A ZRÍNYI MIKLÓS NEMZETVÉDELMI EGYETEM KIADVÁNYA

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET

ALAPÍTVA 1949

MAGYAR HONVÉDSÉG TÁMOGATÓ DANDÁR

Kommunikáció 2009
Communications 2009

HÍRADÓ TANSZÉK

ZMNE

BJKMK

10

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, 2009-ben az ISO 14001 szabványoknak is sikeresen megfelelt. A Pro-M felkészültségével bizonyítja elkötelezettségét az EDR felhasználók, valamint a számukra elengedhetetlen információbiztonság iránt. A vállalat célja a jelenlegi felhasználói körön kívüli ügyfelek jövőbeni – a megszokott kiemelkedő színvonalú – kiszolgálása. A vállalat a civil TETRA felhasználás támogatásában hasonló eredmények elérését tűzte ki célul maga elé.

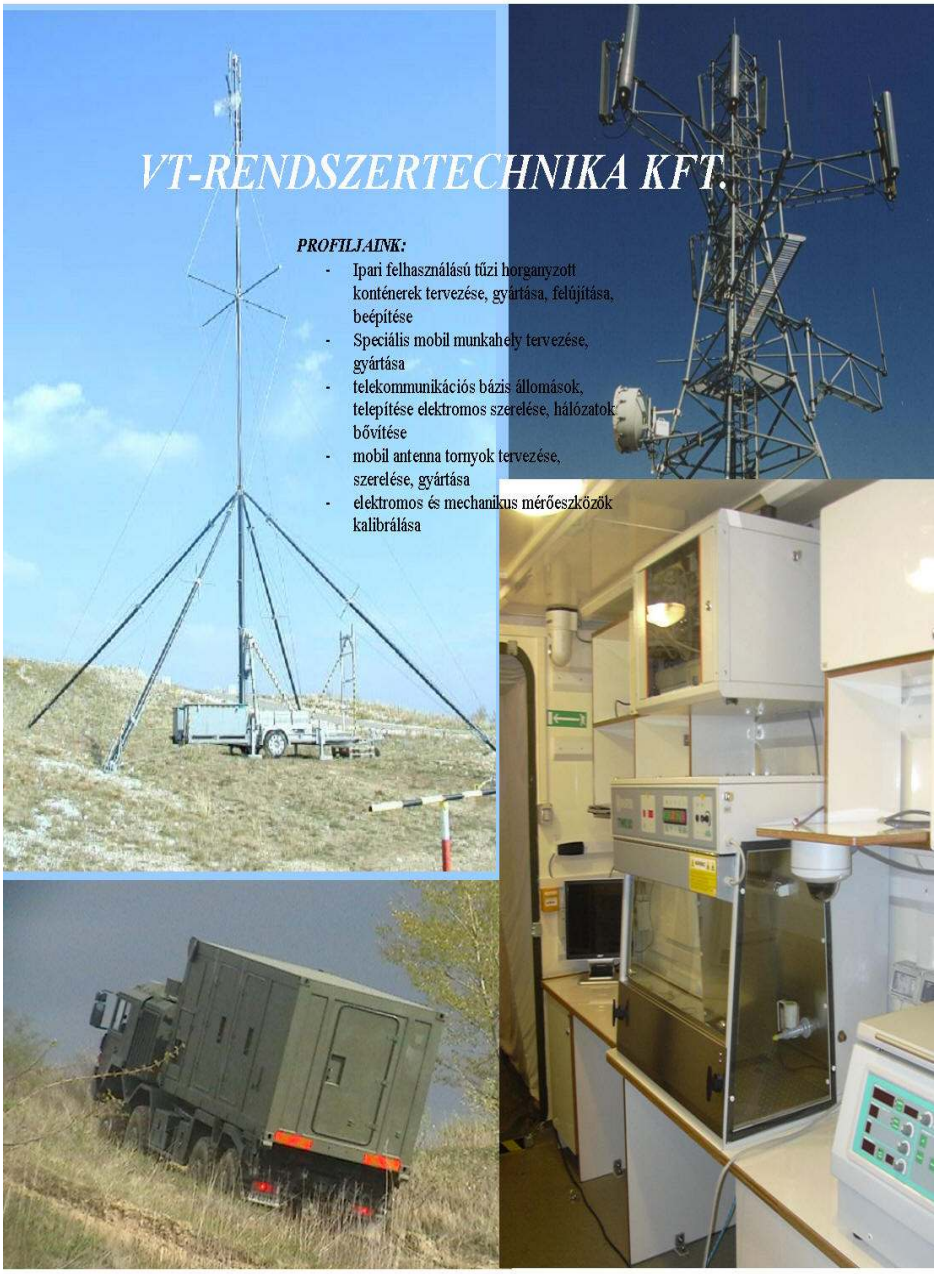
Bővebb tájékoztatásért látogasson el a **www.pro-m.hu** honlapra.

Pro-M Zrt.
A Magyar Telekom Csoport tagja

VIDEOTON
VT-Rendszertechnika Kft

AQAP-2110
No: 196340
No: 159610

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

Zrínyi Miklós Nemzetvédelmi Egyetem

Budapest, 2009. október 14.

A tudományos kiadványt lektorálták:
Prof. Dr. Rajnai Zoltán mk. alezredes, egy. tanár
Dr. habil. Sándor Miklós nyá. ezredes, 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, 150 példányban

ISBN 978-963-7060-70-0

TARTALOMJEGYZÉK

A Jubileumi nemzetközi szakmai tudományos konferencia kommunikációs partnere:

T-Systems

A tudományos konferencia támogatói:

Alcatel-Lucent Magyarország Kft.

Fercom Kommunikációs Kft.

Hoeller Electonic Kft.

Hírközlési és Informatikai Tudományos Egyesület

Hungaro DigiTel Kft.

Kapsch Telecom Kft.

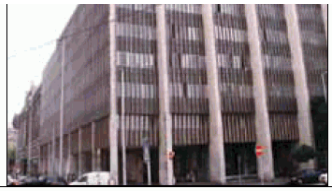
Magyar Villamos Művek Zrt.

Pro-M Zrt.

SCI-Network Távközlési és Hálózatintegrációs ZRt.

SIEMENS ZRt.

VIDEOTON VT-Rendszertechnika Kft.



A CÉG CÍME

Hírközlési és Informatikai Tudományos Egyesület
1055 Budapest, Kossuth tér 6–8. 422. iroda
Telefon: 353-1027
Fax: 353-0451
E-mail: info@hte.hu
Web: www.hte.hu

MENEDZSMENT

Dr. Sallai Gyula
elnök

Horváth Pál
főtitkár

Nagy Péter
ügyvezető igazgató

A Hírközlési és Informatikai Tudományos Egyesület (HTE) a magyar távközlés, műsorszórás, elektronika és információtechnológia területén dolgozó műszaki, gazdasági, tanácsadó és oktatási szakemberek önkéntes és független szakmai egyesülete. A HTE-nek mintegy 1300 egyéni és közel száz jogi tagja van. A jogi tagok között egyaránt található ipari, kereskedelmi, szolgáltató, kutató-fejlesztő tevékenységet végző nagyvállalat és kisvállalkozás, oktatási és más intézmény. Az 1949-ben alapított egyesület tagja a Magyar Természettudományi Egyesületek Szövetségének, a MTESZ-nek, valamint az Institute of Electrical and Electronics Engineering, Inc. (IEEE) és az IEEE Communications Society testvéregyesülete.

Az egyesület küldetésének tekinti az információs és kommunikációs technológiák konvergenciájának a segítését, tagjai szaktudásának és szakértelmének a bővítését a hazai és nemzetközi műszaki és tudományos eredményekről szóló tájékoztatással, a szakterület társadalmi jelentőségének és érdekeinek képviseletét, valamint az eltérő szakmai vélemények és feladatok összehangolását. Küldetésének megfelelően a HTE kiváló lehetőséget nyújt a szakterület új eredményeinek, trendjeinek a megismerésében, az egyes részterületek szakmai tapasztalatcseréjében, a cégek, cégcsoportok eredményeinek a megismertetésében, a szakemberek egymás közötti kapcsolattartásában. Komplex tudását felhasználva ugyanakkor a szakterületét érintő műszaki, gazdasági és társadalmi kérdések elemzésében, a vélemények szintetizálásában és az érintett tudományos, ipari, szolgáltatói, oktatói és államigazgatási szervezetek felé való kommunikálásában is rendszeresen szerepet vállal.

Munkáját részint az egyes részterületekre koncentráló szakosztályokba szerveződve végzi, részint áttekintő jellegű nagyrendezvények létrehozásával, szervezésével látja el. Rendszeresen megrendezett konferenciái például a Távközlési és Informatikai Projekt Menedzsment Fórum, a Távközlési és Informatikai Hálózatok Szeminárium és Kiállítás vagy a Televízió és Hangtechnikai Konferencia és Kiállítás.

Ugyanakkor a HTE nemzetközi konferenciák hazai szervezésében is részt vállal mind szakmai, mind logisztikai téren, ilyen volt például a World Telecommunications Congress 2006, a 16th IST Mobile and Wireless Communications Summit 2007, a Networks 2008 vagy az IEEE Wireless Communications and Networking Conference 2009.

A HTE saját kiadású, tudományos igényű szaklapja a Híradástechnika folyóirat, amelynek évente hat száma magyarul, négy száma angol nyelven jelenik meg. A folyóirat szerkesztését a hazai szerkesztőbizottság mellett egy 18 tagú International Advisory Committee is segíti. A HTE egyéni és jogi tagjait az egyesület életéről, rendezvényeiről és a szakma érdekesebb híreiről a HTE Hírlevél havonta tájékoztatja.

CÉGTÖRTÉNET

1949
Megalakult a Híradástechnikai, Finommechanikai és Optikai Tudományos Egyesület (HTE), a cégbejegyzés dátuma 1949. január 29-e. Irodája az V. kerületi Szalay u. 4. szám alatti épületben volt.

1952
A tagok egy része 1950-ben kiválik és megalakítja az Optikai és Kinotechnikai Tudományos Egyesületet. A HTE neve ekkor lett Híradástechnikai Tudományos Egyesület. 1952-ben a tagok egy része megalakítja a Méréstechnikai és Automatizálási Tudományos Egyesületet.

1968
Az átalakulást követve a postai szakemberek átléptek a Közlekedéstudományi Egyesület (KTE) postai tagozatába, majd 1985-ben visszatértek a HTE-be.

1998
A HTE tevékenysége a távközlés és az informatika konvergenciájának következtében egyre inkább összefonódik az informatikai területtel, ezt kifejezve nevet is változtat, új neve: Hírközlési és Informatikai Tudományos Egyesület.

2009
A HTE a megalakulásának 60. évfordulója tiszteletére a 2009-es évet jubileumi évnek nyilvánította. Az év kiemelkedő eseménye lesz a november 4-ei jubileumi HTE Kongresszus, amelyet a 60. születésnap jegyében rendeznek meg.

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.
ARMCOM Zrt.
Fercom Kommunikációs Kft.
Hoeller Electronic Kft.
Hírközlési és Informatikai Tudományos Egyesület
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
MH Támogató Dandár

A szervező bizottság elnöke:
Prof. Dr. 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

A KOMMUNIKÁCIÓ konferencia-sorozat tizedik évfordulóján tisztelettel köszöntjük Önt.

Amikor nekiláttunk az első konferencia szervezésének, mi magunk sem gondoltuk azt, hogy konferenciánk az országhatárokon túlnyúlva évről-évre sikeresebb és színvonalában emelkedett lesz. Előadóink, köztük páran ma már a tanszék tiszteletbeli tagaju, professzorok, PhD doktorok, PhD hallgatók, tanárok, tanártársaink, vezető ipari szakemberek lettek.

Sikerült egy asztalhoz ültetni a gyártót, a felhasználót, a megrendelőt. Mindenkit, aki a híradástechnika gyártásában, üzemeltetésében – akár katonai, akár polgári viszonylatban - érdekelt.

Új eszközöket, eljárásokat, eljárási módokat mutatunk be, sok esetben az országban elsőként, a gyakorlatban alkalmazva.

Amikor ezt a jubileumi kiadványt, a Kommunikáció 2009 (Communications 2009) tudományos kiadványának könyv változatát kezükbe veszik, kérjük gondoljanak az elmúlt évek sikeres és kevésbé sikeres konferenciáira, a szervezőkre, az előadókra és a résztvevőkre.

Tekintsünk bizakodva a következő tíz év elé.

Budapest, 2009. 09. 29.

A szervező bizottság

VÖRÖS Béla[1]

60 ÉVE ALAKULT MEG A MAGYAR NÉPHADSEREG

A II. VILÁGHÁBORÚ utáni fegyverszüneti egyezmény megkötése, az új demokratikus hadsereg szervezése

1944 őszén a magyar nép sorsfordulóhoz érkezett. Az európai népeknek oly sok szenvedést okozó fasiszta Németország és csatlósai számára nyilvánvalóvá vált, hogy a szovjet és a szövetséges hadseregek csapásai következtében elvesztették a háborút.

Németország szövetségesei ezt felismerve egymás után kiléptek a háborúból, egy részük fegyverrel fordult szembe vele.

Szeptember végére a szovjet csapatok elérték Magyarország határát, az ország teljes csődbe, a végső pusztulás szélére jutott. Az antifasiszta erők a Magyar frontba tömörülve követelték Horthy Miklós kormányzótól és a kormánytól, hogy Magyarország a szövetséges hatalmakkal szemben szüntesse be az ellenségeskedést, kössön fegyverszünetet és üzenjen hadat Németországnak. A nyugati szövetséges hatalmak közölték, hogy Horthy-éknak a fegyverszünetet a Szovjetuniótól kell kérni.

1944. szeptember végén magyar delegáció ment Moszkvába, amelynek tagjai: Faragó Gábor vezérezredes, gróf Teleki Géza és Szent-Iványi Domokos voltak.

1944. október 11-én megkötötték az előzetes fegyverszünetet. Ennek végrehajtását azonban nem készítették elő, nem szervezték meg. Horthy október 15-én fegyverszünetet kérő proklamációjáról előzőleg tájékoztatták Németországot. A proklamáció október 15-én déli 12 órakor hangzott el a rádióban.

A németek még aznap délután Horthyt és kormányát lemondásra és Szálasi Ferenc nyilasvezér miniszterelnökké való kinevezésére kényszerítették.

A nyilas uralom a németekkel szövetkezve, a Magyar Királyi Honvédség részvételével a háború folytatása mellett foglalt állást. Az ezt követő nyolc hónap alatt az egész országot hadszíntérré változtatták. A Szálasi kormány elrendelte minden 14-70 éves magyar állampolgár hadkötelezettségét nemre való tekintet nélkül.

A németek oldalán harcba kényszerített magyar tisztek és katonák egy része felismerte, hogy a háború további folytatása esztelenség. Tömeges volt a szökések száma, egyre többen adták meg magukat a szovjet hadseregnek.

A Magyar Nemzeti Függetlenségi Front 1944. december 2-án alakult meg Szegeden a Független Kisgazdapárt, a Magyar Kommunista Párt, a Szociáldemokrata Párt, a Nemzeti Parasztpárt, a Polgári Demokrata Párt és a Szakszervezetek részvételével.

A kommunista párt akcióprogramját fogadták el. Ez célul tűzte ki a nemzet aktív részvételét az ország felszabadításában, a fasiszta szervezetek feloszlatását, a háborús bűnösök felelősségre vonását, radikális földreformot, a dolgozók helyzetének javítását és a sztrájkjogot.

[1] Szerző: Vörös Béla nyá mk. ezredes

1944. december 14-én Debrecenben megtartotta alakuló ülését az Ideiglenes Nemzetgyűlés előkészítő bizottsága.

A bizottság a szövetséges nagyhatalmak hozzájárulásával és a Függetlenségi Frontba tömörült pártok megegyezése alapján jött létre. A felszabadult országrész közel 50 helységében választásokat tartottak. Az Ideiglenes Nemzetgyűlésben 230 képviselő foglalt helyet. 1944. december 21-én összeült országgyűlés megválasztotta az Ideiglenes Nemzeti Kormányt. Miniszterelnök Dálnoki Miklós Béla vezérezredes, a honvédelmi miniszter Vörös János vezérezredes lett. A kormányban 3 kommunista párti, 2 szociáldemokrata párti, 1 parasztpárti, 2 kisgazdapárti, 4 pártonkívüli volt.

Az Ideiglenes Kormány a Függetlenségi Front programját fogadta el. Legsürgősebb feladatának tekintette a fegyverszünet megkötését a Szovjetunióval és a szövetséges nagyhatalmakkal. A német elnyomók és nyilas bérenceik elleni harc és hazánk felszabadításának meggyorsítása érdekében az Ideiglenes Nemzeti Kormány megszervezte a nemzeti haderőt, a magyar függetlenség és az állami szuverenitás egyik legfőbb biztosítékát.

1944. december 28-án a Minisztertanács az Ideiglenes Nemzetgyűlés felhatalmazása alapján hadat üzent Németországnak.

A magyar fegyverszüneti egyezményt 1945. január 20-án írták alá Moszkvában. Ebben Magyarország elismerte, hogy elvesztette a háborút. Tudomásul vette, hogy megszüntette a háborúskodást a szövetségesek ellen és hadat üzent Németországnak. Kötelezte a magyar kormányt, hogy fegyverezze le az ország területén lévő német csapatokat, a német hadfelszereléseket hadizsákmányként adja át a szövetségeseknek és internálja a német állampolgárokat.

Nyolc gyaloghadosztállyal a szövetségesek oldalán vegyen részt a háborúban és az ország területén biztosítsa a szovjet csapatok szabad mozgását.

Magyarország vonja vissza csapatait és közigazgatását az 1937. december 31. előtti határok mögé.

Utasította a magyar kormányt: helyezze hatályon kívül az úgynevezett zsidótörvényeket, tiltsa be a szövetséges hatalmak elleni propagandát.

Magyarország az okozott károkért köteles kártérítést fizetni oly módon, hogy 300 millió dollárból 200 milliót a Szovjetunió kapjon, míg 100 millió dolláron Csehszlovákia és Jugoszlávia osztozzon.

A fegyverszüneti egyezmény betartásának ellenőrzésére Szövetségi Ellen-őrző Bizottságot állít fel, működésének anyagi feltételeit a magyar kormánynak kell viselni.

A magyar kormány a fegyverszüneti egyezmény előírásait 1945 nyarára a jóvátételt és az anyagi ügyeket leszámítva teljesítette.

A fegyverszüneti szerződés megkötését követően azonnal megkezdődött az új magyar hadsereg szervezése. A kormány kiadta a toborzásról szóló felhívást.

Az első magyar alakulatok, amely a szovjet hadsereg alárendeltségében, de magyar katonai vezetés alatt működött: az 1. Magyar Vasútépítő Hadosztály 1945. január közepére alakult meg 3668 fővel. Feladata a hidak, vasutak, alagutak helyreállítása és a front utánpótlási útjainak biztosítása volt.

A Budai Önkéntes Ezred a Budán körülzárt és a szovjet hadsereg oldalára átállt magyar tisztekből, katonákból alakult meg, akiket a hadifogolytáborokból szerveztek.

A magyar katonák harcoltak a Déli pályaudvaron és környékén, a Svábhegyen és részt vettek a Várhegy ostromában is. A 2500 fős alakulatból 600-an haltak hősi halált.

Az Ideiglenes Magyar Kormány toborzási felhívása a felszabadított városokban és falvakban 1945. január 30-án jelent meg.

A magyar katonai vezetés egy időben négy hadosztály megszervezéséhez fogott hozzá. Az 1. hadosztály Jászberényben, az 5. hadosztály Szegeden, a 6. hadosztály Debrecenben, a 7. hadosztály pedig Miskolcon alakult.

1945. április második felére sok nehézség és akadály ellenére két hadosztály, az 1. és 6. került olyan helyzetbe, hogy a szovjet hadsereg legfelsőbb parancsnoka engedélyezte elvonulásukat a hadműveleti területre.

A hadsereg személyi állományának biztosítása elvileg két úton volt lehetséges: sorozással, kötelező behívással, illetve önkéntes jelentkezés, toborzás útján.

A kötelező behívás azért nem volt lehetséges, mert a katonakötelesek többsége még a fronton vagy hadifogolytáborokban volt. Rendeletet adtak ki, amely kimondta: "Azok a honvéd egyének, akik az új honvédségbe önként jelentkeznek (ideértve az önként jelentkező hadifoglyokat is) és szolgálatot teljesítenek, földhöz juttatandóknak minősülnek. Elhalálozásuk esetén ez a jog a legközelebbi hozzátartozókat illeti meg."

A 6. hadosztályba a volt partizánok, Nyíregyháza, Hajdúhadháza, Debrecen és más hadifogolytáborok katonái és a környék lakói jelentkeztek. A hadosztály létszáma 8500 fő, parancsnoka Székely László vezérkari ezredes. Szervezete: a 16., a 17., a 18. gyalogezred, a 11. tábori tüzérezred, a 6. utászzászlóalj, a 6. híradószázad, a 6. gépágyús üteg és a 6. seregvonat.

Fegyverzetük a Magyar Királyi Honvédségben rendszeresített, a szovjet hadsereg által zsákmányolt fegyverekből állt.

Az 1. hadosztály Jászberényben alakult meg. Parancsnoka Szalai Tibor ezredes. Szervezete hasonló volt a 6. hadosztályéhoz: az 1., a 2., a 3. gyalogezred, az 1. tüzérezred, az 1. légvédelmi ágyús üteg, az 1. utászzászlóalj, az 1. híradószázad, az 1. hadosztályvonat.

A két hadosztálynál bevezették a nevelőtiszti intézményt, amely az új hadsereg demokratikus jellegét volt hivatva biztosítani. A régi szolgálati szabályzat jó néhány pontját törölték, így a katonák kikötését, stb.

Az 1. és a 6. gyaloghadosztály megszervezése, harcbavetésre való felkészítése lényegében április elejére befejeződött. Április második felében kaptak parancsot az Ausztriába való indulásra. A hadosztályok a III. Ukrán front alárendeltségébe kerültek. Mivel a háború befejeződött, csak kisebb tisztogató akciókban vettek részt.

Május 13-án az 1. és a 6. gyaloghadosztály a III. Ukrán front parancsnokától parancsot kapott a hazatérésre.

A Magyar Honvédség helyzete a II. Világháború befejezése után

Az 5. és a 7. gyaloghadosztályt a Szövetségi Ellenőrző Bizottság engedélyével az Ideiglenes Nemzeti Kormány 1945 májusában-júniusában feloszlatta. Az idősebbeket leszerelték, a fiatalabbakat a szervezés alatt álló határvadászzászlóaljakhoz osztották be. A határőrség parancsnokává Pálffy György ezredest nevezték ki.

A határőrzászlóalj egy jó ideig a hadsereg legnagyobb létszámú része lett. A honvédség létszámát a Szövetségi Ellenőrző Bizottság engedélyével jelentősen csökkentették. 1945 nyarán 65000 főre, őszre 40000-re, 1946 tavaszára 20000 főre csökkentették.

1947. február 10-én, a párizsi magyar békeszerződésben, amit az Országgyűlés júniusban törvénybe iktatott, Magyarország visszanyerte teljes szuverenitását és függetlenségét. A Szövetségi Ellenőrző Bizottság beszüntette tevékenységét. A békeszerződés Magyarországnak 65000 fős hadsereget engedélyezett. Ötezer főnyi személyzettel 90 repülőgépet tarthatott meg. A békeszerződés megtiltotta atomfegyverek, rakéták tartását és hadianyag gyártását.

A békeszerződés értelmében a megszálló csapatokat 90 napon belül ki kellett vonni Magyarországról, de lehetővé tették, hogy a Szovjetunió az ausztriai szovjet megszállási övezet utánpótlási vonalainak biztosítására csapatokat tarthasson az országban. Ennek létszáma 1955-ig, az Ausztriával kötött békeszerződés megkötéséig 60-80 ezer fő volt.

1955 után a szovjet csapatok magyarországi tartózkodását 1989-ig a Varsói Szerződés politikai- katonai szervezete tette lehetővé.

A magyar honvédség szerepe a háborús károk helyreállításában, az újjáépítésben

A II. Világháború befejezése után az országban a békét és a biztonságot 1947 februárjáig a Szövetségi Ellenőrző "háromhatalmi" (szovjet, angol, amerikai) Bizottságának vezetésével, a megszálló szovjet csapatok biztosították.

Ez a bizottság határozta meg a honvédség, benne a határőrség, a rendőrség, az összes fegyveres szervezet létszámát, szervezetét, fegyverzetét.

A Szövetségi Ellenőrző Bizottság úgy döntött, hogy 1945. május után a frontról hazatérő honvédalakulatokból munkásegységeket kell létrehozni. A háború az egész ország területén óriási károkat okozott. Az ország kifosztva, a városok, városrészek romokban, a vasúti sínek felszaggatva, hidak felrobbantva, hírközlő központok összezúzva, a földekben és vizekben halált rejtő lövedékek, aknák voltak.

Megsemmisült 1424 közúti és 848 vasúti híd.

1100 km vasúti vágányt tettek tönkre. A dunai, tiszai hidakat is felrobbantották. Ezért elsődleges feladat volt a hírközlés, a szállítás, az összeköttetés megteremtése. A honvédségi munkásalakulatokra azért is szükség volt, mert az országban kevés volt a munkáskéz. Több mint egymillió ember halt meg, 600 ezer férfi volt hadifogságban, egymillió ember menekült nyugatra és vándorolt valahol Európa útjain.

1945 júniusában alakult meg az újjáépítési dandár, az újjáépítés segítése céljából. Októberig 5000 fő dolgozott a Budapest-Cegléd, a Szolnok-Debrecen, a Rá-

kos-Hatvan vasútvonalon és vasúti hidakon, de dolgoztak a Déli vasúti összekötő hídon, később a Kossuth híd építkezésén is.

1945 októberében alakult meg az 1. műszaki hadosztály, 10000 fő körüli létszámmal. Zömében a budapesti hidak újjáépítésén, továbbá a szolnoki, a szentesi, az algyői tiszai hidak helyreállításán dolgoztak. A műszakiak végezték a Duna, később a Balaton aknamentesítését. Ők tisztították meg a földeket a fel nem robbant bombáktól, lőszerektől és aknáktól.

Ebben a munkában sokan életüket vesztették.

1946-ban 2 hónap alatt 558 tűzszerész 1 639 096 db robbanótestet hatástalanított. Ezek a katonák a nap minden órájában szembekerültek a halállal. 1946 végéig 200 aknakutató és tűzszerész áldozta életét az ország újjáépítéséért folyó sajátos munkában. Több százra tehető azok száma, akik megrokkantak. Még 1997-ben több, mint 50 év után is haltak meg tűzszerészek a háborúból visszamaradt robbanó szerkezetek hatástalanítása közben.

Az előzőekben már szó volt a határőrségről. Szerepük 1946 tavaszától vált igen jelentőssé. Kettős feladatuk volt. Egyrészt meg kellett akadályozni a csempészést, amely az inflációs időkben igen nagy mérteket öltött, erősen veszélyeztetve ezzel a stabilizációt, másrészt meg kellett akadályozni, hogy a közönséges bűnözők szabadon járjanak-keljenek át határon. 1946-ban 6989 jogtalan határátlépőt, 5726 csempészt, 345 menekülő SS katonát, szökött háborús bűnöst fogtak el. Ez alatt az idő alatt fegyveres harcban 3 határvadász katona halt meg, 17-en pedig súlyosan megsebesültek.

1945-1948 között katonáink a nemzet becsületéért fogtak fegyvert, markolták meg a munka szerszámait. A honvédség akkori vezetőinek többsége becsülettel teljesítette kötelességét. Egy részük később a Magyar Néphadseregben a legmagasabb rendfokozatokig is eljutott.

Sajnos, ezek az évek sem voltak hibáktól, bűnöktől mentesek.

1945 után a Magyarországra visszatért hivatásos katonákat az újjászerveződő honvédség igazoló bizottságai elé állították. E bizottságok tagjai a koalíciós pártok és a honvédség képviselőiből álltak, ők voltak hivatottak eldönteni és minősíteni az egykori hivatásos tisztek, tábornokok második világháborús magatartását, az új honvédségben való alkalmasságukat.

Az igazoló bizottság döntései: dicsérettel igazolt, igazolt, rendfokozatának megfosztása, vezetői állásra alkalmas, vagy alkalmatlan. Az igazolt tiszteknek megmondták, hogy szolgálatukra igényt tartanak vagy sem

A katonai vezetésben csak azok a nélkülözhetetlen, feddhetetlennek tekintett egykori legfelsőbb katonai vezetők maradhattak, akik élvezték a baloldali koalíciós pártok bizalmát és szakértelmükre szükség volt.

1948 után száz nyugdíjas katonatisztnek a nyugdíját csökkentették, majd megvonták. A volt legfelsőbb szintű katonai vezetőket otthonaikból kitelepítették. A Népbíróság és a katonai bíróságok 53 elmarasztaló ítéletet hoztak. Ezek egy része megalapozatlan volt, ezért 1989 után közülük többet rehabilitáltak.

Sajnos a II. Világháborús hivatásos katonatisztek többségét megbízhatatlannak ítélték. Kezdetben még a munkavállalási lehetőségeiket is korlátozták, kivéve a mérnökökét és orvosokét, akiknek többsége gyakorolhatta hivatását. 1953 után az

ellenük folyó diszkriminációt megszüntették, a kitelepítettek hazatérhettek. Csak az 1960-as években mehettek normális körülmények között nyugdíjba.

Az új honvédség vezetésébe 1945 után sok tartalékos tiszt került hivatásos állományba, vezető beosztásokba. Pár év alatt magas tábornoki beosztásba néhány, antifasiszta beállítottságú, volt hivatásos tiszt került.

Például:

- Révai Kálmán huszárfőhadnagyból- vezérőrnagy,
- Pálffy György századosból- altábornagy,
- Sólyom László századosból- altábornagy,
- Köteles Jenő főhadnagyból- altábornagy,
- Variházy Oszkár őrnagyból- vezérőrnagy,
- Görgényi Dániel századosból- vezérőrnagy,
- Király Béla őrnagyból- vezérőrnagy, 1990 után vezérezredes lett.

Közülük többen koncepciós perek áldozatai lettek.

1947 júniusától a békeszerződés megkötése után az ország visszanyerte önállóságát. A kormány, benne a Honvédelmi Minisztérium maga határozta meg a honvédelemmel kapcsolatos feladatokat. Természetesen ez sem nélkülözte a belső pártharcokat.

A Honvédelmi Minisztérium 1947-1948. évre tervet készített. Ebben a hadsereg létszámának stabilizálását határozta meg. A hadosztályok továbbra is kerethadosztályok maradtak, ami azt jelentette, hogy a törzseket, szervezeteket továbbra sem töltötték fel. A Határőr-parancsnokságot Határőr-Főparancsnokságra változtatták.

Megszüntették a műszaki vezetési törzset, s csapatait az újonnan szervezett műszaki kiképző tábor alá rendelték. Önálló fegyvernemmé alakult a honvéd hadihajós osztály. HM közvetlenként egy önálló repülőszázadot, valamint egy rádiófelderítő századot szerveztek.

1947 júniusában honvédelmi miniszteri rendelet mondta ki, hogy október 1-jével Honvéd Kossuth Akadémia néven tiszti és tiszthelyettesképző iskolát állítanak fel. Elrendelték a tisztek továbbképzését a Hadiakadémián.

Az 1947. augusztusi választások után Veres Péter, a Nemzeti Parasztpárt elnöke lett a honvédelmi miniszter. Az 1947. évre az a jellemző, hogy a hadseregen belül megerősödtek a baloldal erői.

1948 februárjában Pálffy György altábornagyot nevezték ki a honvédség főparancsnokának Kuthy László vezérezredes helyére, aki 1945 előtt a Magyar Királyi Honvédség altábornagya volt. A Kiképzési és Nevelési Csoportfőnökségen belül az eddigi nevelési osztály helyett Jánosi Ferenc alezredes vezetésével Nevelési Alcsoportfőnökséget szerveztek. Ez irányította a nevelőtiszteket, a propaganda-, a kulturális nevelést. A politikai munka átszervezése kapcsán született döntés a nevelőtiszti intézmény megszüntetésére, a politikai tiszti intézmény bevezetésére.

1948 után, különösen 1949-1953-ig a honvédség fejlesztése hazánk anyagi lehetőségeit figyelmen kívül hagyva erőltetett ütemben folyt. Ezt a hidegháborús feszültséggel, majd 1950-től a koreai háború kirobbanásával, a III. Világháború lehetőségével indokolták.

A nemzetközi helyzet téves megítéléséhez hozzájárult a Tájékoztató Iroda 1949-es hibás határozata, amelynek eredményeképpen a szocialista országok szakí-

tottak Jugoszláviával. Nekünk mint szomszédos országnak ez azt jelentette, hogy ellenséggel kell szembenéznünk. Ezt támasztották alá Rajk László és társai koncepciós perével, amelyben egyértelműen utalást tettek a várható támadásra.

Emiatt az ország lakosságának életkörülményei jelentősen romlottak. Az osztályharc állandó éleződésének dogmatikus elmélete súlyos károkat okozott és a törvénytelenségek sorozata következett be. Tisztességes, becsületes katonák is áldozatul estek, ártatlanul haltak meg vagy kerültek börtönökbe. Rehabilitálásukra csak 1956-ban és 1990 után került sor.

A Magyar Honvédség története 1945-1948-ig terjedő időszakának jellemzői:

- biztosította az ország függetlenségét, szuverenitását, 1947 után határaink védelmét;
- részt vállalt az ország újjáépítésében, a népgazdaság segítésében;
- jelentős szerepet töltött be a magyar fiatalok nevelésében;
- a honvédség nevét megváltoztatták, hogy elnevezésében is igazolják, hogy ez a hadsereg a népé, a nép érdekeit védi, Néphadsereggé változtatták;
- bár a hadsereg nevéből kimaradt a honvéd szó, de a folyamatosság érdekében a következő mintegy több mint 40 évet nem hagyhatjuk feltáratlanul.

A MAGYAR NÉPHADSEREG 1949 - 1956

A néphadsereg megalakulása

1948-ra az ország társadalmi-politikai helyzete úgy alakult, hogy a Szovjetunióval és a szomszéd országokkal megkötött kölcsönös barátsági és együttműködési szerződések végrehajtása szükségessé tette a honvédség fejlesztését, az új körülményeknek megfelelően néphadsereggé való átalakítását. Ennek kezdeti lépései már az előző években kezdődtek, de az átszervezés és fejlesztés, a néphadsereggé való átalakítás alapvetően 1949-ben valósult meg. Az igaz, hogy az elnevezés néphadsereg lett, de a katona megmaradt, mint "honvéd". Ez azt az évszázados elkötelezettséget tükrözte, hogy a fő feladat továbbra is a hon, a haza védelme.

Az új típusú hadsereg fejlesztésénél első lépésként egy alapvetően új, a szocialista néphadsereg célkitűzéseinek megfelelő tisztikar kialakítása, a szükséges új létszám biztosítása, kiválogatása, kiképzése volt.

A második világháború után a Magyar Honvédségben a Honvéd Kossuth Akadémián, a Honvéd Hadbiztos Akadémián már 1947-ben megkezdődött a tisztképzés és továbbképzés és a közben létrehozott Honvéd Akadémián pedig a vezérkari tisztképzésre is sor került.

A hadsereg gyorsított ütemű fejlesztése szükségessé tette a nagyobb létszámú tisztképzést. Ezt a célt valósították meg az 1949-ben létrehozott fegyvernemi tiszti iskolák.

A hadseregfejlesztés gyorsított ütemének kielégítése érdekében a tisztképzés időtartamát egy évben határozták meg, ezt később 2 évre emelték.

A tiszti iskolákra ebben az időben a megfelelő szakképzettség biztosítása érdekében kiképzőnek több, a régi hadseregben szolgált és szakmai, valamint háborús tapasztalatokkal rendelkező tisztet, tiszthelyettest osztottak be.

Az újjáalakuló hadseregbe pedig katonai felkészültségük miatt több száz régi tisztet és tiszthelyettest hívtak vissza és vették igénybe tudásukat, ismereteiket.

Az 1949-50-ben már a tiszti iskolákon felavatott és kibocsátott tisztekkel együtt, alapvetően megváltozott a tisztikar összetétele, ami a néphadsereg további fejlődésének nagyon fontos és meghatározó tényezője volt.

Az 1950-es évtől kezdődően a hadsereg fejlesztésénél az elérendő cél a 70 000 fős létszám kialakítása volt. Ennek érdekében új szervezeteket, új díszlokációt, laktanyákat, raktárakat, bázisokat kellett létrehozni.

Ezt a szövetségesi elkötelezettségből adódó fejlesztést még inkább erősítette a Jugoszláviával szemben kialakult ellenséges viszony is. 1951-re a hadsereg létszáma már 250 000 főt számlált.

Az ország Dunántúli, Duna-Tisza-közi, valamint Tiszántúli, keleti és északi részein új hadtestek, hadosztályok, ezredek, szakfegyvernemi alakulatok jöttek létre.

Magyarország földrajzi helyzetéből adódóan a meghatározó fő cél két haderőnem kifejlesztése volt.

E haderőnemeken belül a fegyvernemek és szakcsapatok arányát úgy kellett kialakítani, hogy az így megszervezett és kiépített hadsereg a szövetségesekkel együtt működve képes legyen az ellenség megsemmisítésére, hazánk védelmére.

Ezzel egy időben az ország vezetése feladatként határozta meg, hogy az ipart és a mezőgazdaságot olyan mértékben kell fejleszteni, hogy az képes legyen a háborúban és békében egyaránt a lakosság és a hadsereg szükségleteit kielégíteni.

A néphadsereg szervezete

A tisztképzés rendszerének újjáalakításával, gyorsításával egy időben, mint alapvető főfeladatot az ország légvédelmének megszervezését tartották. Ennek érdekében már 1948 őszén megalakították az Országos Légvédelmi Parancsnokságot és létrehozták a Honi Légvédelmi Haderőnemet.

1949-ben az új korszerű hadsereg irányítási igényeinek és követelményeinek megfelelően átszervezték a Honvédelmi Minisztériumot.

A Honvédelmi Minisztérium Elnöksége helyett: A Honvédelmi Miniszter Irodája, a Honvédség Felügyelője helyett: A Honvédség Csapatainak Szemlélője, a Fegyvernemi Szemlélők helyett: Fegyvernemi Parancsnokságok, az Anyagi Főcsoportfőnökség helyett Hadtáp Szolgálat Főnökség alakult meg. Az Országos Légvédelmi Parancsnokság pedig a vezérkar főnökének alárendeltségéből a honvédelmi miniszter közvetlen alárendeltségébe került.

A Határőrség kikerült a honvédelmi miniszter alárendeltségéből és a belügyminiszter alárendeltségébe került.

Az 1949. év második felében új hadrend lépett életbe, melynek eredményeként több "A" típusú, tehát teljesen feltöltött és "B" típusú, tehát keretjellegű magasabb egységet /hadosztály, dandár/ szerveztek és állítottak fel. Ezzel egy időben vette kezdetét a Honvédelmi Minisztérium és a magasabbegységek alárendeltségében a szakcsapatok felállítása és kiépítése is.

A hadsereg átszervezésével, fejlesztésével együtt meghatározó és megoldandó feladatként jelentkezett a hadsereg új fegyverzettel való ellátása, megfelelő laktanyai elhelyezése, anyagi /ruházat, élelmezés, egészségügyi ellátás/ biztosítása.

Az eddigi kis létszámú hadsereg csak könnyű fegyverzettel, azzal is hiányosan volt ellátva. Az átszervezett és fejlesztett hadsereg működésének alapvető feltétele új, korszerű haditechnikával való ellátása volt.

Mindezek biztosítása az ország helyzetéből adódóan nagy problémát jelentett. A legszükségesebb pénzügyi és anyagi feltételek alapvetően biztosíthatóak voltak, de az is tény, hogy 1949-50-ben az ország még nem rendelkezett hadiiparral, mivel az a második világháborúban teljesen elpusztult.

A háború előtt és alatt gyártott magyar konstrukciójú fegyverek, hadianyagok elavultak, korszerűtlenek voltak, tehát az új hadsereg felfegyverzése szempontjából nem jöhettek számításba.

A szükséges fegyverzet biztosításának egyetlen lehetséges formája a szövetséges Szovjetunió segítsége volt. A szovjet hadsereg a második világháborúban alkalmazott fegyverei kiállták a próbát és nem egy fajtájuk, főleg a páncélos fegyverek harci jellemzői a világszínvonalat képviselték.

Már 1948-ban a két ország kormányközi tárgyalásain egyezményt írtak alá, amely biztosította a Magyar Néphadsereg első fejlesztési ütemének fegyverzetét.

A Honvédelmi Minisztérium az 1949. év elején a Haditechnikai Intézet számára követelményrendszert határozott meg a hazai fegyverfajták kikísérletezésére, több felszerelés hazai gyártásának előkészítésére.

A Honvédelmi Minisztérium szovjet licenc alapján készült fel egyes fegyverfajták hazai gyártására és egyes fegyverek hazai továbbfejlesztésére is.

Másik lényeges feladat volt az új alakulatok elhelyezése és a haditechnikai, valamint ellátási és egyéb felszerelések részére szükséges raktárak biztosítása. A meglévő és háborús károkat szenvedett laktanyák és egyéb objektumok rendbehozása, új objektumok építése sürgős feladatként jelentkezett.

Csak egy példa ezek közül: a megalakuló Zalka Máté Híradó Tiszti Iskola részére kijelölt Budaörsi úti, volt Károly király laktanya a háború után internálótábor volt és annak rendbe rakása, a tisztképzés feltételeinek megteremtése komoly pénzügyi, anyagi-technikai és munkaszervezési feladatokat jelentett. Nem volt könnyű fel-adat az újonnan felállítandó hadosztályok elhelyezési feltételeinek megteremtése sem. Ezért a magasabbegységtörzseket ideiglenesen, volt főúri kastélyokban /pl. Keszthely / helyezték el. Az ország több pontján /pl. Tab/ gyors ütemben folyt az új lakanyák és tiszti lakások, szállók építése.

A hadsereg új fejlesztési, szervezeti formáinak kialakítása, a diszlokációval kapcsolatos feladatok végrehajtása sem volt könnyű, mert e téren sem a régi, sem az új tisztikar megfelelő tapasztalatokkal nem rendelkezett. Ezt még nehezítette és komoly nehézségeket okozott a hadseregen belül is a kialakult személyi kultusz és a törvénytelenségek okozta személyi veszteségek. A törvénytelenségek áldozatai lettek a néphadsereg kiemelkedő vezetői közül Pálffy György altábornagy, később Sólyom László, Illy Gusztáv altábornagy, Révay Kálmán, Beleznay István, Porffy György vezérőrnagyok és még több elismert katonai vezető.

A fentebb felsorolt nehézségek, problémák ellenére a néphadsereg szervezeti felépítése, a kiképzés színvonala megfelelően alakult.

Az elért eredményeket bizonyította a már 1949 nyarán megtartott első harcászati gyakorlat is. A megfelelő létszámú, felszereltségű, kiképzettségű hadsereg teljes kiépítése az ezután következő évek megfeszített munkáját igényelte.

A hadsereg gyorsított ütemű fejlesztését indokolta a nemzetközi helyzet roszszabbodása, a Jugoszláviával kapcsolatos sajátos szakítás. A hadsereg személyi állományának nehéz időszakot jelentettek az 1950-1953-as évek, mivel ebben az időben a hadsereg fokozott mennyiségi fejlesztés miatt, állandó átszervezésben volt, ami kedvezőtlenül hatott a kiképző munkára, a fegyelem állapotára.

A fejlődés különösen a légierőnél és a honi légvédelmi csapatoknál volt szembetűnő, de tovább folytatódott a szárazföldi csapatoknál is. Újabb hadtestet és hadosztályokat állítottak fel. Ez a gyors ütem, az új laktanyák elhúzódó építése és késve történő átadása, a raktárak, lövegszínek és elhelyezési anyagok hiánya miatt csak tovább fokozta a nehézségeket.

Továbbra is sürgető feladat volt a tiszti állomány hiányainak pótlása, a már működő tisztképző iskolákon és a Katonai Akadémián a tisztképzés erősítése, valamint a Szovjetunió tisztképző intézeteibe beiskolázásra kerülő hallgatók létszámának növelése.

A magyar felsőfokú tisztképzés biztosítása érdekében a Hadiakadémia 1950-ben elkezdődött többszörös átszervezés után, 1955-ben Zrínyi Miklós Katonai Akadémia névvel folytatta a legfelsőbb szintű tisztképzést.

A csapatok képzettségi színvonalának emelése érdekében elrendelték a csapattisztek és katonák számára a folyamatos továbbképzést, a szabályzatok tanulmányozását. A parancsnoki továbbképzéseket általában havonta az elöljáró parancsnokok tartották.

Az alakulatok kiképzésénél nagy hangsúlyt kapott a harctéri körülmények feltételei között tartott gyakorlati képzés.

Ennek érdekében a hadosztályok, ezredek, szakcsapatok a laktanyai elhelyezésből tavasztól-őszig /márciustól-szeptemberig/ tábori körülmények között, terepen folytatták a kiképzést. Ilyen nyári táborok létesültek az egész országban Böhönyétől Vésztőig, Csopaktól Hárosszigetig, Nagyoroszitól Budaörsig stb. Itt, ezeken az erdős, dombos területeken külön a törzsek, külön az alakulatok sátrakban történő elhelyezés mellett tevékenykedtek. Az elhelyezés és az ellátás minden esetben komoly feladatot jelentett a hadtápszolgálat számára és nem volt könnyű az összeköttetés biztosítása sem. A gyakorlati kiképzés, a harci technika kezelése, a lőgyakorlatok a katonák számára nehéz fizikai igénybevételt jelentettek. Ezek a táborhelyek általában a békehelyőrségektől távol eső területeken voltak. Ebből adódóan komoly problémaként jelentkezett a katonák, tisztek és tiszthelyettesek számára a hozzátartozókkal, családdal való kapcsolat fenntartása, a kimenők, eltávozások megoldása.

A kiképzés eredményességének fokozása érdekében nagy súlyt helyeztek a korszerű harci technika magas szintű kezelésének elsajátítására, a lőgyakorlatok eredményes végrehajtására, a parancsteljesítésre, a fegyelem erősítésére, a rendkívüli események számának csökkentésére, az ügyeleti és őrszolgálatnak a szabályzatokban előírtak szerinti teljesítésére.

Gondot fordítottak a polgári lakossággal való kapcsolat erősítésére, a tiszti, tiszthelyettesi, tisztesi tekintély növelésére.

A hadsereg népszerűségét szolgálták a polgári szervekkel közösen szervezett kulturális rendezvények, az ipari és mezőgazdasági üzemlátogatások. Az 50-es években nagy jelentőséget tulajdonítottak az évente május 1-én és április 4-én

megtartott katonai díszszemléknek. A díszszemle fegyelmezett végrehajtása jól képzett, harcra kész fegyveres erő meglétét tükrözi. Ez egyben a fegyelem, a parancsteljesítés pontos végrehajtásának a vizsgája is, amely egyben erősíti a katonai csapatszellemet, a közös akaratot.

1953-ban a politikai helyzetben, a kormány vezetésében történt változás következtében csökkenteni kezdték a hadsereg létszámát, ami a tisztikart is érintette. Ez nagyfokú bizonytalanságot eredményezett. Megállapították, hogy nem kielégítő az emberekről való gondoskodás, szaporodtak a beosztottakkal szembeni durvaságok. Újból sok tiszt került tartalékállományba, vagy áthelyezésre.

Ez után az átmeneti év után, 1954-ben a hadsereg fejlesztésének új időszaka kezdődött, amit az atom- és más tömegpusztító eszközök megjelenése követelt meg. Olyan döntés született, hogy az alapvető szervezeti kereteket változatlanul hagyva, fokozatosan a hadsereg minőségi összetételén, a kiképzés színvonalán, a fegyelem területén kell nagymértékben változtatni, javítani.

Ebben az időben a vezető nagyhatalmak katonai szakemberei az atomfegyvereket már nemcsak hadászati, hanem harcászati, hadműveleti felhasználásra is alkalmazhatóknak tartották.

Ez az addig érvényben lévő elvek felülvizsgálatát követelte.

Az új fegyver a csapatok olyan szervezeti, minőségi átalakítását követeli meg, hogy azok az atomcsapás okozta pusztítás ellenére is képesek legyenek megőrizni vagy helyreállítani harcképességüket. Az akkori szovjet katonai doktrínának megfelelően ez így volt, ezzel biztosítható, ha a csapatok gépesítettségi fokát növelik és a páncélos erőket tovább fejlesztik. Szükségessé vált a gépkocsizó lövészhadosztályok megszervezése. Létrehozták a gépkocsizó lövészezredeket. A hadosztályok megerősítésére harckocsi-rohamlöveg és közepes harckocsi egységet szerveztek

Követelményként a kiképzésben is fokozottan előtérbe került, hogy a csapatok sajátítsák el a korszerű tömegpusztító fegyverek alkalmazásának viszonyai közötti tevékenységet. Az eddig kiadott harcászati szabályzatok, a tömegpusztító eszközök körülményei közötti harctevékenységgel ugyan nem foglalkoztak, de 1955-ben már több olyan segédlet jelent meg, amely útmutatást adott a tömegpusztító eszközökkel vívott harcra való felkészítésre.

Belépés a Varsói katonai szervezetbe

Az 1955-ös év a néphadsereg további fejlődését meghatározó eseménye volt a Varsói Szerződés létrehozása.

Miután a nyugati hatalmak 1955. május 9-én a Német Szövetségi Köztársaságot is felvették a NATO tagjai közé, 1955. május 11-én Varsóban összeült a szocialista országok, köztük hazánk kormányküldöttsége is és a NATO ellensúlyozására barátsági és kölcsönös segítségnyújtási szerződést kötöttek. Ez a szerződés a Varsói Szerződés elnevezéssel került a történelembe és 1955. május l4-én írták alá.

1955 júliusában a négy nagyhatalom / Amerikai Egyesült Államok, Szovjetunió, Anglia, Franciaország / képviselői értekezletének eredményeként a nemzetközi kapcsolatokban némi enyhülés következett be.

Ennek hatására a Magyar Népköztársaság Minisztertanácsa úgy döntött, hogy az év végéig 20 000 fővel csökkenti a hadsereg létszámát. Ez újólag bizonytalanná

tette és nehezítette a hadsereg helyzetét, rontotta a fegyelem és kiképzés színvonalát.

1956 közepére az országban, a társadalomban olyan helyzet alakult ki, amely mind jobban hangsúlyozta a felgyülemlett ellentmondásokat. A nép körében mindinkább erősödött és szélesedett az a felismerés, hogy a meglévő feszültségeket a meglévő rendszer megreformálásával lehet megoldani. Komoly erők szervezkedtek a nép, a munkásság támogatásával a változtatás forradalmi úton történő végrehajtására.

A hadseregben is kialakultak a különböző nézetek. Ettől függetlenül a néphadsereget lényegében meglepetésként érték az 1956. októberi felkelés és forradalom eseményei.

Az 1956. október 23-a után Nagy Imre vezetésével megalakult az új kormány, mely a válságos helyzetből, forradalmi úton független Magyarországként való kijutást határozta el.

A Nagy Imre kormány jóváhagyásával - a forradalom vezető szerveiként - az egész országban, így a Honvédelmi Minisztériumban és a Néphadseregben, a csapatoknál is megalakultak a Forradalmi Bizottságok, amelyek a felső vezetés egységes irányításának hiánya miatt hatékony szerepet nem töltöttek be. Ezért a hadseregben továbbra is nagymértékű bizonytalanság, tájékozatlanság légköre uralkodott.

1956 november 4-én a Kádár János vezetésével megalakított új kormány a szövetséges szovjet csapatok segítségét kérte. A magyar forradalmi erők rövid ellenállása után az új kormány vette át a hatalmat és kezdte meg a Szovjetunióval való szövetségi viszony és a Varsói Szerződésből adódó követelmények teljesítése érdekében, a hadsereg újjászervezését.

A MAGYAR NÉPHADSEREG 1957 - 1990

Az 1956-os forradalom és szabadságharc leverése után a Magyar Néphadsereg szétzilálódott. A tisztikar egy része leszerelt, egy része a karhatalomban szolgált, míg egy kisebb része külföldre távozott. A november 4-i szovjet támadás után a magyar alakulatokat bekerítették, fegyverletételre kényszerítették. A fegyveresen ellenálló csoportokat elfogták, illetve megsemmisítették. A katonák többségét néhány nap után hazaengedték.

A megalakult Magyar Forradalmi Munkás-Paraszt Kormány Budapestre költözött és megkezdte a karhatalmi alakulatok szervezését.

Az 1. tiszti ezred november 9-én alakult meg a Dózsa György úti Sport Tiszti Iskolán. Főként volt államvédelmi tisztekből, partizánokból, BM. dolgozókból, pártmunkásokból és honvédtisztekből állt. Budapesten még két honvéd- és egy belügyi ezred követte. Vidéken - megyei szinten - szintén megkezdődött a karhatalmi alakulatok felállítása. Feladatukat a Karhatalmi Utasítás rögzítette. Eszerint a fő feladat az MSZMP irányításával a belső rend védelme, a forradalmi harcokban résztvevők elfogása, a közbiztonság helyreállítása és a szocialista rendszer újraindításának biztosítása volt.

A karhatalmi tagság egyik feltétele a "Tiszti Nyilatkozat" aláírása volt, melyben az aláíró feltétel nélkül alárendelte magát az új kormánynak és egyetértett a szovjet "segítség" jogosságával. A karhatalom 1957 júniusáig fokozatosan megszűnt.

A Magyar Néphadsereg létszámát az 1956. decemberi kormányhatározat 64 ezer főben állapította meg. Ez kevesebb volt, mint az előző létszám fele. Tisztekből kb. 8 000 fő felesleg volt. Egy részét átvette a határőrség, 2 000 fő polgári állományba került, ezren leszereltek. Akiknek nem jutott beosztás, azok részére átképző tanfolyamokat szerveztek.

1957. január 20-án Münnich Ferenc vezetésével - aki akkor a fegyveres erők minisztere volt - küldöttség utazott Moszkvába. Itt határozták meg az elkövetkezendő idők feladatait, többek között a tisztképzés megreformálását is.

Ennek keretében a korábbi 13 tiszti iskolát megszüntették és helyette Budapesten az Egyesített Tiszti Iskolát hozták létre. A két akadémiát is összevonták. A Honvédelmi Minisztérium létszámát 1860 főre redukálták.

A korábbi nyolc hadosztályt háromra csökkentették. Csökkentették a légierőt és a honi légvédelmet is.

1958-tól megkezdték a Varsói Szerződés körzetében a közös légvédelem kiépítését.

A Néphadsereg ezután lassú fejlődésnek indult. 1959-ben 4 gépkocsizó lövészhadosztály, 1 tüzérdandár, 1 hadihajós dandár, 13 fegyvernemi ezred és számos szakalegység állt a vezetés rendelkezésére. Ekkor a hadsereg létszáma 84 033 fő volt.

A Magyar Néphadsereg korszerűsítése

1960. május 17-én a HM vezetését Czinege Lajos tartalékos alezredes vette át, akit a kormány altábornaggyá léptetett elő. Az ő vezetésével indult meg az a nagyfokú technikai átalakulás, amely a szovjet technika megvásárlásával felzárkózott a Varsói Szerződés Politikai Testülete és annak vezérkara által megállapított színvonalra.

A honvédelmi miniszteri funkció ebben az időben is inkább politikai megbízás volt. A hadseregfejlesztés igazi munkáját a vezérkari főnök vezetése alatt dolgozó vezérkar végezte. A kidolgozói tevékenységet a csoportfőnökségek hajtották végre.

A technikai fejlesztést ötéves időszakokra bontották. Az első időszak 1961-1965 között, a második 1965-1970, a harmadik 1971-1980 között zajlott.

Ezen időszakok alatt a hadsereget a mindenkori szovjet követelményeknek megfelelően többször átalakították. A legnagyobb átalakulás 1961-ben a Budapesten az 5. hadsereg megalakulásával és a hozzá tartozó alakulatok diszlokációjával valósult meg. A szárazföldi csapatokon kívül átszervezték a légvédelmet, a hátországot, a hadtápszolgálatot, az iskolákat, a fegyvernemi főnökségeket, a hadkiegészítést, vagyis a hadsereg minden részét. Ez év végén a hadsereg parancsnokság Székesfehérvárra diszlokált.

A szárazföldi hadsereg parancsnoka Csémi Károly vezérőrnagy, helyettese Martics Pál vezérőrnagy, politikai helyettese Kutika Károly vezérőrnagy, törzsfőnöke Kálazi József ezredes lett.

A honi légvédelem - mint a másik haderőnem - ugrásszerű fejlődésnek indult. 1962-ben már 14 harci osztállyal rendelkezett. A vadászrepülő csapatokat MIG-21 típusú repülőgépekkel teljesen átfegyverezték. A légvédelem 84 rakétaindító állvánnyal és a hozzájuk rendszeresített rakétákkal biztosította hazánk légterét. A

hatékony vezetést az újjáalakult és korszerűbb lokátorokkal felszerelt rádiótechnikai csapatok biztosították.

Természetesnek vették, hogy a növekvő hadsereghez nagyobb irányító apparátus is tartozik. Több csoportfőnökség alakult és a politikai és személyügyi vezetésből főcsoportfőnökség lett. Nagy gondot fordítottak a politikai nevelésre. Külön agitációs és propaganda-csoportfőnökség biztosította a szükséges politikai anyagokat.

Belügyi hatáskörből a HM alárendeltségébe helyezték a polgárok védelmét és 1962-ben megalakult az Országos Légoltalmi Parancsnokság, majd létrehozták a Polgári Védelem Országos Parancsnokságát is.

1965-ben átszervezték a megyei hadkiegészítő parancsnokságokat és összevonták a járási kiegészítő parancsnokságokat.

1966-ban a szárazföldi csapatoknál hadtesteket szerveztek. A hadsereg fokozatosan bővült, egyre újabb és újabb fegyvernemi alakulatok jelentek meg. Például a szárazföldi rakétacsapatok, a rádióelektronikai harc csapatai, a páncélozott lövészcsapatok.

A fegyverzetek fejlesztésével együtt járt az új alakulatok létrehozása, a hadsereg újabb és újabb átrendezése.

1973-ban megalakult az 1. Honi Légvédelmi Hadseregparancsnokság, és a Csapatrepülő-Parancsnokság. 1975-ben létrehozták a Rádióelektronikai Főnökséget és a vezérkar tudományos osztályát, ezzel egyidejűleg megszüntették a Hadtudományi Intézetet.

A hadtáp egy részéből egy új szervezetet, a Beruházási és Fenntartási Főnökséget hoztak létre. Minden különálló szervezet csökkentette a HM létszámát, ami az 1970-es években 2000 fő volt.

Az 1970-es években a Néphadsereg az alábbiak szerint épült fel:

Ξ szárazföldi hadsereg:

- 3 gépesített lövészhadosztály,
- 1 harckocsihadosztály, közvetlenek,

Ξ szárazföldi hadtest:

- 2 gépesített lövészhadosztály,
- hadtestközvetlenek,

Ξ csapatrepülők:

- 1 szállítóhelikopter-ezred,
- 1 felderítőrepülő-ezred,
- 1 harcihelikopter-zászlóalj,
- 1 szállítórepülő-század,
- 1 biztosító-kiszolgáló zászlóalj,

Ξ honi légvédelmi hadsereg:

- 2 honi légvédelmi hadosztály,

- hadseregközvetlenek.

Ξ hátországvédelmi erők:
- komendánsezred,
- híradóezred,
- műszaki ezred,
- őrezred,
- pontonos dandár,
- híradózászlóalj,
- komendánszászlóalj,
- sugárértékelő főközpont,
- állásépítőzászlóalj,
- tűzszerészzászlóalj,
- felderítőzászlóalj,
- Budapesti Helyőrségparancsnokság,
- komendánshivatalok,
- raktárak, javítóműhelyek stb.

Ξ hadtápszervek:
- tábori hadtápközpont,
- mozgósítási törzs,
- hadtápátrakóközpont,
- kommunális igazgatóságok,
- Repülőorvosi Kutató Intézet,
- A MN kórházai,
- építési és beruházási főnökség,
- katonai közlekedési főnökség és alakulatai,
- katonai közlekedési főnökség,
- üzemanyag, ruházat stb. raktárai,

Ξ pénzügy:
- Számító- és Nyugdíjmegállapító Központ.

A hadseregátalakítás hatodik és hetedik ötéves tervében még voltak változások. Ezek a légvédelmet és a repülőcsapatokat érintették.

Szerepünk a Varsói Szerződésben

Az 1955-ben megalakult védelmi közösség tagjaként az 1956-os forradalom és szabadságharc miatt 1960-ig nem volt szerepünk.

Magyarországon 1956 előtt kisebb szovjet haderő, az 1955-ben felállított Különleges Hadtest állomásozott. A magyar csapatokkal közösen az volt a feladatuk, hogy lezárják az osztrák-magyar határt és biztosítsák a felvonuláshoz szükséges közlekedési útvonalakat és a vasúti szállítást.

A honi légvédelem kiépítette a koalícióval együttműködő légvédelmi rendszerét. 1962 tavaszán hazánk területén került sor az első együttműködési gyakorlatra DUNA fedőnévvel. Ebben magyar, szovjet és román törzsek és csapatok vettek részt.

A magyar hadvezetés és a csapatok folyamatosan részt vettek a közös irányítás alá tartozó országok gyakorlatain. Az együttműködési gyakorlatokon kívül kétoldalú gyakorlatokat is terveztek: magyar-szovjet, román-szovjet, lengyel-szovjet stb.

Ezeknek a gyakorlatoknak az volt a céljuk, hogy ellenőrizzék a csapatok hadrafoghatóságát, a parancsnoki kar és a törzsek felkészültségét az esetleges háborúban rájuk háruló feladatok ellátásával kapcsolatban. A honvédelmi feladatokon kívül a gyakorlatoknak politikai céljai is voltak, az internacionalista szellem és a "testvéri hadseregek" közötti barátság erősítése.

A gyakorlatok többségükben egy feltételezett NATO-támadás elhárítására, majd a támadó fél területi elfoglalására irányultak.

A vezetés és fejlesztés egyértelműen a Szovjetunió kezében volt. A lehetséges együttműködés érdekében a hadsereg bizonyos területein a fegyverek és a haditechnika eredeti szovjet vagy licenc alapján itthon gyártott eszközökből állt.

Az erőviszonyok alakulásának köszönhetően Európában 1945 óta nem volt háború. Bár sokszor feszült volt a nemzetközi helyzet, de mindig sikerült békés megoldásokat találni. Ebben sokat köszönhet a világ az elmarasztalt Nyikolaj Hruscsovnak, később pedig a politikai rendszerek teljes átalakításában résztvevő és irányító Mihail Gorbacsovnak. Mindketten a szovjet kommunista párt főtitkárai, a Szovjetunió elnökei voltak.

A magyar néphadsereg technikai fejlődése

Az 1960-as évek elejétől a néphadsereg két haderőnemre, a szárazföldi és honi légvédelmi csapatokra tagolódott. Alapvető fegyvernemei a gyalogság, a tüzérség, a páncélosok és a légierő.

A gyalogság mozgatása gépkocsikkal történt, a tüzérség vontatása már gépesítve volt. A páncélos csapatok T-34-es harckocsikkal, a repülők MIG-15-ös vadászrepülőkkel, LI-2-es szállítórepülőkkel és PO-2-es felderítő repülőkkel voltak ellátva. A honi légvédelmet korszerű rakétakomplexumokkal látták el. 1962-ben a légvédelem 14 harci osztállyal, 80 szuperszonikus és 80 hangsebesség alatti repülőgéppel rendelkezett.

1960-tól megkezdődött a gyalogság páncélozott járművekkel való ellátása. 1965-ben rendszeresítették a magyar fejlesztésű és gyártású páncélozott harcjárművet,a PSZH-t. A gyalogsági fegyverek közül kiszorultak a karabélyok és helyettük a szovjet gépkarabélyokat, golyószórókat és géppuskákat rendszeresítették. Egyéni páncéltörő eszközként megjelent az RPG-2, majd az RPG-7.

A második világháborús T-34-et felváltotta a T-54, majd a T-55-ös harckocsi.

A lövészeknél rendszeresített harckocsi alegységek PT-76 típusú könnyű harckocsikat kaptak.

A tábori tüzérség is új fegyvereket kapott, így a 85 mm-es páncéltörő ágyút, a 152 mm-es tarackokat, a BM-21 típusú sorozatvetőket. A tábori tüzérséget is ellátták tűzvezető lokátorokkal.

A légvédelmi tüzérség fejlődött talán a legjobban. Sz-60 típusú 57 mm-es lövegeket, ZSZU-23 típusú önjáró gépágyúkat, ZU-2-es géppuskákat kaptak. A hadosztályok légvédelmi ütegeit, SON-9-es tűzvezető lokátorokkal irányították.

1977-ben jelentek meg a légvédelmi rakéták. Ekkor telepítették a Budapestet körülvevő légvédelmi gyűrűt.

A szakcsapatok is jelentősen fejlődtek. A harc megvívásában lényeges szerepet játszó szovjet és hazai gyártású híradástechnikai eszközök biztosították a szükséges összeköttetéseket békeelhelyezésben, a közös és együttműködési gyakorlatokon. Lehetővé tették, hogy a rádióhíradás felváltsa a vezetékes összeköttetésen alapuló információáramlást. Megjelentek a személyi vezetési eszközök, átalakultak a hírtovábbítás technikai rendszerei. Kis- és nagyteljesítményű szovjet rádióállomások biztosították a csapatok híradását.

Nagyot fejlődött a vegyivédelem. Kialakították az esetleges atomháború következményeinek mérési rendszerét, fejlesztették az egyéni védőeszközöket. Az első lépcsőben páncélvédetté tették a vegyicsapatok technikáját. 1967-től magyar gyártmányú mentesítő gépkocsikat rendszeresítettek.

1970-től automatizált rendszerekkel mérték a nukleáris hatásokat, elemezték a harci gázok összetételét.

A műszaki csapatokat 1960-tól gépesítették. A műszaki munkák ezredtől felfelé munkagépekkel történnek. Ugyancsak munkagépek végzik a harcárkok ásását, a fedezékek földmunkáit. Elemekből összerakható védelmi építményeket képesek gyorsan összerakni. Munkagépekkel biztosítják az útépítést.

A vízi átkelést a pontonos alakulatok önjáró rendszerekkel, gyorsan biztosítják. A kisebb folyókat, patakokat hídrakó gépkocsikkal, harckocsikkal, rövid időn belül áthidalják.

Összességében az elmúlt 35 év alatt a Magyar Néphadsereg technikai ellátottságban óriásit fejlődött. Bár gazdaságilag az utóbbi tíz évben a fegyverellátás területén már nem tudta követni a szovjetek által diktált iramot, amiből a gondok egyenesen következnek.

A magyar haditechnika, járműtechnika, lokátor-, repülő- és híradástechnika ma már elavultnak tekinthető.

A rendszerváltás előzményei

A Honvédelmi Minisztérium szervezetében 1989 októberében minőségi változás következett be. A Magyar Köztársaság kormánya úgy döntött, hogy a HM átszervezésével különválasztja annak politikai és katonai szerepét.

Létrehozta a Magyar Honvédség Parancsnokságát, amely a minisztériumtól elkülönítve, katonailag irányítja a csapatokat. Megszabta a honvédelmi miniszter feladatait, amelyben többek között szerepel a nemzetközi szerződésekből eredő feladatok ellátása és a törvényességi felügyelet a honvédség katonai szervezetei felett. Javaslatokat készít elő a honvédelmi politika kérdéseiben, kialakítja a fejlesztési koncepciókat, elvégzi a tárcaközi egyeztetéseket.

A honvédség főparancsnoka a mindenkori köztársasági elnök.

A Magyar Honvédség első parancsnoka Lőrincz Kálmán altábornagy, majd vezérezredes volt. Államtitkári besorolásban szolgálati elöljárója volt a honvédség teljes személyi állományának.

Törzskari szervezete:

- a Vezérkar, alárendeltségében a
- Hadműveleti Csoportfőnökség,
- Felderítő-,
- Szervezési-, a Mozgósítási-,
- Híradó- és automatizálási Csoportfőnökség és egyéb szervek.
- Kiképzési és Szárazföldi Főcsoportfőnökség,
- Anyagi-technikai Főcsoportfőnökség.

A MAGYAR HONVÉDSÉG NEVÉBEN ÉS RENDSZERÉBEN IS ÁTLAKULT.

CSÁSZÁR János

HA5SIK, ITT A HA5PA /AM

Világra szóló rekordkísérlet

Rádiós kapcsolat mozgó járművekről a Nemzetközi Űrállomással

Az első magyar műhold (MASAT-1) kísérleti tesztje

A ZMNE színeiben Császár János őrnagy,

a Híradó Tanszék (MSc képzés) volt hallgatója

A tervezett világrekord szervezését még az elmúlt év őszén kezdtük el. A Műszaki Egyetemmel és a Puskás Tivadar Távközlési Technikummal karöltve arra az elhatározásra jutottunk, hogy a Nemzetközi Űrállomáson tartózkodó Simonyi Károllyal a rádiós kapcsolatokat mozgó járművek bevonásával hajtsuk végre. A forgalmazásban részt vevő járművek széles skáláját vettük igénybe, vagyis előzetes listánkon szerepelt kerékpár, autó, vitorlás hajó, motoros hajó, repülőgép és hőlégballon is. Később „berepült" egy sárkányrepülő is az ablakon, ezzel listánk szép kerekre duzzadt. Járműveink rádiós operátorait mozgó multi-expedíciós társaknak kereszteltük el. Tervezett kísérletünk azért számított világrekordnak, mert még senki sem próbált kapcsolatba lépni a Nemzetközi Űrállomáson utazó űrturistával úgy, hogy közben hőlégballonon, sárkányrepülőn illetve kerékpáron utazik.

A Nemzetközi Űrállomással való rádiós kapcsolat létesítését az alábbi mozgó állomásokkal terveztük. Ezt a hivatalos listát kapta meg Simonyi Károly is.

List of the participants of the Special Orbit nr.2
Group nr. 2.

Callsign	**Operator**	**Notes**
HA **80 MRASZ**	Laci	Hq stn. of the Hungarian Radioamateur Society
HA **5** Cecil **H**elen/AM	Istvan	Airplane
HA **7** Tamas **M**aria/AM	Tibor	Airplane
HA **5** Peter **A**ladar/AM	Captain: Janos Passengers: HA5OJ Istvan, HA7TR Andras	Hot air balloon

HA **5** Viktor **I**bolya/AM	Imre	Two seats glider
HA **5 B**ela **F**erenc / P	Henrik	Bicycle
HA **3 S**andor **I**lona **O**lga/MM	Jozsef	Ship
HA **5 C**ecil **S**andor **I**lona/MM	Laszlo	Sailboat
HA **5 R**adio **T**echnika	Bandi	Stn. of journal „Radiotechnika”

Mint a listából is kiderül, én a hőlégballonos repülés és rádiós forgalmazásának megszervezését kaptam feladatul. A rádiózás és a hőlégballonozás számomra már nem volt ismeretlen, hiszen már több alkalommal forgalmaztam és versenyeztem mozgásban lévő hőlégballonról.

Terveim között szerepelt a rekordnak számító rádiós kapcsolat megörökítése fényképen, videón és hanganyagon is. Az előkészületek során felmerült az IP kamera használata is. Számítógépes adatátvitelünk biztosítását 5GHz-es tartományban működő eszközökkel terveztük végrehajtani.

Rádiókészülékünkkel és antennánkkal szemben támasztott követelmények között elsősorban a mobilitásra, a balesetmentes közlekedésre, a könnyű kezelhetőségre és a biztos rádiós kapcsolatra fordítottuk a legnagyobb figyelmet. A biztos rádiókapcsolat egyik feltételeként az üzemi tartalékként szolgáló adó-vevő jött számításba. Mint utóbb kiderült, ennek a döntésnek nagy hasznát vettük. A két adó-vevőhöz két antennát terveztünk. Az antennák iránykarakterisztikáját figyelembe véve, választásunk a helikális változatra esett.

Adó-vevő készülékként egy ICOM-821, valamint egy YAESU FT-857 jött számításba. Készülékeinket akkumulátoros táplálással ellátva fotós táskákban helyeztük el. A hangfrekvenciás jelet, valamint az antenna kimenetét meghosszabbítottuk, ezáltal biztosítottunk lehetőséget a könnyebb külső csatlakozáshoz. A táská-

ban elhelyeztünk egy másik vevőkészüléket is, melyen a földi állomások felmenő jeleit vettük.

Rádiós felszerelés

Tájékoztatásul annyit, hogy a kommunikáció adás és vételi ága különböző frekvenciákon történt. Az űrállomásra felmenő jel frekvenciáját az utolsó pillanatokban kaptuk meg, míg a lejövő – mindenki által hallható – jel publikus volt a közönség számára. Ez az óvintézkedés azért történt az űrállomás részéről, hogy idegenek ne zavarják meg adásainkat.

A rádiós felszerelés és az antenna ismertetése után a forgalmazásban részt vevőkről ejtenék néhány szót. A mellettem álló két úriember - Tóth István (HA5OJ) és Szabó András (HG7TR) - a Puskás Tivadar Távközlési Technikum rádióklubjának jeles tagjai.

A rádiós kapcsolat műszaki és forgalmazási kialakításában, valamint a mobil rádiók összeállításában is ők segédkeztek.

A helikális antenna elkészítését Tóth István vállalta magára. Az általa összehozott remekmű került a rekordkísérletben részt vevő mozgó járművek közül a hőlégballonra, az egyik repülőgépre és a kerékpárra is.

A rádiós forgalmazás menetét és módját is együtt határoztuk meg. A duplex üzemmód kialakítását két vevőkészülékkel úgy oldottuk meg, hogy az egyik készülék hangfrekvenciás jelét a fülhallgató bal, míg a másik készülékét a fülhallgató jobb oldalára tettük ki. A mobil rádiót ábrázoló képen jól látszanak az aranyozott jack aljzatok, amibe a fülhallgatóinkat csatlakoztattuk.

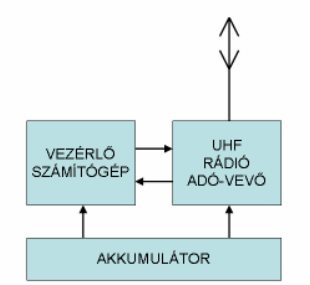
A hőlégballon operátorai

Az űrállomással való kapcsolatteremtésre az előzetes adatok szerint 6-7 perc állt rendelkezésre. Ebből mi 30-32 másodpercet szántunk a forgalmazásunkra. A nekem biztosított egy periódusra kellett megterveznem az üdvözlő szövegünket és a másik két rádiós társam hivatalos kommunikációját is. Mint utólag kiderült, a rossz forgalmazási körülmények miatt és az ilyen esetben előjövő lámpaláz hatására az összeköttetés tervezett szövege egy kicsit megváltozott.

