utolsó üzenetek központi és helyi visszaellenőrzése;
- A központban az adatforgalmi naplók ellenőrzése az érintett eszközre az esemény bekövetkezte és az azt megelőző 1 napban (ha valami észrevétel van, akkor a kereséséi idő kiterjesztése nagyobb intervallumra).
- **Átkonfigurálás:**
- A rendszer analízis megkezdésével az érintett eszköz és az azon küldött üzenetek fokozott ellenőrzése;
- Az érintett eszköz központi átsorolása egy külön csoportba, melyen gyakoribb kulcscseréket végeznek, illetve a rajta küldött információkat az esemény bekövetkezte után az esemény súlyossága szerint meghatározott időpontig külön

visszaellenőriznek. (visszakérdezéses és ellenőrző kódú üzenetek forgalmazásával megerősítés);
- Az érintett eszköz kimeneti telefon, vagy kommunikációs vonalának lecserélése;
- A bejelentkezési azonosítók azonnali lecserélése.
- **Módosítás:**
- Az érintett berendezés KEK, DEK kulcscseréjének módosítása (megváltoztatása, gyakoribbá tétele);
- A bekövetkezett esemény, és az elvégzett környezeti és információs analízis szerinti védelmi rendszer cseréje;
- Amennyiben az esemény jellege megköveteli úgy az eszköz, vagy környezet megváltoztatása, a befogadó páncélszekrény lecserélése, a páncélszekrény kódjának megváltoztatása (ha az esemény szerint ez is elégséges);
- Az analízis eredménye szerint további érzékelők bekötése az elektronikus védelmi rendszerbe, vagy a meglévő érzékelők beállításának módosítása;
- Az elektronikus védelmi rendszer reakcióidejének időbeli változtatása (véletlenszerűen és csökkentett várakozási időkkel).
- **Analízis:**
- A helyzet kiértékelése, a sérült vagy kiszivárgott, vagy felderített információ kockázatának elemzése;
- Az információs vagy adatkockázat kitudódásának mértékében történő ellenintézkedések megtervezése és elrendelése;
- Az eseménysúlyosság környezeti okainak feltárása (biztonsági szabályok betartása, személyi felelősség megállapítása, információvédelmi szabályok átdolgozása, új szabályok beiktatása);
- A helyzet azonnali konszolidálása mellett, lényeges a kockázati mátrix szerint helyzetértékelés, valamint a várható kihatás és a módosítandó tényezők meghatározása.
- **Személycsere:**
- Az információvédelem megsérülése miatt azonnal el kell kezdeni a kapcsolódó személyek ellenőrzését és átvilágítását;
- Az adat és információvédelem sérülése miatt a közvetlenül és közvetve érintett személyek ellenőrzésével a közvetlenül felelős személyek felelőségi szintjei szerint a személyi döntéseket meg kell hozni.
- **Hatásanalízis**
- A rendszer ismételt működőképességének helyreállítása után azonnal meg kell kezdeni a közvetett és közvetlen károk felderítését és azok kihatásainak vizsgálatát a további működtetésre;
- A bekövetkezet eseményeket alapul véve a többi telepített helyre nézve szimulálni kell, és a szükséges módosításokat mint megelőző intézkedést kel foganatosítani;
- Károkozás és esemény bekövetkezte nélkül is javasolt időszakonként a telephelyeken a hibaanalízis, és hatásanalízis időszakos elvégzése, mivel a körülmények és az események dinamikusan változnak.

12. Rendszer kiegészítő lehetőségek

A rendszer kiegészíthető belső kamera rendszerrel és védett digitális videó rögzítővel vagy központtal, melyet úgy kell elhelyezni, hogy a tevékenységet nem, de a védett zónába való belépést, illetve mozgást rögzítse, illetve közvetítse azon időben mikor rejtjeltevékenység nem folyik.



6. sz. ábra: Kiegészítő lehetőségek (forrás: szerző)

Célszerű a rendszer saját tűzoltó védelmi rendszerrel ellátni, illetve ha az illetékes hivatal nem érzi ezt szükségesnek, akkor a tűzvédelmi rendszert a szoba saját védelmi rendszerébe bekötni. (Ez esetben tűz esetén, a rendszer törli a kulcsokat és algoritmusokat, tehát „illetéktelen" tűzoltók is beavatkozhatnak. A szigorúbb NATO szabályok szerint csak az arra kijelölt személyek illetve szervek végezhetnek oltó, mentő, biztosító tevékenységet a védett zónában.). Amennyiben a védett információ és rendszer megköveteli a hosszabb áramszünet esetére (vagy áramszünetnek álcázott akkumulátor lemerítéses támadás esetére) célszerű a védelmi rendszer saját aggregátorral történő tartalék áramforrásának biztosítása. A szoba védelmi és észlelő rendszerét NEM szabad összekötni más idegen védelmi rendszerekkel. A szobának csak a riasztó rendszerét szabad illetve célszerű bekötni az idegen védelmi rendszerbe, de oda is csak kijelzéses, riasztásos módban. Magasabb védelmi szintek estén alkalmazható még, passzív padozatra helyezett járásérzékelők valamint, infra- és, vagy lézersorompók kialakítása melyek szintén a saját szoba elektronikus központjába kerülnek bekötésre.

13. Összegzés, következtetések

Az IP alapú rejtjelző eszközök a felhasználhatóságuk sokoldalúságából adódóan, nagyon szenzitív eszközök, melyek környezeti és önvédelmi biztonsága illetve biztosítása ebből adódóan sokoldalú megfelelést és biztonságot követel. Napjaink és a jövő védett és biztonságos kommunikációját lehetővé tevő berendezések, és környezetük védelmét legalább olyan komolyan kell venni, mint a védendő infor-

mációt. Az információs rendszerek világában a legnagyobb érték maga a jó és pontos információ és adat. Az nyer, aki ezen adatokat mielőbb megszerzi, és oly módon juttatja el a feldolgozókhoz, és felhasználókhoz hogy annak tartalma a védettségéből kifolyólag mások számára rejtve és a biztonságosan jut át egy információéhes és nagyon kíváncsi hálózaton.

Felhasznált források:

[1] NATO rejtjel szabályzat
[2] 79/1995. évi kormányrendelet
[3] 1995/LXV tv.
[4] 164/2002. évi kormányrendelet
[5] MK ORF előírásai
[6] MK NBF előírásai
[7] Thales rejtjelző rendszerek kialakítása kézikönyv

Attila BLEIER

CHALLENGES OF THE 21ST CENTURY AND THE REQUIREMENTS OF THE HUNGARIAN ARMY

Introduction

From the 90' the way battles are being fought has gone through significant changes. There has been a progress in the 2nd wave material based warfare to the 3rd wave (4th generation) information based warfare. The NATO emphasizes this change in its doctrines and it appears in the Joint Forces Doctrines of the Hungarian Army. In this paper we will be looking for an answer to the following questions: which are those challenges that the communication system of the Hungarian Army has t o fulfill. In order to answer this, the Joint Forces Doctrine of the Hungarian Army will be evaluated in the light of the challenges of the 21st century.

Challenges of the 21st Century

By 2000 NATO has become the most powerful military alliance of the world, and with this NATO has accepted to give and adequate answer to the military and political challenges of the early 21st century. The most important challenges are the adequate answer to terrorism, and change of the warfare and the armed forces as the infocommunication technologies advance. In this paper we would like to deal with the latter question.

Fourth generation warfare

At the end of the 20th Century with the Gulf Wars, a new form of warfare – the so called - 4th generation warfare appeared. The 4th generation warfare emphasizes acquiring information superiority in order to achieve decision superiority and advantage. By having the proper information as soon as possible, decision makers can decide earlier and better which has a decisive effect on the battle.

Therefore it is crucial to acquire and maintain information superiority in present and future wars and crises. The question is which methods should be used to acquire and maintain information superiority. This set of questions – so called information warfare – are one of the most research topic in military and military technology science. In this paper we would like to focus on the communication technology related aspects of this.

Requirements of military IT applications for the communication network

NATO Network Enabled Capabilities doctrine emphasizes the usage of military information technology. Such systems are, for example, WWMCCS, GCCS, NMCS command control systems used by the US. Armed Forces, and JOPES operation planning system. The Royal Armed Forces in Great Britain use IARCCIS and THISTLE, the Bundeswehr (German Armed Forces) use HEROS command control system, ADLER artillery information system, EIFEL, which is information system of the German Air Force, the French Army uses SGEA and STRIDA. [Munk pp.131-164]

By using such systems it is required to rethink the present communication infrastructure. Former „voice-based" approach do not fulfill the requirements of the modern information and command& controll systems, as these applications generate tremendous amount of data traffic. A new – information centric – approach is required and the communication systems must be upgraded accordingly. This of course can not mean that the traditional systems should be replaced completely from day one, but a migration path is required from the present state to reach the future final state.

The other important change in military information systems are the integration of the different data and information systems – which requires stronger interoperability between the systems. This will mean of course lot of interoperability problems to fight with, but still this also implies that the systems providing different services should not be handled as separated systems, but should be handled as such system elements which provide a set of resources. This requires a new (information based) approach, where the resources are give and the communication system provide service via network resources. This approach is in line with the principles of the NATO Network Enabled Capabilities doctrine. [Munk p. 96-99]

In the long run, the spread of the Network Centric Warfare will be also a new challenge – this is also part of the NATO doctrine. In this concept every unit from the sensors to the execution units – every unit – is connected via (an IP based) communication network, which helps the different level decision makers , because they will be presented practically the same level of information – at the same time – as the executive units. The deployment of this concept require significant requirements for the battlefield, and the stationary communication systems.

The usage of the battlefield communication system will also significantly increase, since it can help the decision maker various ways. Eg. Sensors watching different signs of life functions, can continuously report about the status of the soldier to both the commander and the medical support team, or in case of armed vehicles the different sensors can send various reports about the status of the vehicle to the technical support team. Live video signals can be sent from the execution team. Of course these signals require the appropriate quality of service from the communication network, as the different data must be handled with different priorities and characteristics, in the battlefield and in the stationary communication system. Eg. These aggregated traffic, will result in increased amount of traffic and new way of handling in the stationary communication system.

Increase the level of mobility is also crucial, most importantly in the battlefield communication system. The technologies as Wimax emerge, and it is also likely that in certain cases EDR [PÁNDI2007] and civilian mobile technologies will in emergency situations be used [MAROS2005, MAROS2006]. A mutual benefit from these technologies are that they can be deployed relatively easily, quicly and as the situation demands it, but they provide significantly smaller bandwidth as compared to fiber.

Another important requirement is to increase the available bandwidth, the availability and resiliency in both the battlefield and the stationary communication systems.

The requirements defined by Joint Forces Doctrine of the Hungarian Army

The development path to be followed by the Hungarian Army is determine by the Joint Forces Doctrine (Összhaderőnemi Doktrína – ÖHD). The latest version was accepted in 2007 and it is under investigation, new version will come out probably early next year. A significant role is given for the C4 system in the new version but we are not covering in this chapter what the changes are, only the currently available version is being covered.. In this chapter the requirements for this research will be covered – and how the requirements defined by the ÖHD effect this field of research (stationary communication system of the Hungarian Army).

The Joint Forces Doctrine defines the tasks for which the Armed Forces of the Hungarian Republic must be prepared for. "The armed forces of the Hungarian Republic must be prepared for both conventional military defense operations and to solve those conflicts which directly effect the safety of our country or our allies, and mean a danger for the stability of our region." [ÖHD pp.11] The communication system of the Hungarian Army must be examined focusing on the following two task (eg. Defense operations and conflict handling operations). Traditionally defense operations are mostly helped by the inland stationary communication system , while the conflict handling operations are most probably handled by a field communication system, but the borderlines are not so strict.

The Joint Forces Doctrine also defines what sort of threats and conflicts must the Armed Forces be prepared for. The strengthening of the international terrorism is defines as one of the the most important threats which mean both the stationary and the field communication network must be designed and implemented in a way the it gives the necessary answer for this threat.[ÖHD pp.11] .

The doctrine defines the C4 system as a battle support force. [ÖHD p. 17], in connection with this 2 definitions need to be clarified: the definition of battle support and the relationship between the supporting and the supported parties. "The battle support means that the fighting force must be supported with reconnaissance data and fire power, providing support for executing its maneuver, and limiting the movement capabilities of the enemy forces, that contain air defense, the protection against mass destructions weapons, the electrical- , informational- , command-control-,psychological operations and the civil-military cooperation and public relations. [ÖHD pp 27]. As we can see , support with data and information is defined as a key aspect both directly and indirectly (via the electrical-, informational-, command-control, and psychological operations) – in which the C4 system plays a key role. The support with data and information, and the electrical-, informational operations are becoming more and more important, as they are required to achieve information (and later decision) advantage. This task puts the C4 sytem of the Hungarian Army into a crucial position.

The other important definition regarding the battle support is the relationship between the supporting and supported parties.[ÖHD p. 28-29]. The Joint Forces Doctrine defines the main principles regarding the so-called support service. A further step in this would be the support and service level agreement which is to be covered later.

Furthermore, there are several parts in the Joint Forces Doctrine where C4 system is given a crucial role. Eg. Definition of the command center , and the C4ISR centre is directly dealing with the forwarding of the information which is to be done on the communication infrastructure.

The 11th chapter of the ÖHD deals with the communication and information system which is defined by the Joint Forces Doctrine as follows:„a különböző vezetési szintek tevékenységéhez szükséges, rugalmasan változtatható, egységes elvek, módszerek és tervek alapján létrehozott; feladat, hely és idő szerint koordinált híradó és informatikai eszközök, eljárások, valamint az információs tevékenységeket végrehajtó szakállomány összessége." [ÖHD pp.87]. The Joint Forces Doctrine defines the communication and information system as a whole, in accordance with the NATO Doctrine – this implies a unified organization (this is currently not the case in the Hungarian Army). It is also important to note that the people responsible for the informations operations are also part of the communication and information system in this definition.

The following requirements are defined for the communication and information system in the Joint Forces Doctrine (grouped into 3 main groups):

- Operation, development and integration with the current systems: the communication and information system must be : standardized, compatible , interoperable, interchangeable, identical. These requirements are important to provide a unified system which brings operational and development benefits (Operational benefits eg.: less swap supply is needed, the costs of system integration and training is less, it is easier to solve the operation team, and the people have to learn less vendor-specific standards, it is easier to change from one system to another or maybe use another system as a backup – these are important benefits for the development of the systems
- Special military application requirements: high availability and quick reaction requirements. Eg. Reaction capability , reliability, firmness, resiliency, mobility and in-time operation. There are similar requirements present in the civil sphere, in the field of providing telecommunication service – so it is important that similar principles should be used at the Hungarian Army as at telecommunication providers.
- Information security requirementy: authentication, security , being hidden, electrical information security. This is a special requirement for the government and the military. This is of course are taken very seriously currently as well in the Hungarian Army.

The Joint Forces Doctrine defines the C4 system during different circumstances like in peace, catastrophy and war. In peace it is a system operated over the stationary system of Hungarian Army with peace-time staff, of which has the necessary capabilities to fulfill the requirements defined by the peacetime

command and control, training and operation. The conflict reaction operations and our NATO commitments require another important aspect – the interoperability capability with the different international systems. In war, based on the same basis the C4 system of the Hungarian Army must be capable of Joint Forces planning, command and control support and to support the NATO defense forces. [ÖHD p. 87-92]

The main requirement defined by the Joint Forces Doctrine for peacetime is that the C4 should be design for the support of the activities of the user, a.k.a it must be user-friendly, and in terms of capabilities it must be designed for wartime application[ÖHD p. 87-92]

As mentioned earlier, the Joint Forces Doctrine of the Hungarian Army considers the information operation team as part of the C4 system, therefore the information operations are tasks of the organization responsible for the C4 system. The information operations are defined in the 12th chapter of the Doctrine. [ÖHD p. 93-97]

The infocommunication system is part of the definitions of the information (measures and counter-measures) operations. This area of warfare develops dynamically, and is given a higher priority in the NATO forces as well. The military activities and capabilities of the information operations are done in the communications centers. The Doctrine defines the communications centers as critical nodes, by losing certain capabilities of the node can have a serious impact on the Command and Control capabilities.[ÖHD p. 97]. Therefore it is high priority to have a constant defense of the stationary and field communication centers – from any kind of attack. .

Electrical warfare is also defined in conjunction with C4 system [ÖHD p. 109-112]. The communication centers are primary target for the electrical warfare, therefore the defense against any type of electrical attack is an important priority when designing and implementing a C4 system. There are also further – less important - references to the C4 system in the Joint Forces Doctrine.

As we can see the principles defined in the previous chapter – the capability of system integration, information operations and mobility are considered as a high priority in the Joint Forces Doctrine of the Hungarian Army. However the leading nations of the NATO consider a more important role for the C4 system eg on the field of information operations or stationary and field communication. These changes will hopefully be reflected in the new, revised version of the Doctrine.

Summary

The new millennium has brought new challenges for both the Hungarian and international infocommunication systems for military applications. The most important challenges are the evolving 4th generation information-centric warfare, and the serving the needs of the military information and communication system which are being used on a broader scale, and the support of new military infocommunication concept has been mentioned in the second chapter.

In the third chapter the requirement of the Joint Forces Doctrine have been highlighted – and what sort of prerequisite and needs are defined in the Joint Forces Doctrine in my field of research eg the communication and information

system of the Hungarian Army. The doctrine has also been compared with the requirements defined in the second chapter, how much the Hungarian Army fulfills those challenges defined in the first chapter.

In this chapter I highlighted that the Joint Forces Doctrine defines the communication and information system of the Hungarian Army, as a battle support system. I also suggested a new approach in the supporting / supported relationship. I have defined the main principles (system integration, military technical and security especially information security principles) for grouping the requirements defined in the Joint Forces Doctrine. I have emphasized that the information operations are tasks of the team responible for the communication and information system.

The Joint Forces Doctrine defines the main principles for the design and operation of the communication and information system of the Hungarian Army. This principles suggest that methods and devices used for high availability networks in civil life can be applied, taken into consideration the special needs of the military application.