A Műszaki Egyetem fejlesztésében készült MASAT-1 kommunikációs alrendszer terepi mérésében is részt vettünk. Dudás Levente, a Masat-1 kommunikációs alrendszeréért felelős vezető mérnöke felkért minket, hogy vegyünk részt a hamarosan űrpályára kerülő első magyar műhold tesztelési feladataiban. Nagy örömmel vettük a felkérést. A magunkkal vitt 10x10 cm-es dobozka a Masat-1 kisműhold egyik működő modellje volt – amely tartalmazott egy UHF sávú rádió-adó-vevőt, egy vezérlő számítógépet, valamint a tápláló akkumulátort.

A képen nagyon jól látszik a kosár alá belógatott „kocka”.

A modell feladata repülés közben az volt, hogy a neki sugárzott, digitálisan modulált rádiójeleket dekódolja, és visszasugározza a földi vezérlő állomásnak, ahol ezen adatok eltárolásra kerülnek az utólagos kiértékeléshez. A vett jel hiányában adott idő elteltével azonosító kódsorozatot sugároz a Masat-1, amely lehetővé teszi, hogy - egy rádióvevő és a hozzá kapcsolt számítógép segítségével – érzékeljük még abban az esetben is, ha a vett jel szintje jóval a zajszint alatt van.



A Masat-1 elvi felépítése


Masat-1 a kosár alá lógatva felépítése

A Masat-1 hívójele: HA5MASAT
Üzemi frekvenciája: 437.345 MHz
Moduláció: 2FSK

A rádiózással kapcsolatos előkészületekről és az első magyar műhold teszteléséről már beszéltem, most jöjjön az IP kamera beüzemeléséről néhány szó.

Hőlégballonos repülésünket és a rádiós forgalmazásunkat élő adásban szerettük volna közvetíteni a Puskás Tivadar Távközlési Technikum műholdas laborjában.

Ezáltal az érdeklődő média is real-time módban tudja majd nézni a hőlégballonban történteket. Az élőkép megjelenítésével több feladatot vettünk a nyakunkba. Ezek közé tartozott a célnak megfelelő – hangot is továbbító - kamera kiválasztása, megvétele, szoftveres tesztelése, a hőlégballonra való biztonságos felszerelése, mobilizált üzemeltetése, valamint a rögzített jel továbbítása rádiós, majd vezetékes módon, illetve a vételi oldalon való megjelenítése. Ezek közül csak a biztonságos rögzítést és a jel rádiós úton való továbbítását elemezném.

Rádiós technika szerelése

Az IP kamera rögzítéséhez két alapvető feltételt szabtunk. Elsőként, hogy a kosárban folyó lényegi tevékenységet lássa. Másodikként pedig azt, hogy a biztonságos rögzítés megfelelően legyen kialakítva úgy, hogy a szabad mozgásban minket ne akadályozzon.

A hőlégballon kapitányával (SUP-AIR BAALON CLUB), Szűcs Sándorral egyeztetve ezt is sikerült megoldanunk a képen látható módon. Szerény véleményem szerint ez nagyon jól sikerült.

Következő nagy feladatunk az IP kamera jelének továbbítása volt.

A videojelet tartalmazó IP felület továbbítását egy lapantennával egybeszerelt routerrel oldottuk meg. Az 5 GHz-en működő egységből kettőt kellett vennünk. Ezek felkonfigurálása és a kamerához való illesztése, majd tesztelése szintén néhány napot vett igénybe.

A Ballon kosarára való felfüggesztéssel is gondunk volt, mivel antennánkat menet közben a vételi állomás felé kellett forgatnunk. Ezt a feladatot a repülés során videós kollégánk, Enyedi Zoltán látta el.

Rádiós rekordkísérletünkhöz szükséges előzetes feladatainkat a fenti sorokkal nagyjából felvázoltam. Ne higgye senki, hogy csak ennyiből álltak előkészületeink. Lehetne még sorolni az elaprózott ténykedéseinket, de akkor egyhamar nem jutnánk beszámolóm végére. Egyet azért mégis megemlítenék az előzetesen végre-

hajtott feladatokból. A hőlégballon kapitányával több ízben egyeztettem a rádiós feladatokat illetően. Ezek közé tartozott, hogy az adás és a vétel során zavaró tényezőnek számít az égőfej használata, vagyis a gáz elégetésekor hallatszó hangos zaj. Közöltem vele, hogy nekem 35-40 másodperces csendre lenne szükségem a forgalmazás során. Erre azt a választ kaptam, hogy minden megoldható. Rádiós forgalmazásom előtt intsek neki, hogy egy perc van hátra a kapcsolat felvételéig. Ekkor elkezdi felfűteni a kupola belsejét úgy, hogy emelkedésünk elérje a 3-4 m/s sebességet. A hőlégballon felfelé tartó haladása, sebességének nullára esése, majd a lefelé tartó 3 m/s sebesség eléréséig bőséges egy perc áll rendelkezésemre.

Ezzel a kis epizóddal is szeretném érzékeltetni, hogy milyen sok, apró tényező befolyásolhatja expedíciónk sikeres kimenetelét.

Az indulás pillanatai

Eljött a várva-várt nap, vagyis 2009. április negyedike.

Az előre megtervezett repülésünk végrehajtását az időjárás nem akadályozta meg. Nagyon szép, szélcsendes idő fogadott minket az agárdi strand bejáratánál. Időben érkezett a helyszínre a ballonos társaság, az egyetemistákból álló csoport és a meghívott média is. Nagyon sok nézelődő és érdeklődő vett minket körül. A pilótával való egyeztetés után azonnal nekiláttunk az IP kamera tartójának felszereléséhez, az antennák felrakásához és a rádiókat tartalmazó táskák felcsatolásához. Pilótánk 16:15-kor jelezte, hogy készen áll az indulásra.

Dudás Levente, a Műszaki Egyetem mérnöke elhelyezte a Masat-1-et a kosár oldalára. Ekkor kiadtam az indulási parancsot. Ballonunk fél perc múlva elrugaszkodott a földtől.

Az elsődlegesen használt adó-vevőt ekkor bekapcsoltam. Megrökönyödve hallottam, illetve nem hallottam az FM üzemmód jellegzetes zaját. Gyors hibakeresés következett. A hőlégballon emelkedésével az én adrenalin szintem is ment

felfelé. A hibát igen, de az okát nem tudtam megtalálni. Ugyanis egy közeli műszaki eszköz elektromos zaja S10-es értékű jelet indikált az adó-vevőm kijelző műszerén. A hiba forrását utólag elemezve arra jutottunk, hogy valószínűleg a velünk utazó videósok egyik gépe lehetett a hiba forrása. Ekkor úgy döntöttem, hogy az alap kiépítettségű készülékem adás oldalát használva bekapcsolom a társamnál lévő tartalék adó-vevőt, mint vevőkészüléket.

Levegőben

Hangfrekvenciás csatlakozójára felraktuk Tóth István (HA5OJ) fülhallgatóját. Így a vevő oldali kommunikációnk a lejövő frekvencián rendben volt. Szabó András (HG7TR) fülhallgatójára annak a vevőkészüléknek a hangfrekvenciás kimenetét csatlakoztattam, amely a kommunikációnk felmenő ágát figyelte.

A megváltozott körülményekre nagyon jól reagáltunk mind a hárman. A videokamerát kezelők ebből semmit sem észleltek. Másik két rádiós társammal összefordulva hallgattuk a fülhallgatónkban hallható hívásokat.

Egymással közöltük a hallott információkat. Bandi 16:32-kor meghallotta az első állomás hívását, avagy a HA80MRASZ hívójelet.

Tudtuk, hogy nemsokára mi fogunk következni. Én a készülékemmel még mindig nem hallottam az űrállomás hangját. Pisti szólt, hogy most hívják az első repülőgépet. Ekkor intettem – és szóltam is – a kapitánynak, hogy nyomhatja a gázt az égőfejbe. Kívülről egy jól összeszokott és nyugodt csapatnak látszódhattunk, pedig vérnyomásunk maximális értéke már a hihetőségi határt súrolhatta.

Én még mindig csak a zajt hallottam a fülhallgatómon keresztül. A végtelennek tűnő zaj - melyet a pilótánk okozott a gázégővel – egyszer csak abbamaradt.

Készülékem hangos sistergésében meghallottam saját hívójelem utolsó két betűjét. No, innen jött a lámpaláz, hiszen én következtem.

Forgalmazás előtt

Több éves rádiós múlttal rendelkezem már, de az elmúlt napok kimerítő munkái, a kialvatlanság és a nem mindennapi esemény hatására mondtam én mindent, csak azt nem, amit kellett volna mondanom vagy olvasnom. Igen olvasnom, mert erre az esetre is felkészültem, vagyis a riportom kinyomtatott szövegét a kezemben tartottam. Riportom a következő volt:

HA5-ös Simonyi Károly itt a HA5-ös Péter Antal /AM, a ***HG7TR Bandi****, és a* ***HA5OJ Pisti.*** *Adásodat 59-el jól vesszük. A nevem János. Üdvözöl a hőlégballon kapitánya, valamint a Puskás Tivadar Távközlési Technikum Rádióamatőr Klubja.*

Jelenleg 1200 méter magasságban a Velencei-tó déli részén repülünk.

Velünk van az első magyar műhold kísérleti példánya, melynek működését repülés közben teszteljük.

Sok sikereket kívánunk. HA5-ös Péter Antal /AM. Vétel.

A szöveg kivastagított részét HG7TR (Bandi) és HA5OJ (Pisti) mondta azért, hogy nekik is hivatalosan elismert legyen a Nemzetközi Űrállomással való kapcsolat.

A 33 másodpercig tartó riportunk elhangzása után vételre kapcsoltunk. A hangos zajban csak azt hallottuk, hogy Simonyi Károly az utánunk soron következő állomást hívja. Nagyon örültünk annak, hogy riportunkra nem mondta azt, amit az előző két állomásnak, hogy nem hallja őket. Fél perc elteltével kihúztam az adóvevőből a fülhallgatómat, hogy a riporter is tudja rögzíteni a hanganyagot. A ballon kapitánya ekkor a haladásnak megfelelően nyomta tovább a gázt az égőfejbe, hogy tudja melegíteni a kupolában lehűlt levegőt. Eközben a közel nyolc percig tartó

forgalmazásban nem értettünk minden beszédet. Nagyon örültünk a sikeresnek tűnő összeköttetésünknek.

A mobil multi-expedícióban részt vevő két repülőgép lejött hozzánk. Tettek két-három tiszteletkört körülöttünk. Fénykép és videó készítése elindultak Budapest irányába.

A multi-expedíció repülői

re sikerült. Megérkeztek kísérő autóink is. Ismételt riportokat készítettek velünk az ott lévő média munkatársai. Nagyon boldogok voltunk.

Összepakoltuk rádiós felszereléseinket, majd elindultunk videósunk lakására, aki a Velencei-tó északi részén lakik.

Három új taggal bővült a hőlégballonnal utazók tábora. Ezt az avatásnak nevezett ceremóniát Zoli barátunk kertjében, lelkes ünneplés közepette hajtottuk végre.

Az esti híradó megtekintése után kaptuk a telefont, hogy gondok vannak a rádiós összeköttetésekkel. A repülő közlekedési eszközök összeköttetései nem sikerültek. Ekkor egy kicsit elszomorkodtunk. Két nap múltán - mikor a rádiós társak által rögzített felvételeket visszahallgattuk – derült ki, hogy Simonyi Károly a forgalmazásunk ideje alatt visszaszólt, hogy „hallok egy jelet, de nem érthető, sajnos”.

Sikeres leszállás

Tehát összeköttetésünket úgy igazolta vissza, hogy jeleinket veszi, de azok nem érthetőek. Rádióamatőr berkekben ez viszont nem számít összeköttetésnek.

A mozgó járművek és a Nemzetközi Űrállomás közötti rádiós összeköttetésre szervezett magyar rekordkísérlet így csak félig sikerült, az ebből adódó konklúziókról egy másik előadásban tennék említést.

Rekordkísérletünk során tesztelt Masat-1 földi állomása viszont az elvárásoknak megfelelően, vagyis kiválóan hajtotta végre a vele szemben támasztott követelményeket.

Élménybeszámolóm mondanivalóját szándékosan nem a látványos rekordkísérlet kihangsúlyozására fordítottam, hanem arra, hogy mennyi energiát invesztáltunk ebbe a nem mindennapi esemény lebonyolításába. Továbbá azt szerettem volna kihangsúlyozni a kedves olvasó számára, hogy egy több éves rutinnal rendelkező ember is kerülhet olyan helyzetbe, ami kizökkenti a napi kerékvágás menetéből, de a begyakorolt, vagy beidegződött tapasztalatai alapján sikeresen végre tudja hajtani a reá bízott feladatokat.

Nagyon örülök annak, hogy ebben a világra szóló rekordkísérletben részt vehettem. Köszönöm a Zrínyi Miklós Nemzetvédelmi Egyetem Híradó Tanszékének maximális támogatását.

A Masat-1 működési paramétereinek terepi kísérletével a ZMNE is elmondhatja, hogy hozzájárult az első magyar műhold sikeres teszteléséhez.

Mi is valójában a Masat–1?

Képzeljünk el egy eszközt, amely kisebb és könnyebb egy dobozos tejnél, napenergiával működik, és egy mobiltelefonnál is kevesebbet fogyaszt. A világűr szélsőséges körülményei között is képes üzeneteket küldeni, és közben gyorsabban száguld, mint egy puskagolyó. Ez **az első magyar műhold**.

A **Masat–1** (a név a „magyar" és a „satellite" szóból származik) egy kisméretű, úgynevezett pikoszatellit lesz, egy **10x10x10 centiméteres kocka**, mely **legfeljebb 1 kilogramm** tömegű lehet.

Építése egy pilot projekt, **elsősorban oktatási célt szolgál**. Tekinthetjük egy műszaki kísérletnek, melynek **eredményei a jövőben nagy segítséget jelenthetnek egy összetettebb űreszköz elkészítéséhez**. Pályára állása után a földi állomásokra küld majd információkat.

A kis méret és tömeg nem zárja ki a fedélzetére kerülő egységek **bonyolult, gondos tervezés**t igénylő felépítését. A start körülményeit elviselő mechanika tervezése, megvalósítása, az alrendszerek kiépítése és tervezése a jóval nagyobb műholdakkal azonos problémát vet fel.
A Masat–1 **tudományos célja** a szerkezet félaktív mágneses stabilizálása és a környezeti paraméterek, mint a hőmérséklet és gyorsulásvektorok mérése.

A Masat–1-et a tesztelések után, előreláthatóan **2010 elején bocsátják** majd **fel a világűrbe**.

http://cubesat.bme.hu

Kapcsolat

Projektvezető:
Dr. Gschwindt András
egyetemi adjunktus
gschwindt@cubesat.bme.hu

Projektmenedzser (kapcsolattartó)
Horváth Gyula
(1) 463-2992
horvath@cubesat.bme.hu

Sajtóinformáció:
sajto@cubesat.bme.hu
http://cubesat.bme.hu/sajto

Támogatók

MOBITEL Bt. HA5CH | Váry Kft. HA7JOL | Wacker Silicones HA8AR

A Magyar Köztársaság Kormánya

Jelenlegi és jövőbeni küldetéseinkhez további partnerek jelentkezését várjuk.

Masat–1 – Az elsők közt

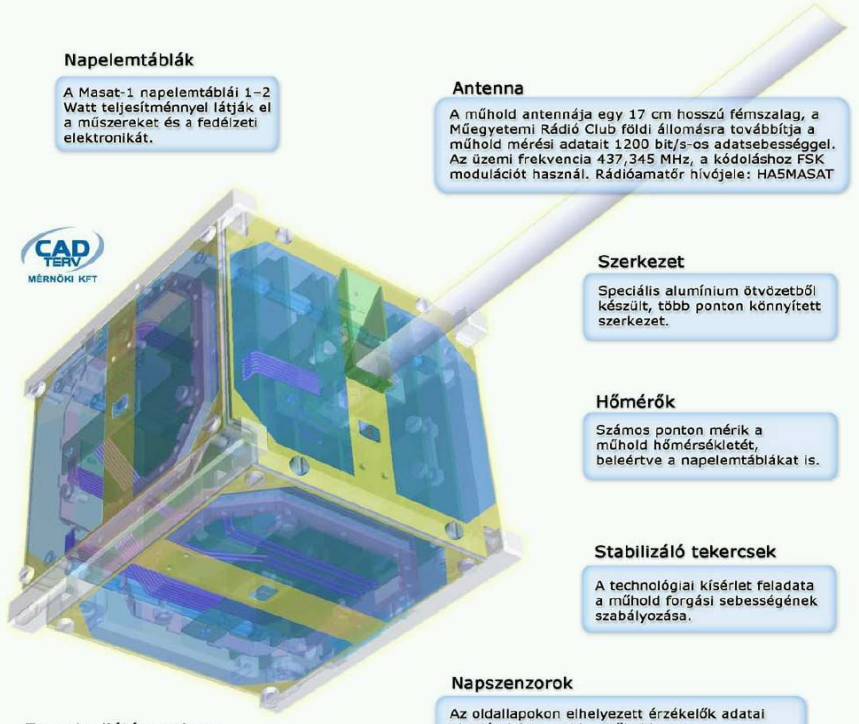
Mi építjük Magyarország első műholdját. Ha hazánk teljes jogú tagja lesz az Európai Űrügynökségnek (ESA), az **ország gazdasága nyithat az űripar felé**, de ehhez szakemberekre van szükség.

A Budapesti Műszaki és Gazdaságtudományi Egyetemen 2007 szeptembere óta folyik az első magyar műhold tervezése, fejlesztése és építése. A Masat–1 fejlesztői 2006 óta több hasonló nemzetközi projektben vettek részt, és most először vágtak bele önállóan egy űreszköz elkészítésébe. A fejlesztő csapat tagjai **lelkes mérnökhallgatók és doktoranduszok**, akik az Elektronikus Eszközök és a Szélessávú Hírközlés és Villamosságtan T székekkel együttműködésben dolgoznak, a BME Űrkutató Csoport szakmai támogatásával.

A kocka műholdak (angol nevükön *cubesat*) ötlete néhány évvel ezelőtt az USA-ban merült fel, és azóta több mint 40, különböző egyetemeken készült, hasonló műhold állt pályára. A Masat–1 lesz **az első magyar**.
A csapat a jövőben egy kétszer-háromszor ekkora műhold építését tervezi, amely méreténél fogva már komolyabb tudományos kísérleteket is végezhet. A fejlesztésben részt vevő mérnökök hosszú távon képesek lesznek arra, hogy **ipari megrendelésekre** építsenek hasznos feladatokat ellátó műholdakat.

Ha szeretne részese lenni az első magyar műhold építésének, kérjük adójának 1%-ával támogassa a Masat–1-et: Műegyetemi Rádió Club, adószám: 19005072-2-43.
További támogatási lehetőségek a weboldalunkon.

http://cubesat.bme.hu/tamogatas



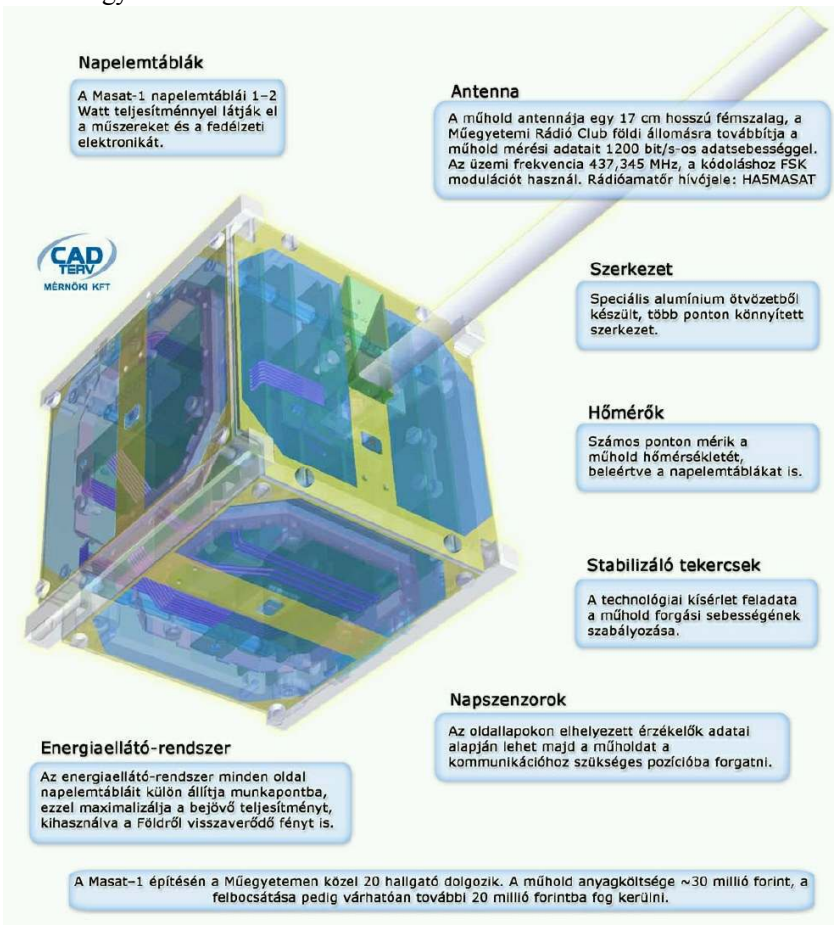
A Masat–1 építésén a Műegyetemen közel 20 hallgató dolgozik. A műhold anyagköltsége ~30 millió forint, a felbocsátása pedig várhatóan további 20 millió forintba fog kerülni.

CSÁSZÁR János – DUDÁS Levente

RÁDIÓS KAPCSOLAT A NEMZETKÖZI ŰRÁLLOMÁSSAL[1] ÉS A MASAT-1 – AZ ELSŐ MAGYAR MŰHOLD – KOMMUNIKÁCIÓS ALRENDSZERÉNEK TESZTJE[2]

[1]Császár János HA5PA villamosmérnök, okl. védelmi vezetéstechnikai rendszertervező
[2]Dudás Levente HA7WEN, okl. villamosmérnök, a Masat-1 műhold kommunikációs alrendszeréért felelős vezető mérnök

A Budapesti Műszaki és Gazdaságtudományi Egyetemen 2007 szeptembere óta folyik az első magyar műhold tervezése, fejlesztése és építése. A Masat-1 fejlesztői 2006 óta több hasonló nemzetközi projektben vettek részt, és most először vágtak bele önállóan egy űreszköz elkészítésébe.



A Masat-1 felépítése

A kocka műholdak (angol nevükön *cubesat*) ötlete néhány évvel ezelőtt az USA-ban merült fel, és azóta több, mint 40, különböző egyetemeken készült, hasonló műhold állt pályára. A Masat-1 lesz az első magyar.

A fejlesztő csapat tagjai lelkes mérnökhallgatók és doktoranduszok, akik az Elektronikus Eszközök és a Szélessávú Hírközlés és Villamosságtan Tanszékkel együttműködésben dolgoznak, a BME Űrkutató Csoport szakmai támogatásával. Ha hazánk teljes jogú tagja lesz az Európai Űrügynökségnek (ESA), az ország gazdasága nyithat az űripar felé, de ehhez szakemberekre van szükség.

Támogatóink

Képzeljünk el egy eszközt, amely kisebb és könnyebb egy dobozos tejnél, napenergiával működik, és egy mobiltelefonnál is kevesebbet fogyaszt. A világűr

szélsőséges körülményei között is képes üzeneteket küldeni, és közben gyorsabban száguld, mint egy puskagolyó. Ez az első magyar műhold.ú

A Masat-1 (a név a „magyar” és a „satellite” szóból származik) egy kisméretű úgynevezett pikoszatellit lesz, egy 10x10x10 cm-es kocka, mely legfeljebb 1 kg tömegű lehet.

A Masat-1 építése egy pilot projekt, elsősorban oktatási célt szolgál. Tekinthetjük egy műszaki kísérletnek, melynek eredményei a jövőben nagy segítséget jelenthetnek egy összetettebb űreszköz elkészítéséhez. Pályára állása után a földi állomásokra küld majd információkat.

A kis méret és tömeg nem zárja ki a fedélzetére kerülő egysége bonyolult, gondos tervezést igénylő felépítését. A start körülményeit elviselő mechanika tervezése, megvalósítása, az alrendszerek kiépítése és tervezése a jóval nagyobb műholdakkal azonos problémát vet fel. A Masat-1 tudományos célja a szerkezet félaktív mágneses stabilizálása és a környezeti paraméterek, mint a hőmérséklet és a gyorsulásvektorok mérése.

A Masat-1-et a tesztelések után, előreláthatóan 2010 elején bocsátják majd fel a világűrbe.

A csapat a jövőben egy kétszer-háromszor ekkora műhold építését tervezi, amely méreténél fogva már komolyabb tudományos kísérleteket is végezhet. A fejlesztésben részt vevő mérnökök hosszú távon képesek lesznek arra, hogy ipari megrendelésekre építsenek hasznos feladatokat ellátó műholdakat.

Ha szeretne részese lenni az első magyar műhold építésének, kérjük adójának 1%-ával támogassa a Masat-1-et: Műegyetemi Rádió Club, adószám: 19005072-2-43. További támogatási lehetőségek a weboldalunkon: http://cubesat.bme.hu/tamogatas

MUNK Sándor[2]

A KOMMUNIKÁCIÓ FOGALOMRENDSZERÉNEK KERETEI AZ INTERGRÁLÓDÓ INFORMÁCIÓS TECHNOLÓGIÁK KORÁBAN

(Frameworks of communication terminology in the era of information technology integration)

Absztrakt: Napjaink senki által nem vitatott jelensége az információs tevékenységeket támogató technológiák forradalmi ütemű fejlődése, integrációja, konvergenciája. Mindez maga után vonja az egyes szakterületek közötti együttműködés kibővülését. Tényként fogadható el, hogy az egymással egyre szorosabb kapcsolatba kerülő szakterületek fogalomrendszere nincs egymással harmóniában, ami egyre növekvő mértékben akadályozza a hatékony együttműködést. Ezen terminológiai problémák különösen jelentős szerepet játszanak az oktatásban. Jelen publikáció áttekinti, elemzi a kommunikáció alapvető fogalmainak rendszerét; ehhez vizsgál és értelmez néhány alapvető fogalmat; majd elemzi a kommunikáció egyes alapvető fogalmait, fogalom-megnevezéseit.

One of the unquestioned phenomena of our age is revolutionary development, integration, convergence of technologies supporting information activities. This involves the extension of cooperation between individual professional areas. It is a fact that the concepts, and ideas of professional areas, building more and more strong connections with each other, are not in harmony and that increasingly impedes the efficient cooperation. Such terminology problems play especially important role in education. This publication reviews, and analyses system of basic concepts of communication; discusses and interprets some fundamental concepts; and analyses some basic concepts and terms of communication.

Kulcsszavak: információtechnológia, kommunikáció, távközlés, integráció, terminológia ~ information technology, communication, telecommunication, integration, terminology

Bevezetés

A XXI. század eleje óta gyakorlatilag már senki által nem vitatott, minden szakterület és szakember által elfogadott jelenség a különböző információs tevékenységeket támogató technológiák (számítástechnika, híradástechnika, nyomdatechnika, méréstechnika, irányítástechnika, irodatechnika, oktatástechnika, stb.) forradalminak nevezhető ütemű fejlődése, technológiai alapjaik egységesülése és egyre inkább funkcionális integrációjuk, konvergenciájuk.

A technológiák konvergenciája, integrálódása értelemszerűen maga után vonja az egyes szakterületek és szakembereik közötti együttműködés jelentőségének és tartalmának kibővülését, illetve a különböző információs technológiákat felhaszná-

2 ZMNE BJKMK Informatikai tanszék, munk.sandor@zmne.hu

ló szervezetek, személyek hatékony alkalmazáshoz szükséges ismeretanyagának megnövekedését. Mindez azzal jár, hogy korábban egymással kevésbé együttműködésre szoruló szakembereknek kell egymással információt cserélniük, egymás ismeretanyagát a szükséges mértékben megismerniük, illetve hogy a felhasználóknak korábban egymástól elkülönülő szakterületek által nyújtott ismeretanyagokat kell elsajátítaniuk, "integrálniuk".

Nem minősíthető új megállapításnak az sem, hogy az egymással egyre szorosabb kapcsolatba kerülő – valamikor a jövőben talán egy közös szakterület részévé váló – szakterületek fogalomrendszere a sajátos igények, megközelítések és a saját múlt, szakmai fejlődés következtében nincs egymással harmóniában. Ezek a különbözőségek, fogalmi heterogenitás egyre növekvő mértékben akadályozzák és fogják akadályozni a hatékony együttműködést, az egyes szakterületek ismeretanyagának összehangoltságát, egységes rendszerbe történő integrálódását. A mind az elmélet, mind a gyakorlat oldaláról növekvő mértékben jelentkező igények szükségessé, elkerülhetetlenné teszik egy közös, átfogó, az egymással szoros kapcsolatba kerülő szakterületek számára is megfelelő fogalomrendszer kialakítását.

Az egymással szoros kapcsolatban álló szakterületek terminológiai problémái különösen jelentős szerepet játszanak az oktatásban, ezen belül is elsősorban az integrált ismeretek nyújtására létrehozott szakok esetében, mint amilyen a ZMNE BJKMK Informatikai és Hírközlési Intézetének felügyelete alatt álló védelmi vezetéstechnikai rendszerszervező mesterszak, amelyben egymáshoz kapcsolódó, egymást kiegészítő, illetve egymásra épülő szakmai törzstantárgyak és szakirányú tantárgyaknak kell biztosítaniuk egy integrált ismeretanyagra támaszkodó tudás, képességek (kompetenciák) kialakítását.

Az Informatikai és Hírközlési Intézet tanszékei és szakemberei ezt a problémát természetesen felismerték és 2008 őszén egy intézeti munkacsoport keretében kísérletet tettek egy, a szakon folyó oktatást megalapozó terminológiai kutatás beindítására, azonban erre az oktatási és kutatási feladatok, illetve az éppen folyó akkreditációs felkészülés miatt nem jutott megfelelő kapacitás. A jelen publikációban foglaltak e tervezett kutatás részét képezik, elsőként a kommunikáció, távközlés fogalomrendszeréhez kapcsolódóan.

Külön ki kell emelnem, hogy magam – informatikus lévén – nem vagyok a vizsgált szakterület szakembere, így a publikációban foglaltak minden bizonnyal tartalmazhatnak hibás értelmezéseket, megállapításokat, elképzeléseket, javaslatokat. Ennek ellenére azt gondolom, remélem, hogy néhány dolog egy bizonyos értelemben kívülálló szemével is talán felismerhető, néhány javaslat megfogalmazható.

Mindezek alapján jelen publikáció célja, hogy áttekintse, elemezze a kommunikáció – az információtovábbítás, információcsere – és annak technikai támogatása alapvető fogalmainak rendszerét. Ezen belül célja:

- néhány alapvető és a kommunikációs technológiák területén is alkalmazott alapvető fogalom vizsgálata, értelmezése;
- a kommunikáció alapvető fogalmainak, fogalom-megnevezéseinek tartalmi vizsgálata, elemzése;
- néhány következtetés, javaslat megfogalmazása a további kutatómunkához.

Már e helyen is jelezni kell, hogy a jelen publikációban foglaltak – különösen a szerző lehetőségeiből következően – nem törekednek teljességre és semmiképpen sem jelentik (nem is célozzák) a kommunikáció alapfogalmai vizsgálatának a lezárását, viszont vitaalapként hozzájárulhatnak – minimálisan a ZMNE keretei közötti, esetleg a katonai alkalmazásban is elfogadott – terminológiai jellegű kutatásokhoz, egy integrált fogalomrendszer kialakításához és az ehhez hasonló feladatokat természetesen el kell végezni a kapcsolódó szakterületeken is.

Néhány Alapvető fogalom vizsgálata, értelmezése

A kommunikációhoz – és bármely más, információs tevékenységek technikai támogatásához – kapcsolódó fogalmak egységes keretek közé illeszkedő vizsgálatához először elengedhetetlen olyan általános fogalmak vizsgálata és értelmezése, mint: eszköz, rendszer, szolgáltatás. Ezeket ugyanis az egymáshoz egyre közelebb kerülő szakterületek mindegyike használja, így egységes értelmezésük mintegy alapját képezi egy összehangolt fogalomrendszernek. A felsorolt fogalmak kiválasztása viszonylag önkényes, ezek mellett más – szintén alapvető – fogalmak (pld. hálózat, infrastruktúra) vizsgálata is szükséges lehet, ez azonban már további kutatások tárgyát kell képezze. Jelen fejezet alapvetően az említett három fogalom tartalmának áttekintő vizsgálatát, egységes értelmezésük kereteinek kialakítását célozza, amelyet megelőz az alkalmazott terminológiai vizsgálatok "szellemiségének" és módszerének bemutatása.

A terminológiai vizsgálatok alapjai

Jelen publikáció – és a szerző általában is érvényes – határozott elképzelése, hogy terminológiai vizsgálatok alapját mindenekelőtt az egyes fogalmak tartalmának elemzése kell képezze és csak ezt követően, ennek alárendelten lehet, vagy kell vizsgálni a fogalmak megnevezéseit. Ez utóbbiakat ugyanis többek között nyelvi hatások, kialakult hagyományok, sőt sok esetben egyes szakmai körök presztízs-szempontjai is befolyásolják. Elismerve azt a tényt, hogy egy jól megválasztott megnevezés, építve a benne szereplő összetevők már létező értelmezéseire, jelentős mértékben segíti, sőt sokszor körül is határolja az általa jelölt fogalom tartalmának értelmezését, mégis mondható, hogy a megnevezés csak egy címke, ami viszonylag szabadon megválasztható. Azonos tartalom és eltérő címke[3] kevésbé nehezíti az együttműködést, információcserét, közös értelmezést, mint az egymástól eltérő, egymást csak átfedő tartalmú fogalmak léte.

A terminológiai kérdések vizsgálata során szembe kell nézni azzal a ténnyel is, hogy a gyakorlatban, különösen a szakmai és jogi szabályozókban az alkalmazott fogalmak tartalmának és megnevezésének meghatározása során számos olyan tényező is érvényesül, amelyek nem abszolút jellegűek, hanem a szabályozandó terület, vagy a szabályozást megalkotó szakmai kör sajátosságaiból fakadnak. Ezt a jogszabályok általában korrektül jelzik is a "jelen szabályozás alkalmazásában" jellegű megfogalmazásokkal.

[3] Például 'távközlő rendszer' és 'távközlési rendszer', vagy 'szolgáltatás' és 'szolgálat' ha ezek ugyanazt a tartalmat jelölik és egyikükhöz sem kapcsolódik tartalmában is eltérő értelmezés. Meg kell jegyeznünk, hogy e két példa is abba a csoportba tartozik, amikor egy idegen nyelvű (pld. angol) szakkifejezés magyar fordításai vetekszenek egymással és a mellettük szóló érvek alapvetően nyelvi (presztízs?), nem pedig szakmai jellegűek.

Tudományos értékű vizsgálatok során megítélésem szerint a jogszabályokban, vagy adott szakterületek fogalomjegyzékeiben megtalálható fogalmakat (meghatározásokat) nem szabad "isteni kinyilatkoztatásként" kezelni, ugyanakkor nem is szabad a tudomány "elefántcsont tornyából" feltétlenül új, "jó" fogalmakat alkotni, ugyanis a fogalmaknak és a megnevezéseknek is meg van a maguk "élete" és elsősorban gyakorlati alkalmazhatóságukra, elterjedtségükre alapozva mélyen gyökerezhetnek szakmai közösségekben. A gyakorlatban bekövetkező változások, fejlődés szükség esetén úgyis maga után vonják a fogalom meghatározások folyamatos fejlesztését, változását.

Oktatási szempontból viszont elengedhetetlen az egyes, elsősorban alapfogalmak részletesebb vizsgálata, a gyakorlatban előforduló meghatározások fogalomalkotási szabályoknak megfelelő elemzése, az egyes összetevők (legközelebbi magasabb szintű fogalom = genus proximum, megkülönböztető jegy = differentia specifica) feltárása, elemzése, szükség esetén pontosítása. Fogalmak, fogalomrendszerek elsajátításához, fogalmak közötti viszonyok bemutatásához általában szükség van rendszerező, csoportosító fogalmak bevezetésére és teljes körű osztályozások kialakítására is, amelyek a gyakorlatban esetleg nem szükségesek.

Eszközök, rendszerek

Az információs tevékenységek, folyamatok, köztük a később tárgyalásra kerülő kommunikáció támogatásában alapvető szerepet játszanak az eszközök, amelyek meghatározására részletesebb indoklás és hivatkozások nélkül a következőt fogadjuk el:

Eszköz: Egy tevékenység végrehajtását megkönnyítő, lehetővé tévő tárgy.

Az eszközök közé tartoznak az egyes műveletek önálló (emberi beavatkozás nélküli) végrehajtására képes gépek (='működő' eszközök), amelyek elsősorban fizikai műveletvégzésre képesek, de működésük irányítása, ellenőrzése továbbra is az ember feladata, valamint a vezérlőberendezéssel kiegészített, nagyobbrészt önállóan működő, de szükség és igény esetén emberi beavatkozást biztosító automatizált (='önállóan működő') eszközök.

Általános eszközökkel nem találkozhatunk, csak ***adott funkció(ka)t megvalósító eszközök*** léteznek. Minden eszköz esetében adott a rendeltetése, vagyis hogy az milyen tevékenység, vagy tevékenységek végrehajtásának elősegítésére, megvalósítására van szánva.[4] Ennek megfelelően az eszközök osztályozhatóak, sajátos eszköztípusok határozhatóak meg annak alapján, hogy milyen tevékenységek elősegítésére, megvalósítására alkalmasak. Az információs tevékenységekhez kapcsolódóan a funkcionális osztályozásnak megfelelően beszélhetünk tehát többek között az információtovábbítást, az automatizált adatfeldolgozást, az információszerzést, vagy a helymeghatározást támogató eszközökkel.

Az eszközök egy másik lehetséges csoportosítása technológiai sajátosságaik alapján történhet. Ennek megfelelően léteznek ***adott technológiára épülő eszközök***. Ezek közül az információs tevékenységeket támogató eszközök között napjainkban alapvető szerepet az elektronikai (elektronikus) eszközök játszanak, de léteznek (léteztek) mechanikus, elektromechanikus, pneumatikus, vagy más típusú eszközök

[4] Természetesen számos eszköz alkalmas lehet eredeti rendeltetésétől eltérő alkalmazásra is.

is. Ezen fogalmak rendszerezése, értelmezése azonban további vizsgálatokat igényel majd, különös tekintettel az elektronikus jelző eltérő értelmezéseire, illetve a köznyelvben – és esetenként a szakmai nyelvben – kialakult, tényleges jelentéséhez csak közvetve kapcsolódó, sok esetben nem a lényeget kifejező alkalmazására.[5]

Az eszközök egy része, az úgynevezett ***egyedi, autonóm eszközök*** önmagukban, más eszközök igénybevétele nélkül képesek az adott tevékenységek elősegítésére, megvalósítására. Ezek azonban általában egyszerűbb feladatok, műveletek végrehajtása során alkalmazhatóak. Ebbe a csoportba tartoznak például a kézi számológépek, az egyedi mérőkészülékek, vagy a hagyományos (csillagászati) navigáció eszközei.

Napjainkban az információs tevékenységeket már jellemzően nem egyedi eszközök, hanem egymással ***együttműködő eszközökből álló eszközrendszerek*** támogatják. Egyes tevékenységek esetében ez magától értetődő, hiszen például az információtovábbítás támogatásához legalább két eszközre van szükség. Más esetekben a több eszközből álló rendszerek előnyei elsősorban az egyes eszközök által nyújtott azonos, vagy sajátos képességek megosztásában rejlenek. Információs tevékenységeket segítő eszközrendszerek közé tartoznak többek között a különböző kommunikációs, navigációs (helymeghatározó), felügyeleti és folyamatirányító, műsorszóró és számos más típusú rendszerek.

Bár az előzőekben említett rendszerek esetében beszélhetünk önmagukban az együttműködő technikai eszközök rendszeréről, az alkalmazás szempontjából fontosabb szerepet játszanak a meghatározott funkciók megvalósítására – meghatározott [információs] tevékenységek elősegítésére, megvalósítására, vagyis meghatározott [információs] szolgáltatások nyújtására – rendszerbe szervezett technikai eszközök, más erőforrások, valamint a működtetésben érintett szervezetek, személyek együttesei.

Technikai (működő) rendszer: Meghatározott tevékenységek elősegítésére, megvalósítására rendszerbe szervezett technikai eszközök, más erőforrások, valamint a működtetésben közreműködő szervezetek, személyek együttese.

A rendszer fogalommal kapcsolatban feltétlenül szükséges meghatározni, hogy milyen szempontok alapján jelölhetőek ki egy rendszer határai, vagyis mely eszközök, erőforrások, személyek tartoznak egy rendszerhez és melyek nem. Ennek vizsgálata más kérdésekhez hasonlóan szintén további munkát igényel, így ebben a publikációban csak egyetlen, alapvető szempontot fogalmazunk meg. Ez pedig az egységes felügyelet, irányítás, döntési jogkör megléte, ami nélkül csak egymással – szorosan, vagy lazábban – együttműködő rendszerekről beszélhetünk, nem pedig egységes rendszerről. Ennek a kérdésnek az erőforrás-kihelyezés/kiszervezés (outsourcing) megjelenésével és elterjedésével egyre növekvő jelentősége van.

Funkciók, szolgáltatások

Az előzőekben megfogalmazottaknak megfelelően adott típusú (pld. kommunikációs, navigációs, azonosító, stb.) eszközök, rendszerek rendeltetése meghatározott [információs] tevékenységek végrehajtásának elősegítése, megkönnyítése, vagy egyenesen teljes körű megvalósítása. Mindezt az adott ***eszközök, rendszerek***

[5] Lásd például az elektronikus aláírás, elektronikus kormányzat fogalmakat.

sajátos ***képességei*** és ezekre épülő ***funkciói*** biztosítják. Egy adott eszköz, rendszer funkciói alatt általában mindazon speciális folyamatokat, feladatokat, tevékenységeket értjük, amelyek megvalósítására, végrehajtására az eszközt, rendszert tervezték. Ezek körét a funkcionális specifikáció, leírás rögzíti. Az említett képességek és funkciók az eszközök fejlesztése, a rendszerek létrehozása során a támogatandó tevékenységek igényeinek megfelelően kerülnek kialakítása, azonban a későbbiekben új, korábban talán még nem is létező tevékenységek támogatására is alkalmat nyújthatnak.

A különböző eszközök, rendszerek képességei, funkciói az alkalmazás, igénybevétel esetén ***szolgáltatások*** formájában realizálódnak, ami alatt a szokásos értelmezésnek megfelelően nem kézzel fogható eredménnyel járó (vagyis nem "termelő") tevékenységet, munkavégzést értünk. Mivel a nyújtott szolgáltatások elősegítik adott tevékenységek végrehajtását, ezek a fogalmak elhelyezhetőek a következő modellben is:

[támogatott] tevékenység→ szolgáltatások ← [támogató] eszköz, rendszer

A támogatott oldalon találhatóak azok a személyek, szervezetek, folyamatok, amelyek az adott szolgáltatásokat egyes tevékenységeik során igénybe veszik, felhasználják. A támogató oldalon állnak azok a rendszerek, eszközök, amelyek az említett szolgáltatásokat nyújtják, azok igénybevételének feltételeit megteremtik és folyamatosan fenntartják. Végül a két fél "között" helyezkednek el az információs tevékenységek támogatására irányuló szolgáltatások. Ezeket ma már többnyire egy új, negyedik szektor (információs szektor, információgazdaság) részének tekintik.

Az ***információs szolgáltatások*** két nagy csoportját az információszolgáltatások, illetve az információs tevékenységek megvalósítása képezik. Az előbbiek alapvető célja a felhasználók számára hasznos információk – felhasználói információigények, vagy a szolgáltatói döntések alapján történő – megszerzése, megkeresése, előállítása, rendelkezésre bocsátása. Az utóbbiak rendeltetése pedig meghatározott műveletek (átalakítás, tárolás, továbbítás, stb.) végrehajtása a felhasználók által rendelkezésre bocsátott információkkal. Ezen elemi szolgáltatásokból természetesen összetett szolgáltatások alakíthatóak ki.

Információs szolgáltatás: Információs tevékenységek támogatása információk szolgáltatásával, vagy információs műveletek végrehajtásával.

Az információs tevékenységeket támogató eszközök, rendszerek korábban jellemzően ***specifikus funkciók*** támogatására, ***specifikus szolgáltatások*** nyújtására voltak képesek, még egy-egy átfogó információs tevékenységi területen – pld. információtovábbításon, információrögzítésen, információmegjelenítésen – belül is. Önálló eszközök, rendszerek támogatták a beszédkommunikációt (távbeszélő, rádió), a karakteres üzenetek továbbítását (távíró), vagy képek továbbítását (telefax). Más és más eszköz volt képes az álló és a mozgókép, valamint a hang rögzítésére, majd lejátszására (fényképezőgép, kamera és képrögzítő, mikrofon és hangrögzítő).

Az információtechnológia fejlődésének egyik alapvető jellemzője az információs tevékenységeket támogató eszközök, rendszerek képességeinek, az általuk nyújtott szolgáltatások körének bővülése, korábban önálló eszközök, rendszerek által biztosított ***funkciók, szolgáltatások integrációja***. Ma már egy, a mindennapok során használt eszköz – a "mobiltelefon" – képes távbeszélő szolgáltatásra, egysze-

rű szöveges üzenetek cseréjére, fényképek készítésére, információk tárolására, vagy hang- és mozgókép-felvételek lejátszására, esetleg helymeghatározásra. Vagy egy Internetre csatlakozó "számítógép" képes távbeszélő, képtelefon, telefax, videokonferencia szolgáltatás nyújtására, közvetítésére.

Az egyes eszközöket, rendszereket, a biztosított funkciók, szolgáltatások körének bővüléséből következően, egyre nehezebb besorolni egyetlen funkcionális (pld. kommunikációs, információrögzítő, helymeghatározó, szórakoztató elektronikai, stb.) kategóriába és értelmetlen lenne minden egyes ilyen eszköz, rendszer számára a konkrét szolgáltatások alapján egyedi kategóriát kitalálni. Mindez természetesen elsősorban a tudományos és oktatási szférára vonatkozó megállapítás, mivel a gazdasági és mindennapi életben a kategorizálást és megnevezést egyéb (praktikus és szubjektív) szempontok is befolyásolják.

A ***több funkciót, szolgáltatást nyújtó eszközök, rendszerek*** funkcionális jellemzésére, illetve a különböző csoportokba tartozóak összefoglaló megnevezésére példa a polgári életben – azon belül is elsősorban a kormányzati és az oktatási szférában – az 'infokommunikációs'[6] kategória, illetve a NATO és magyar katonai alkalmazásban a 'híradó és informatikai' (communication and information [systems]) [1, 2-8.o.] jelző.

Az előbbi fogalom a kommunikációs szakterületen jelent meg és kezdeti értelmezése szerint a távközlés, az informatika és az elektronikus média integrációját jelentette. [2; 3] Ezt követően tágabb értelmezések is megjelentek: "… az infokommunikációs rendszerek jóval többet jelentenek, mint csak az informatikai és távközlési rendszerek konvergenciájából kialakuló rendszerek. Ebbe beletartoznak mindazon rendszerek is, melyek az érzékelés, irányítás, vezérlés funkcióit látják el. Így pl. e kategóriába sorolhatók azok a repülőtéri leszállító és irányító rendszerek is, amelyek a távközlési rendszereken és a számítógép-hálózatokon keresztül csatlakoznak más rendszerekhez." [4, 1.o.] Az infokommunikációs jelző úgy tűnik, napjainkban csak korlátozottan elfogadott, alkalmazott és ami ennél is fontosabb, tartalmának egységes értelmezése sem alakult ki.

A különböző eszközök, rendszerek szolgáltatásaikat nyújthatják ***önállóan***, vagy ***más eszközök, rendszerek szolgáltatásainak felhasználásával***. Az információs szolgáltatások így a gyakorlatban összetett, egymásra épülő elemekből álló struktúrát alkotnak. A más rendszerek által leggyakrabban igénybevett szolgáltatások közé mindenekelőtt a kommunikációs szolgáltatások tartoznak, mivel saját kommunikációs képességek kialakítása többnyire nem gazdaságos és nem is hatékony. A nyújtott szolgáltatások feltételei, az ehhez szükséges – másoktól igénybevett – szolgáltatások az adott rendszerek "belső ügyei", a szolgáltatásokat igénybevevő felhasználók számára alapvetően érdektelenek, tulajdonképpen számukra "láthatatlannak" kell maradjanak.

Néhány Kommunikációs alapfogalom, fogalom-megnevezés vizsgálata, elemzése

Az információtovábbítást, információcserét támogató eszközök, rendszerek régóta támogatják az emberi tevékenységet. E szakterület legtágabb keretét a két, vagy

[6] A fogalom eredeti angol kifejezése: information and communication technologies (ICT) = információs/informatikai és kommunikációs technológiák.

több fél közötti információtovábbítás, információcsere (kommunikáció) képezi.[7] Az információ áramolhat két fél között, egy fél és több másik között, valamint több fél között. A kommunikáció legegyszerűbb formája az ugyanazon helyen és időben jelenlévő felek közötti, segédeszközök nélküli, közvetlen kommunikáció. Minden más esetben a kommunikáció megvalósításához más személyek, vagy eszközök, rendszerek igénybevételére van szükség.

A kommunikáció típusai, alapfogalmai

A kommunikációs folyamat során az áramló információk a felek – a küldő és a fogadó – által egységesen értelmezett (egyeztetett) információ-reprezentációk formájában kerülnek továbbításra. Ezek hordozói lehetnek: az emberi hang, beszéd, gesztusok; valamilyen anyagi hordozó; vagy valamilyen anyagi (fizikai, kémiai, stb.) folyamat meghatározott jellemzői. A két utóbbi megoldás képezheti alapját a közvetett kommunikáció két különböző megvalósítása megkülönböztetésének.

Az első változatban az információtovábbítás a küldő fél által létrehozott információhordozó (küldemény) minden átalakítás nélküli fizikai továbbítására, a fogadóhoz történő eljuttatására épül. A második változatban a továbbítandó információ, pontosabban annak a küldő által előállított – szemléletes, vagy szimbolikus, hagyományos, vagy elektronikus – reprezentációja a továbbítás előtt az átvitel technikai megvalósításának függvényében átalakításra, majd az így létrehozott közvetítő reprezentáció (jel, jelsorozat) átvitelét követően az eredeti, vagy a kívánt formára visszaalakításra kerül.

Összegzésképpen tehát a kommunikációhoz kapcsolódóan négy alapvető fogalom megfogalmazása szükséges, amelyek a következőek:

K1: két, vagy több fél közötti információtovábbítás, információcsere.

K2: közvetítő személyek, segédeszközök felhasználása nélküli információtovábbítás, információcsere.

K3: információhordozók átalakítás nélküli, fizikai továbbítására épülő információtovábbítás, információcsere.

K4: információk jellé, jelsorozattá történő átalakítására, a jel(ek) átvitelére, majd az eredeti, vagy más kívánt formára történő visszaalakítására épülő információtovábbítás, információcsere.

A K1 fogalom megnevezése gyakorlatilag egyértelműen elfogadottan ***kommunikáció*** (communication[8]), a K2, K3 és K4 fogalmak pedig a kommunikáció fogalmának teljes – és hosszú távon érvényes – osztályozását képezik. A három utóbbi fogalom megnevezése, illetve a kapcsolódó kifejezések tartalma mind magyar, mind angol nyelven mutat eltéréseket. A K2 fogalom megnevezése általában ***közvetlen személyközi kommunikáció*** (direct interpersonal communication), azonban meghatározásai esetenként már eltérhetnek K2 tartalmától. Kutatásunk téma-

[7] Az információtovábbításban, információcserében résztvevő felek alatt általában embereket értünk, de a fogalom értelmezhető élőlények között is.

[8] Az egyes számban értelmezett **communications** kifejezés (1) a kommunikáció során alkalmazott eszközöket, (2) a kommunikációhoz kapcsolódó technika-területet [híradástechnika], valamint (3) közlekedést jelöl.

köre miatt ezzel a fogalommal a továbbiakban részletesebben már nem foglalkozunk.

A K3 fogalom megnevezésére egységesen elfogadott kifejezés gyakorlatilag nem létezik, egy változat lehet a ***küldemény-alapú kommunikáció***. Ez a megoldás jellemzően a ***postai szolgáltatások*** – a katonai alkalmazásban a futár- és tábori posta szolgáltatások – közé tartozik. Ide sorolható mindenekelőtt a levélpostai küldemények továbbítása, a csomagszállítás egy része (információhordozók továbbítása), valamint a hírlapterjesztés. E kommunikációs megoldás sajátos változata került alkalmazásra az 1970-es évekig a felderítő műholdak felvételeinek továbbítására, amikoris az exponált filmek fémkapszulában, ejtőernyővel jutottak vissza a Földre.

Távközlés

A K4 fogalom megnevezésére a ***távközlés*** (telecommunication[9]) kifejezés látszik a legalkalmasabbnak, amelynek legtöbb meghatározása közel áll, de nem azonos K4 tartalmával:

> ***A Magyar Nyelv Értelmező Szótára****: Híreknek főképp elektronikus készülékeken (telefon, távíró, rádió, stb.) való továbbítása* [5, 542.o.]
>
> ***New Oxford Dictionary****: Vezeték, távíró, telefon, vagy műsorszórás segítségével megvalósított távolsági kommunikáció.* [6] ***Webster's Dictionary****: Telefon, távíró, stb. segítségével megvalósított kommunikáció tudománya vagy technikája.* [7, 1459.o.]
>
> ***Magyar Nagylexikon****: Bármilyen természetű jelek, jelzések, nyomtatott, v, kézírás, hang, kép, ezekből összetett híranyagok átvitele vezetékes, rádió-, optikai v. más elektromágneses rendszerekkel.* [8, 241.o.]
>
> ***IEC Vocabulary, AComP-1, AAP-6****: 1. Vezetékes, rádió-, optikai, vagy más elektromágneses rendszerek segítségével megvalósított kommunikáció. 2. Jelek, jelzések, írás, képek és hangok, vagy bármilyen hírek, értesülések átvitele, kisugárzása, adása, vagy vétele vezetékes, rádió-, optikai, vagy más elektromágneses rendszerek segítségével.* [9, 701.01.05.; 10, 701.01.05.; 11, 2-T-4 o.]
>
> ***Wikipédia****: Eszközökkel segített távolsági átvitel kommunikáció céljára. Korábban ez füstjelek, dobok, szemafor, zászlók, vagy fénytávíró használatát igényelte. Napjainkban a távközlés jellemzően elektronikus eszközök – pld. telefon, televízió, rádió, számítógépek – használatát igényli.* [12]

A meghatározások jó részéből látható, hogy azok alapvető eltérése K4 tartalmától – gyakorlati okokból – abban áll, hogy esetükben az átvitel a vezetékeken folyó

[9] Az egyes számban értelmezett **telecommunications** kifejezés a távközléshez kapcsolódó technika-terület [távközléstechnika] megnevezése.

elektromos áramhoz, illetve az elektromágneses mezőhöz kapcsolódik. Az információt hordozó jelsorozat átvitelére azonban elméletileg más fizikai jelenségek – például mechanikai rezgések, radioaktív sugárzás, stb. – is alkalmasak, sőt ilyenek már a gyakorlatban is alkalmazásra kerültek (akusztikus hullámokra épülő vízalatti kommunikáció, vagy szeizmikus hullámokra épülő földalatti kommunikáció[10]). És bár gyakorlati alkalmazásra még nem került sor, de az élő szervezetekben hatékonyan működik a kémiai folyamatokra épülő kommunikáció is.

Mindebből következően a K4 fogalom tovább osztályozható az átvitel során felhasznált anyagi folyamat jellege szerint. Ezek egyike lehet a szakirodalomban előforduló távközlés fogalom tényleges jelentése, amelyet ennek megfelelően valójában elektromos, elektromágneses [jelek segítségével megvalósított] távközlésnek kellene nevezni.

K4a: információk elektromos, elektromágneses jellé, jelsorozattá történő átalakítására, a jel(ek) átvitelére, majd az eredeti, vagy más kívánt formára történő visszaalakítására épülő információtovábbítás, információcsere.

Az elektromos, elektromágneses távközlés helyett használható az elektromos, elektromágneses kommunikáció kifejezés is, mivel a jelzőből már következik a jelsorozattá történő átalakítás, majd átvitel. Ugyanez igaz a további jelzős szerkezetű kifejezésekre, mint az akusztikus távközlés, szeizmikus távközlés, kémiai távközlés, stb.

Más szempontból jelent eltérő értelmezést a távközlés 'nagyobb távolságot áthidaló, technikai eszközökkel segített kommunikáció' jellegű meghatározása. Ez ugyanis magában foglalja a K3 fogalom tartalmát is, hiszen a hagyományos postai kommunikációs szolgáltatások is nagyobb távolságot hidalnak át és technikai (pld. szállító), sőt speciálisan a kommunikációs folyamat során felhasznált (pld. levélosztályozó, elosztó, stb.) eszközök segítségével kerülnek megvalósításra.

Hírközlés, elektronikus hírközlés

A távközlés mellett magyar nyelvben és jogi szabályozásban szerepel a ***hírközlés*** kifejezés is, ami magában foglalta a postai, a távközlési és a műsorszóró szolgáltatásokat. Ezen szakterületek Magyarországon 1990-ig mind a Magyar Posta keretében működtek és akkor váltak szét három önálló szervezetre.

> ***A Magyar Nyelv Értelmező Szótára**: Ált. hírek közlése. 1. (hiv.) Hírügynökségeknek az a tevékenysége, hogy eljuttatják egymáshoz és a sajtóhoz a híranyagot. [13, 264.o.]*
>
> ***2001. évi XL. tv. a hírközlésről**: Küldemény, adat, jel, kép, hang, továbbá bármilyen információ hírközlő infrastruktúra rendeltetésszerű felhasználásával történő továbbítása, vétele. [14, 110.§ 27.] Hírközlési szolgáltatás: olyan, más részére ellenszolgáltatásért végzett távközlési és postai tevékenység, amely küldemény, adat, jel, kép, hang, továbbá bármilyen információ továbbítása a hírközlési infrastruktúra használatával. [14, 110.§ 29.] Hírközlő*

[10] Például búvárokkal, tengeralattjárókkal, illetve bányászokkal, föld alatt rekedtekkel folytatott kommunikáció céljaira.

hálózat: a postai hálózat, illetve a távközlő hálózat. [14, 110.§ 31.]

A fentiek alapján tulajdonképpen azt mondhatjuk, hogy hírközlés $\subseteq$ K3 $\cup$ K4. A kifejezéssel leírt összefoglaló fogalom inkább gyakorlati (pld. jogi szabályozási), mint elméleti jelentőségű, mivel a benne foglalt kommunikációs módok között az információtovábbítási szolgáltatás funkcióján kívül kevés hasonlóság mutatható ki.

A két, egymástól jelentős mértékben eltérő szakterület ('távközlés', 'postai tevékenység') a későbbiekben a szabályozás szintjén ismét különvált, az új, immár elektronikus hírközlési törvényben a postai tevékenység érdemben már nem szerepel. Az új törvény nem határozza meg a hírközlés, vagy az elektronikus hírközlés fogalmát, azonban többek között tartalmazza az elektronikus hírközlési tevékenység és az elektronikus hírközlő hálózat definícióját:

> ***2003. évi C. tv. az elektronikus hírközlésről**: Elektronikus hírközlési tevékenység olyan tevékenység, amely bármely értelmezhető formában előállított jel, jelzés, írás, kép, hang vagy bármely természetű egyéb közlemény elektronikus hírközlő hálózaton keresztül egy vagy több felhasználóhoz történő eljuttatását szolgálja, így különösen ... [15, 188.§ 15.]*
>
> *Elektronikus hírközlő hálózat: átviteli rendszerek és – ahol ez értelmezhető – a hálózatban jelek irányítására szolgáló berendezések, továbbá más erőforrások, melyek jelek továbbítását teszik lehetővé meghatározott végpontok között vezetéken, rádiós, optikai vagy egyéb elektromágneses úton, beleértve a műholdas hálózatokat, a helyhez kötött és a mobil földfelszíni hálózatokat, az energiaellátó kábelrendszereket, olyan mértékben, amennyiben azt a jelek továbbítására használják, a műsorszórásra használt hálózatokat és a kábeltelevíziós hálózatokat, tekintet nélkül a továbbított információ fajtájára. [15, 188.§ 19.]*

A fenti meghatározásokat elemezve megállapítható, hogy érdemi tartalmi eltérés nem mutatható ki a távközlés fogalmához képest és a törvényelőkészítés időszakában szakmai körökben is többen foglalkoztak a távközlés ~ hírközlés kifejezések használatának kérdésével és fejezték ki véleményüket az elektronikus hírközlés kifejezés bevezetésével szemben. [16, 17]

Az elektronikus hírközlési szabályozás joganyagaiban legelterjedtebben használt, forrásokkal alátámasztható fogalmakat a Nemzeti Hírközlési Hatóság egy online módon elérhető fogalomjegyzékben gyűjtötte össze (ami az 'elektronikus hírközlési' helyett az 'infokommunikációs' jelzőt viseli). [18] A fogalomjegyzék magyar és angol definíciókat és megnevezéseket (esetenként többet is), illetve ezekhez kapcsolódó forrásokat tartalmaz. Ezek között találhatjuk a következőket:

> *Hírközlés (communication): A hírközlés bármely információ cseréjét vagy átvitelét jelenti véges számú résztvevő között nyilvánosan elérhető elektronikus hírközlési szolgáltatások útján.*
>
> *Elektronikus hírközlő hálózat (electronic communications network): Átviteli rendszerek és – ahol ez értelmezhető – a hálóz-*

zatban jelek irányítására szolgáló berendezések, továbbá más erőforrások, melyek jelek továbbítását teszik lehetővé meghatározott végpontok között vezetéken, rádiós, optikai vagy egyéb elektromágneses úton, beleértve a műholdas hálózatokat, a helyhez kötött és a mobil földfelszíni hálózatokat, az energiaellátó kábelrendszereket, olyan mértékben, amennyiben azt a jelek továbbítására használják, a műsorszórásra használt hálózatokat és a kábeltelevíziós hálózatokat, tekintet nélkül a továbbított információ fajtájára.

Távközlési szolgáltatások (telecommunications service): Olyan szolgáltatások, amelyek nyújtása teljesen vagy részben jelek átviteléből és irányításából áll a távközlő hálózaton keresztül[, kivéve a rádió és televízió műsorszórást].

Távközlő hálózat (telecommunications network): A távközlő hálózatok magukban foglalják az átviteli berendezéseket, ha értelmezhető, a kapcsoló berendezéseket és egyéb erőforrásokat, amelyek lehetővé teszik a jelek átvitelét meghatározott végpontok között fémvezető, fényvezető, rádióhullámok vagy egyéb elektromágneses közeg segítségével.

A fentiekből látható, hogy a távközléshez és hírközléshez kapcsolódóan a magyar köznapi, szakmai és tudományos nyelvben jelző formájában egyaránt találkozhatunk a ***távközlési és távközlő***, illetve ***hírközlési és hírközlő*** kifejezésekkel. E jelzők használata, a felhasználásukkal képzett kifejezések tartalmának elemzése azt mutatja, hogy a változatok érdemi különbséget nem takarnak, önálló értelmezést nem hordoznak, legalábbis ezzel kapcsolatos fogalmi érvekkel nem találkozhatunk. Egyik, vagy másik jelző választása, alkalmazása tehát csak meghatározott szakmai körök tartalmi következményekkel nem járó nyelvhasználatának tekinthető.

Külön megfontolást igényel az a kérdés, hogy az elektronikus hírközlés kifejezésben szakmailag mennyire megfelelő, indokolt az elektronikus jelző használata. Az ehhez kapcsolódó részletesebb vizsgálat egy további publikáció célja lehet, most csak annyit érdemes megjegyezni, hogy az 'elektronika' fogalma és így az 'elektronikus' jelző és az 'elektronikus eszköz' fogalom tartalma nem egyértelműen értelmezett. Leggyakoribb értelmezés szerint az elektronika az elektronok nemfémes vezetőkben, elsősorban félvezetőkben történő áramlásával foglalkozó tudomány és technikaterület. Tágabb értelemben viszont az elektronikus jelző mindazon eszközökkel kapcsolatos lehet, amelyek elektromos, digitális, mágneses, vezeték nélküli, optikai, elektromágneses, vagy hasonló képességekkel rendelkeznek.

Gondolatok, javaslatok, további feladatok

A publikációban foglaltak alapján összességében megállapíthatjuk, hogy a kommunikáció (távközlés, hírközlés, híradás), az informatika (számítástechnika), illetve az információtechnológia más, szélesebb körben elterjedő szakterületei – legalábbis oktatási célokat szolgáló – egységes fogalomrendszerének kialakítása szükségessé teszi a valamennyi szakterületen alkalmazott alapfogalmak meghatározá-

sát, rendszerezését, egységesen elfogadott értelmezésük kialakítását. Ezek közé tartoznak többek között a jelen publikációban röviden tárgyalt eszköz, rendszer és szolgáltatás fogalmak, de ezek részletesebb vizsgálata és más fogalmak (pld. hálózat, infrastruktúra, stb.) egységesen elfogadható tartalmának egyeztetése.

A különböző szakterületek az előzőekben említett alapfogalmak specializált, jelzős kifejezésekkel megnevezhető fogalmait használják, amelyek összhangját biztosítani kell a közös alapfogalmakkal. Ennek során kisebb gondot jelent a speciális rendeltetésű eszközök, rendszerek meghatározása és megnevezése, azonban egyre jelentősebb problémát fog okozni (és okoz máris) a több funkciót megvalósító, különböző – többnyire különböző szakterületekhez is tartozó – típusú szolgáltatásokat nyújtó eszközök, rendszerek osztályozása, megnevezése.

Amennyiben nem akarjuk, hogy új és új eszköz- és rendszertípusok nagy számát kelljen bevezetni, elkerülhetetlen lesz az információs tevékenységeket támogató, információs szolgáltatásokat nyújtó – egyre szorosabban együttműködő, egymáshoz konvergáló, sőt egymással fokozatosan integrálódó – szakterületek együttesének egy közös jelzővel történő megnevezése, amely lehetővé teszi majd az eszközök, rendszerek típus-megjelölését is. Az eddigi tapasztalatok arra utalnak, hogy erre az infokommunikációs jelző alkalmazása várhatóan nem került elfogadásra, megoldást – mint minden más ilyen esetben – a nyelvi alkalmazás, esetünkben a köz- és szaknyelvi alkalmazás fogja kiválasztani.

Az információtovábbítást, információcserét támogató szakterület, a kommunikáció alapfogalmainak áttekintése azt mutatja, hogy ha nem a létező kifejezésekből és azok értelmezéséből, hanem a szükségesnek ítélt fogalom-tartalmakból indulunk ki, akkor még az alapfogalmak rendszerében is kimutathatóak fogalmi problémák (megnevezés hiánya a 'küldemény-alapú' kommunikációra; eltérő, szűkebb értelmezés a távközlés fogalma esetében). Hasonló fogalmi problémát jelent a távközlés, hírközlés, elektronikus hírközlés kifejezések tartalmának gyakorlati azonossága, ami választást igényel. Emellett feladatot jelent a kisebb nyelvtani jellegű eltérések (távközlő, távközlési, hírközlő, hírközlési) értelmezése, kiszűrése is.

A jelen publikációban foglaltak egy sokkal nagyobb kutatási feladat első, apróbb lépéseit jelenthetik, így akár a benne szereplő kérdések többszöröse is megfogalmazható további feladatként. Ezek közül elsőként egy módszertani megközelítés következetes alkalmazását tartom fontosnak, ez pedig az érintett szakterületek fogalmainak tartalmi szempontú felülvizsgálata, ami nem kizárólag a létező fogalmak értelmezésére, hanem például az egyes fogalmak alárendelt fogalmainak (típusainak) osztályozásra épülő meghatározására épül és első lépésben nem is foglalkozik e fogalmak létező, vagy hiányzó megnevezéseivel.

Második legfontosabb feladatnak tartom a különböző szakterületek által közösen, de nem feltétlenül azonos értelemben használt – általánosabb tartalmú – kifejezéseinek, illetve az ezek által jelzett fogalmaknak az összegyűjtését, rendszerezését és egységesen értelmezett tartalmuk meghatározását, illetve a konvergenciából, integrációból fakadó terminológiai kérdések feldolgozását, megoldását.

Végül, mint azt már más alkalmakkor és fórumokon is javasoltam, a kutatási eredményeket egy széles körben (de minimálisan az Informatikai és Hírközlési Intézet tagjai, valamint a védelmi vezetéstechnikai rendszerszervező szak hallgatói; második lépésben a ZMNE oktatói és hallgatói; harmadik lépésben a MH híradó,

informatikai és kapcsolódó szakterületei; végül a teljes nyilvánosság számára hozzáférhető módon) közre kellene adni egy wiki-alapú rendszerben, ami kiválóan alkalmas fogalmak bemutatására, értelmezésére, a köztük fennálló kapcsolatok kiépítésére.

Felhasznált irodalom

[1] AAP-31(A), NATO Glossary of Communication and Information Systems Terms and Definitions. – NATO Standardization Agency, Brussels, 2001.

[2] COM (97) 623, Green Paper on the Convergence of the Telecommunications, Media and Information Technology Sectors, and Implications for Regulation. Towards an Information Society Approach. – Commission of European Communities, 1997.

[3] Sallai Gyula-Abos Imre: A távközlés, információ- és médiatechnológia konvergenciája. – Magyar Tudomány, 2007/7. (844-851.o.)

[4] Haig Zsolt: Az információbiztonság komplex értelmezése. – Hadmérnök különszám (Robothadviselés 6. Tudományos Szakmai Konferencia, 2006. november 22.), 2006.

[5] A Magyar Nyelv Értelmező Szótára. VI. kötet. Sz-Ty. – Akadémiai Kiadó, Budapest, 1966.

[6] The New Oxford Dictionary of English on CD-ROM – Oxford University Press, 1999.

[7] Webster's Encyclopedic Unabridged Dictionary of the English Language. – Gramercy Books, New York/Avenel, 1989.

[8] Magyar Nagylexikon. Tizenhetedik kötet. Szp-Ung. – Magyar Nagylexikon Kiadó, Budapest, 2003.

[9] IEC Electropedia: The World's Online Electrotechnical Vocabulary. - International Electrotechnical Commission, 2009. [www.electropedia.org, 2009.08.19.]

[10] AComp-1(A), NATO Communications Glossary. English and French. – NATO Military Agency for Standardization, 2000. október

[11] AAP-6(2008), NATO Glossary of Terms and Definitions (English and French). – NATO Standardization Agency, 2008

[12] Wikipedia: The Free Encyclopedia. – Wikimedia Foundation Inc. [en.wikipedia.org/wiki/Telecommunication 2009.09.18.]

[13] A Magyar Nyelv Értelmező Szótára. III. kötet. H-Kh. – Akadémiai Kiadó, Budapest, 1965.

[14] 2001. évi XL. törvény a hírközlésről.

[15] 2003. évi C. törvény az elektronikus hírközlésről

[16] Balogh Zsolt György: A készülő egységes hírközlési törvényről. – Jogi Fórum, 2001.[www.jogiforum.hu/publikaciok/17 2009.09.19.]

[17] Jutasi István: Gondolatok az "elektronikus hírközlés" szóhasználatról. – Híradástechnika, 2004(LIX.)/3. (48.o.)

[18] Infokommunikációs Definíció Gyűjtemény. – Nemzeti Hírközlési Hatóság, 2004. [www.nhh.hu/definicio-tar/index.html 2009.09.18.]

RAJNAI Zoltán:

LA CULTURE EUROPÉEENNE MILITAIRE DANS LA FORMATION UNIVERSITAIRE

La Présidence française de l'Union européenne s'est particulièrement attachée à développer l'action commune des Européens dans le domaine de la gestion de crises. De nombreuses opérations militaires et civilo-militaires ont notamment été menées sous son impulsion. La PESD commence ainsi à faire un usage croissant de ses potentialités et à s'organiser pour être en mesure de répondre concrètement aux besoins de sécurité communs. On connaît surtout la série d'initiatives prises au profit des investissements militaires et de l'harmonisation des systèmes militaires. Force est de constater que la formation professionnelle des personnes appelées à gérer ce processus a dans le même temps été quelque peu négligée. Cette question a néanmoins été remise à l'ordre du jour, à travers l'initiative européenne pour les échanges de jeunes officiers, inspirée du programme Erasmus, discutée par les ministres de la défense des pays membres de l'Union européenne à Deauville en octobre 2008 puis adoptée officiellement en novembre 2008 par le Conseil de l'Union européenne. Il s'agit d'ouvrir les frontières du savoir et, en l'espèce, de permettre aux jeunes officiers européens, dès leurs premières années d'études, d'acquérir une compréhension supranationale des questions de sécurité et de défense et de développer une attitude commune à cet égard.

Il est clair que tous les pays doivent s'employer à réformer leur outil de défense. L'initiative a tout d'abord été présentée et discutée lors du Sommet informel des Ministres de la défense de l'Union européenne à Deauville, les 1er et 2 octobre 2008. Ces derniers ont constaté que les échanges et contacts entre officiers européens étaient insuffisants. Ils ont donc décidé de traiter la question en

amont, c'est-à-dire au stade de la formation initiale des officiers. A cette occasion, les Etats membres de l'Union européenne ont fait état d'offres de formations croisées. La République tchèque a par exemple annoncé que son université de défense militaire adhérerait au programme Erasmus dès 2010; les Portugais ont indiqué qu'ils souhaitaient s'engager dans la formation linguistique commune ; la Hongrie, la Slovaquie, la Grèce ont également fait part de leur intention d'inscrire leur université de défense ou académie supérieure militaire ou leur enseignement dans le cadre de ces échanges.

Progressivement, l'idée s'est imposée de s'inspirer dans la mesure du possible des enseignements tirés du programme Erasmus et des potentialités qu'il offre.

La plupart des écoles et des académies militaires se sont déjà intégrées au processus de Bologne pour faciliter la reconnaissance de leur milieu propre.

Dans l'étude élaborée par le Secrétariat général du conseil de l'Union européenne, la formation initiale est définie comme suit: La formation initiale des officiers commence après le recrutement. Elle comprend la formation professionnelle et la formation supérieure jusqu'au mastère inclus (si celui-ci fait partie de la formation initiale) Elle comprend des sous-catégories : la formation académique, la formation militaire de base et la formation professionnelle dispensée dans d'autres écoles ou instituts militaires.

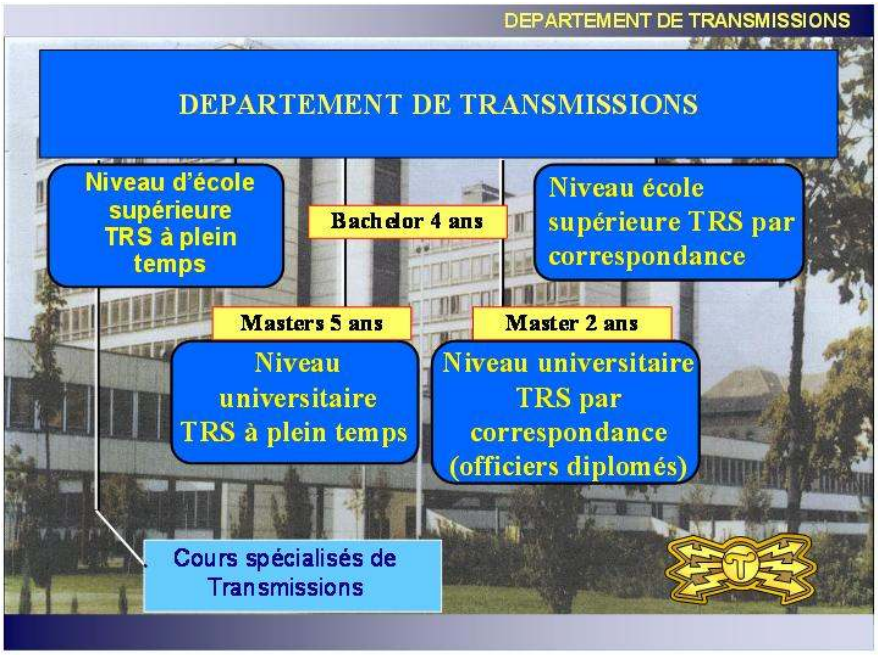
L'étude constate qu'un grand nombre de ces établissements de formation ont déjà mis en place des systèmes d'échange dans un cadre multilatéral.

La proportion de jeunes officiers ou de personnels enseignants aujourd'hui concernés par les différents programmes d'échanges existants, bilatéraux ou multilatéraux, y compris le programme Erasmus, demeure limitée.

Un certain nombre de difficultés permettent d'expliquer cette insuffisance. Par exemple, la durée des cursus, l'organisation des programmes et la nature même de la formation initiale (activités académiques ou d'entraînement) des officiers diffèrent souvent de manière significative entre les Etats membres, même si le processus de Bologne contribue à atténuer ces différences. On peut également citer le problème du coût de certains échanges ou les difficultés linguistiques.

La capacité des forces armées européennes à travailler ensemble est en effet devenue déterminante pour préparer et conduire des opérations militaires multinationales de plus en plus complexes. Elle implique une coopération accrue entre Etats membres pour la formation des officiers.

L'initiative européenne pour les échanges de jeunes officiers offrira la possibilité aux officiers européens, dès le stade de la formation initiale, de suivre une partie de leur formation dans un autre Etat membre. Elle favorisera ainsi la mobilité des étudiants et des enseignants des écoles militaires et elle favorisera des approches partagées pour la formation des jeunes officiers européens, notamment dans le domaine de la PESD. Les Etats membres ont donc agréé un ensemble de mesures concrètes pour encourager et faciliter les échanges entre leurs institutions nationales de formation, en s'appuyant sur le Collège européen de sécurité et de défense. Ces mesures seront mises en oeuvre à la fois à l'échelon européen et à l'échelon national. Elles s'appuieront sur les échanges bilatéraux et multilatéraux existants.



De manière générale, l'impulsion politique donnée doit contribuer à aider les académies militaires à s'adapter à l'espace européen de l'enseignement supérieur annoncé par le processus de Bologne, et à faciliter leur adhésion à la Charte Erasmus. Elle devrait inciter à faire converger les contenus des formations initiales, notamment en favorisant les échanges d'expériences et de meilleures pratiques. Elle fournit une occasion unique de réaliser un réseau de collaboration entre les différentes institutions de formation initiale des officiers.

La Présidence française a veillé par ailleurs à faire connaître l'initiative inspirée d'Erasmus en y consacrant deux séminaires. Le 13 et 14 novembre à l'Ecole militaire de Paris, il s'agissait d'identifier les offres et les demandes de formation initiale et croisée des officiers et d'établir une cotation harmonisée des modules de formation offerts. Le 16 décembre, une réflexion sur la portée concrète de l'initiative s'est tenue à l'école militaire française de Saint-Cyr Coëtquidan, accueillant la participation d'élèves de toutes les académies militaires européennes. Saint-Cyr est réputée notamment pour les visites qu'elle organise dans chaque filière et à tout niveau d'études, ainsi que pour son semestre international qui oblige tous les étudiants à partir se former à l'étranger en vue de la rédaction d'un mémoire de mastère.

RAJNAI Zoltán - KORONCZAI Tibor

ELEKTRONIKUS ALÁÍRÁS HITELESÍTÉS

A kommunikáció meghatározó tényezője az emberi civilizáció kialakulásának. Az emberek népesedésével, terjeszkedésével a kommunikációs távolságok is megnövekedtek. Az évszázadok során az üzenetek továbbításának a módja nagyon megváltozott, de a követelmény, hogy az üzenet tartalmát illetéktelenek ne ismerjék meg, valamint a feladó és a címzett azonos legyen a vélt személyekkel változatlanok maradtak Az elmúlt századokban az aláírónak és a dokumentumnak az összekapcsolódása a papír segítségével valósult meg. Az elektronikus kommunikáció elterjedése felgyorsítja az üzenetek továbbítását. Az elektronikus üzenet váltásának számtalan előnye van, ezért manapság már nem lehet lemondani róluk. A napjainkban globálissá vált informatikai rendszerben az üzenetek közös csatornán haladnak, nagymértékben megkönnyítve az illetéktelenül beavatkozni szándékozók dolgát. Az információs társadalom, az Internet, az elektronikus kereskedelem fogalmai már nem a távoli jövőt, a várható lehetőségeket, hanem a mindennapi valóságot jelentik.

A hitelesítés és a titkosítás hagyományos eszközei ebben a világban nem alkalmazhatóak, tehát új eljárásokra van szükség. Egy személyt nem csak a kézjegye alapján azonosíthatunk, hanem az ujjlenyomata vagy a szivárványhártyája rajzolta alapján is. Digitális környezetben ezek a jellemzők önmagukban használhatatlanok, hiszen elektronikus eszközökkel tökéletesen reprodukálhatók. Saját személyünk azonosítására egy olyan formát kell választanunk, amely megőrzi egyediségünket, használható hitelesítésre vagy titkosított adatok megfejtésére, de ezt mégsem kell kiadnunk kezünkből. Ez a technológia az elektronikus aláírás. Az elektronikus aláírás a kétkulcsos titkosítás alkalmazására épül, ezért használata elképzelhetetlen a támogató nyilvános kulcsú infrastruktúra (PKI)11 megfelelő fejlettsége nélkül, azaz a digitális aláírás szolgáltatás lényegében a PKI szolgáltatás.

A PKI szolgáltatásai az azonosítás, a titkosítás és a digitális aláírások kulcs menedzsmentjei általános eszközeikké válnak az Internet/ Intranet alkalmazásoknak, beleértve a biztonságos üzenetkezelést és az elektronikus kereskedelmet.

A nyilvános kulcsú eljárás jellemzői

A privát hálózatok és az Intranet alkalmazások alapelve a nyilvános kulcsú infrastruktúra. A PKI az Internet (TCP/IP) technológiát alkalmazó hálózat biztonságosságának feltételeit nyújtja, evvel lehetőséget teremtve a biztonságos szolgáltatásnak. A szolgáltatásokhoz a titkosító kódolás és a digitális aláírás alkalmazásával biztosítható, a szigorú felhasználói azonosítás, az adatok védelme, a teljesség, valamint a letagadhatatlanság.

A PKI lényegében meghatározott biztonsági szolgáltatások köre, amely lehetővé teszi a nyilvános vagy másképpen a kétkulcsos, aszimmetrikus titkosítás, és az

[11] PKI / Public Key Infrastructure / Nyilvános kulcsú infrastruktúra

X.509-es ITU-T ajánlás szerint ISO/IEC 9594-8 szabványos tanúsítványok használatát

A PKI alapszolgáltatása a nyilvános kulcsok biztosítása, ennek ellenére a nyilvános kulcsokat a kulcskibocsátó digitális tanúsítványba csomagolja. A digitális tanúsítvány védi a nyilvános kulcs sértetlenségét, és emellett hitelesítési lehetőséget biztosít. A nyilvános kulcs hitelességét a kulcskibocsátó, a tanúsító hatóság (CA) 12 a saját privát kulcsával képzett digitális aláírásával a tanúsítványon.

A PKI estében egyidejűleg minden felhasználónak legalább két kulcspárral kell rendelkeznie. Kell egy kulcspár a titkosításra és a megfejtésre, egy másik pedig a digitális aláírásra és ellenőrzésre. A nyilvános kulcsú titkosítás szépsége abban rejlik, hogy széleskörűen hozzáférhetővé teszi a bizalmas hiteles információkat. Az emberek és a rendszerek nyilvános kulcsait nyílt nem hiteles környezetben tárolják, csupán a kulcs privát felét kell szigorúan őrizni.

A PKI nyújtja azt a technológiát, infrastruktúrát és eljárást, amely lehetővé teszi a digitális aláírások és vagy a nyilvános kulcsú titkosítás használatát. A PKI fő funkciója az elektronikus iratok, vagy más elektronikus adat átvitel titkosításra, szignálásra, aláírásra vagy az információs forrásokhoz való hozzáférés engedélyezésére való jog.

A nyilvános kulcsú eljárás architektúra elemei

A nyilvános kulcsú infrastruktúra architektúrájának elemei a digitális tanúsítványok létrehozását, ellenőrzését, továbbítását és használatát biztosítják.

A tanúsítvány alanya és használója

A legalapvetőbb PKI architektúra elem a tanúsítvány alanya, amely egy személy. Bármely jogi személynek - cég, rendszer - lehet nyilvános kulcsa. A jól felépített PKI architektúra a következő elemeket tartalmazza:

Tanúsító hatóság (CA)

A nyilvános kulcsú titkosítás abban az esetben használható, ha a felhasználókat biztosítani tudjuk, hogy a kapcsolatuk biztonságos, azaz a felek azonossága és kulcsai érvényesek és hitelt érdemlőek. Ez a bizonyosság megköveteli, hogy a PKI minden felhasználója regisztrált azonosítóval rendelkezzen. Ezek az azonosítók a digitális formában tárolt nyilvános kulcsú tanúsítványok. A tanúsító hatóság a felhasználó számára tanúsítványokat bocsát ki, amelyben egy sor adatot saját privát kulcsú digitális aláírásával tanúsít. Ezek között hiteles információt nyújt a következőkről:

A felhasználó megkülönböztető nevéről (DN)13, amely tartalmazza a nevet és kiegészítő attribútumot, amely segítségével a felhasználó azonosítható. A felhasználó nyilvános kulcsa melynek segítségével kódolhatók az előfizetőknek szánt üzenetek, illetve ellenőrizhető az elektronikus (digitális) aláírás és az üzenet teljessége. A tanúsítvány érvényességének tartalma (pl. a kibocsátás és a lejárat napja).

[12] CA / Certificate Authority / Tanúsító hatóság

[13] DN / Distinguished Name / Megkülönböztető név

Regisztrációs hatóságok (RA)

Az RA önállósága lehetséges változat, jobbára a CA egy alárendelt szerveréről van szó, amelyre a CA a felhasználók regisztrációjával kapcsolatos menedzselési funkciókat alkotja.

PKI adattárak (repository)

Alapesetben legalább két fontos adattárat alkalmaz a PKI architektúra. A tanúsítványokat és visszavonási listákat egy nyilvános, könnyen elérhető adatbázisban kell tárolni, és elosztásukat biztosítani. Általában relációs adatbázisokat használnak, bár a PKI adattárakban a leglogikusabb megoldás, mégis a LDAP14 alapú név/címtár szolgáltatás.

Név/címtár (directory) integráció

Ez igen lényeges a PKI működése szempontjából. A legtöbb szállító PKI terméke LDAP alapú kapcsolatot használ, nemcsak a tanúsítványok, de a CA-k és más PKI elemek számára is lényeges a címtár adatok előállítása.

Visszavonási listák (CRL)

A hitelességüket elvesztett tanúsítványokat a CA köteles visszavonni, erre a lejárati idő előtt számtalan ok szolgálhat, (pl. a tanúsítványnak a megfelelő nyílt kulcshoz tartozó valamelyik privát kulcsot kompromittálják).

Tanúsítvány kibocsátó pontok

A CA a második típusú adattárból (név/címtár) biztosítja a tanúsítványok és a visszavonási listák szervezeten belüli és kívüli elérhetőségét. A jó tanúsító hatóság a kibocsátó pontok replikációjával megteremti a felhasználók számára a hierarchiába tartozó valamennyi tanúsítvány automatikus letölthetőségét.

Kulcs és tanúsítványmenedzselési eszközök

A menedzselési eszközök biztosítják a kiadott tanúsítványok különböző adatainak kötelező nyilvántartását. A lejárt vagy visszavont kulcsokat tartalmazó tanúsítványokat archiválni kell. A tanúsítványok a hozzájuk tartozó kulcsok archiválását, megújítását, a biztonsági másolat és a visszaállíthatóság segíti.

A kulcs és tanúsítvány menedzselés területei:

- Kulcsok visszaállíthatóságának visszaállíthatósága
- Letagadhatatlanság biztosítása
- Kulcsok és tanúsítványok frissítése
- Kereszttanúsítás

A tanúsítvány érvényességének lejáratakor a megújításhoz a CA felhasználja a kérelmező meglévő, már ellenőrzött adatait vagy új nyilvános kulcs generálását. A PKI archív adattár másik lehetősége a kulcs pár visszaállíthatóságának a biztosítása, amely csak szigorúan ellenőrzötten, a tulajdonos beleegyezésével történhet. A kétkulcsos titkosítást, digitális aláírást alkalmazó személyek, szervezetek jogos igénye, hogy titkosított adatot akkor is megfejthessék ha elvesztették a privát kulcsukat. Ez azt jelenti, hogy az adott vállalat, amelyhez a felhasználó tartozik, megköveteli a kulcsok biztonsági másolatát, annak a tárolását és helyreállíthatóságát.

[14] LDAP / Lightweight Directory Acces Protocol /

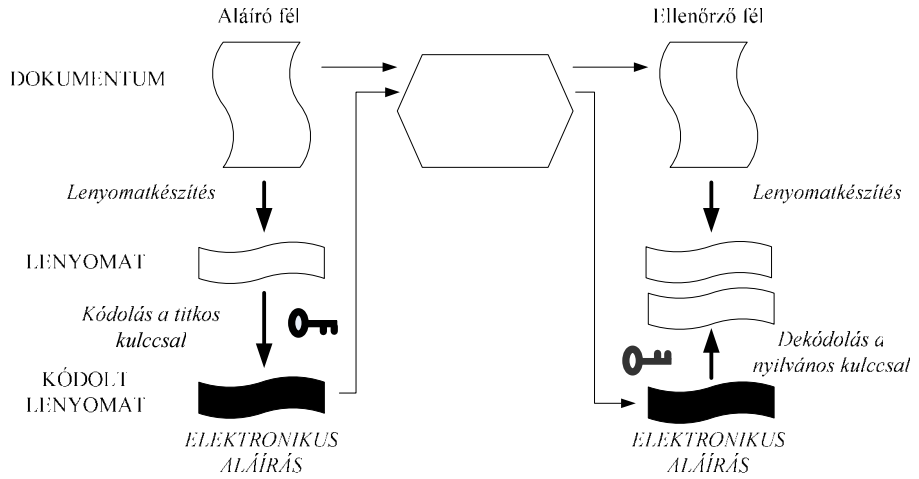
Nyilvános kulcsú eljárással létrehozott elektronikus aláírás

Az általánosan megfogalmazott elvárások, követelmények szempontjából a jelenleg ismert és használt technikai megoldások közül a nyilvános kulcsú eljárás során két kulcsot, (kriptográfiai nyilvános kulcs, és az aláírás-létrehozó adat) kell használni. Az aláíró kulcs segítségével elhelyezett elektronikus aláírás bonyolult matematikai és kriptográfiai megoldások, műveletek összessége. Mindkét kulcs digitális jelek sorozatának fogható fel, amelyeket sajátos programokkal kell kezelni. A titkos kulccsal az aláíró képes az elektronikus iraton egy kizárólag rá jellemző aláírást létrehozni, illetve az adatokat titkosítani. A titkos kulcshoz tartozó nyilvános kulcs segítségével a címzett ellenőrizheti az elhelyezett elektronikus aláírást, sőt képes a titkos kulcs tulajdonosának az adatokat küldeni. A titkosításhoz és annak feloldásához eltérő aszimmetrikus algoritmust használnak, melynek lényege hogy lehetetlen a titkosított üzenetet ugyanazzal a kulccsal megfejteni és fordítva.

Nyilvános kulcsú elektronikus aláírás alapvető tulajdonságai

Az adott elektronikus aláírás kizárólag egy aláíró személyhez kapcsolódik. Az aláírás ténye kétséget kizáróan bizonyítható, azaz az üzenet küldője utólag nem hivatkozhat arra, hogy azt nem írta alá. Valamint kimutatja, ha az adott dokumentum az aláírást követően megváltozott, bizonyos feltételek mellett pedig az aláírás időpontja is hitelesen rögzíthető.

Az üzenetek titkosítása és dekódolása két különböző kód segítségével történik. A nyilvános kulcs alapján, abból gyakorlatilag lehetetlen a titkos kulcsot megfejteni, így nincs lehetőség az elektronikus aláírás hamisítására sem. A nyilvános kulcs birtokában megállapítható, hogy a vizsgált aláírás a hozzá tartózó titkos kulcs segítségével készült-e vagy sem.



Az elektronikus aláírás készítése és ellenőrzése

Az elektronikus aláíráshoz használatos kulcsok az aláíró személyétől fizikailag elkülönülhetetlen file-okban, floppyk esetleg chipkártyák formájában jelennek meg. A nyilvános kulcs bárki által megismerhető, ezáltal határozható meg a kulcs tulajdonosának személyazonossága. A titkos kulcsot titokban kell tartani. Ha, a

titkos kulcsot tartalmazó adathordozót a tulajdonosa elveszti, gondoskodni kell egy újabb titkos kulcs és a hozzátartozó nyilvános kulcs beszerzéséről.

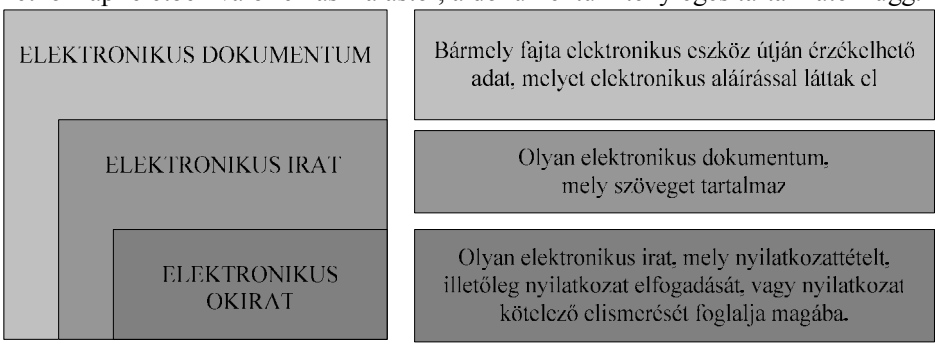
A címzett a dokumentum alapján egy szoftver segítségével újra elkészíti annak digitális lenyomatát. Ezt követően a digitális aláírást a nyilvános kulcs segítségével dekódolja. A dekódolás folytán megkapja az aláíró által készített digitális lenyomatot. Amennyiben a két digitális lenyomat azonos, a dokumentum az aláírása óta nem változott. Ha címzett által használt nyilvános kulcshoz tartozó titkos kulccsal készült az elektronikus aláírás, akkor az aláíró azonosítható. Az elektronikus aláírás használata a gyakorlatban könnyen megtanulható módszer.

Az elektronikus dokumentum fajtái

Az elektronikus aláírás arra alkalmas, hogy elvileg bármilyen fajta számítástechnikai úton létre jött adatot (dokumentumot) aláírjanak vele, vagyis nem csak írott szövegeket, de digitális hangfelvételeket, képeket vagy akár szoftvereket is. Az elektronikus dokumentum ennek megfelelően többféle lehet:

- Elektronikus dokumentum
- Elektronikus irat
- Elektronikus okirat

Az elektronikus dokumentum fogalma magában foglalja az elektronikus iratot és okiratot, az elektronikus irat pedig az elektronikus okiratot. Az elektronikus dokumentum fajtája részben a joghatástól - a hitelesítés módjától részben pedig a hétköznapi életben való felhasználástól, a dokumentum tényleges tartalmától függ.



Elektronikus dokumentum

Az elektronikus dokumentum, olyan elektronikus eszköz útján értelmezhető adat, mely elektronikus aláírással van ellátva. Ez lehet szöveg kép, hangfelvétel, szoftvertervrajz, digitális fénykép, film stb. A dokumentum fogalmába bármely fajta elektronikus eszköz útján érzékelhető adatot értjük feltéve, hogy ezt valamilyen - különböző hitelességű - elektronikus aláírással láttak el. Amennyiben a dokumentumnál alkalmazott aláírás fokozott biztonságú vagy minősített lesz, úgy a hétköznapi életben az elektronikus dokumentumot főleg szerződések teljesítésénél fogják használni, míg a katonai alkalmazásban főleg a nyilvántartott, vagy fontos dokumentumok továbbítására. A lényeg minden esetben az, hogy sokféle fájltípustól és tartalomtól függetlenül megállapítható lesz, hogy ki teljesítette és milyen

minőségben és az időbélyegző használatával még a teljesítés ideje is ellenőrizhető lesz, aminek a késedelmes teljesítés estén lehet jelentősége.

Elektronikus irat

Az elektronikus iratok az elektronikus dokumentumoknak egy olyan csoportját alkotják, amelynek alapvető funkciója, hogy betűkkel szöveget közöljenek.

Az elektronikus irat szöveget tartalmaz, bár illusztrálásra, hatósági azonosításra egyéb adatok képek, információk is szerepelhetnek benne. Az elektronikus irat jog általi elismerésének minimális követelménye, hogy a benne foglalt információk hozzáférhetők és későbbi hivatkozásra is alkalmasak legyenek. Ki kell emelni, hogy az elektronikus aláírás és irat alkalmazását, az egyes minisztériumok és önálló hatáskörű szervek saját hatáskörükben döntik el, hogy az egyes szakterületeken milyen ütemezésben kívánják bevezetni.

A kormányzaton belül hiteles elektronikus dokumentumok cseréjéhez, további elemzést igényel az elektronikus iratok levéltári archiválása, az állami és szolgálati titkot képező információk elektronikus irat formájában történő kezelése.

Elektronikus okirat

Az elektronikus okirat, olyan elektronikus irat, amely a nyilatkozattételt, nyilatkozattétel elfogadását vagy nyilatkozat kötelezőnek elismerését foglalja magában. Az elektronikus okirat, az okirati bizonyítási eszközök virtuális megfelelője, azzal hogy a nyilatkozat mellett a megfelelő technikai védelem is egy lényeges eleme.

A gyakorlatban ezt a dokumentumfajtát használják a szerződések megkötésénél, illetve a különféle egyéb jognyilatkozatok megtételénél. Fontos, hogy bizonyos jognyilatkozatoknál továbbra is kizárt lesz az elektronikus forma. Speciális megközelítést igényel az elektronikus aláírás szabályozása az állami közszféra területén. E körbe tartozó szervezetek államhatalmi, bírói, ügyészi, központi és helyi közigazgatási szervek, rendészeti és rendvédelmi szervek, önkormányzatok - piaci szereplők, vonatkozásában is érvényesíteni kell az elektronikus aláírásra és iratra vonatkozó általános eljárásokat és elveket.

Hangsúlyozni kell, hogy az egyszerű elektronikus dokumentumok tárgyi bizonyítási eszköznek, az elektronikus okirat pedig okiratnak minősül. Az utóbbinak erősebb bizonyítási eszközei lesznek.

Az elektronikus aláírás fajtái

Az elektronikus aláírás, melynek 3 fő fajtáját különbözteti meg a törvény, részben bizonyító erővel részben pedig a mindennapi funkció használata szerint:

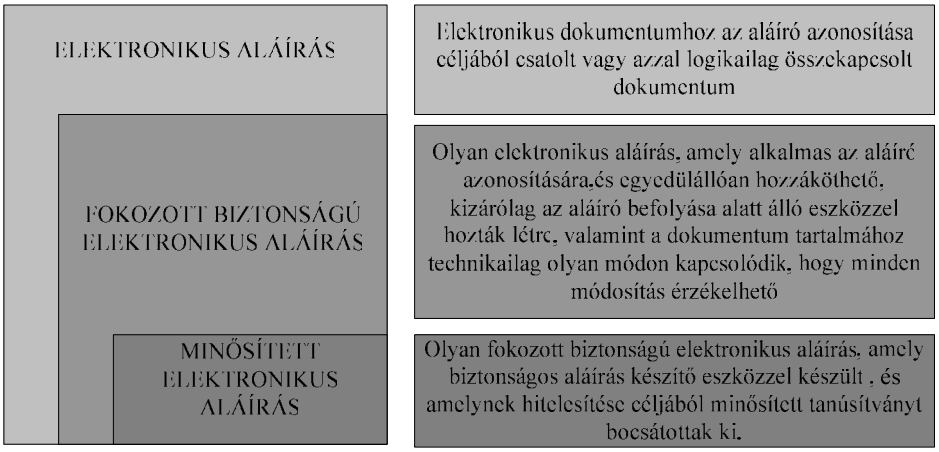
- Elektronikus aláírás
- Fokozott biztonságú elektronikus aláírás
- Minősített elektronikus aláírás.

Elektronikus aláírás (ES)[15]

Az elektronikus aláírás az elektronikus dokumentumhoz azonosítás céljából végérvényesen hozzárendelt, vagy azzal logikailag összekapcsolt elektronikus adat, dokumentum. Ilyen lehet, pl. az elektronikus levél végére írt név, illetve az is, ha a

[15] ES / Electronic Signature / Elektronikus aláírás

saját kézzel írt aláírást elektronikus képként a levélhez csatoljuk. Elektronikus formában tárolt adat, amely hozzá van kapcsolva, vagy logikailag hozzá van rendelve más elektronikus adathoz, amely így egy azonosítási eljárást alkot. Ennek az eljárásnak nem sok bizonyító ereje van. Ezen belül azok az aláírások is beletartoznak, amelyek csak alacsony színvonalon alkalmasak az aláíró személyének hitelesítésére, azonosítására illetve arra, hogy bizonyíthatóvá tegyék, az aláírt szöveg megváltozott-e az aláírás óta.



Fokozott biztonságú elektronikus aláírás

A fokozott biztonságú elektronikus aláírás olyan aláírás, amely alkalmas az aláíró azonosítására és egyedülállóan hozzá köthető. Olyan eszközökkel hozzák létre, mely kizárólag az aláíró befolyása alatt áll. A fokozott biztonságú elektronikus aláírás a dokumentum tartalmához kapcsolódik, hogy minden, az aláírás elhelyezését követően az iraton, illetve dokumentumon tett módosítás érzékelhető. A nyilvános kulcsú eljárással létrehozott aláírás megfelel a fokozott biztonságú elektronikus aláírással szemben támasztott követelményeknek. A fokozott biztonságú elektronikus aláírást is, a minősített elektronikus aláíráshoz hasonlóan a hitelesítés-szolgáltató tanúsítja, de az alkalmazott technológia, ennek biztonsági foka, vagy a hitelesítés- szolgáltató körülményei miatt a bizonyító ereje alacsonyabb. A biztonságos aláírás létrehozó eszközök nem változtathatják meg az aláírásra szánt adatot, és nem akadályozhatják meg az ilyen adat aláírójának történő megmutatását, az aláírási folyamatot megelőzően.

Minősített elektronikus aláírás

A minősített elektronikus aláírás olyan, nyilvános kulcsú eljárással készült fokozott biztonságú elektronikus aláírás, amelyet biztonságos aláírás-létrehozó eszközzel hoztak létre, és amelynek a hitelességét minősített tanúsítvány igazolja. A biztonságos aláírás-létrehozó eszközökkel és a tanúsítványt kibocsátó hitelesítési szolgáltatóval szembeni követelményeket külön jogszabály határozza majd meg. Az elektronikus okirat minősített aláírással történő ellátása a bizonyító erő szempontjából jut jogi jelentőséghez. A minősített elektronikus aláírás jogi szempontból

a teljes bizonyító erejű magánokirattal egyenértékű bizonyító eszköz. Akkor jön létre, ha a fél az iratot az elejétől a végéig saját kezűleg írja és aláírja, tanúkkal hitelesíti, vagy ügyvéddel ellen jegyzi.

Szolgáltatások

Az elektronikus aláírással kapcsolatos szolgáltatások köre:

- Hitelesítés szolgáltató
- Időbélyegző szolgáltatás
- Aláírás-létrehozó eszközön aláírás-létrehozó

Hitelesítés szolgáltatás

A hitelesítés szolgáltatás lényege abban rejlik, hogy a szolgáltató a nyilvános kulcs alapján megadja az aláíró adatait, tanúsítja a két kulcs összetartozását és érvényességét. A hitelesítés szolgáltató a fenti adatokról tanúsítványt bocsát ki, nyilvántartást vezet, fogadja a tanúsítvánnyal kapcsolatos változások adatait, nyilvánosságra hozza a tanúsítványhoz tartozó szabályzatokat, az aláírás ellenőrző adatokat (nyilvános kulcsok) és a tanúsítvány aktuális állapotára (különösen a visszavonásra) vonatkozó információkat. A hitelesítési szolgáltatás is lehet garanciális jellegű minősített elektronikus aláírás hitelesítési szolgáltatás.

A hitelesítés szolgáltató szerepe

Távollevők közötti kommunikáció esetén a címzett nem tud meggyőződni arról, hogy a nyilvános kulcshoz tartozó magánkulcs a feladó kizárólagos birtokában van-e vagy sem. Az aszimmetrikus kódolás önmagában nem jelent teljes megoldást a távollevők közötti kommunikáció esetén az azonosítási problémára. A jelzett probléma megoldásához szükség van egy megbízható harmadik fél bevonására is. A megbízható harmadik fél, a hitelesítés szolgáltató, akinek feladata kettős. Egyfelől meg kell győződnie arról, hogy a nyilvános kulcshoz tartozó magánkulcs a feladó birtokában van, és erről egy tanúsítványt kell a feladó rendelkezésére bocsátania. Másfelől pedig nyilvántartást kell vezetnie, publikálnia kell az általa kibocsátott tanúsítványokról és azok aktuális állapotáról (érvényességéről, érvényesség megszűnéséről és annak okáról, időpontjáról, stb.).

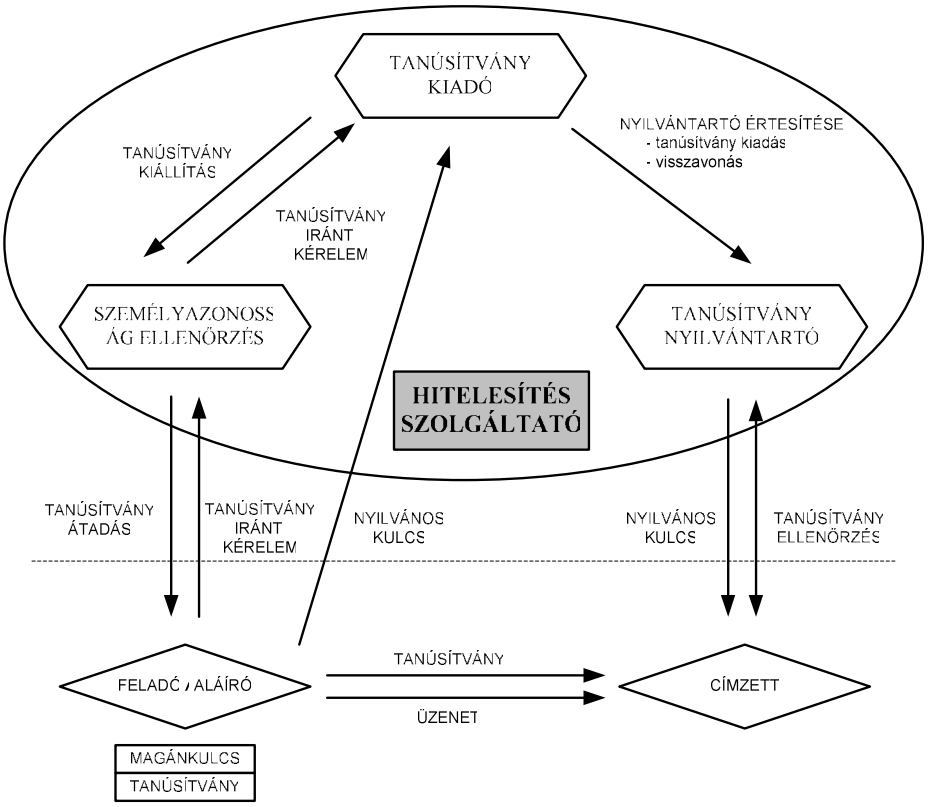
A hitelesítés szolgáltató által kibocsátott tanúsítványt, annak kibocsátásától kezdve, a feladó csatolhatja az általa küldött, és a magánkulcs segítségével titkosított üzenetekhez. A címzett ellenőrizni tudja a tanúsítvány érvényességét, és megbizonyosodhat arról, hogy a tanúsítványt még nem vonták vissza.

Tanúsítvány

A hitelesítés szolgáltató által kibocsátott tanúsítvány a kriptográfiai nyilvános kulcs és a kulcsot használó, azaz a dokumentumot aláíró személy azonos adatinak az összetartozását, illetve a két kulcs érvényességét igazolja. A tanúsítvány alapján győződhetünk meg arról, hogy az aláírás magától az aláírótól származik. A hitelesítési szolgáltató által kibocsátott tanúsítványt, a dokumentum aláírója csatolja a (saját titkos kulcsával) titkosított és aláírt üzenethez. Az aláíró aláírása a saját nyilvános kulccsal, a tanúsítványon szereplő aláírás pedig a hitelesítési szolgáltató nyilvános kulcsával ellenőrizhető.

Minősített tanúsítvány

Minősített tanúsítványt kizárólag minősített szolgáltatók bocsáthatnak ki. A minősített elektronikus aláírás olyan nyilvános kulcsú eljárással készült fokozott biztonságú elektronikus aláírás, amelyet biztonságos aláírás létrehozó eszközzel hoztak létre, és a hitelességét minősített tanúsítvány igazolja. Minősített tanúsítvány hiányában nem lehet minősített elektronikus aláírást létrehozni. A minősített hitelesítés szolgáltatónak lehetősége van alacsonyabb biztonsági fokú, nem minősített tanúsítvány kibocsátására, továbbá arra is, hogy különböző feltételekkel (pl. felelősségvállalás mértéke) állítson ki tanúsítványokat (tanúsítvány típusokat).



A minősített tanúsítványnak tartalmaznia kell:

- annak megjelölését, hogy a tanúsítvány minősített tanúsítvány, a hitelesítés-szolgáltató és székhelyének (ország) azonosítóját, az aláíró nevét, vagy egy álnevet, ennek jelzésével,
- az aláírónak külön jogszabályban a szolgáltatási szabályzatban, illetőleg az általános szerződési feltételekben meghatározott speciális jellemzőit, a tanúsítvány szándékolt felhasználástól függően,
- az aláírás-ellenőrző adatot (nyilvános kulcsot), amely az aláíró által birtokolt aláírást készítő adatnak (magánkulcs) felel meg,

- a tanúsítvány érvényességi idejének kezdetét és végét, a tanúsítvány azonosító kódját
- az adott minősített tanúsítványt kibocsátó hitelesítés szolgáltató fokozott biztonságú elektronikus aláírást,
- a tanúsítvány használhatósági körére vonatkozó estleges korlátozásokat, a tanúsítvány felhasználásának korlátait,
- más személy (szervezet) képviseletére jogosító elektronikus aláírás tanúsítványa estén a tanúsítvány e minőségét és a képviselt személy (szervezet) adatait.

A minősített kiadványokat kiadó hitelesítés szolgáltatókkal kapcsolatos követelmények:

A hitelesítés-szolgáltatók kötelességei:

- a szolgáltatás nyújtáshoz szükséges megbízhatóságának biztosítása,
- gyors és biztonságos címtár szolgáltatás működésének biztosítása, és biztonságos és azonnal rendelkezésre álló visszavonás címtár szolgáltatás működésének biztosítása,
- annak biztosítása, hogy a tanúsítvány kiadásának vagy visszavonásának dátuma és időpontja pontosan meghatározható legyen,
- megfelelő eszközökkel köteles ellenőrizni annak a személynek az azonosságát, és specifikus jellemzőit, aki részére a minősített tanúsítványt kiállítja,
- olyan alkalmazottak foglalkoztatása, akik megfelelő szakértelemmel, gyakorlattal és a szolgáltatással kapcsolatos végzettséggel rendelkeznek,
- megbízható rendszerek és elektronikus aláírás termékek használata, amelyek megfelelő védettséggel rendelkeznek módosítás ellen, és amelyek biztosítják a technikai és kriptográfia biztonságot az eljárások során,
- intézkedéseket kell tenni a tanúsítványok hamisítása ellen, és abban az esetben, amikor a hitelesítés-szolgáltató készíti a magánkulcsot biztosítani kell a folyamat bizalmasságát,
- megfelelő pénzügyi források biztosítása a törvényben lefektetett követelmények teljesítése érdekében, különösen tekintve a kár okozási felelősség kockázatának elviselésére, pl. megfelelő biztosítások alkalmazásával,
- az összes lényeges, a minősített tanúsítványokkal kapcsolatos információ tárolása megfelelő időtartamra, különös tekintettel arra, hogy a tanúsítványok jogi eljárásokban bizonyítékként szerelhetnek. Ez az információ tárolás történhet elektronikusan is, a hitelesítés-szolgáltató kulcs kezelési szolgáltatását igénybe vevő személy aláírás-létrehozó adatait nem tárolhatja, és nem másolhatja a szolgáltató,
- a szolgáltatást igénybe venni kívánó személyt még a szerződéses kapcsolat létrejötte előtt megfelelő módon tájékoztatni kell a szolgáltatás igénybevételének pontos feltételeiről és kikötéseiről, beleértve a használat korlátozásait, az önkéntes minősítést, reklamációs eljárásokat, a vitás kérdések elintézésének módjait. Ezt az információt írásban akár elektronikus formában érthető nyelvezettel kell megadni.

- Lényeges részeit ennek az információnak kérésre elérhetővé kell tenni a kibocsátott tanúsítványban bízó harmadik fél számára is, megbízható rendszerekben kell tárolni a tanúsítványokat, olyan ellenőrizhető módon, hogy csak feljogosított személyek készíthetnek új bejegyzéseket és végezhetnek módosításokat az információ hitelessége ellenőrizhető legyen a tanúsítványok nyilvánosságra hozatala csak a tulajdonos hozzájárulásával történhet, és bármilyen technikai változás, amely ezen biztonsági követelményeket veszélyezteti nyilvánvaló kell legyen a kezelő számára.

Az elektronikus aláírást létrehozó adat kiadása előtt a szolgáltató ellenőrzi a leendő aláíró személyazonosságát, esetleg jogosultságát (pl. cégbejegyzés esetében), ehhez adatokat kérhet más szervektől is. A tanúsítvány kibocsátásával garanciát vállal a szolgáltató. Minősített okiratot csak olyan személy adhat ki, aki kötelező felelősség biztosítással rendelkezik. A minősített hitelesítés szolgáltató a törvény, rendelkezése folytán jogosult nem minősített tanúsítványt kibocsátani.

Időbélyegző

Az elektronikus dokumentumhoz kapcsolt időbélyegző elhelyezésével a szolgáltató tanúsítja a dokumentum tartalmát az adott időpontban. Az időbélyegzés tulajdonképpen elektronikus aláírás, amely lehet egyszerű időbélyegzés, illetve magasabb szintű időbélyegzés is.

Aláírás-létrehozó eszközön aláírás-létrehozó adat elhelyezése

Az aláírás-létrehozó eszközön aláírás-létrehozó adat elhelyezése tulajdonképpen magát az elektronikus aláírást jelenti. Az aláírás-létrehozó eszköz olyan hardver illetve szoftver, amely a titkos kulcs segítségével elektronikus aláírást generál. Az aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezésével névvel illetett szolgáltatás úgy értelmezhető, hogy a szolgáltató által rendelkezésre bocsátott szoftver vagy hardver (aláírás-létrehozó eszköz) segítségével az aláíró hozzájut a kriptográfiai magánkulcsához, avagy titkos kulcshoz (az aláírás-létrehozó adathoz), és ezek használatával lehet a dokumentumon elektronikus aláírást elhelyezni. A nyilvános kulcsot (aláírás-ellenőrző adat) a szolgáltató állapítja meg és rendeli hozzá a titkos kulcshoz. A nyilvános kulcsot bárki megismerheti, azt a szolgáltató köteles nyilvánosan kezelni, és kérésre rendelkezésre bocsátani.

A magyar kormányzati nyilvános kulcsú eljárás

A kormányzati PKI szükségességének kérdése több aspektusból is vizsgálható.

Egyrészről vizsgálandó, hogy az állampolgárok különböző állami, illetve önkormányzati szervekkel való (részben törvényileg előírt) elektronikus úton történő kapcsolattartását hogyan lehet egységesített formába öntve, hiteles módon megvalósítani.

Másrészről felmerülhet az igény a kormányzat szereplőinek (minisztériumok, önkormányzatok, felügyelő hatóságok, stb.) egységes PKI rendszer alá vonása.

Harmadik szempontként említést kell tenni az üzleti szféra esetleges igényeiről, amelyek tükrében szükséges lehet egy egységes PKI rendszer kiépítése a gazdasági élet szereplői részére. A civil szféra részére nyújtott szolgáltatások terén azt kell megállapítani, hogy

A kormányzati szervek összefogásának érdekében létrejött az Egységes Kormányzati

Gerinchálózat (EKG), amely a minisztériumok számára nyújt egységes szolgáltatásokat.

Az elektronikus aláírás és irat joghatályát megteremtő törvény várhatóan két fő területre terjed ki és segíti elő a fejlődését. Ez a két terület az elektronikus kereskedelem és polgár barát közigazgatás. Nem véletlen, hogy az EU különböző szervezetei kitüntetett figyelemmel kísérik, milyen fejlesztések, és mekkora előrehaladás jellemzi ezt a két területet a tagállamokban. Az elektronikus kereskedelem terjedését jelentősen akadályozza az elektronikus úton köthető szerződések, illetve az elektronikus fizetési tranzakciók iránti bizalmatlanság. Az államigazgatás, közigazgatás hatékonyságának növelése, korszerűsítése jelentős szerepet játszik az állampolgár és a közigazgatás résztvevői, a „hatóságok" kapcsolatának javulásában, és a demokratikus közigazgatás előmozdításában.

Felhasznált irodalom:

[19] 2001. évi XXXV. törvény az elektronikus aláírásról

[20] 2009. évi LII. Törvény a hivatalos iratok elektronikus kézbesítéséről és az elektronikus tértivevényről

[21] 2009. évi LX. Törvény az elektronikus közszolgáltatásról

[22] www.ekk.gov.hu/hu/informaciok/archivum/ihm/IHM_vegfelhasznaloitanusitvany.pdf

[23] www.ihm.hu/tarsadalom/kutatasok/PKI_ismertetes.pdf

[24] Gerencsér András: Architektúrák az informatikában, Jegyzet a BKÁE Vezetőképző Intézet informatikai menedzser hallgatói számára, 1999.

[25] Spisák Andor: Nyilvános kulcsú infrastruktúra architektúrák, Hadmérnök 2006 I. évf. 1. szám.

VÁNYA László[16]

ELEKTRONIKAI HADVISELÉSI ÁLLOMÁS FEJLESZTÉSE SZOFTVERRÁDIÓ TECHNOLÓGIÁVAL – AZ INTERJAM PROJEKT

Absztrakt: A szoftvervezérlésű rádióeszközök17 (SDR – Software Definied Radio) rohamos terjedése az infokommunikációs piacon az eszközök egész sorát termelte ki. A technológia fő törekvése az, hogy a hardvereszközök változatlanul hagyása mellett a működtető programok cseréjével legyenek a berendezések továbbfejleszthetők. Ez a szándék olyan hosszú amortizációs idejű rendszereknél, mint a haditechnikai eszközök, különösen kedvezőnek tűnik. Jelen írás egy, a szoftverrádió technológia előnyeinek kihasználására épülő fejlesztési projektet mutat be, amely során a fejlesztők egy új elektronikai hadviselési állomás építésén dolgoznak. Rámutat arra is, hogy az állomás más rendeltetésű fegyvernemek, szakcsapatok számára is hasznosítható képességekkel fog rendelkezni.

Kulcsszavak: szoftverrádió, elektronikai hadviselés, kiképzés

Bevezetés

A szoftvervezérlésű rádió [1], más megnevezéssel a szoftverrádió technológia egyértelműen a digitális korszak szülötte. Korábban csak úgy lehetett egy eszközben – legyen az rádió, műszer, vagy más műszaki alkotás – új szolgáltatást, képességet implementálni, ha új áramköröket, modulokat építettek be. A modulrendszerű fejlesztés filozófiája egy ideig megfelelőnek látszott, létrejöttek a cserélhető modulokból felépített műszerek, híradástechnikai berendezések, kialakultak a keretrendszerek szabványai. Mai szemmel nézve ezek előnyei, - pl. a gyors cserélhetőség meghibásodás esetén - megmaradtak, azonban a digitalizálásnak és a számítógépes vezérelhetőség hatalmas térnyerésének köszönhetően az eszközök „tudása” átköltözött a vezérlő programokba, a hardverelemek pedig univerzális építőkockákká váltak. Egy kis túlzással azt mondhatjuk, hogy csak a működtető szoftver különböztet meg ma egy rádiót egy radartól.

Hozzávetőleg a rendszerváltástól számított időben bekövetkezett politikai, gazdasági, katonai és szervezeti változások a haditechnika területén egybeestek az analóg-digitális korszakváltással. E korszakváltással és hatásaival részletesen foglalkoztam a Kommunikáció 2006 konferencián [2], ezért az abban leírtakat nem ismétlem, hanem az azóta történt eseményekről kívánok képet adni a továbbiakban.

[16] Szerző: Dr. Ványa László okl. mk. alezredes, egyetemi docens, a ZMNE BJKMK Információs Műveletek és Elektronikai Hadviselés Tanszék tanszékvezetője.

[17] A szoftverrádió a Software-Defined Radio (SDR) Forum [1] definíciója szerint: „olyan rádiótechnológia, amelyek szoftveres úton lehetővé teszi a modulációs eljárások széles körének kiválasztását, a széles, vagy keskenysávú üzemmódokat, a forgalmazás különböző eljárásokkal való rejtését, titkosítását, az adott hullámsávban jelenleg, vagy akár a jövőben használatos szabványok, eljárások rugalmas beépítését, alkalmazását.”

Az Interjam projekt létrejötte

A fentebb hivatkozott konferenciacikk utolsó bekezdése így hangzott: „Véleményem szerint egy teljesen a szoftverrádió filozófiára épülő új elektronikai hadviselési eszközrendszer kifejlesztésének ma műszaki-technikai akadályai nincsenek, hanem döntés és feladatszabás, valamint nem kevés anyagi erőforrás kérdése. Ehhez persze a mai, korszerű körülményekre illeszkedően meg kell határozni a végrehajtandó feladat mennyiségi és minőségi paramétereit, azokhoz a szükséges berendezések harcászati-műszaki követelményeit, majd a végrehajtandó folyamatokat, eljárásokat. Ezután meg kell határozni a hordozó szükségletet, majd a rendszer vezetéséhez és üzemeltetéséhez szükséges szervezeti kereteket kidolgozni. Ez nem kevés munka, de az elektronikai hadviselés mai színvonalán nincs más megoldás, mert most olyan időket élünk, amikor nem szabad régi, elavult berendezések összevásárlásával látszatképességeket létrehozni." [2. 83.p.]

Véleményemet továbbra is fenntartom, bár amikor ezeket a sorokat leírtam, nem sok reményt láttam arra, hogy a helyzet gyökeresen megváltozzon és egy kisebb, vagy nagyobb elektronikai hadviselési eszközfejlesztési program induljon. A nyugvópontról való elmozdulást sajnos továbbra sem a potenciális alkalmazók által kezdeményezett megoldáskeresés okozta, hanem egy pályázati felhívás, amelyet a Nemzeti Kutatási és Technológiai Hivatal tett közzé Jedlik Ányos Program néven 2007-ben.

A Nemzeti Kutatási és Technológiai Hivatal nevében a Kutatás-fejlesztési Pályázati és Kutatáshasznosítási Iroda felhasználás orientált kutatás-fejlesztések támogatására 2007-ben pályázatot hirdetett Jedlik Ányos Program címen. A támogatás céljaként a kiíró az alábbiakat fogalmazta meg:

„A program a gazdaság versenyképességének növelését és a fejlődés fenntarthatóságát kívánja elősegíteni korszerű technológiák területén végzett középtávú, felhasználás orientált stratégiai kutatás-fejlesztéssel. Célja az innováció ösztönzése a magyar K+F stratégiai szempontok figyelembevételével. A program keretében benyújtott projektjavaslatoknak egyértelmű, világos célkitűzéssel kell rendelkezniük, amelynek megvalósításához több területet átfogó (cross-diszciplináris) technológiai megoldások alkalmazhatók."

A gazdasági és társadalmi kihívások K+F megoldásaira a program négy alprogram keretében nyújtott lehetőséget projektjavaslatok benyújtására.

Az alprogramok a gazdaság versenyképességének növelését a nano- és mikrotechnológiák, az információs és kommunikációs technológiák, a biotechnológiák, valamint az anyag- és gyártástechnológiák, - mint alkalmazott kulcstechnológiák -, területein végzett felhasználás orientált kutatás-fejlesztéssel kívánta elősegíteni az alábbi tématerületeken:

1. Egészséges ember
2. Versenyképes ipar
3. Versenyképes agrárium
4. Élhető, fenntartható környezet"[3]

Az Interjam projekt hivatalos címe: „Integrált elektronikai felderítő és zavaró rendszer fejlesztése", amelyet egy négy tagból álló konzorcium nyújtott be.

A konzorcium tagjai:

- a SAGAX Informatikai Szervező és Tanácsadó Kft;

- a Budapesti Műszaki és Gazdaságtudományi Egyetem, Szélessávú Hírközlés és Villamosságtan Tanszéke;
- a Zrínyi Miklós Nemzetvédelmi Egyetem Információs Műveletek és Elektronikai Hadviselés Tanszéke, valamint
- a HM Elektronikai, Logisztikai és Vagyonkezelő ZRt.

A projekt vezetője Dr. Eged Bertalan, a SAGAX Kft. ügyvezető igazgatója.

A projektdokumentumban az alábbi célokat fogalmaztuk meg:

- egy olyan két fő egységből álló felderítő-zavaró berendezés kifejlesztése és prototípusának megépítése, amely a 20-3000 MHz frekvenciasávban képes elektronikai felderítést és mintegy 800 W kimenő teljesítménnyel elektronikai zavarást végrehajtani;
- az SDR technológia segítségével lehetővé tenni, hogy többbrendeltetésű, pl. rádiófelderítő-zavaró, radarfelderítő-zavaró, GSM felderítő-zavaró, GPS zavaró, vagy rádiókommunikációs célú feladatban alkalmazzuk ugyanazt az állomást, illetve az egyes üzemmódok közötti gyors átkapcsolást egy másik szoftver futtatásával oldjuk meg;
- a projekt keretében kifejleszteni:
  - a felderítő (ESM) és a zavaró (ECM) modul vezérlő szoftverét, valamint az állomás önálló működtetését biztosító programot;
  - a teljesítményerősítő egységeket és a szükséges tápegységeket;
  - a harmonikus szűrőbankot és az antennakapcsoló egységet.
- a projekt keretében integrálni a szélessávú és monitoring vevőt az adórendszerrel és egy kompakt, gyorsan konfigurálható, kis terepjáróba építhető állomásváltozatot megépíteni. [4]

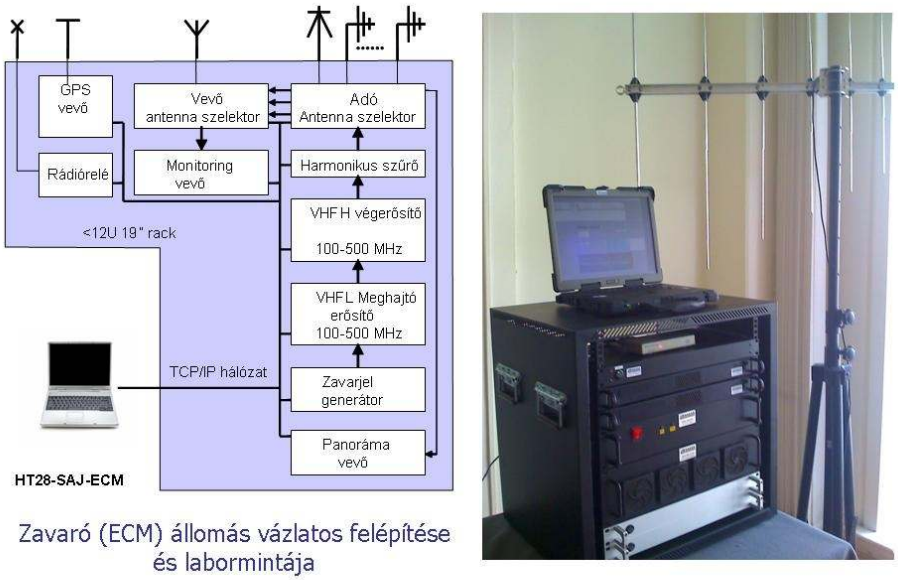
Az 1. képen a rendszer adómoduljának (ECM) vázlatos felépítése és labormintája látható.

A koncepció szerint kidolgozható többféle hordozó platformra optimalizált rendszerváltozat is, amely pl. könnyű terepjáróba, páncélozott szállító harcjárműbe, helikopterbe vagy szállító repülőgépbe is beépíthető, amennyiben a megfelelő tápellátási feltételek és antennaszerkezetek rendelkezésre állnak. A többplatformos, de azonos rendszerfelépítés előnye, hogy akár különböző fegyvernemeknél működtetett berendezések között létrehozható a távvezérlési, együttműködési, centralizált irányítási kapcsolat, azonos adatformátumokat és kommunikációs kapcsolatokat alkalmazhatnak.

A zavarási feladatokra szolgáló egységek skálázhatóságával ún. „light” és „heavy” változatok is kialakíthatók, amelyek az antennák és a szükséges energiaellátás módosításával harcászati, vagy hadműveleti szintű harci alkalmazásban is részt vehetnek, miközben az alapberendezések uniformizáltak. Az SDR technológia lényegéből adódóan ez a rendszerfelépítés lehetővé teszi, hogy többbrendeltetésű, pl. rádiófelderítő-zavaró, radarfelderítő-zavaró, GSM felderítő-zavaró, GPS zavaró, vagy rádiókommunikációs célú feladatban alkalmazzuk ugyanazt az állomást, illetve az egyes üzemmódok közötti gyors átkapcsolást egy másik feladatszabással, vagy működtető program futtatásával oldjuk meg.

A projekt az ütemtervnek megfelelően haladt és így az első időszak munkálatait leíró időszakos projektbeszámolót 2008 októberében kellett elkészíteni.

A projektbeszámoló a szükséges pénzügyi és egyéb dokumentációkon kívül részletes 1-2 oldalas magyarázószöveggel, szakmai leírással alátámasztott feladat-értékelést tartalmazott, amelyben az adott részfeladatban dolgozó konzorciumi tagok bemutatták az általuk elért eredményeket.



Zavaró (ECM) állomás vázlatos felépítése és labormintája

1. kép. A zavaró (ECM) állomás vázlatos felépítése és labormintája

A szakmai beszámoló szigorú feladat- és időrendben haladva az alábbi fő területek beszámolóit tartalmazta:

- felderítési és zavarási technikák vizsgálata;
- felderítés hatékonysági minősítő eljárás kidolgozása;
- teljesítmény összegző fejlesztése;
- zavarjel generátorok fejlesztése;
- antenna szelekciós és szétosztó egység fejlesztése;
- moduláris tápegység család fejlesztése;
- adó teljesítmény erősítő fokozatok fejlesztése;
- nagysebességű iránymeghatározási algoritmus tervezése és szimulációja;
- vevőkészülék távvezérelhetőség kifejlesztése;
- rendszer vezérlési struktúra kidolgozása;
- rendszer vezérlő szoftver specifikálása.

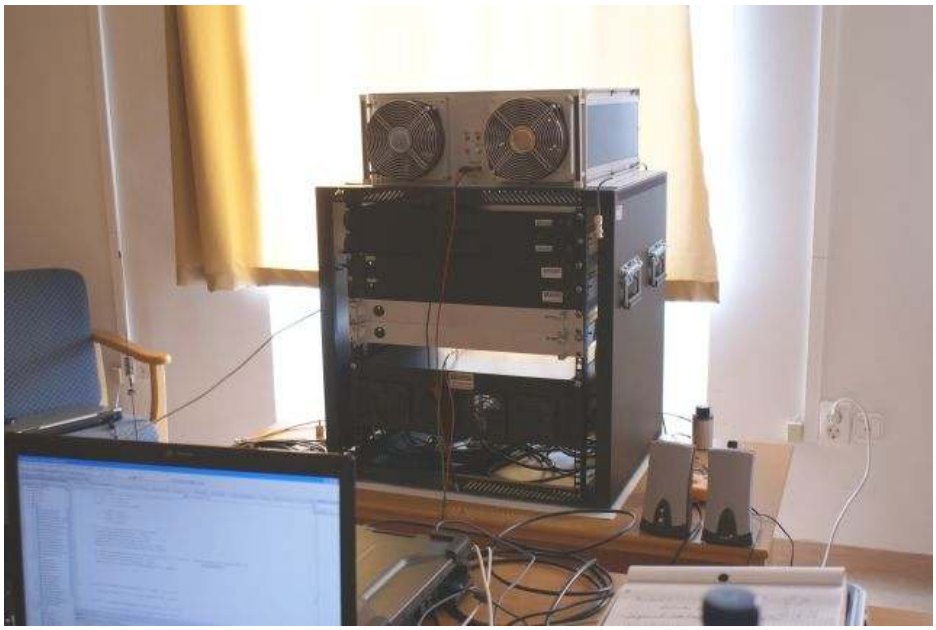
Gyakorlati kísérletek és tesztelések

Az eszköz- és szoftverfejlesztések 2009. nyár elejére olyan fázisba értek, hogy lehetőség nyílt közel terepi körülmények között kipróbálni, tesztelni egyes rend-

szerelemek működését, valódi kommunikációs alájátszó eszközökön kipróbálni a felderítési, zavarási algoritmusok működését.

Erre a feladatra jó alkalmat szolgáltatott a ZMNE 2009. évi „VIRRADAT 2009" zárógyakorlata, amelyre a várpalotai Bakony Harckiképző Központ Szimulációs Gyakorló Központjában került sor. [5] A gyakorlatvezetőség, az alárendelt kötelékek munkahelyek berendezkedése után került sor a felderítő-zavaró eszközök telepítésére, egyelőre irodai környezetben, hiszen most nem az eszközök és a kezelőállomány „tűrőképességének" kipróbálása volt a cél, hanem a működési folyamatok megfigyelése, a megtervezett algoritmusok hatékonyságának ellenőrzése, valamint a felfedett programhibák elhárítása. Az alájátszó forgalmi rendszerek szerepét a központ területén települt híradó eszközök által biztosított összeköttetések játszották.

Jelentős esemény volt ez, mert sok-sok év telt el azóta, hogy az utolsó hazai zavarókötelék (24. BG fz. EH szd. - Eger) végrehajtotta az utolsó valós rádiózavarási feladatot, majd felszámolták a zavaró alegységeket is és kivonták az utolsó zavaró berendezést is a rendszerből.



2. kép. Az Interjam projekt berendezései a ZMNE zárógyakorlatán, tesztelés során

A tesztelési feladatra a majdani adóegységnek csak negyedét, egy 200 W-os modulját alkalmaztuk. Az algoritmusok a fejlesztői elvárásoknak megfelelően működtek, néhány racionális megfontolással tovább is tökéletesítettük őket. A telepített berendezések a 2. képen láthatók munka közben. A gyakorlat során naponta beszámoltunk a gyakorlat vezetőségének a végrehajtott szakmai feladatokról. A gyakorlat értékelése során az is elhangzott, hogy az elkövetkező években is szükséges a szakállományok aktív zavarviszonyok közötti gyakoroltatása, ezért a

tervezéskor ilyen feladatok beépítése, illetve a résztvevők körének bővítése is szükséges lehet.

A projekt második szakasza 2009. szeptemberében zárul. Ekkor kell beszámolnunk az előrehaladásról, részleteiben az alábbi feladatok végrehajtásáról:

- zavarás hatékonyság minősítési eljárás kidolgozása;
- integrációs rendszerterv kidolgozása;
- moduláris tápegység család fejlesztése;
- teljesítmény összegző fejlesztése;
- kimenő szűrőbank fejlesztése;
- zavarjel generátorok fejlesztése;
- frekvencia kiterjesztő felkeverő fejlesztése;
- szektorsugárzó adó antenna rendszer fejlesztése;
- antenna mechanikai elemek tervezése és gyártása;
- nagysebességű iránymeghatározási algoritmus implementációja;
- vevőkészülék távvezérelhetőség kifejlesztése.

A rendszer valós körülmények közötti kipróbálása, továbbfejlesztése

A projekt hátralévő, mintegy bő egy évében többször lesz arra szükség, hogy valós elektronikai környezetben, valós rádióforgalmi rendszerek üzemelés közben teszteljük. Ezt a feladatot terveink szerint a Magyar Honvédség különböző szintű híradó rendszergyakorlatain oldhatnánk meg. Ez kölcsönösen előnyös mind a fejlesztőknek, mind a híradó berendezéseket üzemeltető szakállomány részére. A zavarviszonyok közötti kiképzés hasznos a gyakorló állomány számára is, mert egészen más elméletben beszélni a zavarvédelemről, és egészen más a berendezéseken megtapasztalni, amennyiben egyáltalán érzékelhetőek.

Az Interjam projekt kitűzött célja tehát egy mintaállomás kifejlesztése, amiből ha több is készül, adódik a következő feladat: egy felsőbb, irányító szint létrehozása, amely képes az alárendelt állomások számára feladatokat adni, köztük optimálisan elosztani, a kapott adatokat feldolgozni, megjeleníteni, majd az aktív, zavarási feladatokat optimális rendben szétosztani az alárendelt állomások között. E feladat együttest egy újabb projekt – az Intersys - keretében kívánjuk megfogalmazni, és a Nemzeti Technológiai Program egy következő fordulójában megpályázni

Az Interjam projekt eredményeire alapozva a megfogalmazott legfontosabb célok:

- iránymérési képességek kifejlesztése az állomásokra;
- a kifejlesztett állomások hálózatba kapcsolása;
- az irányítóállomás vezérlőprogramjának kifejlesztése;
- a térinformatikai alapú vezetési algoritmus kifejlesztése.

A projektjavaslat a Jedlik Ányos pályázat szerves folytatása lesz, a jelenleg futó projektből nyert tapasztalatok feldolgozásával.

Az Intersys projekt célja tehát egy olyan elektronikai hadviselési rendszer felépítése, amely egy önálló eleme képes összekapcsolni három-öt felderítő-zavaró rendszerállomást (Interjam), gyűjti és feldolgozza a felderítési információkat, feladatot szab az alárendelt állomásainak, irányítja azok működését, ellenőrzi a vég-

rehajtás hatékonyságát és együttműködik a szomszédos hasonló vezetési szintekkel. A működési filozófia alapját az adatok térben és időben való feldolgozása, tárolása, az állomások valós térbeli pozícióiból és a terep digitális térmodelljéből képzett hullámterjedési vizsgálatokon alapuló zavarhatékonysági számítások képezik, amelyeket összefoglaló néven térinformatikai alapú harcvezetési rendszernek nevezünk.

Hazai fejlesztésben, hazai szakembergárda bevonásával, a csapatok honi bázisán lefolytatható kiképzés nagyságrendekkel csökkenti a járulékos költségeket, a rendszer teljes élettartamára számolt bekerülési költséget, nem is beszélve a garanciális és garanciaidő utáni szervizelési és logisztikai feladatok ellátásáról. A hazai munkaerő alkalmazása a hazai munkahelyek megtartását erősíti, munkahelyet teremthet, hazai adó és járulékfizetést generál. A beinvesztált hazai szellemi tőke a világszínvonalú hazai szürkeállomány megtartása és a jogtulajdonosi viszonyok országon belül tartása mind-mind az ország érdekeit szolgálja.

A hazai fejlesztés mellett szól továbbá az is, hogy ha a sorozatgyártásra kerülő rendszer nem csak egy szervezethez kerülhet kis darabszámban, hanem a képességei okán több katonai és nemzetbiztonsági szervezethez is, mind hazai, mind nemzetközi missziós feladatokban, ami tovább csökkenti az egyes rendszerekre eső fajlagos fejlesztési költséget, így gazdaságosabban alakítható ki a logisztikai és szervizháttér.

FELHASZNÁLT IRODALOM

[1] SDR Forum honlapja: www.sdrforum.org

[2] Dr. Ványa László: Út a szoftverrádió és szoftver rádiózavaró állomások felé, Kommunikáció 2006. konferencia kiadványa, ZMNE, 2006. 76-83. p. ISBN: 978-963-7060-18-2

[3] Jedlik Ányos program - K+F projektek támogatása.

[4] http://www.nkth.gov.hu/palyazatok-eredmenyek/jedlik-anyos-program/jedlik-anyos-program-f (2008.12.15.)

[5] Pályázati konzorcium: „Integrált elektronikai felderítő és zavaró rendszer fejlesztése” - benyújtott projektdokumentum.

[6] Sikeresen végetért a nemzetvédelmi egyetem zárógyakorlata várpalotán. http://portal.zmne.hu/portal/page?_pageid=34,88456&_dad=portal&_schema=PORTAL (2009. 09. 11.)

Balázs PÁNDI[18]

ANALYSIS OF THE FIELD COMMUNICATION SYSTEM, TO INCREASE APPLICABILITY AND EFFICIENCY

Abstract: This article is summarises the findings of the author described in his PhD dissertation, on the topic of increasing the applicability and efficiency of the field communications system with the computerisation of certain parts of the combat document system.

Keywords: computerisation, combat documents, field communications system

I. Definition of the scientific problem

Regarding the topic it can be stated, that except for the continuously modified development concept, field-exercise, and experiment, the only one element of the field communication system has gone through effective changes, which does not substantially change the problem that the entire system is technologically obsolete, and outdated in terms of application methodology and organisation.

According to short term expectations, the field communication system will keep staying in operation. The improvement of the technological conditions of the current system cannot be expected, in this case – *confirmed by military experts* – only the complete replacement can be the solution. After making these observations, the candidate raises the question of how to make the current field communication system more capable of meeting the requirements of modern military operations – *until the time of replacement*.

In the candidates' view – *using a system based approach* – in case of the field communication system, the improvement of the *application mode* and the strongly connected *system elements*, or in other words the *application methodology* can be temporarily solution, especially in light of the fact that the regulations concerning the application, have been invalidated over half a decade ago without any replacement.

II. Research objectives

1) Due to the lack of professional regulations, find analyse and evaluate all laws and normative, based on which the current requirements, expectations from the system can be clearly defined.

2) In knowledge of the requirements, expectations present and evaluate the applicability and field of applications of the field communication system. On a system based approach identify and define the application modes of and connected system elements of the communication system, which can be modified or converted to bring the applicability of the field communication network closer to the level required by the command and control system.

3) As a solution for the modification or conversion, develop a user software application, which can be applied in both domestic and international terms, using the existing software and hardware environment – essentially – without any additional investment.

[18] Author: Pándi, Balázs (MA – software engineer, economist)

4) Define and make a recommendation on the further development directions and methods of the software application to be developed.

III. Conclusion

1) The candidate has pointed out that the greatly unregulated state of the field communication system is caused by the lack of professional regulations regarding the communication system. Despite current unregulated state, the field communication system will stay in operation, during which the application is – mainly – organised, executed based on the previous policies. The modernisation programmes of the stationary subsystems were not followed by the modernisation of the field segments applied by the land forces. The technology, policies, and methodology used by the communication system is obsolete, only complete replacement can be the solution, but until the time of replacement, the current system has to be operated. He has recommended the creation of a branch regulation in order to resolve the current unregulated state.

2) The candidate has exposed, that the available financial-technical assets, do not make it possible or necessary to computerise the entire document system. Because of this, the end-parameters, based on which the elements or application modes of the document system which require replacement or modification can be identified. He has pointed out that the computerisation of certain diagrams – within the – communication and computer plan in the combat document system of the brigade using a specialised software application can enhance the reaction time of the command and control of the field communication system, through which the command and control activity of the troops can be brought close to what's defined in the expectations.

3) Based on the partial results he has managed to identify the application mode, and subsystems, whichs' computerisation can promote the improvement the command and control activity in the field communication system. During this, based on the user requirements, through continuous refinement steps he has developed a specialised software application. He has identified the software environment for the actual implementation. The software has been tested, during which the minimal technical-technological conditions, requirements, hardware requirements regarding the system have been ascertained. The product has been evaluated, and the directions of further development have been identified.

IV. Contribution to knowledge

The candidate considers the following as contribution to knowledge:

1) He has processed, analysed and evaluated using scientific methods, the laws, normatives, and doctrines, based on which he has identified the current requirements for the efficient application of the field communication system.

2) He has proved regarding the application – using the given the current obsolete technological abilities - of the field communication system, that with the computerisation of the communication and computer command and control methodology the efficiency of the application of the system can be increased. He has identified the group of system elements and application modes, which can be computerised.

3) Based on the application modes, and connected system elements, which can promote the improvement the command and control activity – starting from user requirements – identified the most suitable programming language, and developed an upgradable specialised software application related to the computerisation of certain parts of the command document system.

Some references:

[7] A Magyar Köztársaság biztonság- és védelempolitikájának alapelveiről szóló 94/1998. (XII.29.) OGY határozat, Complex DVD jogtár, CJDVD-09/01. szám, Budapest, ISSN 1788-5027, 2009. január 31.

[8] Andrade, Chris – Livermore, Shwan – Meyers, Mike – Van Vliet, Scott: Professional WPF Programming, .NET Development with the Windows Presentation Foundation, WROX, ISBN 978-0-470-04180-2, 3. oldal. 2007.

[9] Applegate, D.L. – Bixby, R.E. – Chvátal, V. – Cook, W.J.: The Traveling Salesman Problem, A Computational Study, Princeton University Press, ISBN 978-0-691-12993-8, 373-469. oldal, 2006.

[10] Cormne, Thomas H. – Leiseron, Charles E. – Rivest, Ronald L. – Stein, Clifford: Introduction to Algorithms, Second Edition, MIT Press and McGraw-Hill, ISBN 0-262-03293-7, 561-643. oldal, 2001.

[11] Fekete, Károly: Modelling the videoconference in mission, „Kommunikáció 2007.” nemzetközi szakmai-tudományos konferencia, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, ISBN 978-963-7060-31-1, 126. oldal, 2007. október 16.

[12] Finszter Géza: A rendészeti rendszer alkotmányos és közjogi alapjai (2. számú előtanulmány az átfogó rendészeti stratégia társadalmi vitájához), Rendőrség Tudományos, Technológiai és Innovációs Tanácsa, Budapest, 16-17. oldal, 2008.

[13] Griffiths, Ian – Adams, Matthew: .NET Windows Forms in a nutshell, O'Reilly, ISBN 0-596-00338-2, 3. oldal, 2003.

[14] Liberty, Jesse – Xie, Donald: Programming C Sharp 3.0 5th edition, O’Reilly, ISBN 10-0-596-52743-8, 3-6. oldal, 2007.

[15] Magyar Honvédség Összhaderőnemi Doktrína 2. kiadás, Magyar Honvédség kiadványa, Budapest, Ált/27. szakutasítás, 45-60. oldal, 2007.

[16] Pándi Balázs: A tábori hírrendszer erőforrásaival való gazdálkodás újszerű megközelítése (PhD értekezés tervezeti példánya), Zrínyi Miklós Nemzetvédelmi Egyetem KMDI, Budapest, 75-80. oldal, 2009.

[17] Rajnai Zoltán: A gépesített hadtest információs kapcsolatainak és hírrendszerének elemzése hadműveletekben, Akadémiai Közlemények, Budapest, ISSN 1218-5507, 1996/210. szám, 140-143. oldal, 1996.

[18] Rajnai Zoltán: A kommunikációs rendszerek tervezését segítő szoftverek igényei, „Kommunikáció 2000.” nemzetközi szakmai-tudományos konferencia, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 147. oldal, 2000. október 4.

[19] Rajnai Zoltán: A tábori alaphírhálózat korszerűsítésének lehetőségei, „Kommunikáció 2000.” nemzetközi szakmai-tudományos konferencia, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 95. oldal, 2000. október 4.

[20] Roman, Steven: Access Database Design & Programming 3rd Edition, O'Reilly, ISBN 0-596-00273-4, 126-129 oldal, 2002.

[21] Royce, Winston W.: Managing the development of large software systems, Proceedings of IEEE WESCON 26, 328-338. oldal, 1970.

[22] Szöllősi Sándor: Konvergáló hálózatok fejlődési trendjei, a technikai alkalmazhatóság kérdései a Magyar Honvédség infokommunikációs rendszerében, doktori (PhD) értekezés, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 58. oldal, 2007.
[23] Szücs Ervin: Rendszer és modell I., Egységes Jegyzet (ELTE TTK), Kézirat, Tankönyvkiadó, Budapest, 99-100. oldal, 1987.

Erik PÁNDI – Balázs PÁNDI[19]

OPTIMISATION OF THE RISK FACTORS OF THE COMMUNICATIONS SYSTEM USING THE COMPUTERISATION OF CERTAIN APPLICATIONS[20]

Abstract: Overwhelming problems concerning the field communication system are well known among military – in particular communications – professionals. According to short term expectations however, the field communication system will keep staying in operation. The improvement of the technical conditions of the current system can not be expected, as in this case – also approved by military experts – only complete replacement can be the solution. Thus the question arises, how to make the current field communication system more capable of meeting the requirements of modern military operations – until the time of replacement. In my opinion in case of the field communication system, the improvement of the application mode and the strongly connected system elements, or in other words the application methodology can be temporarily solution, especially in light of the fact that the regulations concerning the application, have been invalidated over half a decade ago without any replacement.