Rövidítésjegyzék

WWMCCS – World-Wide Military Command and Control System (Világméretű katonai vezetési rendszer)

GCCS – Global Command and Control System (Globális vezetési és irányítási rendszer)

NMCS – National Military Command System (Nemzeti katonai vezetési rendszer)

JOPES – Joint Operation Planning and Execution System (Összhaderőnemi hadművelet-tervező és végrahajtó rendszer)

IARCCIS – Interim ACE Rapid Reaction Corps Information System (ACE Gyorsreagálású hadtest átmeneti informatikai rendszere)

HEROS – Heeres Führunginformations System (für die rechnerunterstützte) Operationsführung in Staeben (Csapatvezetési információs rendszer, hadműveleti vezetés a törzsekben)

ADLER – Artillerie-, Daten-, Lage- und Einsatz-Rechner (Tüzérségi, adat, helyzet és bevetési számítógép hálózat

SGEA - Systéme de Guerre Électronique de l'Avant (Elektronikai hadviselési rendszer)

STRIDA – Systéme de Traitment et de Représentation des Informations de Défense Aérienne (Légvédelmi információk kezelésének és megjelenítésének rendszere)

TDM – Time Division Multiplex (Időmultiplexált)

IP – Internet Protocol (Internet Protokoll)

QoS - Quality of Service (Szolgáltatásminőségi paraméterek)

SLA – Service Level Agreement (szolgáltatási szint szerződés)

BER – Bit Error Rate (Bithibaarány)

round trip delay – az a késleltetési idő amíg egy IP csomag egy útvonalat oda – vissza megjár

MPLS – Multiprotocol Label Switching – többprotokollos címkekapcsolás

ZMNE – Zrínyi Miklós Nemzetvédelmi Egyetem

IETF – Internet Engineering Task Force – szabványügyi szervezet

IEEE - Institute of Electrical and Electronics Engineers, Inc – szabványügyi szervezet

ITU – International Telecommunication Union – szabványügyi szervezet

ETSI – European Telecommunication Standard Institute

Wimax - Worldwide Interoperability for Microwave Access – Vezetéknélküli adatátviteli szabvány

UMTS – Universal Mobile Telecommunication System – 3-dik generációs mobiltelefonia szabványrendszere

STANAG - Standardization Agreement – NATO szabvány

NATO – North Atlantic Treaty Organization - Nemzetközi védelmi szövetség

AARMS - Academic and Applied Research in Military Science – ZMNE nemzetközi folyóirata

Felhasznált Irodalom

[1] Kommunikáció 2005 I.-II., Communications 2005 I.-II., 2005/10 Zrínyi Miklós Nemzetvédelmi Egyetem, Zrínyi Miklós kiadó, Budapest, p. 601 ISBN 963 7060 11 1

[2] Kommunikáció - 2006, Communications - 2006, 2006/10 Zrínyi Miklós Nemzetvédelmi Egyetem, Zrínyi Miklós kiadó, Budapest, p. 391, ISBN 978-963-7060-18-2

[3] Kommunikáció 2007 I.-II., Communications 2007 I.-II., 2007/10 Zrínyi Miklós Nemzetvédelmi Egyetem, Zrínyi Miklós kiadó, Budapest, p. 511, ISBN 978-963-7060-31-1

[4] Dr. Munk Sándor: Katonai informatika a XXI. század elején, 2007, Zrínyi Kiadó, p. … ISBN: 978 963 327 419 4

[5] dr. Rajnai Zoltán, dr. Fekete Károly: Tanulmány a Wimax használhatóságáról a Magyar Honvédség hírrendszerében, 2007

[6] dr. Haig Zsolt: Információs műveletek I-II jegyzet, 2008

[7] dr. Haig Zsolt, dr. Vass Sándor, dr. Ványa László: Elektronikai Hadviselés, 2008

[8] dr. Haig Zsolt: Integrált felderítés és elektronikai hadviselés, jegyzet, 2008,

[9] http://www.wikipedia.org

[10] [MAROS2005] Maros Dóra, Mészáros Árpád

[11] Kommunikáció 2005 I.-II., Communications 2005 I.-II., 2005/10 Zrínyi Miklós Nemzetvédelmi Egyetem, Zrínyi Miklós kiadó, Budapest, p. 601 ISBN 963 7060 11 1,pp.203-209

[12] [MAROS2006] Maros Dóra

[13] Kommunikáció - 2006, Communications - 2006, 2006/10 Zrínyi Miklós Nemzetvédelmi Egyetem, Zrínyi Miklós kiadó, Budapest, p. 391, ISBN 978-963-7060-18-2 , p. 154-168

[14] [PÁNDI2007] Pándi, Erik, Pándi , Balázs

[15] Kommunikáció 2007 I.-II., Communications 2007 I.-II., 2007/10 Zrínyi Miklós Nemzetvédelmi Egyetem, Zrínyi Miklós kiadó, Budapest, p. 511, ISBN 978-963-7060-31-1, pp.254-260.
[16] [ÖHD] A Magyar Honvédség Összhaderőnemi Doktrínája, 2003-as kiadás
[17] [Munk] Dr. Munk Sándor: Katonai informatika a XXI. század elején, 2007, Zrínyi Kiadó, p.264, ISBN: 978 963 327 419 4

Álmos DINNYÉS –Erik PÁNDI[106]

THE IRISK SOFTWARE TO SUPPORT THE EXTENDED HAZOP ANALYSIS

Abstract: *The HAZOP analysis is used to identify the week points of processes, and to collect suggestions to reduce the risks. The disadvantage of this method is that it doesn't take financial aspects into consideration. The iRisk software is based on the principles of the HAZOP analysis, but extends it with financial aspects in terms of possible causes and of the suggested actions and changes. This software will also give a clear view on the possible problems - like missing documentation (e.g. manuals, safety instructions) or duplications - within the company's documentation management. The iRisk software was applied at the analysis of the ammonia factory at the Nitrogénművek Rt. (Pét, Hungary).*

Keywords: HAZOP analysis, risk assessment, risk management, documentation managemen.

1. Introduction

Companies using quality assurance, environmental protection and safety management systems need to rationalize their operation and organizational structure that means the redundancies in the organizational structure and in the documentation system have to be eliminated, and the standalone management systems have to be harmonized [1]. The result of such a rationalization will be an integrated management system with parallel working management subsystems linked with each other by integrating systems that are the common

- documentation management;
- training;
- controlling;
- and risk management systems.

The iRisk software has been developed as an IT support tool for the risk management system [2]. This software helps not only to collect and analyze risk information, it will be linked to the controlling system and to the documentation management system. The iRisk software is based on the principles of the HAZOP analysis, but extends it with a financial aspect, this is why it will give a comprehensive view about the processes. The software is made up of a Microsoft Access database and a graphical user interface (GUI) developed in Visual Basic 6.0 programming language. The iRisk software was tested in the ammonia factory of the Nitrogénművek Rt. (Pét, Hungary).

2. The iRisk database

This software is used to support collecting data at on-site workshops with various teams, this is why the software has only restricted network support. This means, only eight users are able to access the database at the same time directly

[106] authors: Álmos Dinnyés PhD, Pelikan Hardcopy International AG, IT Support; asc. prof. Erik Pándi PhD, ZMNDU, Department of Communications

with the MS Access application or through the graphical user interface of the iRisk. It is also possible using database-replicas for working without network connection, in this case the replicas have to be synchronized with the master database regularly. In order to keep the integrity of the database the built in cascading functions are in use. The MS Access database of the software contains the information below:

- the structure of the organization:
- companies;
- factories;
- the operational parameters of the processes;
- the guide words that describes the possible deviations; additional information to the guide words:
- related documentation;
- alarm, signaler and intervening systems;
- causes of the deviations;
- the consequences of the deviations;
- suggestions to decrease the risks.

3. The iRisk GUI

The iRisk software has an easy-to-use graphical user interface (GUI) with multilingual support: the user can select the language at the start. The translations of the GUI are kept in the "Languages" table of the database, and additional language support can be appended easily. The default operations on the forms are:

- adding new items,
- modifying and,
- deleting existing items.

The iRisk GUI offers two ways for the data entry: new values can be entered manually or any existing values can be selected from lists in order for fast data entry. If the user try on the graphical user interface to execute an operation with insufficient data an error message will pop up and the operation will be canceled.

4. The structure of the organization

The software uses a 3 levels structure to store the process information. It is suggested to use the first level for company information, this will make comparative analysis possible. On the second level can be defined the factory or the site, and the third level is for processes. The enterprize hierarchy can be set up of course in various ways. If no comparative analysis is planned (e.g. in case of small enterprizes) the first two levels can be the same, or the second level can be used for processes so that the third level can be more detailed. The term "process" means in case of iRisk a part of the operational process, which has unambiguous input and output, can be identified and its length is manageable for the analysis. If it is required it is possible to add more level with the slightly modification of the database and the GUI.

5. The operation parameters

Edit, delete or add operation parameters for the selected process can be done on the operation parameters maintaining form. The mandatory fields on this form are

the description of the parameter and the expected value in normal circumstances. The iRisk software adds unique key to each parameter in order to prepare them for reporting [3].

6. Guide words

The guide word maintenance formis the most important part of the iRisk software. The guide words (e.g. no, more, other than, higher than) describe the possible deviations from the normal operation. Properties of the selected operation parameter by guide words are summarized on this form:

- Consequences;
- Causes;
- Instruments;
- Safety tools;
- Documentation;
- Suggestions.

In the top left corner of the guide words maintenance form can be seen in not editable textboxes the selected enterprize, factory, process and operation parameter. The guide words can be selected from the list in the top right corner of the form. At the bottom of the form are the consequences and causes linked to the selected guide word. The additional data of the deviation described with the current guide word can be accessed using the buttons at the bottom of the form. The key of the successful analysis is to prepare all the necessary information and documentation before starting the workshop, and it is highly recommended to involve the top management in the risk assessment process.

6.1. Consequences

The consequences form is to maintain information about the direct and indirect consequences of the deviation:

- short description of the possible damage;
- the frequency of the possible damage;
- direct or indirect consequence;
- the financial consequences of the the possible damage.

In order to determine the financial effects of the deviation the consequences have to be detailed so that as many the factors have to be taken into consideration as it is necessary. For example in case of an accident in the workplace the factors below have to taken into consideration:

- outage because of the accident;
- new safety tools;
- costs of the investigation and documentation of the investigation of the accident;
- compensation;
- penalty;
- penalty;
- costs of the replacement of the injured employee (training of a new employee and/or overtime);
- others.

6.2. Causes

The causes form contains information about the direct and indirect causes of the deviation:

- direct or indirect causes;
- description of the cause.

The details of the causes - like in case of the consequences - can be seen not on the guide words maintenance form, but on this subform.

6.3. Instruments

In this part of the software are stored the basic information of the display and signaling instruments and of the intervention systems related to the selected guide word. In the description field a unique identification number has to be entered for the reporting. In case of the analysis at the Nitrogénművek Rt. the identification numbers from the ISO process descriptions and flowcharts were used.

6.4. Safety tools and equipments

This iRisk form shows the list of the applied safety tools and equipments to reduce the risk of injury.The mandatory fields are in this case only the description of the safety tool (e.g. extinguisher) and safety equipment (e.g. gas mask). It is highly recommended to enter the details (e.g. manufacturer) as well.

6.5. Documentation

On the documentation form are listed all risk management documentation, user manuals, process descriptions, instructions and emergency recovery plans. The documentation data sheet contains the following fields:

- the identification number and name of the document (including the related chapter or page number of the document if necessary);
- type document:
- general documentation related to the operation parameter (e.g. related instructions of the quality management and/or environmental protection system);
- documentation concerning to the instrument (e.g. maintaining plan, certification plan);
- safety instructions (e.g. fire protection and evacuation plan);
- others if requested.

This feature of the iRisk system is used to discover the problems - holes or duplications - within the documentation system. At the end of the analysis the iRisk will list the operation parameters without adequate documentation - e.g. lack of the emergency plan - priorized by risk [4]. If the company uses document management system it is recommended to enter the network address (URL) of the document in order to create a relation between the two systems.

6.6. Suggestions

The other very important iRisk form is the suggestions maintenance. This form is to collect all suggestions to reduce the risk level. The iRisk allows to enter practically unlimited number of suggestions. The mandatory fields of this form are:

- the description of the suggestion;

- expected effects of the realization of the suggestion;
- expected financial effects (decreasing costs and/or raising the incomes) of the realization of the suggestion. The standard HAZOP method doesn't require any financial information, but in the extended HAZOP analysis it is required to estimate the financial effects of the suggestions. Therefore it is recommended to collect the suggestion in - at least - three steps. In the first step all risk reducing ideas are collected with a team using brain storming techniques. In the following step these ideas have to be cleaned and specified and entered into the iRisk system [5]. The final step, the priorization is made by the iRisk software.

7. Reporting

The iRisk software includes reports that are necessary for the risk analysis. These reports are Access parameterized queries, this tool can be used also to modify existing and developing new reports. The reports can be exported into various formats (e.g. xls, csv) or even directly into the database server (e.g. MS SQL server) of the company's controlling system for further processing. The standard iRisk reports are the followings:

- HAZOP report;
- Suggestions ordered by priority;
- Operation parameters and guide words without documentation.

8. Summary

The extended HAZOP analysis supported by the iRisk software gives information not only about the risks of the company, but its results can be used to define a strategy to optimize the risks, to explre and to solve documentation problems. Although the software was tested in the chemical industry it is capable to use in various areas.

References

[1] Szalai, Sándor – Mika, János: Az új évezred környezeti kockázatai, Védelem, Budapest, 1998, ISSN 1218-2958, pp 45, No 5, Vol 1998;

[2] Póserné Oláh, Valéria: IT kockázatok, elemzésük, kezelésük, Hadmérnök, Budapest, 2007, ISSN 1788-1919, pp 207-208, No 3, Vol 2007;

[3] Kaplan, Robert S. – Norton, Peter D.: Eszköz, ami mozgásba hozza a startégiát – Balanced ScoreCard – Kiegyensúlyozott startégiai mutatószámrendszer, KJK Kerszöv, Budapest, 2002, ISBN 963 224 816 3, pp 42-43;

[4] Nagy, Rudolf – Halász László: Monitoring és lakossági riasztó rendszer és a kritikus infrastruktúra-védelem összefüggései, Hadmérnök, Budapest, 2008, ISSN 1788-1919, pp 70-72, No 2, Vol 2008;

[5] Ipari biztonsági kockázatkezelési kézikönyv, KJK Kerszöv, Budapest, 2004, ISBN 963 224 816 3, pp 207

TAKÁCS Attila[107]

AZ E-KORMÁNYZAT ÉS AZ INTEROPERABILITÁS NÉHÁNY KÉRDÉSE

Absztrakt: Európában az e-kormányzat (elektronikus kormányzati eszközök) mára minden szinten jól beágyazódott a közigazgatási szakpolitikák és tervek közé mind helyi, mind regionális, mind nemzeti és pán-európai szinten. Európai szinten az eEurope 2005, és jelenleg az i2010 cselekvési tervek hangsúlyozzák az e-kormányzat fontosságát és szólítanak fel gyors előrehaladásra [1]. Az egyablakos és az összekapcsolt kormányzás megvalósításáról könnyebb beszélni, mint megvalósítani azt. A polgárok igényeinek megfelelő szolgáltatások biztosításához szükségszerűen együttműködést kell kialakítani a közigazgatási szerveken belül és azok között és ehhez alapvetően meg kell változtatni az állami szektor eljárásmódját, működési elvét [2]. Számos alkalommal a polgárok igényeinek ténylegesen csak a hagyományosan különböző közigazgatási szervek által nyújtott információk, illetve szolgáltatások összegzésével lehet eleget tenni. Sőt, a polgároknak a szolgáltatás-ellátás középpontjába helyezése inkább arra utal, hogy ugyanazon szolgáltatás eléréséhez több kommunikációs csatornával kellene ellátni őket. E hatalmas korszerűsítési munka során a Kormányzat hamar felismerte az interoperabilitás (IOP) jelentős szerepét. A szerző jelen publikációjában, kormányzati anyagokra támaszkodva összefoglalja az e-kormányzat és az inetroperabilitás néhány, a napjainkat is meghatározó kérdéseit.

Kulcsszavak: e-kormányzat, információtechnológia, interoperabilitás.

1. Bevezetés

Az egyablakos és az összekapcsolt kormányzás megvalósításáról könnyebb beszélni, mint megvalósítani azt. A polgárok igényeinek megfelelő szolgáltatások biztosításához szükségszerűen együttműködést kell kialakítani a közigazgatási szerveken belül és azok között és ehhez alapvetően meg kell változtatni az állami szektor eljárásmódját, működési elvét. Számos alkalommal a polgárok igényeinek ténylegesen csak a hagyományosan különböző közigazgatási szervek által nyújtott információk, illetve szolgáltatások összegzésével lehet eleget tenni. E hatalmas korszerűsítési munka során hamar felismerték az interoperabilitás (IOP) jelentős szerepét. Első pillantásra is látszik, hogy az összes interoperabilitási akadály legyőzése nem lesz egyszerű feladat. Egyes esetekben a hatóságok a jogi korlátok miatt nem cserélnek adatokat, vagy azért mert nincsenek olyan jogszabályok, amelyek kötelezővé tennék a hatóságok közötti együttműködést, vagy azért mert az adatvédelmi és a személyiségi jogokat védő törvények nem teszik lehetővé, hogy a közigazgatási szervek kicseréljék adataikat. Ezeken túlmenően, még a szükséges jogi keretek megléte esetén sem lesz egyszerű dolog megszervezni a megfelelő munkafolyamatokat a szervezetek között és a szervezeteken belül. Ugyanakkor még abban az esetben is, ha ez megoldódik, akkor is szükséges, hogy az összes

[107] szerző: Takács Attila, PhD-hallgató, ZMNE KLHK Hadtudományi Doktori Iskola

együttműködő hatóság egyetértsen a cserélt adatokra vonatkozóan. Végezetül, az automatikus adatcserének technikailag megvalósíthatónak kell lennie még azokban az esetekben is, ahol a résztvevő közigazgatási szervek eltérő információs rendszerekkel rendelkeznek. Az e-kormányzati projekteket politikai okokból gyakran rövid idő alatt kell megtervezni, kialakítani és leszállítani. Ennek gyakran az lett az eredménye, hogy Európa különböző részein több hasonló projektet és programot találtak ki újra meg újra, ami meglehetősen komoly fejlesztési költségekkel járt. Ez különösen igaz a regionális és helyi kezdeményezések esetében, amelyek gyakran nem vették figyelembe a máshol már létező helyes gyakorlat példáit, amelyek átvehetők és a helyi körülményekhez igazíthatók lettek volna.