Keywords: computerisation, combat documents, NHíIR, field communication system

1. Theoretical approach

"Planning of present-day communications networks requires a new perspective from every network designer professional, who is working on the installation, application and required modification of the new digital network of the Hungarian Army. This planning process however cannot take place in the "analogue" system still conventional and accustomed today. In other words in the plan it on paper, send it as instruction and the communications units will try to install it and operate it fashion." – stated a military researcher-expert nearly a decade ago [1].

Based upon my analysis it can be stated, that the majority of the field communication sub-system National Communications and Computer System (NHíIR), or in other words the field communication system is still working this way, namely "using the conventional analogue system", that is the plan it on paper, send it as instruction and the communications and computer commanding staff, and specialist units and sub-units will try to install, operate and exercise command and control over it.

According to the effective strategic theories, two fundamental concepts can be seen. From one side in case of the application of national land forces, a force consisting of light infantry battalions, light infantry sub-units, combat-supporting,

[19] Authors: Pándi, Erik (PhD – military science), Pándi, Balázs (MA – software engineer, economist).

[20] This paper was supported by the Bolyai János Research Scholarship of the Hungarian Academy of Sciences.

and combat-servicing-supporting troops is applied. In case domestic application of this force the usage of battalion, or company level troops has to be planned. On the other hand the complete modernisation of the current field communication system is not likely to happen in the near future, despite the fact that effective modernisations, experiments, and field exercises are taking place on tactical level [2].

Based on these, primarily considering the possibility of domestic application of the forces, it can be said that the current – mainly analogue – field segment of the NHíIR will continue to be the main instrument of the communication and computer system as the subsystem of the command and control system. Independently of doctrinal factors, in the current peace-time organisation of the combat troops of the land forces primarily consists of two infantry brigades, differing in organisational structure – integrating the organisation of infantry battalions - , that form the primary basis of the military organisations serving as stand by units in the NATO reaction force, dedicated for NATO, or to be applied in domestic military operation firstly, and the forces serving abroad in future military operations secondly.

So after analysing the issues of communications and computer networks on a tactical-operational higher-unit level, it can be found that both the superior military organisation, the assigned commander of the infantry brigade, and the specialised (sub-)units are working together, cooperate, in the technical development of the field communication, providing data and information transfer, supporting the command and control function of the infantry brigade. It can be observed, that the significance of the field communication system has reduced, with conflicts becoming more and more asymmetric, and with the reduction of size of the forces taking part in crisis response, and at the same time the increase of their applicability and mobility. The emphasis has shifted towards wireless communications connections, which is not supported by the fact that the field communication network only has a limited radio connection interface, it does not support the connection of radio devices of mobile users, or mobile command centres in large numbers, thus in case of application of mobile combat-troops, or tactical units, these can only be commanded by mainly using radio stations outside the network [3].

As another branch of the complex topic of communications and computer networks, it can be said regarding the own field communication system of the infantry brigade, that the structure of the organisational elements, the cooperation regulations of command and control, and application of the assigned personnel and technical equipment is currently also done by the traditional organisational principles. Related to this it can be established, that – *essentially* – the necessity for the operation of the field communication system, makes it necessary that the specialised staff follows standardized requirements during the application of the system, the basis for which is still the previous main regulation.

After studying the field communication network and the own communication system of the infantry brigade, it is my opinion that the command and control system of the field segment of the NHíIR can be considered essentially obsolete on every level. It is not- or only with limitations suitable for – among other things – the application of digital services on a tactical level, multimedia information

transfer, accessing of services provided by digital networks, reducing paper based information exchange, and control and management of fast and authentic data-transfer.

2. Issues regarding computerisation

I regard the combat document system, and combat documents of the communications and computer service as an administrative element of the application regulations of the field communication system. Today these are produced using two methods, both of which however can – essentially – be considered as manual, or slightly computerised. Despite the changed environment due to the convergence of telecommunications and information technology, in my opinion the display of information on traditional media is still a required part of the command and control system of the communication system, however it has to be considered as a main objective to reduce this to a required and satisfactory level. The applicability of combat document system, through its' communication and computer command and control is an influencing factor of the command and control of higher-units, and thus also an influencing factor of the success or failure of the military operations executed with it [4].

Firstly it can be stated regarding the issue of combat documents prepared on different media – but mainly on paper, manually -, that today it would be practically feasible implement the computerisation of activities requiring maps, however its' implementation until the replacement of the communication system currently cannot be considered as an optimal solution. Secondly in case of the traditional text based documents manual preparation and processing – considering the technical possibilities, and traditional but proven military-specialised staff of the national forces – is likely to stay in operation, even though the scope of modernisation of the communication system is reducing. Based on these, it can be established, that concerning the expectations regarding the reduction of traditional media, the elements of the combat document system represented with tables or diagrams can become suitable for computerisation.

According to the expert opinion on system-based thinking it is: „not only (not primarily) necessary for decomposing the existing systems into parts (elements on the bottom level), organising the elements, revealing the internal and external connections of the system, recognising the necessity and possibilities of diverse examination aspects (interdisciplinary cooperation), but also for assembling systems meeting the new requirements and in harmony with the environment from the existing elements. […] Operating of the existing systems – according to some predefined aspects – under optimal operating conditions makes it necessary to renew or replace certain parts. [...] Due to the development of society not only the level of requirements for the operation of the system, but also – the previously mentioned – security domain has also changed. The "unchanged" technical system generally – due to the continuous change of environment - is becoming obsolete, useless, in other words it is relatively regressing. [...] The conclusions of system analysis – because of the above mentioned things – are not forever valid, but these have to be revised from time to time due to the change of environmental conditions and the (moral and financial) deterioration of certain parts of the system. This

means that, operating the current systems makes continuous renewal, replacement of parts, improvement of application methods, and creation of new systems necessary." [5]. Taking the previously mentioned into account, I find that – although the complete system will be replaced – the replacement of certain parts, or the modification of application methods can improve the operation of the entire system. Based on this, after reviewing the combat document system, in my opinion that the computerisation of certain diagrams within the communication and computer plan of the infantry brigade using a specialised software application, and the integration of this into the communication and computer command and control system can help in bringing the application of tactical-operational higher-units closer to what's defined in the expectations.

3. Summary, conclusions:

- The newly defined requirements and expectations against the field subsystem of the NHíIR are known, however only the current technological capabilities are available for reaching these. Due to the temporary, or continuous use of the field communication system, its' operation has become necessary. Professional operation of the system requires the formalised and regulated nature of the processes. Due to this the operation of communication system in practice is still done according to the invalidated main regulation.
- The organisational structure of the field communication system is unchanged. New functions assigned for the land forces of the Hungarian Army, impose new requirements for the staff on the field of the commanding and controlling troops. Part of this is related to the field of communication and computer networks. Due to the limited technical resources of the mainly analogue system, the utilisation of the reserves organisational resources can be a temporary solution. Supporting the new challenges regarding command and control, can be assisted by the more efficient operation of the command and control system of the field communication system.
- The combat document feature plays a key role in the operation of the command and control of the field communication system. The majority of combat documents are prepared manually. Planning-organising, operating activity in case of the computerisation of the entire combat document system can optimise the spatial and temporal activity of the command and control system of the communication system. The available financial-technical assets do not make it possible to computerise the entire document system. System-based thinking requires the end-parameters, based on which the elements or application modes of the document system which require replacement or modification to be identified.

Main findings of the publication:

- The lack of main regulation does not support the creation or the – limited – development of conditions, circumstances of professional operation.

- The computerisation of certain diagrams – within the – communication and computer plan in the combat document system of the brigade using a specialised software application can enhance the reaction time of the command and control of the field communication system, through which the command and control activity of the troops can be brought close to what's defined in the expectations.

References:

[1] Rajnai Zoltán: A kommunikációs rendszerek tervezését segítő szoftverek igényei, „Kommunikáció 2000." International science conference, Zrínyi Miklós National Defence University, Budapest, pp 147, 4.10.2000.;

[2] A Magyar Köztársaság biztonság- és védelempolitikájának alapelveiről szóló 94/1998. (XII.29.) OGY határozat, Complex DVD jogtár, CJDVD-09/01. szám, Budapest, ISSN 1788-5027, 2009. január 31.

[3] Rajnai Zoltán: A gépesített hadtest információs kapcsolatainak és hírrendszerének elemzése hadműveletekben, Akadémiai Közlemények, Budapest, ISSN 1218-5507, 1996/210. szám, 140-143. oldal, 1996.

[4] Pándi Balázs: A tábori hírrendszer erőforrásaival való gazdálkodás újszerű megközelítése (PhD értekezés tervezeti példánya), Zrínyi Miklós National Defence University PhD School on Military Science, Budapest, pp 75-80, 2009.

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

PÁNDI Erik – PÁNDI Balázs[21]

A KATONAI HÍRRENDSZEREKKEL KAPCSOLATOS STRATÉGIAI KIHÍVÁSOK ÉS ELVÁRÁSOK[22]

Absztrakt: Jelen közlemény az ágazati szabályozók nagyfokú hiányossága miatt a jogszabályi háttér révén összegzi és elemzi a hazai katonai távközlő rendszerekkel kapcsolatos stratégiai kérdéseket annak érdekében, hogy a jelenlegi tábori hírrendszer alkalmazhatósága hatékonyságának esetleges növelése szakmai alapjait megteremtse.

Kulcsszavak: fenyegetettség, katonai műveletek, katonai stratégia, tábori hírrendszer.

Bevezetés

Hazánk geo- és biztonságpolitikai helyzetében közel két évtizeddel ezelőtt elkezdődött változások lényegében az elmúlt tíz esztendő során csúcsosodtak ki, amely időszakban országunk két – *a kontinens államalakulatai szempontjából meghatározó* – szövetségi rendszer tagjává vált. Az egykori fegyveres erők szerepe és dominanciája is megváltozott, így amíg az egyik részének feladatrendszere a rendészet irányába szélesedett, addig a másiké az ország fegyveres védelme, illetve a koalíciós keretek között folytatott *háborús* és *nem háborús* katonai műveletek területén bővült. A rendszerek teljes kiforrottságában azonban tapasztalhatók némi hiányosságok, hiszen az a körülmény, amely szerint az EBESz, ENSz, EU, NATO és más nemzetközi békefenntartó erőknek a válságövezetekben kifejtett tevékenysége során a katonai és rendőri működés közeledett és közeledik egymáshoz, azt a magyarországi múltban gyökerező hitet erősíti – *talán még napjainkban is* –, hogy a rend védelmében a rendőrséget hadseregként, a katonaságot pedig rendőrségként lehet működtetni [1]. A hibáktól eltekintve azonban leszögezhető, hogy világunk permanensen változó biztonságpolitikai környezetében globális biztonságunk megőrzésében és fenntartásában mind a katonai, mind a rendészeti szervezetek szerepe itthon és külföldön egyaránt fokozódott.

A kutatási témával összefüggő problémakör elmélyüléséhez a katonai doktrínák folyamatos változása is hozzájárult, hiszen a feladatrendszerhez rendelt technikai erőforrások meghatározása és tervezése stabilnak tekinthető alapkoncepció nélkül reménytelennek tűnő feladat. E folyamatok egyenes következménye a még rendszerben levő, de erkölcsileg amortizált, korszerűtlen – *a modern hadviselést már egyre kevésbé támogató, ugyanakkor* – kényszerűségből alkalmazni szükséges eljárásrend és metodika szerint működtetett technikai (elektronikai) eszközállomány, amely egyre súlyosabb kompatibilitási és interoperabilitási problémaforrást jelent nem csak a koalíciós műveleteknél, hanem már a hazai felhasználás során is. A problémát komplexebbé teszi – *a katonai szervezetek esetében korábban elképzelhetetlennek tűnő* – szabályozatlanság ténye is, amely a korszerűsítés nélkül

[21] Szerzők: Pándi Erik (PhD), ZMNE Híradó Tanszék; Pándi Balázs (közgazdasági programozó matematikus, doktorjelölt), Gordon és Webster Tanácsadó ZRt.

[22] Jelen közlemény a Bolyai János Kutatási Ösztöndíj támogatásával készült.

kivont szakutasítások révén teremt – *mind a szolgálati ág szervezetét és eljárásrendjét, mind a technikai eszközrendszer alkalmazását tekintve* – exlex[23] állapotot.

A kutatás során arra kerestünk válaszokat, hogy az érvényben levő békehadrend szerint működő nemzeti haderő szárazföldi katonai szervezeteinek vezetését és irányítását támogató, jelenleg rendszeresített tábori hírrendszerek katonai alkalmazását – *adott peremfeltételek mellett* – korszerűsíteni hivatott informatikai (elsősorban: szoftver) alrendszer gyakorlati kialakítását elsődlegesen mely stratégiai kérdések befolyásolhatják. A vizsgálatokat a joganyagok, valamint a mértékadó szakirodalom analizálása révén hajtottuk végre, amely során a NATO tagságunkkal kapcsolatos általános kérdések mellett a Nemzeti Híradó és Informatikai Rendszert (NHíIR) érintő általános szakmai követelményekkel, valamint a katonai kihívásokkal kapcsolatos részkérdések is áttekintettük.

1. Vizsgálati szak

1.1. Joganyagok áttanulmányozása

A **legfőbb joganyagok** vizsgálata során megállapítottuk, hogy azok egyrészről rögzítik azon tényt, amely szerint tagállami viszonylatban meg kell valósulnia nemzeti haderőerő fenntartásának és fejlesztésének, másrészről ezeknek olyan haderőknek kell lenniük, amelyek egyénileg, de elsősorban kollektív módon is képesek egy fegyveres támadással szembeni küzdelem sikeres megvívására. A tagországoknak – *vállalásaikban tett képességeik területén és mértékében* – részt kell venniük szövetségi keretekben végrehajtott – *földrajzi szempontból indifferens – háborús* és *nem háborús* katonai műveletekben egyaránt. Magyarország távlatosan részt kíván vállalni egy dandár méretű erő hat havi harci és egy zászlóalj méretű erő tartós (hat hónapon túli) nem harci körülmények közötti alkalmazására, avagy egy zászlóalj méretű erő tartós (hat hónapon túli) harci és egy zászlóalj méretű erő tartós (hat hónapon túli) nem harci jellegű tevékenységének biztosításában. Mindezen feladatok teljesítése azonban csak a reális veszélytényezők felmérése eredményeit felhasználva prognosztizálható védelmi szükségletek alapján rendelkezésre bocsátható anyagi-pénzügyi források mentén képzelhető el, ugyanakkor hazánk katonai fejlesztéseit köteles egyeztetni a szövetséggel.

A joganyagok áttekintése alapján kijelenthetjük, hogy célként fogalmazódott meg a szárazföldi haderőnem vezetés-irányítási funkcióit kiszolgáló tábori híradó és informatikai rendszerek továbbfejlesztésének prioritása. Megítélésünk szerint ennek egyik oka, hogy szövetségesi státusunkkal párhuzamosan Magyarországon is megkezdődött a vezetés-irányítás hazai elméletrendszerének átalakulása, amely ugyanakkor rögös utat jár be, hiszen jól megfigyelhetők az e folyamatokkal kapcsolatosan kialakult bizonytalanságok is. Másrészről az elméleti felismerés mellett a Magyar Honvédség (Honvédség) egyes műveleti tapasztalatai is elősegíthették a fejlettebb tagállamok bevált gyakorlatainak – *egyelőre még csak tervekbe való* – beépülését. Mindezek mellett leszögezhető, hogy a kialakítandó rendszer egyik markáns sajátja a vezetési eszközök, az információs eszközök, híradó és informatikai eszközök magas szintű alkalmazása lehet. Az alfejezetben rögzítetteket röviden összegezve és értékelve megállapítható, hogy:

[23] Törvényen (jogszabályokon) kívüli.

- A tábori hírrendszerrel, mint a katonai szervezetek vezetés-irányítási rendszerének technikai alrendszerével kapcsolatos **stratégiai elvárások** az elmúlt két évtizedben **jelentősen megváltoztak**. A jelenlegi helyzet ellentmondásos, hiszen a technikai modernizáció vontatottan, csak néhány részterületet magába foglalóan zajlott le [2], azonban a hírrendszer alkalmazásával összefüggő szabályozók (szakutasítások) többsége – *újabbak kiadása nélkül* – visszavonásra kerültek. Ezen állításunk eklatáns példája a szárazföldi csapatok híradásszervezési elveire és követelményeire szakutasítás[24] kiadásáról szóló 057/1983. (HK 08.) MN híradófőnök intézkedés, amely az egyes szükségtelenné vált rendelkezések hatályon kívül helyezéséről szóló 39/2003. (HK 10.) HM utasítás alapján vesztette érvényét.[25] Tekintettel arra, hogy a korábbi tábori technikai alrendszerek napjainkban is alkalmazás alatt (rendszerben) állnak, ezért a Honvédség híradó és informatikai szakállományának egyrészt továbbra is szükségszerű a szakutasításban foglalt elveket és követelményeket szolgálatuk során figyelembe venni, másodsorban azokat a kiképzés és oktatás során alkalmazni.[26]
- A jogszabályok tagállami (elsősorban: EU, NATO, illetőleg EBESz, ENSz) viszonylatban feltételezik egyrészről **katonai erő fenntartását és fejlesztését**, másrészről olyan erő fenntartását, amely **egyénileg**, de elsősorban **kollektív módon is képes egy fegyveres támadással szembeni küzdelem sikeres megvívására.** Harmadrészt, feltételezik továbbá, hogy hazánk **részt vállal expedíciós** (egy dandár méretű erő hat havi harci és egy zászlóalj méretű erő tartós [hat hónapon túli] nem harci körülmények közötti alkalmazására; vagy egy zászlóalj méretű erő tartós [hat hónapon túli] harci és egy zászlóalj méretű erő tartós (hat hónapon túli) nem harci jellegű tevékenységére)**,** illetőleg **katasztrófaelhárítási (katasztrófavédelmi, valamint –felszámolási) feladatok végrehajtásában.** Mindezen feladatok teljesítése azonban csak a **reális veszélytényezők felmérése eredményeit** felhasználva **prognosztizálható védelmi szükségletek alapján rendelkezésre bocsátható anyagi-pénzügyi források mentén** képzelhető el.
- Szövetségi tagságainkkal egyidejűleg a vezetés-irányítás hazai elméletrendszere átalakulóban van, a szakirodalom alapján megfigyelhető e folyamattal kapcsolatosan kialakult bizonytalanságok. Ennek ellenére leszögezhető, hogy a rendszer egyik sajátja a vezetési eszközök, az információs eszközök, **híradó és informatikai eszközök magas szintű alkalmazása.** A szövetségi eljárásrend alapján kialakuló rendszer technikai támogatása tehát elsőrendű, ezért megfogalmazódott, hogy **a szárazföldi haderőnem katonai képességeinek fejlesztése során előnyben kell részesíteni** a vezetés-irányítási funkciókat kiszolgáló **tábori híradó és informatikai rendszerek továbbfejlesztését**.

[24] Röviden: Hír/126. szakutasítás, amely 20 éven át volt hatályban, mindvégig ideiglenes jelleggel.

[25] Az utasítás 2003. május 1-jén lépett hatályba.

[26] Oktatási felhasználásra példa: Dr. Sándor Miklós – Farkas Tibor: A lövészdandár híradása c., tavaly megjelent ZMNE BJKMK Híradó Tanszék egyetemi jegyzet, amelynek 53. oldalán a Hír/126. szakutasítás, mint felhasznált irodalom egyértelműen feltüntetésre került.

1.2. Általános szakmai követelmények feltárása

Az **általános szakmai követelmények** vizsgálata során megállapítottuk, hogy a klasszikus, hírrendszerrel kapcsolatos fogalmi definíció 2007-re már szakmailag árnyalt, korrekt módon került meghatározásra, azonban a szakmai főkérdések (általános követelmények, a rendszer felosztása, szervezési és alkalmazási alapok) tisztázásán túlmenően egyéb – *részletes* – hazai szabályozás nem készült el. A nemzeti rendszerek megszervezésének és alkalmazásának alapelvei a jelenlegitől eltérő, korszerű képességeket is feltételeznek a használatban levő híradó és informatikai rendszerekről. Megítélésünk szerint e követelmények többségét elsősorban a stacioner rendszer képes teljesíteni, szemben a jelenleg rendszeresített tábori hírrendszerben alkalmazott alrendszerekkel, eszközökkel. Az alfejezetben rögzítetteket röviden összegezve és értékelve megállapítható, hogy:

- A klasszikus, hírrendszerrel kapcsolatos **fogalmi definíció** megváltozására lényegében véve hazánk NATO-hoz való csatlakozását követően néhány évvel került sor első ízben. A szövetségesi dokumentumok (szabványok, ajánlások), elvek figyelembe vételével az ÖHD 2. kiadása, 2007-ben már szakmailag árnyalt, korrekt módon határozta meg a híradó és informatikai rendszert, amelyet Nemzeti Híradó és Informatikai Rendszer, vagyis **NHíIR** néven illettünk [3]. Leszögezhető azonban, hogy **a doktrínán túlmenően egyéb** – *részletes* – **hazai szabályozás nem készült el**.
- A fejlettebb haditechnikai infrastruktúrával és ebből kifolyólag a hazaitól eltérő katonai, szakmai eljárásrenddel, gyakorlattal rendelkező szövetséges országok révén a doktrína által **a híradással és informatikával**, mint szolgálati ággal (szakmával) **szemben megfogalmazott általános követelmények és elvárások komplexebbé váltak**, jellemzően kiemelve a kompatibilitás és interoperabilitás részterületeit. A teljes rendszer elvi felépítésének alapvető logikája gyökeresen nem tér el a korábban is alkalmazott elmélettől.
- **Rendelkezésre állnak** a nemzeti rendszerek **megszervezésének és alkalmazásának alapelvei**, amelyek már **a jelenlegitől eltérő, korszerű képességeket is feltételeznek**[27] a használatban levő híradó és informatikai rendszerekről. Megítélésünk szerint e **követelmények többségét elsősorban a stacioner rendszer képes teljesíteni**, szemben a jelenleg rendszeresített tábori hírrendszerben alkalmazott alrendszerekkel, eszközökkel. Álláspontunkat véleményünk szerint alátámasztják mérvadó katonai szakértők is, akik leszögezték, hogy: *„…a külföldi rendszerekkel történő együttes üzemeltetésben még igen sok a kompatibilitási, interoperabilitási probléma, valójában csak a digitális központok szintjén tekinthető megoldottnak. […] A kompatibilitási problémák az eszközök sokrétűségéből fakadnak (generációs különbségek, csatlakozásoknál eltérő fizikai kialakítások, eltérő adatátviteli eljárások, eltérő üzemmódok és képességek, gyártói sajátosságok) és valószínűleg rövid időn belül nem oldhatók meg."* [4].

[27] Napjaink korszerű katonai híradó és informatikai rendszerei esetében a videokonferencia szolgáltatást már alapszolgáltatásként kell kezelni [5].

1.3. Katonai kihívások áttekintése

A **katonai kihívások** részkérdéseinek áttekintése során arra a megállapításra jutottunk, hogy a szárazföldi haderő alapvető komponensei a – *légi szállításra is alkalmassá tett* – lövészzászlóaljak (esetlegesen: század harccsoportok). Fő feladatuk, hogy az ellenség egységei és alegységei ellen sikeres, illetőleg harcászati magasabbegységei ellen korlátozott eredményű harcot folytassanak. Összességében tehát csak harcászati alkalmazással kell számolni, mindezt ütközet és harc formájában. Tervezési szempontból, a háborús küszöb alatti konfliktusok esetében a lövészzászlóaljak feladataikat önállóan, a szokásos békefenntartó eljárásmódhoz hasonlóan hajtják végre. Szükség esetén, ideiglenes jelleggel támadó vagy védelmi harcot is folytathatnak. Ellenséges támadás esetén feladataikat korlátozott ideig önállóan, majd koalíciós összhaderőnemi kötelékben teljesítik. Az alfejezetben rögzítetteket röviden összegezve és értékelve megállapítható, hogy:

- Magyarországnak mind ***háborús***, mind ***nem háborús*****, aszimmetrikus** jellegű katonai műveletekben való részvételre **szükséges felkészülnie**. Hazánk katonai doktrínája elsősorban **hagyományos jegyeket** hordoz magán, amely alapján a nemzeti haderő **harcászati alkalmazásával** lehet számolni, mindezt **ütközet** és **harc** formájában.
- A tábori hírrendszer vizsgálata szempontjából releváns nemzeti haderő **szárazföldi komponenseinek** legfőbb **feladatrendszere** – *több évszázados hagyományos gyökereihez képest lényegileg* – **nem változott**. Az összhaderőnemi katonai műveletekben történő alkalmazása során, a haderőnemek együttműködése kapcsán azonban **feladatai végrehajtásának összetettsége bonyolultabbá** vált, **komplexitása fokozódott.**
- A szárazföldi haderő **alapvető komponensei** a – *légi szállításra is alkalmassá tett* – **lövészzászlóaljak** (esetlegesen: század harccsoportok), amelyek **könnyű lövész alegységeket**, **harci támogató** és **harci kiszolgáló csapatokat** foglalnak magukba. Fő funkciójuk, hogy **az ellenség egységei és alegységei ellen sikeres**, illetőleg **harcászati magasabbegységei ellen korlátozott eredményű harcot** folytassanak.
- **Háborús küszöb alatti** konfliktusok esetében a lövészzászlóaljak feladataikat **önállóan hajtják végre**. Ellenséges **támadás esetén** feladataikat **korlátozott ideig önállóan**, majd koalíciós összhaderőnemi kötelékben hajtják végre. Az önálló végrehajtás során feladataikat a **szokásos békefenntartó eljárásmódhoz hasonlóan** teljesítik. Szükség esetén, **ideiglenes jelleggel támadó** vagy **védelmi harcot** is folytathatnak.

2. Összegzés

2.1. Következtetések

A kutatás során megismert információkat **mérlegelve az alábbi következtetéseket vontuk le:**

- A honvédelem rendszerében, valamint a nemzeti haderő szerkezetében az elmúlt két évtized során mennyiségi és minőségi változások álltak be. A honvédelem és ezen belül a Magyar Honvédség stratégiai feladatrendszere több ízben módosult, illetőleg alakult át, amely napjainkra már konszolidáltnak tekinthető. A stratégiai feladatrendszerek (doktrínák) permanens módosulása, il-

letőleg hazai specifikumok miatt több szakterületen a korszerű hadviselés követelményeinek megfelelő technikai modernizáció nem, vagy csak részben zajlott le.

- Az NHíIR egészét tekintve mind a stratégiai elvárások és követelmények, mind a modernizációs programok megfogalmazódtak. A stacioner alrendszerek korszerűsítési programjait a szárazföldi haderőnemnél rendszeresített tábori alrendszerek nem követték. Az alrendszerben felhasznált technológia, valamint eljárásrend és metodika korszerűtlen. A visszavont, de az új stratégiai szabályozók megalkotása ellenére sem pótolt szakutasítások hiánya miatt a szolgálati ág több szintjén exlex állapot alakult ki.
- Az NHíIR tábori alrendszereiben tapasztalható működési anomáliák az idő előrehaladtával egyre mélyülő kompatibilitási és interoperabilitási problémaforrásokat jelentenek nem csak a koalíciós műveleteknél, hanem a hazai alkalmazás során is.
- Hazánk katonai doktrínája mind az önálló, mind a szövetségi keretekben végrehajtott *háborús* és *nem háborús* katonai műveletek során alapvetően egységszintű (legfeljebb harcászati-hadműveleti magasabbegység szintű) katonai szervezetek harcászati, vagy békefenntartó eljárásmód szerinti alkalmazását irányozza elő.

2.2. Megállapítások

A kutatásokkal kapcsolatos főbb megállapításaink:

- A tábori hírrendszer korszerűsítése elkerülhetetlen. Az NHíIR tábori alrendszerével kapcsolatos modernizációs programok továbbra is vontatottan haladnak, eredmény csak középtávon várható.
- Az exlex állapot ellenére a tábori hírrendszer továbbra is rendszerben van, amely során az alkalmazás – *többségében* – a korábbi eljárásrend alapján kerül megszervezésre és végrehajtásra.
- Megfontolás tárgyává célszerű tenni ágazati szabályozó(k) megalkotását annak érdekében, hogy a fennálló exlex helyzetből adódó szakmai bizonytalanságok feloldhatók legyenek.
- A teljes modernizációig terjedő átmeneti időszak hossza indokolttá teszi a tábori hírrendszer képességeinek új elvárásokhoz történő – *adott peremfeltételek melletti* – hozzáigazítását.

Felhasznált irodalom:

[1] Finszter Géza: A rendészeti rendszer alkotmányos és közjogi alapjai (2. számú előtanulmány az átfogó rendészeti stratégia társadalmi vitájához), Rendőrség Tudományos, Technológiai és Innovációs Tanácsa, Budapest, 16-17. oldal, 2008.

[2] Rajnai Zoltán: A tábori alaphírhálózat korszerűsítésének lehetőségei, „Kommunikáció 2000.” nemzetközi szakmai-tudományos konferencia, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 95. oldal, 2000. október 4.

[3] Magyar Honvédség Összhaderőnemi Doktrína 2. kiadás, Magyar Honvédség kiadványa, Budapest, Ált/27. szakutasítás, 45-60. oldal, 2007.

[4] Szöllősi Sándor: Konvergáló hálózatok fejlődési trendjei, a technikai alkalmazhatóság kérdései a Magyar Honvédség infokommunikációs rendszerében, dokto-

ri (PhD) értekezés, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 58. oldal, 2007.

[5] Fekete, Károly: Modelling the videoconference in mission, „Kommunikáció 2007.” nemzetközi szakmai-tudományos konferencia, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, ISBN 978-963-7060-31-1, 126. oldal, 2007. október 16.

PÁNDI Balázs – PÁNDI Erik[28]

AZ ALKALMAZHATÓSÁG HATÉKONYSÁGÁNAK NÖVELÉSE A TÁBORI HÍRRENDSZEREKBEN[29]

Absztrakt: A témakör kapcsán lefolytatott előzetes kutatások során behatárolásra kerültek azon használati módok és a hozzá szorosan köthető rendszerelemek, amelyek elektronizálása (gépesítése) elősegítheti a tábori hírrendszer vezetés-irányításának feszességét. E kívánalom teljesülése esetén, megítélésünk szerint a csapatvezetés és -irányítás operativitása is fokozható. Jelen közlemény összefoglalja az elektronizálás főbb mozzanatait.

Kulcsszavak: adatbázis, elektronizálás, vízesés modell.

Bevezetés

Előzetes kutatásaink alapján kijelenthető, hogy a harci okmányrendszer tekintetében a híradó és informatikai terv – *és azon belül meghatározott* – vázlatok célszoftver útján történő elektronizálása elősegítheti a tábori hírrendszer vezetés-irányításának feszességét, amelyen keresztül a csapatok vezetés-irányítási tevékenysége közelíthető az elvárásokban megfogalmazottakhoz. A célszoftver fejlesztése történhet a **vízesés modell** alapján. E megoldás a szoftverfejlesztésben legelterjedtebb felülről-lefelé történő fejlesztési metódus, amelynek lényege, hogy a felhasználói igényeket megfogalmazó specifikációból kiindulva, folyamatos finomítási lepéseken keresztül érhetünk el magához a megvalósított végtermékhez [1].

1. A modell kialakításának fő fázisai

A kialakítás lépései:

a) igényfelmérés;
b) tervezés;
c) megvalósítás;
d) kész termék kiértékelése;
e) karbantartás (esetlegesen).

1.1. Igényfelmérés

A **harci okmányrendszer** vizsgálata során megállapítottuk, hogy a vázlat és táblázat formájában megjeleníthető elemeket, összességében véve a **híradó és informatikai terv** elektronizálását célszerű valamely matematikai eljárás révén megvalósítani. Ennek keretében áttekintettük az érintett **harci okmányokat**,[30] vagyis meghatároztuk, specifikáltuk azok adattartalmát.

[28] Szerzők: Pándi Balázs (közgazdasági programozó matematikus, doktorjelölt), Gordon és Webster Tanácsadó ZRt.; Pándi Erik (PhD), ZMNE Híradó Tanszék.

[29] Jelen közlemény a Bolyai János Kutatási Ösztöndíj támogatásával készült.

[30] Vezetékes híradás vázlata; rádiórelé híradás vázlata; rádióhíradás vázlata; futár- és tábori posta járatok menetrendje.

1.2. Tervezés

A célszoftver megtervezése az **objektum-orientált tervezési módszer** alapján történt. Ennek lényege, hogy a program egyes elemei, azok adattagjai, eljárásai, eseményei és a köztük lévő kapcsolatok absztrakt, úgynevezett objektumként, a konkrét megvalósítástól függetlenül kerül reprezentálásra. E módszer segítségével az objektumokat különböző absztrakciós szintű sablonok, úgynevezett osztályok segítségével finomíthatjuk, csökkenthetjük a köztük felmerülő redundanciát, amely által hatékonyabbá tehetjük a program fejlesztését és magát a programot is. Az osztályok finomítási technikája, más néven specializáció,[31] szintén szemlélteti a korábban említett vízesés elméletet. A tervezés során az objektumorientált programtervezésben általánosan elterjedt UML modellezési szabványt alkalmaztuk, amely egy általános vizuális tervezési módszertant ad a szoftverfejlesztés számos fázisára, úgymint:

a) a felhasználói funkciókat modellező használati eset modellre;

b) a program nagyobb komponensei és az ezek együttműködését modellező komponens modellre;

c) az osztály és objektum modellre;

d) a konkrét működését modellező aktivitás modellre.

1.3. Megvalósítás

A felhasználói igényeket megfogalmazó specifikációból kiindulva, folyamatos finomítási lepéseken keresztül érkeztünk el az implementáció, a célszoftver megalkotásának fázisába.

1.3.1. Szoftverkörnyezet

A konkrét megvalósításhoz kiválasztott szoftverkörnyezet **a NATO-ban jelenleg standardnak tekinthető Microsoft Windows, és Office megoldások.** A Windows operációs rendszer alá történő fejlesztésben jelenleg szintén standardnak számító **Microsoft .NET** keretrendszer alatt, a szintén iparági standardnak számító, magas szintű objektum-orientált **C# nyelven zajlott** [2]. A **.NET keretrendszer használatának előnye**, hogy számos előre gyártott standard osztályt és komponenst tartalmaz, ami jelentősen meggyorsítja a fejlesztést, mivel ezek a funkcionalitását nem kell külön megvalósítani.

Az **adatbeviteli felülethez** a .NET keretrendszer **WindowsForms alrendszerét használtuk**, mivel ez számos kész adatbeviteli elemet és adattáblázati elemet tartalmaz [3]. A **jelentéskészítő** komponens által készített gráfok a .NET keretrendszer újabb változatának grafikus felhasználói interfész technológiája a **Windows Presentation Foundation (WPF)** segítségével kerültek megvalósításra, mivel itt az adatok és a grafikus elemek közötti kapcsolatot a rendszer beépítetten kezeli, továbbá lehetővé teszi a modell grafikus szerkesztésének lehetőségét egy továbbfejlesztett verzióban [4]. A **táblázatok html formátumban kerültek megvalósításra** mivel ez egy standard formátum, ami szerkeszthető **Microsoft Office alkalmazásokban,**[32] viszont a megjelenítéséhez elegendő lehet bármely internetes böngésző is.

[31] Származtatás, vagy öröklődés.

[32] Illetőleg akár közvetlenül, szövegesen is.

A **tábori hírrendszer modelljét tároló adatbázis technológiára** a konkrét példaalkalmazás a **Microsoft Access JET** adatbázisa volt, bár a szoftveralkalmazás tetszőleges standard **OLE DB protokollon keresztül elérhető adatbázist támogat**. A példában a választás azért esett a Microsoft Access JET adatbázisra, mivel ez Microsoft Office környezetben akár az alkalmazás nélkül is megnyitható, valamint lekérdezhető, illetve könnyen hordozható [5]. Gyakorlati tapasztalataink alapján, ehhez hasonló méretű adatbázisoknál akár tömörítés nélkül is továbbítható a tábori hírrendszer jelenlegi **n x 10 kbit/s** adatátviteli sávszélességű infrastruktúráján keresztül.

1.3.2. Tesztelés

A tesztelési fázis lényegében az adatbázisok kísérleti jellegű feltöltésével és a műveletek ellenőrzésével történt meg. A teszt során a különböző helyzetek modellezésére is sor került, többek között a feltételezett rombolások okán szükségessé váló átcsoportosításokból eredő, a tábori hírrendszer működését módosító szituációk.

1.3.2.1. Rendszerkövetelmények

A tesztek során kialakított tapasztalatok, illetőleg a levont következtetések alapján megfogalmazhatókká váltak a rendszer működtetésével összefüggő minimális műszaki-technikai feltételek, követelmények. Az elektronizált rendszer következő fő **hardverelemei** tekintetében kerültek elvárások megfogalmazásra:

a) processzor;
b) operációs rendszer;
c) memória;
d) merevlemez-terület;
e) monitor;
f) vizuális megjelenítő (nyomtató).

Processzor:

A célszoftver szoftver eredményes igénybevételéhez legalább **233 MHz órajelű processzor**[33] szükséges.

Operációs rendszer:

A célszoftver az alábbi operációs rendszereken üzemeltethető (futtatható) biztonságosan:

a) Microsoft Windows Vista;
b) Microsoft Windows XP;
c) Microsoft Windows Server 2003;
d) Microsoft Windows 2000 Service Pack 3 (SP3).[34]

Memória:

A szoftver érdemi, biztonságos alkalmazásához legalább **128 MB RAM** memória szükséges.

[33] Típusát tekintve lehet: Pentium.
[34] Avagy ezek fejlettebb (újabb) típusain, verzióin.

Merevlemez-terület:

A célszoftver **1-5 MB** szabad lemezterületet igényel az adatbázis méretétől, vagyis a katonai szervezet nagyságától függően.

Monitor:

Az érdemi alkalmazáshoz legalább **800x600 képpont felbontású, 256 szín megjelenítésére képes** Super VGA rendszerű monitorra lehet szükség.

Vizuális megjelenítő (nyomtató):

Lényegében véve bármilyen típus biztosítja a hagyományos, papíralapra történő vizuális megjelenítést.

1.4. A késztermék kiértékelése

A célszoftverbe sikeresen bevitelre és tárolásra került a híradás és informatika működési modellje. Ezt követően a szoftver rövid válaszidővel sikeresen előállította azon harci okmányokat, amelyek előzetesen kiválasztásra kerültek. E körülmények alapján, megítélésünk szerint a *„laborkörülmények”* közt elvégzett tesztet sikeresnek értékelhető.

1.5. Karbantartás

A karbantartás kérdései lényegében a továbbfejlesztés problematikáját foglalja magába, amelyet a következő alfejezetben fejtettünk ki.

2. Továbbfejlesztési lehetőségek

A kifejlesztett szoftver gyakorlatba történő bevezetése megköveteli mindazon fejlesztési lehetőségek előzetes meghatározását, amelyek a közép- és hosszútávú gyakorlati alkalmazást elősegíthetik. Megítélésünk és gyakorlati tapasztalataink alapján, három olyan terület sorolható fel előzetesen, amelyeken fejlesztési lehetőségek adódhatnak.

Grafikus modellezés, térinformatika:

A tábori hírrendszer modelljének grafikus tervezése a továbbfejlesztési lehetőségek első területe. Ennek az előfeltételeit megteremti a WPF technológia használata, amely megkönnyíti a grafikus felhasználói interakciókat. Ennek a továbbfejlesztési iránynak része lehet akár egy olyan térinformatikai fejlesztés is, amelynek segítségével a híradó- és informatikai főnökök a hírhálózatot a konkrét terepviszonyok szerint tudják megtervezni és elhelyezni egy digitális térképen.

A futár és tábori posta útvonalának optimalizálása:

Amennyiben a modell kiegészül, és az egyes alegységek közötti távolságok is feltüntetésre kerülnek, akkor további fejlesztési lehetőségek merülhetnek fel, úgymint a futár és tábori posta útvonalak optimalizálása. A körjáratok optimalizálása a számítástudományban jól ismert utazóügynök probléma[35] egyik fajtájának felel meg.

Ez a probléma bonyolultság elméletből közismerten az NP teljes komplexitási osztályba tartozik, ezért a globális optimum keresése jelenlegi tudásunk szerint nem oldható meg hatékonyan, azaz a probléma méretétől függően, polinomiális időben. Azonban kis állomásszám esetén[36] alkalmazhatók az operációkutatásban

[35] Travelling Salesman Problem (TSP).

[36] Hozzávetőleg 200 állomásig.

ismert branch-and-bound és lineáris programozási eljárások, illetve léteznek hatékony, azaz a P komplexitási osztályba tartozó heurisztikus algoritmusok, mint például a legközelebbi szomszéd[37] algoritmus, vagy a Lin-Kernighan algoritmus melyek közel optimális megoldást adnak nagy állomásszám[38] esetén is [6].

Automatikus újraszervezés és optimális erőforrás kihasználás:

A továbbfejlesztés során **a tábori hírrendszer szervezeti és technikai erőforrásaival való gazdálkodás nagyfokú automatizálása is megoldható lenne**. Ennek részét képezi, a hírhálózat újraszervezése esetleges meghibásodás vagy rombolás esetén, illetve a hálózat meglévő erőforrásainak optimális kihasználása az adatok optimális útvonalon történő továbbításával. A hírrendszer újratervezése során figyelembe vehetők az egyes korlátozó tényezők, például RFL listák is.

A hírhálózat újraszervezésére alkalmazható lehetne a gráfokban minimális feszítőfát meghatározó Kruskal, vagy Prim algoritmus. Az optimális útválasztásnál használható továbbá a számítógéphálózatok útvonal szervezésénél alkalmazott RIP[39] alapjául szolgáló Dijkstra illetve Bellman-Ford algoritmus [7].

3. Összegzés

Az előzetes kutatási részeredményekre támaszkodva behatároltuk azon *használati módot* és a hozzá szorosan köthető *rendszerelemeket*, amelyek elektronizálását tervezni lehet. Az elektronizálást jelentő célszoftver megalkotását a vízesés modell alapján végeztük el. Az igényfelméréstől kezdve a tervezésen, a megvalósításon, a kiértékelésen keresztül jutottunk el teljes végeredményig, majd ezt követően megfogalmaztuk a továbbfejlesztési lehetőségeket.

A célszoftver megtervezéséhez objektum-orientált tervezési módszert alkalmaztunk. A tervezés során az általánosan elterjedt UML modellezési szabványt alkalmaztuk, amely egy általános vizuális tervezési módszertant ad a szoftverfejlesztés számos fázisára. A konkrét megvalósításhoz kiválasztott szoftverkörnyezet a NATO-ban jelenleg alapszoftvernek tekinthető Microsoft Windows és Office megoldások. A Windows operációs rendszer alá történő fejlesztés a Microsoft .NET keretrendszer alatt, magas szintű objektum orientált C# nyelven zajlott. A tároló adatbázis technológiára a konkrét példaalkalmazás a Microsoft Access volt, bár az alkalmazás tetszőleges standard OLE DB protokollon keresztül elérhető adatbázist támogat. A konkrét példára eső választást a hírrendszer technikai elavultsága indokolta, mivel a generált adatbázis akár tömörítés nélkül is továbbítható a rendszeren.

A tesztelés az adatbázisok kísérleti jellegű feltöltésével és a műveletek ellenőrzésével történt meg. A teszt során a különböző helyzetek modellezésére is sor került, többek között a feltételezett rombolások okán szükségessé váló átcsoportosításokból eredő, a tábori hírrendszer működését módosító szituációk.

A rendszerkövetelményeket oly módon állítottuk össze, hogy azok a jelenlegi tábori hírrendszer által nyújtott technológiai környezetben is alkalmazhatók legyenek, vagyis a tervezés a *szükségszerű* és *elégséges* peremfeltételek mellett került

[37] Nearest Neighbour (NN).
[38] Akár több százezer.
[39] Routing Information Protocol.

végrehajtásra. A kifejlesztett szoftver gyakorlatba történő bevezetése megköveteli mindazon fejlesztési lehetőségek előzetes meghatározását, amelyek a közép- és hosszútávú gyakorlati alkalmazást elősegíthetik. Megítélésünk és gyakorlati tapasztalataink alapján a grafikus modellezés, térinformatika, az útvonal optimalizálás, valamint az automatikus újraszervezés és optimális erőforrás kihasználás területén lehetséges a továbbfejlesztési lehetőségek irányait keresni.

Felhasznált irodalom:

[1] Royce, Winston W.: Managing the development of large software systems, Proceedings of IEEE WESCON 26, 328-338. oldal, 1970.

[2] Liberty, Jesse – Xie, Donald: Programming C Sharp 3.0 5th edition, O'Reilly, ISBN 10-0-596-52743-8, 3-6. oldal, 2007.

[3] Griffiths, Ian – Adams, Matthew: .NET Windows Forms in a nutshell, O'Reilly, ISBN 0-596-00338-2, 3. oldal, 2003.

[4] Andrade, Chris – Livermore, Shwan – Meyers, Mike – Van Vliet, Scott: Professional WPF Programming, .NET Development with the Windows Presentation Foundation, WROX, ISBN 978-0-470-04180-2, 3. oldal. 2007.

[5] Roman, Steven: Access Database Design & Programming 3rd Edition, O'Reilly, ISBN 0-596-00273-4, 126-129 oldal, 2002.

[6] Applegate, D.L. – Bixby, R.E. – Chvátal, V. – Cook, W.J.: The Traveling Salesman Problem, A Computational Study, Princeton University Press, ISBN 978-0-691-12993-8, 373-469. oldal, 2006.

[7] Cormne, Thomas H. – Leiseron, Charles E. – Rivest, Ronald L. – Stein, Clifford: Introduction to Algorithms, Second Edition, MIT Press and McGraw-Hill, ISBN 0-262-03293-7, 561-643. oldal, 2001.

PÁNDI Balázs – PÁNDI Erik[40]

A KOMMUNIKÁCIÓ HATÉKONYSÁGÁT EMELŐ CÉLSZOFTVER GYAKORLATI MEGTERVEZÉSE[41]

Absztrakt: A tábori hírrendszer kapcsán végzett előzetes kutatásaink alapján megállapítottuk, hogy a jelenlegi elavult technikai rendszer működési hatékonysága javítható – egyúttal alkalmazási kockázata csökkenthető – a harci okmányrendszerek egyes elemeinek elektronizálásával. A célszoftver megalkotása a vízesés modell alapján történt. Jelen közlemény a tervezés fázisait mutatja be.

Kulcsszavak: adatbázis, elektronizálás, objektum-orientált tervezési módszer, vízesés modell, UML modellezési szabvány.

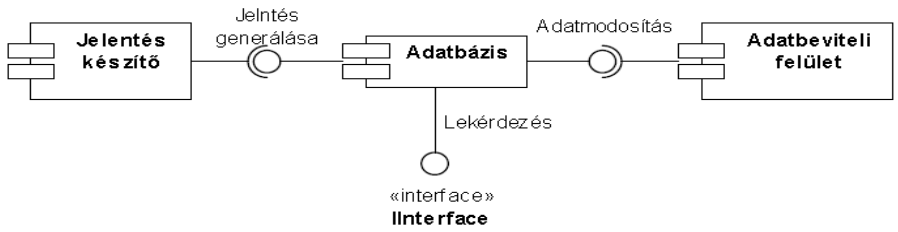
Bevezetés

A célszoftver megtervezése az **objektum-orientált tervezési módszer** alapján történt. A tervezés során az objektumorientált programtervezésben általánosan elterjedt UML modellezési szabványt alkalmaztuk, amely egy általános vizuális tervezési módszertant ad a szoftverfejlesztés számos fázisára [1].

1. Tervezés

A célszoftver alapvetően három fő részre, avagy komponensre bontható az alábbi megfontolások szerint:

a) adatbázis réteg;
b) adatbeviteli felület;
c) jelentéskészítő.



1. számú ábra: a komponens modell (készítette: Pándi Balázs)

1.1. Adatbázis réteg

A modellből látható, hogy a szoftver fő eleme az adatbázis réteg, amelynek feladata egyrészt a tábori hírrendszer modelljének tárolása, másodrészt biztosítania kell, hogy az lekérdezhető legyen külső programok részére, illetőleg elérhető legyen a többi komponens számára.

[40] Szerzők: Pándi Balázs (közgazdasági programozó matematikus, doktorjelölt), Gordon és Webster Tanácsadó ZRt.; Pándi Erik (PhD), ZMNE Híradó Tanszék.

[41] Jelen közlemény a Bolyai János Kutatási Ösztöndíj támogatásával készült.

1.2. Felhasználói felület

Az adatbázisréteghez kapcsolódik a felhasználói vagy adatbeviteli felület, amelynek célja, hogy a híradó és informatikai főnök ezen keresztül, általános számítógép-felhasználói ismeretek birtokában tudja mosósítani a tábori hírrendszer modelljét.

1.3. Jelentéskészítő

A jelentéskészítő rész célja egyértelmű, fő feladata, hogy az adatbázisban tárolt tábori hírrendszer modellje alapján automatizáltan generálja a harci okmányrendszer elemeit, vagyis a híradó és informatikai tervhez kötődő harci okmányokat.

1.4. A tábori hírrendszer modellje

Tekintettel arra, hogy a dandár híradó és informatikai főnöke vázlatokat összevontan is készíthet, ezért az általunk kialakított modell a következő három részből tevődik össze:

a) a rádióhíradás modellje;
b) a rádiórelé és vezetékes híradás modellje;
c) a futár és tábori posta híradás (járatok menetrendje) modellje.

A teljes modell az egyes modellrészletek folyamatos bővítésén keresztül kerül bemutatásra.

1.4.1. Rádióhíradás modellje

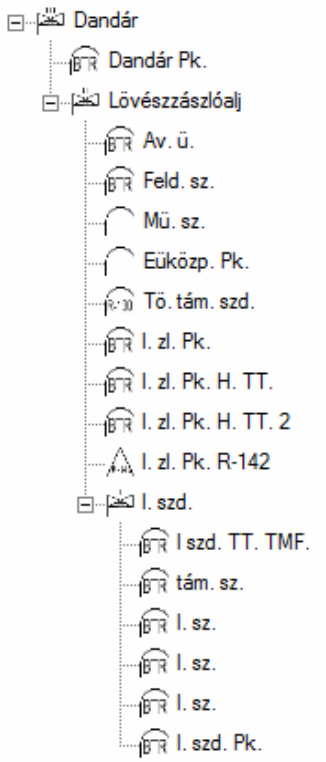
A rádióhíradás modelljét, mint matematikai rendszert természetesen elemek alkotják a következők szerint:

a) törzsek, egységek és alegységek;
b) rádiókészülékek (berendezések);
c) rádió irányok és rádióhálók (rádiócsatornák);
d) személyi állomány (egyes harcosok, csoportok);
e) rádiós kapcsolatok.

Törzsek, egységek, alegységek:

A tábori hírrendszerbe integrált törzsek, egységek, alegységek hierarchikus szervezete. A szervezeti hierarchia csúcsán elhelyezkedő dandártörzstől a hierarchia alján lévő egyes szakaszoknál található híradó komplexumokig, illetőleg egyes eszközökig terjed. A szervezeti felépítés több módon is modellezhető, mint például szervezeti fával[42], illetve egy úgynevezett szülő-gyermek táblázattal, amelyben minden egyes szervezeti egység esetében feltüntetésre került azon elöljáró törzs, amelynek alárendeltségében végrehajtja a katonai műveletek során jelentkező feladatait. Az általunk kialakított modellben mindkét megoldás lényegében megvalósításra került.

[42] Organogram.



2. számú ábra: a szervezeti egységek organogram útján történő megjelenítésének egy változata (készítette: Pándi Balázs)

Rádiókészülékek (berendezések):

Az egyes alegységek[43] harcjárműveiben, harci eszközeibe telepített, illetve az egyes harcos katonák részére speciális igénybevételre kiadott rádiókészülékek számos tulajdonsága feltüntethető a modellben, többek között harci-technikai, illetőleg logisztikai jellegű adatok.

Rádió irányok és rádióhálók (rádiócsatornák):

Az előre meghatározott rádió irányok és rádióhálók tulajdonságai feltüntethetők a modellben, úgymint adás-vételi frekvenciák, üzemmódok, egyéb műszaki-technikai adatok.

Személyi állomány (egyes harcosok, csoportok):

Az egyes szervezeti egységeknél szolgálatban lévő harci állomány egyes tagjai, illetőleg minden tagja a modell részét képezhetik. A személyi állomány adatai, mint például név, rendfokozat, azonosító, illetve egyéb kapcsolódó adatok is szerepelhetnek a modellben.

Rádiós kapcsolatok:

Az egyes szervezeti egységek kapcsolatait összegzi az egyes rádiócsatornákhoz rendelt rádióeszközök révén. Egy rádió alapértelmezésben egy rádiócsatornához

[43] Századok, ütegek, szakaszok, illetve rajok.

csatlakozik, azonban a modell több opcionális kapcsolatot is lehetővé tesz. A kapcsolatok szintén több módon reprezentálhatók, úgymint:

a) kapcsolati listával (amely a kapcsolódó rádiókat és csatornákat sorolja fel);

b) kapcsolati mátrixszal;

c) gráffal.

Az általunk kialakított modellben – *célszerűségi megfontolásokból* – a kapcsolati lista, valamint a kapcsolati mátrix reprezentáció került kidolgozásra.

A rádióhíradás matematikai modellje:

A **rádióhíradás modellje** és a reá vonatkozó szabályok egzakt módon definiálhatók a következőkben kidolgozott **matematikai modell** segítségével.

A modell egy páros gráffal reprezentálható. Legyen R véges halmaz a rádiók halmaza, $V \subseteq \wp$ (R) véges halmaz a rádiócsatornák halmaza, K véges halmaz a személyi állomány halmaza. $A \subseteq \wp(R) \times \wp(K)$ véges halmaz a törzsek, egységek és alegységek halmaza.

$R \cup V$ a gráf csúcsainak halmaza. 3.1.

$VR = VRA \cup VRO$ az élek, azaz a vonalak és rádióeszközök (berendezések) közötti kapcsolatok halmaza, ahol:

$VRA = \{(x, Y) : Y \in V, x \in R, x \in Y\}$ az alapértelmezett kapcsolatok halmaza, 3.2.

$VRO = \{(x, Z) : Z \in V, x \in R, x \in Z\}$ az opcionális kapcsolatok halmaza. 3.3.

A gráf csúcsaira a következő feltételek teljesülnek:

$K \cap A = \varnothing$, $V \cap A = \varnothing$, $V \cap K = \varnothing$, $R \cap K = \varnothing$ azaz a törzsek, egységek, alegység, rádióeszközök, rádiócsatornák és személyi állomány különállóak. 3.4.

$(R1,K1) \in A$, $(R2,K2) \in A$, $R1 \cap R2 = \varnothing$, $K1 \cap K2 = \varnothing \Rightarrow (R1 \cup R2, K1 \cup K2) \in A$, azaz két különböző törzsnek, egységnek, alegységnek létezik közös fő törzse, egysége, alegysége, vagyis a törzs, egység, alegység hierarchikus szerkezetűek. 3.5.

A gráf éleire következő feltételek teljesülnek:

$(x, Y) \in VRA$, $(x, Z) \in VRA \Rightarrow Y = Z$, azaz egy rádióeszköz alapértelmezetten csak egy rádiócsatornához kapcsolódhat. 3.6.

Amennyiben, a fentiekben vázolt modellben a rádióeszközöket tetszőleges vezetékes vagy vezetéknélküli készülék (rádió- vagy rádiórelé eszköz) egy csatornájaként és a vonalakat tetszőleges vezetékes vagy vezetéknélküli csatornaként, illetőleg vonalként kezeljük (fogjuk fel), úgy **a modell alkalmas lehet a teljes tábori hírrendszer modellezésére is**. Abban az esetben, amennyiben a modell e módszer

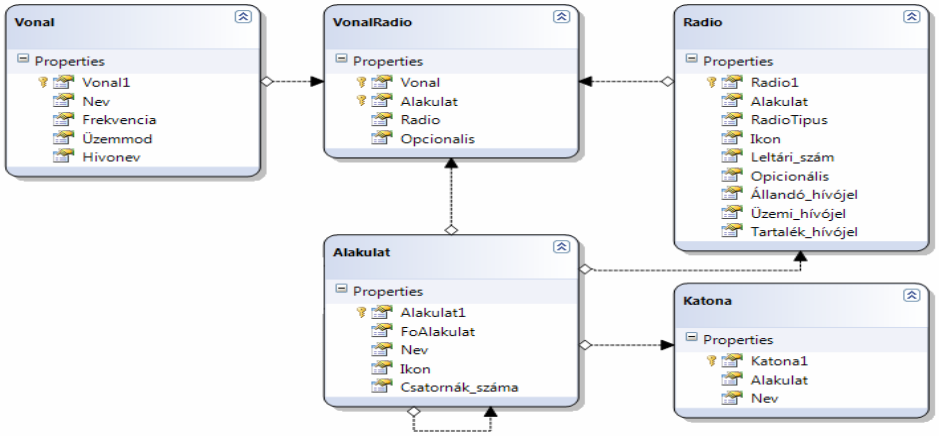
szerint kerülne kialakításra, úgy – *megítélésünk szerint* – olyan végeredményre juthatunk, amely túlzottan is általánosítana, egyúttal nem használná ki a rádiórelé és vezetékes híradás, illetve a futár és tábori posta híradás (járatok menetrendje) elemeinek speciális tulajdonságait. Előzőek alapján és okán a modellt ezért kiegészítettem új modell elemekkel, úgymint:

a) a rádiórelé és vezetékes híradás,

b) a futár és tábori posta híradás (járatok menetrendje) elemeivel.

Rádióhíradás osztály modellje:

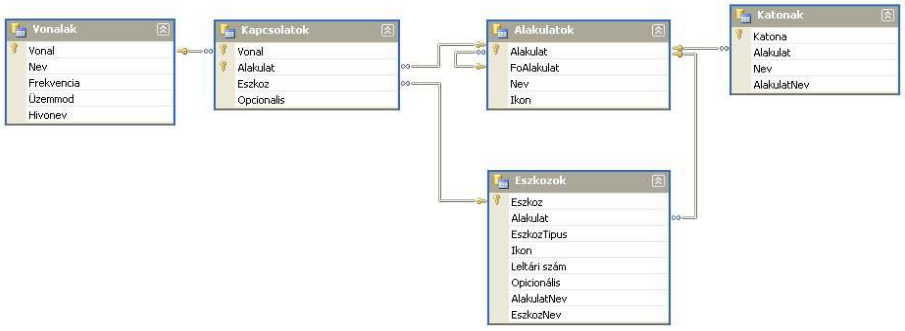
A korábbiakban megfogalmazottak alapján, a fejlesztés következő fázisát, a rádióhíradás osztálymodelljét a következő UML szabvány szerint diagrammal lehetséges reprezentálni:



3. számú ábra: a rádióhíradás osztály modellje (készítette: Pándi Balázs)

Rádióhíradás adatbázis modellje:

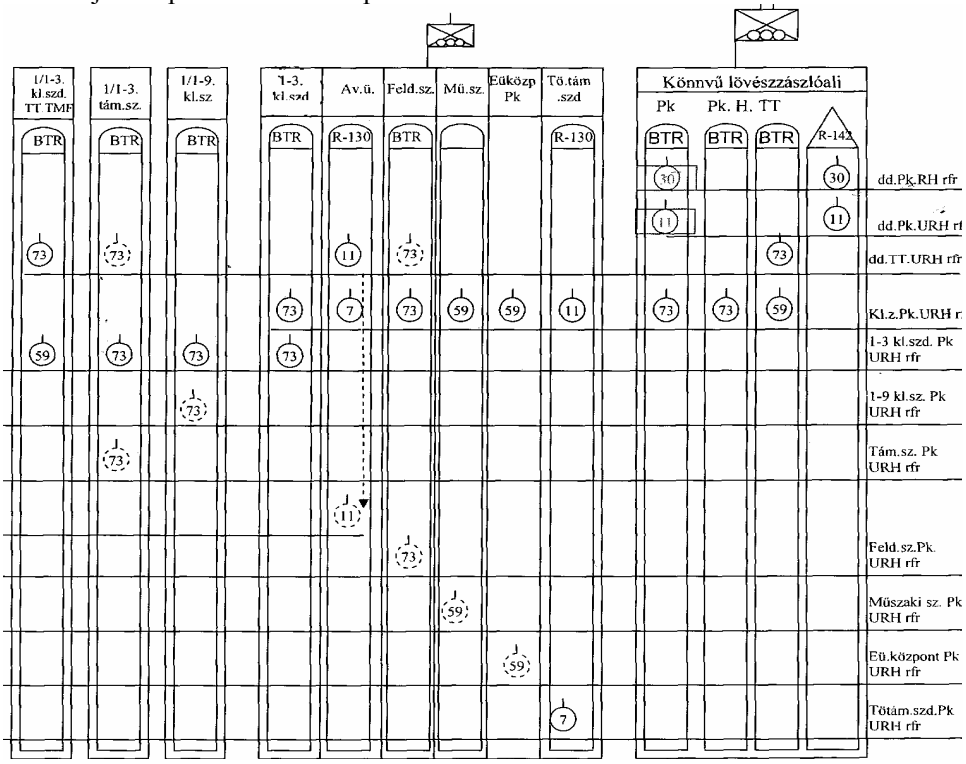
A fenti, absztrakt objektummodell könnyen megvalósítható az alábbi relációs adatbázis sémával:



4. számú ábra: a rádióhíradás adatbázis modellje (készítette: Pándi Balázs)

Ez a reprezentáció talán azért célszerű, mivel kellőképpen rugalmas a változások karbantartásához, új szervezeti egységek egyszerű felvételéhez, valamint **rombolások hatásainak szimulálásához**, illetve alkalmas nagymennyiségű kapcsolódó adat tárolására, úgymint a tábori hírrendszer egyes pontjain szolgálatot ellátó

egyes szolgálati személyek és azok adatainak tárolására. A relációs adatbázis sémában a törzsek, egységek, alegységek szervezeti felépítésének modellezése szülő-gyerek táblázat reprezentációval történik, ami alapján előállítható a szervezeti modellezésnél gyakran használt szervezeti fa reprezentáció is. A kapcsolatok modellezése az adatbázis sémában kapcsolati lista reprezentációval történik. A táblában szereplő opcionális mező azt jelöli, hogy az adott kapcsolat alapértelmezett-e avagy opcionális. Mindezek alapján, szintén előállítható a rádióhíradás ábrázolásánál elterjedt kapcsolati mátrix reprezentáció:



5. számú ábra: a rádióhíradás kapcsolati mátrix reprezentációjának egy változata (forrás: Dr. Sándor Miklós – Farkas Tibor, ZMNE Híradó Tanszék) [2]

1.4.2. Rádiórelé és vezetékes híradás modellje

Korábbiakban rögzítettek alapján a rádiórelé és vezetékes híradás kérdéseit a tervezési folyamat során összevontan kezeltük.

Rádiórelé és vezetékes híradás modelljének elemei:

A rádióhíradás modelljében szereplő szervezeti egységeket kiegészítettük a harcászati-hadműveleti magasabbegységnél rendszeresített **rádiórelé eszközök**, valamint **vezetékes eszközök** által biztosított **csatornák és vonalakkal**. A rádiórelé eszközök az esetek meghatározó részében félkészletenként kerültek telepítésre. Egy félkészletnek adott számú rádiórelé csatornája van, amelyeket az elöljáró, vagy alárendelt vezetés-irányítási törzsek vezetékes (esetlegesen: rádiós) eszközeinek egyes vonalaihoz lehet csatlakoztatni. A kapcsolat üzemmódja (távbeszélő, fax, esetenként még: géptávíró) szintén a modell részét képezi. A

félkészletek vezetéknélküli összeköttetésen keresztül kapcsolódhatnak egy másik egység, alegység félkészletéhez, továbbítva a hozzácsatlakozatott vezetékes (vagy rádió) eszközök jeleit. A modellben ezt **rádiórelék közötti vezetéknélküli (rádiós) kapcsolatnak** nevezetem el. Egy másik lehetséges mód a félkészletek csatlakoztatására az úgynevezett **átjátszás**, amely processzus során az adott egységnél, alegységnél rendszeresített két félkészlet a vezetékes kapcsolatokon keresztül kerül összekapcsolásra. Ennek révén a rádiórelék közötti vezetéknélküli kapcsolat átjátszható másik félkészlet irányába. A modellben ezt **rádiórelék közötti vezetékes kapcsolatnak** fogtam fel. A **vezetékes híradás modelljében** vezetékes eszközök kapcsolódhatnak más vezetékes eszközökhöz megadott csatornákon, vagy vezetékes kapcsolaton keresztül. A kapcsolat üzemmódja (távbeszélő, fax, illetőleg géptávíró) szintén a modell részét képezi.

Rádiórelé és vezetékes híradás matematikai modellje:

A rádióhíradás matematikai modelljében felvázolt gráf modellt kiegészítjük a következő elemekkel. Legyen $CS \subseteq \mathbb{N}$ a csatornák halmaza, ahol $\mathbb{N}$ a természetes számok halmaza.

Legyen T = {„R”, „RO”„V”} a relé-relé kapcsolat típusainak halmaza (rádiós, opcionális rádiós, vezetékes).

Legyen továbbá $RE \subseteq \wp(CS)$ véges halmaz a rádiórelék halmaza.

A modellben szereplő törzsek, egységek alegységek kiegészülnek a rádiórelékkel és a vezetékes csatornákkal: $A \subseteq \wp(R) \times \wp(K) \times \wp(RE) \times \wp(CS)$.

A csúcsok halmaza ezek után $R \cup V \cup RE$ lesz. 3.7.

Az élek halmaza pedig $VR \cup RV \cup RR \cup VV$ lesz ahol:

$RV = \{(re, rcs, a, vcs) : re \in RE, rcs \in CS, rcs \in RE, a = (ar, ak, are, acs) \in A, vcs \in CS, vcs \in acs, re \notin are\}$ a relé-vezetékes kapcsolatok halmaza 3.8.

$RR = \{(re_1, re_2, t) : re_1 \in RE, re_2 \in RE, t \in T\}$ a relé-relé kapcsolatok halmaza 3.9.

$VV = \{(a_1 , cs_1 , a_2 , cs_2) : a_1 = (ar_1, ak_1, are_1, acs_1) \in A, cs_1 \in CS, cs_1 \in acs_1, a_2 = (ar_2, ak_2, are_2, acs_2) \in A, cs_2 \in CS, cs_2 \in acs_2, a_1 \neq a_2\}$ a vezetékes kapcsolatok halmaza 3.10.

A gráf csúcsaira a következő feltételek teljesülnek:

$CS \cap A = \varnothing$, $CS \cap K = \varnothing$, $CS \cap R = \varnothing$, $A \cap RE = \varnothing$, $R \cap RE = \varnothing$, $K \cap RE = \varnothing$, $V \cap RE = \varnothing$ azaz a törzsek, egységek, alegységek, rádióeszközök (berendezések), vonalak, személyi állomány, csatornák, relék különállóak 3.11.

A gráf éleire következő feltételek teljesülnek:

$(re, rcs, a_1, vcs_1) \in RV, (re, rcs, a_2, vcs_2) \in RV \Rightarrow a_1 = a_2$, $vcs_1 = vcs_2$, azaz egy rádiórelé egy vezetékes csatornán csak egy vezetékes eszközhöz csatlakozhat 3.12.

$(re_1, rcs_1, a, vcs) \in RV, (re_2, rcs_2, a, vcs) \in RV \Rightarrow re_1 = re_2$, $rcs_1 = rcs_2$, azaz egy törzs, egység, alegység egy vezetékes csatornán csak egy rádióreléhez csatlakozhat 3.13.

$(re_1, re_2, t) \in RR \Rightarrow (re_1, re_3, t) \notin RR$ vagy t = „RO” illetve $(re_2, re_1, t) \in RR \Rightarrow (re_3, re_1, t) \notin RR$ vagy t = „RO”, azaz egy relé ugyanolyan nem opcionális módon legfeljebb egy reléhez csatlakozhat 3.14.

$(re_1, re_2,$ „V”$) \in RR \Rightarrow a = (ar, ak, are, acs) \in A, re_1, re_2 \in are$, azaz vezetékes kapcsolat csak azonos törzsnél, egységnél, alegységnél lévő relék között lehet 3.15.

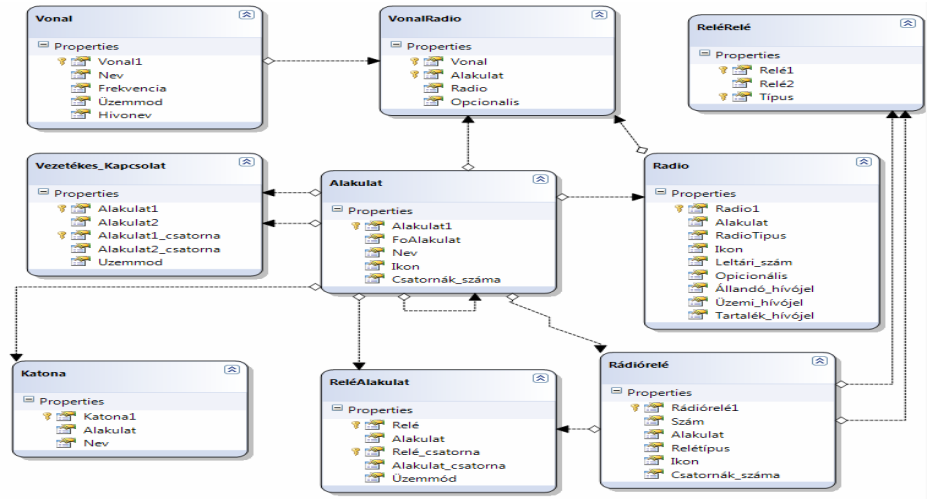
$((a , cs , a_1 , cs_1) \in VV, (a , cs , a_2 , cs_2))$ vagy $((a_1 , cs_1 , a , cs) \in VV, (a_2 , cs_2 , a , cs)) \in VV \Rightarrow a_1 = a_2 , cs_1 = cs_2$, azaz egy törzs, egység, alegység egy vezetékes csatornán csak egy vezetékes eszközhöz csatlakozhat 3.16.

$(re, rcs, a, vcs) \in RV \Rightarrow ((re, re_2,$ „V”$) \notin RR, (re_2, re,$ „V”$) \notin RR)$ illetve $((re, re_2,$ „V”$) \in RR$ vagy $(re_2, re,$ „V”$) \in RR) \Rightarrow (re, rcs, a, vcs) \notin RV$, azaz egy relé vagy vezetékes eszközökhöz, vagy másik relén kapcsolódik másik reléhez 3.17.

$((re, rcs, a, vcs) \in RV$ vagy $(re, re_2,$ „V”$) \in RR$ vagy $(re_2, re,$ „V”$) \in RR) \Rightarrow ((a, vcs, a_2, vcs_2) \notin VV, (a_2, vcs_2, a, vcs,) \notin VV)$, illetve $((a, vcs, a_2, vcs_2) \in VV$ vagy $(a_2, vcs_2, a, vcs,) \in VV) \Rightarrow ((re, rcs, a, vcs) \notin RV, (re, re_2,$ „V”$) \notin RR, (re_2, re,$ „V”$) \notin RR)$, azaz egy vezetékes eszköz, vagy egy másik vezetékes eszközhöz, vagy egy reléhez csatlakozik. 3.18.

Rádiórelé és vezetékes híradás osztály modellje:

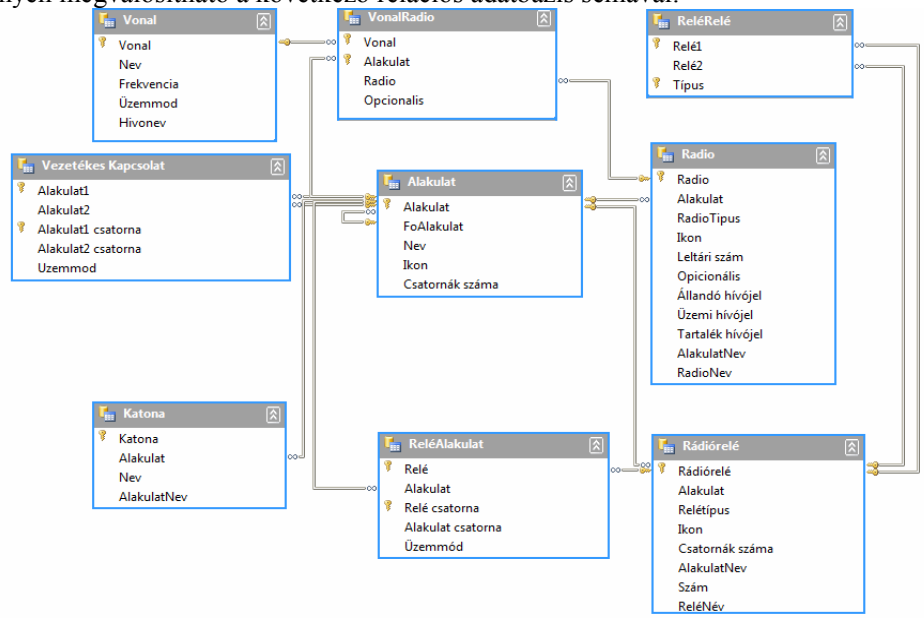
Az előző alfejezetekben rögzítettek szerint, a fejlesztés újabb fázisát, a rádiórelé és vezetékes híradás osztálymodelljét az alábbiak szerint lehetséges feltüntetni:



6. számú ábra: a rádiórelé és vezetékes híradás osztály modellje (készítette: Pándi Balázs)

Rádiórelé és vezetékes híradás adatbázis modellje:

Hasonlatosan a rádióhíradás kérdésköréhez, az absztrakt objektummodell könnyen megvalósítható a következő relációs adatbázis sémával:



7. számú ábra: a rádiórelé és vezetékes híradás adatbázis modellje (készítette: Pándi Balázs)

1.4.3. Futár és tábori posta híradás (járatok menetrendje) modellje

A híradó és informatikai terv utolsó elemként – *az előző megoldások analógiájára építve* – a futár és tábori posta járatok menetrendjével kapcsolatos modell felállítására került sor.

Futár és tábori posta híradás modelljének elemei:

A futár és tábori posta híradás elmélete és gyakorlata lényegesen kisebb matematikai problémát jelent. A második fejezetben rögzített vizsgálati részeredmények alapján a híradás ezen vállfajának megszervezése során az úgynevezett irányjárattal, vagy körjárattal kell számolni. Az irányjárat során a futár a kiindulópontból bejárja az egység, alegységek törzseit, illetve meghatározott szervezeti egységeit, úgy hogy minden állomás érintése után visszatér a kiindulópontba. A körjárat során a futár körbejárja a számára meghatározott szervezeti egységeken kialakított állomásokat, majd visszatér a főharcálláspontra.

Futár és tábori posta híradás modelljének matematikai modellje:

A korábbi modell kiegészül az irány- és körjáratok útvonalával. Az útvonalalak irányított gráf formájában reprezentálhatók.

A csúcsok a törzsek, egységek, alegységek: $A \subseteq \wp(R) \times \wp(K) \times \wp(RE) \times \wp(CS)$. 3.19.

Az élek pedig $VR \cup RV \cup RR \cup VV \cup KJ \cup IJ$, ahol:

$KJ = \{ (a_1, a_2) : a_1, a_2 \in A\}$ a körjárat útszakaszai, 3.20.

$IJ = \{ (a_1, a_2) : a_1, a_2 \in A\}$ az irányjárat útszakaszai 3.21.

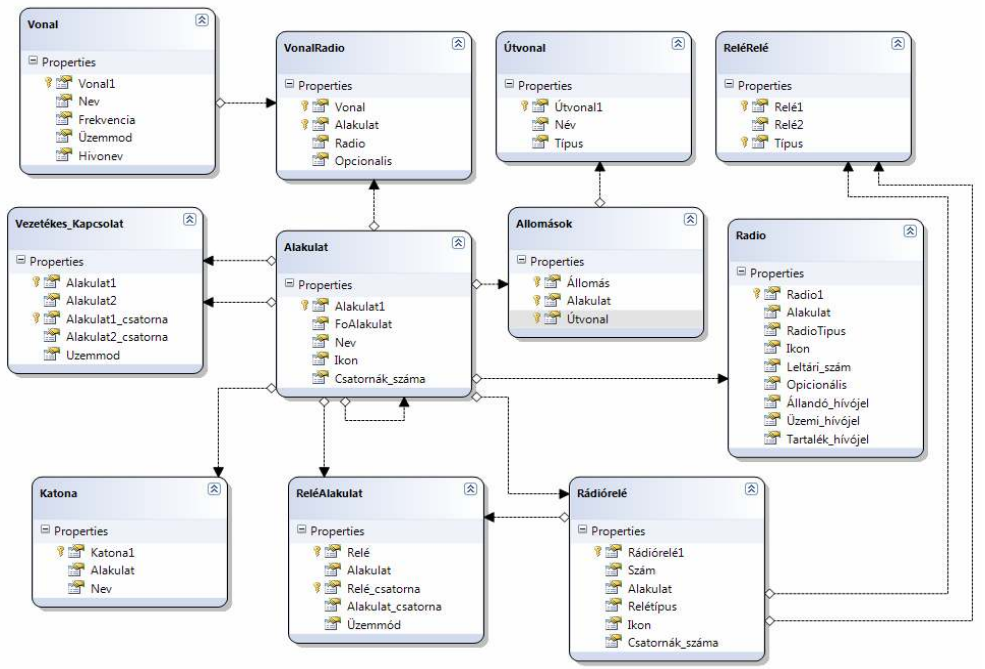
A gráf éleire a következő további feltételek vonatkoznak:

$KJ = \{(a_{10}, a_{11}), \ldots (a_{1n}, a_{10}) : a_{10} \neq \ldots \neq a_{1n} \} \cup \ldots \cup \{(a_{m0}, a_{m1}), \ldots (a_{mk}, a_{m0}) : a_{m0} \neq \ldots \neq a_{mk}\}$ 3.22.

$IJ = \{(a_{10}, a_{11}), (a_{11}, a_{10}), \ldots (a_{10}, a_{1n}), (a_{1n}, a_{10}), : a_{10} \neq \ldots \neq a_{1n} \} \cup \ldots \cup \{(a_{m0}, a_{m1}), (a_{m1}, a_{m0}), \ldots (a_{m0}, a_{mk}) , (a_{mk}, a_{m0}) : a_{m0} \neq \ldots \neq a_{mk}\}$ 3.23.

Futár és tábori posta híradás osztály modellje:

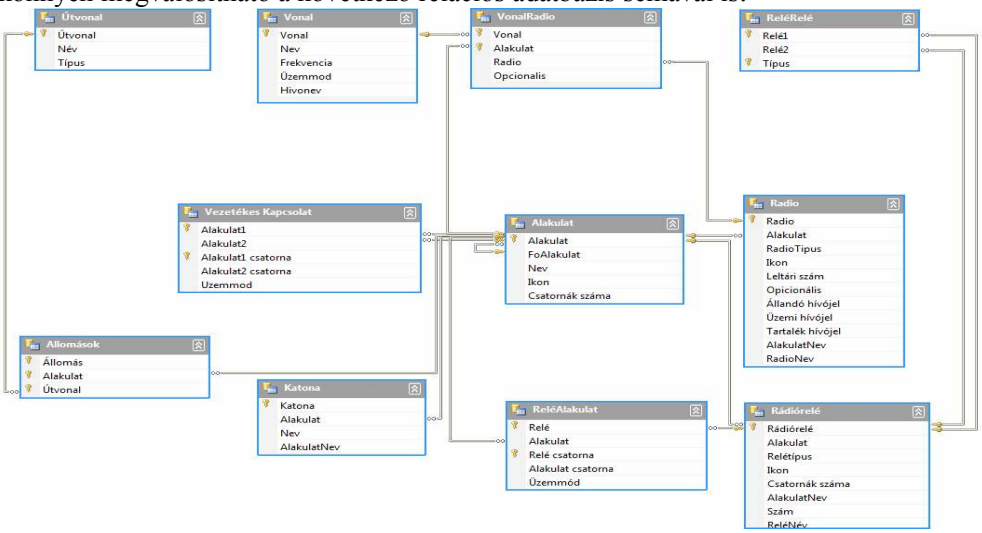
Az előzőekben megállapítottak szellemében, a fejlesztés következő fázisát, a futár és tábori posta híradás (járatok menetrendje) osztály modellje az alábbiak szerint rajzolható fel:



8. számú ábra: futár és tábori posta híradás (járatok menetrendje) osztály modellje (készítette: Pándi Balázs)

Futár és tábori posta híradás modelljének adatbázis modellje

Hasonlatosan az előző adatbázis modellekhez, fenti absztrakt objektummodell könnyen megvalósítható a következő relációs adatbázis sémával is:



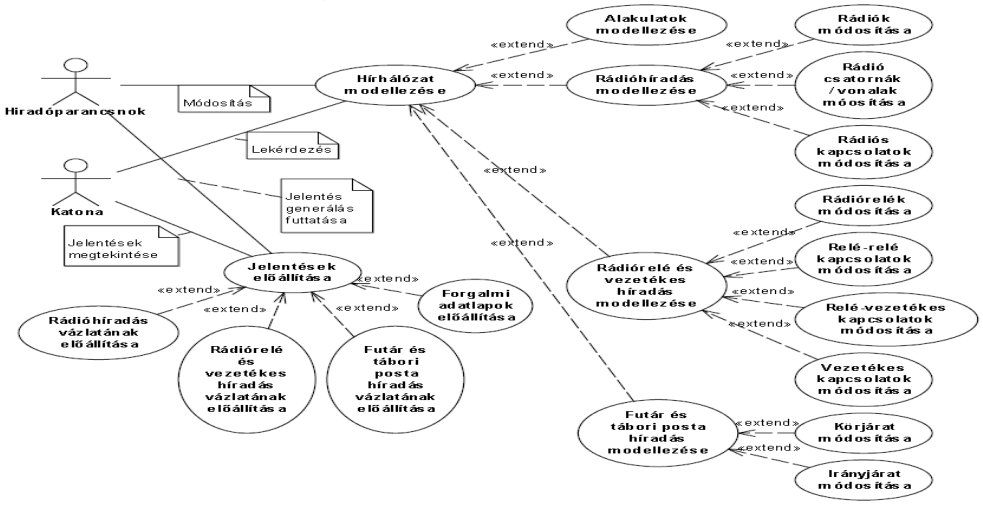
9. számú ábra: futár és tábori posta híradás (járatok menetrendje) adatbázis modellje (készítette: Pándi Balázs)

2. Működés

A célszoftver révén igénybe vehető funkciókat az UML szabvány által definiált **használati eset modell** segítségével, használatának munkafolyamatát az **aktivitás modell** segítségével modellezhetjük.

2.1. Használati eset modell

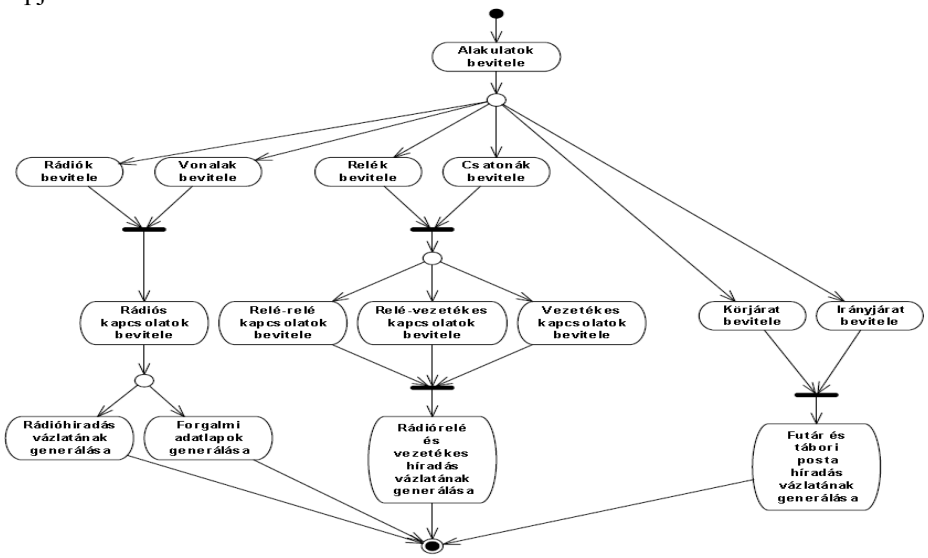
Az esetmodell grafikus megjelenítésére alapvetően a következőkben összegzett – *UML 2.0. szabványnak megfelelő* – ábra állítható fel:



10. számú ábra: a célszoftver használati eset modellje (készítette: Pándi Balázs)

2.2. Aktivitás modell

A modell felrajzolására összességében véve az alábbiak szerint részletezettek alapján kerülhet sor:



11. számú ábra: a célszoftver aktivitás modellje (készítette: Pándi Balázs)

Összegzés

A kutatás végrehajtásával, illetőleg jelen közleményben leírtakat mérlegelve az alábbi következtetéseket vontuk le:

1) A tábori hírrendszer elavult technológiájára való tekintettel olyan célszoftver megalkotását kellett tervbe venni, amelynek használatakor a hardverigény minimális. Az objektumorientált tervezési módszer vízesés modell alapján történő alkalmazása célravezető, amelynek keretében az UML modellezési szabvány révén a szoftver megalkotható.

2) A hardverigény optimalizálása mellett szükségszerű a célszoftvert oly módon megalkotni, hogy az a szakállomány részére rövid idő alatt elsajátítható, illetőleg harci alkalmazás során könnyen kezelhető legyen. Erre a célra a NATO-ban jelenleg standardnak tekinthető Microsoft Windows és Office megoldások jelentik a megfelelő szoftverkörnyezetet.

3) A célszoftver – *esetleges* – középtávú alkalmazása megköveteli a továbbfejlesztés irányainak meghatározását.

A kutatásokkal kapcsolatos főbb megállapításaink:

1) A célszoftver egyszerűsége, optimális erőforrásigénye révén az egyes harci okmányok elektronizációja megvalósítható.

2) Az elektronizáció révén elősegíthető a tábori hírrendszer vezetés-irányítási tevékenysége hatékonyságának emelése.

Felhasznált irodalom:

[1] Alhir, Sinan Si: UML in a Nutshell, ISBN 1-56592-448-7, 71-107. oldal, 1998.

[2] Sándor Miklós – Farkas Tibor: A lövészdandár híradása, egyetemi jegyzet, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 36. oldal, 2008.

PRISZNYÁK Szabolcs – PÁNDI Erik – FARKAS Tibor[44]
AZ INFORMÁCIÓTECHNOLÓGIAI RENDSZER VESZÉLYEZTETETTSÉGI KÉRDÉSEI A RENDVÉDELEM TERÜLETÉN[45]

Absztrakt: Jelen közleményben a szerzők a Rendőrség integrált információtechnológiai ágazata kialakulása műszaki-technikai és egyéb aspektusainak vizsgálatának markáns eredményeit teszik közzé. Ezeken a területeken tett megállapítások alapján feldolgozzák az ágazatot érintő veszélyeztetettség néhány kérdését.

Kulcsszavak: határőrség, információtechnológia, informatika, konvergencia, rendőrség, távközlés.

1. Előfelvetés

A rendőrség integrált informatikai szervezetével kapcsolatos műszaki kérdéseket úgy érdemes vizsgálni, hogy előtte mindkét jogelőd szervezet informatikai műszaki felépítését, fejlődését célszerű bemutatni. A műszaki területet informatika tekintetében sokféleképp felbontható, de véleményünk szerint három önálló részre célszerű bontani, a vezetékes távközlésre (kommunikációra), a vezeték nélküli kommunikációra, és a számítástechnikára. Természetesen ez a három terület mára – legalábbis eszköz, és technológia szinten mindenképpen – konvergálódott, hiszen ma már nem beszélhetünk telefonvonalról, vagy számítógép hálózatról, mert az adat-, és beszédtovábbítás integrált formában IP alapon történik. Ma már minden távbeszélő központ számítógép. A rádiórendszerek is digitális alapon, számítógéppel vezérelve működnek. Egy olyan nagy, és összetett szervezet esetében, mint a rendőrség nagyon nehéz csupán műszaki alapú vizsgálatot végezni, hiszen egy informatikai rendszer a technológiai elemek és azok kapcsolatain kívül a fejlesztő, és üzemeltető humán erőforrással, illetve a külső és belső szabályzói környezettel, ezek kölcsönhatásaival, ok-okozati összefüggéseivel alkot koherens egészet.

2. Az integrációt követő feladatok

2.1. Vezetékes rendszerek

A rendőrség és határőrség integrált működésének első napjaitól megoldandó problémák sorát generálja, hogy az informatika integrációjának előkészítése nem kellő részletességgel történt meg. HŐR OPK-ORFK szinten történtek tárgyalások, de ezek többször megrekedtek, viszonylag kevés kézzelfogható eredményt hoztak. Így a teljes informatikai rendszer átalakítását előkészítés nélkül az új szervezetben kellett megkezdeni. WAN hálózat szintjén gyakorlatilag két különböző fastruktúrából kellene egy olyan új hálózatot kialakítani, amelyik a szervezet minden reális informatikai igényét hatékonyan képes kiszolgálni. A hálózat ilyen jellegű átalakítása rendkívül bonyolult, idő, munka, és pénzigényes. Ráadásul fontos adminisztra-

[44] Szerzők: Prisznyák Szabolcs r. fhdgy. (okleveles védelmi vezetéstechnikai rendszertervező), Pándi Erik r. alez. (PhD), Farkas Tibor fhdgy. (okleveles haditechnikai menedzser, PhD-hallgató).

[45] Jelen közlemény a Bolyai János Kutatási Ösztöndíj támogatásával készült.

tív problémák is fellépnek. A leglényegesebb, hogy a határőrségnél valamennyi bérelt vonalra egyetlen szerződés létezett a HŐR OPK, és a legnagyobb távközlési szolgáltató között. Így az egyszerre nagy mennyiségű vonal bérlete jobb alkupozíciót, ebből következően kedvezőbb anyagi feltételekkel történő szerződéskötést biztosított, mindemellett további rendszertechnikai előny volt, hogy az OPK gazdálkodhatott az adott vonalmennyiséggel, így szükség esetén sávszélességet bővíthetett egy másik kevésbé kihasznált vonal terhére, vagy az esetleg megszűnő kirendeltség felszabaduló vonalát (sávszélességét) máshol új vonal létesítésére, vagy meglévő vonal sávszélességének bővítésére fordíthatta.

A rendőrségnél - a decentralizált irányításból, és gazdálkodásból következően – a vonalak bérletére a megyék külön-külön kötöttek szerződéseket. Az ORFK egy központi szerződés megkötését tervezi, a fent ismertetett korábbi határőrségi szerződésben tapasztalható előnyök miatt. Ez azonban rendkívüli adminisztratív munkával jár elsősorban a rendőrség decentralizált költségvetési rendszere miatt. Ennek lebonyolítása az eddig eltelt közel másfél évben nem fejeződött be. Mindeközben több megyében is lejártak a szolgáltatóval kötött szerződések, ezeket a folyamatos hang-, és adatkommunikáció biztosítása céljából meg kellett újítani. A beszerzési eljárások lebonyolítására a GEI-k IT Osztályai jogosultak, de a szerződéseket az MRFK-k nevében kötik. Technológiailag az új szerződések esetében az IP complex megoldásokat részesítik előnyben.

A területi és helyi szervezeti elemek több helyen létesítettek olyan rendszertechnikai megoldásokat, mely megkönnyíti az együttműködésüket. Itt elsősorban további vonalak bérlésére, vagy mikrohullámú kapcsolatok kiépítésére kell gondolni. A rendőrség az integrációval a határőrség ingatlanjainak döntő többségét is átvette, ezeket használja is, hiszen a szervezeti változások, főként a gazdasági ellátó igazgatóságok (GEI-k) megalakulása miatt ezek jelenleg nélkülözhetetlen objektumok. Volt példa arra is, hogy egy korábban megszűnt – már eladásra szánt, - határőrizeti kirendeltség objektumát reaktiválni kellett, mert csak így volt biztosítható az elhelyezés. A korábban onnan leszerelt és bevont teljes informatikai eszközparkot ismét működőképes állapotba kellett hozni. Kijelenthetjük, hogy nem csak az újonnan létrehozott GEI-kkel, és a megmaradó határőrizeti szervekkel való kommunikáció biztosítása okoz problémát, hanem sok esetben a korábban egy objektumban üzemelő területi és helyi szervezeti elemeké is. Ennek az az oka, hogy az átszervezés következtében az elhelyezésük adott esetben egy-egy város különböző pontjain található objektumokban történt. Amennyiben az ilyen ingatlanok nincsenek hang-, és adatátviteli hálózattal összekötve, könnyen előfordulhat, hogy két megyei osztály egymással történő kommunikációját csak Budapesten keresztül lehet biztosítani. Az ilyen esetek különösen igazak azokon a helyeken, ahol a korábbi határőr igazgatóságok nem megyeszékhelyeken, sőt sok esetben más megyében voltak.

Ezeket a problémákat az ORFK Információtechnológiai és Műszaki Főosztály Hálózat,- és Rejtjelfelügyeleti Osztály igyekezett orvosolni, így ezek – a fontossági sorrendet szem előtt tartva – megoldásra kerültek. Az integrációt követően országszerte több MRFK- városi kapitányság közti adatvonal sávszélessége esetében került sor bővítésre, így sikerült elérni, hogy ebben a szegmensben ma már a legalacsonyabb sávszélesség 256 Kbps, de az átlagosan jellemző érték 512 Kbps. A

használaton kívüli – megszűnt határőr – objektumok esetében a vonalak lemondásra kerültek, de mivel ezek a határőrségi mennyiségi szerződés részét képezték, ezért lehetőség volt az átcsoportosításukra.

Összességében kijelenthető, hogy nagyon sok szakmai feladattal jár még, mire a hálózat logikai, és fizikai értelemben is a szervezeti struktúrához, - illetve a szervezeti elemek elhelyezéséhez is - igazodik. Mindezeket a feladatokat természetesen úgy kell végrehajtani, hogy a szervezet informatikai szolgáltatásait mindvégig folyamatosan biztosítani kell.

Problémát okoz az MRFK-ORFK adatvonalak túlterheltsége, különösen azon MRFK-k esetében, amelyek olyan megyeszékhelyen találhatóak, melyek egyben GEI székhelyek is. Ezeknek a vonalaknak a sávszélesség bővítése egyre sürgetőbbé válik. A GEI-k esetében megoldást jelenthetne külön bérelt vonal beüzemelése, vagy - abban az esetben, ha a GEI korábbi határőr objektumban található - a korábbi határőrségi bérelt vonal elkülönítése.

A rendőrség nem rendelkezik meghibásodás esetére tartalék útvonalakkal. Meg kell vizsgálni annak lehetőségét, hogy a rendőrség milyen módon csatlakozhatna az Elektronikus Kormányzati Gerinchálózathoz (EKG), mely az említett esetekben alternatívát kínálhatna. Az EKG több (négy) országosan kiépített optikai gyűrű, amely jelenleg a megyeszékhelyek kormányzati szerveinek hálózati szolgáltatásait hivatott biztosítani, így az MRFK-ORFK vonalakon jelenthetne ez megoldást. Vannak olyan feladatok, amelyek végrehajtására csak a még távolabbi jövőben kerülhet csak sok, ilyen pl. a távbeszélő számmezők átstrukturálása, vagy éppen a Rendőrség IP cím mezőinek újra kiosztása[46]. Ezek mind megoldandó, nagy kihívást jelentő szakmai feladatok.

2.2. Rádiórendszerek

A rádiózás tekintetében mindkét szervezet életében harmadik időszaknak nevezhető szakasz kezdete nagyjából a két szervezet integrációjára tehető. Ekkor vezették be az Egységes Digitális Rádió távközlő rendszert (EDR). Igaz ennek bevezetése a határőrségnél valamivel korábban, a 2007-es évben megtörtént, a rendőrségnél pedig csak az integrációt követően 2008 első felében. Ez a rendszer már nem rendőrségi, határőrségi, de még csak nem is belügyi fejlesztésű, tulajdonú. Az EDR létrehozását a kormány határozta el, fejlesztését a Miniszterelnöki Hivatal koordinálja, a szolgáltatást pedig a Pro-M Zrt.-től vásárolják.

Az EDR egy rendkívül magas rendelkezésre állást biztosító, zárt rádió-távközlő rendszer, melynek célja, hogy olyan professzionális összeköttetést valósítson meg a különféle készenléti és rendvédelmi szervek között, amely gyorsabbá, hatékonyabbá és biztonságosabbá teszi az egyes feladatok végrehajtását. Az EDR tehát egy olyan kormányzati megoldás, amelyet a rendőrségen kívül további védelmi, és készenléti szervek is alkalmaznak.

A rádiórendszer szabványa európai uniós ajánlás, így alkalmas arra, hogy a Schengeni Egyezményhez tartozó országok rendvédelmi szerveinek együttműködését is támogassa. A rendszer előnyei elsősorban a digitális kommunikáció nyújtotta lehetőségekben rejlenek, ezek a következők:

[46] Jelenleg mind a telefonszámok, mind az IP címek esetében a rendőrségi, és a korábbi határőrségi rendszerek vegyes használatban vannak, elsősorban elhelyezés függvényében.

- több beszédcsatorna,
- nincs egymásra forgalmazás,
- gyorsabb kapcsolat felépítés,
- tisztább beszédkommunikáció,
- nem lehallgatható,
- elveszett készülék gyorsan, és egyszerűen kitiltható a rendszerből,
- SDS (SMS) küldési lehetőség,
- hagyományos telefonálási lehetőség.

A rendszer hatékony kihasználásának kulcsa a figyelmes előkészítésben, tervezésben rejlik. A legfontosabb a beszéd-csoportok megfelelő kialakítása. A hatékonyság nagyban függ a különböző szintek diszpécserétől is, hiszen ő – gyakorlatilag on-line üzemben – módosíthat beállításokat.

Az adatkommunikációs, és az SDS nyújtotta lehetőségeket kihasználva olyan, új megoldásokhoz juthatunk, mint pl. a gépkocsi rendszám alapján a rádióval a központi számítógépes adatbázisból történő lekérdezések. Az EDR-ben rejlő lehetőség, hogy a készülékek műholdas helymeghatározó rendszerhez (GPS) kapcsolódását kihasználva, olyan további informatikai rendszerek alapját képezheti, mint pl. térinformatikai rendszerek, csapatvezetési rendszerek, vezetői döntéstámogató rendszerek. Az EDR - a technológián túl - a rendőrségi informatika életében hozott legfőbb változása, hogy a teljes szolgáltatást külső vállalkozás biztosítja, így – a korábbiakkal ellentétben – nincsenek fenntartási, javítási feladatok.

2.3. Az információtechnológia (számítástechnika) jelene és jövője

Az integrációt megelőző előkészítés a számítástechnika esetében is kívánnivalókat hagyott maga után. Ez elsősorban annak köszönhető, hogy az új szervezeti struktúra véglegesítése, valamint a vezetők kinevezése nem sokkal az integráció tényleges bekövetkezte előtt történt meg (2007. november-december). A hátralévő egy-másfél hónapban csak a személyzeti kérdések eldöntésére maradt idő. Az integrációhoz szükséges feladatok közül csak a két szervezet központi DNS[47] adatbázisának integrálása történt meg. Ez azt eredményezte, hogy az integráció időpontjában az egy városban (egy megyében, régióban) lévő rendőri, illetve volt határőr szervek rendszerei kizárólag az ORFK-n keresztül voltak képesek egymással kapcsolatot teremteni. A hálózati túlterheltség elkerülése érdekében a területi szervek informatikai szakemberei egyedi helyi megoldásokkal kötötték össze az objektumok hálózatait. A lehetséges megoldást elsősorban a földrajzi, az infrastrukturális, és a technikai lehetőségek határozták meg. Alkalmazott megoldás a mikrohullámú rendszeren történő LAN meghosszabbítás, a bérelt vonalon történő routolt kapcsolat kialakítása, vagy esetleg speciális modemekkel saját földkábelen történő összeköttetés, de ezeken kívül is számos alternatívával találkozhatunk. Ezek az egyedi, - és az idő rövidsége miatt nem is minden esetben a legjobb – megoldások még bonyolultabbá, sérülékenyebbé teszik a hálózatot.

A hálózatok összekötésével, illetve az új szervezetek felállásával, elhelyezésével újabb problémák sora generálódott. A korábbi határőrségi számítógépek csak a

[47] DNS: Domain Name System

HORAD[48]-ban működtek, ha a hálózatban nem találtak domain controllert[49], akkor teljesen használhatatlanokká váltak. Mivel a rendőrség nem támogatta az Active Directory megoldást, ezért valamennyi korábbi határőrségi számítógépet újra kellett telepíteni. A hálózatok összekötésekor minden hálózatban legalább kettő – egy rendőrségi, és egy határőrségi – DHCP szerver kezdte osztogatni az IP címeket. Ez címütközést nem okozott, mivel a határőrség és a rendőrség korábban eltérő IP szegmenseket használt, de ha egy számítógép a másik szervertől kapott IP címet, akkor saját hálózatát nem tudta elérni. Így a határőrségi DHCP szervereket le kellett állítani, és átmeneti megoldásként – amíg mindenki át nem lépett a rendőrségi hálózatba – kézi IP-címzést kellett végezni. Ezek a problémák bár apróságnak tűnnek, de a gyakorlatban a teljes informatikai rendszer alapjaihoz tartoznak. A felmerült problémák megoldása óriási megterhelést jelentett a technikusi állomány, illetve a rendszergazdák számára. Mindehhez még hozzáadódott, hogy az új, megújult, kibővített, vagy csak máshova költöző szervezetek elhelyezésénél a helyiségek informatikai szempontból történő megfelelőségét a vezetők csak sokadlagos szempontként vették figyelembe. A hálózati csatlakozással nem rendelkező épületrészekbe az IT csoportoknak kellett kiépíteni a kapcsolatot. Ez sok esetben csak a hálózatok – szakzsargonnal kifejezve – „túlswitchelésével" volt lehetséges, ami pedig – az előírásoknál több aktív eszköz alkalmazása, és hosszabb hálózati szegmensek miatt - a megfelelő működést veszélyeztette[50].

A hardver elemeket vizsgálva elmondhatjuk, hogy a határőrség felszabaduló számítógépeit felhasználva a rendőrség rendkívül sokat profitált az integrációból. Lehetőség nyílt a legelavultabb asztali számítógépek használatból történő kivonására. Mindezekhez hozzátartozik még, hogy a rendőrségen 2008-ban több lépcsőben központi fejlesztések is történtek, amelyek új asztali számítógépek, és nagy teljesítményű hálózati nyomtatók üzembe állításában nyilvánultak meg. Ezek zömében célzott fejlesztések voltak, és a 2008-ban bevezetett úgynevezett objektív felelősségvállalással kapcsolatos rendőrségi feladatok, valamint az újonnan megalakult GEI-k informatikai támogatását célozták meg. Az asztali számítógépek technikai fejlettségének tekintetében tehát nagy előrelépés történt, de egy olyan szervezetnél, ahol hozzávetőleg 15 ezer számítógép működik, az amortizáció szinte folyamatos. A határőrség korábbi asztali és hordozható számítógépei szinte kivétel nélkül a jogutód MRFK-hoz, vagy a regionális GEI-hez kerültek, ellenben az igazgatósági szervereket, illetve a nagy mennyiségű adattárolásra szolgáló diszk alrendszerek többségét az ORFK bevonta, és saját hatáskörben használja tovább.

A szoftverrendszer tekintetében elmondhatjuk, hogy szinte teljes egészében a rendőrség korábbi rendszerei maradtak további használatban. Történt mindez annak ellenére, hogy az ágazati minisztérium az integráció kapcsán külön költségvetési részt különített el – a határőrségi szoftverek rendőrségen belüli használatának

[48] HORAD: Határőrség Active Directory

[49] A számítógép, illetve a felhasználó azonosítására alkalmas, ahhoz nélkülözhetetlen, kitűntetett szerepkörű központi számítógép.

[50] Mindeközben előfordult, hogy a határőrség által nem sokkal az integráció előtt teljesen felújított minden informatikai igényt maximálisan kielégítő, klíma berendezéssel, riasztóval, tűzjelző berendezéssel felszerelt helyiséget a rendőrség raktárként használta tovább.

biztosítása érdekében történő – fejlesztésekre. Az egyetlen alkalmazás, amely – nemzetközi előírásoknak megfelelően – természetesen továbbra is kötelezően használatban maradt a hazánk schengeni külső határain üzemelő határforgalom ellenőrző rendszer.

A rendőrségnél használt Novell Netware hálózati operációs rendszer, és a Microsoft Windows XP – vagy korábbi Windows 2000, sőt néhány esetben Windows 98 – kliensek együttműködése számos – elsősorban informatikai biztonsági kérdésre visszavezethető – problémát felvet, melyek legnagyobb része a szabályozottság hiányából adódik. A gyakorlatban ez azt jelenti, hogy a felhasználók úgy is dolgozhatnak a számítógépükön, ha nem azonosítják magukat felhasználói név, jelszó párossal. Ebben az esetben az asztali gépen – szintén a szabályozatlanság miatt – rendszergazdai jogosultságok birtokában kerülnek, amely jelentős károkat képes okozni egy hálózatban. Ebben az esetben nem érik el az állomány kiszolgálón tárolt adatokat, de képesek hálózatban nyomtatni (IP alapú nyomtatás), és egyéb hálózati programokat – pl. Robotzsaru – használni, amelyek a Novell-t figyelmen kívül hagyva szintén tisztán IP szinten működnek, igaz ezeknél a programoknál általában magába a programba történő belépéskor nélkülözhetetlen a felhasználó azonosítása. A fentiekből megállapíthatjuk, hogy a Novell Netware használata szokásjogon alapul, egy-egy szervezeti elem – általában osztály – vagy használja a közös állományok tárolására, vagy nem. A legrosszabb esetben az egyik – vagy több – kliens oldali Windows operációs rendszerű számítógépeken hoznak létre állomány, vagy gyakrabban könyvtár (mappa) megosztásokat, melyeket Windows munkacsoportos technikával használnak. Ezt a megoldást – az irracionálisan nagy hálózati forgalom generálása miatt – a Microsoft is csak 10 számítógépnél kevesebbet alkalmazó hálózatokban ajánlja, elképzelhető, hogy milyen túlterheltséget okozhat ez egy több száz számítógépet magába foglaló hálózatban. Mindezen felsoroltakat a rendőrségnél is felismerték, és elhatározás született a teljes Microsoft infrastruktúrára történő áttérésre. Az elkészült tervek szerint a címtár, fájl, nyomató, DNS, DHCP szolgáltatásokat Microsoft alapokon biztosítanák, egyedül az elektronikus levelező szolgáltatást nyújtaná továbbra is a Novell Groupwise. A megvalósítás az országos, és a regionális szerverek telepítéséig jutott, majd megtörtént a címtár konvertálása is, de a fejlesztés ezen a szinten megrekedt, véleményünk szerint a vezetői utasítás, illetve szabályozás hiányában. A Microsoft infrastruktúrára történő áttérés a szervezet teljes volumenében a közeljövő legnagyobb rendőrségi informatikai feladata lesz.

Alkalmazói programok tekintetében a legkönnyebb helyzetben a gazdálkodási, és a személyzeti szakterület volt, hiszen ott a programokban nem történtek változások, és mivel korábban is mindkét szervezet azonos rendszereket használt egyszerű volt az átállás. Ez még annak ellenére is elmondható, hogy a gazdálkodási folyamatokat kizárólag a regionális GEI-kben végzik. Ennek hátránya, hogy mint korábban ismertettem a magyarországi munkaerő mobilitás – vagyis annak hiánya – miatt ezek a szervezetek munkaerőhiánnyal küzdöttek[51]. Kénytelenek voltak új dolgozókat felvenni, és nekik megtanítani az alkalmazásokat.

[51] Osztályvezetőnél alacsonyabb beosztású dolgozók (a mobilitás hiányában) szinte nem is kerültek a GEI-kbe a szomszédos megyék rendőri, vagy határőrizeti szervezeteitől.

A rendőrség szinte egyetlen szakmai alkalmazása a Robotzsaru rendszer, mivel szinte minden új feladat ennek keretei közt kerül megoldásra. Az államigazgatási szervezetek közül 2008-ra talán csak a rendőrség maradt, amely nem rendelkezett elektronikus iktatással, és ügykezeléssel, így ennek bevezetése vált az egyik legsürgősebb feladattá. Kézenfekvő lett volna a határőrségnél korábban alkalmazott Lotus Notes alapú rendszer bevezetése, kiváltképp annak tudatában, hogy a rendszert teljes mértékben átalakították rendőrségi használatra. Mindezeken felül az alkalmazás egy több mint fél évtizede bevált rendszer volt, melyet a korábbi határőrségi dolgozók – az új felállás szerint a rendőrségen minden negyedik ember – jól ismertek. A rendőrség – mint jogutód szervezet – rendelkezett a program használatához szükséges jogosultságokkal, igaz ezeket a nagyobb szervezet miatt bővíteni kellett volna. A fenti döntő érvek nem bizonyultak elegendőnek, hogy a rendőrség a Lotus Notes alkalmazása mellett döntsön. Helyette saját fejlesztésre szánták el magukat, így a Robotzsaru rendszer egy újabb modullal bővült. Ezt a modult folyó év elején vezették be, így nagyon kevés még a tapasztalat az alkalmazást illetően, de az már nyilvánvaló, hogy a HŐR Adminisztrátor[52] jobban skálázható volt, és szélesebb körű feladatmegoldást tett lehetővé.

Fentiekből látható, hogy a rendőrségi számítástechnika terén a rendezettség kívánnivalókat hagy maga után, szokásjogokon alapul a szabályozatlanság. Természetesen ez nem, vagy nem csak műszaki kérdés, hanem a szervezeti, igazgatási, és műszaki vonal metszete. A jövőbeni feladatok alapja a Rendőrség Ideiglenes Informatikai Biztonsági Szabályzatának bevezetése. Mindennek a felhasználók oktatásával kell kezdődnie. A biztonsági szabályokat érdemes lenne már az új Windows Active Directory-s (PoliceAD) környezetben alkalmazni. A rendszer kialakítása során a fő szempontoknak a határőrségnél korábban alkalmazottaknak kell lenniük (azonosítás, programok, és adatok központi redundáns tárolása, stb.). Az ideiglenes szabályzatot később felül kell vizsgálni, és célszerű pontosítani (pl. rendőrségi jogtiszta alkalmazások köre), illetve kibővíteni (pl. kritikus alkalmazások mátrixával).

A jövőben megoldandó feladat lesz a napjainkban egyre fontosabb körzeti megbízotti rendszer információhoz, informatikai eszközhöz juttatása, melyek biztosítják a központi adattárak biztonságos elérését is.

A rendelkezésre álló strukturált adatbázisokban, vagy strukturálatlan adathalmazban rejlő lehetőségeket célszerű lenne kihasználni, hiba lenne ennek elmulasztása. A hasznosításnál elsősorban a napjainkban rendelkezésre álló adatbányászati, szövegbányászati lehetőségek alkalmazására gondolok. Ezek a modern technikák lehetőséget nyújthatnának komoly vezetői döntéstámogató rendszer(ek) kialakítására, vagy a szervezetben meglévő, és rögzített adat-, és tudáshalmaz elemei közti eddig nem ismert vagy fel nem tárt kapcsolatok, összefüggések felismerésére. A távolabbi jövőben olyan lehetőségek is felmerülhetnek, hogy az azonosításra akár egy chipkártya is használható, amely akár a szolgálati igazolvány is lehetne.

[52] A határőrségi Lotus Notes alapú iktató, és ügykezelő rendszer elnevezése.

3. Összegzés következtetések

Az informatika műszaki hátterének elemzése rendkívül összetett feladat. Egyrészt maga a szigorúan vett műszaki terület is szerteágazó, és az új technológiák alkalmazásával ez a hatás egyre erősebb. Másrészt az informatika műszaki háttere önállóan szinte nem is vizsgálható, hiszen a szervezeti, és igazgatási témakörrel való kapcsolódás kikerülhetetlen.

A leghosszabb múltra a vezetékes távközlés tekint vissza. Az integrációt követően két országos kiterjedésű – bizonyos részeiben egymással párhuzamosságot, de sok tekintetben eltérő struktúrát mutató – hálózatot kellett eggyé alakítani, egységesen üzemeltetni. Vizsgálataink alapján **arra a következtetésre jutottunk, hogy a hálózat integrációjának előkészítése nem kellő részletességgel történt meg**. Ennek eredménye, hogy az újonnan létesített összeköttetések esetében a hang-, és adatkommunikációt döntően nem a szakmailag optimális, hanem a legegyszerűbb, és leggyorsabb módszerrel valósították meg. Javaslatunk szerint a korábbi kettős (rendőrségi, és határőrségi) **IP és telefonszámmező kialakítást újjá kell szervezni egy korszerű, és egységes struktúrába**.

A vezeték nélküli (rádiós) kommunikáció vizsgálatakor megállapítottuk, hogy az EDR bevezetése – szerencsésen – gyakorlatilag egybeesett a két szervezet integrációjával, ami rendkívül nagy előnyt jelentett. Az EDR további – beszédkommunikáción túli – lehetőségeinek kiaknázása a jövő feladata, **javasoltuk a komplex, modern térinformatikai lehetőségek alkalmazásának tervezését, bevezetését**.

Az informatika területén megállapítottuk, hogy – bár a Rendőrség sokat nyert az integrációval – a szakmai előkészítés itt is hiányos volt, elsősorban a hálózatok, és alkalmazások egységesítése tekintetében. **Hibának, és pazarló döntésnek tartjuk a határőrségi rendszerek további használatától – a Schengeni Információs Rendszer kivételével - történő elzárkózást.** Véleményünk szerint **a rendőrségnek mielőbb be kell vezetnie a Windows tartományos rendszert (PoliceAD),** melynek biztonságos működését minden részletre kiterjedő **belső szabályzókkal és utasításokkal** kell elérni. A jövőben a korábbiaknál kiemeltebb figyelmet kell fordítani a felhasználók oktatására is.

Felhasznált irodalom:

[1] Budai Attila: Mikroszámítógép rendszerek, LSI oktatóközpont, Budapest, 1999. ISBN 963 577 278 5

[2] F. Haté Katalin: Adatbiztonság, adatvédelem, SZÁMALK Kiadó, Budapest, 2000.

[3] Gál Tamás – Szabó Levente – Szerényi László: Rendszerfelügyelet rendszergazdáknak, SZAK Kiadó, Budapest, 2007. ISBN 978 963 9131 98 9

[4] Kónya László: Számítógép-hálózatok, LSI Oktatóközpont, Budapest, 1999. ISBN 963 577 222 X

[5] Mitnick, Kevin D. – Simon, William L.: A legendás hacker – A megtévesztés művészete, Perfact-Pro Kft., Budapest, 2003. ISBN 963 206 555 7

[6] Mitnick, Kevin D. – Simon, William L.: A legendás hacker – A behatolás művészete, Perfact-Pro Kft., Budapest, 2006. ISBN 963 864 725 6

[7] Pándi Erik: A hazai zártcélú hálózatok szerepének átalakulása az elektronikus közigazgatási szolgáltatások bevezetése és kiterjesztése folyamatában, Hadmérnök II. évfolyam 2. szám, Budapest, 2007. ISSN 1788 1919

[8] Stanek, William R.: Microsoft Windows Server 2003 Administrator's Pocket Consultant Microsoft Press, Redmond, 2003. ISBN 0 7356 1354 0
[9] Szász Gábor - Kun István – Zsigmond Gyula: Kommunikációs rendszerek, LSI Oktatóközpont, Budapest, 2000. ISBN 963 577 275 0
[10] Tannenbaum, Andrew S.: Számítógép-hálózatok, Panem Kiadó, Budapest, 1999. ISBN 963 545 213 6

PRISZNYÁK Szabolcs – PÁNDI Erik – TAKÁCS Attila[53]

A RENDVÉDELMI INTEGRÁLT INFORMÁCIÓTECHNOLÓGIAI ÁGAZAT EGYES KOCKÁZATI TÉNYEZŐI[54]

Absztrakt: A közlemény révén a szerzők célja az integrált Rendőrség információtechnológiai ágazata igazgatási kérdéseinek – mint időszerű problémának – feldolgozása kapcsán tett főbb megállapításainak összefoglalása és ismertetése, illetőleg egyes kockázati tényezők megfogalmazása.

Kulcsszavak: információtechnológia, Határőrség, informatika, MITS, Rendőrség, Schengeni Végrehajtási Egyezmény, távközlés.

1. Alapvetés

Magyarország 2007. december 22.-én – kilenc további állam társaságában – csatlakozott a Schengeni Végrehajtási Egyezményhez. A fenti események már évekkel korábban a Határőrség teljes szervezetét tekintve rendkívüli változásokat vetítettek előre. A Kormány a Határőrség Rendőrségbe történő integrációja mellett döntött. Az integráció megvalósítását Kormányhatározat írja elő[55]. Az Alkotmány módosításáról szóló törvény[56] indoklása szerint Magyarország teljes jogú schengeni tagságát követően a határrendészeti feladatok rendszere oly mértékben átalakul, hogy azt a Rendőrségen belüli határrendészeti szolgálati ág is megfelelő hatékonysággal el tudja látni. Az Alkotmánymódosítást követen a Rendőrség alapvető feladata a közbiztonság, a közrend, és az államhatár rendjének védelme, mely utóbbi a Rendőrségről szóló törvény[57] szerint magába foglalja az államhatár rendjének fenntartását, a határforgalom ellenőrzését, és a külső határokon az államhatár őrzését is.

Fent ismertetett integráció mind a Rendőrség, mind a Határőrség eddigi történetének legnagyobb mértékű, legátfogóbb átszervezése volt. Ha mindezekhez hozzávesszük a több, mint 150 éves múltra visszatekintő Belügyminisztérium 2006-ban történő teljes átalakítását – melynek értelmében az önkormányzati, és a rendészeti feladatok szétválasztásra kerültek oly módon, hogy a rendészeti tevékenység kormányzati szintű feladatainak végrehajtását a továbbiakban az Igazságügyi, és Rendészeti Minisztérium végzi – akkor nyilvánvalóvá válik, hogy az utóbbi néhány évben a magyarországi rendészeti struktúra teljes változásának lehetünk tanúi.

Két szervezet bármilyen jellegű egybeolvadása, integrációja – vagy a versenyszférában használt kifejezéssel fúziója – mindig rendkívüli feladatokat ró a szerve-

[53] Szerzők: Prisznyák Szabolcs r. fhdgy. (okleveles védelmi vezetéstechnikai rendszertervező), Pándi Erik r. alez. (PhD), Takács Attila r. alez. (okleveles villamosmérnök, PhD-hallgató).

[54] Jelen közlemény a Bolyai János Kutatási Ösztöndíj támogatásával készült.

[55] Az államháztartás hatékony működését elősegítő szervezeti átalakításokról és az azokat megalapozó intézkedésekről szóló 2118/2006 (VI. 30.) Korm. Határozat 4. pont f.) alpontja

[56] Az 1949. évi XX. törvényt a 2007. évi LXXXVIII. törvény módosította, hatályos: 2008. január 1.-től.

[57] A Rendőrségről szóló 1994. évi XXXIV. törvény (Rtv.)

zetet működtető logisztikai szervezeti elemekre. Ezek közül is különösen érdekes – napjaink legdinamikusabban fejlődő iparága – az informatika feladatrendszere egy ilyen mértékű átszervezéskor. Biztosítania kell, hogy a számítástechnikai, és távközlő rendszerek, hálózatok zavartalanul üzemeljenek az átszervezés időszakában, és azt követően is, úgy hogy közben maradéktalanul kiszolgálják a rendőr szakmai szervezeti elemek ilyen jellegű igényeit, természetesen immár a határrendészeti szolgálati ág feladatrendszerével, ebből adódó igényeivel is számolva. Mindezen szolgáltatások összességét az informatikai szervezetnek – mint a gazdasági szervek részének – úgy kell biztosítania, hogy közben magának az informatikának a szervezete is gyökeresen átalakul.

Célunk volt az integrált Rendőrség információtechnológiai ágazatának szervezeti, igazgatási, és műszaki kérdéseinek – mint időszerű problémának – feldolgozása. Értelmeztük az informatikai igazgatást, valamint a stratégiák szerepét az igazgatásban. Célunk volt, hogy rámutassunk a stratégiák, és az egymásra épülő hatékony szabályozás szükségességére, szerepére.

2. A Rendőrség IT ágazatának igazgatása

2.1. Az informatikai igazgatás tárgya

A rendvédelmi szervek informatikai igazgatásával kapcsolatban leginkább a rendészeti szakvizsgára felkészítő tanfolyamokra kiadott jegyzetek nyújtanak átfogó tájékoztatást. Az informatikai igazgatás tárgyát magát az informatikát vizsgálva megállapíthatjuk, hogy magára a kifejezésre nem alakult ki egyértelműnek, és egységesen elfogadottnak tekinthető definíció. Ez abból adódik, hogy a vizsgált terület viszonylag fiatal tudományág, ám rendkívül gyorsan, rengeteget változva, bővülve fejlődik. A terminológiai zűrzavar minden fiatal tudományágra jellemző. Egy általánosan elfogadott megfogalmazása szerint *az informatika egy erősen interdiszciplináris tudomány, amely az információk létrehozásával, gyűjtésével, szervezésével, tárolásával, továbbításával, visszakeresésével (szolgáltatásával), fordításával, közlésével, átalakításával, reprodukálásával és felhasználásával foglalkozik, felhasználva más tudományágak eredményeit (pl.: matematika, szimbolikus logika, kibernetika, rendszerelmélet, automatizálás, biológia, pszichológia, pedagógia, nyelvészet, szemantika, szemiotika, stb.)*. Egyes definíciók az üzemeltető humán erőforrást (személyzetet) is a fogalomkör részeként határozzák meg.

Az informatikát szakterületekre bonthatjuk, a felbontás alapját sokféle szempontrendszer képezheti, de olyan felsorolást szinte lehetetlen készíteni, amelyben ne lennének átfedések, melyeket a technika rohamos fejlődése produkál. Olyan mértékben összeolvadt néhány korábban önálló szakterületként fejlődő ágazat, hogy szabályozásuk ma már függetlenül elképzelhetetlen. Legmarkánsabb példa erre a híradástechnika (vezetékes, és vezeték nélküli), és a számítástechnika esete. Ma már egy telefonközpont, egy mobiltelefon is szoftverrel működik, eltűnik a különbség a hang, a kép, és az adatátvitel technikai feltételei között. A hálózati kapcsolóelemek programozhatók. A számítógépeken zenét lehet hallgatni, filmet lehet nézni, megjelenik az elektronikus sajtó, és az elektronikus könyvtárak is szaporodnak. Teljes egészében még nem sikerült tisztázni az informatika fogalmát, de újabb és újabb fogalmakat sorolunk a tárgykörbe, mint pl. információtechnológia, infokommunikáció.

2.2. A stratégiák szerepe az igazgatásban

Az informatikai igazgatási hierarchia, akárcsak más társadalmi, gazdasági területen a legmagasabb szintről indul. Sajátossága, hogy a jogi kereteken kívül nagyon sok szabvány, kvázi szabvány, iránymutatás, szakmai konvenció, és szokás rendezi a felmerülő kérdéseket. Az informatikai feladatokra és informatikai szervezetekre vonatkozó szabályozás viszonylag kisszámú, de jelentősen bővül a kör, ha az informatikai tevékenységet közvetve befolyásoló jogszabályokat is figyelembe vesszük. Ezek vonatkozhatnak az informatikai eszközökkel kezelt adatokra (adatkezelési jogszabályok), a számítástechnikai eszközökkel történő gazdálkodásra (beszerzési, gazdálkodási szabályok), a rendszerek összekapcsolására (adatvédelmi, és biztonsági szabályok), vagy akár az – elektronikus – ügyiratok kezelésére (ügyviteli szabályzatok).

Az informatika fejlődése szükségessé tette, hogy a legfelsőbb szinten kerüljenek megfogalmazásra a stratégiai szempontok, fejlesztési irányok. Először 1993-ban készült átfogó informatikai stratégia, a Nemzeti Informatikai Stratégia, amely meghatározta a felzárkóztatás irányát, legfontosabb lépéseit. Ezt követően 2001-ben készült a Nemzeti Információs Társadalom Stratégia, amely alapját képezte a későbbi Magyar Információs Társadalom Stratégiának (MITS).

A MITS nem jogi erővel felruházott szabályzatgyűjtemény, de megfogalmazza a célkitűzéseket, elvárásokat. Egy ilyen stratégia, minden ágazat együttműködését igényli. A különböző ágazatok elkészítették a saját ágazati stratégiájukat, az irányításuk alá tartozó intézmények pedig az intézményi stratégiájukat. Az ágazati, és intézményi stratégiákban konkrét feladatok, illetve szabályozandó területek kerülnek meghatározásra. Ezeknek megfelelően 2003-ban készült el a Belügyminisztérium ágazati szintű középtávú informatikai stratégiája (2003-2006). Mint az évszámokból látható, ekkor még az EU, illetve a Schengeni csatlakozás előtt álltunk, ezért a nemzetközi szervezetekhez történő integráció ágazati szintű informatikai feltételeinek megteremtése volt a fő elvárás. A másik fő irányvonal az elektronikus kormányzat felé mutatott, hangsúlyozva a lakossági szolgáltatások lehetőségét, fontosságát. Ez akkor markánsan megjelenhetett, hiszen az önkormányzatok, és ezzel együtt a legfőbb lakossági kormányzati szolgáltatónak nevezhető okmányirodák is a Belügyminisztérium hatáskörébe tartoztak. Természetesen a rendvédelmi szervekkel szemben is tartalmazott megfogalmazásokat a stratégia. Utólag értékelve látható, hogy részben megvalósultak a tervek. Az elmaradt fejlesztések pedig nem elsősorban hanyagságra, vagy finanszírozási kérdésekre vezethetők vissza, hanem sokszor technológiai fejlődésre (vagy éppen nem fejlődésre). Hiszen előre nagyon bizonytalan meghatározni egy ilyen dinamikus ágazat fejlődési irányait, ezek ütemét. Talán még ennél is bizonytalanabb, egyes szolgáltatásokra való társadalmi igény mértékének évekkel korábban történő meghatározása.

2.3. Jogszabályi, ágazati, intézményi szabályozás, igazgatás

Az informatika területén az egész társadalmat érintő, fontosabb kérdésekben törvényi szabályozásra is sor kerül. Az informatika és az egyéb területek összefonódását mutatja, hogy sok esetben más területre vonatkozó jogszabály tartalmaz informatikát is érintő szabályokat. Az egyik ilyen jogszabály a személyes adatok védelméről, és a közérdekű adatok nyilvánosságáról szóló törvény, amely az információs rendszerekben gyűjtött, tárolt, feldolgozott adatokra vonatkozóan szigo-

rú előírásokat tartalmaz. A jogszabályban leírtakat később a rendőrségi, és az azóta hatályon kívül helyezett határőrségi törvény is tovább szabályozta. Kifejezetten informatikával összefüggő törvény az elektronikus aláírásról szóló törvény, a hírközlési törvény, majd helyette később az elektronikus hírközlési törvény, és az elektronikus kereskedelmi szolgáltatásokról, és az információs társadalommal összefüggő szolgáltatásokról szóló törvény.

Alacsonyabb szinten – Kormányrendelettel, miniszteri rendeletekkel – szabályoznak olyan a rendvédelmi szerveket hatványozottan érintő kérdéseket, mint a zártcélú hálózatok üzemeltetése, vagy a kormányzati frekvenciagazdálkodás. Több informatikai tárgyú miniszteri utasítás – korábban belügyi, majd igazságügyi és rendvédelmi – is készült az ágazatra vonatkozóan. Ezek vonatkozhatnak egy-egy feladat elvégzésére, vagy pedig általánosan a teljes ágazatra kiterjedő érvényességgel.

A kormányzati, az ágazati és az intézményi stratégiákat, jogszabályokat, rendeleteket, határozatokat, utasításokat az egyes szervezeteknél, intézményeknél hajtják végre. Itt fogalmazódnak meg a hétköznapi feladatok, itt készülnek a különböző intézkedések, utasítások, szabályzatok. A minisztériumokhoz hasonlóan itt is általában kétféle szabályozás történik, egyrészt a teljes szervezetre vonatkozó általánosan érvényes átfogó utasítások készülnek, ilyen pl. az adott szervezet Informatikai Biztonsági Szabályzata. Másrészt szabályozható utasítással egy-egy feladat végrehajtása, vagy esetleg egy informatikai rendszer üzemeltetése. Mindkét fajta szabályozásnál elengedhetetlen, hogy – mivel ezek viszonylag alacsony szintű szabályozások – a magasabb rendű szabályzókkal összhangban legyenek. Az utasítások előkészítési fázisában ügyelni kell arra is, hogy ne csak a magasabb szintű, hanem az azonos szintű – de más szakterületi – szabályzókkal se ütközzenek, sőt egymást kiegészítve[58], támogatva hatékonyan szabályozzák – igazgassák – a működést.

A Határőrség és a Rendőrség korábbi informatikai szabályozását tekintve elmondható, hogy a Határőrség informatikai környezete, informatikai feladat végrehajtása szabályozottabb volt. Ez egyrészt adódhat abból a tényből, hogy mint korábban említettem a Határőrség inkább katonai szervezetnek volt tekinthető, a Rendőrség pedig inkább közigazgatási szervként működött. Másrészt a Határőrség centralizáltabb volt, a Rendőrség viszonylag decentralizált szervezet, ami nem csak az irányítási, szabályozási struktúrát tekintve igaz, hanem a gazdasági irányítást is. A Határőrség informatikai rendszere mind hardver, mind szoftver tekintetében fejlettebb volt, mint a Rendőrségé. Jó példa erre, hogy a Határőrségnél már 2002-től elektronikusan történt a hivatalos levelezés, az iktatás, és iratkezelés[59] a teljes szervezetre kiterjedően, és ezt – mint informatikai tevékenységet – szabályozni kellett. A komplettebb szabályozás képét mutathatja az a szubjektív érzés is, hogy a Határőrségnél pontosabban, és szigorúbban betartották a szabályzatokat, utasításokat, mint a Rendőrségnél (ez éppen a centralizált katonai beállítottságra vezethető vissza).

[58] Pl. Informatikai Biztonsági Szabályzat összhangban legyen az Adatvédelmi Szabályzattal.

[59] A Rendőrségnél ezt 2009. január 1.-től vezették csak be.

Az integrációval egy időben valamennyi határőrségi belső szabályzó hatályát vesztette. A szervezeti változások, és feladatbővülés következtében sok rendőrségi szabályzó is aktualitását veszítette. A legfontosabb belső szabályzó – az Informatikai Biztonsági Szabályzat[60] – csak a 2008-as év végére készült el, és 2009. január 1.-től ideiglenesen hatályos egy év időtartamra. Véleményünk szerint az utasítások, szabályzatok elkészítéséhez hasonlóan fontos – ha nem fontosabb – ezeknek az állomány számára történő oktatása. Az oktatás hiánya kockázati tényezőt jelent, hiszen ha ezek nem tudatosulnak a végfelhasználókban, az veszélyezteti a bevezetés – sőt a teljes rendszer – sikerét is. Az igazgatás területén tehát – a technológiával lépést tartó folyamatos szabályozás mellett – a Rendőrség állományának rendszeres, szakszerű – amennyiben szükséges munkaterülettől, beosztástól függően differenciált – oktatását tartjuk a legfontosabb jövőbeni feladatnak. E nélkül nem várható el a tudatos magatartás sem.

3. Összegzés, következtetések

A kutatás során a rendelkezésre álló szakirodalom tanulmányozásával igyekeztünk meghatározni az informatikai igazgatás tárgyát, magát az informatikát. Megállapítottuk, hogy egyértelmű, és egységes definíció nem alakult ki, ez elsősorban a tudományág fiatal voltának, és napjainkban is végbemenő folyamatos változásának, fejlődésének, bővülésének az eredménye. Elemeztük a stratégiák szerepét az informatikai igazgatásban, ezt a munkát elsősorban a kormányzati és ágazati szinten készült stratégiák tanulmányozásával végeztük el. Véleményünk szerint a rendvédelmi területen időszerűvé vált egy új ágazati szintű középtávú informatikai stratégia kidolgozása. Ezt megkövetelik az utóbbi időszakban végbement változások (minisztériumi szintű átalakulás, Rendőrség – Határőrség integrációja, stb.). A logikai utat tovább folytatva az ágazati szintű stratégia kidolgozását a Rendőrség középtávú informatikai stratégiájának kidolgozása kell, hogy kövesse.

Bemutattuk a törvényi, ágazati, intézményi szabályozást. Véleményünk szerint – a Rendőrség, és a Határőrség integrációját követően – az egyik legsürgetőbb szakfeladat a rendőrségi informatika belső szabályzóinak mielőbbi aktualizálása, az eddig hiányzó szabályzók megalkotása. Erre jó alapot adhatnak a korábbi határőrségi tapasztalatok. Véleményem szerint ez az egyik legfontosabb pillére a hatékony, nagy rendelkezésre állású, biztonságos informatikai szolgáltatásoknak mind az üzemeltetői, mind a felhasználói oldalról. Javaslatot tettünk az újonnan bevezetett szabályzók felhasználói körben történő eddigieknél hatékonyabb oktatására, melyekhez célszerűen igénybe vehetőek az elektronikus távoktatás eszközei, módszerei is.

Felhasznált irodalom:

[1] Bögel György – F. Ható Katalin – Keresztes József – Salamonné Huszty Anna – Zárda Sarolta: Szervezési és vezetési ismeretek, SZÁMALK Kiadó, Budapest, 2001.

[2] Dorkó Zsolt: A Rendőrség IT szolgálata működésének kritikai elemzése a hatékonyság optimalizálása érdekében, ZMNE, XXIX. ITDK Budapest, 2008.11.19.

[60] 60/2008. (OT32.) ORFK utasítás a Rendőrség Ideiglenes Informatikai Biztonsági Szabályzatának kiadásáról.

[3] Dr. Kassai Károly: A Magyar Honvédség információvédelmének – mint a biztonság részének – feladatrendszere, doktori értekezés, ZMNE, Budapest 2007.
[4] Közigazgatási és integrált rendészeti vezetési ismeretek I-II. kötet, Rendészeti Szakvizsga Bizottság, Budapest 2005.
[5] Közigazgatási és integrált rendészeti vezetési ismeretek I-II. kötet, Rendészeti Szakvizsga Bizottság, Budapest 2008.
[6] Pándi Erik: A rendőrségi információtechnológiai szervezet fejlesztésének néhány kérdése, Hadmérnök III. évfolyam 3. szám, Budapest, 2008. ISSN 1788 1919
[7] Sebestyén Attila: Az informatikai fejlődés stációi és determinánsai a működés szemszögéből, ZMNE, XXIX. ITDK. Budapest, 2008.11.19.

PAPP Zoltán – PÁNDI Erik – KERTI András[61]

A SZÁMÍTÓGÉP-HÁLÓZATOK ELLENI TÁMADÁSOK MÓDSZERTANA[62]

Absztrakt: Jelen közlemény révén a szerzők a kritikus infrastruktúrák egyikének, a számítógép-hálózatok elleni támadások módszertana tárgykörében lefolytatott kutatásaik egy szintetizált változatát kívánják közreadni.

Kulcsszavak: hamisítás, kritikus infrastruktúra, számítógép-hálózatok, támadás, védelem.

Bevezetés

Kultúránk és társadalmunk fejlődése során az emberek egyre nagyobb mértékben használják a rohamosan fejlődő technika és a kialakuló új technológiák által nyújtotta lehetőségeket, illetve mindennapjaik folyamán – anélkül hogy ez a szélesebb társadalmi rétegekben tudatosulna – támaszkodnak is rájuk napi tevékenységük során mind munkahelyükön, mind magánéletükben, mind pedig szűkebb-tágabb környezetükben. Ezek a megoldások napi életünket kényelmesebbé, munkánkat hatékonyabbá, ugyanakkor gyorsabbá is teszik.

Az információkon alapuló szolgáltatások kiesése konkrétan meg is fogalmazható, akár számszerűen is leírható társadalmi, egyéni, gazdasági és katonai érdekeket veszélyeztethetnek, ami miatt ezen rendszereknek védelme kiemelt feladata minden országnak, rendvédelmi, katonai, költségvetési és gazdasági szervezetnek. Az információs rendszerek üzemzavarainak „előidézése" mögött számos motiváció meghúzódhat. Anyagi haszonszerzés végett bűnözők támadhatják a gazdasági (banki) rendszereket, terroristák zavar- és félelemkeltés érdekében rombolhatják a kommunikációs, közlekedési hálózatokat, zavargások idején tüntetők az ellenük felvonultatott rendvédelmi erők kommunikációjának akadályozásával, azok tevékenységének hatékonyságát ronthatják.

Háborús időszakban a hadviselő felek a másik fél kommunikációs rendszereinek zavarásával, pusztításával káoszt idézhetnek elő a csapatvezetési és fegyverirányítási rendszerekben, a közlekedési és közművek infrastruktúrájának támadásával az ellenség logisztikai és utánpótlási lehetőségeit szűkítik. A műsorszóró, tömegtájékoztató rendszerek működésének korlátozásával a lakosság tájékoztatását, irányítását (pl. a sorkötelesek mozgósítását, óvóhelyek megnyitására vonatkozó adatok közlését) akadályozhatják, illetve e tájékoztatást szolgáló rendszerek feletti részleges, vagy teljes uralom megszerzésével, a pszichológiai hadviselés részeként befolyásolni is tudják az ellenség katonáit, hátországának lakosságát.

Mivel a különböző indíttatású és eltérő eszközrendszerrel rendelkező támadók támadásainak célpontját jelentő különböző fontosságú információs rendszerek alapjai már minden esetben fejlett informatika és kommunikációs eszközök rendkívül bonyolult halmaza – melynek számos eltérő biztonsági szinttel rendelkező eleme van – így legtöbb esetben a szembenálló felek e rendszerek elemei által alkotott úgynevezett kibertérben végrehajtott műveletek révén próbálnak meg ma-

[61] Szerzők: Papp Zoltán őrgy. (BA, MA), Pándi Erik r. alez. (BA, MA, PhD), Kerti András mk. alez. (BA, MA, PhD-hallgató).

[62] Jelen közlemény a Bolyai János Kutatási Ösztöndíj támogatásával készült.

guk számára minél nagyobb előnyt kicsikarni, az ellenség számára pedig minél nagyobb hátrányt okozni. A kibertérben megindított műveletek során elért eredményekre alapozva, vagy akár ezzel párhuzamosan kezdődhetnek meg a fizikai síkon végrehajtandó hadműveletek.

1. Hamis megszemélyesítés és jogosultságszerzés

A számítógép-hálózatok elleni támadások egyik legkézenfekvőbb, egyszerűbb módszere a hamis megszemélyesítés. Az információs rendszerek szolgáltatásait igénybevevők (emberek és programok) legtöbb esetben különböző jogosultságokkal férnek hozzá szolgáltatásokhoz, erőforrásokhoz. A rendszernek ezért valamilyen módon hitelesítenie kell a rendszer szolgáltatásainak igénybevételét kezdeményező felet, hogy az csak az őt megillető jogosultságokat kapja meg. Először a kezdeményező fél azonosítót küld magáról a rendszernek, amit követően az hitelesíti a kezdeményező felet: a kapott azonosítót összeveti az adatbázisban tárolt azonosítókkal. Ha talál egyezést, a kezdeményezőnek engedélyezi a rendszer használatát a talált azonosítóhoz tartozó hozzáférési jogokkal.

Komplex rendszerekben (számítógépes hálózatokban) az elemek is kommunikálnak egymással, és ezeknek is azonosítaniuk kell magukat, hogy a hitelesítés megtörténhessen, és az illetéktelen hozzáférés kizárható legyen. Hálózati közegekben legbiztonságosabbak azok a módszerek, amikor a felhasználó által birtokolt elektronikus eszköznek a rendszertől kapott valamilyen karaktersorozatot egy meghatározott algoritmus alapján át kell alakítania, majd visszaküldenie a rendszernek, oly módon, hogy ezt az átalakítást csak ő tudja az adott eredménnyel elvégezni. Erre a célra titkosító algoritmusok alkalmasak. Ennek a módszernek előnye a jelszóval szemben, hogy a valódi titok (a titkos kulcs) nem halad át a hálózaton.

A legsebezhetőbb rendszerek azok, ahol jelszavas védelem sem működik, hanem a hitelesítés csak felhasználói névhez, gépeknél pedig csak az IP címhez kötődik. A fenti módokon alapuló hitelesítési protokollok támadásának egyik legkézenfekvőbb módszere az, hogy a támadó a szükséges jelszót magától a felhasználótól szerzi meg (kifigyeli, kibeszélteti, stb.). A támadó a felhasználói azonosítót és az ahhoz tartozó jelszót megszerezheti akkor is, ha azt a hálózaton keresztül nyílt szövegként, titkosítás nélkül küldik át, és a támadó pedig képes az átvivő hálózathoz, illetve bizonyos hálózati elemekhez valamilyen módon hozzáférni. A hamis megszemélyesítés és jogosultságszerzés nagyon veszélyes támadás. A módszerrel a támadó akár teljes befolyást szerezhet a számítógépen, az adatokat megsértheti, megismerheti. A védekezés elsődleges alapja a minél erősebb azonosító eljárás és a tikosított kommunikáció alkalmazása. Fontos továbbá a humán felhasználók oktatása, meggyőzésük a biztonsági intézkedések betartásának szükségességéről és viselkedésük rendszeres ellenőrzése. E területen a támadási módszerek:

- jelszavak kifigyelése;
- jelszavak kicsalása;
- jelszavak megfejtése;
- jelszavak lehallgatása.

2. Hosztazonosítók hamisítása

Egy kiszolgálónak (hosztnak) lehet saját azonosítója (például az IP címe), olyan, amit a felhasználók ismerniük (például a www.tanulmany.hu forma). A kettő közötti oda-vissza megfeleltetést különböző protokollok segítségével a hálózati elemek végzik.

2.1. IP cím hamisítás

Bizonyos kommunikációs hálózatokban (például telefonhálózatokban) az igénybevevők felek azonosítását a hálózat felügyeletét ellátó alrendszer végzi, így a kommunikációban résztvevőknek nem kell a másik fél azonosításával, hitelesítésével foglalkozni. Az Internet óriási hálózatában azonban az azonosítást másként oldották meg. Az Internet Protokoll-ban a hosztok maguk helyezik el a feladót jelző forráscímet az IP csomagokban, a datagrammákban. Ebből kifolyólag az is előfordulhat, hogy véletlenül vagy szándékosan, hogy a berendezés úgy van programozva, hogy ne a saját, tényleges IP címét, hanem attól eltérő IP címet helyezzen el a kimenő csomagok forráscím mezejében (IP spoofing).

Az IP csomagot a hoszttól átvevő útválasztó elvileg képes ellenőrizni, hogy a hoszt hamis vagy valós forráscímet alkalmaz-e, azonban az útválasztók kezelői a felhasználó szervezeteknél, illetve az Internet-szolgáltatónál többnyire ezt az ellenőrzést nem végzik el. Az IP csomagok forráscímének hamisítása önmagában nem támadás, azonban több típusú támadásnak is kísérő feltétele vagy elősegítője. Hamisított forráscímű IP csomagokkal történő támadás esetén a megtámadott oldalon nagyon nehéz felderíteni a csomagok valódi feladóját, továbbá ha a támadó a hamisított címet állandóan változtatja, akkor a megtámadott oldalon az útválasztóban nehéz kiszűrni a támadó csomagokat. A hamis forráscím jellemző kísérője a szolgáltatásbénító támadásoknak, de feltétele a felépült kapcsolatba, hosztok közötti bizalmi viszonyba támadó számítógéppel történő belépésnek, hamis megszemélyesítésnek is.

A forráscím hamisítás elleni védekezés legegyszerűbb és leghatékonyabb módja az, ha az útválasztókból nem küldik tovább az olyan csomagokat, melyek nem az általuk kiszolgált hálózatokhoz tartoznak, melyek egy útválasztóba olyan interfészen érkeztek, amely mögött nem létezhet az érkezett forráscímmel rendelkező hoszt. A vizsgálat egyrészt az útválasztók ilyen vizsgálatokhoz szükséges erőforrásainak szűkössége miatt, másrészben pedig a gondos konfigurálás igénye miatt az útválasztókat üzemeltető szolgáltatóknál többnyire elmarad, mivel az IP címek vizsgálata a szűrések elvégzőjét, hanem az Interneten máshol lévő felhasználókat védik elsősorban.

2.2. DNS hamisítás

A felhasználók általában domain-névvel adják meg a felkeresni kívánt kiszolgálót (például a webszervert). A számítógép ilyenkor a konfigurációban megadott domain-név szerverhez (DNS) fordul, hogy megkapja a domain- névhez tartozó IP címet. Ha ennek a lokális név szervernek nincs birtokában a keresett cím, akkor elindul a domain-név fán és megkeresi azt a szervert, amelyik a választ meg tudja adni. A támadó több ponton is támadhatja a domain-név szerver rendszert. A magasabb szintű szerverek általában igen jól védettek, mivel kizárólag a domain-név szolgáltatást adják, felhasználóik gyakorlatilag nincsenek. Nagyobb a sikeres tá-

madás esélye a lokális szerverek, esetleg az átmeneti tároló (caching) név szerverek esetében. A helyi hálózatokban rendszerint többfunkciós szerverek adják a domain-név szolgáltatást is. Ha a támadó hatalmába tud keríteni egy ilyen lokális szervert, akkor a hálózat gépeinek kérdéseire tetszése szerinti IP címeket adhat válaszul.

A támadó a hamisított IP címen berendezhet egy olyan szervert, amely kapcsolatfelvétel során a felhasználó felé úgy viselkedik, mint az eredeti szerver, ezért a felhasználó nem veszi észre, hogy nem az általa kívánt hoszttal van kapcsolatban. Ebben a helyzetben azután többféle visszaélés követhető el. A támadó például hamisíthat egy bejelentkező weblapot, és így megtudhatja a felhasználó azonosítóját, jelszavát. A DNS hamisítás ellen a leghatékonyabb védekezés a digitális aláírás és tanúsító szervezet által hitelesített hoszt azonosítás, és annak felhasználói oldalon történő ellenőrzése.

3. „Belépés a kapcsolatba" típusú támadások

A kapcsolatba történő belépéses támadások jellemzője, hogy a támadó egy már kiépült, valamilyen formában hitelesített kapcsolatba épül be. E típusú támadásoknál az erős hitelesítés nem ad védelmet, mert a támadó ezzel a módszerrel megkerüli a hitelesítési eljárást. Különösen veszélyes, ha két gép között bizalmi kapcsolat van, és a hitelesítés pusztán csak IP cím alapján történik. A támadó dolga akkor a legkönnyebb, ha közel tud kerülni az adatátviteli hálózathoz. Ebben a helyzetben mindenekelőtt a lehallgatás merül fel, mivel így értékes információkhoz, jelszavakhoz lehet hozzájutni. A támadó célja azonban nem csak az lehet, hogy az áldozat nevében belépjen valamilyen rendszerbe, hanem az áldozatot olyan információval akarja megtéveszteni, amiről az áldozat azt hiszi, hogy az általa felkeresett rendszertől érkezik, miközben az adatot a támadó határozza meg.

A támadó beékelődik a két fél közé, miközben minden kommunikáció átmegy rajta úgy, hogy az átmenő adatokat céljának megfelelően módosíthatja, a felhasználónak hamis adatokat prezentálhat (esetleg a kiszolgálóval is hamis adatokat közöl). Így adott esetben a felhasználótól olyan információt is kicsalhat, amihez egyszerű lehallgatással nem jutna hozzá, mert a szituáció nem fordulna elő, a szerver ilyen információt nem kérne. E típusú támadás alapesete az, amikor a helyi hálózatot leválasztó útválasztó nem szűri ki a hamisított IP forráscímű csomagokat, a hálózaton belül pedig a hosztok nem titkosítva kommunikálnak egymással.

Ha az A hoszt már túljutott a hitelesítésen, ami után csupán IP cím alapján tölti fel a fájlokat a B hosztra. A támadó valamilyen szolgáltatásbénító támadással kizárja a kommunikációból az A hosztot, úgy hogy közben annak hamisított címével csomagokat küld a B hosztnak. Innentől lehetősége van arra, hogy a B hosztra a saját adatait bejuttassa. A válasz üzeneteket nem fogja megkapni, de ezek részben kiszámíthatók, másrészt nincs is rájuk szüksége. Ha az A hosztnak megfelelő jogosultságai voltak, akkor a támadó egy olyan könyvtárba juttathat be egy általa készített fájlt, amely a következő lépésben már számára a saját gépéről is teljes értékű hozzáférést tesz lehetővé a B hoszthoz. Strukturált kábelezésű kapcsolt helyi hálózatban a hosztok nem hallják egymás forgalmát, így ha a támadó hatalmába kerít egy hosztot, a másik hoszton folyó kommunikációt, az ott kiadott jelszót általában nem tudja lehallgatni. Az ARP (Address Resolution Protokoll – Címleképzési /

Meghatározó Protokoll) üzenetek manipulálásával azonban elérheti, hogy a rendszer úgy tudja, hogy a másik hoszt IP címére menő üzeneteket neki kell továbbítani. Így ha a másik hoszt már hitelesítette magát valahol, akkor ebbe a kapcsolatba be tud lépni, a válaszokat is megkapja.

A kapcsolat ellopása ellen leghatékonyabban a titkosított kommunikáció alkalmazásával lehet védekezni.

4. Kártékony programok

Kártékony, vagy kárt okozó programról (malware) beszélünk, amikor a számítógépen olyan programok vannak, amelyek a felhasználónak közvetlenül, vagy közvetve kárt okoznak, vagy okozhatnak. Kárt okozó programok kapcsán legtöbben a vírusra, férgekre, trójai és hátsó ajtót nyitó programokra gondolnak, de okozhat kárt, például egy rosszul megírt felhasználói program is, amely helytelen működése következtében a felhasználó akarata ellenére tesz kárt a számítógépen.