2. Fogalmi háttér

Az e-kormányzat nem más, mint az információs és kommunikációs technológia használata a közigazgatásban, kombinálva a szervezeti átalakítással és az új készségek fejlesztésével – a közszolgáltatások és demokratikus folyamatok tökéletesítése és a közpolitikák támogatottságának erősítése érdekében. [3]. Az irodalomban egyesek ennél a széles értelemben vett meghatározásnál inkább az „eGovernance" (e-kormányzás) kifejezést használják, jelen közlemény, igazodva az uniós nomenklatúrához az „e-kormányzat" (e-kormányzat) kifejezést alkalmazza. Az interoperabilitás alatt az információs és kommunikációs technológiai (ICT) rendszerek és az általuk támogatott ügyintézési folyamatok azon képességét érti a publikáció, amely lehetővé teszi a folyamatok közötti adatcserét és az információk és tudás kölcsönös megosztását [4].

3. Az interoperabilitás típusai

Az e-kormányzati IOP elemzésénél lényeges, hogy megfelelő tipológiát használjunk. Jelenleg számos javaslat létezik az IOP tipológiákra vonatkozóan [5]. Az Európai Interoperabilitási Keretrendszer által bevezetett IOP tipológiáját (EIF) elfogadva az alábbiakat kell figyelembe venni [6]:

a) technikai IOP aspektusok. A technikai interoperabilitás a számítógépes rendszerek, és szolgáltatások összekapcsolásának technikai kérdéseire vonatkozik;

b) szemantikai IOP aspektusok. A szemantikai interoperabilitás biztosítja a kölcsönösen megosztott információ pontos jelentésének érthetőségét bármely más alkalmazás számára, amelyet eredetileg nem erre a célra fejlesztettek ki. A szemantikai interoperabilitás lehetővé teszi, hogy a rendszerek összekapcsolják a kapott információt más információs forrásokkal, és azt érthető formában dolgozzák fel;

c) a szervezeti IOP aspektusok. A szervezeti interoperabilitás meghatározza az ügyviteli eljárásokat, és lehetővé teszi azon szervek közötti együttműködést, amelyek információt kívánnak cserélni, de eltérő belső struktúrákkal és folyamatokkal rendelkezhetnek, továbbá meghatározza a felhasználói közösség szükségleteire vonatkozó aspektusokat is;

d) az IOP irányítást az Európai Közigazgatási Hálózat (EPAN) 5. sz. e-kormányzat Munkacsoport megállapításainak megfelelően egy újabb, kutatást igénylő fontos megfontolásnak kell tekinteni. Az IOP irányítás azokkal a politikai, jogi és strukturális feltételekkel foglalkozik, amelyek

alapvető fontosságúak az interoperábilis alkalmazások kifejlesztése és használata szempontjából [7].

4. Az interoperabilitás irányítása

Az EPAN szerint az interoperabilitás irányítása a szervezetek belső és külső határain átnyúló ügyintézési folyamatok és információs architektúrák koordinációját és egymáshoz hangolását jelenti. Célja bármely lehetséges akadály, beleértve a törvényi, kulturális és egyéb akadályokat is, azonosítása, kezelése, illetve elhárítása annak érdekében, hogy meg lehessen valósítani a szolgáltatások összesítését és az információ kölcsönös megosztását. A tipikus érdekeltségi helyzet arra enged következtetni, hogy több olyan közigazgatási szerv van, amely kész együttműködni, hogy összevont e-kormányzati szolgáltatásaikkal jobban meg tudjanak felelni a polgárok szükségleteinek (például a családi események kapcsán). Ezen a szinten az alábbi kérdéstípusokkal kell foglalkozni:

a) vannak-e jogi megszorítások, és azokat hogyan lehet elhárítani?

b) melyik szerv felelős a megfelelő IOP szabványok létrehozásáért és fenntartásáért?

c) megvannak-e a szükséges készségek?

d) hogyan lehet kifejleszteni az „együttműködés kultúráját"?

e) hogyan kell kezelni a változást?

f) ki dönt az együttműködés módjáról?

A kutatás kezdőpontját a virtuális vállalkozásokkal foglalkozó irodalom írja le, amely szerint a koordinációt különböző modelleknek megfelelően lehet megvalósítani, ezek között az alábbiak találhatók [8]:

a) hierarchikus modell, amelyben az egyik szervezet kezdeményezi a folyamatot és eldönti a workflow végrehajtásának módját. Ez a modell további alkategóriákra bontható attól függően, hogyan alakítja ki a folyamat kezdeményezője a workflow formáját:

központosított, ahol az egyik domináns vagy delegált szerv önkényesen dönt a formáról. Résztvevő, ahol a workflow formájáról meghozandó a döntéshez a folyamatban részt vevő összes szervezettel konzultálnak. Decentralizált, ahol az egyes szervezetek önállóan döntenek a teljes workflow rájuk eső részéről;

b) piaci modell, ahol nem születik formális megállapodás, de a workflow-t kezdeményező szervezet kiválaszthat egy szolgáltatót, beleértve az interfészt is, amelyet a kölcsönös adatcsere és a workflow számára biztosít;

c) ad-hoc modell, amelynél nem határozzák meg előre a workflow-t, a folyamat alakulását a szervezetek az adott pillanatban döntik el.

A jogszabályok hatását illetően a helyes gyakorlatok elemzése jelentős eredményekkel járhat. Például az írek helyes gyakorlatainak esetéből kitűnik, hogy nem csupán a szükséges új jogszabályok meghatározására van szükség, hanem arra is, hogy ezeket a jogszabályokat idejekorán alkossák meg, hogy el lehessen kerülni a jogszabályok és az adott gyakorlat közötti komoly konfliktusok kialakulását. Ezt támasztja alá a svéd helyes gyakorlat esete, amely dokumentálja a projekt több mint egy éves komoly késését a lassan mozduló törvényhozás miatt.

5. Szervezeti interoperabilitás

A szervezeti IOP azoknak a szervezeteknek együttműködésére vonatkozik, amelyek kölcsönös információcserét szeretnének megvalósítani, ugyanakkor eltérő belső struktúrákkal és folyamatokkal rendelkeznek. A szervezeti IOP létrehozásának célja az összes szervezeti akadály legyőzése, ami által lehetővé válik a megfelelő szervezeten belüli és szervezetközi workflow kialakítása. Az interoperabilitás létrehozására irányuló szervezeti megoldásokat illetően az EIF (Európai Beruházási Alap) megvizsgálja és elveti a kétoldalú megoldásokat, előnyben részesítve a többoldalú megoldások alkalmazását. Itt minden egyes együttműködő partner azonos IOP megoldást alkalmaz. Így ezt az egyetlen megoldást csak egyszer kell megvalósítani és az mindegyikük igényeinek megfelel. Ezenkívül az EIF arra is utalást tesz, hogy a szubszidiaritás elve előírja a felelősség decentralizálását. Az EIF továbbá javasolja az úgy nevezett „ügyintézési interoperabilitási interfészek" (BII) bevezetését, amelyek révén a különböző tagállamok közigazgatási intézményei képesek lesznek páneurópai szintű interoperabilitás megvalósítására egyes e-kormányzati szolgáltatások céljából. Az interoperabilitás kérdéseire adott szervezeti megoldások tekintetében az EPAN olyan ügynöki szolgáltatás létrehozását javasolja, amely kölcsönösség alapján, szolgáltatási szintű megállapodásoknak megfelelően és útmutatók használatával közös funkcionalitást biztosítana a háttérszolgáltató végrehajtó szervek számára. Svédországban például egy új vállalkozás létrehozásához a vállalkozóknak két szervet kellett felkeresniük: egyet a cég nyilvántartásba vételével, és egy másikat a cég adózásával kapcsolatban. A svéd helyes gyakorlat esetében az adott workflow-kat áttervezték és ennek eredményeként ma már egyetlen helyen lehet intézni a cégek nyilvántartásba vételének teljes procedúráját és így nemcsak az ügyfelek, hanem az érintett szervek is időt és pénzt takaríthatnak meg.

6. Szemantikai interoperabilitás

Szemantika az adatok jelentését és használatát jelenti [9]. Ilyen módon, amikor szükségessé válik a közhivatalok közötti információcsere a szemantikai interoperabilitás különösen fontos lesz. A főbb szemantikai konfliktusok az adatstruktúrához és az adatok jelentéséhez kapcsolódnak. Egy másik osztályozás arra enged következtetni, hogy a szemantikai konfliktusok az adatok szintjén és séma szinten fordulhatnak elő [10]. Az adatok szintjén jelentkező konfliktusok az adat domainekben jelentkező különbségek, amelyek a hasonló adatok eltérő reprezentációja és értelmezése miatt keletkeznek. Az alábbi adat-szintű konfliktusok előfordulása lehetséges:

a) adatérték-konfliktusok, például a „külföldi" az egyik adatbázisban azt jelentheti, hogy a személy nem az ország állampolgára, míg egy másikban azt, hogy a személy nem az Európai Unió polgára;

b) adatreprezentációs konfliktusok, például egy időpont reprezentációja az egyik adatbázisban 06-30-2005 lehet, a másik adatbázisban 30-06-2005, míg a harmadikban 30-Jun-2005;

c) adategység-konfliktusok, például épületek magassága az egyik adatbázisban centiméterben, a másikban hüvelykben szerepelhet;

d) adatpontossági konfliktusok, például az épületek magasság szerinti

osztályozása lehet „magas", „közepes" és „alacsony" az egyik adatbázisban és A, B, C vagy D szintű a másikban;

e) adatok nyelvi konfliktusai, például, amikor az információt különböző nyelveken tárolják. A séma szintű konfliktusokat a logikai struktúrák eltérései, illetve a metaadatokban található következetlenségek jellemzik. Az alábbi séma szintű konfliktusok előfordulása lehetséges:

elnevezéssel kapcsolatos konfliktusok, például „Állampolgár" elnevezés az egyik adatbázisban ugyanannak az információnak begyűjtésére szolgál, mint a „Kedvezményezett" elnevezés a másik adatbázisban. Általánosításhoz kapcsolódó konfliktusok, például azok, amelyek akkor merülnek fel, amikor az egyik adatbázisban egy reprezentáció van az „Állampolgárra", a másik viszont két külön reprezentációt tartalmaz „Férfiakra" és Nőkre".

Egyéb séma szintű konfliktusok is előfordulhatnak, például egységazonosító konfliktusok, séma izomorfizmus konfliktusok, összesítési konfliktusok, szemantikai különbségek, stb. A szemantikai IOP megoldásokat és más kapcsolódó kutatásokat gyakran kategorizálják három szélesebb terület szerint: kiosztás (mappings) alapú, közvetítő alapú és lekérdezés-orientált megközelítések. A kiosztás alapú megközelítés megvalósítására általában szövetséges (vagy globális) sémát hoznak létre, és kiosztásokat létesítenek a szövetséges (vagy globális) sémák és a résztvevő helyi sémák között. A közvetítő alapú megközelítés egy olyan közvetítő használatát tartja tanácsosnak, amely domain-specifikus ismerettel, mapping ismerettel, illetve specifikusan a különböző autonóm információs források koordinációjára kifejlesztett szabályokkal rendelkezik. Ez meglehetősen közel van ahhoz a multilaterális megoldási formához, amelyet az Európai Interoperabilitási Keretrendszer javasolt az IOP -nak európai szinten történő biztosítása céljából. A lekérdezésorientált megközelítés interoperábilis nyelvek használatát javasolja, amelyek képesek több adatbázist átfogó lekérdezéseket megfogalmazni. Feltehetőleg ez a legkevésbé megfelelő megközelítés az e-kormányzat szempontjából, mivel ellentétben állhat a szubszidiaritás elvével.

A szemantikai IOP területén jelenleg folyó kutatás végső célja a különböző rendszerek közötti összes szemantikai konfliktus teljesen automatizált kezelése. Sőt elfogadott, hogy az általános környezet folyamatosan változik, ezért bármikor új rendszereket lehet felvenni, másokat kivonni. Megjegyzést érdemel azonban, hogy más területektől eltérően (például. e-kereskedelem) az e-kormányzat területén a szemantikai IOP -követelmények listája sokkal rövidebb, mivel az ugyanazon szolgáltatást nyújtó szervek általában nem versenyeznek egymással. A belga helyes gyakorlat esetében kulcsszerepet játszott az XML sémák adattartalmáról és a különböző intézményeken és különböző szolgáltatásokon átívelő adatértelmezésről hozott megállapodás. A közszolgáltatásban hagyományos felhasználást alapul véve az egyes intézmények kifejlesztették saját sémájukat és adatstruktúrájukat. Azonban szükségessé vált az intézmények közötti megállapodás létrehozása, amelynek érdekében még akkor is kompromisszumra kellett jutniuk, ha ehhez alapvető adatbázisaikon változtatniuk kellett.

Tárgyalások kezdődtek, például a név, a cím, stb. értelmezéséről, majd közös megegyezésre jutottak. Ezeknek a kormányzat által elfogadott reprezentációknak általános használata kormányzati hatáskörben kötelező. Hasonlóképpen, az osztrák

helyes gyakorlat esetében is megállapításra került, hogy a szabványosított elektronikus fájlcsere biztosítása előtt álló négy nagy kihívás közül az egyiket a közösen használt nyelvtan és szabványok képviselik. Megemlítendő, hogy a szabványok meghatározásának folyamata a megvalósítás során több okból is nehézségekbe ütközött. A dán OIOXML helyes gyakorlat eset az adatszabványok nyomasztó fejlesztési ciklusáról, nyelvi problémákról (ebben az esetben azzal kapcsolatban, hogy választani kellett a dán és az angol között), a szabványosítástól való húzódozásról és a megértés és a kötelezettségvállalás hiányáról számol be.

7. Technikai interoperabilitás

A technikai IOP felöleli az összes technikai kérdést (technológiák, szabványok, házirendek), mivel csak így lehet garantálni, hogy az együttműködő szervek információs rendszereinek technikai komponensei képesek legyenek az együttes munkára. Figyelmet érdemel, hogy a technikai IOP nem csak a technológiákra és a fizikai kapcsolatok rétegére vonatkozik (például a hálózati protokollokra), hanem a szervezeti és szemantikai rétegeket támogató technológiákra is. A technikai IOP osztályozásának több eltérő módja van. Például az Egyesült Királyságban az e-Kormányzati Interoperabilitás Keretrendszer (e-GIF) az interkonnekcióra, az adatintegrációra, a metaadatok tartalomkezelésére és az e-szolgáltatások hozzáférhetőségére vonatkozó technikai házirendeket és műszaki specifikációkat ad ki. Másik példa a Német Interoperabilitási Keretrendszer (SAGA ver. 2.1), amely műszaki szabványokat ajánl az alábbi területekre javasolt architektúra támogatása céljából: folyamatmodellezés, adatmodellezés, alkalmazás-architektúramodellezés, ügyfél, megjelenítés, kommunikáció, összeköttetés az adminisztrációval és biztonság.

A technikai fejlesztések gyorsan követik egymást, különösen azok, amelyek az internethez kapcsolódnak. Ennek következtében a technikai IOP útmutatók általában az összes e-kormányzati szolgáltatásnál javasolják az internet használatát. Az internet könnyen elérhetővé tette a technikai interoperabilitást [11]. A technikai IOP eléréséhez általában az internetes szabványok használatát ajánlják. Például a hálózati réteg esetében a TCP/IP-t ajánlják, mint az alapvető internetes kapcsolatok létesítésének széles körben elterjedt hálózati szabványát; a megjelenítési réteg szabványosítására a HTML-t ajánlják; az adatkapcsolat-réteg esetében a leggyakrabban használt szabvány az XML stb. A szemantikai IOP esetében kiemelkedik az XML jelentősége, amely az információ reprezentációjának de-facto szabványa. Az XML-et gyakran tekintik több interoperabilitási kérdésre adható válasznak. Azonban az XML önmagában csak az adathierarchiát képviselő közös keretrendszer létrehozását tudja biztosítani. Kiegészítő specifikációkra van tehát szükség az összetettebb logikai adatstruktúrák és típusok meghatározásához és jóváhagyásához, különösen azokban az esetekben, amikor a szükségletek a hierarchiák vagy az egyszerű taxonómiák reprezentációjánál többet kívánnak [12]. Az ilyen esetekben alkalmazható technológiák között lehetnek tématérképek, amelyek témák és azok dokumentumokban való előfordulásának, valamint a témák közötti társulások ábrázolására használhatók. Köztük van a Forrásleíró Keretrendszer (RDF), amely meghatározza a modell és az XML szintaxis, amely a metaadatok ábrázolására és átadására szolgál. Az RDF specifikációk könnyűsúlyú ontológiai rendszerrel támogatják az ismeretek cseréjét a weben. Általában bármely internetes forrást webol-

dalként és annak tartalmaként szokás leírni. Azonban az OWL egy olyan szemantikai jelölőnyelv a webforrások számára, amely lehetővé teszi az ontológia átadását a weben [13]. A webszolgáltatások kontextusában, az OWL vezetett egy másik, a webszolgáltatások követelményei egy másik fontos szabványának, az OWL-S-nek meghatározásához. Az OWL-S olyan ontológia, amely szemantikai információ segítségével határozza meg a webszolgáltatásokat. Az OWL-S lehetővé teszi a szolgáltatás tulajdonságainak és képességeinek deklaratív hirdetését is, amely felhasználható a szolgáltatás automatikus felderítésére, lehívására és leírására [14].

Szervezeti IOP esetében sok fontos területen számos szabvány létezik, például a folyamat modellezés és a folyamat átszervezés terén. Például a szervezetek közötti workflow-k esetében a vonatkozó workflow-specifikációk tartalmazzák a BPEL4WS-t (a webszolgáltatások vezénylése, folyamata és kompozíciója). Az üzleti folyamatok végrehajtási nyelve a webszolgáltatások használatának elősegítésére (BPEL4WS vagy BPEL) XML-en alapuló adatcsere formátumban van specifikálva. Ezen kívül, más fontos specifikációs workflow szabványok a következőket tartalmazzák: BPML (üzleti folyamatok modellezési nyelve), BPMN (üzleti folyamatok modellezési jelölésrendszere), BPSS (az üzleti folyamatok specifikációs sémája az OASIS része, alapja az ebXML az SML alapú eBusiness), WSCŐ (W3C Web Services Choreography Interface, webszolgáltatások koreográfiai felülete), WSCL (Web Service Choreography Language – webszoláltatások koreográfiás nyelve), XPDL (XML Process Definition Language – folyamatmeghatározás nyelve) stb. [15].