Ha a számítógépbe bejuttatott kártékony program működésbe lép, akkor az egyik lehetséges következmény és kár az adatok, információ részleges vagy teljes elvesztése, illetve azok illetéktelen kezekbe kerülése. Kárként jelenik meg másrészről a leállásból és helyreállításból fakadó üzemkiesés, annak elhárítására és a rendszer működőképességének visszaállítására fordított erőforrások költsége. A kártékony programokat a terjedés módja szerint három fő kategóriába sorolják: vírusok (virus), férgek (worm) és trójaiak (trojan). A kártékony programok családján belül specialitásuk miatt szokás megkülönböztetni a hátsó ajtót nyitó programokat (backdoor), amelyek nem rombolják közvetlenül a megtámadott rendszert, hanem kiszolgáltatják azt a támadónak.

4. 1. Vírusok

A vírus definíciójára a szakirodalomban többfajta meghatározás is létezik. A vírus általában egy olyan program, amely más programot fertőz meg oly módon, hogy a saját kódját beilleszti a megtámadott programba, ami ezután vírusként viselkedhet, így további programokat fertőz meg, így a vírusfertőzés mértéke folyamatosan nő. A megfertőzött vírust tartalmazó programot vírusgazdának nevezik. A vírus képes önmagát reprodukálni, vagyis esetleg módosított formában másolatot készíteni az őt alkotó kódrészletről. A vírus önmagában terjedni nem tud, minden esetben szüksége van egy másik programra, amely a vírust alkotó kódrészt futtatja. Csak olyan fájl válhat vírussá, melynek futtatásra alkalmas formátuma van. A vírusokat a fertőzött programok típusai szerint az alábbiak szerint osztályozhatóak.

- fájlvírusok;
- bootvírusok;
- makrovírusok;
- szkript-vírusok.

4. 2. Trójai programok

A trójai programot jóindulatú alkalmazásnak álcázzák, miközben ártó kódot tartalmaz. A trójai a felszínen hasznos, vagy esetleg szórakoztató funkciókat mutat, miközben a háttérben rejtve, ártó szándéktól vezérelten kártékony műveleteket végez az áldozat gépén. Miután a megtévesztett felhasználó aktív közreműködése a trójait sikeresen elindítja, az elrejtőzik. A trójai munkakönyvtára általában a rendszermappa eldugott alkönyvtárainak valamelyikében található meg, amit egy átla-

gos felhasználó nem szokott böngészni. Az első indulás után gyakori, hogy a trójai átnevezi magát, így megtévesztő néven fog futni, amit a felhasználó rendszerfájlnak gondol. Bizonyos fejlett trójai programok képesek úgy futni, hogy önmaguk a futó programok közt (tasklist) nem szerepelnek.
A bejuttatott trójai program egyes esetekben portot nyit a támadott hoszton, amely várja a kapcsolódást egy távoli – támadó – számítógépről. Ilyen esetekben, amikor a bejutott program lehetővé teszi a támadónak a megtámadott gép távoli irányítását már hátsó ajtóról (backdoor) beszélnek. Napjaink legelterjedtebb trójai programjai éppen a hátsó ajtót nyitó, rejtett távoli hozzáférést biztosító programok (RAT: Remote Access Trojan). Ezek a programok teljes hozzáférést biztosítanak a támadott hoszthoz, hozzáférhetővé teszik a merevlemezen tárolt állományokat, programokat tudnak futtatni, állományokat képesek le- és feltölteni, így a támadó teljes ellenőrzés alatt tudja tartani a támadott számítógépét. Néhány trójai esetében a szervercsomag – a beépített számos funkció miatt –nagy méretű, így ezeknek bejuttatását egy kis méretű, speciálisan erre a feladatra tervezett program (dropper) végzi. Előfordulhat, hogy a bejuttatott program kapcsolódik ki egy webhelyre, és onnan tölti le a parancsokat tartalmazó fájlt. Ez azért hatékonyabb módszer, mert ha a belső hálózatról elérhető az Internet, akkor a tűzfal nem tudja kiszűrni, hogy böngésző, vagy esetleg a kártékony program végez webes kommunikációt.
A behatolás után a károkozás mértéke csak a betörő szándékaitól függ. Bizonyos támadók rombolás céljából telepítenek trójai programokat a támadott gépre, ami gyakran dokumentumok, adatbázisok, levelek végleges elvesztését jelentheti. Más támadók csak rémisztgetni akarják áldozataikat, üzeneteket megjelenítve a képernyőjén. A módszer használatával előfordulhat az is, hogy a támadó a célhoszt adatbázisainak tartalmát módosíthatja, így a támadott döntés előkészítő folyamataira gyakorolhat hatást. A vírusoknál megismert indulási mód, mely szerint a vírus indítását az őt hordozó vírusgazda végzi el ezeknél az önálló programoknál nem tud működni. Ezek a programok az elindulásukat a gépen futó operációs rendszerre bízzák a feladatot, befészkelve magukat az automatikus indítási folyamatok közé.

4.3. Férgek

A féreg (worm) a vírustól annyiban különbözik, hogy kódját nem írja be a lemez boot szektorába, vagy valamely hasznos programba (vírusgazda), hanem önálló futtatható fájlban tartalmazza. A trójai programoktól viszont abban különbözik, hogy nem akarja magát hasznos programnak álcázva futtatni a felhasználóval, hanem képes a hálózatban különböző módszerekkel magát tovább terjeszteni. A terjedés során ugyanúgy gondoskodik önmaga elindulásáról, mint a trójai programok. Találkozhatunk azonban olyan féreggel is, amelyik csak az első elinduláskor végzi tevékenységét, ez idő alatt küldi magát el a lehetséges célpontok felé.
A férgek céljaik elérése érdekében három funkcióval – keresés, terjedés és kártékony kód futtatása – rendelkeznek. Hasonlóan a vírusok keresőrutinjához a férgek is áldozatokat keresnek, csak itt nem fájlokról, hanem további számítógépekről van szó. A keresést végző rész egyetlen feladata, hogy a rendelkezésre álló összes kommunikációs vonalat pásztázva további támadható célpontot találjon. A mai férgek megelégszenek a vezeték összeköttetésű hálózattal, azonban a közeljövőben számolni lehet azzal, hogy a későbbi férgek egyéb kommunikációs csatornákon

(például WiFi, Bluetooth) is áldozatokat kereshetnek. Abban az esetben, ha a féreg megfelelő célpontot talál, megpróbálja önmagát arra a helyre továbbítani.
A kártékony tevékenység nem minden esetben tartozik a féreg fő profiljához, de rombolhat is. Miután a féreg megfertőzött egy gépet, az azon végrehajtható rombolás mértéke már csak a támadó szándékaitól függ. A rombolás lehetséges mértékét befolyásolja, hogy a féreg a megfertőzött környezetben milyen (például rendszergazdai vagy felhasználói) jogosultságokkal rendelkezik. Sok féreg célja az, hogy hátsó kaput nyisson a fertőzött rendszereken. Van olyan gyakori metódus is, hogy a féregnek van egy terjedési időszaka, amikor az a cél, hogy minél több gépre eljusson, majd egy megadott – általában dátumhoz kötött – időpontban a féreg minden példánya aktiválja a kártékony kódot futtató funkcióját (logikai bomba), ami legtöbbször egy szolgáltatásbénító támadás valamelyik előre meghatározott célpont felé.

4.4. Egyéb kártékony programok

Vannak olyan kártékony programok is, amelyek nem biztosítanak teljes körű távoli hozzáférést, hanem csak egy-egy speciális célra kerültek kifejlesztésre, úgymint:

- jelszókeresők;
- billentyűzetfigyelők;

5. Szolgáltatásbénító támadások

Szolgáltatásbénító (DoS: Denial of Service) támadásnak azokat a támadásfajtákat nevezik, amelyek vagy a közvetítő hálózatnak rontják le az áteresztőképességét, teszik lehetetlenné a hasznos üzenetcsomagok áthaladását, vagy pedig a hosztokat terhelik le oly mértékben, hogy azok alig vagy egyáltalán nem lesznek képesek a hasznos hálózati kapcsolatok felépítésére.
A nagy terhelést okozó támadások egyik fajtája azon alapul, hogy a hálózatban igen nagy adatforgalmat gerjeszt, ezáltal mintegy forgalmi dugókat hoz létre a hálózat egyes szakaszain. A nagy terhelés megbénítja a hálózati kapcsolóeszközöket, de betelíti a közöttük lévő adatátviteli kapcsolatokat is. A támadások másik típusa a hosztokat célozza meg. A támadó a hosztot a hálózatról érkező nagy mennyiségű, rendszerint speciális adatcsomaggal, üzenettel árasztja el, aminek a feldolgozása annyira leterheli a számítógépet, annyira leköti az erőforrásait (CPU idő, memória), hogy a hasznos működésre képtelenné válik. Egyes speciális üzenetek akár önmagukban, vagy kis számban is alkalmasak arra, hogy a számítógépet olyan állapotba juttassák, hogy erőforrásait teljesen elhasználja, esetleg puffer túlcsordulás következzen be, a gép leálljon.
A szolgáltatásbénító támadások kivitelezésére jellemzően a hálózati protokoll hierarchia harmadik-negyedik szintjén lévő protokollokat (IP, ICMP, TCP, UDP) használják, amelyeknek rendszerint szabad átjárásuk van a hálózatban, a hálózati kapcsolóelemeken. E támadás alapesetében szükség van egy egységnyi idő alatt meglehetősen nagyszámú adatcsomagot kibocsátani képes számítógépre, ami egy viszonylag nagy átbocsátóképességű hálózati kapcsolattal rendelkezik, és erről a számítógépről küldenek minél több adatcsomagot a megtámadásra kiszemelt számítógépre. Ha a célpont egy gyengébb áteresztőképességű hálózati kapcsolattal rendelkezik, akkor ez a csatorna telítődik a támadó adatcsomagjaival, és a hasznos

forgalmat képező adatcsomagok csak alig, vagy egyáltalán nem jutnak át rajta. Ugyanez a helyzet akkor is, ha az áteresztőképesség az áldozat oldalán is elég nagy, de az ottani számítógép teljesítménye gyengébb. Ha olyan adatcsomagok kerülnek továbbításra, melyek feldolgozása sokkal több erőforrást igényel, mint azok kibocsátása, akkor a célpont nem lesz képes megbirkózni a terheléssel, így vagy csak minimális hasznos adat feldolgozására lesz képes, vagy pedig teljes mértékben leáll.

Az ilyen jellegű támadások esetében a legelterjedtebb típus az elosztott szolgáltatásbénító (DDoS: Distributed Denial of Service) támadás. Itt a támadási láncban multiplikátorok vannak, a támadásban nagyon sok számítógép vesz részt. A támadott hosztot, illetve annak hálózatát a támadást felügyelő számítógép irányítása alatt lévő számítógépek, az úgynevezett ágens árasztja el adatcsomaggal, így a támadásban részt vevő számítógépek és hálózatok egyenkénti teljesítményének nem kell kimagaslónak lennie ahhoz, hogy összességükben a legnagyobb teljesítményű hálózatok vagy hosztok megbénítására is képesek legyenek.

A multiplikátor számítógépek vagy olyan gépek, amelyek felett a támadó az irányítást átvette, és azokon céljának megfelelő programot futtat (úgynevezett zombi gépek), vagy a számítógépek szabályosan működnek, de a támadó az alacsonyabb szintű hálózati protokolloknak olyan tulajdonságait használja ki, amelyek önmagukban, nem szándékoltan is alkalmasak hozzájárulni a szolgáltatásbénításhoz. Az ágens számítógépek a támadás során legtöbbször nem a saját IP címükkel küldik a csomagokat, hanem hamisítottat használnak. A támadás folyamán nincs szükség arra, hogy a célponttól származó esetleges válaszüzenetek az ágensekhez visszajussanak. A hamisított IP címek megnehezíti az ágensek hálózatban elfoglalt helyének meghatározását, valamint a védekező oldalon egy hatásos csomagszűrés alkalmazását is. Az elosztott támadás velejárója, hogy rendkívül nehézzé teszi a támadás leállítását, mivel sok különböző hálózatból sok számítógépet kell elszigetelni, kiiktatni ahhoz, hogy a támadás megszűnjön, továbbá a támadást irányító számítógépet is szintén nagyon nehéz azonosítani. A szolgáltatásbénító támadások közvetlenül nem jelentenek veszélyt az adatokra, nem történik adatvesztés, adathamisítás, adatszerzés. Egyes esetekben azonban a támadók más támadások leplezése vagy megvalósíthatósága érdekében gátolják valamelyik hoszt, vagy hálózatrész működését, és így másodlagosan a szolgáltatásbénítás is szerepet játszik adatok ellen irányuló más jellegű támadás sikerre vitelében. A szolgáltatásban történő fennakadás ugyanakkor bizonyos szolgáltatás típusoknál természetesen önmagában is hatalmas károkhoz vagy veszélyekhez vezethet (például banküzem, felügyeleti, vagy irányító-rendszerek). A támadások fajtái lehetnek:

- SYN elárasztás;
- ICMP elárasztás;
- halálos ping;
- land-támadás;
- IP szegmentációs támadás;
- router interfész blokkolása;
- egyéb szolgáltatásbénító támadások.

6. A kiszolgáló számítógép gyengeségeit kihasználó támadások

6.1. Nyitott portok és sebezhetőségek felderítése

A hosztok nyitva lévő portja pontosan meghatározzák a rajtuk futó hálózati szolgáltatásokat, a gép hálózatban betöltött szerepüket, így a támadók is ezeket a portokat vizsgálják át előszeretettel ahhoz, hogy a rendszer réseit, gyenge pontjait távolról kifürkészhessék. A portok feltérképezését, vagyis a gépen vagy gépeken lévő nyitott portok keresését nevezik portszkennelésnek, amit még általában nem tekintenek támadásnak, de mindenképpen támadási kísérletet megelőző tevékenységnek tekinthető.

Az esetlegesen meglévő biztonsági rések, sebezhetőségek feltérképezésre irányuló eljárás a nyitott portok felderítésén túlmenően azt is vizsgálja, hogy az eddig ismert sebezhetőségek közül nincs-e már valamelyik jelen a támadott hoszton. E tevékenységhez a támadó egy jól felépített és naprakész adatbázist használ, ami tartalmazza az ismert sebezhetőségeket, illetve azt, hogy ezek meglétére milyen jelek utalnak. A különböző operációs rendszerek, valamint az egyes portok és az azokat kezelő alkalmazások vonatkozásában folyamatosan kerülnek napvilágra olyan hibák, sebezhetőségek, melyek megfelelő támadóeljárással távolról is kihasználhatók. A támadóeljárások szinte minden esetben széles körben is ismertté válnak. A támadó ezért gyakran úgy jár el, hogy az áldozat hoszt távolról történő feltérképezésével első lépésben megállapítja, hogy milyen sebezhetőségekre számíthat az adott hoszton, majd a második lépésben azokkal a támadási eljárásokkal próbálkozik, amelyek a lehetséges sebezhetőségeket használja ki.

Egy adott porthoz kapcsolódó szolgáltatás tehát nem más, mint egy hálózati kommunikációt folytató program, ami kimenetét nem a képernyőn jeleníti meg, hanem csak a háttérben fut. Az ilyen programok az úgynevezett démonok (daemon), illetve Windows terminológiával élve a szervizek (service). A böngészők, email kliensek ezekkel a démonokkal kommunikálnak a fenti portokon keresztül. Például egy megírt levél elküldésekor a levelezőprogram a háttérben a beállított levéltovábbító SMTP szerver 25-ös portjához csatlakozik, és továbbítja a levelet, mivel a megfelelő beállításokat használva pontosan tudja, hogy melyik porton keresztül kell a szervert keresni, hogy a levél sikeresen célba érjen.

6.2. Port-feltérképezési technikák

A portok feltérképezése – amellyel felfedezhetők a kiaknázható kommunikációs csatornák – folyamatosan zajlik az Interneten. A módszer lényege az, hogy a támadó a hálózaton át egymás után próbálja ki a hoszt valamennyi portját, majd feljegyezi azokat a portokat, amelyek valamilyen aktivitást, nyitottságot mutattak, megfeleltek az aktuális feltételeknek. A szkennelés végső célja, hogy a támadó felderítse a nyitott portokat a vizsgált hoszton. Erre a célra különböző technikák léteznek és nem mindegy, hogy az alkalmazott eljárás milyen gyors és milyen megbízható. Emellett ezek a módszerek részét képezik a modern hálózati monitoring technológiáknak is. A hálózati kommunikáció során a kliens és a szerver között felépülő csatorna különböző állapotokon megy keresztül. A kapcsolat létesítésétől a csatorna lezárásáig több állapot különböztethető meg, melyeket külön-külön lehet vizsgálni. A szkennelési típusok az alábbiak lehetnek:

- TCP Connect Scan;

- TCP SYN Scan;
- TCP FIN Scan;
- UDP „ICMP port elérhetetlen” Scan.

6.3. Sebezhetőségek feltérképezése

A biztonsági réseket, sebezhetőségeket feltérképező programok, az úgynevezett vulnerability scannerek azon felül, hogy portszkennelést végeznek, felderítik a gép sebezhető pontjait is. A biztonsági rést pásztázó programok alapja egy jól felépített és naprakész biztonsági rés adatbázis (vulnerability database). Működésük hasonló a fenti portszkennelési technikákhoz, csak ez kiegészül azzal, hogy a célgépen kiderített portokon futó szolgáltatások vonatkozásában megvizsgálja az ismert biztonsági hibák meglétét, így a támadó képet kap a hoszt sebezhetőségének mértékéről. A saját rendszerét ellenőrző rendszergazdának az ilyen módszerek nagymértékben segítik a munkáját, de a támadók gyakran alkalmazzák ezeket a módszereket valamely gép gyengeségének feltérképezésére a betörés előkészületeként. Az így kiderített gyengeségre a támadónak már csak a megfelelő támadó kódot (exploit) kell alkalmazni az eszköztárából, hogy eredményesen támadja a kiszemelt gépet.

7. Hálózati elemek gyengeségeit kihasználó támadások

Napjainkban a számítógépek hálózatba integrálása általánossá vált, így bármely szervezet rendszere gépek százait szervezi egységbe az információ hatékonyabb megosztása, feldolgozása érdekében. A hálózati struktúra tükrözi a szervezeti felépítést is: néhány gépből álló lokális hálózatokat hub-ok, hidak, kapcsolók és útválasztók csatolnak magasabb egységbe, amelyeket útválasztók, átjárók, tűzfalak kapcsolnak már általában a nagyterületű hálózatokat jelentő még magasabb egységbe. A hálózati elemek gyengeségei alatt olyan sebezhetőségeket kell érteni, melyek a hálózati architektúra kialakításából, vagy a hálózati protokollok tervezési elveiből, megvalósítási gyakorlatából, vagy a hálózat belső működéséhez szükséges berendezések (kapcsolók, útválasztók stb.) sebezhetőségeiből adódhatnak. Fajtái lehetnek:

- áthallásos hálózat lehallgatása;
- ARP tábla megmérgezése;
- forrás vezérelt útválasztás;
- kapcsolat eltérítése;
- routerek elleni támadások.

Összegzés

Napjainkban a számítástechnikai rohamos fejlődése révén odajutottunk, hogy minden kritikus infrastruktúrának van olyan infokommunikációs központja, alrendszere, ami az adott infrastruktúrában zajló folyamatokat vezérli, szabályozza, így gyakorlatilag már minden kritikus infrastruktúra egyben kritikus információs infrastruktúra is egyben, mivel az érintett infrastruktúra információs alrendszerét támadva a teljes rendszer működése akadályozható, befolyásolható, lebénítható. A kritikus információs infrastruktúrák számítógép-hálózati hadviselés eszközeivel történő támadása a potenciális elkövetők, támadók körét kiszélesítheti, tekintettel

arra a körülményre, hogy a szükséges eszközrendszer, a számítógép elterjedtségéből adódóan bárhol és bárki által viszonylag olcsón beszerezhetők, és különböző programok révén felvértezhetők olyan képességekkel, melyek fegyverré alakíthatják át, ami a földrajzi elhelyezkedéstől függetlenül alkalmazható. Ennek következtében ezekkel az eszközökkel végrehajtott támadások száma egyre nagyobb mértékben fog növekedni.

A kibernetikus térből érkező támadások célpontjai legtöbb esetben a polgári rendszerek, mivel ezek ellen a legkönnyebb a támadást kivitelezni, mert ezek általában kevésbé védettek, nincsenek fizikailag elválasztva a különböző intézmények belső, zárt rendszereitől, valamint egyéb más, közcélú, nyílt rendszerektől (például az Internetről). A „cyberbűnözők" által a gazdasági rendszerek (például bankok) ellen végrehajtott támadások száma is növekedő tendenciát mutat, minduntalan újabb és újabb módszerekkel, trükkökkel igyekeznek anyagi haszonhoz jutni.

A kritikus információs infrastruktúrák hálózatai általában már technikailag igen jól védettek, ahol biztonsági protokollokkal nehezítik az információkhoz való hozzáférést, azonban a tervezőknek több olyan körülménnyel is számolniuk kell (például hanyag, felelőtlen alkalmazottakkal), melyek áthatolhatóvá teszik az egészen biztonságosnak hitt rendszereket is. A fenyegetettség szintjét nehéz meghatározni, mert ezt befolyásolja a kiválasztott számítógépes hálózat típusa, az alkalmazott hardver- és szoftverkörnyezet, az operációs és biztonsági rendszerek fejlettsége, valamint az alkalmazott támadási módszer is.

A biztonság alapvető feltétele a védelmi rendszer egységessége, valamint a felhasználók jogosultságainak, tevékenységének és rendszerelemek működésének folyamatos adminisztrációja és ellenőrzése. A hardverek és szoftverek állandó fejlődéséhez hasonlóan támadók módszerei is folyamatosan változnak, finomodnak, így elengedhetetlen követelmény a biztonsági rendszerek állandó frissítése a preventív intézkedések meghozatala a biztonsági szakterületek mindegyikén.

Felhasznált irodalom:

[1] Haig Zsolt: Az információs társadalom információbiztonsága http://portal.zmne.hu/download/bjkmk/bsz/bszemle2008/4/12_Haig_Zsolt.pdf (Letöltés: 2009. 04. 20.);

[2] Haig Zsolt: Információs társadalmat fenyegető információalapú veszélyforrások. Hadtudomány, XVII. évf. 3. sz. 2007. szeptember. ISSN 1215-4121 http://www.zmne.hu/kulso/mhtt/hadtudomany/2007/3/2007_3_4.html (Letöltés: 2009. 04.);

[3] Haig Zsolt - Várhegyi István: A cybertér és a cyberhadviselés értelmezése, Hadtudomány, 2008 elektronikus szám. ISSN 1215-4121 (http://mhtt.eu/hadtudomany/2008/2008_elektronikus/2008_e_2.pdf Letöltés: 2009. 04. 22.);

[4] Haig Zsolt – Várhegyi István: Hadviselés az információs hadszíntéren 2005. Zrínyi Kiadó;

[5] Huszár Zsuzsanna: Info-kommunikációs technológiák (PTE - egyetemi jegyzet);

[6] Kovács László: Számítógépes hálózatok támadása, védelme. Budapest, 2004.

[7] Muha Lajos: A Magyar Köztársaság kritikus információs infrastruktúráinak védelme, PhD értekezés, 2007.;

[8] Varga János Péter: Kritikus információs infrastruktúrák értelmezése (Hadmérnök, III. Évfolyam 2. szám. 2008. június).

PAPP Zoltán – PÁNDI Erik – TÖREKI Ákos[63]

A FENYEGETETTSÉG EGYES ASPEKTUSAI AZ INFORMÁCIÓS INFRASTRUKTÚRÁK TEKINTETÉBEN[64]

Absztrakt: A közleményben a szerzők egyes olyan részkutatásaik eredményeit foglalják össze, amelyek az információs infrastruktúrák fenyegetettségének kérdéseivel és aspektusaival foglalkoznak.

Kulcsszavak: ellentevékenység, fenyegetettség, információs infrastruktúra, sérülés, támadás, zavarás.

1. A kritikus információs infrastruktúrák értelmezése

1.1. Az információ értelmezése

Az információ definiálása tudományonként eltér, de általában bizonytalanságot csökkentő, értelemmel bíró adatot értenek alatta, mely ennek megfelelően igen sokféle formában megjelenítve, különböző technológiájú adathordozón rögzítve létezhet. Az információ, hasonlóan fontos szerepet játszik a világban, mint az anyag és az energia. Az információ a megfelelő helyen, a szükséges időben és a kellő formában való rendelkezésre állása esetén olyan vagyonként – egyes értelmezések szerint erőforrásként – fogható fel, melynek értéke van, és ezt az értéket – más fontos üzleti javakhoz hasonlóan – a szervezetnek a hatékony működésének szempontjából védenie kell. Az információ analizálása során az alábbi jellemzőket lehet, illetve kell megvizsgálni, melyekből lehet következtetni, annak használhatóságára, minőségére:

- időszerűség, aktualitás, gyakoriság, időperiódus, megbízhatóság, jelentőség, teljesség, tömörség, terjedelem, igazolhatóság, egyértelműség, teljesítmény, világosság, pontosság, rendezettség, megjelenés, számszerűsíthetőség, elérhetőség.

Az információs hadviselés során alkalmazott különböző eljárások, módszerek arra irányulnak, hogy a fenti minőségi jellemzők manipulálása révén az ellenség döntéshozatali folyamataira ráhatással legyenek. Elérni kívánt cél az, hogy az ellenség a szükséges információkhoz ne jusson hozzá (elérhetőség), ne a szükséges időben kapja meg az információt (időszerűség és aktualitás), a kapott információk pontatlanok legyenek (pontosság) és ne legyenek ellenőrizhetők (megbízhatóság, igazolhatóság), stb. Amennyiben az alkalmazott eljárás, vagy eljárások összessége minél több minőségi jellemzőt érint, annál eredményesebbnek tekinthető az információs támadás.

1.2. Az infrastruktúrák általános értelmezése

Az infrastruktúra kifejezés, a magában foglalt jelentéstartalom folyamatosan bővül, hiszen a műszaki fejlesztéseknek, a technológiai megújításnak köszönhetően újabb és újabb infrastruktúraelemek, fajták jelennek meg. Utóbbi időkben éppen az

[63] Szerzők: Papp Zoltán őrgy. (BA, MA), Pándi Erik r. alez. (BA, MA, PhD), Töreki Ákos fhdgy. (MA, PhD-hallgató).

[64] Jelen közlemény a Bolyai János Kutatási Ösztöndíj támogatásával készült.

infokommunikációs infrastruktúra térnyerése és a „hagyományos” infrastruktúrákra gyakorolt hatása miatt vált esedékessé újraértelmezése. Az infrastruktúra feladata, hogy alapvetően biztosítsa egy adott ország igazgatásának, rendészeti szerveinek és gazdaságának normális működését, a termelést, a fogyasztást és az elosztás folyamatát a gazdaság mindenkori fejlettségének megfelelő szellemi és technikai színvonalon. Nélkülözhetetlen szerepet tölt be a bővített újratermelés biztosításában, valamint a lakosság életkörülményeinek javításában, a területi különbségek csökkentésében. Az infrastruktúra az infrastruktúrák rendszereire épül, azokat összefogja, egybekapcsolja. Ezek a rendszerek egymást feltételezik. Bármelyikük hiánya súlyos működési zavarokat okozhat, más infrastruktúrák működésének hatásfokát leronthatja, így védelmük, illetve – országok közötti konfliktus esetén – támadásuk kiemelt prioritást élvez.

1.3. Információs infrastruktúrák értelmezése, típusai

Az információs infrastruktúrák rendeltetésük szerint kettő csoportba sorolhatók:

- funkcionális információs infrastruktúra:
- Fizikailag teszik lehetővé a társadalom egy információs funkciójának zavartalan működését, tehát infrastruktúrális alapon információs alapszolgáltatásokat nyújt.
- támogató információs infrastruktúra:
- Létrehozzák, folyamatosan biztosítják a funkcionális információs infrastruktúrák kiterjedt halmazainak zavartalan működéséhez, fejlődéséhez szükséges anyagi és szellemi feltételeket, illetve egyéb támogatási hátteréket.

A funkcionális információs infrastruktúrák a különböző infokommunikációs rendszerek köré csoportosíthatók:

- különböző kiterjedtségű számítógépes hálózatok (LAN, MAN, WAN, WWW)
- vezetékes távközlő rendszerek (analóg, ISDN)
- vezeték nélküli távközlő rendszerek
- mobiltelefon rendszerek (GSM)
- diszpécser mobil földi hálózatok (TETRA)
- személyhívó rendszerek
- műholdas távközlési rendszerek
- műholdas navigációs rendszerek (GPS, GALILEO)

A támogató infrastruktúrák lehetnek:

- villamos energetikai ellátó rendszerek;
- elektronikai és informatikai vállalatok;
- elektronikai és informatikai kutatóintézetek;
- raktárak és nagykereskedelmi ellátó szervezetek;
- elektronikai és informatikai képzéssel foglalkozó intézmények.

Az infrastruktúrák általában valamilyen kapcsolatban, illetve összefüggésben állnak egymással, így kiterjedtségük alapján is lehet osztályozni őket:

- globális (világméretű);
- regionális (kontinentális (pl.: európai);

- nemzeti (országos).

A globális információs infrastruktúrák alatt összekapcsolt információs rendszerek és az őket összekapcsoló rendszerek világméretű összességét értjük, melyek magukba foglalják a kommunikációs infrastruktúrákat, számítógépeket és egyéb berendezéseket, szoftvereket, alkalmazásokat, az információtartalmat; az infrastruktúra összetevőit fejlesztő, gyártó, forgalmazó és szervizelő szervezeteket és személyeket, valamint az infrastruktúrákat használó szervezeteket. A regionális információs infrastruktúrák a globális információs infrastruktúrák szerves részének tekinthetők; a világot behálózó információs infrastruktúrák régiókra bonthatók, melyek lehetnek például kontinensek, vagy különböző szövetségi rendszerek által meghatározott határvonalak. A nemzeti információs infrastruktúrák alatt különböző szervezetek, eszközök és erőforrások széles körben hozzáférhető egységes rendszerét értjük, melyeknek elsődleges rendeltetése, hogy egy adott ország kormányzati, rendészeti, gazdálkodási, illetve egyéb szervezetei és állampolgárai alapvető információ- és információs szolgáltatás-igényeinek elsősorban az adott ország határain belüli kielégítése.

1.4. Kritikus információs infrastruktúrák értelmezése

Az infrastruktúrákra meghatározott definíciót ki lehet bővíteni az adott infrastruktúra kritikusságára vonatkozó ismérvekkel is, melyek tudományáganként, szakterületenként jelentősen eltérhetnek. A szakirodalom általában három jellemző köré csoportosítva vizsgálja a kritikusság mibenlétét:

- kiterjedés;
- súlyosság;
- időbeli hatás.

Az Európai Unió meghatározása szerint a kritikus infrastruktúrákhoz, azok a fizikai erőforrások, szolgáltatások és információtechnológiai létesítmények, hálózatok és infrastrukturális berendezések tartoznak, melyek működésének zavara, megsemmisülése komoly következményekkel járna az állampolgárok egészségére, biztonságára, védelmére, gazdasági jólétére, illetve az államigazgatás hatékonyságára. A kritikus információs infrastruktúrák a kritikus infrastruktúrák egy szűkebb részét jelenti. Az informatika jelenlegi fejlettségi szintjén ma már minden infrastruktúrát különböző bonyolultságú, tagolt szintű és rendeltetésű infokommunikációs rendszerek vezérelnek, irányítanak és ellenőriznek, így az információtechnológia vívmányaira épülő infrastruktúrák egy ország idegrendszerének is nevezhetőek, ezért önmaguk és részeik is kritikus infrastruktúrának minősülnek. A fentiek alapján a kritikus információs infrastruktúrák alatt az alábbiakat értelmezhetjük:

- energiaellátó rendszerek rendszerirányító infokommunikációs hálózatai;
- infokommunikációs hálózatok (vezetékes, mobil, műholdas);
- közlekedés szervezés és irányítás infokommunikációs hálózatai;
- vízellátást szabályzó infokommunikációs hálózatok;
- élelmiszerellátást szabályzó infokommunikációs hálózatok;
- egészségügyi rendszer infokommunikációs hálózatai;
- pénzügyi-gazdasági rendszer infokommunikációs hálózatai;
- ipari termelést irányító infokommunikációs hálózatok;
- kormányzati és önkormányzati szféra infokommunikációs hálózatai;

- védelmi szféra infokommunikációs hálózatai.

Az információs társadalom információs infrastruktúráinak komplex rendszere egymásra épülő, egymást feltételező, egymást kölcsönösen támogató infrastruktúrák szövevényes hálózataiból tevődik össze. Az összekapcsolódó infrastruktúrákon keresztül az esetleges üzemzavarból vagy szándékos támadásból fakadó problémák felhalmozódhatnak, váratlanabb és lényegesen súlyosabb működésbeli zavart okozhatnak az adott állam létfontosságú szolgáltatásaiban. Az infrastruktúrák összekapcsolódásai és egymástól való függőségei sérülékenyebbé teszi őket a különböző fizikai és információs támadásokkal szemben. Amennyiben az infrastruktúrarendszer bármely csoportját, elemét támadás éri, az közvetlenül vagy közvetve negatívan befolyásolja a vele függőségi viszonyban lévő más struktúrák működését is.

2. A kritikus információs infrastruktúrák működési zavarainak, sérüléseinek, támadásának és megsemmisülésének következményei

2.1. A kritikus információs infrastruktúrák elleni fenyegetések

A modern nyugati társadalmak működése szinte elválaszthatatlan módon kapcsolódik az információs infrastruktúrákhoz, illetve az általuk nyújtott szolgáltatásokhoz. Az állampolgárok ezen rendszereknek a működését természetesnek veszik, eredendőnek tekintik létezésüket. A körülöttünk lévő információs világot nagyszámú, bonyolult, komplex módon felépített és egymással szorosan együttműködő infrastruktúrák építik fel, így egyik működésének zavara különböző mértékben kihat a többi működésére is, és azokban is zavarokat, bizonyos esetekben teljes leállást okozhat. A kritikus információs infrastruktúrák vonatkozásában az alábbi veszélyeket különböztethetjük meg:

- szándékos, illetve ártó jellegű cselekményekkel, tevékenységekkel összefüggő veszélyek;
- bűncselekmények (gyújtogatás, rongálás, lopás, rablás, szabotázs, számítástechnikai rendszer és adatok elleni bűncselekmény, közérdekű üzem működésének megzavarása);
- gazdasági, vagy politikai indítékból, kritikus informatikai rendszerek és hálózatok ellen elkövetett visszaélések, illetve cyber-támadások;
- terrorcselekmények és annak eszköz, illetve járulékos cselekményei (kiemelten robbanóanyaggal, lőfegyverrel való visszaélés, CBRN támadások);
- fegyveres konfliktusok (háború, fegyveres csoportok támadása, polgárháború);
- természeti eredetű veszélyek, melyek az emberi tevékenységtől függetlenül, klímaváltozás, a természet erőinek hatására, elemi csapásként fordulnak elő;
- civilizációs eredetű, technológiai veszélyek, melyek az emberi tevékenységgel összefüggésben, helytelen emberi beavatkozás, mulasztás, figyelmetlenség, vagy technikai, konstrukciós hibák hatására következnek be.

Amennyiben a vizsgált körbe tartozó rendszerek a támadások célpontjai, úgy az eredményesség függvényében a társadalom egyre szélesebb rétegeire lehetnek kihatással. A társadalom belső viszonyait teljesen szétzilálhatja a közlekedési, a

kommunikációs, a gazdasági-pénzügyi rendszerek egyes elemeinek funkcionális kiesése, mivel a begyakorolt napi rutin megoldások megszűnésére nincsenek felkészítve az emberek és szervezetek. Például a közlekedés szervezését irányító rendszerek funkcióinak zavara jelentősen kihat a társadalom működésére. A lakosság mozgásának nehézségei miatt más infrastruktúrák üzemeltetésében résztvevő személyek nem jutnak el munkahelyükre, az áruszállítás akadályoztatásából adódóan az infrastruktúrák zavartalan működéséhez szükséges anyagok, áruk, szolgáltatások nem érnek célba, így a hatás más rendszerekre is kiterjedhet, átterjedhet.

A villamos energia-elosztó rendszerek kiesése szinte minden más infrastruktúra működésére, illetve azok szolgáltatására kihatással lehet. Itt nem elhanyagolható az időbeli hatás sem, ami különösen kritikussá teszi az ágazatot, mert hatása szinte azonnal jelentkezik más rendszereknél. Más infrastruktúrák az áramszolgáltatás átmeneti kiesésére általában rövidebb-hosszabb ideig fel vannak készítve (például egészségügyi intézményekben lévő áramfejlesztők lépnek üzembe áramkimaradás esetén), azonban ebben az esetben is más energiahordozókra vannak utalva (például egy kórház esetében az áramfejlesztők szénhidrogénekkel működhetnek), és amennyiben azok működésében is zavarok jelentkeznek, akkor a kérdéses rendszer, illetve infrastruktúra működésében szintén zavarok jelentkezhetnek.

2.2. A kritikus információs infrastruktúrák támadása

Egy ország ideghálózatának tekinthető kritikus információs infrastruktúrák ellenei támadások előkészítése, megszervezése és végrehajtása – információs műveletek keretében – rendkívül összetett és összehangolt tevékenységet feltételez, ami alatt egyrészt technikai, másrészt pedig humán oldali összetevőket kell érteni. A támadók akcióik sikeressége érdekében három pillérre építenek: az infokommunikációs rendszer elemeinek sérülékenységére, a védelem elhanyagolására, valamint a humánerőforrás jelentette kockázatokra. A katonai megközelítés szempontjából legfontosabb célobjektumok az ellenség alábbi létesítményei:

- vezetési rendszerelemei (eszközök, vezetési pontok, vezetők);
- fegyverirányító rendszereit és fegyverei;
- felderítő rendszerei;
- elektronikai hadviselési rendszerei;
- kommunikációs és híradórendszerei;
- informatikai eszközeit és rendszerei;
- információi;
- támogató és egyéb infrastrukturális létesítményei.

Azonban a kritikus információs infrastruktúrák nem csak katonai szervezetek, hanem hacker-ek (számítógépes hálózatokat feltörők), hacktivisták (politikai indíttatású hacker-ek), cracker-ek (programfeltörők, szoftverkalózok), jerk-ek (vandálok), phreak-ek (kommunikációs hálózatokat feltörők), számítógépes bűnözők, ipari kémek, sértődött alkalmazottak és terroristák célpontjai lehetnek, akiknek különbözőek a motivációik és eltérőek lehetőségeik. Az információs műveletek alapelve szerint a fenti célpontokon, célobjektumokon keresztül a katonai és adott esetben polgári, kormányzati, közigazgatási, ellátás-szervezési funkciókat is lehet, kell támadni. Az elv szerint nem az információs támadás közvetlen célpontjai je-

lentik a valódi célt, hanem azokon keresztül a befolyásolásra kiválasztott, tervezett vezetési funkciók akadályozása, korlátozása.
Technikai megvalósítás terén a végrehajtás többszörösen összetett feladat. Egy hatékony támadás csak több frontos, azaz egy időben több információs infrastruktúra támadását feltételezi. Továbbá van néhány olyan – ma már nagyon jól védett – kritikus információs infrastruktúra, ami hatékonyan nem is támadható információs oldalról, azaz a támadás hagyományos eszközöket – fizikai pusztítást, rombolást – feltételez. Ugyanakkor a XXI. században a modern fegyveres erők és gazdasági szervezetek által működtetett információs infrastruktúráik elterjedten használják ki az elektromágneses tér által nyújtott lehetőségeket a kommunikáció, navigálás, fegyverirányítás, ellenőrzés, felderítés során. Ezen a területen alkalmazott kifinomult, különböző rendeltetésű elektronikai eszközök jelentős mértékben tudják növelni a szervezetek hatékonyságát, illetve támaszkodnak is rájuk feladatok végrehajtása során. Ebből kifolyólag egy információs infrastruktúra elleni hatékony támadás során megkerülhetetlen az alkalmazott elektronikai eszközök elektromágneses energiák által történő támadása.

A humán oldali összetevők között kiemelt helyen a szükséges felkészültség meglétére kell gondolni. A rendkívül összetett és bonyolult, a legfejlettebb információtechnológiai és védelmi megoldásokat alkalmazó rendszerek támadása igen magasan képzett és felkészült szakemberek rendelkezésre állását igényli, akik kiképzése, vagy megnyerése rendkívül nehéz feladat lehet (például terrorista szervezetek számára).

2.2.1. A kritikus információs infrastruktúrák fizikai támadása

Az információs infrastruktúrák szolgáltatásainak megszüntetésének legegyszerűbb, legkézenfekvőbb módja a rendszer kritikus elemeinek, illetve összeköttetéseinek kiiktatása, fizikai megsemmisítése. Ez a legkülönbözőbb eszközökkel megoldható, függvényében annak, hogy a támadónak milyen eszközrendszerek állnak rendelkezésére, milyen messze van a céltól, illetve a kritikus infrastruktúrát milyen eszközökkel, módszerekkel igyekeznek megóvni a külső behatásoktól. A fizikai támadás érkezhet földről, levegőből, vízfelszínről, vagy éppen víz alól indított eszközök révén, de ide sorolhatók a helyszínen bevetett különleges erők is. Az infrastruktúrák egyszeri, vagy folyamatos támadása, pusztítása nagymértékben csökkenti annak használhatóságát. A fizikai támadások célpontjai lehetnek a már fentebb tárgyalt infrastruktúrák, melyek ellen bevetett eszközök, eszközrendszerek kiválasztása az adott szituációtól függ.

A fizikai támadásnak azonban lehetnek finomabb formái is. Az infrastruktúra zavarát, egyes elemei ideiglenesen lebénítását elő lehet idézni rombolás nélkül is. Ilyen megoldás lehet például az elektromos távvezetékekben rövidzárlatot okozó grafitbomba. Ezek a bombák ugyanúgy kerülnek alkalmazásra, mint hagyományos társaik, csak a robbanás következtében nem a kinetikus energia fejti ki a hatását, hanem a szétszóródó grafitszálak rátelepednek a távvezetékek lezáró ellenállásaira, aminek következtében azok vezetővé válnak, és a földön keresztül rövidzárlatot okoznak a távvezeték hálózatban.

A kritikus információs infrastruktúrák kisebb elemei (például a telekommunikációs átjátszóállomások tornyai) lényegesen kisebb fizikai védelemmel vannak ellátva, így azokat közelről, helyből primitív eszközökkel is tudják rombolni a

vandálok, bűnözők, esetleg terroristák, illetve az ellenség, akik cselekményeikkel az elem fontosságából adódóan a teljes rendszerben csak kisebb kiterjedésű zavarokat okozhatnak, bár ez a zavar a támadott elemek számának növelésével fokozható. Míg egy bonyolult felépítésű, összetett rendszer (például egy légi irányítási komplexum) lényegesen nagyobb védelmet élvez, így azt csak távolabbról, precíziós fegyverek alkalmazásával lehet sikeresen pusztítani, azonban egy eredményes támadás esetében mind a fizikai kár, mind a területi hatás lényegesen nagyobb lehet.

2.2.2. A kritikus információs infrastruktúrák támadása az elektronikai hadviselés eszközeivel

Az elektronikai hadviselés a katonai tevékenység azon része, mely az elektromágneses tér energiáinak elemzésével meghatározza, felderíti, csökkenti, vagy akadályozza az elektromágneses spektrum ellenség által történő használatát. Elősegíti az értékelő, döntéshozó folyamatokat, hozzájárul a szervezéshez és a szervezet hatékony irányításához. Az elektronikai védelem biztosítja az elektromágneses és egyéb fizikai tartományok saját részről történő hatékony használatát, az ellenség elektronikai támogató és ellentevékenysége, valamint a saját csapatok nem szándékos elektromágneses interferenciái ellenére.

Az elektronikai támogató tevékenység a fenyegetés azonnali jelzése érdekében az elektromágneses kisugárzások felkutatására, elfogására, azonosítására és helyének meghatározására irányul. Fontos terület az elektronikai felderítés, ami az információszerző tevékenység szempontjából általában kettős céllal kerülhet végrehajtásra. Egyrészt az infokommunikációs rendszerekben tárolt és továbbított adatokhoz való hozzáférés és azok felhasználása céljából. Másrészt a hatékony támadás kivitelezéséhez szükséges célinformációk megszerzése céljából.

A kritikus információs infrastruktúrák elleni támadások eredményessége nagymértékben függ attól, hogy a támadást végrehajtó birtokában van-e azoknak az információknak, melyek a támadni kívánt rendszer fizikai (földrajzi) elhelyezkedésére, strukturális összetételére, hardver és szoftver összetevőire, a rajta zajló adatforgalom céljára, mennyiségére, esetleges gyenge pontjaira, és annak jellegére, valamint az adott információs rendszer üzemeltetőire és felhasználóira vonatkoznak. Az elektronikai ellentevékenység az elektromágneses és irányított energiák alkalmazását jelenti abból a célból, hogy akadályozza, vagy csökkentse az elektromágneses spektrum ellenség által való hatékony használatát. Három fő szakterületre bontható:

- elektronikai zavarás;
- elektronikai megtévesztés;
- elektronikai pusztítás.

3. Összegzés

Magyar aspektusból tekintve bő fél évtizeddel ezelőtt kidolgozásra került a Magyar Információs Társadalom Stratégiáról (MITS) és annak végrehajtásáról szóló – napjainkban is hatályos – 1126/2003. (XII.12.) Korm. határozat, amely felvázolta (vizionálta) az e-Magyarország tudatos megvalósítását. E folyamatban az állami szektor szereplőinek kiemelt felelőssége van, hiszen hazánknak a tudásalapú társadalmi modell kialakításában vállalt elkötelezettsége Európai Uniós csat-

lakozásunkkal erősödött. Elérendő célként fogalmazódott meg, hogy Magyarországon tíz éven belül tudásalapú gazdaság, modern információs társadalom, állam és önkormányzat alakuljon ki. A felzárkózás egyik kulcsa az információs és kommunikációs technológiák alkalmazásának államapparátusban, közszférában, vállalkozásokban illetve az egyén szintjén történő kiterjesztésében és a gyakorlatba való sikeres átültetésében rejlik.

Az elmúlt évtizedben tehát létrejött az elektronikus szolgáltatások infrastruktúráját képező Elektronikus Kormányzati Gerinchálózat (EKG), majd az elmúlt néhány évben a Központi Elektronikus Szolgáltató Rendszer is [182/2007. (VII.10.) Korm. rendelet]. A védelmi szféra kommunikációs lehetőségeit illetően szintén változások álltak be. A zártcélú hálózatokról szóló 50/1998. (III.27.) Korm. rendelet 2006 végén hatályosult módosítása alapján a korábbi hálózatgazdák száma jelentősen, mintegy harmadára csökkent, ami révén a Miniszterelnöki Hivatalt vezető miniszter, a legfőbb ügyész, valamint a honvédelmi miniszter tarthatta meg státuszát. A centralizáció révén a fennmaradt hálózatgazdák együttműködési kötelezettsége természetszerűleg fokozódott. A centralizációs folyamatok ellenére az Új Magyarország Fejlesztési Terv elfogadásáról szóló 1103/2006. (X.30.) Korm. határozat azonban a magasabb minőség elérésének egyik akadályaként azonosítja be a közszolgáltatások alacsony szintű infokommunikációs támogatottságának helyzetét. A joganyag a közszolgáltatások korszerűsítését az e-közigazgatás és az e-közszolgáltatások infrastruktúrájának fejlesztésében jelöli meg, amelynek egyik szerves részeként tekinthetők a védelmi célú infokommunikációs rendszerek is. E sajátos – és a szövetségi tagsági viszonyainkból adódó – lokális fejlődési folyamatok mellett globális kihívások is megjelentek, úgymint a kritikus infrastruktúrát érintő biztonsági kockázatok, veszélyeztetettség, illetőleg fenyegetettség. A kormányzatok által összeállított e-közigazgatási stratégiák alapján megállapítható a tervezett komplex magyar e-kormányzati infrastruktúra néhány jellegzetessége, így a létrejövő megoldások centralizáltak lesznek, interneten vagy az EKG-n keresztül elérhetővé válnak, alapvetően szolgáltatásorientált architektúra alapon fogják tervezni, valamint webes technológiákra fog épülni. Ezek a tervezési elvek olyan tipikus fenyegetéshalmazt jelentenek, melyekkel minden rendszernek számolnia kell. A magyar szakirodalom eddig kevéssé foglalkozott a speciális e-közigazgatási fenyegetésekkel, azonban a tervezett technológia ismeretében további, releváns fenyegetésekkel lehet számolni. A centralizációs folyamatok révén a korábban szétosztott információk egy földrajzi helyen, akár egy belső hálózaton sőt, a virtualizációt figyelembe véve akár egy számítógépen is megtalálhatókká váltak. Védelmi intézkedéseket alkalmazás szinten nem lehet megfogalmazni, így környezeti biztonsági célokat lehet kialakítani. A magyar kormány jól láthatóan eltökélt az informatikai (infokommunikációs) biztonság kultúrájának elterjesztésében. Az első fontos lépéseket megtette, vagy éppen megtenni készül. Ez a munka azonban lassan halad, a biztonsági fenyegetések egyre szaporodnak, így szükség van olyan tudományos munkára, amely segíti a lerakott alapokra történő építkezést. Ezen terület igen sajátos aspektusának tekinthetők – többek között – a katonai rendszerek, hiszen a Magyar Köztársaság Nemzeti Katonai Stratégiájáról szóló 1009/2009. (I.30.) Korm. határozat 27. pontja előirányozza a híradó és informatika területe rendszerszemléletű fejlesztésének hálózatalapú működés kialakítása révén történő

megvalósítását. Látható, hogy a nagyfokú integráltság okán a kockázatok, illetőleg fenyegetettség alól a honvédelmi szféra sem mentesülhet. A nemzeti katonai kommunikációs rendszerek lokális és globális biztonsági helyzete, a kormányzati rendszerekkel való együttműködésük okán fellépő veszélyeztetettségük kevéssé tisztázott, így az elméleti alapok meghatározása véleményünk szerint a jövő egyik tudományos feladatának tekinthető, amelynek egy igen vékony szegmensét kívántuk jelen közleményben bemutatni.

Felhasznált irodalom:

[1] A Nemzetbiztonsági Hivatal Évkönyve, 2003. Budapest, ISSN 1785-9212;
[2] Az informatikai biztonság kézikönyve. Verlag Dashöfer Szakkiadó, Budapest, 2002.;
[3] Gyányi Sándor: DDOS támadások veszélyei és az ellenük való védekezés. Hadmérnök, 2007. november 27. Különszám. ISSN 1788-1919;
[4] Green Paper on a European Programme for Critical Infrastructure Protection. Brussels, 17.11.2005. COM(2005) 576 final;
[5] Haig Zsolt – Várhegyi István: Hadviselés az információs hadszíntéren 2005. Zrínyi Kiadó;
[6] Dr. Kovács László: Számítógépes hálózatok támadása, védelme. Budapest, 2004.;
[7] Dr. Lencse Gábor: Hálózatok biztonsága (egyetemi jegyzet);
[8] Magyar Információs Társadalom Stratégia, IHM, 2003.;
[9] Muha Lajos: A Magyar Köztársaság kritikus információs infrastruktúráinak védelme, PhD értekezés, 2007.;
[10] Munk Sándor: Információs színtér, információs környezet, információs infrastruktúra;
[11] MTA-SZTAKI: Az informatikai hálózati infrastruktúra biztonsági kockázatai és kontrolljai (2004.);
[12] Varga János Péter: Kritikus információs infrastruktúrák értelmezése (Hadmérnök, III. évfolyam 2. szám. 2008. június);
[13] Váti KHT: Az infrastruktúra szerepe a területi fejlődésben, a térszerkezet és az infrastruktúra fogalmai

NIEBERL József

VEZETÉK NÉLKÜLI SZENZORHÁLÓZATOK

Napjainkban az élet minden területén több száz elektronikai eszköz vesz bennünket körül. Az informatika rohamos fejlődése már néhány évvel ezelőtt lehetővé tette kis méretű, alacsony tápfeszültségről üzemelő számítógépek építését. Lendületet kapott az ezekből az eszközökből épített szenzorhálózatok kutatása, fejlesztése.

Az eszközök összekötésére, hálózatba szervezésére különböző adatátviteli interfészeket, protokollokat alkalmaznak. A vezetékes megoldások mellett egyre inkább elszaporodnak a vezeték nélküli kommunikáció eszközei. Ez az átvitel technika nem csak a kábeleket, a fix topológiát szünteti meg, hanem szabadságot, kényelmet és mobilitást biztosít számunkra eszközeink hordozhatósága és könnyű áttelepítése okán.

A számítógépek közötti vezeték nélküli kommunikációt IEEE szabványok írják le. Az eltérő igényeknek megfelelően sokféle különböző vezeték nélküli hálózattípus létezik, amelyek adatátviteli sebességben, hatótávolságban, energia- és erőforrásigényben is széles skálán mozognak.(RF ID, Bluetooth, ZigBee, WiFi, GSM, GPRS, UMTS, WiMax, stb.). Léteznek olyan vezeték nélküli megoldások is melyek nincsenek felkészítve hálózatban való működésre és az adatbiztonság kérdéseket sem kezelik megfelelően.

A hálózatokban ISM(Industrial, Scientific, Medical frekvenciasáv) sávú rádiós kommunikációt alkalmaznak, felmerült az igény szabványok kidolgozására, amelyek biztosítják több rendszer egymás mellett élését, együttműködését. A ZigBee rendszerek felépítése működése nemzetközi szabványban rögzített (IEEE802.15.4). E szabvány alapján kialakíthatók közepes és nagyméretű vezeték nélküli szenzorhálózatok. Nagy biztonságú AES titkosítást használó, robusztus, kis energiaigényű rendszer. Mindez a legkisebb fogyasztás mellett tetszőleges (fa, csillag, háló) topológiában. Hálózati, biztonsági és alkalmazási rétegek specifikációjával ellátott eszköz. A kapcsolat megvalósítás általában az integrált funkciók és a programozható szoftver használatának kombinációjával történik. Létrehozhatóak vele intelligens, autonóm hálózatok.

A teljes szabvány és annak számtalan alkalmazási lehetőségének ismertetése nélkül kiemelnék néhány fontos tulajdonságot, melyek átgondolása rávilágít ezen technológia alkalmazási területeire, előnyeire. Ezek az eszközök helyi lokális vezeték nélküli hálózatot hoznak létre. A hálózat egy kitüntetett pontja az adatkoncentrátor, ami általában egy átjáró is az egyéb globális hálózatok felé.

A topológiák megértéséhez ismernünk kell az eszközzel megvalósítható kapcsoló típusokat.(Node-okat) Ebből háromféle létezik.

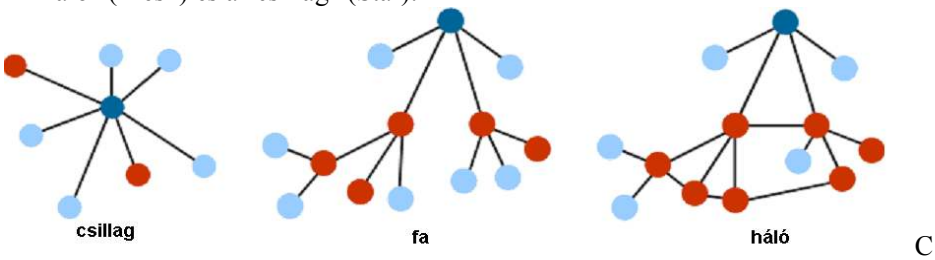
A Co-ordinator, melyből minden applikációban általában egy darab szerepelhet. Rendszerint ezzel kapcsolódik a hálózat a központi adatgyűjtő egységhez vagy

külső hálózatokhoz. Ez az eszköz kapja a nullás azonosítót, és ő vezérli a frekvenciaválasztást. Ezen kívül még számos funkciót lát el az inicializálásban is.

Router az node, amely a fa és háló topológiák használatakor a különböző egységeket összeköti egymással. Üzeneteket továbbít az egyik pontból a másikba. A csillag topológiában nincs rá szükség, mert itt a Co-ordinator tölti be ezt a szerepet. A fában olyan pozícióban vannak, hogy mind fel, mind lefele képesek eljuttatni a csomagokat. A háló összeköttetésekben bárhova kerülhetnek, ahol engedélyezni kívánjuk a keresztirányú adatáramlást.

End Device-nak hívjuk azt a node-ot, mely a hálózat végpontjain áll. Adatküldésre és fogadásra alkalmas, de továbbításra nem. Ez az eszköz képes sleep módba menni, hogy takarékoskodjon az energiával.

A felsorolt kapcsoló típusokból három topológia hozható létre. Ez a "fa" (Tree), A "háló" (Mesh) és a "csillag" (Star).



C sillag topológia: A középpontban egy Co-ordinator áll, mely az őt körülvevő End Device-okkal kommunikál. Ez a legegyszerűbb és a leglimitáltabb kiterjedésű hálózati megvalósítás. Előnye az egyszerűség, könnyű tervezés, direkt kapcsolatok. Hátránya hogy csak korlátolt hatókörű.

Fa struktúra: A Co-ordinator nem csak végpontokkal, hanem Routerekkel is kapcsolatban áll, melyek kiterjesztik a hatótávolságot, és elágazásokat is létrehoznak, így nő az áthidalható távolság és az eszközök száma.

Háló: Abban különbözik a fa topológiától, hogy itt a Routerek és End Device-ok egymás közt is küldenek adatot, így rövidebb, biztonságosabb utak jöhetnek létre. Leprogramozható hogy adott node meghibásodása esetén a hálózat hogyan reagáljon.

A ZigBee rétegek alapvető definíciói az OSI modellnek megfelelőek.

A fizikai réteg(PHY) specifikálja az adatátviteli szolgáltatást az interfésztől a fizikai átvitel megvalósításának lényegéig. Ez a layer irányítja a rádiófrekvenciás adásra vonatkozó beállításokat. Kezeli a csatornaváltásokat, az energia és jelvezérlést. Interfész funkciója van.

A legkisebb fogyasztás érdekében minimalizálták a kitöltési tényezőt, amely az az idő, melyen belül aktívan adó teljesítmény van jelen a rendszerben. Ennek érdekében, a lehetőségekhez képest minél nagyobb frekvenciára van szükség.

A stack réteg az az átmenet, mely összeköti a program által megvalósított funkciókat a fizikai réteggel. A Stack-ből vezérelhető a rádió, a kódolás, a címek megadása. Itt jönnek létre a kapcsolatok, itt tárolódnak a beállított profilok és iktatódnak be a gyártó-specifikus elemek. Ebben a rétegben jelenik meg a licencek és a

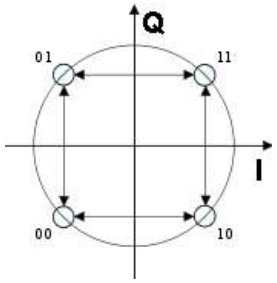
hálózat közti kapcsolat, itt generálódnak a biztonsági szintek. Általában a Stack automatikusan meghívódó függvények együttese.

Applikációs szint. Ide kerül az általunk megírt program, és itt kerül végrehajtásra. Meg kell felelnie bizonyos normáknak, hogy értékátadás jöhessen létre a Stack felé. Ennek a rétegnek része az APS , amely a fontosabb elemek közti kommunikációt valósítja meg.

A ZigBee szabványt implementáló áramkörök az általános mikroprocesszor elemeken túl rendelkeznek néhány kiegészítő modullal.

Az AES titkosítás gyorsító, egy 128bites titkosító kódot kezelő koprocesszor. A fő processzor minimális beavatkozása árán egy állandó, kapcsolatba ágyazott védelmet biztosít. AES-CCM (Counter with CBC-MAC encryption) egy olyan titkosító eljárás, mely csomagonként biztosít gyors kódolást és dekódolást. A hitelesítés mértéke függ a kód hosszától. Ez a feltételezés abból indul ki, hogy minél hosszabb egy titkosítandó kód, annál nehezebb lesz azt visszafejteni. A vevőket úgy alkották meg, hogy azok aktiválni tudnak egy újraküldés elleni védelmet is. Ezek után minden chip ACL-jében (acces controll list) definiálja, hogy mely kapcsolatokhoz melyik titkosítási szintet használja, és milyen kulcsot küld el. (bővebb információ: Irodalomjegyzék - AES kódolásról)

A MAC gyorsító a CRC ellenőrző kódok generálását, és a címek ellenőrzését végzi. Ezen kívül automatikus nyugtákat is hivatott küldeni, valamint belső időzítővel méri és jelzi a túl sokára, vagy az abszolút meg nem érkező válaszokat.



Az O-QPSK (Offset Quadrature Phase Shift Keying) modem az első igazi rádiós blokk a chipben. Itt történik meg a moduláció és a demoduláció. Ez a digitális modulációs eljárás azon alapul, hogy a vivőjel több fázissal rendelkezhet. Az egyes információkat az kódolja, hogy a jel a fázisok közt hogyan váltakozik. (egyes fázisok más és más bitet reprezentálnak) Az O-QPSK négy különböző fázisátmenetet különböztet meg. A maximális fázisugrás 90°, szemben a hagyományos QPSK-val, ahol ez 180° volt. Ez azt eredményezi, hogy a jel sosem megy át az origón, hiszen egyszerre csak egy bit változhat.

A Rádió 2.4 GHz-es az ISM sávban működik, ami ingyenes alkalmazást tesz lehetővé. A nemzetközi szervezetek ezt a sávot jelölték ki engedély nélküli haszná-

latra. A sáv mindenütt szabadon igénybe vehető a világon, ami rendkívüli térfoglalást tesz lehetővé.

A ZigBee protokoll néhány újszerű eleme:

Alkalmazásprofilok: A ZigBee az alkalmazás profilokon keresztül támogatást nyújt a csomópontok közötti egységes kommunikációra. Egy profil az alkalmazások üzeneteinek formátumára vonatkozó megegyezés. Egy meghatározott célú hálózatban az alkalmazások előre definiált üzeneteket váltanak egymással, például egy épületautomatizálási rendszerben a kapcsolók és a lámpák között ki-bekapcsolásra vonatkozó üzenetek továbbítódnak.

Eszközök felderítése: Egy, a hálózatba bekerülő csomópont előzetes konfiguráció nélkül képes kapcsolatot teremteni az általa igényelt alkalmazásprofilt támogató eszközökkel. Erre a felderítés (discovery) funkció nyújt lehetőséget. Lehetőség van egy meghatározott eszköz egy adott végpontjáról lekérdezni, hogy milyen profilt támogat, illetve egy azonosító alapján meg lehet határozni a keresett profilt támogató eszközök listáját.

A protokoll támogatást biztosít továbbá az adatátvitel hitelességének és bizalmasságának biztosítására, az útvonalak felderítésére, a rádió adási, vételi üzemmódjának szabályozására, az előforduló hálózati hibák kezelésére.

Összefoglalva, a ZigBee alkalmas különféle topológiájú adatgyűjtő hálózatok kialakítására, a szenzorok számára elérhető alacsony energiafogyasztás mellett. További előny az alkalmazási réteg fejlettsége, a hálózat önjavító képessége.

Perspektívák

A ZigBee jó lehetőséget kínál szabványos megoldások létrehozására. Rengeteg lehetőség kínálkozik a vezetékes átvitel ésszerű kiváltására, a komfort vagy a költséghatékonyság miatt.

Használható biztonsági rendszerekben, beltéri, kültéri környezetmonitorozó rendszerekben, lakossági, ipari, katonai területeken veszélyes anyagok, gázok jelenlétének érzékelésére, ezek hosszútávú monitorozására. Személy, áru, veszélyes anyag épületen belüli (ahol a GPS technológia nem alkalmazható) azonosítására, követésére. Olcsó megoldás lehet a közlekedésben szükséges azonosítási problémák megoldására (Felhajtott e a jármű egy útszakaszra? Nem szükséges fizikai kaput építeni, kialakítható egy biztonságos vezeték nélküli elektronikus kapu is a kérdés megfigyelésére). Használható továbbá épületfelügyeleti, energiagazdálkodási, szellőztető rendszerekbe. Audio átviteli kódolást tömörítéssel, titkosítással is meg lehet valósítani.

Rendkívül nagy biztonságú személy, áru, veszélyes anyag követés alakítható ki ezen eszközök felhasználásával. Mivel ezek az áramkörök programozhatók, az adóteljesítményük is programból szabályozható, beépített AES titkosító processzorral rendelkeznek így kitűnően alkalmazhatók biztonsági rendszerekbe is. Ellentétben az RF ID eszközökkel nem szükséges nagy teljesítményű gerjesztés a chipek aktiválásához. Ez a tulajdonság kizárja az RF ID technológiát a veszélyes illetve robbanóanyagok követési megoldásaiból. Az RF ID eszközök kifejezetten csak

rövidebb azonosító kódot képesek kommunikálni néhány 10 cm távolságba. A ZigBee eszközök alkalmazásával lehetőség van az azonosításra kis energiájú adóteljesítmény mellett (0.01mW) néhány méteres mikrócellán belül is. Például kiemeltek-e egy doboz robbanóanyagot a szállító jármű rakteréből. A rendszer azonnal képes jelezni, mikor, hol, ki végezte a műveletet, amennyiben a jármű, a kezelők és a robbanóanyagok is el vannak látva azonosító eszközökkel.. Az eszközök képesek egyéb környezeti adatokat is mérni, például hőmérséklet, páratartalom, fény stb., mely adatok a robbanóanyag környezetéről is információkat szolgáltat.

Rendkívül fejlett az energiafelhasználás és menedzselés ezekben az áramkörökben, egy AA méretű elem használatával, percenkénti mérés- kommunikáció esetén is kialakítható 3-5 évig is üzemképes eszköz.

Biztonsági szempontból az eszközök igen magas fokú adatbiztonság elérését teszik lehetővé a teljes kommunikációs csatornán a szenzortól az elemző központig, így megbízható hálózatok építhetők illetéktelen lehallgatásokkal, támadásokkal szemben. Ugyanakkor ezek az eszközök mindenki számára elérhetők, szabadon engedélyek nélkül is használhatók azaz a bűnözök és terroristák kezében is ugyanezt a hatékonyságot biztosítják.

Alkalmazási példa:

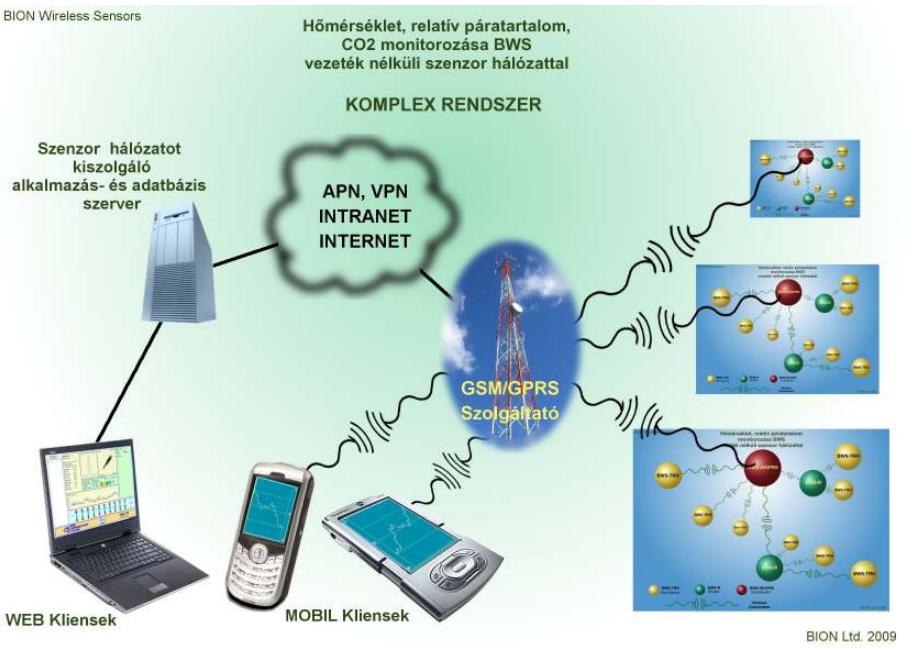
BWS (BION Wireless Sensors) szenzorrendszer alkalmazása beltéri levegőminőség ellenőrzésére

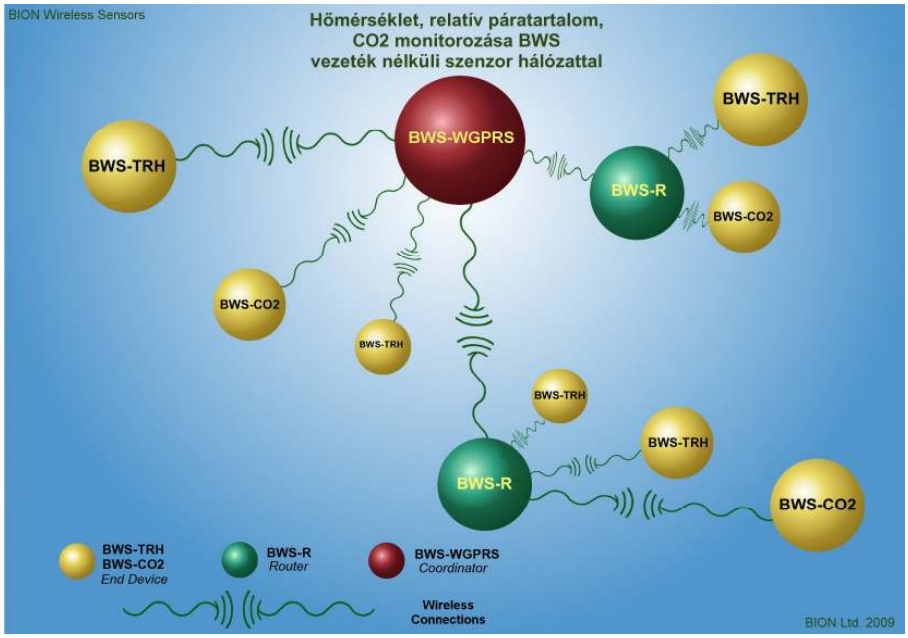
A levegő minőség kérdéskörével egyre több tudományos kutatás, ipari megoldás és törvényi szabályozás foglakozik. A közvetlen környezetünk, otthonunk, munkahelyünk és egyéb közösségi terek levegőminőség kérdéskörével a beltéri levegőminőség(indoor air quality) szabványok előírások foglalkoznak. A bemutatott rendszer a beltéri levegő minőség mérésére monitorozására készült.

A rendszer funkciói:

Beltéri levegőminőség jellemzéséhez szükséges paramétereket méri, az adatokat egy helyi vezeték nélküli hálózaton (ZigBee) keresztül valamint a GSM/GPRS hálózaton keresztül egy központi adatkezelő szerverhez továbbítja. A mért adatok: hőmérséklet, páratartalom, CO2, opcionálisan veszélyes gázok, szálló por. A mért adatok adatbázisba kerülnek tárolásra, a valós idejű és a korábban mért értékek megjeleníthetők WEB-es és Mobil alkalmazások segítségével. A rendszer az üzemeltetéshez szükséges adatokat is méri, kezeli. Ilyenek az elemállapot, térerő viszonyok, stb. A rendszer alkalmas légtisztító berendezések vezérléséhez.

A rendszer felépítése:





A rendszer működése:

A szenzorok mérik az adott jellemzőt (Temperature, RH, CO2, Dust, stb.) ezeket a jellemzőket a lokális vezeték nélküli ZigBee hálózaton keresztül egy adat-

koncentrátorhoz továbbítják. A szenzorok különböző kivitelűek, elemes illetve hálózati tápellátással rendelkeznek.

Az adatkoncentrátor fogadja a beérkező adatokat, kontrollálja a ZigBee hálózat működését. Az adatok a koncentrátorból GPRS kommunikációt használva a központi adatkezelő szerverhez jutnak, itt adatbázisban tárolódnak. Szintén ehhez a szerverhez kapcsolódnak a felhasználók WEB illetve Mobil eszközökkel. Az adatok megjelenítését mindkét platformon JAVA alkalmazások, illetve MIDLET-ek biztosítják.

A rendszer előnyei:

- Szolgáltatás orientált
- Távolról (Interneten keresztül) tetszőlegesen vezérelhető, ellenőrizhető
- A szenzorhálózat által nyújtott szolgáltatások dinamikusan bővíthetőek
- A hálózat struktúrája működés közben alakítható és bővíthető
- Vezeték nélküli, kétirányú kommunikáció
- Folyamatos szenzor-adat elérést tesz lehetővé
- Folyamatos a hálózati funkciók monitorozása
- Riasztások, eseménykezelés, statisztikák
- Megbízható
- Szabványos

Felhasznált irodalom

[1] 802.15.4 IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)

[2] ZigBee Specification http://www.zigbee.org/en/spec_download/download_request.asp

[3] ZigBee Alliance http://www.zigbee.org/

[4] http://www.cs.berkeley.edu/~daw/papers/15.4-wise04.pdf (AES titkosításról)

[5] Data Sheet – JN5121 Jennic (chip datasheet)

[6] [6] http://standards.ieee.org/getieee802/download/802.15.4-2006.pdf

JURENKA Oszkár

GYORSAN TELEPÍTHETŐ, SŰRÍTETT LEVEGŐVEL KITOLHATÓ, MECHANIKUS, TELESZKÓPOS ÉS SZAKASZOLT ÁRBOCOK

HAZAI KÉPVISELET

HOELLER ELECTRONIC KFT.
H-2092 Budakeszi, Fő u. 29.
Tel : +36 (23) 450 188 - Fax : +36 (23) 452 333
E-mail : iroda@hoeller.hu
Website: www.hoeller.hu

KÖZPONT ÉS ANGLIAI GYÁR

CLARK MASTS TEKSAM LTD
Binstead, Isle of Wight, PO33 3PA
Tel : +44 (0)1983 563691
Fax : +44 (0)1983 566643
E-mail : sales@clarkmasts.com

A CLARK MASTS GYORSAN FELÁLLÍTHATÓ ÁRBOCCSALÁDJA

QT ÁRBOCOK
KÉNYELMES ÉS KÖNNYŰ ÁRBOCOK SZÁZFÉLE CÉLRA

A kézipumpával kitolható teleszkópos QT árboc antennák felemelésére, hangtechnikai mérések elvégzésére, levegőszennyezettség mérésére és sokféle egyéb olyan készülék elhelyezésére alkalmas, amelyeknél a forgathatóságra nincs szükség.

ST ÁRBOCOK
KISMÉRETŰ ÁRBOC,
RÁZÁSÁLLÓ KONSTRUKCIÓ

Az ST teleszkópos árboc 3 hüvelykes alaphenger átmérőjű és a PT típusú árbochoz hasonlít, csak kisebb az átmérője és a fajlagos teherbírása is. A kinyújtás után forgatható. Ámbár szeret használat esetén ideális, ha a feltelepítés nem szükséges vagy terjedelmes.

MT ÁRBOCOK
GYORS ÉS KÖNNYŰ EMELÉS -BEHÚZÁS

Az MT típusú árboc négy hüvelykes hengerekből áll, amelynél a kitolt és visszahúzott állapotban maradó szakaszok hosszarányának köszönhetően a másfél vagy két hüvelyk átmérőjű felső szakasz felemelése akár 10 és 20 kg közötti lehet a kívánt magasságtól függően. Kizárólag digitálcserés kivitelben kapható.

QT ÁRBOCOK
KÉNYELMES ÉS KÖNNYŰ ÁRBOCOK SZÁZFÉLE CÉLRA

A kézipumpával kitolható teleszkópos QT árboc antennák felemelésére, hangtechnikai mérések elvégzésére, levegőszennyezettség mérésére és sokféle egyéb olyan készülék elhelyezésére alkalmas, amelyeknél a forgathatóságra nincs szükség.

PT ÁRBOCOK
AZ EREDETI TELESZKÓPOS CLARK ÁRBOC

A PT típusú árboc anyaga edzett alumíniumötvözet, teleszkópos szakaszai lehetővé teszik a forgatást is. A PT árboc talprészén levegőcsatlakozó található. Ideális eszköz tanulmányokra és közvetítő kocsiban való használatra.

YT ÁRBOCOK
KINYÚJTVA ERŐS, BEHÚZVA KOMPAKT

Az YT sorozat a PT árboc család továbbfejlesztése. A talprésze ott azonos átmérőjű, azért terhelhetősége és kinyújthatósága némileg nagyobb, mint 45 cellás társáé. Kis behúzási magasságnál és hosszú dejű kinyújtás esetére mindkét típus el van látva vezetőgallérral és zárócsavarral. Tartozékok sokasága áll rendelkezésre a különböző járművekhez a telepítés könnyítésére.

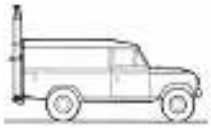
CLARK MASTS – GYORSAN FELÁLLÍTHATÓ ÁRBOCRENDSZER

ÁRBOCTELEPÍTÉS

A *CLARKMASTS* minden terméke alkalmas zöldmezős, járműves vagy objektumhoz rögzített telepítésre. Ehhez gazdag tartozékcsomag áll rendelkezésre. Ha a telepítéshez segítségre van szüksége, akkor szíveskedjék felvenni a kapcsolatot a Clark Masts céggel és utolérhetetlen tapasztalattal rendelkező szakembereink örömmel segítenek a kérdéses telepítési probléma megoldásában.

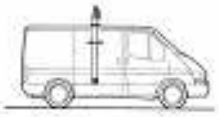
SZABADTÉRI TELEPÍTÉS

A csak részben állandó szabadtéri telepítéshez a tartozékok széles választéka áll rendelkezésre, beleértve a terílenből és kevlarból készült alsó, középső és felső árbocmerevítő köteleket, az árboctalp szerelvényeit és a földbe verhető cövekeket is. A merevítő kötelek élettartamát adnak automatikus megfeszítésre és az árboc forgatására a rakonyasávú antennák tényleges beállításához, ehhez azonban nem kell a meglévő telepítést újrakezdeni, ha az antennát más irányba akarjuk állítani.



KÜLSŐ TELEPÍTÉS JÁRMŰRE VAGY OBJEKTUMRA

Jármű vagy objektum külső részére (például házfalra) a külső telepítőbilincsek használatával szerelhetjük fel az árbocot. A szerelvények az állandó helyre telepített árboc rögzítése mellett 360 fokos forgathatóságot és az antenna beállítása után irányrögzítést is lehetővé tesznek. Az árboc teljes forgathatósága kinyújtott és behúzott állapotban egyaránt megmarad. A terílen és kevlar merevítő kötelek az ilyen típusú telepítésnél is használhatók. Részben állandó szerelésre a csukló rögzítőbilincsek alkalmasak, amelyek lehetővé teszik az árboc gyors lebontását.



TELEPÍTÉS JÁRMŰ BELSŐ TERÉBE

Az árboc telepíthető a tetőcsomagtartón keresztül a jármű belső terébe vagy konténerbe is. A tetőmezőbe szerelt időjárásvédett csapágyperselyben az árboc körbeforgatható. Az árbocon belső figyelmeztető kapcsoló helyezhető el, amely a jármű mozgását megakadályozza az árbock kinyújtás ideje alatt.

TELEPÍTÉS TETŐCSOMAGTARTÓRÓL

Ez a módszer lehetővé teszia behúzott állapotban is hosszúárboc tetőcsomagtartón való tárolását abban az esetben, amikor végégésre szerelve függőleges helyzetben túl hosszú lenne. A csomagtartóról görgőcsapokon lefelé dőlésre kerül az árboc vízszintesből függőleges helyzetbe, majd az első része az árbocteljon rögzítődik. Ezt követően az árboc kihúzható és a kitörő kötelekkel a szokásos módon megerősíthető. A teleszkópos árbocok ebben az esetben akár 34 méterre is kinyújthatók.

CLARK MASTS – GYORSAN FELÁLLÍTHATÓ ÁRBOCRENDSZER

CLARK MASTS™

- MINŐSÉGI TERMÉKTÁMOGATÁS
- MINŐSÉGI VEVŐSZOLGÁLAT

Szupererős árbocok

XT Árbocok		
Típus	Teljes magasság	Maximális fejterhelés
4 szakaszos árbocok		
XT40-4	4.08 m	130.0 kg
XT60-4	6.08 m	130.0 kg
XT80-4	8.08 m	130.0 kg
XT100-4	10.00 m	130.0 kg
5 szakaszos árbocok		
XT50-5	5.08 m	130.0 kg
6 szakaszos árbocok		
XT6-6	6.08 m	130.0 kg
XT8-6	8.08 m	120.0 kg
XT10-6	10.08 m	110.0 kg
XT12-6	12.08 m	100.0 kg
XT15-6	15.08 m	80.0 kg
XT18-6	18.08 m	60.0 kg
XT26-6	26.08 m	50.0 kg
8 szakaszos árbocok		
XT90-8	9.00 m	90.0 kg
XT110-8	11.08 m	75.0 kg
XT140-8	14.08 m	65.0 kg
XT200-8	20.08 m	50.0 kg
XT300-8	30.08 m	40.0 kg

Vontatható árbocok		
Típus	Teljes magasság	Maximális fejterhelés
602/15	15.00 m	65.0 kg
602/21	21.00 m	40.0 kg
602/30	30.00 m	15.0 kg
604/15	15.00 m	80.0 kg
604/18	18.00 m	60.0 kg
604/26	26.00 m	50.0 kg
604/30S	30.00 m	40.0 kg

Katonai árbocok

TYPE 73 árbocok		
Típus	Teljes magasság	Maximális fejterhelés
T5/10	10.00 m	75.0 kg
T5/13	13.00 m	75.0 kg
T5/16	16.00 m	70.0 kg
T5/18	18.00 m	70.0 kg
T5/20	20.00 m	60.0 kg
T5/24	24.00 m	55.0 kg
T5/30	30.00 m	50.0 kg

PU árbocok		
Típus	Teljes magasság	Maximális fejterhelés
PU5	5.00 m	10.0 kg
PU8	8.00 m	10.0 kg
PU10	10.00 m	10.0 kg
PU12	11.40 m	10.0 kg

Series 90 árbocok		
Típus	Teljes magasság	Maximális fejterhelés
90/10	10.00 m	300.0 kg
90/16	16.00 m	280.0 kg
90/20	20.00 m	250.0 kg
90/24	24.00 m	220.0 kg
90/30	30.00 m	200.0 kg
90/40	40.00 m	100.0 kg

CLARK MASTS – GYORSAN FELÁLLÍTHATÓ ÁRBOCRENDSZER

A CLARK MASTS 1957 ÓTA FEJLESZTI ÉS GYÁRTJA A MECHANIKUS, SZAKASZOLT, TELESZKÓPOS ÉS SŰRÍTETT LEVEGŐVEL FELÁLLÍTHATÓ ÁRBOCRENDSZEREKET

WT ÁRBOCOK

ERŐS ÁRBOC, AKÁR 30 MÉTERRE IS KITOLHATÓ

A WT árbocok nagyobb szilárdsága a 8 colos árboctalpnak köszönhetően lehetővé teszi a 30 méter emelési magasság elérését. Mobil használat esetén csak vízszintes helyzetben szállítható. Ehhez többféle tetőnyereg is rendelkezésre áll.

XT ÁRBOCOK

LEGERŐTELJESEBBEK A VÁLASZTÉKBAN

Az XT árbocok előnye a kikötés nélküli stabilitás. Képesek akár 130 kg teherhelést is elviselni. A járműre vagy járműbe az árbocok függőleges helyzetben vannak beépítve. Szilárdsága következtében a mai telekommunikációs berendezések többségénél nélkülözhetetlen.

VONTATHATÓ ÁRBOCOK

PÓTKOCSIRA SZERELT TELESZKÓPOS ÁRBOC

Az opcióként rendelhető 802 és 804 típusjelű berendezés valóban a legértékesebb, flexibilis és gazdaságos eszköz, ha rádiótornyok vagy más készülékek gyors telepítésére van szükség 30 m magasságban. Példa: mobiltelefon antenna.

TYPE73 ÁRBOCOK

FÜGGŐLEGESEN KITOLHATÓ SZAKASZOLT ÁRBOCOK

Jellemző tulajdonságok: Alumíniumötvözetből készült árbocszakaszok, a kikötést szabályozó csörlőrendszer, a háromlábú szerelő szerkezet és az árbocemelő felvonó. Ez jellemzi a klasszikus TYPE 73 árbocot 1970 óta.

PU ÁRBOCOK

EGYSZERŰ KONCEPCIÓ, KIFINOMULT RÉSZLETEK

A maga nemében páratlan megoldás a PU teleszkópos árboc kézi kitolhatósága. Az egyes szakaszokat keresztcsap rögzíti. Terepen vagy járműre építve minden környezetben használható

SCAM ÁRBOCOK

ROBUSZTUS, PNEUMATIKUS, TELESZKÓPOS ÁRBOCOK

A hadseregben eltöltött 35 évi bizonyította, hogy a járműre szerelt SCAM ideális választás terepen állva saját súlya fokozza a stabilitást. Esetleg újabb felhasználási terület lehet a modern légi felderítő eszközök magasba emelése.

SERIES 90 ÁRBOCOK

A 40 MÉTERES NAGY ÁRBOCEMELŐ

A szakaszolt árboc 100 kg antennateherhelést enged és 40 m magasra emelhető nagy stabilitással és biztonsággal. Négylábú emelőszerkezet, központos szabályozású (90°) feszítő kötelek. Az egyszerű emelő több árboc telepítésére felhasználható.

CLARK MASTS – GYORSAN FELÁLLÍTHATÓ ÁRBOCRENDSZER

TÖREKI Ákos – TÓTH András[65]

A MAGYAR HONVÉDSÉG ÁLLANDÓ TELEPÍTÉSŰ KOMMUNIKÁCIÓS RENDSZERÉNEK SZERVEZETI HÁTTERE

Absztrakt: Amint az köztudott – főként szakmai berkekben – a Magyar Honvédség katonai kommunikációs infrastruktúrájának alapját két fő információtovábbító rendszer alkotja. E két pillér nem más, mint a tábori kommunikációs rendszer, valamint az állandó telepítésű (stacioner) kommunikációs rendszer. Jelen közleményünkben ez utóbbi üzemeltetésére, fenntartására kialakított szervezeti elemek bizonyos szintig mélyülő struktúráját, továbbá helyét és szerepét kívánjuk elemezni, amelyből levont következtetéseink a katonai kommunikációs (infokommunikációs) rendszerek tárgykörében megkezdett kutatásaink első részeredményeinek összefoglalásaként is tekinthető. Anyagunk révén egyúttal betekintést kívánunk nyújtani a Magyar Honvédség felsőszintű híradó és informatikai rendszerei szakirányításának rendjébe, metodikájába.

Kulcsszavak: Hadműveletei és Kiképzési Főosztály, Honvéd Vezérkar, Honvédelmi Minisztérium, Informatikai és Információvédelmi Főosztály, Magyar Honvédség, szakirányítás, Támogató Dandár, zártcélú hálózatok, 43. Nagysándor József Híradó és Vezetéstámogató Ezred.

Bevezetés

A Magyar Honvédség állandó telepítésű kommunikációs rendszere lényegében zártcélú hálózatnak tekinthető a vonatkozó jogszabályok alapján. A zártcélú hálózatok körében az elmúlt alig fél évtizedben mélyreható változások történtek, amelyet nagyfokú centralizálás jellemzett. Napjainkban lényegében három hálózatgazda funkcionál hazánkban: a legfőbb ügyész, a Miniszterelnöki Hivatalt (MeH) vezető miniszter, valamint a honvédelmi miniszter. Legfajsúlyosabb hálózatgazdának a MeH miniszter tekinthető, így a hálózatok együttműködése terén megváltozó körülményekhez a honvédelmi ágazatnak is szükségszerű volt igazodnia.

1. Szakmai irányítás, hálózatgazdai feladatok

A honvédelmi tárca, valamint a Magyar Honvédség híradó-informatikai felsőszintű szakirányítási rendje összetett halmazt alkot, mint szakmai, mint pedig szolgálati tekintetben. A Honvédelmi Minisztérium apparátusán belül két főosztály végzi a szakterület vezetésével, irányításával kapcsolatos feladatokat.

Az Informatikai és Információvédelmi Főosztály a honvédelmi miniszter alárendeltségében a jogi szakállamtitkár közvetlen irányítása alatt végzi a tárcaszintű, tárcaközi, valamint nemzetközi informatikai szakfeladatokat, továbbá az információvédelmi szakterület felsőszintű tervezési, szervezési és irányítási feladatait.

A Hadműveleti és Kiképzési Főosztály viszont a Magyar Honvédség katonai szervezetei híradó és informatikai rendszereire vonatkozó szabályzók kidolgozását,

[65] Szerzők: Töreki Ákos fhdgy. (MA, PhD-hallgató), Tóth András fhdgy. (MA, PhD-hallgató).

a végrehajtás szakmai irányítását végzi, továbbá minisztertől átruházott jogkörben felel a Magyar Honvédség zártcélú távközlési és informatikai hálózat hálózatgazdai szakmai feladatai[66] ellátásáért is. A főosztály szervezetileg a Honvédelmi Minisztériumba integrált Honvéd Vezérkar részét képezi, tehát a Honvéd Vezérkar főnökének alárendeltségébe tartozik.

2. Működés, üzemeltetés

A zártcélú hálózat üzemeltetési, fenntartási feladatait ellátó réteg a felsőszintű irányításhoz hasonlóan ugyancsak összetett. Elkülöníthetünk hálózat üzemeltetői és katonai üzemeltetői funkciókat, melyek az alábbi ábra alapján illeszkednek a szakmai hierarchiába:

1. ábra: Az üzemeltetés szakmai irányítási rendszere
Forrás: HM HKF

Visszatérve a közlemény címéhez, nézzük meg a stacioner rendszereket működtető szervek helyét, szerepét és felépítését.

3. Hálózatüzemeltetés

Az országos hálózat üzemeltetési rendjéért egy vezérkar közvetlen katonai szervezet, az MH Támogató Dandár felel, tehát a dandár jelenik meg, mint hálózatüzemeltető. A dandár jogállású szervezetet a honvédelmi miniszter 2007. január 1-jei hatállyal alapította többek között a Nagytarcsa helyőrségben felszámolt MH Híradó és Informatikai Parancsnokság feladatköre zömének integrálásával.

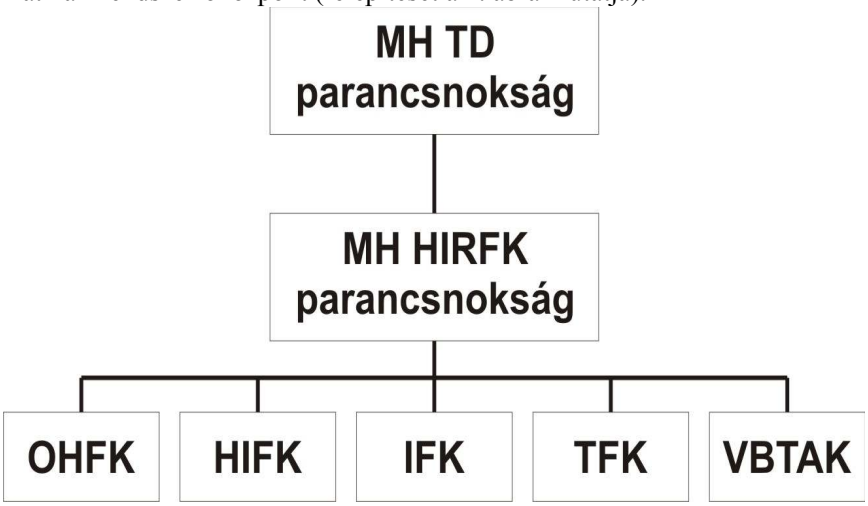
Az alapító okirata így fogalmaz a dandár alaptevékenységéről (a szakterület vonatkozásában): *„A Honvédelmi Minisztérium (...) és a katonai felső vezetés*

[66] Lásd: a zártcélú távközlő hálózatokról szóló 50/1998. (III. 27.) Korm. rendelet.

*részére a híradó, informatikai és elektronikus információvédelmi szolgáltatások és azok technikai feltételeinek biztosítása…"*67

Bár a fenti sorokból még nem derül ki a Támogató Dandár hálózatüzemeltetői státusza, tovább tanulmányozva az alapító okiratot, illetve ismerve a szervezet felépítését megjelennek azok a feladatkörök és a rájuk épülő alegység(ek), melyek mutatják azt.

A híradó és informatikai szakfeladatok ellátására a dandáron belül egy külön szervezeti elem került kialakításra, melynek struktúrája merőben eltér minden más katonai egységétől, alegységétől. Ez a végrehajtó alegység az MH Híradó és Informatikai Rendszerfőközpont (felépítését a 2. ábra mutatja).



2. ábra: Az MH Híradó és Informatikai Rendszerfőközpont felépítése
Készítette: Töreki Ákos

A Rendszerfőközpont a dandár híradó és informatikai szakfeladatokat ellátó ezred szintű szervezete. Rendeltetése a HM és a katonai felső vezetés béke- és minősített időszaki kommunikáció technikai feltételeinek biztosítása, az MH zártcélú távközlő és informatikai hálózatának üzemeltetése, felügyelete, információvédelmének biztosítása.

Alegységei feladatrendszeréből kitűnik, hogy tárcaszintű, illetve a Magyar Honvédség egészére kiterjedő szakmai területet fednek le tevékenységükkel.

Az Országos Hálózat-felügyeleti Főközpont (OHFK) végzi például a HM és a katonai felső vezetés zártcélú távközlő és informatikai hálózatainak üzemeltetését, a teljes (országos) hálózat távfelügyeletét, továbbá végrehajtja a hálózati aktív elemek konfigurálását, a forgalmi adatok gyűjtését és feldolgozását és ezáltal a hálózat működésének elemzését.

A Híradó és Informatikai Főközpont (HIFK) – az illetékességi körébe eső objektumok vonatkozásában – biztosítja a HM és a katonai felső vezetés nyílt és védett kommunikációja technikai feltételeit.

[67] A Magyar Honvédség Támogató Dandár alapításáról szóló 121/2006. (HK 23.) számú HM határozat.

Az Informatikai Főközpont (IFK) fő feladata a katonai információs rendszerek informatikai követelményrendszerének meghatározása, a megvalósítási és működtetési javaslatok kidolgozása, továbbá részt vesz az információs rendszerek megvalósításában is.

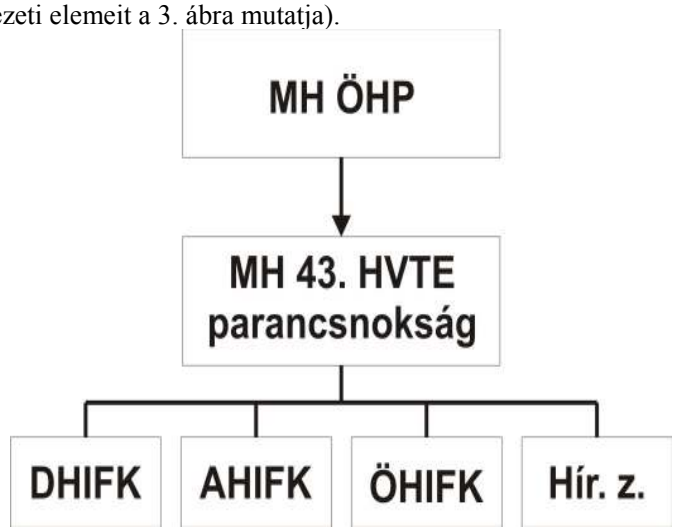
A Távközlési Főközpont (TFK) a Magyar Honvédség híradó és informatikai rendszerei üzemeltetésével, fenntartásával és fejlesztésével kapcsolatos tervező-szervező és adminisztratív feladatokat végzi.

A Vezetésbiztosító és Támogató Alközpont funkcióját tekintve mobil kommunikációs feltételeket képes biztosítani a vezérkar részére tábori körülmények között.

Mindazok mellett, hogy a Támogató Dandár – szakalegysége révén – biztosítja az országos hálózat üzemeltetési feltételeit, a hálózatgazda szakmai irányítása mellett felelős az erőforrásokkal történő gazdálkodásért és a hatósági állásfoglaláshoz szükséges adatszolgáltatásért is, továbbá ellátja a HM Hadműveleti és Kiképzési Főosztály szakmai képviseletét a fejlesztési célú beruházások során.

4. Katonai üzemeltetők

A stacioner kommunikációs rendszer katonai üzemeltetői szegmensét az MH Összhaderőnemi Parancsnokság adja, végrehajtó katonai szakmai szervezete az MH 43. Nagysándor József Híradó és Vezetéstámogató Ezred (híradó és informatikai szervezeti elemeit a 3. ábra mutatja).



3. ábra: Az MH 43. Nagysándor József Híradó és Vezetéstámogató Ezred híradó és informatikai alegységei
Készítette: Töreki Ákos

Az ezred biztosítja az Összhaderőnemi Parancsnokság és alárendelt katonai szervezetei részére a híradó és informatikai szolgáltatások igénybe vételét, felhasználhatóságát a stacioner – nyílt és védett – híradó és informatikai központok üzemeltetésével.

A Dunántúli Híradó és Informatikai Főközpont (DHIFK), valamint az Alföldi Híradó és Informatikai Főközpont (AHIFK) biztosítja az ország dunántúli, illetve alföldi régiójába eső katonai objektumok vonatkozásában a nyílt kommunikáció

technikai feltételeit. Ezen túlmenően adatokat gyűjt az adott régió stacioner híradó és informatikai hálózatáról.

Az Összhaderőnemi Informatikai Főközpont (ÖHIFK) a Magyar Honvédség zártcélú informatikai hálózatának második szintű támogatását végzi, valamint üzemelteti az Összhaderőnemi Parancsnokság informatikai rendszerét.

A Híradózászlóalj rendeltetése az Összahderőnemi Parancsnokság vezetési pont hírközpontjainak telepítése, üzemeltetése, vezetési rendszerének megfelelő tábori hírrendszer kiépítése és üzemeltetése a meglévő állományával és eszközeivel.

Összegzés, megállapítások

Megállapítható, hogy a közigazgatás területén megváltozott irányítási struktúrához a honvédelmi ágazat is igazodott, átalakítva mind az irányító, mind a végrehajtói szintjeit. Összességében látható, hogy a hálózatüzemeltető és katonai üzemeltető feladatok – amellett, hogy más-más léptéket képviselnek – szakmailag nem különíthetők el, mivel azok egymásra épülnek. Ahhoz, hogy a végfelhasználói kör számára a vezetési igényeknek megfelelő szolgáltatás váljon elérhetővé, elengedhetetlen a szakmai együttműködés.

A közleményben felsorakoztatott, az állandó telepítésű hálózat üzemeltetését, fenntartását végző szervezetek a szakirányítás rendjének megfelelően, szoros együttműködésben látják el feladatukat annak érdekében, hogy a vezetés és irányítás technikai feltételei minden időben biztosítottak legyenek mind a katonai szervezetek, mind az állami (közigazgatási) szervezetek irányába.

Felhasznált irodalom:

[1] http://www.hm.gov.hu/miniszterium/jogi_szakallamtitkar
[2] http://www.hm.gov.hu/miniszterium/hm_informatikai_es_informaciovedelmi_foosztaly
[3] http://www.hm.gov.hu/miniszterium/hm_hadmuveleti_es_kikepzesi_foosztaly
[4] Pándi Erik – Takács Attila: A hazai közigazgatás elektronizálásának helyzete, Hadtudományi Szemle, I. évf. 1. szám, Budapest, 80-84. oldal, 2008.
[5] 121/2006. (HK 23.) számú HM határozat a Magyar Honvédség Támogató Dandár alapításáról
[6] 123/2006. (HK 23.) számú HM határozat a Magyar Honvédség 43. Nagysándor József Híradó és Vezetéstámogató Ezred alapításáról

TÓTH András[68]

A TÁBORI C2 AUTOMATIZÁLT VEZETÉSI ÉS IRÁNYÍTÁSI RENDSZER ALKALMAZHATÓSÁGA A MAGYAR HONVÉDSÉG CSAPATVEZETÉSI RENDSZERÉBEN

A C2[69], mint képesség az érvényben lévő híradó és hadműveleti követelmények alapján egy zászlóaljharccsoportra vetítve került kidolgozásra elméleti síkon, figyelembe véve a jelenlegi híradó és informatikai erőket, eszközöket. Az elmélet kidolgozásánál az alábbi hadműveleti és híradó követelmények, tevékenységek kerültek figyelembe vételre:

A, a hadműveleti tevékenységek típusa:

- hagyományos hadviselés, támadás, védelem;
- békefenntartó, kikényszerítő műveletek;
- szakalegységek tevékenysége;
- válságreagáló műveletek;
- CIMIC70, PSYOPS71, HUMINT72 tevékenység;
- együttműködési tevékenység

B, az információ csere (hang, adat, kép, szöveg, stb.) követelményeit figyelembe véve a hangsúly az információ jellemzőin van:

- hordozó típusa (adat, hang, video stb.)
- minősége (gyakoriság, időbeniség, biztonság)
- mennyisége (terjedelem, sebesség)

C, a zászlóalj képességei nemzeti követelmények alapján:

- támadó és védelmi műveletek megvívása különböző időjárási és terepviszonyok között nappal és éjszaka (korlátozott látási viszonyok között) egyaránt;
- saját csapatok oltalmazása és védelme;
- a siker kifejlesztése, a visszavert ellenség üldözése egy magasabb kötelék részeként;
- harcászati manőverek tűzzel, mozgással, a kettő kombinációjával;
- objektumok, terepszakaszok elfoglalása, biztosítása, megtartása és visszaszerzése;
- az ellenséges erők megsemmisítése, semlegesítése, lefogása, zavarása, térnyerésének megakadályozása, kedvező irányba terelése;
- az ellenség által telepített és tűz alatt tartott akadályok leküzdése;
- színlelés, az ellenség megtévesztése;

[68] Szerző: Tóth András fhdgy. (MA, PhD-hallgató).

[69] Command and Control – vezetés és irányítás

[70] Civil-Military Co-operation – civil-katonai együttműködés

[71] Psychological Operations – lélektani műveletek

[72] Human Intelligence - az emberi kapcsolatok felhasználásával folytatott titkos információszerzés

- az ellenség vagy a terep felderítése, megkerülése, megtisztítása (szabaddá tétele), elszigetelése;
- együttműködés könnyű, nehéz, szövetségi vagy speciális erőkkel;
- műveletek folytatása valamennyi éghajlati, időjárási és terepviszonyok között nappal és éjszaka;
- vízi akadályok leküzdése menetből, illetve rövid előkészítést követően (kétéltű műveletek);
- légi kiszállítással végrehajtott műveletek;
- támogató és stabilitást elősegítő műveletek;
- 72 órás, folyamatos műveletek folytatása saját készletekkel.

Technikai követelmények

A rendszer céljából, rendeltetéséből adódóan a követelményekben fontos meghatározni a civil (polgári) rendszerekkel való kompatibilitás követelményét egyaránt73. A polgári szabványok, illetve eszközök alkalmazásának lehetősége a költséghatékonyság elérése miatt, kiemelt fontosságú. Fontos, hogy minden műveleti alkalmazás esetén a moduláris rendszer könnyű átjárhatóságot tudjon létesíteni a polgári szabványú eszközök között, ellenőrzött környezetben. Ebből eredeztethető az a nagyon fontos követelmény, miszerint a rendszernek biztosítania kell a folyamatos rendelkezésre állási képességet. Jelenleg ez csak polgári eszközökkel valósítható meg, amelyek a tábori körülményeknek nem felelnek meg, ezért azokat „katonásítani" kellene (porálló, vízálló, ütésálló).

Az információ szükséges védelmének biztosítása és az átjárhatóság nyílt és minősített rendszerek között szintén egy kiemelten fontos követelmény a rendszer kiépítésének tervezésénél. Azonban ennek kialakításánál figyelembe kell venni, hogy jelenleg nyílt rendszeren minősített adat nem továbbítható. Így a kommunikáció csak egy irányú lehet és az adathalász tevékenységet igen nehéz lesz megakadályozni. A szoftverek moduláris felépítése a legalkalmasabb egy rugalmas rendszer kialakításához. Fontos az azonos és más típusú modulokkal való kiegészíthetőség is. A meglévő fejlesztési koncepcióban szereplő tábori rendszer elemek rendkívül sok, különböző felépítésű komplexumot tartalmaznak. Közel azonos funkció, de különböző kialakítások találhatók meg jelenleg a híradó rendszerben.74

Fontos, hogy a beszerzésre kerülő rendszer szoftver alkalmazható legyen, minden fegyvernem, szakág és technikai eszköz tekintetében. Ehhez nem csak a rendszerszoftver moduláris kialakítása, hanem az eszközpark, technikai eszközök tipizált, moduláris kialakítása is alapvető. Előnye, hogy nem igényel plusz szakfelkészítéseket. Akit kiképzünk, az bármely azonos funkciójú típust tudja magabiztosan, magasabb szinten kezelni. Könnyebbé válik a rendszer kiegészítése. A moduláris felépítés mellett nagy hangsúlyt kell fektetni a rendszer kiesése elleni védelemre, illetve a gyors áttérés lehetőségére a helyettesítő rendszerre.

73 pl.: katasztrófavédelmi feladatok

74 pl.: HK-1/G, HK-1-CS/G, HK-1-K/G, HK-2/G, RR-RFP/G, HIK/G; PK-1 pc, PK-2 pc, PK-3 pc; PK-1 /G, PK-2 /G, PK-3 /G, PK-4 /G, ERIP, illetve különböző fegyvernemi, szakági platformok

Alapvető fontosságú, hogy a rendszer kiesése esetén a műveletek végrehajtása önállóan is megvalósuljon. Ebből azonban ered az a probléma, hogy minden autonóm felhasználó, rendelkezni fog a műveletekre vonatkozó adatokkal, adatbázisokkal, amelyek illetéktelen kezekbe kerülésével igen sebezhetővé teszik, vagy kudarchoz vezethetik a műveletet, és rengeteg áldozatot okozhatnak, ezért alapvető a korszerű hálózatfelügyelet és menedzsment megvalósítása.

Fontos a rendszer elemek illetéktelen hozzáférésének biztosítása, adatkinyerés elleni védelme. Ennek megvalósítására egy manuálisan és távfelügyeleti rendben működő beépített adattörlési funkció javasolt. Egyéb biztonsági funkciók kialakítása során egy szigorúan szabályozott hierarchikus konfigurációs kontroll alkalmazása szükséges. Ez alapvető feltétele a hírrendszer nehéz sebezhetőségének. Fontos, hogy a rendszerhez való illetéktelen hozzáférés nagy bonyolultságú és azonnal kiszűrhető, elhárítható legyen.

Kiemelkedő jelentőségű kérdés a különböző eszközökben és vezetési pontokon alkalmazott informatikai eszközök és berendezések adathalász elleni védelme, amit véleményem szerint szoftveresen és hardveresen is meg kell oldani. A problémakörrel kapcsolatosan az alábbi kérdések merülhetnek fel:

- Amennyiben adatokat tartalmaz, az információk illetéktelen kezekbe jutását hogyan lehet megakadályozni? Azonnal megsemmisíthető biztonságosan az információ?
- Ha a katonát támadás éri, akkor az egyén az életét, vagy az adatokat fogja menteni?

A rendszer felügyelete, karbantartása és üzemeltetése szempontjából fontos, hogy minden hálózati elem táv-menedzselhető legyen ez alapvető feltétele a távoli karbantartásnak, crypto kulcselosztásnak és számos szolgáltatás kialakításának. Ezzel megoldható a szoftver verziók frissítése, a rendszer kiegészítése eddig még meg nem fogalmazott igények kielégítéséhez. Nem elhanyagolható egy megbízható kommunikációs protokoll alkalmazása a hálózati elemek között kiegészítve a megfelelő sávszélességgel. Ezek mellett alapvetően szükséges a jelentések, információk normalizálása, szabványosítása. Létfontosságúvá válhat egy Tábori Hálózat-felügyeleti és Menedzsment Központ kialakítása a szoftver/rendszer karbantartása, menedzselése érdekében. Azonban ennek kialakítása béketámogató, békefenntartó, nemzetközi környezetben nehézkes.

Hagyományos hadviselés során elsődleges prioritás kell, hogy legyen a kifogástalanul, minden körülmények között működő, titkosítható rádióösszeköttetés megléte a századparancsnoktól az alárendelt szakaszok, illetve rajok felé. A korszerű vezetés érdekében meg kell oldani minden egyes harc- és gépjármű GPS adóval való ellátását és ennek összekapcsolását a rádióval, amely így valós idejű helymeghatározást biztosítana a parancsnok számára. A rádióhálón keresztül történő kommunikáció biztosítja az alegység, illetve különböző fegyvernemi, szakági platformok megfelelő vezetettségét és irányítottságát a harcérintkezés közben. A kommunikáció ilyen esetekben nem haladja meg a jelentések és utasítások rendjét, amelyeknek alapvetően rövidnek, tömörnek és lényegre törőnek kell lennie. Az információ jellemzője raj, illetve szakasz szinten audio, gyakorisága parancs szerint, terjedelme ne haladja meg az értelmezhetőség határát.

Századparancsnoki szinten szükséges az infrastruktúra bevezetésén gondolkodni. A zászlóaljparancsnok elhatározása, parancsa, a törzs részlegeinek bedolgozásai valós idejű megjelenése a századparancsnok monitorán meggyorsítja a feladatvétel, illetve tisztázás folyamatát, segít felkészülni a parancsnoknak saját alárendeltjei eligazításában. Azonban a tisztázatlan intézkedések, parancsok tervezetei gyakran zavaróak lehetnek a végrehajtásra való felkészülésben, mert sok redundáns és pontatlan információt tartalmaznak. A rendszer természetesen visszafelé is működik, a beérkező jelentések összegzése és rendezése, valamint továbbküldése felgyorsul. A századparancsnok integrálása a felderítő rendszerbe biztosítja számára a szükséges felderítési információkat, segíti a feladat tervezésében, valamint a kétirányúságból fakadóan biztosítja az elöljáró valósidejű információkkal való ellátását.

Missziós feladat ellátása közben megnő a raj és a szakasz, mint szervezeti elem jelentősége. A Magyar Honvédség legnagyobb létszámú alegysége, amely ilyen feladatban részt vett zászlóalj volt, de legkisebb eleme a raj, amely önállóan hajtott végre feladatot több esetben. Eltérően a harcfeladat végrehajtásától, amikor a századparancsnok közvetlenül vezeti szakaszait, rosszabb esetben rajait is, szükséges a rajparancsnok ellátása mobil vezetési rendszer elemeivel. Több olyan missziós feladat van,[75] amikor szükséges lehet az állandó összeköttetés fenntartása számítógépes rendszeren keresztül. Ebben az esetben a számítógépes rendszer – amely fejlett térképészeti programmal rendelkezik – GPS-el való összekapcsolása biztosítja a kiküldő parancsnok valós idejű információval való ellátását. Ilyen esetekben a rajparancsnoknál lévő mobil vezetési rendszer elemének rendelkeznie kell mindazokkal a modulokkal, mint amivel rendelkezik a századparancsnok a hagyományos hadviselés során.

Fontos a kommunikációs modul, amely a rendszerelemek közötti kommunikációt biztosítja. Adatbázisos formátumban, amely térképi megjelenítéssel is képes működni, szükséges a saját és felderítési modul, amely biztosítja a saját, illetve az ellenséges erők helyzetét és az ehhez kapcsolódó információt. A rendszernek képesnek kell lennie térképész üzemmódban a NATO szabványnak megfelelő szimbólumok megjelenítésére, azok mozgatására.

A döntések meghozatala és azok végrehajtásának figyelemmel kísérése a parancsnok és a törzs feladata marad. Nekik kell felmérniük a harchelyzetben beállt változásokat és kiválasztani a legjobb tevékenységi változatot. A helyzet pontos ismerete világosabb képet biztosít a döntések meghozatalához. Ehhez biztosítani kell, hogy a rendszerben lévő bármilyen szintű parancsnok képes legyen figyelemmel követni a szomszédos erők tevékenységét, és ezzel biztosítani, ha ott negatív irányban következik be elmozdulás, időben reagálni tudjon rá. A rendszernek biztosítania kell hadijátékok, begyakorlások lejátszását, képesnek kell lennie grafikusan megjeleníteni a saját és ellenséges erőket, valamint a magasabb felderítő forrásokhoz való kapcsolódást, a beérkező adatok automatikus vételét, a régiek automatikus archiválását, illetve a logisztikai pontosítások automatikus végrehajtását. Missziós tevékenységek során a zászlóalj szintű harcvezetési rendszernek biztosítania kell az elöljáró rendszerébe és a békefenntartó/missziós feladatokat végrehajtó nemzetközi környezetbe való integrálódást.

75 pl. járőrözés, konvojkísérés

Rádió híradás és digitális adatátvitel

Alkalmazás, harc megvívása esetén a vezetés-irányítási rendszerben a jelenleg megszervezett lépcsőzetes rádióforgalmi rendszerek (zpk-i, szdpk-i, szpk-i, stb.) jól alkalmazhatók, a digitális adatátvitel ráépíthető az alábbi feltételek figyelembe vételével:

- minden harc- és gépjármű, a mobil elemek, együttműködők, megerősítők rendelkeznek a megfelelő mennyiségű számítástechnikai, digitális híradótechnikai eszközökkel,
- az „orosz" típusú rádiórelé állomás kiváltásra került digitális rádiórelé állomással, RR/G rendszer gépkocsi,
- a K-1 –es távbeszélőközpont és az informatikai központ gépkocsi (GAZ-66 gépjárművön, semmilyen informatikai eszközzel nem rendelkezik) kiváltásra került híradó és informatikai központ (HIK) konténerrel, vagy HK1/G állomással,
- az R-142 rádióállomás kiváltása PK1/G és RFP/G állomásokkal,
- beszerzésre kerültek a C2 szoftverek, valamint a digitális rádiókészülékeken továbbítandó információkhoz egy olyan célszoftverek, amelyek szakaszparancsnoki szintig a rádiókhoz kapcsolódó informatikai eszközre telepítve képesek rádióhálóban egyszerre, egy időben (a rádióhálóba késve történő belépés esetén utólagos adatküldéssel) több tagállomás részére digitális adatokat továbbítani oly módon, hogy a rádiócsatornán átmenő beszédátvitel nem szakad meg, továbbra is megbízható marad.

A rendszerrel kapcsolatos követelmények

Az alegységek esetében a híradó és informatikai központ alkalmazása kulcsfontosságúvá válik, mivel ez kezeli le és koncentrálja az elöljáró (kontingens parancsnokság) és az alárendeltek közötti információ cserét. Biztosítja nem honi területen való alkalmazás esetén a nagytávolságú híradó összeköttetéseket (műholdas kapcsolat, rövidhullámú rádióösszeköttetés).

Digitális információ áramlás során az informatikai hálózatnak, a C2 rendszernek és az egyéb szoftvereknek biztosítania kell:

- a megfelelő informatikai, információs és kommunikációs támogatással, a harc sikeres megvívását, a kapott feladatok, célok teljesítését, illetve a napi tevékenységek elvégzését;
- az ellenség csapatairól, eszközeiről, települési helyeiről, harcrendi elemeiről, azok pillanatnyi állapotairól kapott felderítési adatok gyűjtését, fogadását, real-time76 feldolgozását, tárolását, megjelenítését;
- a saját csapatokról, eszközeikről, települési helyeikről, harcrendi elemeikről, azok pillanatnyi állapotairól kapott adatok fogadását, real-time feldolgozását, tárolását, megjelenítését;
- adatbázis információk digitális térképeken történő megjelenítését;

[76] valós idejű

- digitális térképi adatbázis felhasználásával metszetek, útvonalak, egyedi igények szerinti megjelenítések és azokkal kapcsolatos értékelések előállítását;
- a meglévő adatbázis adatok alapján tervek, számvetések elkészítését;
- a saját csapatok tekintetében, a beérkezett információk alapján nyilvántartások kezelését;
- felderítési, különféle nyilvántartási, vezetési információk kétirányú kapcsolatát a rendszerelemek között;
- különféle digitális, formalizált nyomtatványok kezelését;
- szöveges üzenetek fogadását, továbbítását;
- archiválást;
- riasztási funkciók ellátását;
- az alárendelt–elöljáró közti kommunikációs kapcsolat kezelését, annak menedzselését.

Véleményezés

A meglévő fejlesztési koncepcióban szereplő tábori rendszer elemek rendkívül sok, különböző felépítésű komplexumot tartalmaznak. Közel azonos funkció, de különböző kialakítások találhatók meg jelenleg a híradó rendszerben. Fontos, hogy a beszerzésre kerülő rendszer szoftver alkalmazható legyen, minden fegyvernem, szakág és technikai eszköz tekintetében. Ehhez nem csak a rendszerszoftver moduláris kialakítása, hanem az eszközpark, technikai eszközök tipizált, moduláris kialakítása is alapvető. Előnye, hogy nem igényel plusz szakfelkészítéseket. Akit kiképzünk, az bármely azonos funkciójú típust tudja magabiztosan, magasabb szinten kezelni. Könnyebbé válik a rendszer kiegészítése. (Ha 100 vonalas központunk van egy modullal kiegészítve 200 vonalat tudunk üzemeltetni).

A moduláris felépítés mellet, nagy hangsúlyt kell fektetni a rendszer kiesése elleni védelemre, illetve a gyors áttérés lehetőségére a helyettesítő rendszere. Alapvető fontosságú, hogy a rendszer kiesése esetén a műveletek végrehajtása önállóan is megvalósuljon. Ebből azonban ered az a probléma, hogy minden autonóm felhasználó, rendelkezni fog a műveletekre vonatkozó adatokkal, adatbázisokkal, amelyek illetéktelen kezekbe kerülésével igen sebezhetővé teszik a műveletet vagy kudarchoz, és rengeteg áldozathoz vezet.

Figyelembe kell venni, hogy a rohamos technológiai fejlődésből adódóan az eszközök, szoftverek életciklusa átlagosan 3-5 év. Félő, hogy mire rendszeresítésre kerül egy megfelelő rendszerszoftver, az elavulttá válik. Ezért elengedhetetlen a rendszerbeállítás idejének rövidítése.

Az adott vezetési pont információcserére vonatkozó követelmények felülvizsgálata a rendszer/szoftver követelmények meghatározása alapvetően fontos. Amennyiben az információ szükséglet szükséges és elégséges követelménye nem kerül meghatározásra abban az esetben a rendszer/szoftver által alkalmazott információ szabványt tág paraméterekkel kell kialakítani, amely az információáramlási sebesség csökkenéséhez vezet.

A vezetési rendszeren belül működő funkcionális területek (irányok) jól lefedik a feladatokat, és kellő számban átfedik egymást. Az alrendszerek működtetésének egységes követelményei is jól megfogalmazásra kerültek.

Fontos követelménynek tartom a rendszer testre szabási jogának kérdését. Célszerű lenne, hogy átadásra kerüljön a Magyar Honvédségnek, bár ezzel szükségessé válik további jól képzett munkaerő alkalmazása. Megvizsgálandó, hogy ha külső cég végzi, mennyire költséghatékony a rendelkezésre állásuk. Tehát melyik megoldás olcsóbb. Valószínű, hogy a döntés harmadik tényezője lesz az, hogy nem tudunk jól felkészült, elkötelezett szakembereknek versenyképes bérezést adni.

A rendszer kommunikációs funkcióinak valóban fel kell készülnie a rádiókon keresztüli szélessávú összeköttetések megfelelően nagy adatátviteli kapacitásának biztosítására, azonban ezt célszerű kiegészíteni, hogy alkalmas legyen a rendszer a jelenleg egyre nagyobb területen elterjedő IP alapú eszközök, IP architektúrájú rendszerek kezelésére.

Az adott alegységre nézve, az alárendelt-előjáró szintek között történő kommunikációra két független irányt kell megvalósítani. Az első feladata, a szinteknek megfelelő szerverek között az adatbázisokkal kapcsolatos adattartalom szinkronizáció biztosítása, mellyel a sajátcsapatokra, illetve az ellenségre vonatkozó, felderítési és állapot információk aktualizálása biztosítható.

A másik vonal, az alárendelt-előjáró közötti, közvetlen utasítási /jelentési/ riasztási csatorna. Ezen közvetlen kapcsolat a rendszer formalizált üzenettípusaival biztosítható, melynél a kommunikációs modul szolgáltatta címjegyzék alapján nyílik lehetőség, gép-gép közötti kapcsolatot létesíteni. A feladat során azonban, kezelni kell azt a problémát, ami abból adódhat, hogy transzparens módú rádiós adatátvitelnél, az MRR rádió berendezések alkotta kommunikációs hálóban, adott parancsüzenet, a rádióháló „üzenetszórásos" működésének következtében, a háló minden tagjához – az azt lehallgatóhoz is – eljut, így terítésre kerül a csak adott szintnek szóló, esetleg bizalmas információ.

A rendszerszoftver, a működési profilnak megfelelő szoftvermodulok, illetve az ezekhez konkrétan szükséges részadatbázis tartalom minden számítógépen telepített kell, hogy legyen (a rendszerszoftver és az azt kiegészítő szoftvermodulok alaphelyzetben telepített, a szükséges részadatbázis tartalom, és a digitális térképi adatbázis állomány cserélhetően rátölthető legyen). Ezzel biztosítható, hogy új feladatelrendelés esetén egy számítógép adminisztrátori beavatkozással bármikor átállítható a feladat végrehajtáshoz szükséges új profilra, és a felhasználáshoz csak a még esetlegesen hiányzó adatállomány átvitelére van szükség. Az adott helyzetben az alkalmazáshoz nem szükséges információk – adatbázisba foglalva minden a saját csapatokra, az ellenségre vonatkozólag elérhető információk, valamint a különböző felbontású térképi adatbázisok adatállománya – az adott alkalmazási szinteknek megfelelő adatbázis szerveren kerül tárolásra. Újabb feladat esetén, a feladatnak megfelelő szűréssel, az alkalmazási szint adminisztrátora tölti le – cseréli – az újonnan szükségeltetett adatbázis tartalmat az egyes terminálokra.

Az általános rendszerkövetelmények esetében véleményem szerint fontos, hogy a rendszer platform független legyen. Nem kizárható, hogy a jövőben a drága MS operációsrendszerekről a sokkal költséghatékonyabb (ingyenes), azonos szolgáltatásokat és grafikus felületet nyújtó operációs és irodai rendszerekre térünk át. A kialakítandó rendszer szoftvernek olyannak kell lennie, mely lehetőséget biztosít mind a PC-s, mind PDA-s alkalmazásra. Ha ez egy szoftverrel nem biztosítható, a PDA-s alkalmazáshoz szükséges változatát külön el kell készíteni.

A rendszerkövetelményekben megfogalmazott telepíthetőségi kritériumok mellett javaslom megvizsgálni a távfelügyeleti telepíthetőség és szoftverfrissítési lehetőséget.

Felhasznált irodalom

[1] Pándi Balázs – Pándi Erik: A jövő várható háborúinak és katonai konfliktusainak hatása a hazai tábori kommunikációs rendszer megújításának folyamatára, „Kommunikáció 2008." Nemzetközi szakmai-tudományos konferencia kiadványa, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2008.

[2] Farkas Tibor: A honvédség tervezett kommunikációs hálózata, Kard és Toll, Honvédelmi Minisztérium, Budapest, 2006.

[3] Kerti András: A polgári élet és a katonai információbiztonság viszonya, „Kommunikáció 2008." Nemzetközi szakmai-tudományos konferencia kiadványa, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2008.

[4] Kozák Miklós: A katonai kommunikációs rendszerek tervezésének és szervezésének alapkérdései (Új Honvédségi Szemle 1997/8. szám)

[5] Hamar Sándor: A katonai hírközlés fejlődésének útjai (Új Honvédségi Szemle 2002/12.)

FLEINER Rita[77]

ADATBÁZIS-KEZELŐ RENDSZEREK KOMMUNIKÁCIÓS PROTOKOLLJAI ÉS SÉRÜLÉKENYSÉGEI

Absztrakt: *A publikáció az adatbázisok kommunikációs protokolljában rejlő sebezhetőségeket mutatja be. Az adatbázisok kommunikációs protokollja az .SQL szabványban nem definiált, de a kliens-szerver kommunikációhoz szükséges folyamatokat (például felhasználói hitelesítés, kapcsolat felépítés, kapcsolat bontás, utasítások és válaszok eljuttatása) valósítja meg.*

Kulcsszavak: adatbázis-kezelő rendszer, adatbázis támadás, adatbázis kommunikációs protokoll

Bevezetés

Napjainkban az informatikai rendszerek jelentős részének működésében lényeges szerepet játszanak különböző adatbázisok. Az adatbázis adatoknak számítógépekben tárolt, valamely adatmodell szerint strukturált gyűjteménye. Az adatbázisokban tárolt adatok kezelését speciális alkalmazások, az úgynevezett adatbázis-kezelő rendszerek biztosítják, melyek több felhasználós, hálózatos környezetben működnek. Adatbázis szervernek nevezzük az egy vagy több adatbázis-kezelő rendszert futtató számítógépet.

Az adatbázisok biztonságának megsértése (működésképtelenné tétele, meghamisítása, a tárolt adatok jogtalan megismerése) az adott informatikai rendszer és az általa nyújtott szolgáltatás biztonságát fenyegeti. Ebből következően lényeges kérdés az adatbázisok megfelelő védelme, melyhez ismernünk kell az adatbázisok biztonságát veszélyeztető fenyegetések különböző formáit.

Jelen publikáció röviden bemutatja az adatbázisok elleni, különböző támadási formákat, majd részletesen elemez egy kevésbé ismert fenyegetettséget, mely az adatbázisok kommunikációs protokolljainak sebezhetőségére épül. A megértés érdekében ismertetjük az adatbázisok kommunikációs protokolljait is.

Adatbázisok fenyegetettségei

Hálózati infrastruktúra sebezhetőségei

Ebbe a kategóriába azok a hálózati támadások tartoznak, melyek az adatbázis szerverek, illetve adatbázis állományokat tartalmazó háttértárak közötti kommunikáció támadására alapulnak, vagy pedig a hálózat tetszőleges pontján lépnek fel, de az adatbázis-kezelő rendszerek szolgáltatásait zavarják meg.

A hálózati adatforgalom lehallgatásának veszélye megjelenik az adatbázisok magas rendelkezésre állásának megvalósításánál (adatbázis tükrözés, fürtözés), ahol adatbázis szerverek kapcsolódnak hálózaton keresztül. Az adatbázis szerverek közötti adatforgalom titkosítás nélkül (vagy gyenge titkosítással) áramlása esetén az adatok lehallgathatóak, ezzel pedig adatbázisok tartalma kerülhet illetéktelenül támadók birtokába.

[77]ZMNE KMDI doktorandusz hallgató, fleiner.rita@nik.bmf.hu

Hálózati szinten jelentkező támadások egyik fajtája a forráscím meghamisítása (spoofing). Ezzel a technikával beékelődéses támadást (man in the middle) lehet kiváltani, ami az adatbázis rétegen belül két, egymással kommunikáló adatbázis szerver esetén használható. A támadás következménye lehet az adatbázis tartalmának a megsértése, vagy az adatbázis szerverek szolgáltatásaiban való károkozás.

Hálózaton keresztül szolgáltatás megtagadása (DoS) típusú támadást lehet az adatbázis szerver ellen indítani, amivel a megtámadott szerver elérhetetlenné tehető.

Hosztok sebezhetőségei

A hosztok (a hálózatba kötött szerver és felhasználói számítógépek) sebezhetőségei alatt a rajtuk futó operációs rendszer és egyéb rendszerprogramok (például adatbázis-kezelő rendszer programja) sebezhetőségét értjük. Adatbázisok biztonságát vizsgálva feladatunk az adatbázis szervereket futtató platformok sebezhetőségeinek feltárása, a rajtuk lévő operációs rendszer és adatbázis szerver rendszerprogramok biztonságát vizsgálva.

Az adatbázis szerverekre vagy anonim kapcsolattal vagy autentikáció után lehet kapcsolódni. A támadó a hitelesítési mechanizmus és információk lehallgatásával, megszerzésével illetéktelenül tud az adatbázis szerverre bejutni. Rendszer szoftverek telepítésekor gyakran, automatikus módon, ismert nevű felhasználók jönnek létre, mely a támadás számára egy jó kiindulási pont. Ugyanis a felhasználónév birtokában a támadónak „csak" a jelszót kell kitalálnia (ami gyakorta nem erős, azaz könnyen megfejthető).

Gyenge konfigurációs paraméterek használata, szoftver hibák (például puffer túlcsordulás, SQL injekció), felhasználói hibák, elavult verziójú programok használata és biztonsági frissítések feltöltésének hiánya kártékony kód lefuttatását, vírusok, trójaiak és férgek rendszerbe való bejutását eredményezheti, illetve szolgáltatás megtagadása típusú támadásra ad lehetőséget. Adatbázis kezelő rendszerek esetén a telepítéskor automatikusan létrejövő táblák, tárolt eljárások, alapértelmezett felhasználónevek és jelszavak sérülékenységi pontot jelentenek. (Célszerű ezeket törölni, és szükség esetén más névvel magunknak létrehozni.)

Rendszerszintű információk (például felhasználói adatok, operációs rendszer és adatbázis szerverprogram típusok és verziók, adatbázis szerver nevek, adatbázis séma részletei) felderítésével jelentős támadások készíthetők elő. Jogosultságok helytelen beállításával, audit és mentési adatok nem megfelelően védett tárolásával, érzékeny (minősített vagy személyes) adatok titkosítás nélküli tárolásával bizalmas információk kerülhetnek illetéktelen kezekbe, ami szintén sérülékenységi pont a rendszerben.

Az adatbázisok kommunikációs protokolljában rejlő sebezhetőségekre épített támadást is ebbe a kategóriába soroljuk és a későbbiekben részletesen bemutatjuk.

Alkalmazások sebezhetőségei

Az alkalmazásokban rejlő sebezhetőségek, programozási hiányosságok az adatbázis támadások egy fontos csoportját jelentik. A következő sérülékenységi kategóriákat különböztetjük meg.

A felhasználói inputok ellenőrzésének hiánya puffer túlcsordulásos, SQL injekciós, illetve XSS (cross-site scripting) támadásra adhat lehetőséget.

Alkalmazások a felhasználók számára megjelenített hibaüzeneteikben adatbázisra, illetve az adatbázis szerverre jellemző információkat fedhetnek fel, ami támadások felépítéséhez ad segítséget, ezáltal sérülékenységi pontot jelent.

Egy adott alkalmazás az adatbázis szervert egyetlen adatbázis felhasználó nevében éri el. Ha az alkalmazás tulajdonosként vagy superuserként csatlakozik az adatbázishoz, sérülékenységet jelent, mivel bármilyen utasítást és lekérdezést lefuttathat, pl. a szerkezeti módosítást (táblák megszüntetése) vagy táblák komplett törlése. Mindig a lehető legkevesebb jogosultsággal rendelkező, az alkalmazás számára önálló és testreszabott felhasználókat kell használni. Ekkor, ha a behatoló meg is szerez valamilyen jogosultságot (hitelesítési információt), akkor is csak akkora változást tud okozni, mint az alkalmazás maga.

Az alkalmazás szintjén az adatbázis lekérdezések, hozzáférések naplózásának hiánya szintén sérülékeny pont lehet a rendszerben, hisz az adatbázis szerver naplóiban egyetlen, az alkalmazáshoz kötött felhasználó jelenik csak meg. Nyilvánvalóan a naplózás nem tud megakadályozni egyetlen ártalmas próbálkozást sem, de segítséget nyújthat annak felderítésében, hogy melyik alkalmazás és ki által lett kijátszva.

Adatbázisok kommunikációs protokolljai

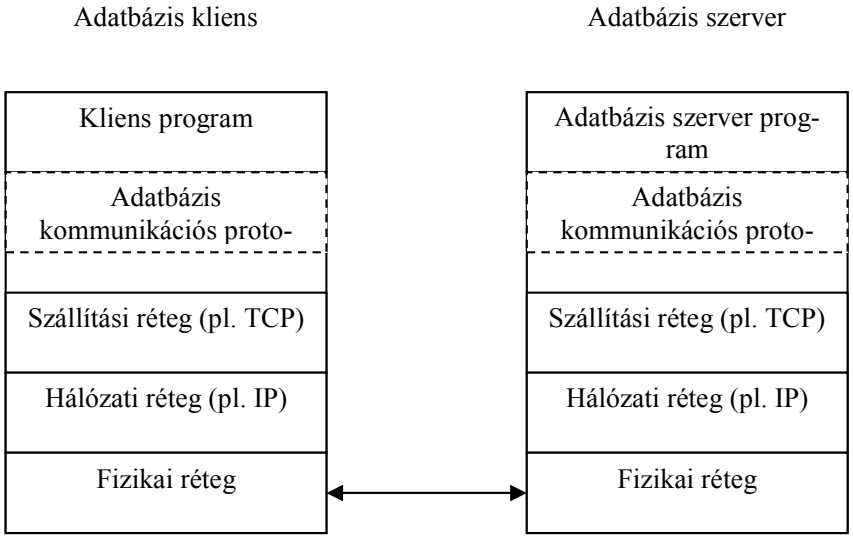
Pár évvel ezelőtt az adatbázis szerverek ellen új támadási forma jelent meg, mely az adatbázisok kommunikációs protokolljában rejlő sebezhetőségekre épít [1]. Az SQL adatbázis lekérdező nyelv bizonyos kliens-szerver kommunikációhoz szükséges folyamatot egyáltalán nem definiál, például létfontosságú, de nem szabványosított a kliens kapcsolat (client session) létrehozása, a kliens-szerver autentikáció folyamata, a parancsok klienstől szerverhez való átadása, az adatok és a lekérdezés státuszának klienshez való eljuttatása, a tranzakciók mechanizmusának megvalósítása. Ezeket a feladatokat a gyártók által kifejlesztett, adatbázis-kezelő rendszer hálózati kommunikációs szoftverei valósítják meg, például Oracle esetében az Oracle Net a TNS (Transparent Network Substrate) protokollal, Miscrosoft esetében a TDS (Tabular Data Stream), IBM esetében pedig a DRDA (Distributed Relational Database Architecture).

Az adatbázisok kommunikációs protokolljai szoftvergyártó függőek, nem szabványosítottak, kódjaik általában nem nyilvánosak. Az OSI modellben a hálózati-szállítási réteg és az alkalmazás réteg között helyezkednek el. Az adatbázis kliens-szerver kommunikációja független a hálózati rétegben használt megvalósítástól, ami lehet például TCP/IP, Named Pipes vagy SDP (Sockets Direct Protocol). Az adatbázis kommunikációs protokolljának helyét szemlélteti az 1. ábra.

A kliens programnak ismernie kell az adott adatbázis-kezelő kommunikációs protokolljának interfészét, ami nem szabványos, így ha megváltozik az adatbázis-kezelő típusa, a kliens programot is módosítani kell. (Ezt a problémát szabványosít interfészek, például ODBC használatával oldják meg, melyek többfajta adatbázis kommunikációs protokollal tudnak kapcsolatot létesíteni, így elfedik a felhasználói program elől, hogy valójában milyen adatbázis-kezelő van használatban.)

Mivel az adatbázisok kommunikációs protokolljai leggyakrabban nem nyílt forráskódúak, független informatika biztonsági szakemberek a tesztelésüket nem (vagy csak nagyon körülményesen) tudják elvégezni, ugyanakkor számos sebezhe-

tőség kerül velük kapcsolatban napvilágra, melyre az adatbázis szoftvergyártók új frissítések kiadásával válaszolnak és próbálják a hibát javítani. A protokollok valószínűleg nem túl modernek, mivel a régi adatbázis szoftverekkel kompatibilisnek kell lenniük. Ugyanis például egy Oracle 8 kliens kapcsolatot tud létesíteni Oracle 10g R2 adatbázis szerverrel és egy Oracle 10g kliens pedig egy Oracle 8 szerverrel. (Ebből következik, hogy a protokollok, több mint 10 évesek.)



1. ábra: Adatbázis kommunikációs protokolljának helye

Adatbázisok kommunikációs protokolljainak sebezhetősége

A kommunikációs protokollok hibáit kihasználó támadások különböző technikákon alapulnak, például a hálózat lehallgatásával az üzenet sorozat kifigyelésén, az üzenet struktúrájának elrontásán, az üzenet mező méretének megváltoztatásán, az üzenet mező tartalmának megváltoztatásán vagy az üzenet sorszámának meghamisításán [1]. A következőkben bejelentett (és már javított) sérülékenységek mögött húzódó okokat mutatunk be.

A hálózat lehallgatása

A felhasználónév/jelszó alapú hitelesítés erőssége érdekében a hibás adatok miatti visszautasítás üzenete nem fedheti fel, hogy rossz felhasználónév vagy pedig rossz jelszó miatt történt az elutasítás. Nem elég azonban arra ügyelni, hogy a hibaüzenet megegyezzen mindkét esetben, hanem a hitelesítési folyamat üzenet struktúrájának is egyeznie kell. Ha a rossz jelszó esetén csak egyszer, rossz felhasználónév esetén pedig kétszer történik üzenetcsere a kliens és a szerver között, akkor az üzenetek lehallgatásával következtetni lehet a hiba okára, ez pedig ellentmond az elvárt tulajdonságnak [1].

Üzenet struktúrájának elrontása

Az adatbázis kommunikációs protokolljának üzenetei meghatározott struktúra szerint épülnek fel. Egy üzenet speciális formájú és szereppel bíró mezőkből épül fel. Az is előfordul, hogy bizonyos üzenet többféle struktúra szerint épülhet fel. A támadás épülhet mezők eltörlésére, mezők megduplázására, hozzáfűzésére, helytelen kombinálására. A támadás következménye lehet például az adatbázis-kezelő rendszer elérhetetlenné tétele, vagy jogosulatlan szerver hozzáférés [1]. Erre a típusra példa az IBM DB2 adatbázis szerverre bejelentett sérülékenység [2], ahol egy eredetileg opcionális mező (ami az adatbázis nevét tartalmazza) hiánya váltott ki nemkívánatos szerver viselkedést.

A támadás kivitelezéséhez a támadónak vagy egy saját programot kell írnia, amivel a manipulált üzeneteit elküldi a szervernek és feldolgozza a kapott választ addig a pontig, amíg a káros hatás bekövetkezik vagy pedig egy TCP proxy segítségével be kell ékelődnie a kliens és a szerver közé, és ebben a pozícióban az elkapott üzeneteket megfelelően módosítva kell továbbítania.

Üzenet-mező méretének megváltoztatása

Egy üzenet-mező lehet fix vagy változó méretű. Változó méret esetén az aktuális méretet egy megelőző mező tartalmazza. Előfordul, hogy az aktuális méretet tartalmazó mező felvehet olyan nagy értéket, aminek megfelelő méretű mező tartalmat a szerver nem képes helyesen feldolgozni és puffer túlcsordulás állapot következik be. A támadás következménye lehet az adatbázis szerver elérhetetlenné tétele vagy tetszőleges kód szerveren való lefuttatása. Bejelentett sérülékenységek [3, 4, 5] alapultak kliens autentikáció előtti rosszul formázott login kérésre, ahol a támadónak egyáltalán nem kellett rendelkeznie hitelesítési információval.

Egy másik típusú támadás mögött az áll, hogy az üzenet több mezője is tartalmazhat méret információt, méghozzá redundáns módon. Ha a méreteket egymással inkonzisztensen adjuk meg, akkor sérülékenységet tudunk kiváltani. Például, ha az üzenet tartalmazza a teljes méretet és minden mező méretét külön-külön is, akkor inkonzisztens állapotot érhetünk el azzal, ha egy mező méretét beállítjuk nagyobbnak, mint a teljes üzenet mérete. Ezzel a szerveren nem várt működést lehet előidézni.

Üzenet-mező tartalmának megváltoztatása

Ezen az elven felépülő támadások viszonylag könnyen kivitelezhetők és nagyon súlyos károkat okozhatnak. A támadó az üzenet mezőjének tartalmát megváltoztatva elérheti azt, hogy sikeres bejelentkezés mellett az ő jogosultságainál többet igénylő SQL utasítást (például adminisztrátori jogkör beállítását) adjon ki, melyet naplózás nélkül végrehajt az adatbázis szerver. Az Oracle szerverek bejelentett sérülékenysége [6] az autentikációs folyamat egyik üzenet mezőjének tetszőleges SQL utasítással való felülírásán alapult, a sikeres bejelentkezés után a manipulált SQL utasítás az autentikációs folyamat jogosultságának (teljes jogkör) figyelembe vételével futott le, nem pedig a bejelentkezett felhasználó jogkörével.

Az ismertetett támadásokból látszik, hogy mind erősen függ az alkalmazott adatbázis-kezelő rendszer által használt kommunikációs protokolltól és ezek hibáit kihasználva tud felépülni.

Összefoglalás

A publikációban az adatbázisok kommunikációs protokolljában rejlő sebezhetőségeket mutattuk be. Az adatbázis szerverek elleni, viszonylag új és kevésbé ismert támadási forma az adatbázisok kommunikációs protokolljaiban rejlő sebezhetőségekre épít Az adatbázisok kommunikációs protokolljai az .SQL szabványban nem definiált, de a kliens-szerver kommunikációhoz szükséges folyamatokat (például felhasználói hitelesítés, kapcsolat felépítés, kapcsolat bontás, utasítások és válaszok eljuttatása) valósítják meg. Az adatbázisok kommunikációs protokolljai nem szabványosítottak, szoftvergyártó függőek, általában nem nyílt forráskóddal rendelkeznek. A támadások különböző technikákon alapulnak, például a hálózat lehallgatásával az üzenet sorozat kifigyelésén, az üzenet struktúrájának elrontásán, az üzenet mező méretének vagy tartalmának megváltoztatásán vagy az üzenet sorszámának meghamisításán.

Felhasznált irodalom

[1] Amichai Shulman: Danger From Below: The Untold Tale of Database Communication Protocol Vulnerabilities http://www.imperva.com/resources/adc/db_comm_protocol.html (2009. 09. 01.)

[2] http://www.securityfocus.com/archive/1/445298 (2009. 09. 01.)

[3] http://www.securityfocus.com/bid/5411 (2009. 09. 01.)

[4] http://www.securityfocus.com/bid/2941 (2009. 09. 01.)

[5] http://www.securityfocus.com/archive/1/445297 (2009. 09. 01.)

[6] http://www.kb.cert.org/vuls/id/871756 (2009. 09. 01.)

TÓTH András[78]

AZ AUTOMATIZÁLT HARCVEZETÉSI ÉS INFORMÁCIÓS RENDSZER MODELL

Az Automatizált Harcvezetési és Információs Rendszer modell egy olyan többszintű rendszer, mely biztosítja a különböző szintű parancsnokok részére mind az ellenséges erők, eszközök, mind a saját csapatok, eszközök tekintetében az összegzett és elemzett információkat; a saját, illetve ellenséges erők, eszközök, harcrendi elemek különböző méretarányú, digitális térképen történő megjelenítését. Segíti a különböző szintű parancsnokok és törzsek harcelőkészítését, a lehető legoptimálisabb harc-, és tűzvezetési döntések meghozatalát; külső információs, vezetési és tűzvezető rendszerek csatolását; békefenntartó küldetések és hagyományos vezetési, harc- és tűzvezetési feladatok informatikai támogatását. Automatizáltan támogatja a felderítési és állapotadatok, parancsok, intézkedések és formalizált jelentések továbbítását, a rendszer elemeinek helyének és állapotának nyomon követését.

A rendszer biztosítja:

- a megfelelő informatikai, információs és kommunikációs támogatással, a harc sikeres megvívását, a kapott feladatok, célok teljesítését, illetve a napi tevékenységek elvégzését;
- az ellenség csapatairól, eszközeiről, települési helyeiről, harcrendi elemeiről, azok pillanatnyi állapotairól kapott felderítési adatok gyűjtését, fogadását, real-time79 feldolgozását, tárolását, megjelenítését;
- a saját csapatokról, eszközeikről, települési helyeikről, harcrendi elemeikről, azok pillanatnyi állapotairól kapott adatok fogadását, real-time feldolgozását, tárolását, megjelenítését;
- adatbázis információk digitális térképeken történő megjelenítését;
- digitális térképi adatbázis felhasználásával metszetek, útvonalak, egyedi igények szerinti megjelenítések és azokkal kapcsolatos értékelések előállítását;
- a meglévő adatbázis adatok alapján tervek, számvetések elkészítését;
- a saját csapatok tekintetében, a beérkezett információk alapján nyilvántartások kezelését;
- felderítési, különféle nyilvántartási, vezetési információk kétirányú kapcsolatát a rendszerelemek között;
- különféle digitális, formalizált nyomtatványok kezelését;
- szöveges üzenetek fogadását, továbbítását;
- archiválást;
- riasztási funkciók ellátását;
- az alárendelt–elöljáró közti kommunikációs kapcsolat kezelését, annak menedzselését.

[78] Szerző: Tóth András fhdgy. (MA, PhD-hallgató).
[79] valós idejű

Megvalósítandó kommunikációs kapcsolatok és adatcsere

A feladatok sikeres végrehajtása érdekében szükséges egy minden körülmények között biztonságosan működő kommunikációs rendszer kiépítése. A hálózatnak meg kell felelnie napjaink minden távközlési követelményének. A rendszer működése során egy időben több kommunikációs utat is meg kell valósítani:

- Szakasz, század szinten, a laptopos (normál pc-s) és PDA-s alapterminálok, a parancsnoki alapterminál és a század szintű szerver között MRR rádión alapuló (adott rádióhálón), folyamatos adatkapcsolat biztosítja az információcserét, a parancs, jelentő és riasztási üzenetcserét.
- A parancsnoki alapterminál MRR80 rádión keresztül (adott rádióhálón) folyamatos adatkapcsolattal részét képezi az elöljáró felé irányuló parancs/jelentő csatornának.
- A szerverek közötti adatbázis tartalmak szinkronizációjára, és az előjárótól az alárendeltekhez továbbítandó komplex tervek, utasítások továbbítására közvetlen kommunikációs csatorna, mely lehet IP alapú LAN, WAN, ISDN csatorna vagy MRR rádióháló.
- Zászlóalj szinten alkalmazott törzsterminálok, parancsnoki funkciójú törzsterminál és a zászlóalj szerver között IP alapú LAN biztosítsa az egymásközi, illetve a szerveren keresztül a szinten kívüli kommunikációt.

A működés során a következő adatkapcsolatokat kell biztosítani:

- Század (zászlóalj) szinten, alapterminál-alapterminál kapcsolat üzenetküldésre;
- Század (zászlóalj) szinten alapterminál-parancsnoki alapterminál közötti kétirányú kapcsolat parancs/jelentő/riasztási feladatokra;
- Század (zászlóalj) szinten alapterminál-szerver kapcsolat a GPS alapú pozícióadatok, és a felderítési adatok továbbítására;
- Század (zászlóalj) szinten szerver-alapterminál kapcsolat a szerveradatbázis aktualizálási, illetve kezdeti beállításkor a részadatbázis állomány letöltése céljából;
- Század-zászlóalj szintek között (előjáró-alárendelt), parancsnoki alapterminál- parancsnoki adatterminálok (a zászlóalj szerveren keresztül) közötti parancs/jelentő/riasztási feladatokra;
- Század-zászlóalj szintek között (előjáró-alárendelt), szerver-szerver közötti adatbázis állomány szinkronizálásra, illetve az előjáró-alárendelt közötti üzenetküldésre;
- Zászlóalj szinten törzsterminál-törzsterminál kapcsolat üzenetküldésre;
- Zászlóalj szinten törzsterminál-szerver kapcsolat adatcserére.

Század szint alatt a kommunikáció lehetősége, a Magyar Honvédségnél rendszeresített Kongsberg MRR rádiókon alapul. A terminálok mellett elhelyezett 1-1 rádió berendezéssel - melyek előre meghatározott adott frekvencián közös rádióhálót alkotnak -, RS232 porton keresztül egyaránt biztosítható a terminálok közötti adat- és beszédátvitel. A jelenlegi rádiók esetén, az adatátvitel sebessége maximum 16kbps (jellemzően 2,4 – 9,6 kbps). Az információ átvitelére lehetőséget kell adjon

[80] Multi Role Radio – többfunkciós rádió

a terminálok Ethernet felülete is, de jelenlegi eszközeink ezt az átviteli utat még nem biztosítják. Ez a lehetőség csak az alkalmazást megelőző, adminisztrátori beállításoknál, és a részadatbázisok letöltésénél kerülhet kihasználásra.

A század, zászlóalj szint esetén, a kommunikációs kapcsolatokat két főbb részre kell bontanunk. Az egyik során, a szintek közötti kommunikációt kell megvalósítani. Ez a jelen rendszerelgondolás keretein belül, a csatlakozó felületek biztosítását tartalmazza, az átviteli úthoz szükséges komplex átvitel technikai rendszereszközöket nem. A másik, a szinten belüli, terminálok közötti kapcsolatot kell, hogy megvalósítsa, melyre egy LAN hálót kell biztosítani. A LAN háló kialakításához – feltételezve, hogy a terminálok száma egy adott szint alá várható - szükség van 10/100/1000 MB-os switch-re, mely lehetővé teszi a terminálok hálózatba kapcsolását, és a hálónak külső adatátviteli végberendezéshez történő csatolhatóságát is meg kell oldani a lehetséges tábori kommunikációs eszközöknek megfelelő felülettel router, gateway alkalmazásával.

A rendszer felépítése

A rendszer felépítése többszintű. A korszerű számítógép terminálokon futtatott szoftver készlet, a tervezett alkalmazási szintnek és profilnak megfelelően tartalmazza a következő főbb elemeket:

- zászlóalj törzs terminál;
- szakasz, század, zászlóalj adatbázis szerver;
- szakcsapat terminál;
- alapterminál.