8. Összefoglalás, következtetések

Az interoperabilitás minden olyan esetben fontos, ahol különböző közszolgáltatási szerveknek vagy egységeknek kell együttműködniük abból a célból, hogy az állampolgároknak összegzett szolgáltatásokat, illetve információt nyújtsanak (például családi vagy üzleti esemény kapcsán). Ebből következően az IOP különösen fontos az e-kormányzat előnyeinek realizálása szempontjából, mivel az összekapcsolt és az egyablakos ügykezelés megvalósításának egyik előfeltételét képezi.

Felhasznált irodalom:

[1] Pándi, Erik: Modernisation process of public administration services, „Kommunikáció 2007." Nemzetközi szakmai-tudományos konferencia kiadványa, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2007., ISBN 978-963-7060-31-1, 96. oldal;

[2] Pándi Erik – Pándi Balázs: Az elektronikus közszolgáltatások nemzeti szabályozó hatóság részéről történő támogatottságának kérdései, Hadtudományi Szemle, ZMNE KLHK, Budapest, 2008., 106-109. oldal, 2008/1. szám;

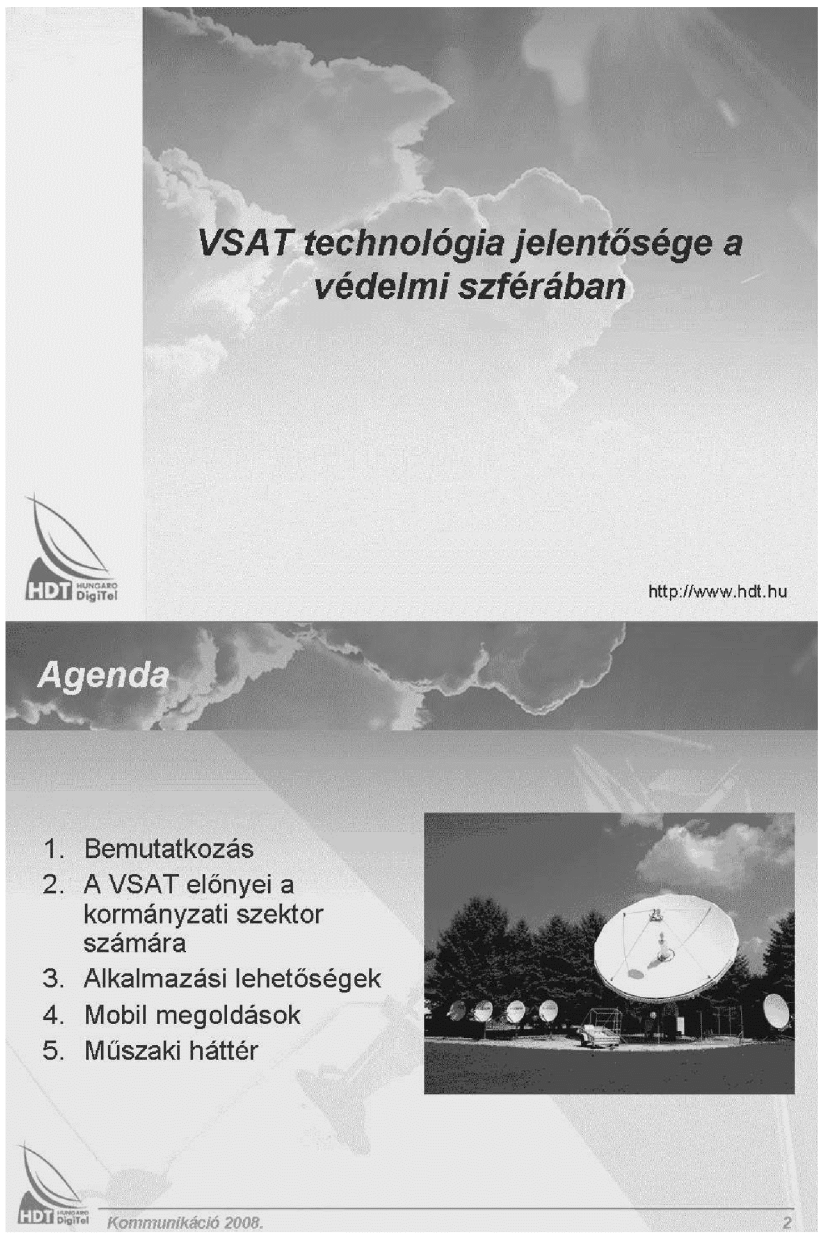
[3] Európai Bizottság, 2003, *Az elektronikus kormányzati eszközök szerepe Európa jövőjében.* A Bizottság közleménye, Brüsszel, 2003.9.26., COM(2003) 567 Final;

[4] IDABC 2004. A páneurópai elektronikus kormányzati szolgáltatások európai interoperabilitási keretrendszere;

[5] Peristeras V. és Tarabanis K., 2006, The C4IF Interoperability Typology Framework. (A C4IF interoperabilitási tipológiai keretrendszer) Journal of Interoperability in Business Information Systems (IBIS), **1**(1), 61-72. oldal;
[6] IDABC 2004. A páneurópai e-kormányzati szolgáltatások európai interoperabilitási keretrendszere. Luxembourg, Európai Közösségek;
[7] Európai Közigazgatási Hálózat, E-Kormányzati Munkacsoport, Az interoperabilitási architektúra kulcsfontosságú alapelvei, 2004.;
[8] R. Tagg: Workflow in Different Styles of Virtual Enterprise. (Workflow a különböző stílusú virtuális vállalatoknál), Australian Computer Science Communication. 2001. 23. sz., 21-28. oldal;
[9] W.A. Woods „What's in a link: Foundations for semantic networks", (Mi van egy linkben: a szemantikai hálózatok alapjai). Representation and Understanding: Studies in Cognitive Science, D.G. Bobrow és A. Colling,. Academic Press, Inc., New York, NY, 1975. 35-82. oldal;
[10] Park, J. és S. Ram (2004). „Information Systems Interoperability: What Lies Beneath?" (Az információs rendszerek interoperabilitása: Mi van mögötte?), ACM, Transactions on Information Systems 22(4): 595–632. oldal;
[11] Kubicek, H. és Cimander, R. (2005), „Interoperability in eGovernment: A Survey on Information Needs of Different EU Stakeholders" (Interoperabilitás az e-kormányzatban: a különböző európai uniós érdekelt felek információs szükségleteinek felmérése) , European Review of Political technologies, 2005. december;
[12] Chase, E. és Straat, M. (2005), „Information Interoperability and Intelligent Documents" (Információs interoperabilitás és intelligens dokumentumok) , eGov-Interop'05 Konferencia, 2005. február 23-24.;
[13] TopQuadrant Technology Briefing, Semantic Technology (a Topquadrant technológia ismertetése, szemantikai technológia), 1.2 verzió, 2004. március;
[14] Vicente, S., Perez, M., Garcia, X., Gimeno, A. és Javier, N. (2005), „eGovernment interoperability on a semantically driven world" (e-kormányzati interoperabilitás a szemantika által hajtott világban) , eGov-Interop'05 Konferencia, 2005. február 23-24.,
[15] Punia D. K és Saxena K. B. C., „Managing Őnter-organisational Workflows in eGovernment Services" (A szervezetközi workflow-k kezelése az e-kormányzati szolgáltatásoknál), ICEC 2004, 500-505. oldal.

Hungaro DigiTel

VSAT TECHNOLÓGIA JELENTŐSÉGE A VÉDELMI SZFÉRÁBAN



Bemutatkozás

Fő tulajdonosaink:

- Antenna Hungária Rt. (TDF csoport) : 55%
- PT Ventures SA (Portugal Telecom csoport): 45%

Piaci részesedés:

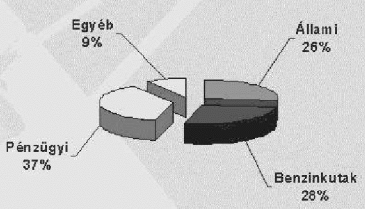
- Magyarország és Közép-Európa piacvezető VSAT szolgáltatója
- Piaci részesedése több, mint 60 %

Alaptőke:	~ 900 M Ft
Éves árbevétel:	~1,7 Mrd Ft
Végpontszám:	~ 3000db

Ügyfeleink

Főbb referenciáink:

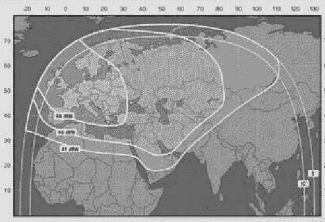
- Magyar Honvédség
- Katasztrófavédelem
- MEH (KözHáló)
- OTP Bank
- MOL
- OMV (Magyarország és Szerbia)
- Shell (Magyarország és Bulgária)
- Agip Hungária
- Lukoil
- Magyar Telekom
- Pantel
- Antenna Hungária



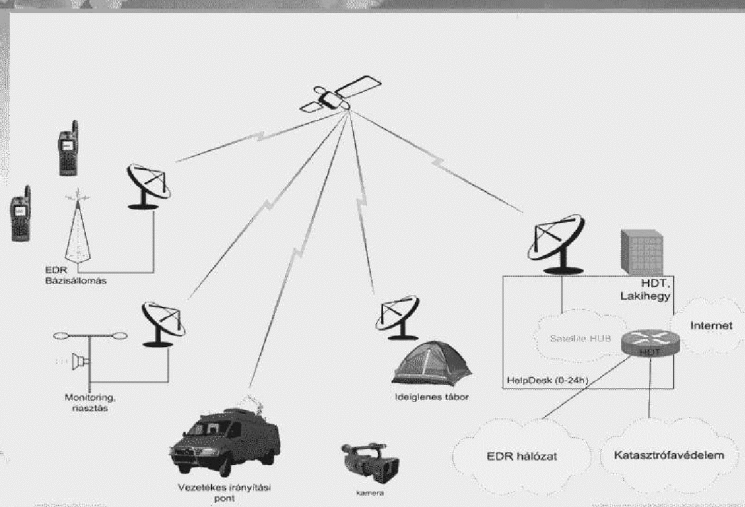
A HDT ügyfeleinek megoszlása tevékenységi kör alapján

A VSAT előnyei a kormányzati szektor számára

- Világ bármely részén igénybe vehető,
- Magyarország és a környező régió teljes lefedése,
- Gyenge infrastruktúrával rendelkező, nehezen megközelíthető helyszínek ellátása,
- Rugalmas, gyors telepíthetőség ,
- Földi infrastruktúrától független,
- Magas rendelkezésre állás.



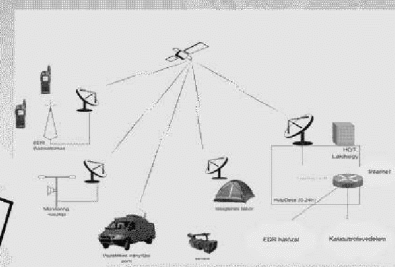
Példák a kormányzati alkalmazási területekre



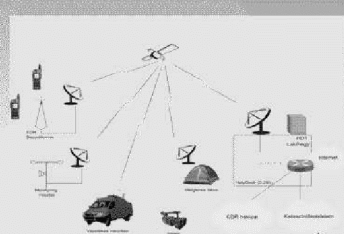
Lehetséges alkalmazási területek – 1

Keskenysávú szolgáltatást igénylő lehetőségek:

- Felügyelet nélküli telephelyek automatizálási, beléptető, stb. rendszereinek távközlési kiszolgálása
- Adatgyűjtő rendszerek (vegyvédelmi vagy árvízvédelmi mérőhelyek távközlési ellátása)



Lehetséges alkalmazási területek – 2



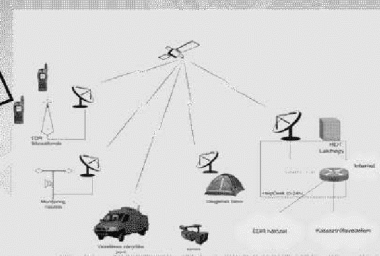
Szélessávú szolgáltatások:

- 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

Lehetséges alkalmazási területek – 3

Szélessávú **kommunikációs** szolgáltatások:

- EDR bázisállomások tartalékolása
- Elsődleges kiszolgálása a földfelszíni hálózattal nem elérhető helyeken
- Telefonközpont kihelyezés
- Szélessávú Internet/Intranet elérés
- Videokonferencia



Mobil megoldások - 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

Mobil megoldások - 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

További mobil megoldások

Moduláris hordozható ant 	- Becsúsztatható modul – könnyű modem váltást tesz lehetővé több modem esetén - 5 perc alatt üzembe helyezhető – nem kell hozzá szerszám, egy személy könnyen kezelheti, kényelmes grafikus felhasználói felület, teljesen automatikus műholdra állás vezérlés - A katonai szabványoknak megfelel – robosztus anyagokból készült (szénszál) és szívós teszteken ment keresztül, hogy kiállja a legzordabb feltételeket és szabványokat - Kompakt, három szállítási lehetőséggel – nemcsak az egyik legkisebb terminál a piacon, de a moduláris felépítése biztosítja a könnyű csomagolási lehetőséget repülő kézipoggyászként, feladandó bőröndként vagy futárral
Bőrönd antenna 	- 5 perc alatt üzembe helyezhető – nem kell hozzá szerszám, egy személy könnyen kezelheti, kényelmes grafikus felhasználói felület, teljesen automatikus műholdra állás vezérlés - Nagyon kicsi méret – 70x47x31cm és 38kg - Kis antenna, nagy adatátviteli sávszélesség – akár több mint 4Mbps

További mobil megoldások II.

In-motion antenna (mozgó járműre) 	- Az egyik legkisebb mozgás közben használható Ku sávú antenna - 4 tengelyes megoldás - Földi és vízi használatra egyaránt alkalmas - Gyors műhold keresés - Azonnali műhold kapcsolat helyreállítás a műholdas rálátást zavaró tereptárgyak melletti elhaladás után - Kis súly – 120 kg - Szélessávú adatkapcsolat, mely akár több mint 4Mbps
Műholdas telefonok 	- Inmarsat és Iridium műholdas telefon megoldások - Globális lefedettség (szinte a teljes Földön) - Nagyon kisméretű készülékek, közel GSM mobil méretben is elérhető - Hang és adatátvitel (BGAN) - Fax átvitel - Adatátvitel max. 492kbps - Folyamatos adatátvitel (streaming) max.: 256kbps

Mobil műholdas felhasználási példák

- Mobil ellenőrzési pont felállítása,
- Parancsnoki gépjárművek bekötése a belső hálózatba,
- Katasztrófavédelmi feladatok szervezése a helyszínről,
- Video jel továbbítás a helyszínről/helyszínekre,
- Hang továbbítás a helyszínről,
- Központi adatbázisok elérése változó helyszínekről.

Biztonságos adatátvitel

- Zárt hálózat
- Nem publikus Internet alapú
- Elkülönített forgalmak kezelése külön VLAN-okban
- Több használatban lévő titkosító rendszerrel együttműködik
- EKG-s csatlakozási lehetőség
- Lehetőség az Internet forgalom központi ellenőrzésére

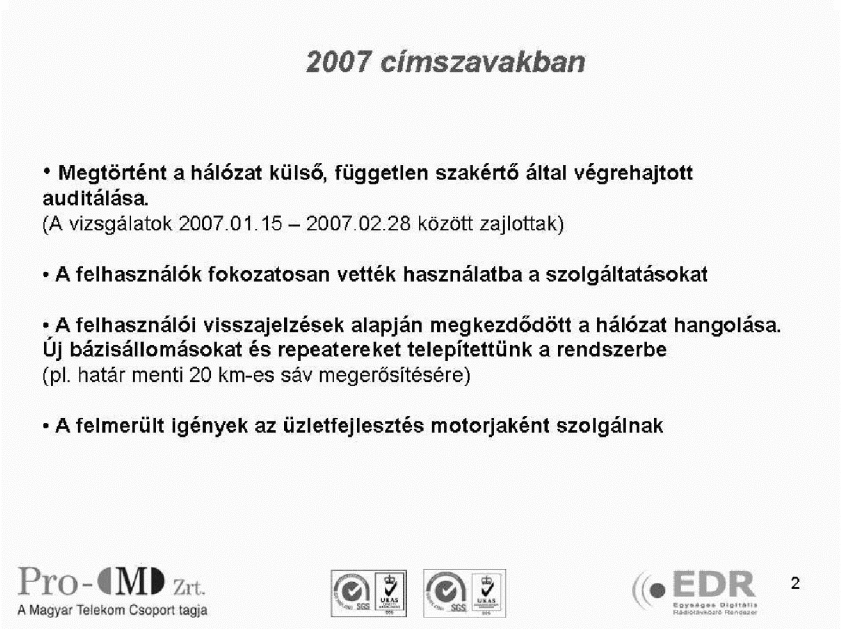
Hálózat-felügyelet

- 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


Köszönöm megtisztelő figyelmüket!
Továbbiakban is szívesen áll rendelkezésükre
Zautasvili Péter
Fejlesztési igazgató
E-mail: zautasvili@hdt.hu
Lázár János
Kereskedelmi igazgató
E-mail: lazar@hdt.hu
2310 Szigetszentmiklós-Lakihegy, Komp u.2.
Tel: 488-8500
Fax: 488-8501
www.hdt.hu
Kommunikáció 2008.
17

MIHÁLYI Gábor

EDR EREDMÉNYEK, VÁRHATÓ FEJLESZTÉSEK



Az audit megállapításai:

Az audit jegyzőkönyv megállapítása:

„A kiépült EDR rendszer a jelenleg rendelkezésre álló szolgáltatások üzemvitelének folyamatos biztosítására alkalmas"

A Megrendelő megállapítása:

„az EDR szolgáltatást a megrendelő szempontjai szerint hivatalosan átvehetőnek értékelem" ...."a Pro-M Zrt. a szolgáltatási szerződésben tett kötelezettségeinek alapvetően eleget tett „

Pro-M Zrt.
A Magyar Telekom Csoport tagja

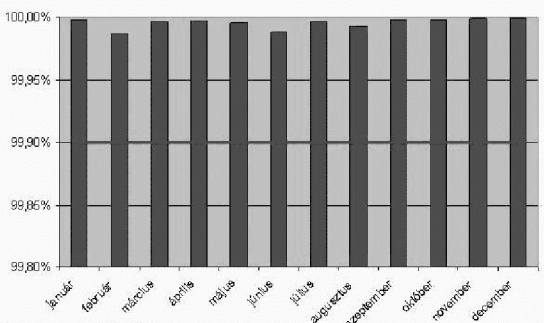
EDR Egységes Digitális Rádiótávközlő Rendszer

3

Részletes adatok az EDR rendszer eddigi teljesítményéről 1.

A bázisállomások rendelkezésre állása minden hónapban <u>túlteljesült</u> a szerződésben rögzített elváráshoz képest

Bázisállomások rendelkezésre állása



- Szerződéses kötelezettség: Az EDR rendszerben levő bármely bázisállomás rendelkezésre állása legalább **99,9%-os** bármely év 3 egymást követő hónapjának 24 órájában (nincs szigetüzem sem).
- Folyamatos túlteljesítés
- Vis Major eset: mobil pótlás 24 órán belül

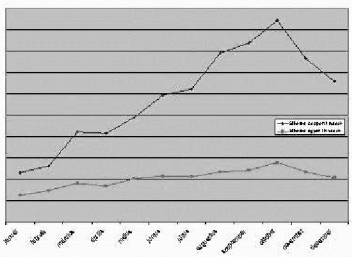
Pro-M Zrt.
A Magyar Telekom Csoport tagja

EDR Egységes Digitális Rádiótávközlő Rendszer

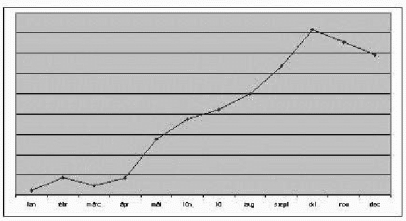
4

Részletes adatok az EDR rendszer eddigi teljesítményéről 2.

A hívások száma év végére közel **két és félszeresére nőtt,** míg a HLR-be regisztrált készülék száma **nem egész kétszeresére.** Ezen belül a csoporthívások száma **közel háromszorosára,** az egyéni hívások száma **közel kétszeresére** emelkedett az év végére



Az SDS-ek száma az év végére **több, mint huszonnyolcszorosára** nőtt



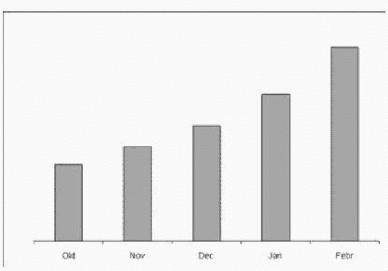
Pro-MD Zrt.
A Magyar Telekom Csoport tagja

EDR Egységes Digitális Rádiótávközlő Rendszer

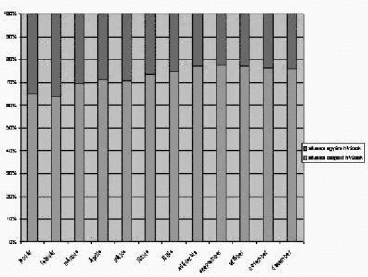
5

Részletes adatok az EDR rendszer eddigi teljesítményéről 3.

Az AVL rendszerben regisztrált készülékek mennyiségi alakulása



A csoporthívások aránya megnőtt az egyéni hívásokhoz képest, a felhasználók a hálózatot egyre inkább „rendeltetésszerűen" használják



Pro-MD Zrt.
A Magyar Telekom Csoport tagja

EDR Egységes Digitális Rádiótávközlő Rendszer

6

EDR felhasználói kör

A felhasználói kör folyamatosan bővült a rendszer használatbavétele során:

- **Országos Rendőr-főkapitányság**
- **Országos Katasztrófavédelmi Főigazgatóság**
- **Országos Mentőszolgálat**
- **Magyar Honvédség és a Nemzetbiztonsági Szolgálatok**
- **OMSZ Légimentő Kht.**
- **Dunai Vízirendészeti Rendőrkapitányság (BRFK - DVRK)**

Pro-M Zrt.
A Magyar Telekom Csoport tagja

EDR

7

EDR ügyfél- elégedettség : pro & kontra

Az EDR szerződésből adódó kötelezettségnek eleget téve, illetve a végfelhasználók valós igényeinek, tapasztalatainak teljesebb megismerése érdekében a Pro-M Zrt. 2007 őszén ügyfél-elégedettségi kutatást végeztetett.

„Az összes megkérdezett átlagosan minden paraméterben jobbnak értékeli az EDR rendszert, mint a korábbi analógot…"

„A Pro-M mindenekelőtt hosszútávon gondolkodó, modern szolgáltató…"

A rendszer hatékonyabb használata érdekében további fejlesztések szükségesek a következő területeken:

- Oktatás
- Automatikus járműkövető rendszer (Pro-Mobil AVL)

Pro-M Zrt.
A Magyar Telekom Csoport tagja

EDR

8

Oktatás

A felhasználók jelenleg közel 34 ezer készülékkel rendelkeznek a feladataik elvégzéséhez. A közvélemény-kutatás alapján a felhasználók 75%-a további oktatást, információt igényelt a készülékről, a hálózatról és annak szolgáltatásairól.

2008. évi fejlesztés

A rendszer kiegészült a díjmentes e-learning szolgáltatással :

- terminálok kezelésére szolgáló interaktív modul használat
- felhasználók hatékony oktatása (jogosultság, illetve Internet hozzáférés szükséges)
- vizsgáztatás (visszacsatolást ad a képzésről).

A meglévő oktatási termek és az ott található szolgáltatások kiegészülnek a következőkkel:

- Sepura készülék szimulátor
- Motorola készülék szimulátor

Automatikus Járműkövető Rendszer (Automatic Vehicle Location [AVL])

Az EDR hálózat része a rendszerben üzemelő járműkövető szolgáltatás. Jelenleg minden járműbe épített készülék rendelkezik GPS koordináta vételére alkalmas vevővel, amely jelek alapján az AVL információval rendelkezik a követett jármű helyzetéről.

2008. évi fejlesztés

A felhasználói felület tekintetében:

- 2000 főnél kisebb települések utcaszintű térképe
- egyes biztosítások során különböző térképi elemek kezelése
- térképek rugalmas kezelése (pl. specifikus rétegek: tűzcsapok, ügyeletes kórházak,stb)
- gyors váltás térképi rétegek között

GPS vevő/konverter upgrade:

- a platformot tekintve - a GPS vevő az AVL részévé válik
- a közös és egységes fejlesztés
- új funkciók bevezetése (pl. GPS adatok tárolása rádió kapcsolat nélkül)

Összegzés:

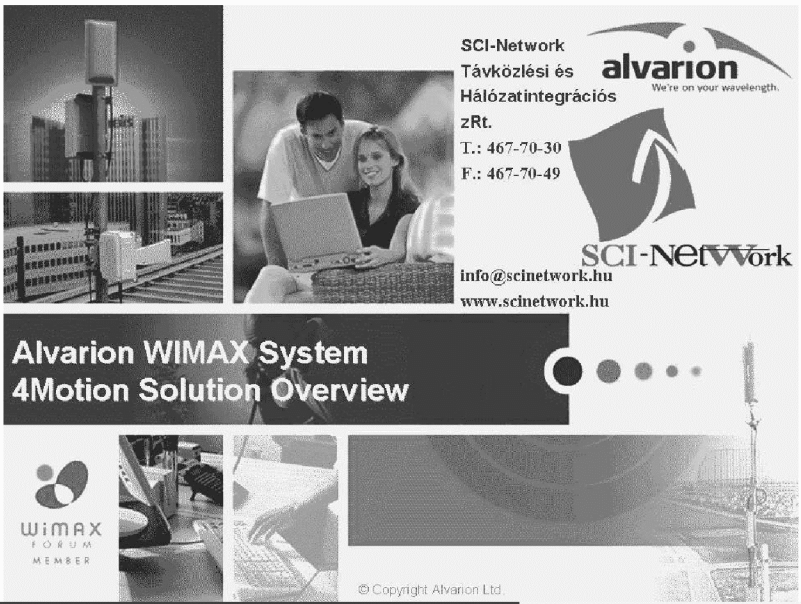
- A rendszer minőségi paraméterei folyamatosan túlteljesülnek
- Az EDR biztos alapot ad a veszélyhelyzeti kommunikációban érintett szervezetek közötti együttműködésre
- Fontos a felhasználók visszajelzése! A hálózat hangolása csak az ügyfelekkel közösen történhet!
- A lefedettséggel kapcsolatos észrevételeket folyamatosan kezeljük! (repeaterek telepítésével, infrastruktúra fejlesztéssel, stb.)
- Felkészültünk a kor és a felhasználók igényeinek megfelelő szolgáltatások fejlesztésére és biztosítására:
  - hamarosan elérhető a hálózatban a széles sávú szolgáltatás (TEDS helyettesítő termék, majd a TEDS)

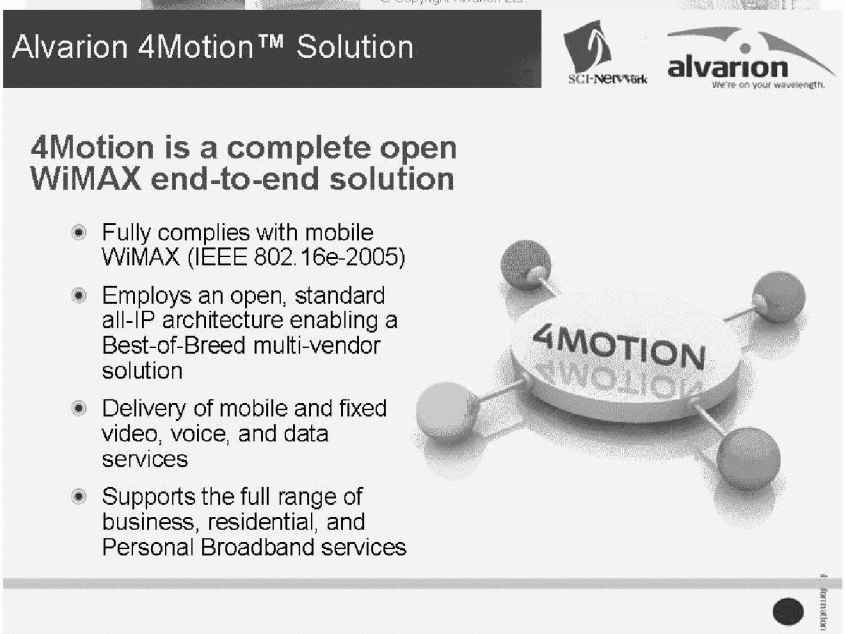
Köszönöm a figyelmet!

Mihályi Gábor
Műszaki és üzletfejlesztési igazgató
Pro-M Zrt.

2008.09.01.

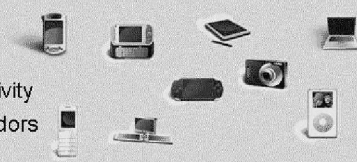
ALVARION WIMAX SYSTEM 4MOTION SOLUTION OVERVIEW





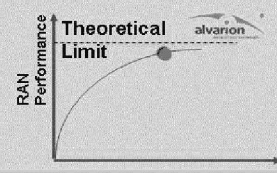
What Makes 4Motion Unique?

- **Open WiMAX™**
  - No entry barriers for new vendors
  - IP Innovation and implementation creativity
  - Freedom to choose combination of vendors
  - Leverage on consumer electronics

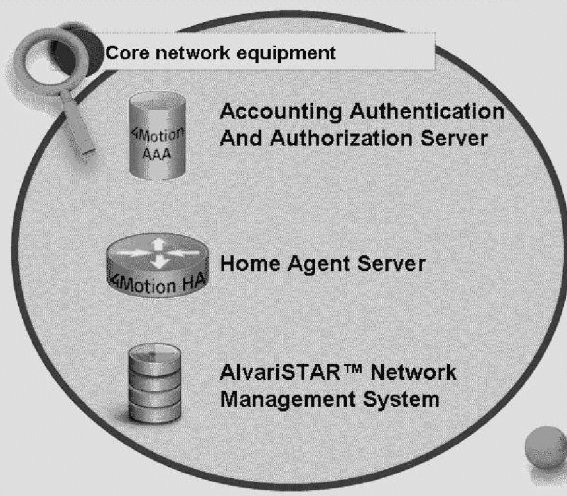


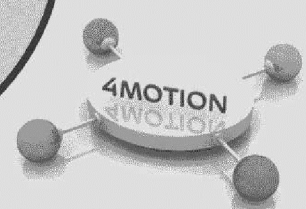
- **Use the world's most deployed WiMAX RAN**
  - #1 WiMAX vendor selected by worldwide leading operators
  - 220 deployments in over 80 countries

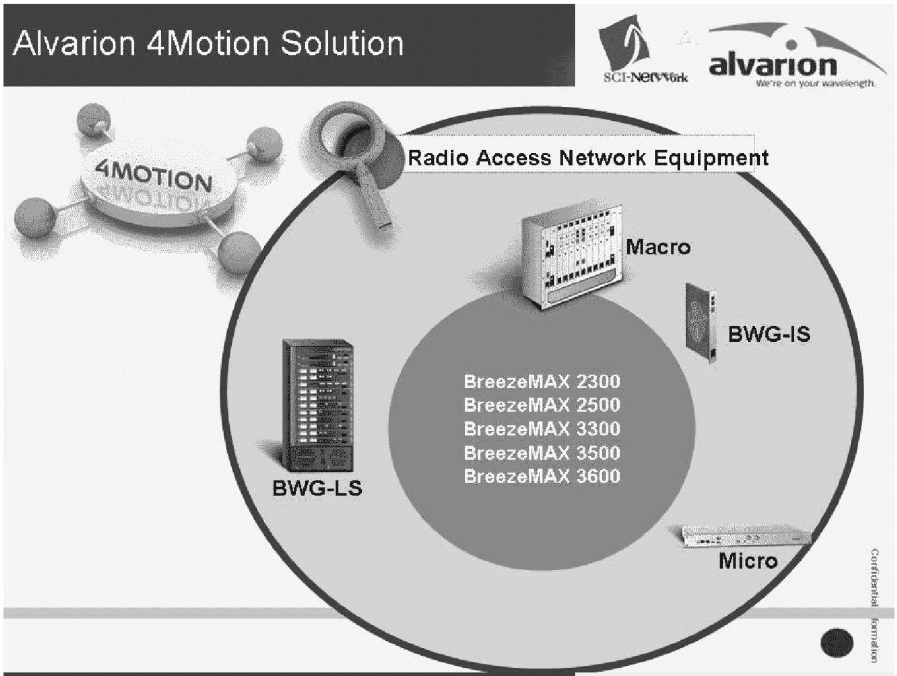
- **Superior WiMAX RAN technology**
  - Broadest radio coverage
  - Best spectral efficiency

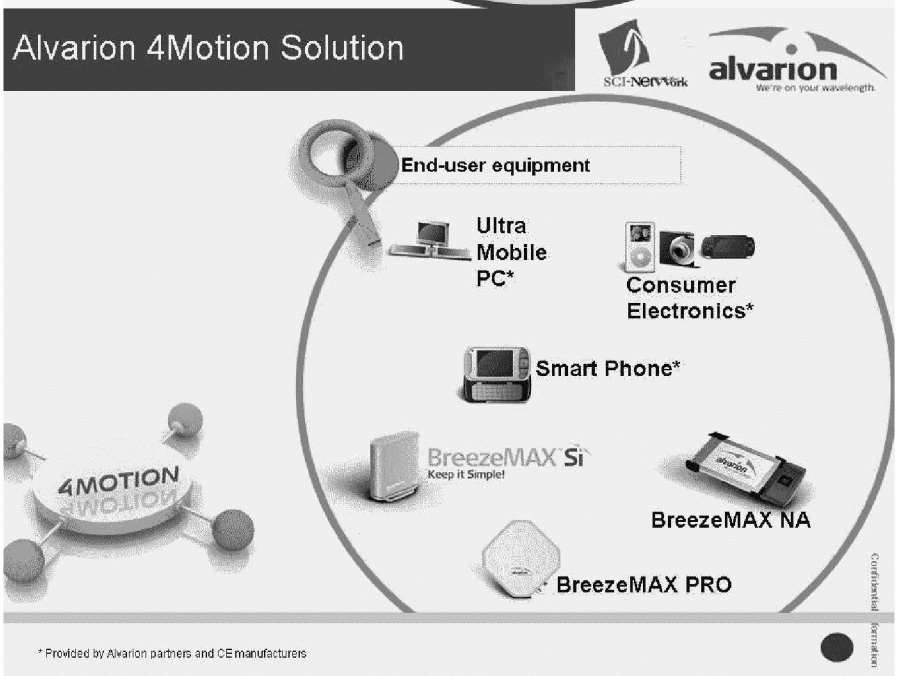


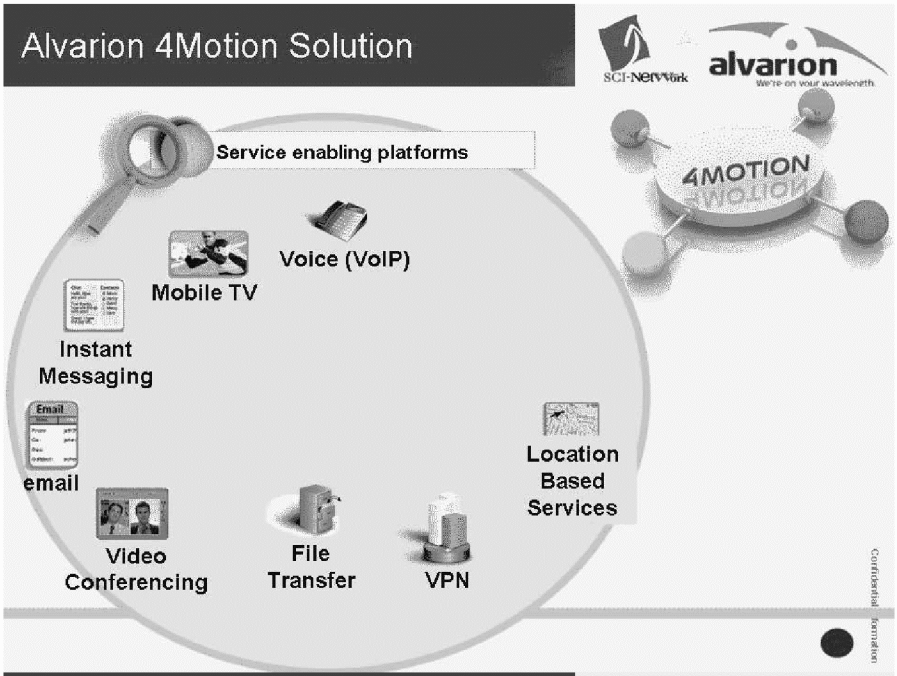
Alvarion 4Motion Solution

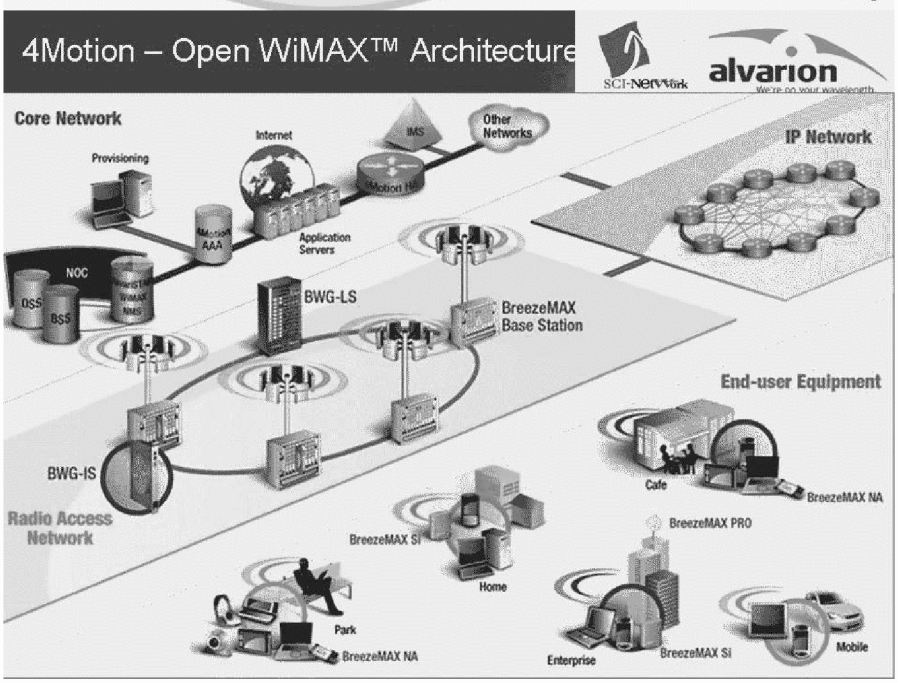


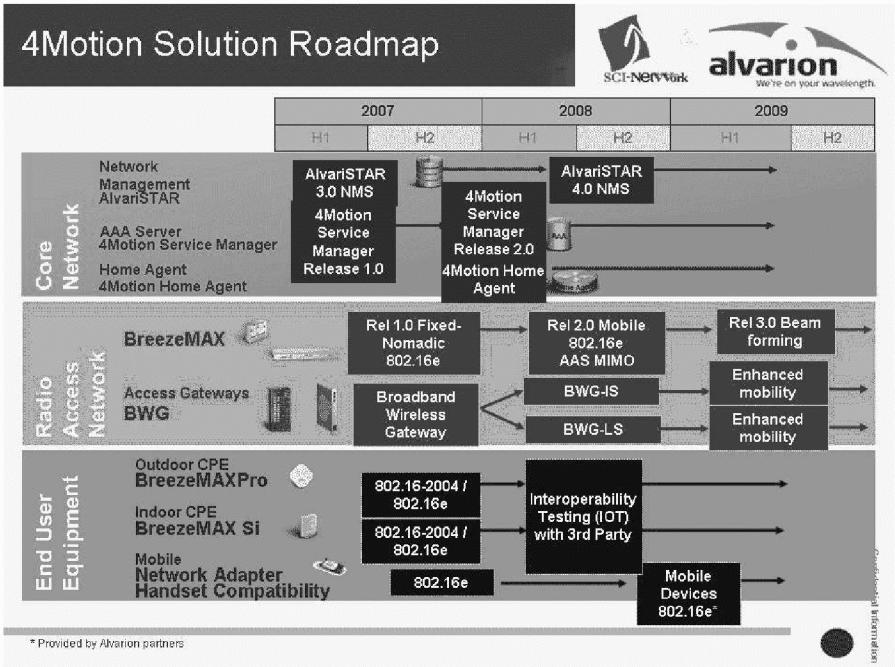


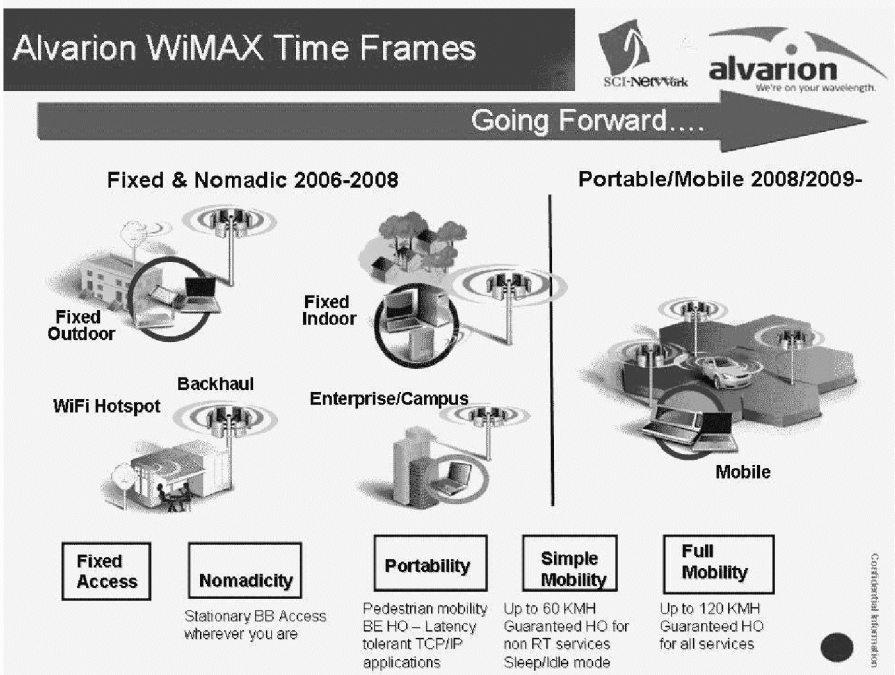

Alvarion 4Motion Solution
SCI-Network
alvarion
We're on your wavelength.
4MOTION
Radio Access Network Equipment
Macro
BWG-IS
BreezeMAX 2300
BreezeMAX 2500
BreezeMAX 3300
BreezeMAX 3500
BreezeMAX 3600
BWG-LS
Micro
Confidential Information

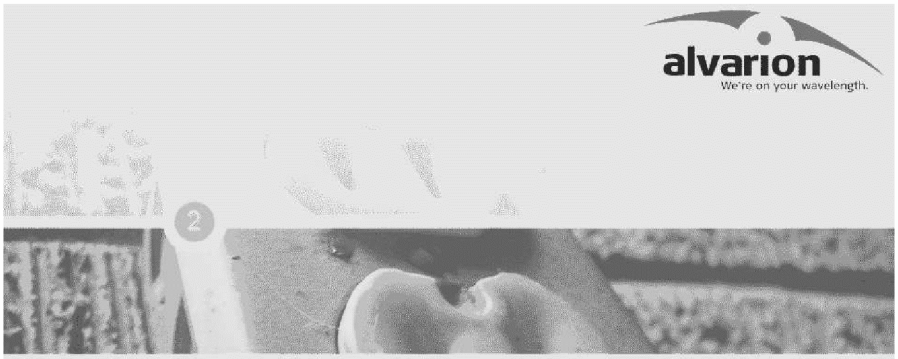

Alvarion 4Motion Solution
SCI-Network
alvarion
We're on your wavelength.
End-user equipment
Ultra Mobile PC*
Consumer Electronics*
Smart Phone*
4MOTION
BreezeMAX Si
Keep it Simple!
BreezeMAX NA
BreezeMAX PRO
Confidential Information
* Provided by Alvarion partners and OE manufacturers


Alvarion 4Motion Solution
SCI-Network
alvarion
We're on your wavelength
Service enabling platforms
4MOTION
Voice (VoIP)
Mobile TV
Instant Messaging
Email
email
Location Based Services
Video Conferencing
File Transfer
VPN
Confidential Information


4Motion – Open WiMAX™ Architecture
SCI-Network
alvarion
We're on your wavelength
Core Network
Internet
IMS
Other Networks
Provisioning
Application Servers
AAA
NOC
OSS
BSS
IP Network
BWG-LS
BreezeMAX Base Station
End-user Equipment
BWG-IS
Radio Access Network
Cafe
BreezeMAX NA
BreezeMAX PRO
BreezeMAX SI
Home
Park
BreezeMAX NA
Enterprise
BreezeMAX SI
Mobile


4Motion Solution Roadmap
SCI-Network
alvarion
We're on your wavelength.
2007
2008
2009
H1
H2
H1
H2
H1
H2
Core Network
Network Management AlvariSTAR
AAA Server 4Motion Service Manager
Home Agent 4Motion Home Agent
AlvariSTAR 3.0 NMS
4Motion Service Manager Release 1.0
4Motion Service Manager Release 2.0
4Motion Home Agent
AlvariSTAR 4.0 NMS
Radio Access Network
BreezeMAX
Access Gateways BWG
Rel 1.0 Fixed-Nomadic 802.16e
Broadband Wireless Gateway
Rel 2.0 Mobile 802.16e AAS MIMO
BWG-IS
BWG-LS
Rel 3.0 Beam forming
Enhanced mobility
Enhanced mobility
End User Equipment
Outdoor CPE BreezeMAXPro
Indoor CPE BreezeMAX Si
Mobile Network Adapter Handset Compatibility
802.16-2004 / 802.16e
802.16-2004 / 802.16e
802.16e
Interoperability Testing (IOT) with 3rd Party
Mobile Devices 802.16e*
* Provided by Alvarion partners

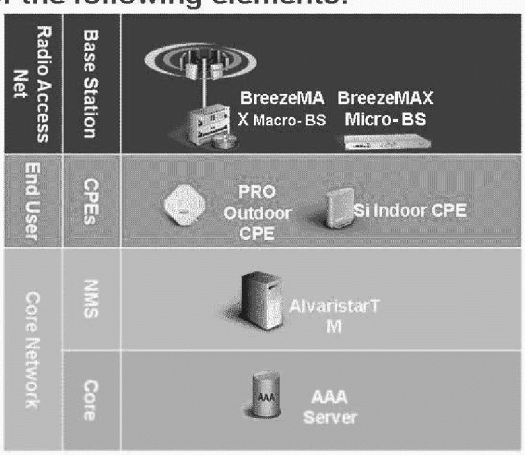

Alvarion WiMAX Time Frames
SCI-Network
alvarion
We're on your wavelength.
Going Forward....
Fixed & Nomadic 2006-2008
Portable/Mobile 2008/2009-
Fixed Outdoor
Fixed Indoor
Backhaul
WiFi Hotspot
Enterprise/Campus
Mobile
Fixed Access
Nomadicity
Stationary BB Access wherever you are
Portability
Pedestrian mobility BE HO – Latency tolerant TCP/IP applications
Simple Mobility
Up to 60 KMH Guaranteed HO for non RT services Sleep/Idle mode
Full Mobility
Up to 120 KMH Guaranteed HO for all services



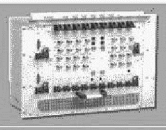
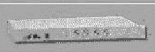
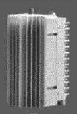
Phase 1: Fixed/Nomadic Solutions

Phase I - Introduction

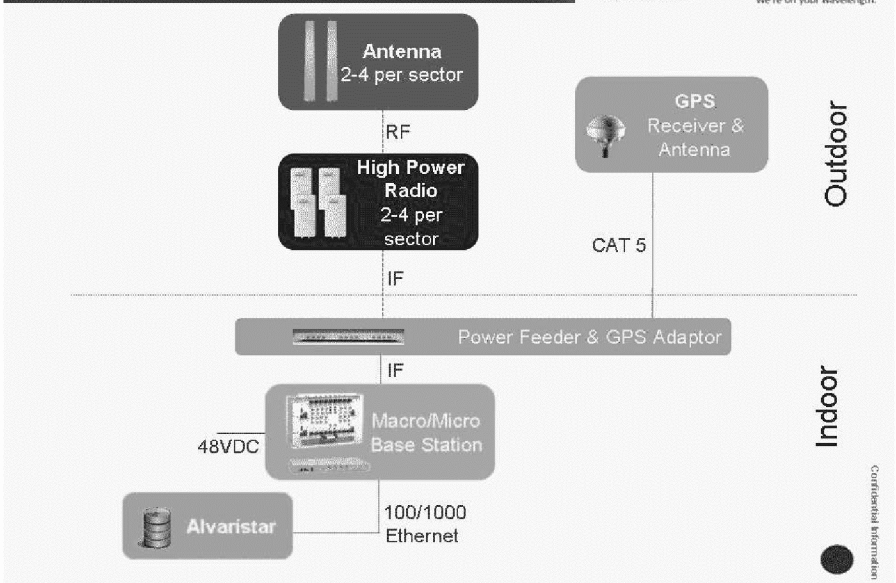
- The solutions in year 2007 addressed fixed and nomadic services
- Solutions comprised of the following elements:
  - **RAN (BreezeMAX):**
    - Macro and Micro BST
  - **End User Equipment**
    - Variety of outdoor and indoor CPEs
  - **Network main components:**
    - Integrated or external AAA Server
    - AlvariSTAR



RAN Building Blocks

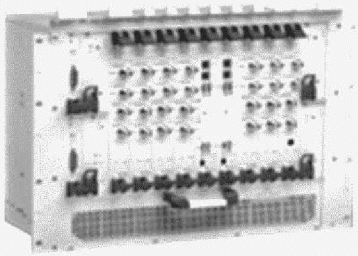
Component	Description	
Scalable, high capacity Base-Station architecture offerings	Modular (Macro) BST	
	Micro BST	
High Power radios	Outdoor unit – 34/36dBm	
Antenna	Single or Dual slant, 60°, 90° or 120°	
GPS	Outdoor and Indoor units For TDD synchronization	

RAN – Base Station Installation Example



Modular BST – Dense Populated Area

- **Suited for dense Urban/Suburban deployments**
- **Modular, supporting up to:**
  - 3 sectors with two carriers or 6 sectors with one carrier
- **4 channel AU-IDU**
- **Support 2nd and 4th order diversity**
- **NPU for GPS support**
- **Scalable, Carrier class platform**
  - Hot swappable functionality
  - Centralized management
- **Standard based Radius interface for operation with AAA server**
- **Local and remote management**

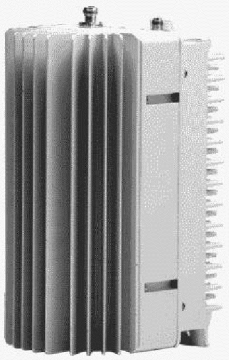


Micro BST – Sparsely Populated Areas

- **Suits for low dense rural deployments**
- **Based on similar hardware components and provides similar functionality as the Modular BST**
- **A compact 1U 19" shelf**
- **Single carrier for low density rural area**
  - Single sector using directional antenna or OMNI antenna
- **Support 2nd and 4th order diversity**
- **-48VDC model**
- **Can operate with all types of HP-ODUs**
- **Standard based Radius interface for operation with AAA server**
- **Local and remote management**

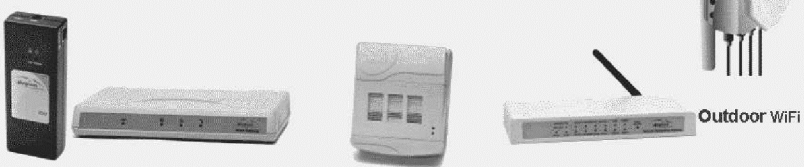
Outdoor unit – High Power ODUs

- **Designed to support world wide frequencies**
- **Detached antenna**
- **1RX / 1TX, 34-36dbm, up to 10Mhz, models:**
  - 2.3GHz – 2 models, ROW / WCS for NA
  - 2.5Ghz - 2 models, each is 100MHz
  - 3.5Ghz - 4 models, each is 50Mhz
  - 3.3Ghz - 2 models, supporting 50Mhz
- **Optional an add-on H bracket for easy deployment**



Outdoor WiMAX Quad Mode CPE

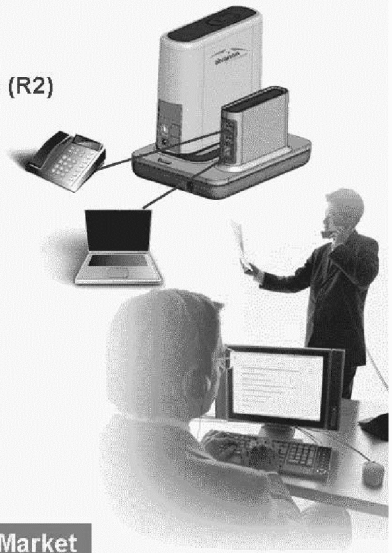
- **Robust and durable outdoor WiMAX CPE**
- **Intel® WiMAX Connection 2250 chip (R2)**
- **Dual mode FDD/TDD duplex (3.3, 3.5, 2.5, 2.3GHz)**
- **Designed for WiMAX 802.16-2004 and 802.16e-2005 air interfaces**
- **Integrated vertical/horizontal antenna or external antenna**
- **IDU to ODU communication via cat 5 cable**
- **Variety of indoor units – Data, Voice & Wi-Fi interface**



IDU data | IDU **Voice** Gateway | **IDU** Voice Gateway + Battery back up | IDU **Networking** Gateway

BreezeMAX Self-Install (Si) WiMAX Quad Mode CPE

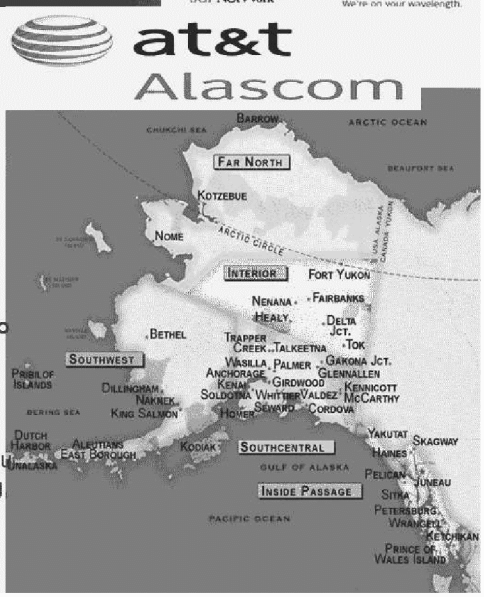
- **Compact, single box, indoor CPE**
- **Dual mode FDD/TDD duplex**
- **Utilize Intel WiMAX Connection 2250 chip (R2)**
- **Designed for WiMAX 802.16-2004 and 802.16e-2005 air interfaces**
- **Data – Ethernet or *USB* interface**
- **Optional integrated 1 or 2 voice**
  - Battery back up option
- **Self-install**
  - ***Zero*** installation fees
  - Installation with smart card/software CD utility
  - Simple and easy for all type of users
- **Connect anywhere**
  - Instant broadband services
  - Nomadic type of services



Enabler for Mass Broadband Residential Market

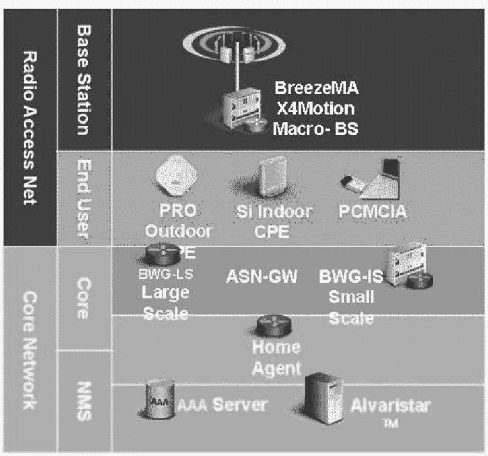
Customer Example – AT&T Alascom

- **Tier 1 operator in Alaska**
- **Provide fixed and nomadic services**
  - 1-3Mbps to customers
- **Equipment**
  - 35 Macro Base stations
  - 6,000 – 9,000 - Si indoor
  - 250 outdoor CPEs
- **Start deployment from Q4/06 and to complete by H2/07**
- **Deployment areas (suburban topology)**
  - Anchorage, Fairbanks and Juneau
  - Delta Junction, Kenai, Petersburg, Nome Ketchikan, Sitka, Wrangell and Valdez



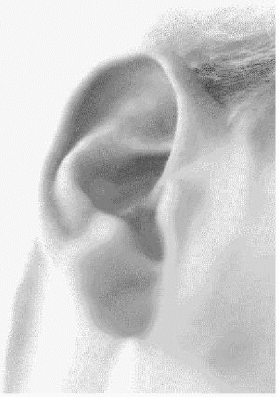
Phase II - Introduction

- **The solution in H1/08 addresses Mobile solutions**
  - Greenfield mobile broadband operators
  - Early adopters of Mobile WiMAX technology
- **Comprised of the following elements:**
  - RAN (BreezeMAX-4M):
    - Macro BST
    - New Antenna Arrays [Tx+Rx] – 2+4, 4+4
  - CPE
    - Fix ODU CPE and SI
    - Mobile Station (MS) – PCMCIA, Handset
  - Network main components:
    - ASN GW (Network Gateway)
      - Small Scale Integrated in BMAX-4M
      - Large Scale third partners
    - AAA Server
      - Integrated or external
    - Home Agent (Roaming Agent)
    - AlvariSTAR

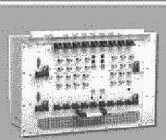


Phase II - RAN Main Messages

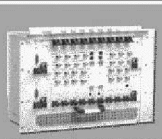
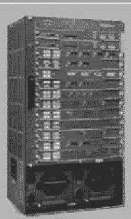
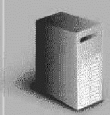
- **Support Mobile WiMAX service**
  - Intra and Inter BST Handoff
- **4Motion 802.16e Certified Solution**
  - Can upgrade Phase I 4Motion TDD BST
- **Open WiMAX architecture**
  - Standard WiMAX Interfaces offers Best of Bread Network Core devices
- **World Wide WiMAX frequencies coverage (masks)**
  - 2.3, 2.3 WCS, 2.5, and 3.5GHz frequencies
  - At 5,7,10Mhz
- **Investment protection**
  - Migration path using variety of CPEs, upgradeable to 802.16e
  - Future proof migration to AAS technologies (MIMO, Beam Forming)



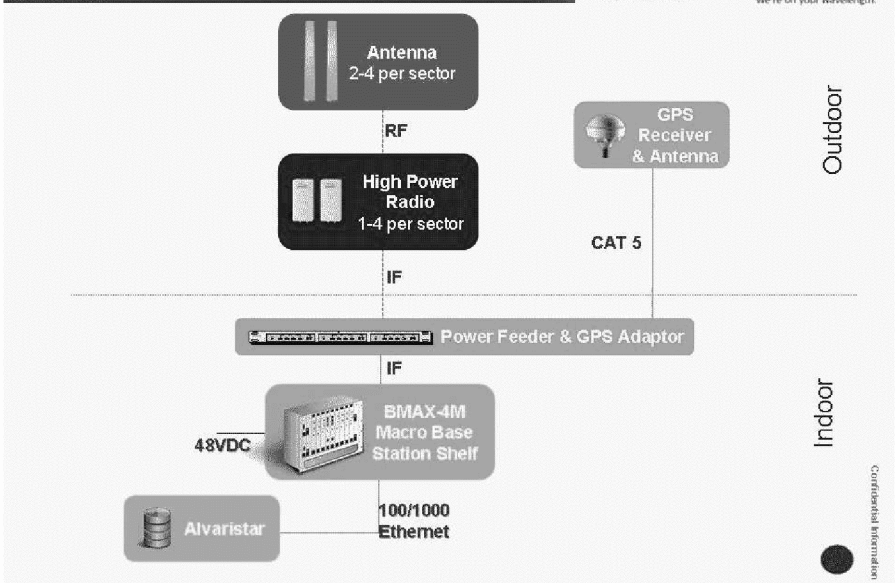
Phase II - RAN Building Blocks

Component	Description	
Scalable, high capacity Base-Station architecture offering	Modular (Macro) BST	
New High Power Radio	> 38dB 2Tx and 4Rx	
Antenna	New Antenna Arrays: 2Tx + 4Rx, 4Tx+4Rx Single, Dual slant, 120°	
GPS	For TDD synchronization Location Based Services	

Phase II - Network Building Blocks

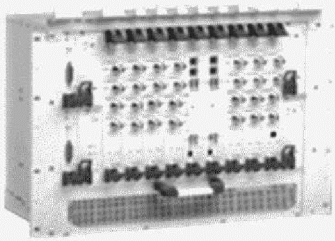
Component	Description	
ASN GW	Network Gateway Enables Mobility	 BMAX-4M with BWG-IS Integrated ASN-GW
BWG-IS	Small Scale Integrated into BreezMAX BST	
BWG-LS	Large Scale ASN-GW From IOT partners (i.e. Cisco)	 BWG-LS Cisco 7600 Multiple ASN GW with Integrated HA and Integrated AAA
Home Agent (HA)	Enables Roaming between WiMAX networks From third party (i.e. Cisco)	
AAA server	Enables Network Entry Authentication, Authorization, Accounting Complementary to BWG-IS	 Third Party AAA From Bridgewater For BWG-IS

BMAX-4M Base Station Installation Example



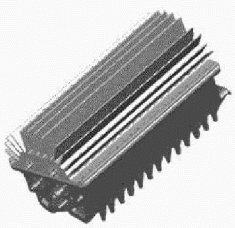
Scalable BMAX-4M Modular BST

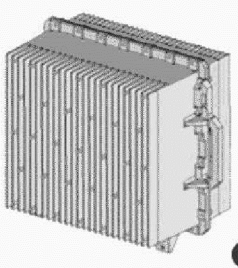
- **Suits for Mobile WiMAX deployments**
  - Dense-Urban / Urban / Suburban / Rural
- **Modular, supporting up to carriers:**
  - 3 sectors w/ 2 carriers
- **Always Support 2nd and 4th order diversity**
- **Carrier Grade Resiliency**
  - Hot swappable functionality
  - Centralized management
  - Design for full redundancy
- **Local and remote management**



Outdoor unit - ODU

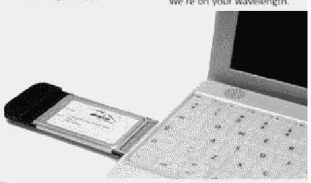
- **Designed to support world wide frequencies**
- **Attached or detached antenna**
- **1RX / 1TX, 34-36dbm, up to 10Mhz, models:**
  - 2.3GHz ROW / WCS for US
  - 2.5Ghz , 2 models, each is 100MHz
  - 3.5Ghz, 4 models, each is 50Mhz
- **2 Rx /1TX 37-39dbm, up to 10Mhz, models:**
  - 3.5Ghz – 1 model, supporting 200MHz
- **4 Rx /2TX 37-39dbm, up to 20Mhz variety of models:**
  - 2.3GHz ROW / WCS (future)
  - 2.5Ghz, BW
  - 3.5Ghz, BW
- **Fully outdoor**
- **Optional an add-on H bracket for easy deployment**





802.16e Certified CPEs

- **Mobile devices are no longer at Customer Premises**
  - Hence CPE is now MS – Mobile Station
- **Three main products**
  - PCMCIA – WiMAX Network Card
  - RGW - Residential Gateway
    - Integrated WiFi AP
    - VOIP services
  - **ODU CPE – MIMO capable**
    - Supports High BW requirements
    - Supports High Coverage requirements
- **Backward compatibility with BreezeMAX Si**



PCMCIA

RGW

Dipole Outdoor Radio
For CPE MIMO

alvarion
We're on your wavelength.

SCI-NetWork

Thank you

SZVÉTEK Ferenc

MOTOTRBO – ÚJ MOTOROLA DIGITÁLIS RÁDIÓK

Miért 12.5kHz TDMA?

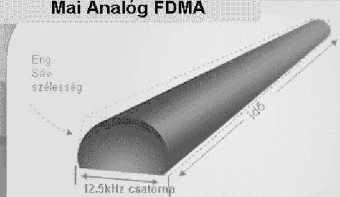
- 12.5kHz TDMA lett kiválasztva az ETSI DMR csoport által, a professzionális felhasználók legjobb kiszolgálása végett
- TDMA sikeresen bevált több kommunikációs szabványban (pl. GSM, DECT, TETRA)
- 12.5kHz csatornaraszter a leghatékonyabb spektrum kihasználtságot eredményezi
- megkönnyíti az egyenes újrafelhasználását a létező PMR spektrumnak
- További előnyök – pl. nagyobb adatátviteli sebesség

MOTOVATION Fercom

2-időréses TDMA 12.5kHz Protokol

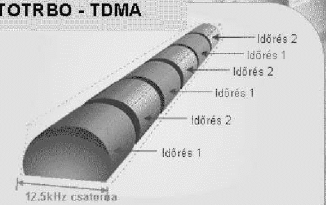
ETSI

Mai Analóg FDMA



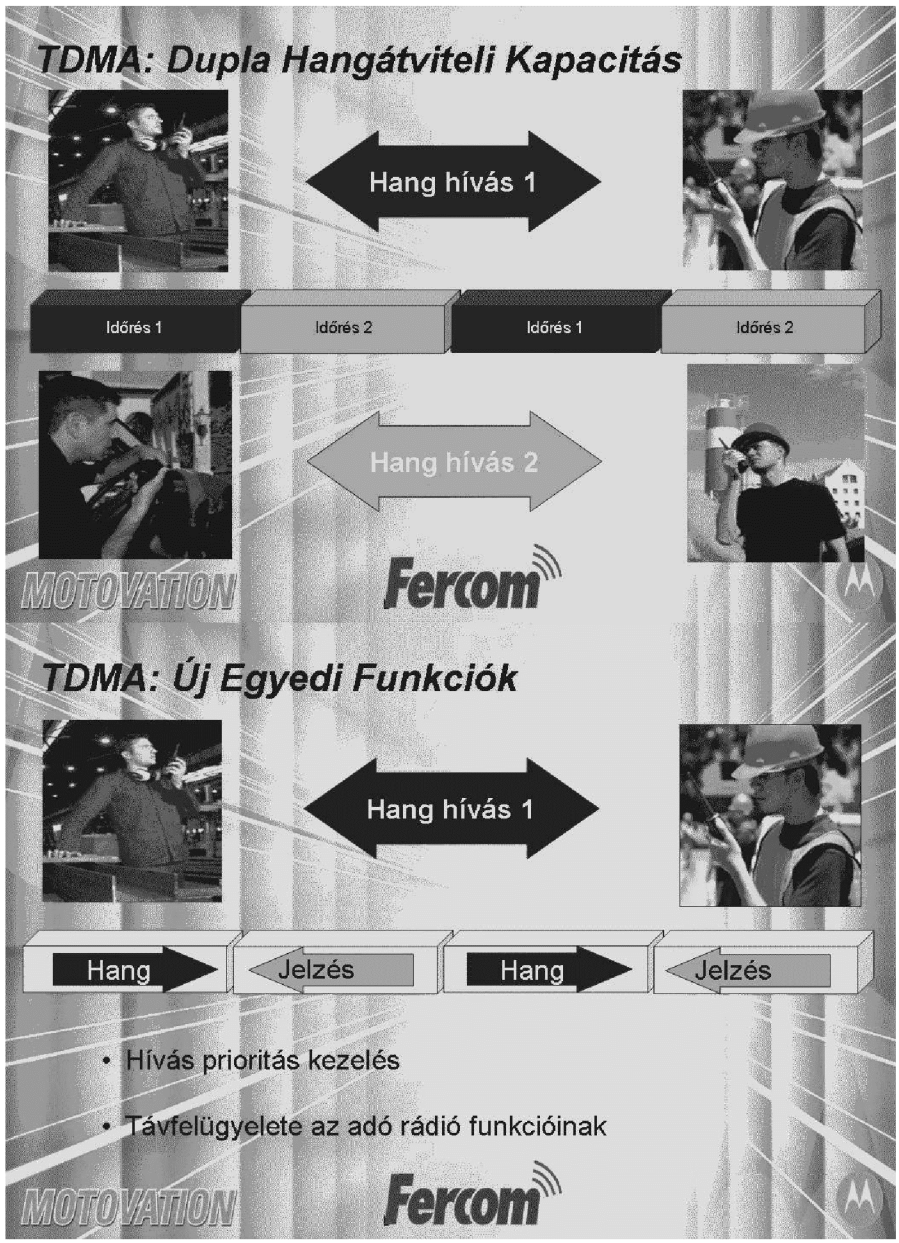
12.5kHz / 25 kHz
– 1 hangátvitel 12.5/ 25kHz csatornán
– 1 átjátszóállomás mindegyik csatornához

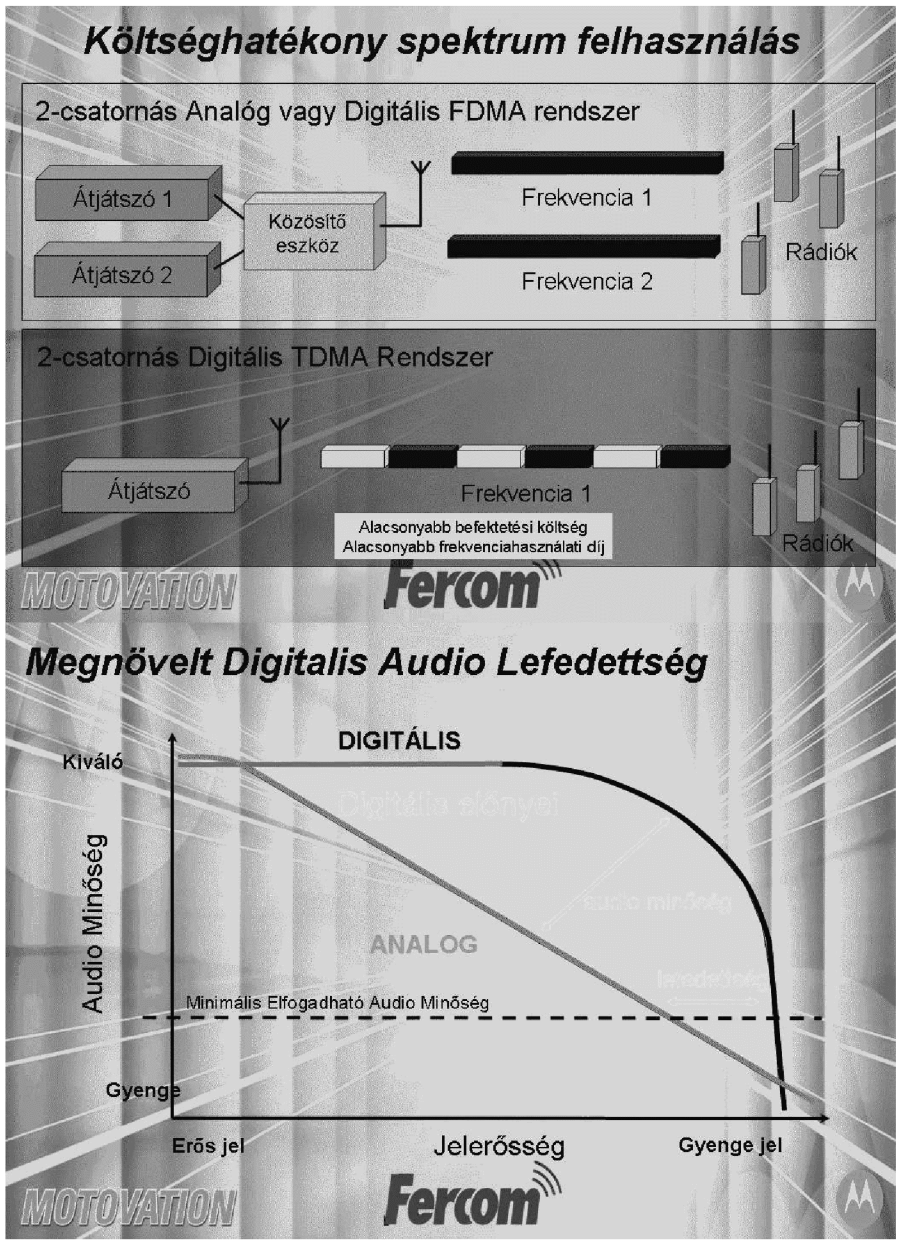
MOTOTRBO - TDMA



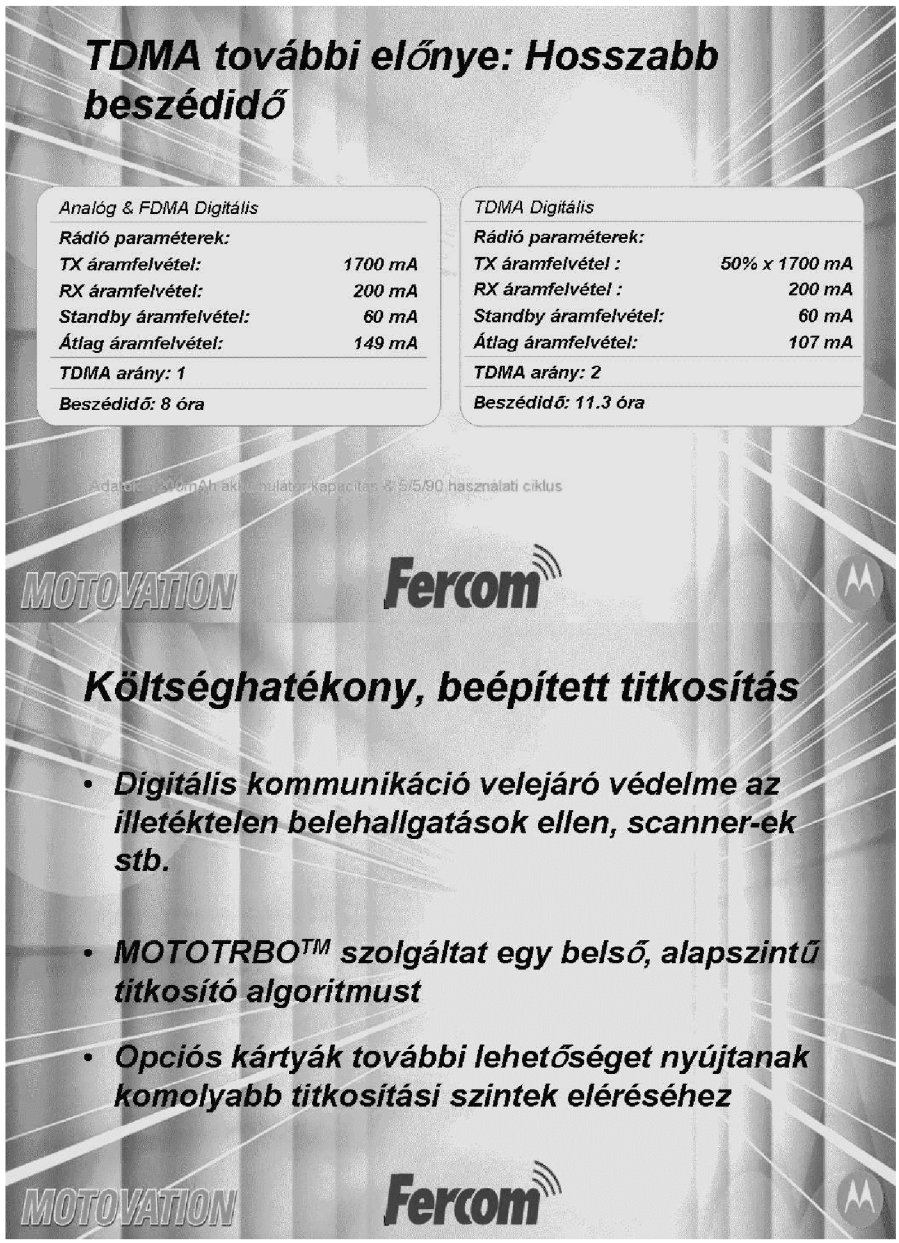
12.5kHz TDMA
– Meglévő csatornát két időrésre osztja
– Kétszeres kapacitást szolgáltat átjátszóállomáson keresztül
– Minőség azonos vagy jobb mint 12.5kHz FDMA
– Közösítő eszközök költségeinek csökkentése

MOTOVATION Fercom


TDMA: Dupla Hangátviteli Kapacitás
Hang hívás 1
Időrés 1
Időrés 2
Időrés 1
Időrés 2
Hang hívás 2
MOTOVATION
Fercom
TDMA: Új Egyedi Funkciók
Hang hívás 1
Hang
Jelzés
Hang
Jelzés
• Hívás prioritás kezelés
• Távfelügyelete az adó rádió funkcióinak
MOTOVATION
Fercom


Költséghatékony spektrum felhasználás
2-csatornás Analóg vagy Digitális FDMA rendszer
Átjátszó 1
Átjátszó 2
Közösítő eszköz
Frekvencia 1
Frekvencia 2
Rádiók
2-csatornás Digitális TDMA Rendszer
Átjátszó
Frekvencia 1
Alacsonyabb befektetési költség
Alacsonyabb frekvenciahasználati díj
Rádiók
MOTOVATION
Fercom
Megnövelt Digitalis Audio Lefedettség
DIGITÁLIS
Kiváló
Audio Minőség
ANALOG
Minimális Elfogadható Audio Minőség
Gyenge
Erős jel
Jelerősség
Gyenge jel
MOTOVATION
Fercom


Növelt Audio Minőség
Adat bemenet
IP Adat Interfész
Hang Bement
AD konverzió
Vocoder
Tördelés Keretbe rendezés
RF Adás
• DVSI AMBE + 2 Vocoder
• Háttérzaj csökkentés
– Érthető kommunikáció zajos környezetben
• Csatornazaj csökkentés
– Csökkenti a zavaró hatásokat (hibakorrekció)
DMR
DVSI Vocoder selected By DMR MoU
MOTOVATION
Fercom
Megnövelt Digitális Hívás és Jelzés
Kiterjesztett hívás és csatorna menedzsment a hatékonyság növelésére
Pont –Alcsoport
Csatorna részfelhasználóinak hívása
Pont-Multipont
Lehetővé teszi a csatorna összes felhasználójának hívását
Késői híváscsatlakozás lehetősége csökkenti az elmaradt hívást
MOTOVATION
Fercom


TDMA további előnye: Hosszabb beszédidő
Analóg & FDMA Digitális
Rádió paraméterek:
TX áramfelvétel: 1700 mA
RX áramfelvétel: 200 mA
Standby áramfelvétel: 60 mA
Átlag áramfelvétel: 149 mA
TDMA arány: 1
Beszédidő: 8 óra
TDMA Digitális
Rádió paraméterek:
TX áramfelvétel : 50% x 1700 mA
RX áramfelvétel : 200 mA
Standby áramfelvétel: 60 mA
Átlag áramfelvétel: 107 mA
TDMA arány: 2
Beszédidő: 11.3 óra
Adatok: 2300mAh akkumulátor kapacitás & 5/5/90 használati ciklus
MOTOVATION
Fercom
Költséghatékony, beépített titkosítás
• Digitális kommunikáció velejáró védelme az illetéktelen belehallgatások ellen, scanner-ek stb.
• MOTOTRBO™ szolgáltat egy belső, alapszintű titkosító algoritmust
• Opciós kártyák további lehetőséget nyújtanak komolyabb titkosítási szintek eléréséhez
MOTOVATION
Fercom

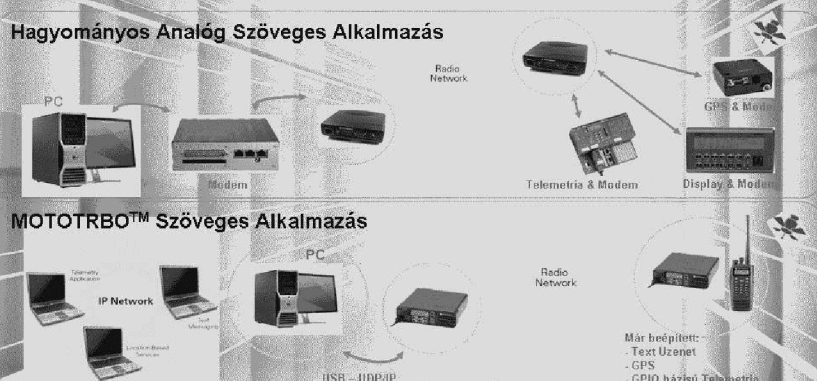
Integrált Adatátviteli Lehetőségek

- Beépített GPS modul
- Beépített adat modem
  - Standard UDP/IP – kompatibilis IP applikációkkal
  - Internet Protokol (IPv4) címzés
  - Kb. 2 kbps védett adatátviteli kapacitás időrésenként
  - Jövőbeli lehetőség – dupla kapacitás dual-slot adatátvitellel

- Standard USB csatlakozás
- Szöveges üzenetátvitel
  - Közvetlen rádió-rádió vagy harmadik fél applikációja (később elérhető)
  - Szabad form (140 karakterig)
  - Előre programozott üzenetek programozói szoftver által (30 üzenetig)

MOTOVATION Fercom

Egyszerű, költséghatékony adat megoldás



MOTOVATION Fercom

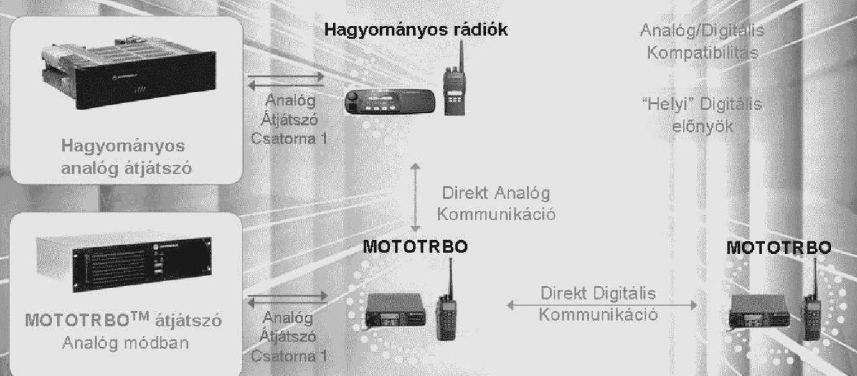

Akadálymentes és Költséghatékony Átállás
• Megfelelés a már meglévő szabályozásnak:
– EN300 086
– EN300 113
• 12.5, 20 & 25kHz csatornaraszter támogatás
• Nincs szükség a meglévő rádiótervek változtatására
MOTOVATION
Fercom
Megbízható befektetés könnyű átállással
– MOTOTRBO lehetővé teszi a rádiónkénti átállást, csatornánkénti átállást, vagy az egész rendszerre vonatkozó átállást
– MOTOTRBO rendszer kettős felhasználással
– MOTOTRBO rádiók képesek pásztázni mind digitális, mind analóg csatornákat
MOTOVATION
Fercom

Akadálymentes és Költséghatékony Átállás

- *Közvetlen kommunikáció Digitális és Analóg rádió között*
  - *MOTOTRBO rádiók támogatják az analóg működést*
  - *Carrier squelch (Vivőre nyitó zajzár)*
  - *CTCSS (PL) & DCS (DPL)*
- *Vegyes módú csatornapásztázás (pl: az analóg és digitális csatornák pásztázása egy időben)*
- *Kézi választás (pl: felhasználó által választható personality-csatorna)*
- *Automatikus választás (pl: vegyes módú csatornapásztázás)*
- *12.5 & 25 kHz analóg sávszélesség támogatott*
- *5-tone opciós kártya támogatott a jövő megjelenésekben*

MOTOVATION Fercom

Lépésenkénti átállás



MOTOVATION Fercom


MOTOTRBO™ Termékválaszték
• Mobil
• DM 3400
• DM 3401
• DM 3600
• DM 3601
• Átjátszó
• DR 3000
• Kézi
• DP 3400
• DP 3401
• DP 3600
• DP 3601
MOTOTRBO™
Professional Digital Two-Way Radio System
• Tartozékok
• Alkalmazások
MOTOVATION
Fercom


MOTOTRBO™ Kézi rádiók áttekintés
– DP 3400/3401/3600/3601
1. Három színű LED
2. Vészhívó gomb
3. Új tartozék csatlakozó RF csatlakozással
4. Nagyméretű PTT gomb
5. 3 oldalsó programozható nyomógomb
6. Csatornaválasztó
7. Ki/Be & hangerő
8. Könnyen használható akkumulátor zár
9. Nagy hangerejű, előre sugárzó hangszóró
10. Mikrofon
– DP 3600/3601
11. Két előlapi programozható nyomógomb
– Két soros kijelző + Alfanumerikus tasztatúra
– Ellenálló, megbízható konstrukció: IP57 víz alá meríthető
– Military Standards 810F
– Egyedi Felgyorsított Élettartam teszt
MOTOVATION
Fercom

DP 3400/3401 Nem kijelzős, kézi készülékek

- UHF 403-470MHz 1-4W
- VHF 136-174MHz 1-5W
- 32 csatorna
- Felhasználó által választható és automatikus analóg/digitális felhasználás
- 3 programozható oldalsó nyomógomb, felső vészhívó gomb
- választható akkumulátor opciók (standard, impres™ & Factory Mutual)
- Egyedi és csoportos töltők (standard & impres™)
- Külső RF port
- IP-over-USB interfész az adatátvitelhez
- Integrált GPS
- Opciós kártya lehetőség
- Kiterjesztett titkosítás

MOTOVATION Fercom

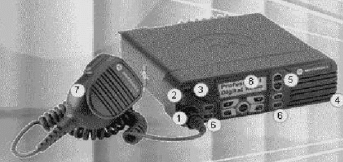
DP 3600/3601 Kijelzős kézi készülék

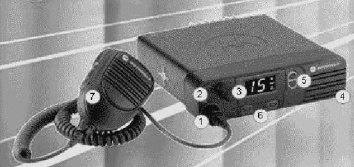
- UHF 403-470MHz 1-4W
- VHF 136-174MHz 1-5W
- 2-soros kijelző
- Támogatott többnyelvűség- Angol, Francia és Spanyol
- 160 csatorna
- 3 programozható oldalsó nyomógomb, 2 előlapi nyomógomb és felső vészhívó gomb
- választható akkumulátor opciók (standard, impres™ & FM)
- Egyedi és csoportos töltők (standard & impres™)
- Külső RF port
- IP-over-USB interfész az adatátvitelhez
- Integrált GPS (DP3601)
- Opciós kártya lehetőség
- Kiterjesztett titkosítás

MOTOVATION Fercom

MOTOTRBO™ Mobil áttekintés

- DM 3400/3401/3600/3601
  1. Ellenálló tartós tartozék csatlakozó
  2. Többszínű LED jelzés
  3. Nagyméretű, könnyen használható hangerő gomb
  4. Nagyteljesítményű hangsugárzó
  5. Nagyméretű, könnyen használható navigációs gombok
  6. Programozható nyomógombok (2 vagy 4)
  7. Kompakt ergonómikus kézibeszélő
  8. DIN kompatibilis beszerelhetőség
- DM 3600/3601
  - Flexibilis, menü vezérelt interfész, felhasználóbarát ikonok





MOTOVATION Fercom

DM 3400/3401 Karakteres kijelző

- UHF 403-470MHz
- VHF 134-176MHz
- 32 csatorna
- 1-25W
- 7-szegmenses kijelző 3 ikonnal
- 2 programozható nyomógomb
- Felhasználó által választható vagy automatikus analóg/digitális üzemmód
- IP-over-USB interfész az adatátvitel számára
- integrált GPS
- Opciós kártya lehetőség
- Titkosítás

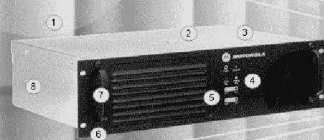
MOTOVATION Fercom

DM 3600/3601 Raszteres kijelző

- UHF 403-470MHz
- VHF 134-176MHz
- 1-25 W
- 160 csatorna
- 2-soros kijelző 9 ikonnal
- Több nyelv támogatása Angol, Francia és Spanyol
- 4 programozható nyomógomb
- Felhasználó által választható vagy automatikus analóg/digitális üzemmód
- IP-over-USB interfész az adatátvitel számára
- integrált GPS
- Titkosítás

MOTOVATION Fercom

MOTOTRBO™ Átjátszó áttekintés



1. 100% 24 órás működés
2. Két egyidejű hang vagy adat csatorna (digitális üzemmódban)
3. Beépített tápegység
4. Analóg vagy digitális működés
5. LED-ek egyértelműen mutatják az adó és vételi módokat
6. Rack-be vagy falra szerelhető
7. Könnyen, stabilan telepíthető
8. Automatizált háttérakkumulátor töltés

MOTOVATION Fercom

DR 3000 Átjátszó

- UHF 403-470MHz
- VHF 136-174MHz
- 25-40 W
- 1-25 W
- 100% 24 órás működés a legmagasabb teljesítmény fokozaton
- Szoftveresen állítható analóg vagy digitális működésre
- Interfész az UPS rendszerekhez
- Jövőben több kapcsolódási felület:
  - Basic I/O
  - USB
  - Ethernet
  - telefon
  - Command & Control
  - UDP/IP

MOTOVATION Fercom

MOTOTRBO Tartozékok

MOTOTRBO

Audio

Audio tartozékok széles skálája a rádió adta lehetőségek kiterjesztésére

Akkumulátorok

Tervezhetően hosszútávú teljesítményt nyújtanak

Töltők

Adaptív, automatikus kondicionálását biztosítják az IMPRES akkumulátoroknak

Hordtáskák

Védelmet nyújtanak és kényelmes használatot

Mobil Tartozékok

Mikrofonok, bázisállomás tartók, hangszórók…

MOTOVATION Fercom

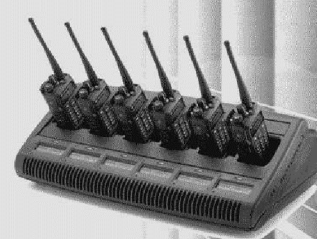
Kiterjesztett Audio Tartozék Interfész

- Programozható gombok elérhetőek a tartozékokon
- Kibővített audio funkciók közel azonos érzetet nyújtanak különböző tartozék fajtáknál
- Megfelel IP57 szabványoknak (csak kézirádió esetében)
- Antenna jel
- USB lehetőség PC csatlakozáshoz

MOTOVATION Fercom

IMPRES™ Smart Energy System

- Nincs többé kézi akkumulátor karbantartás
- Optimalizált életciklus
- Több férőhelyes töltők
- Töltők kompatibilisek a nem-IMPRES akkumulátorokkal
- Kiterjesztett akkumulátor garancia
- IMPRES egy férőhelyes töltő alap tartozékként szállítva a rádióhoz
- IMPRES FM akkumulátor elérhetőség



MOTOVATION Fercom


Új, Egyedi előnyök a vevőink számára
Növelt audio minőség
Dupla beszéd kapacitás
Hosszabb akkumulátor használhatóság
Költséghatékony adat kommunikáció
Osztott Alkalmazások
Csökkennek a használati költségek
Nyílt ETSI Szabványok
Könnyű átállás
MOTOVATION
Fercom
Köszönöm megtisztelő figyelmüket!

Alcatel-Lucent

ALCATEL-LUCENT END-TO-END IP WIRELESS BROADBAND SOLUTIONS FOR WIMAX