Az egyes szintek hardverfelépítése hasonló – ez alól kivételt csak a szerver képez -, a főbb eltérés jellemzően a számítógép konfigurációkon futó, aktivizált szoftverekben, illetve az alapterminálóknál megjelenő PDA-s megvalósításban áll.

A megvalósítandó rendszer alapját egy komplex alapszoftvernek kell képeznie, mely egyrészt tartalmazza a vezérlő, megjelenítő, adat és digitális térképkezelő szoftveregységet, biztosítja a kommunikációs rendszer egységeinek szervízszintű alkalmazását, illetve az adminisztrátori beállításoknak megfelelően, az alkalmazási profilhoz rendelt szoftvermodulok, alkalmazások meghívását, használatát.

Az egyes terminál típusok az alábbi modulokat tartalmazzák:

Alapterminál:

- Komplex alapszoftver;
- Kommunikációs modul;
- Saját csapatok modul;
- Felderítési adatmodul;
- Jelentő és üzenő modul;
- Archiválási és adminisztrációs modul;
- Adatbázis modul.

Szakasz, század, zászlóalj törzs terminál:

- Komplex alapszoftver;
- Kommunikációs modul;
- Saját csapatok modul;
- Felderítési adatmodul;
- Jelentő és üzenő modul;

- Archiválási és adminisztrációs modul;
- Műveleti modul;
- Tervezési modul;
- Irodai modul;
- Külső rendszer interfész modul;
- Meteorológiai információs modul;
- VSB információs modul;
- Egészségügyi ellátó modul;
- Műszaki támogató modul.

Szakcsapat terminál:

- Komplex alapszoftver;
- Kommunikációs modul;
- Saját csapatok modul;
- Felderítési adatmodul;
- Jelentő és üzenő modul;
- Archiválási és adminisztrációs modul;
- Meteorológiai információs modul;
- VSB információs modul;
- Egészségügyi ellátó modul;
- Műszaki támogató modul;
- Adatbázis modul.

Szakasz, század, zászlóalj adatbázis szerver:

- Komplex alapszoftver;
- Kommunikációs modul;
- Archiválási és adminisztrációs modul;
- Jelentő és üzenő modul;
- Adatbázis modul.

A modell elemeinek ismertetése

A komplex alapszoftver

A komplex alapszoftver, keretet nyújtva biztosítja az operációs rendszer, a szoftverelemek, aktivizált szoftvermodulok, a kommunikációs modul és a szükséges adatállományt biztosító adatbázis modul együttfutását, az optimális működésükhöz szükséges adatcserét, az aktivizált szoftvermodulokhoz szükséges követelmények szerinti megjelenítő és digitális térképkezelő szoftveregységet. Az aktivizált szoftvermodulokhoz szükséges kezelői műveletek elvégzését biztosító vezérlő, és interaktív adatkezelő felület valósít meg. Biztosítja a kommunikációs rendszer egységeinek szervízszintű alkalmazását, valamint az adminisztrátori beállításoknak megfelelően az alkalmazási profilhoz rendelt szoftvermodulok, alkalmazások meghívását, használatát.

A felderítési adatmodul

A modul biztosítja a felderítési adatok, azokkal kapcsolatos jellemzők, információk bevitelét, továbbítását; az elöljárótól származó felderítési adatok tárolását, adatbázisszerű és digitális térképi megjelenítését NATO szabvány szerinti taktikai

szimbólumokkal (MIL STD 252581), valamint a felderítési adatok értékelésének megjelenítését. Alkalmas a kiválasztott felderítési információknak a kezelő által meghatározott címzettekhez, illetve – a felderítési adatokra vonatkozó adatbázis frissítése céljából – a szintnek megfelelő szerverhez történő továbbítására; a saját maga által felderített célok, azokkal kapcsolatos jellemzők, információk bevitelére, a szintnek megfelelő szerverbe és az adatbázis modulba történő továbbítására, térképi megjelenítésére NATO szabvány szerinti taktikai szimbólumokkal. Végrehajtható vele a szervertől az alapterminálokra letöltött részadatbázist frissítő üzenetek fogadása, feldolgozása; az aktuálisan kijelölt tereprészlet domborzati viszonyainak, útviszonyainak, járhatóságának értékelése, megjelenítése, és az értékelés eredményeinek szükség esetén továbbítása más rendszerelemek, illetve a szerver adatbázis irányába.

A saját csapatok modul

A modul képes a saját csapatok, egységek, alegységek, kialakított csoportok adatbázis-szerű rendszerben történő nyilvántartására, digitális térképi adatbázison elemenként, vagy adott vezérelvszerinti csoportonként történő layer-szerű megjelenítésére, NATO szabvány szerinti szimbólumokkal. Nyilvántarthatóak vele a saját csapatok technikai eszközei, azok hozzárendelhetőek a digitális térképi adatbázison ábrázolt egységekhez, illetve általa megjeleníthető az eszközökkel kapcsolatos minden fajta információ. Biztosítja a saját csapatok technikai eszközeire vonatkozó látóképesség, láthatóság és felderítő képesség meghatározását, layer-szerű megjelenítését, és az ezekre vonatkozó lekérdezéseket; a rendszer elemektől fogadott real-time pozíció adataik alapján, az elemek valóshelyzetű megjelenítését, azok adatainak tárolását.

A tervező szoftver modul

A tervezés során ez a modul biztosítja a saját csapatok és a felderítési adatok megjelenítését NATO szabvány szerinti taktikai szimbólumokkal; az ellenséges erők, eszközök szervezeti elemek megjelenítését, adott pontból viszonyítottan láthatósági, felderíthetőségi információk megjelenítését, lekérdezhetőségét. Készíthetünk általa menetszámvetést oly módon, hogy a digitális térképi adatbázis alapján utak, földutak, indulási, érkezési és érintő pontok kijelölésével meghatározza az előállt menetvonalat, meghatározza a menetvonal hosszát, biztosítja a menetvonal elemek jelölését, javaslatot tesz különféle szempontok szerinti optimalizált útvonalakra, és az így előállt adatok alapján összegzett számvetést készít. Manőverszámvetést készít oly módon, hogy a digitális térképi adatbázis alapján utak, földutak, fontosabb pontok megjelölésével meghatározza a manőverjellemzőket, javaslatot tesz különféle szempontok szerinti optimalizálásra, és az így előállt adatok alapján összegzett számvetést elkészíti. Az elkészített számvetésekből az alárendelt alegységekre vonatkozó lebontási tervet képez. Alkalmas lőszerkészlet számvetési terv elkészítésére, az alárendeltektől kapott korábbi adatok alapján. Az elkészített terveket tárolja, az adatbázis szerver az alárendeltek irányába, megjeleníthető módon továbbítja.

[81] térképi átlapolás (overlay) – egyes ***térképi*** rétegek egymásra fektetése, szimbólumokkal történő ellátása

A műveleti modul

Az rendszer ezen eleme rendelkezésére bocsátja a felhasználó számára a kommunikációs rendszeren keresztül kapott real-time pozíciós adatok alapján, a rendszer elemeinek valós pozíciós megjelenítését; az ellenségre vonatkozólag beérkezett, vagy manuálisan bevitt adatok, információk osztályozását, csoportosítását, azok alapján a célok megsemmisítésére vonatkozólag célmegjelölést, feladatszabást; az egység, illetve az alárendeltek számára feladatszabást, annak a kommunikációs modullal a megfelelő címzetthez történő azonnali továbbíttatását. Biztosítja az egységek, illetve az alárendeltek által kapott feladatok, tevékenységek megjeleníthetőségét, a pillanatnyi helyzet alapján a teljesítettség nyomon követését.

Az adatbázis modul

A saját és az ellenséges csapatokra vonatkozólag fellelhető adatok fogadására, rendezett tárolására szolgál egyetlen nagy adatbázis részeként, biztosítva a kezelői igények alapján a teljes információtartalomra vonatkozó lekérdezések lehetőségét. A saját és az ellenséges csapatokra vonatkozólag, az egység, és az alárendelt alegységek pozíciós és feladat információinak nyilvántartásának, az egység-azonosítók egymáshoz rendelési nyilvántartásának kezelését, azzal kapcsolatos információk fogadását, tárolását végzi el az adatbázis részeként. Alkalmas az alegységek személyi nyilvántartásának, a veszteségek nyilvántartásának kezelésére, azzal kapcsolatos információk fogadására, tárolására adatbázis részeként, kérés esetén elemeinek továbbítására másik adatbázis modul irányába. Elvégzi a lőszerkészlet nyilvántartásának kezelését, tárolását; az alegységek technikai eszközei állapotának, feltöltöttségi, üzemképességi nyilvántartásának kezelését, tárolását. Biztosítja a vegyi, sugár és bakteriológiai helyzettel kapcsolatos információk fogadását, tárolását egyetlen nagy adatbázis részeként, továbbítását, a kapcsolatos adatbázis állomány kezelését, a védekezési képességek nyilvántartását. A modul szolgáltatja a személyi állománya egészségügyi adatait, rendelkezésre álló gyógyszer, vér és gyógyászati segédeszközök mennyiségét, a veszteségek és erőforrások nyilvántartásának kezelését, azzal kapcsolatos információk fogadását, tárolását, kérés esetén adatok továbbítását; a műszaki anyag, illetve műszaki szempontból a hadszíntéri helyzettel kapcsolatos adatbázis állomány kezelését, azzal kapcsolatos információk fogadását, tárolását, a védekezési képességek nyilvántartását. Képes adminisztrátori beavatkozással, vagy automatizáltan a vele kapcsolatban álló szerverekkel az adatbázis tartalom szinkronizálására, alapterminálok esetén részadatbázis tartalom fogadására. Automatizáltan, az üzenetként kapott információk alapján, az adatbázis tartalom frissíti, szükség esetén azt továbbítja.

A kommunikációs modul

A modul biztosítja a folyamatos információáramlást a rendszerelemek között; a rendszer elemeinek GPS saját pozíció adatainak küldését (percenkénti gyakorisággal), a többi egység ilyen adatainak fogadását az eszközre jellemző azonosítóval és időbélyeggel; a folyamatos adatátviteli kapcsolatot a terminálok, és a szerverek közötti adatcserére NATO szabványosított ADatP-382 link protokoll alapján.

[82] Allied Data Publication No 3 – szövetséges adatok közzététele 3-as változat

Az adatátviteli lehetőségek:

- TCP/IP83 alapon LAN-on, címtábla alapján;
- UDP/IP84 alapon multicast móddal;
- TCP/IP alapon ISDN S0 felületen, címtábla alapján;
- MRR rádióhálón, X25 protokollban;
- MRR rádióhálón, transzparens módon.

Alkalmas szöveges üzenetek átvitelére az elöljáró illetve az alárendeltek irányába; riasztási üzenetek, egészségügyi eseményüzenetek vételére és továbbítására; digitális, formanyomtatványok kezelésére, továbbítására, megjelenítésére választhatóan magyar és angol nyelven. Továbbá biztosítja még az adatbázis szervereknél, a helyi TCP/IP alapú törzsterminálokból álló hálózat, és az alárendelt/előjáró szintek közötti adatátvitelt. Ez történhet, a szerverhez csatlakoztatott MRR rádió(ko)n, vagy a szerverhez csatlakoztatott IP alapú LAN-on, WAN-on keresztül;

Meteorológiai információs modul

Biztosítja az időjárás jelentések vételét, tárolását, bevitelét, megjelenítését, illetve továbbítja azt az alárendelt alegységek és az adatbázis modul részére. Alkalmas meteorológiai adatok, rendszeres jelentések, előrejelzések bevitelére, illetve fogadásra, kezelésre, megjelenítésére a NAMIS85, valamint a KMIR86 rendszertől; a saját csapatoktól származó meteorológiai adatok, rendszeres jelentések bevitelére, fogadására, kezelésére, megjelenítésére.

Jelentő és üzenő modul

Fogadja és megjeleníti az elöljáró, illetve az alárendeltek irányából érkező formalizált és nem formalizált parancsokat, jelentéseket; biztosítja formalizált riasztási, egészségügyi üzenetek készítését, küldését, fogadását, megjelenítését, valamint azokkal csatolt fájlok (szöveges dokumentum, kép) továbbítását a rendelkezésre álló címlista alapján.

Külső rendszer interfész modul

A modul biztosítja formalizált parancsok, célmegjelölési üzenetek küldését, az ÁRPÁD M2 ATR87 irányába, Formalizált üzenetek és felderítési információk fogadását, azok megjelenítését, tárolását az ÁRPÁD M2 ATR irányából (tűzmegfigyelő, tűztámogató pontoktól).

Véleményezés

A rendszer kiszolgálásához szükséges személyi és technikai hátteret jelenleg nem látom biztosítottnak. A leendő szak- és kezelőállományt folyamatosan képezni kell, hogy felkészülten tudja fogadni ezt az új rendszert. Zászlóalj szinten az informatikai állomány létszámának további „lefaragását” meg kell állítani. További felkészült/felkészített szakemberek szükségesek a rendszer működtetéséhez.

---

[83] Transmission Control Protocol/Internet Protocol – átviteli vezérlő protokoll/internet protokoll

[84] User Datagram Protocol – felhasználói datagram protokoll

[85] NATO automatizált meteorológiai információs rendszer

[86] Katonai ***Meteorológiai*** Információs Rendszer

[87] automatizált tűzvezető rendszer

A szoftvereket nem feltétlen MS Windows 2000 professional operációs rendszerre kell fejleszteni, mert a fejlesztési ciklus végére teljesen elavulttá fog válni (mint ahogy napjainkban se jelenik már meg kellő számú frissítés hozzá). Az Automatizált Harcvezetési és Információs Rendszer bevezetését a lehető legkisebb időtényezővel kellene számvetni, mivel az információtechnológia rohamos ütemben fejlődik, nem célszerű a rendszer bevezetését elhúzni, mert elavulttá válik.

A modul rendszert alkalmassá kell tenni újabb modulok fogadására is, álljon készen a modern kor követelményei szerint újonnan megjelenő, eddig nem kidolgozott modulok beintegrálására. A desktop és szerver számítógépek nagy száma miatt félő, hogy csorbulni fog a mobilitás, viszont az ütés és folyadékálló laptopok nagyon jól alkalmazhatók tábori körülmények között. Biztosítani kell egy megfelelő nagyságú raktári készletet és cserealkatrészt a hardverelemekhez, valamint a hardverek modernizációjának lehetőségét új információtechnológiák megjelenése esetén is.

Tábori körülmények között nagy figyelmet kell szentelni a stabil tápfeszültségnek. Ennek biztosítása létfontosságú a számítógépek szempontjából. A wireless LAN kapcsolatot javaslom újra átgondolni annak sebezhetősége miatt. Jelenleg nem állnak rendelkezésre 100%-os biztonságot jelentő WLAN hálózati eszközök. A kommunikációs, híradó részek elemenkénti cseréje nem biztosítaná a vezető szervek és az alárendeltek valós időben történő irányítását a digitális és az analóg anomáliák miatt.

A rádióeszközökön való információ továbbítását alapvetően az MRR rádiók kezelési szabályai határozzák meg. A rádiókezelőknek rendelkezniük kell nemzetbiztonsági bevizsgálással, így a zászlóalj szintű harcvezetési rendszer kezelőinek is. Szükséges meghatározni a rendszerben továbbítható dokumentumok minősítését, a kezelők nemzetbiztonsági bevizsgálásának követelményét is. Minősített dokumentumok továbbítására is szükséges lehet a rendszert kialakítani.

Az Automatizált Harcvezetési és Információs Rendszernek kompromittálódás ellen biztosítottnak kell lennie. Garantálnia kell az azonnali adattörlést mielőtt az eszközök idegen kézbe kerülnének, hasonlóan az MRR rádiókhoz.

Felhasznált irodalom

[1] Pándi Balázs – Pándi Erik: A térinformatika tábori hírrendszerben történő alkalmazásának kérdései, „Kommunikáció 2008.” Nemzetközi szakmai-tudományos konferencia kiadványa, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2008.

[2] Fekete, Karoly: Protocol based considerations of WiMax in military communications networks, „Kommunikáció 2008.” Nemzetközi szakmai-tudományos konferencia kiadványa, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2008.

[3] Dobák Miklós–Marosi Miklós: Vezetés-szervezés, egyetemi tankönyv 4. kiadás, Budapesti Közgazdaságtudományi Egyetem, Budapest, 1996.

[4] Dr. Munk Sándor ezredes: Katonai informatika, Jegyzet a ZMNE hallgatói számára, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 1997.

[5] Rajnai Zoltán–Dr. Sándor Miklós: Út a digitális kommunikációs hálózatok felé I. (ZMNE Egyetemi Közlemények1997/1. szám)

[6] Rajnai Zoltán: A tábori alaphírhálózat korszerűsítésének lehetőségei. (ZMNE, Országos Tudományos Konferencia kiadványa, 2000.)

FARKAS Tibor – NÉMETH József Lajos

A „HÉJÁK" ÉS A „GALAMBOK" MINT A KÖZVÉLEMÉNY ÉS KOMMUNIKÁCIÓ BEFOLYÁSOLÓI

Az Egyesült Államok a nemzetközi közvélemény által történő negatív megítélésének legfontosabb megállapításai a „a világ leggazdagabb országa", „a legnagyobb fogyasztói társadalom", „az egyetlen olyan hatalom, amely mindenbe – kérés nélkül – beleavatkozik" és a kétségkívül rendkívül népszerűtlen iraki háború, amelyet napjainkra egyre kiegészít a már az amerikai társadalmon belül is egyre kevésbé támogatott afganisztáni misszió. Az előbbi megállapításokkal szemben, szinte ellentétesen hatnak azok a pozitív üzenetek, amelyek „az amerikai álomról", „az önzetlen segítségnyújtásról" és „a legjobban működő demokráciát" vetítik elénk. A fentiek alapján tehát felmerül a kérdés: vajon a fenti üzeneteknek mi a valóságalapjuk? Vajon egybeesik-e a kormányzat stratégiája a közvélemény által megfogalmazottakkal? Milyen értékek és érdekek mentén befolyásolható a kormányzat kommunikációja és a közvélemény attitűdje? Az alábbiakban – a terjedelmi korlátok figyelembe vételével – a fenti kérdésekre keressük a választ, különös tekintettel a 2003-as iraki háború előestéjére érvényes kormányzati kommunikációt és közvéleményt befolyásoló „héják" és „galambok" viszonyrendszerére az Egyesült Államokban és a transzatlanti kapcsolatokban.

Néhány elméleti alapvetés

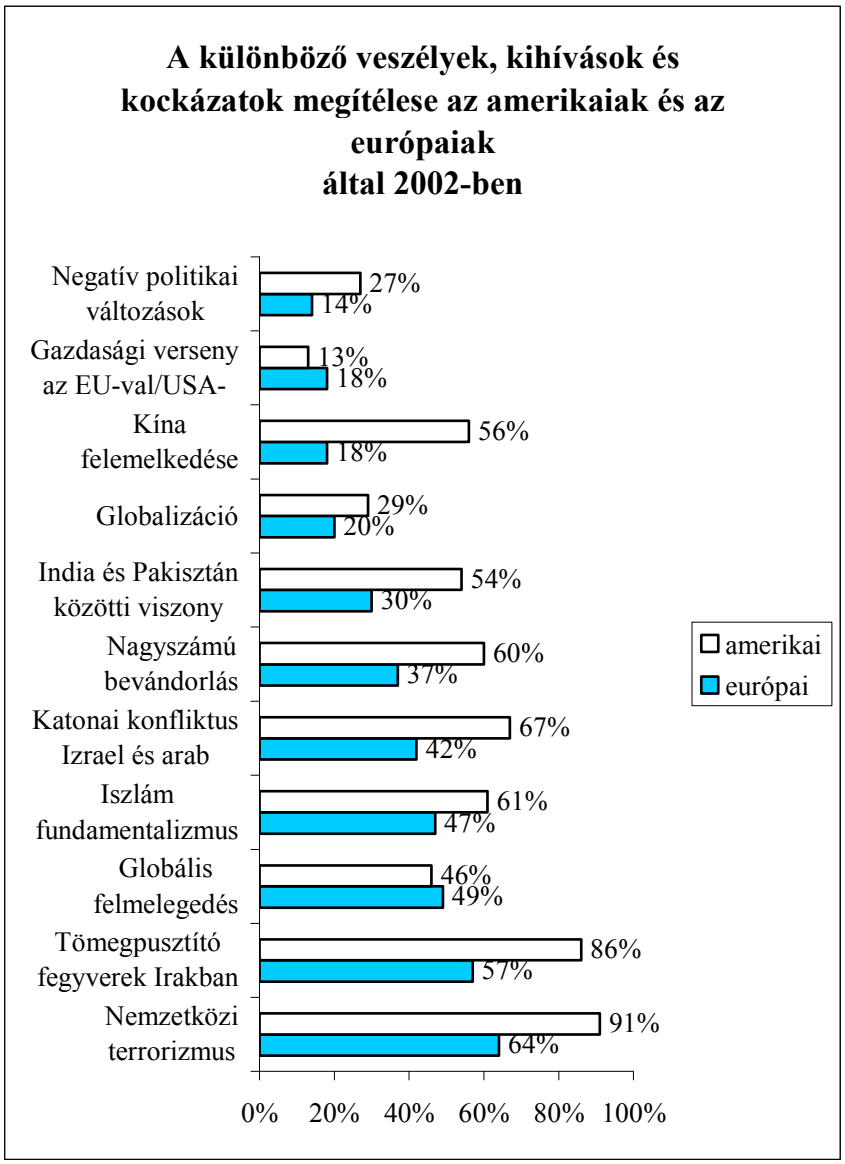
Az Egyesült Államokra a világ közössége a második világháborút előestéjén úgy tekintett, mint egy feltörekvő fiatal nemzetre, amely hatalmasa gazdaságának köszönhetően emberek millióinak ad munkát és biztosít megélhetést, de nem akar tevőlegesen a nemzetközi politika egyik legfőbb formálója lenni. Ebben az időszakban – és az azt megelőző mintegy 200 évben – a nagyhatalmak közötti erőviszonyokat különösen Nagy-Britannia, Franciaország és Németország, valamint Oroszország interakciói dominálták. 1945-re azonban a világ elfogadta, hogy a brit királyság akarva-akaratlanul átadta vezető szerepét Amerikának, amely innentől kezdve a Szovjetunióhoz való viszonya alapján határozta meg magát: ez alapján alakította ki helyét és szerepét a hidegháborúban. Ebben az időszakban a korábban a náci Németországgal szemben is megfogalmazott „jó-rossz" viszonyrendszer kommunikációja folytatódott, amelyben az USA megtartotta a „jó" szerepét, egyúttal a szovjeteket a negatív ellenponttal, a „gonosz" szerepével ruházta fel. A Szovjetunió bukásával gyakorlatilag is beigazolódott az a tétel, amely szerint a „jó legyőzte a rosszat", de immár nem létezett az a kézzel fogható viszonyítási alap, amelyhez képest az amerikaiak önmagukat és tetteiket meghatározták. Ebben az időszakban a közvélemény úgy tekintett Amerikára, mint egy olyan személyre, amely „felnőtt" a feladathoz, mi több, a lehető legjobb teljesítményt produkálta. A részben erre a viselt pozícióra alapozott, hidegháború utáni időszakra vonatkozó elképzelések azonban, amelyek egy biztonságosabb és békésebb periódust vizionáltak, nem váltak valóra: a biztonsági kihívások, fenyegetések és veszélyek száma

megtöbbszöröződött, számos helyi háború tört ki, amelyekben az USA, mint önjelölt „rendcsináló" és „rendfenntartó" jelent meg. (Fontos megjegyezni, hogy ez utóbbi szerepet nem egyszer az európai partnerekre hárította.) A nemzetközi kapcsolatok teoretikusai között komoly vita bontakozott ki arról, hogy a hidegháború utáni években az Egyesült Államok egyedüli világhatalomként vagy más hatalmi gócpontokkal (lásd: Európa, Kína) közösen formálja-e a világpolitikát? Ez az ún. unilaterális-multilaterális viszonyrendszer a napjainkban is tetten érhető a nemzetközi közösség működésének vizsgálatakor. Ebben az időszakban az Egyesült Államokat leginkább úgy lehetett jellemezni, mint a képességeivel tisztában lévő, de felelősségét még nem teljesen átlátó hatalmat. A 2001. szeptember 11-én bekövetkezett terrortámadások után az USA azonnal meghirdette a „terror elleni háborúját - War on Terror", amelyhez a kezdeti időszakban számos ország csatlakozott, bár az ezzel kapcsolatos európai felfogásbeli különbséget már ekkor jól tükrözte a „harc a terrorizmus ellen – Fight Against Terrorism" üzenetrendszere.

A különböző veszélyek, fenyegetések és kihívások megítélése kapcsán 2002-ben egyértelműnek tűnt, hogy a nemzetközi terrorizmus a legjelentősebb probléma, ugyanakkor a különböző gazdasági jellegű kérdések kevésbé tűntek jelentős gondnak az európaiak és az amerikaiak számára. Általában az is megfigyelhető, hogy a megjelenített témakörök szinte mindegyikénél az amerikai (veszély)felfogás erősebben nyilvánult meg, mint az európai.

Fontos megjegyezni, hogy a „jó-rossz" párosítás ekkor ismét feltűnt az amerikai gondolkozásban és stratégiai kommunikációban: itt elég csak a 2002-es amerikai nemzeti biztonsági stratégiában megfogalmazott „gonosz tengelye" kifejezésre gondolnunk (ide sorolták Irakot, Iránt és Észak-Koreát), amely kiegészült az ún. „preemptív csapás"88 eszközével. A 2003 márciusában megindított Irak elleni offenzíva már ennek az eszköznek a konkrét alkalmazását jelentette, egyúttal magával hozta azt a kemény üzenetet is, hogy az USA önállóan, hagyományos szövetségesei nélkül is alkalmazza katonai erejét, ha és amennyiben azt nemzeti biztonsági érdekei megkívánják. Az iraki háború korántsem ment oly könnyen, mint azt korábban feltételezték: bár a hagyományos harccselekmények kétségkívül az amerikaiak győzelmével értek véget, de a háború koránt sem fejeződött be: megkezdődött az irakiak ellenállása, amely egy erőteljes aszimmetrikus hadviselésre kényszerítette az amerikaiakat. A 2003-as iraki háborút követően az USA olyan hatalomként jelent meg a nemzetközi közvélemény szemében, amely inkább a rendelkezésre álló katonai erejét alkalmazta a problémás kérdések megoldásában: más, puha eszközökkel nem akart vagy bizonyos körülmények miatt nem tudott élni. Mindezt tetézte még a különböző terrorszervezetek, de más államok (például: Irán, Észak-Korea) egyre kifinomultabbá és hitelesebbé váló kommunikációja, amely az Egyesült Államokat agresszornak mutatta be.

[88] A preemptív csapás azt jelenti, hogy már a gyanú is elegendő ahhoz, hogy az USA katonai erővel lépjen fel bármilyen ellenféllel szemben.

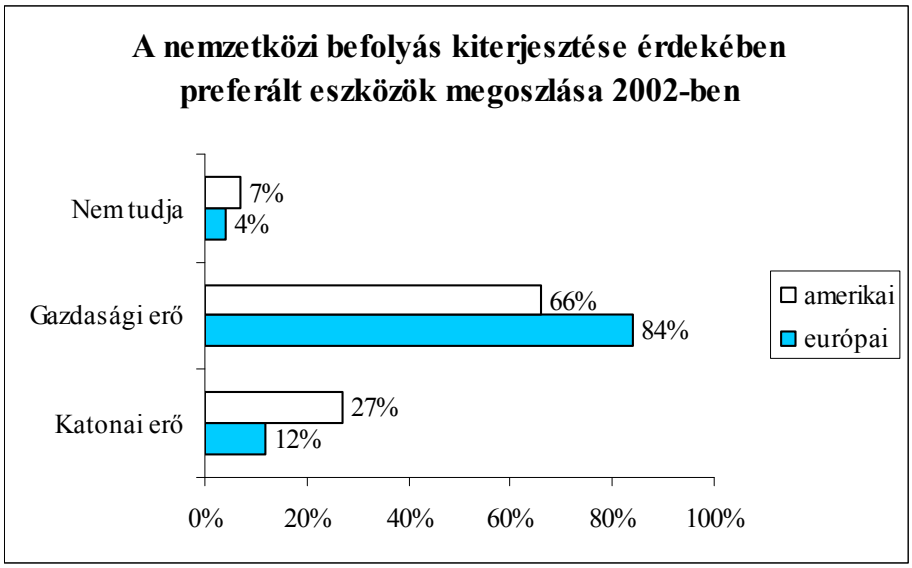


1. számú ábra

(Forrás: www.worldviews.org, letöltve: 2006. május 30.)
(szerkesztette: Németh József Lajos)

A „héják és galambok" az iraki háború előestéjén

2002-ben az amerikai közvélemény jobban preferálta a katonai erő alkalmazását a gazdasági eszközök felhasználásával szemben befolyása erősítése végett, mint az európaiak, azonban mindkét fél számára az elsődleges eszköz továbbra is ez utóbbi maradt.



2. számú ábra
(Forrás: www.worldviews.org, letöltve: 2006. május 30.)
(szerkesztette: Németh József Lajos)

A közvélemény-kutatások eltérő eredményeinek hátterében és adott esetben a kormányzat és a közösség (társadalom) véleménykülönbségében néhány rendkívül jelentősnek mondható alapérték és felfogás áll, amelyek döntően befolyásol(hat)ják a közvélemény aktuális megjelenését. Nemzetközileg elismert szakértők a transzatlanti kapcsolatokban megjelenő attitűdök jobb megértése érdekében olyan tipológiát állítottak fel, amelyben a rendelkezésre álló eszközök (katonai, gazdasági) használata iránti hajlandóság és azok preferálása szerint megkülönböztetik a „héja", a „galamb", a „pragmatista" és az „izolacionista" külpolitikai iskolákat.89

E megkülönböztetés szerint

- a „héják" szerint a háború olykor szükséges az igazság bebizonyítása miatt és a katonai erő fontosabb a gazdaságinál. Ők adott esetben hajlamosak az olyan nemzetközi szervezetek megkerülésére, mint például az ENSZ.
- a „galambok" alapvetően a gazdasági eszközök felhasználásában hisznek, számukra a háború csak a végső stádiumban elfogadott. Előszeretettel támogatják a nemzetközi biztonsági szervezeteket (pl. ENSZ), nagyon fontosnak tartják azok megerősítését. Véleményük szerint erő alkalmazása csak nemzetközi jogosítványok alapján lehetséges.
- a „pragmatisták" úgy gondolják, hogy a háború olykor szükséges, de fontosabbnak tartják a gazdasági eszközöket a katonaival szemben. Elfogad-

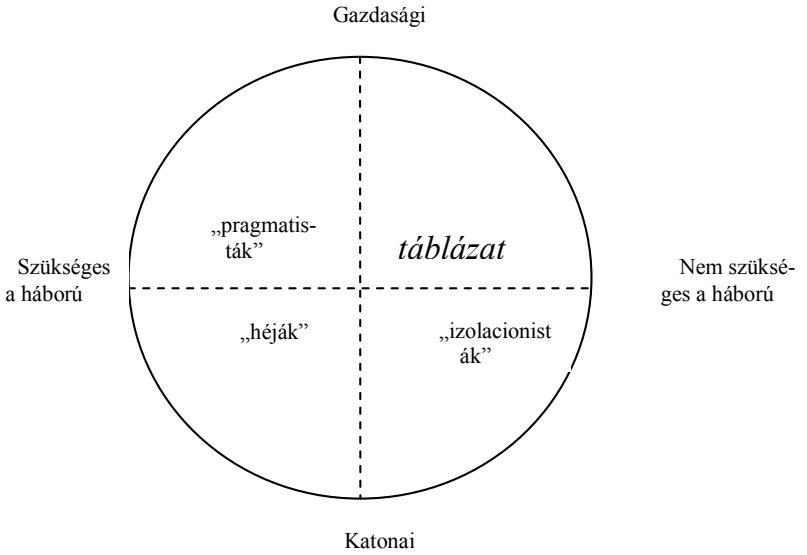
[89] ASMUS, Ronald és EVERTS, Philip P. és ISERNIA, Pierangelo: Power, War and Public Opinion: Thoughts on the Nature and Structure of the Trans-Atlantic Divide, Transatlantic Trends 2003, http://www.policyreview.org/feb04/asmus.html, letöltve: 2006. július 31.

ják és támogatják a nemzetközi szervezeteket, ugyanakkor hajlandóságot mutatnak önálló katonai akciók támogatására, amennyiben nemzeti érdekeik védelme megköveteli azt.

- az „izolacionisták” nem hisznek abban, hogy a háború szükségszerű, hasonlóképpen szkeptikusok a gazdasági eszközök hatásában a nemzetközi kapcsolatokra.

Az alábbi táblázatban összefoglalva láthatjuk a négy csoport egymáshoz való viszonyát:

A külpolitikai attitűdök tipológiája



3. számú ábra

(forrás: http://www.policyreview.org/feb04/asmus.html)

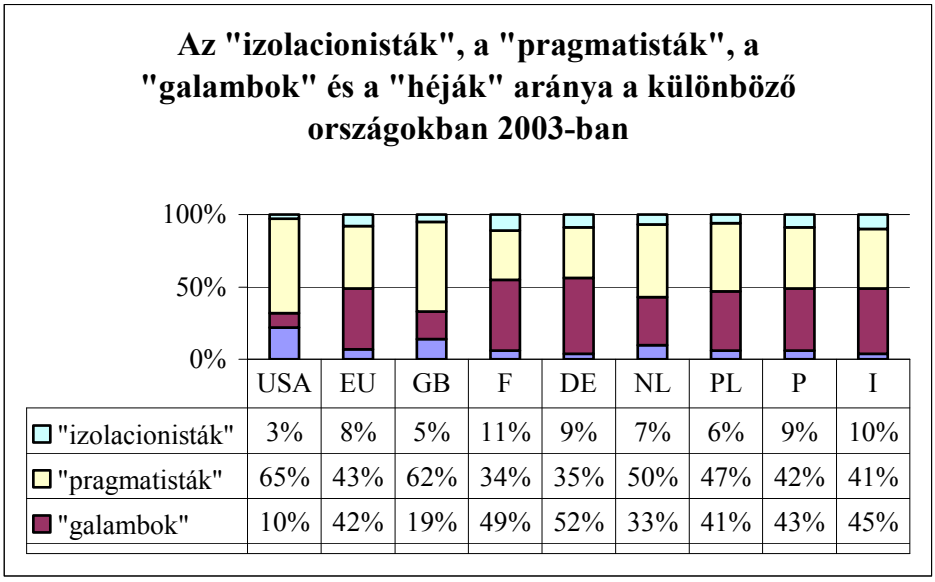
(szerkesztette: Németh József Lajos)

Az ábrán jól látható, hogy a különböző csoportok közötti átjárás biztosított, „vegytiszta” formában a fenti csoportok a nemzetközi kapcsolatokban viszonylag ritkán fordulnak elő.

A fenti négy csoport egymáshoz való viszonyát az elmúlt időszakban a katonai kiadások és az ENSZ szerepének megítélése, a gazdasági segélyezés, a rendelkezésre álló erők gazdasági és/vagy katonai használata, a nemzetközi kapcsolatokban betöltött szerep kapcsán jellemezhetjük a legszembetűnőbb mértékben.

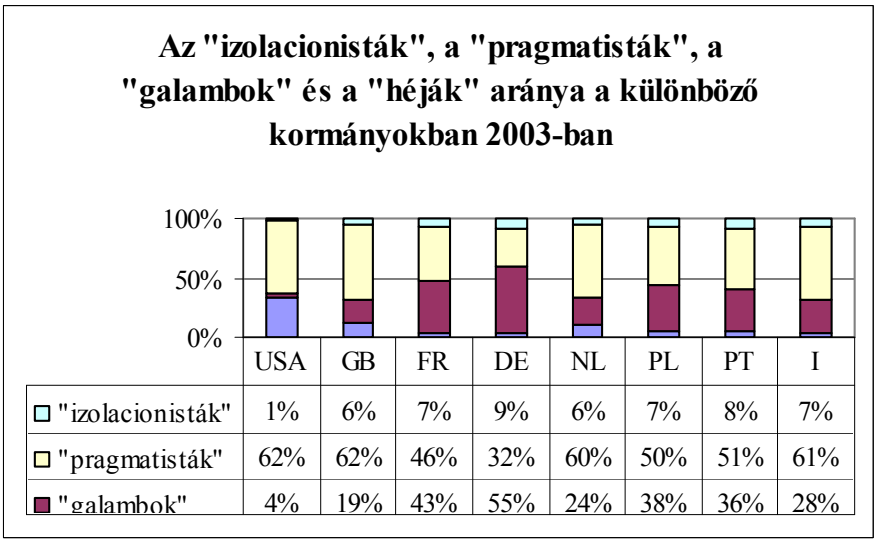
Érdemes szemügyre venni az európai országokon belüli jelentős eltéréseket, amelyek ugyancsak megnehezítik egy egységes európai álláspont kialakítását és végrehajtását.

A fenti felosztást alkalmazták a kormányzó elitek tipizálása kapcsán 2003-ban, akik szerepe a transzatlanti kapcsolatok alakításában mindenképpen mérvadónak mondható:



	USA	EU	GB	F	DE	NL	PL	P	I
"izolacionisták"	3%	8%	5%	11%	9%	7%	6%	9%	10%
"pragmatisták"	65%	43%	62%	34%	35%	50%	47%	42%	41%
"galambok"	10%	42%	19%	49%	52%	33%	41%	43%	45%

4. számú ábra
(forrás: www.policyreview.org/feb04/asmus.html, letöltve: 2006. május 30.)
(szerkesztette: Németh József Lajos)



	USA	GB	FR	DE	NL	PL	PT	I
"izolacionisták"	1%	6%	7%	9%	6%	7%	8%	7%
"pragmatisták"	62%	62%	46%	32%	60%	50%	51%	61%
"galambok"	4%	19%	43%	55%	24%	38%	36%	28%

5. számú ábra
(forrás: www.policyreview.org/feb04/asmus.html, letöltve: 2006. május 30.)
(szerkesztette: Németh József Lajos)

A „héják” aránya jóval magasabbnak volt mondható az USA republikánus kormányában, mint a társadalom egészét tekintve. Franciaország esetében a „pragmatisták” és a „galambok” aránya megfordult, míg a portugál és olasz kormányok esetében az előbbiek voltak döntő fölényben 2003-ban.

Ha a fenti általános tipológiát kivetítjük a felmérésekben résztvevő országokra, jelentős különbségeket fedezhetünk fel:

- Az „izolacionisták” leginkább Franciaországban vannak jelen, jól tetten érhető ez a francia kül- és biztonságpolitikai törekvések „különutas” mivoltában, amely olykor elég jelentős feszültségeket okozott a transzatlanti kapcsolatokban.
- A „pragmatisták” döntően az Egyesült Államokban és Nagy-Britanniában lelhetők fel, ugyanakkor szembetűnő az is, hogy a „héják” leginkább ez előbbi ország tekintetében mérvadóak.
- A „galambok” aránya összeurópai szinten elég magasnak mondható, különösen jellemző ez Németország esetében, ami alapvetően történelmi okokkal magyarázható. Ez utóbbi csoport esetében jelentős különbség van az Egyesült Államok és az európai átlag között, ami részben magyarázatot ad arra, hogy miért is alkalmaz nehezebben Európa fegyveres eszközöket a nemzetközi kapcsolatok vitás kérdéseinek rendezésekor.

Záró gondolatok

A fentiek alapján megállapítható, hogy a transzatlanti közösségben a közvélemény által és számára megállapított legfontosabb üzenetek alapvetően az adott társadalom és kormányzat meghatározott csoportjai által vallott értékek és érdekek mentén jelennek meg. Bár a kormányzati elképzelések és a közvélemény attitűdjei nem mindig esnek egybe, mégis ezek összehangolása elengedhetetlen, amelyet jól példáz az iraki háborút követő „kommunikációs hadviselés”, amelynek eredményeként az USA nem volt képes döntően pozitív képet kialakítani magáról.

A 2007-ben az USA kormánya által kiadott „Nemzeti Stratégia a Nyilvános Diplomáciára és Stratégia Kommunikációra” elnevezésű dokumentum (US National Public Strategy and Strategic Communication) már annak a felismerésnek az eredménye, amely az rendelkezésre álló információk hatékony felhasználásának szükségességét és a vonatkozó célkitűzések és folyamatok rendszerezését mondja ki stratégiai szinten.

Ennek megfelelően az új, Barack Obama vezette demokrata amerikai kormányzatnak komoly kihívásokkal kell szembenéznie mind a „héják” és „galambok” közötti vita rendezésében, mind pedig a nemzetközi közvélemény negatív attitűdjeinek megváltoztatása kapcsán.

Felhasznált irodalom:

[1] Virgil Magee: Strategic Communications in a Multi-National Environment, http://www.articlesbase.com/public-relations-articles/strategic-communications-in-a-multinational-environment-972797.html, letöltve: 2009. szeptember 08.

[2] Robert H. Risberg: Improving the United States Strategic Communications Stategy, US Army War College, 2008. március 15.

[3] US National Public Strategy and Strategic Communication, 2007. június, Amerikai Egyesült Államok kormánya

[4] Németh József: A transzatlanti kapcsolatok néhány vitás kérdése biztonságpolitikai megközelítésben, ZMNE, 2006

FEKETE Károly

AUTONÓM ÜZEMMÓDRA ALKALMAS KOMPLEX MUNKAHELYEK KOMMUNIKÁCIÓJÁNAK KIALAKÍTÁSA

Zrínyi Miklós Nemzetvédelmi Egyetem
Híradó tanszék
Hungária krt. 9-11., 1058 Budapest, Hungary
Tel: + 36-1-432-9000/29153, FAX: +36-1-432-9025,
email: fekete.karoly@zmne.hu

Abstract

Napjainkban a társadalmi-tudományos fejlődés, a felgyorsult életvitel eredményeként az emberek mozgástere kibővült. Egyre intenzívebb jelenlétünk a természetben, folyamatos kontaktusunk a természetben előforduló betegségek, fertőzések lelőhelyeivel illetve esetenként a szándékos biológiai diverziók veszélye miatt megnőtt a valószínűsége annak, hogy lokálisan vagy globálisan fertőzött-szennyezett, az adott terület kommunikációs infrastruktúrájához nem vagy csak korlátozottan hozzáférhető területeken kell speciális orvosi-mentő feladatokat végrehajtani. A feladatok a rendelkezésre állót kommunikációs infrastruktúrát tekintve nem csak nagyvárosi, hanem nomadikus illetve rural környezetben is megjelenhetnek, melyek hatékony végrehajtását egy önálló működésre és a környezetében rendelkezésre álló távközlő, informatikai hálózatokhoz sokoldalúan csatlakozni képes mobil kommunikációs komplexum támogathatja.

Kulcsszavak : biológiai diverzió, komplex kommunikációs munkahely, autonóm üzemmód

A speciális feladat végrehajtását az autonóm üzemelésre is alkamas, mobil kommunikációs megoldások biztosíthatják a kapcsolatot a helyi feladatokat ellátó és a nagyobb távolságra található szakmai vezetés között.
Ennek megfelelően a korszerű, mobil eszközkészletnek biztosítania kell a kiemelt környezetvédelmi fokozat (KVF) feltételei és szélsőséges időjárási (alkalmazási) körülmények mellett, önállóan vagy egyéb rendszerekkel együttműködve, akár katasztrófahelyzetben, rombolt infrastrukturális környezetben az alaprendeltetéssel összefüggő következő működés feltételeket:

- a többcélú felhasználhatóságot;
- normál működést, ABV szennyezéstől mentes környezetben, a teljeskörű kiszolgáló rendszerek kiépítésével települve;
- az alaprendszer és a vizsgálati eljárások végrehajtása alkalmasság szerint funkcionálisan megkülönböztetett és a vonatkozó biztonsági irányelvek előírásai figyelembevételével speciálisan kialakított (csökkentett védelmi fokozatú) változatát;

- a speciális fogadó-előkészítő és azonosító tevékenységek végrehajtásához szükséges, különféle rendeltetésű labortechnikai, illetve diagnosztikai eszközök működését;
- a málházott konténerváltozat közúti, vasúti, vízi és légi szállítóeszközökkel történő szállíthatóságát;
- a szállításkor fellépő igénybevételek elviselését.

    - belső híradást biztosító alrendszer;
    - külső híradást biztosító alrendszer;
- minták regisztrálása, az egyes minták feldolgozásának folyamatos nyomonkövetése;
- adatfeldolgozás:
    - a laboratórium informatikai hálózata;
    - a hálózatba kapcsolt számítógépek;
    - speciális szoftverek;
    - tevékenységirányítási rendszer;
- adatok továbbítása;
- térfigyelő rendszer.

Az ezen összetett feladatrendszer kielégítésére alkalmas kommunikációs eszköz illesztése az alkalmazás helyén rendelkezésre álló kommunikációs környezethez komplex szempontrendszer figyelembe vételét feltételezi.

Egyrészt fontos a komplex munkahely belső hálózatának típusa, másrészt a feldolgozni-továbbítani kívánt információ jellemzői (típus, sebesség, periodicitás), harmadrészt a kapcsolódó külső vezetékes és vezetéknélküli LAN-WAN hálózatok típusa.

Mivel a komplex munkahely belső kialakítása időben megelőzi annak valódi alkalmazását, fizikai kialakításának jellegzetességei miatt a belső kommunikációs megoldás kötött, valamint a belső LAN protokoll készlete IP alapú ezért azon kérdéskör mérvadó a kommunikációs illesztés szemszögéből, mely a külső környezethez való kapcsolódást illeti.

Figyelembe véve az eddig megfogalmazott ajánlásokat a speciális feladatot végrehajtó komplexum kommunikációs illesztésének legfontosabb szempontja a megfelelő OSI-ISO rétegkommunikációs szabványokhoz (ajánlásokhoz) való illeszthetőség figyelembe vétele.

A rétegkommunikáció elve többek között felosztja és egyben determinálja a következő területeket:

- A fizikai közeg kiválasztását, típusát;
- Az Speciális feladatot végrehajtó komplexum fizikai és hálózat függő interfészeinek kialakítását;

- A WAN-LAN hardverelemek típusát;
- A szükséges szoftveralkalmazásokat (ebben a fejezetben nem vizsgált kérdés).

A fizikai (átviteli) közeg az összekötő átviteli közeg természetétől függően lehet fizikailag összekötött és fizikailag nem összekötött kapcsolatokat támogató (bound és unbound: pl. optikai kábelek, elektromos jelvezetékek, rádióhullámok, lézeres összeköttetés). A kábelezés típusa a hálózat architektúrájától függ.

Az Ethernet kapcsoló (switch) a hozzáférési rétegben használt eszköz. Csakúgy, mint a hub, a kapcsoló is több állomást tud a hálózathoz csatlakoztatni. A hub-bal ellentétben, a kapcsoló képes arra is, hogy csak egy meghatározott állomásnak továbbítson egy üzenetet. Amikor az állomás egy másik állomásnak a kapcsolón keresztül küld üzenetet, a kapcsoló fogadja és dekódolja a keretet, majd kiolvassa belőle a fizikai (MAC) címet.

A LAN-on belül az összes állomást elhelyezhetjük egyetlen helyi hálózatba, de szét is oszthatjuk őket több, az elosztási réteggel összekapcsolt hálózatba. A megfelelő eljárás az elvárt eredménytől függ. Ha az állomásokat egyetlen helyi hálózatba tesszük, lehetővé válik, hogy mindenki közvetlenül kommunikálhasson egymással. Ebben az esetben csak egy szórási tartomány van, és az állomások ARP protokollt tudnak használni egymás megkereséséhez.

A forgalomirányítók bonyolultabbá teszik a hálózati konfigurációt, és késleltetést eredményeznek a helyi hálózatból egy másik hálózatba küldött csomag továbbításában. Következésképpen a kiválasztandó forgalomirányítóknak real-time forgalom feldolgozása esetén igen nagy sebességűeknek kell lenniük, hogy a forgalmi torlódásokat elkerüljük.

Vezetéknélküli LAN szabványok

Számos szabványt fejlesztettek ki annak érdekében, hogy a vezeték nélküli eszközök kommunikálni tudjanak egymással. Ezek meghatározzák a használt frekvencia tartományt, az adatátviteli sebességet, az információátvitel módját, stb. (0). A vezeték nélküli technikai szabványok létrehozásáért felelős elsődleges szervezet az IEEE.

Az IEEE 802.11-es szabvány határozza meg a WLAN környezeteket. Négy fő ajánlása létezik az IEEE 802.11 szabványnak, mely különböző jellemzőket ad meg a vezeték nélküli kommunikáció számára. A jelenleg létező ajánlások a 802.11a, 802.11b, 802.11g és 802.11n (a 802.11n a szöveg írásának idején még nem jóváhagyott). Összefoglaló néven, ezeket a technológiákat Wi-Fi-nek (Wireless Fidelity) nevezzük.

Egy másik szervezet, melyet Wi-Fi Szövetség néven ismerünk, a különböző gyártók WLAN eszközeinek teszteléséért felelős. Egy eszközön szereplő Wi-Fi embléma azt jelenti, hogy az eszköz megfelel a szabványoknak és képes más, ugyanezen szabványt használó eszközökkel való együttműködésre.

802.11a:

- Az 5 GHz-es frekvencia tartományt használja.

- Nem kompatibilis a 2.4 GHz-es sávot használó 802.11 b/g/n eszközökkel.
- Hatótávolsága nagyjából a 802.11 b/g hálózatok hatótávolságának 33%-a.
- Más technológiákhoz képest viszonylag költségesebb a megvalósítása.
- Egyre nehezebb 802.11a-nak megfelelő eszközt találni.

802.11b:
- A 2.4 GHz-es technológiák első képviselője.
- Maximális adatátviteli sebessége 11 Mbit/s.
- Beltérben maximálisan 50 méter, kültéren 100 méter a hatótávolsága.

802.11g:
- 2,4 GHz-es technológia
- 54 Mbit/s a maximális adatátviteli sebessége
- Hatótávolsága a 802.11b-val megegyezik
- Felülről kompatibilis a 802.11b-vel

802.11n:
- A legújabb, fejlesztés alatt álló szabvány
- 2,4 GHz-es technológia (a szabvány tervezet az 5 GHz támogatását is említi)
- Megnövekedett hatótávolsággal és átbocsátóképességgel rendelkezik.
- Felülről kompatibilis a meglévő 802.11g és 802.11b eszközökkel (a szabványtervezet a 802.11a támogatását is megemlíti)

Szabvány	Kibocsátás dátuma	Frekvencia	Adatátviteli sebesség (Max)	Maximális hatótávolság*
802.11	1997 Július	2.4 GHz	2 Mbit/s	nem definiált
802.11a	1999 Október	5 GHz	54 Mbit/s	50 m
802.11b	1999 Október	2.4 GHz	11 Mbit/s	100 m
802.11g	2003 Június	2.4 GHz	54 Mbit/s	100 m
**802.11n	1.06-os tervezet elfogadva 2006 November 2.0 tervezet jóváhagyva 2007 Március	2.4 GHz vagy 5 GHz	540 Mbit/s	250 m

1. ábra Az IEEE 802.11-es protokollkészlet alapján működő hálózatok legfontosabb jellemzői

Az IEEE 802.11n szabványt hivatalosan 2009. szeptemberében elfogadták.

Alapvetően két különböző WLAN kiépítési forma létezik: Ad-hoc és infrastruktúrális mód.

Ad-hoc

A vezeték nélküli hálózatok legegyszerűbb formája, amikor két vagy több vezeték nélküli állomást kapcsolunk össze egyenrangú hálózatot létrehozva. Az ilyen hálózatokat ad-hoc vezeték nélküli hálózatoknak nevezzük, és hozzáférési pontot (AP) nem tartalmaznak. Egy ad-hoc hálózat minden állomása a hálózat egyenrangú résztvevője. A hálózat által lefedett terület Független Alapvető Szolgáltatáskészletként (Independent Basic Service Set, IBSS) ismert.

Infrastruktúrális mód

Bár az ad-hoc szervezés megfelelő lehet kisebb hálózatok esetén, nagyobb hálózatoknál egy önálló eszköz alkalmazása szükséges a vezeték nélküli cellában zajló kommunikáció irányításához. Ezt a szerepet a hozzáférési pont látja el, amely eldönti, ki és mikor kommunikálhat.. Egy ilyen típusú vezeték nélküli hálózatban, az egyes STA-k nem képesek egymással közvetlenül kommunikálni. A kommunikációhoz minden eszköznek engedélyt kell kérnie az AP-től. Az AP irányít minden kommunikációt és törekszik arra, hogy minden STA-nak egyenlő joga legyen a közeghez való hozzáféréshez. Egy egyedüli AP által lefedett területet alapvető szolgáltatáskészletként (Basic Service Set, BSS) vagy cellaként ismerünk.

Az alapvető szolgáltatáskészlet (Basic Service Set, (BSS) a WLAN hálózatok legkisebb építőeleme. Egy AP által lefedett terület nagysága korlátozott. A lefedettségi terület kibővítéséhez több BSS is összeköthető egymással egy elosztórendszer (Distribution system, DS) használatával. Ezzel egy Extended Service Set (ESS) jön létre. Egy ESS több hozzáférési pontot használ. Az egyes AP-k különálló BSS-ben vannak.

A vezetékes hálózatokkal ellentétben, a vezeték nélküli hálózatoknak nincsenek pontosan meghatározott határai, így nehéz meghatározni egy-egy vezeték nélküli hálózati megvalósítás hatókörét. Abban az esetben, ha adott a lehetőség, célszerű mindegyik változatát a konténer légterében és azon belül a komplex munkahely belsejében kialakítani. Ez a megoldás hosszútávon biztosítja a nagyon gyorasn fejlődő vezetéknélküli hálózati elemekkel való technikai kompatibilitás lehetőségét.

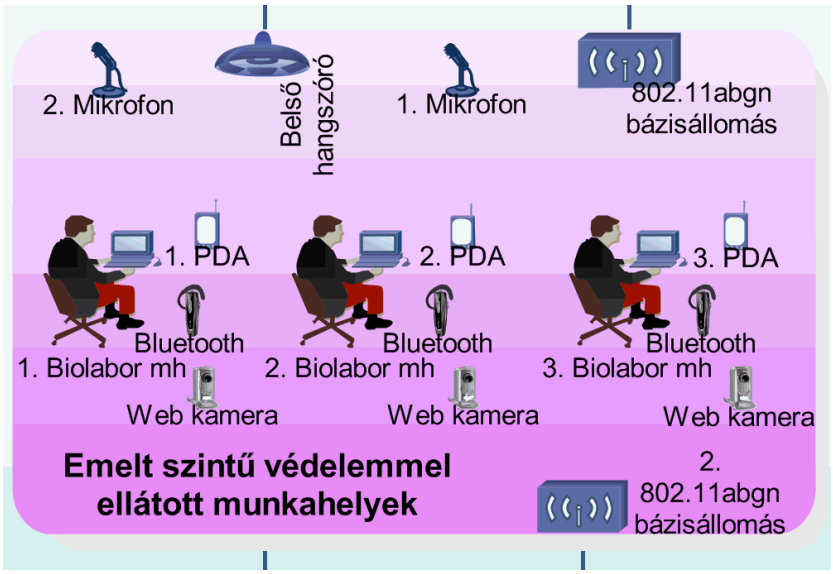
Figyelembe véve az előző fejezetben megfogalmazott ajánlásokat a Speciális feladatot végrehajtó komplexum kommunikációs illesztésének legfontosabb szempontjának a megfelelő OSI-ISO rétegkommunikációs szabványokhoz (ajánlásokhoz) való illeszthetőséget tekintettük. Mindezek alapján javaslatot tettünk az egyes elemekre.

Javaslat a kommunikációs hálózat gyakorlati kialakítására

Az emelt szintű védelemmel ellátott munkahelyek belső kommunikációja

Az alfejezetben és a minőségi követelményben leírtakat figyelembe véve a komplexum belső kommunikációját mind vezetékes, mind vezetéknélküli eszközökre és hálózatokra alapozva célszerű megtervezni. A legbelső, emelt kategóriájú

Komplex munkahely belső kommunikációja célszerűen WLAN alkalmazására kell, hogy épüljön.



2. ábra Az emelt szintű védelemmel ellátott munkahelyek belső kommunikációjának kialakítása (Változat)

A javasolt protokoll az IEEE 802.15 (Bluetooth) és az IEEE 802.11 g-n a megkívánt nagysebességű alkalmazások miatt. Összességében mind a 3 munkahelyet el kell látni Bluetooth beszélőkészlettel, mely lehetővé teszi a szabadkézi, zsinór és kábelmentes munkavégzést, magas készenléti idejével (több óra) garantálja a hosszú idejű munkavégzést illetve folyamatosan viselhető a védőfelszerelés alatt.

A munkavégzés informatikai támogatása hordozható, ütés-leesés-folyadék álló Notebookkal és PDA-val történik. A számítógép legyen alkalmas viszonylag hosszú üzemidő garantálására (5-6 óra) és rendelkezzen viszonylag rövid újratöltési idővel.

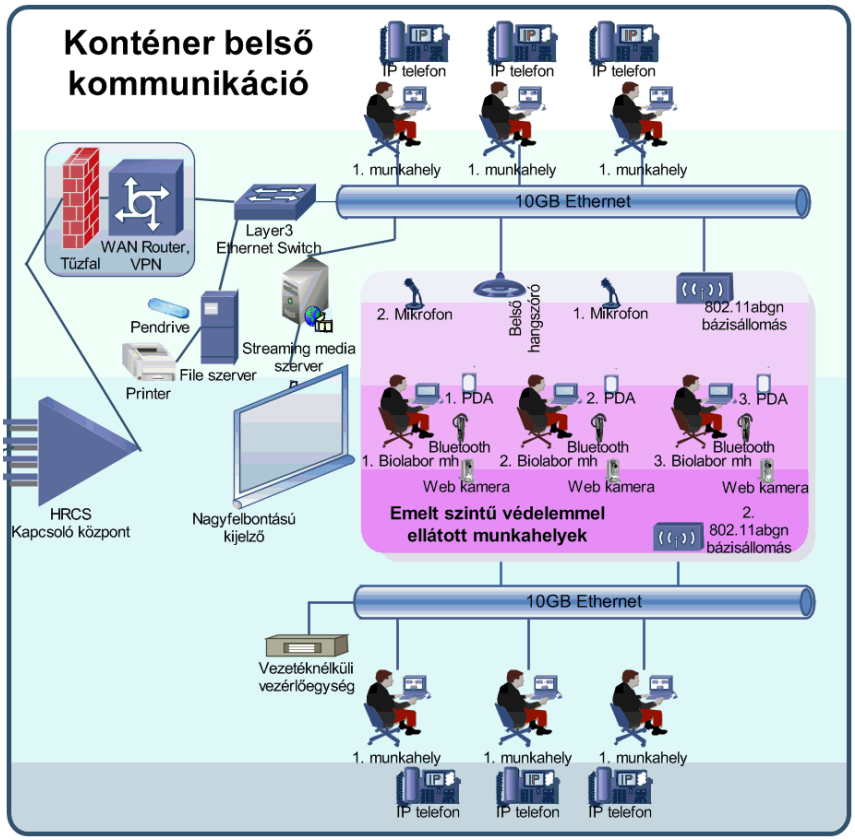
Számítási teljesítménye tegye alkalmassá a speciálisan elvégzendő feladatok támogatására. Megfontolandó különálló, speciális billentyűzet csatlakoztatása, mely a védőkesztyűben is ergonomikus használat feltételeit képes biztosítani.

Mind a hordozható PC-nek, mind a PDA-nak alkalmasnak kell lennie az IEEE 802.11 g-n szabványok támogatására, tekintettel arra, hogy a Komplex munkahely és a konténer egyéb belső munkakörnyezete között a fő kapcsolat vezetéknélküli (2 db 802.11 g-n szabványú hozzáférési pont különböző frekvencia tartományba kijelöléssel). A Notebookok rendelkezzenek jó minőségű Web kamerákkal, melyek a folyamatos mozgóképtovábbítás feltételeit támogatják.

Az operatív irányításra és esetleges veszélyhelyzeti kommunikációra szolgál az előzetesen beépített vezetékes rendszer, mely 2 mikrofonból és 1-2 hangszóróból áll. Célja a vezetéknélküli kommunikációs eszközök véletlen meghibásodása és különleges veszélyhelyzeti körülmények között a minimálisan szükséges kommunikáció biztosítása elegendően magas hangnyomású akusztikus jelekkel. Kialakításuk után legyenek egyszerűen, kevés nyomógombbal kezelhetők.

A speciális feladatokat ellátó konténer belső kommunikációja

A konténer kommunikációja igen nagy sebességű IP alapú megoldáson alapszik. Alapja egy magas hálózati teljesítménnyel rendelkező Layer3 Ethernet kapcsoló, mely képes támogatni a konténer belsejében dolgozó összes személy (9-11 fő) egymástól jelentősen eltérő profilú munkavégzését (3. ábra).

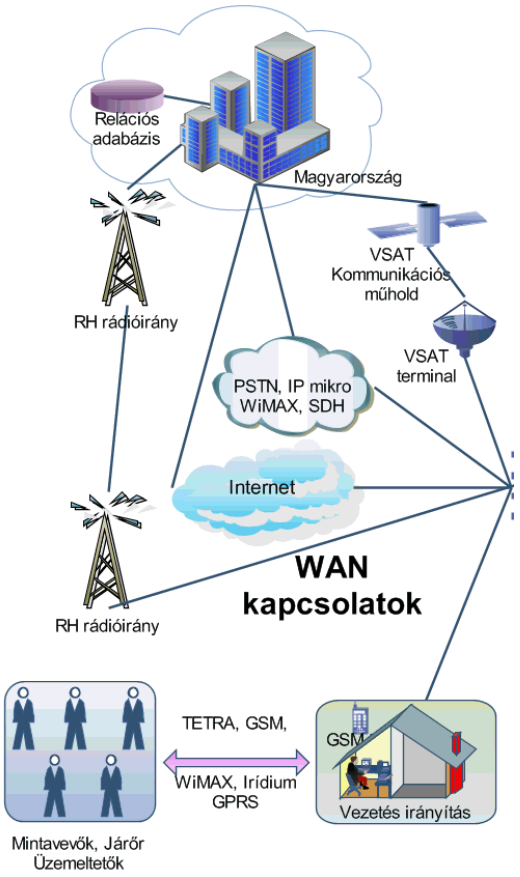


3. ábra Az emeltszintű védelemmel ellátott munkahelyek és a konténer tér kommunikációja (változat)

A munkavégzés esetenként lökésszerű és különböző kommunikációs igényeket generálhat, ezért a megszakításnélküli, folyamatos multimédiás és számítási telje-

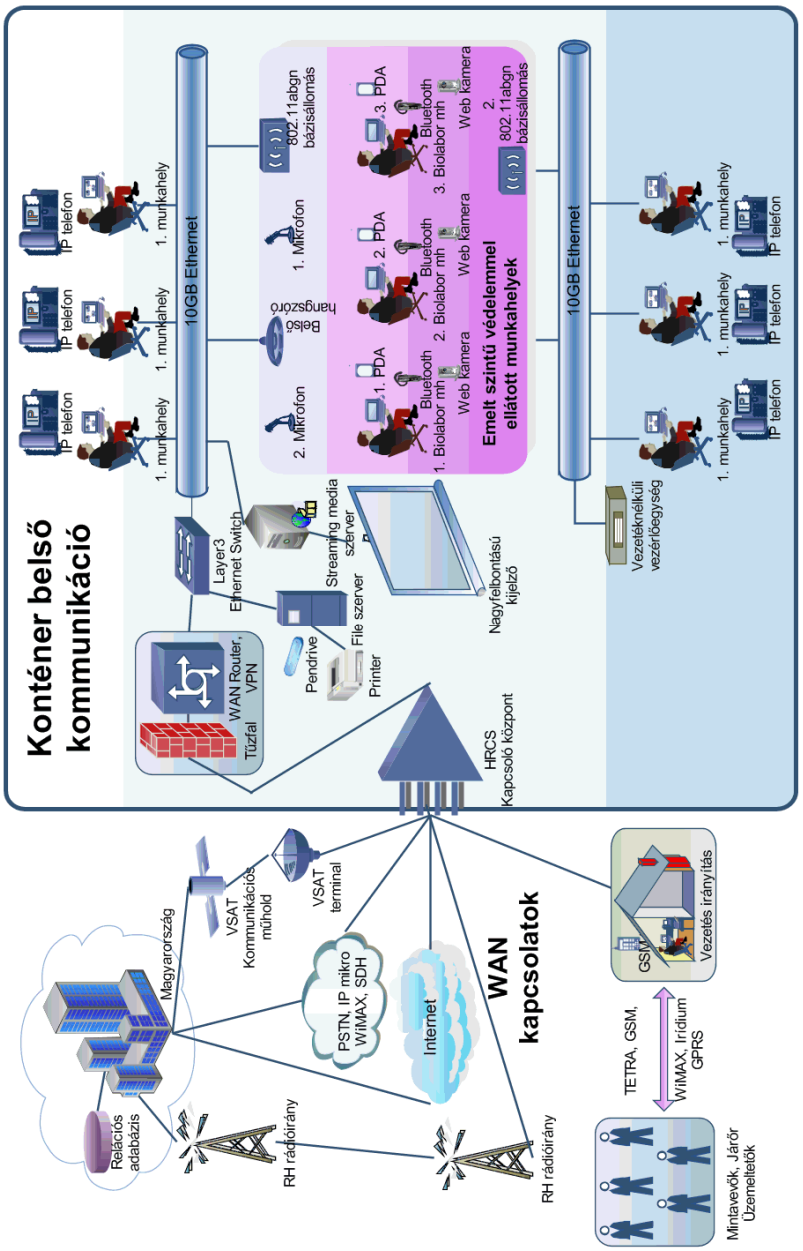
sítmény igényes alkalmazások igen nagysebességű (10GB) Ethernet kapcsolatot feltételeznek.

A konténer belsejében kialakított fizikai átviteli közegnek is támogatnia kell ezt, így optikai szálas fizikai kábel előzetes kiépítése és rögzítése javasolt célszerűen struktúrált kialakítással a konténer falában.



4. ábra Külső és WAN kapcsolatok kommunikációs irányai

A konténer belselyében nyerhetnek elhelyezést, továbbá a vezetéknélküli belső hálózatot vezérlő egység, 6 db munkahely nagyteljesítményű munkaállomásokkal, a hozzájuk kapcsolt VoIP telefonokkal, maga a Layer3 Ethernet kapcsoló, 1 Streaming media szerver nagyfelbontású és közepes-nagy méretű megjelenítővel (Display). Ebben a közös munkatérben található a speciális feladatvégzés során keletkezett adatok középtávú rögzítésére, naplózására, esetenként hordozható háttértárra archiválásra és papíralapú kinyomtatására is alkalmas File szerver.



5. ábra Az MBC System Housing helyi és a nagytávolságú hálózatok jellemző kommunikációs megoldásai (Változat)

A mindenoldalú hálózati és adatbiztonság biztosítására, a szükséges Tűzfal alkalmazások futtatására nagysebességű titkosító WAN routert célszerű alkalmazni, mely egyben kiszolgálja a komplexum kapcsoló központját titkosított információval.

Ehhez a komplexumhoz kapcsolódnak a konténer külső felületén elhelyezett csatlakozóin keresztül a különböző, nagytávolságú kommunikációs hálózatok (Internet, VSAT, Irídium, IP mikro, PSTN, WiMAX, SDH, stb.) és a célszerűen helyben telepített Vezetés-Irányítás kommunikációs vonalai, melynek egy változatát az 5. ábra mutatja.

A javaslatnak megfelelő kialakítás előnyei:

- Robusztus szolgáltatások (külső behatásokkal szembeni ellenállóképesség, túlélőképesség);
- a jelenlegi célirányos megoldásokhoz képest jelentősen nagyobb sávszélesség és adattovábbítási sebesség lehetősége;
- új jövőbeni kommunikációs szolgáltatások bevezetésének lehetősége, a belső kommunikációs rendszer architektúrájának jelentős módosítása nélkül;
- alapvetően olcsó alkalmazások a polgári szférában már bizonyított, elterjedt rendszer és technológia átvételével;
- interoperabilitás és kommunikációs átjárhatóság a nagyvárosi, vidéki és lakot településen kívüli környezet körülményei és a rendelkezésre álló köz- és zártcélú nemzeti és nemzetközi hálózatok között.

Összességében megállapítható:

A globális elérhetőség szempontjából a speciális feladatot végrehajtó komplexumnek a jelen legfontosabb polgári és az ezekkel döntő mértékben összecsengő jövőbeni kommunikációs szabványoknak és ajánlásoknak kell megfelelnie. A kommunikáció és informatika globális konvergenciájának érvényre jutása miatt a leendő a peciális feladatot végrehajtó komplexum egyik legfontosabb jellemzőjeként - a továbbítandó híranyagoktól függetlenül – biztosítania kell azok magas szintű szolgáltatásminőségét (QoS) és a kommunikáció biztonságát.

Javaslatott tettünk a speciális feladatokat ellátó komplexum emelt védelmi szitű, konténeren belüli és WAN kapcsolatainak kialakítására.

Felhasznált irodalom:

[1] Network Centric Warfare, Appendix A: Information Technology Trends and the Value-Creation Potential of Networks, pp. 249., http://dodccrp.org/NCW

[2] Kaveh Pahlavan: Trends in Wireless LANs, Second IEEE Workshop on Wireless LAN, Worchester Politechnic Institute, Worchester, MA 01609.

[3] Jim Zyren, Al Petrick: IEEE 802.11 Tutorial, pp. 1-7.

[4] Sean Convery, Darrin Miller: SAFE: Wireless LAN Security in Depth, Cisco Systems, Inc., San Jose, USA, 2001. pp. 1-48.

[5] Jim Zyren: 802.11g spec: Covering the basics, Strategic Marketing for Wireless Networking, Intersil Corp., Irvine, USA., February 2002., www.commsdesign.com/story/OEG20020201S0035

[6] Szöllősi Sándor: Konvergáló hálózatok fejlődési trendjei, a technikai alkalmazhatóság kérdései a Magyar Honvédség infokommunikációs rendszerében, doktori (Ph.D.) értekezés, Budapest, 2008.

[7] Karoly Fekete: IP solutions in the military communications and information systems, „A katonai kommunikációs rendszerek fejlődési irányai –kihívások és trendek a XXI. században”, Nemzetközi Szakmai Tudományos Konferencia, Budapest, 2001. november 28.
[8] Karoly Fekete: Personal Military Communications System, Kommunikáció 2002 Nemzeközi Szakmai Tudományos Konferencia Különkiadvány, pp. 55-62, ISBN 963 86229 2 X, 2002.
[9] Karoly Fekete: Towards a new generation of WLAN in military communications, Kommunikáció 2005 (Communications 2005) tudományos kiadvány, Budapest, 2005, ISBN 963 7060 11 1, Feltalálási hely: Országos Széchenyi Könyvtár, Zrínyi Miklós Nemzetvédelmi Egyetem Tudományos Könyvtár, pp. 334-340.
[10] Karoly Fekete: New possibilities in the field of WAN-WLAN military communications, Kommunikáció 2004 Jubilleumi Nemzeközi Szakmai Tudományos Konferencia Különkiadvány, pp. 97-10, ISBN 963 86441 5 X, 2004.
[11] Fekete Károly - Pándi Erik - Rajnai Zoltán: Az MBC System Housing terv keretében kialakítandó rendszer híradó és informatikai alrendszere (Tanulmány), Zrínyi Miklós Nemzetvédelmi Egyetem, Egyetemi Kutató Könyvtár, Budapest, pp. 107, 2008.
[12] Fekete Károly – Kerti András - Pándi Erik - Rajnai Zoltán: Infokommunikációs megoldások alkalmazhatósága egy korszerű, mobil biológiai labor esetében, (Összehasonlító tanulmány), Zrínyi Miklós Nemzetvédelmi Egyetem, Egyetemi Kutató Könyvtár, Budapest, pp. 50, 2009.

Attila BLEIER, Zoltán RAJNAI

STRUCTURAL PROBLEMS IN THE FIXED COMMUNICATION SYSTEMS OF THE HUNGARIAN ARMY

The current transport network of the Hungarian Army does not fulfill the needs of the present and future military applications. The following problems have been identified in [[NG_in_MH]] :

1. The network has been built on inhomogeneous network technologies and network elements
2. In certain cases the network resources are not being used appropriately
3. The network is not suitable for military IT applications, which require high bandwidth
4. Due to the lack of high-bandwidth link between the fixed and camp communication networks, the necessary decision support systems can not be implemented
5. The network has certain end-points that are not sufficiently connected to the fixed communication system
6. Topology of the network does not reflect the needs
7. The IP/MPLS protection mechanisms are not being used in the network, the current protection mechanisms are not sufficient for military applications
8. There are no systematic quality of service implemented in the network which results in that the current network works in best effort mode
9. Traffic Engineering is not being used on the network, which results in unequal treatment of the links being used in the network, due to SPF (shortest path first) algorithms
10. there are no relevant network level measurement of the packet network based on which the bandwidth demands of the services can be justified

The problems identified above can be put into 2 categories, structural problems (1-6) and technological problems (7-10). In this paper I would like to focus on the structural problems. In this paper I would like to highlight the roots of these problems, and I would like to give a clear view on how a new approach can help utilize present resources better.

The network has been built on inhomogeneous network technologies and network elements

As described in [[NG_in_MH]], a mixed set of technologies are being used in the Hungarian Army, with SDH, PDH, IP , Ethernet technologies all having a footprint in the network. These require a various range of network interfaces rang-

ing from the different flavors of Ethernet to E1, and other TDM interfaces. The wide set of these interfaces can not be justified by present network technologies capabilities, neither from the services nor from the operation point of view. Present services can all be migrated to an Ethernet/IP/MPLS framework, provided that the necessary set of Quality of Services rules are being held, and each service is provided with the sufficient bandwidth and Quality of Service required for military applications.

So from the services point of view, the mixed set of resources by no means justified. On the other hand the current trends show that the growth of the voice traffic is being flat, as compared to the exponential increase of data traffic. The following study shows the expected growth of traffic according to a major industry player: [TrafficGrowth2009-12], so from future network deployments point of view, the data traffic is significantly overwhelming the voice traffic, and in the current network architectural view, voice, and video are a services and applications on the common IP network.

From the operation point of the view the mixed set of resources are even less justified, since :the present network deployments require a variety of interfaces and technologies, each having their own spare parts set, technology requirements, and specialists. By utilizing a common set of interfaces (eg. Ethernet) one can achieve significant savings on:

1. spare stock by utilizing a common set of technologies/resources/interfaces
2. price/bandwidth ratio of the interfaces are significantly better (eg. Ethernet ports are more cost effective as compared to legacy TDM interfaces)
3. the wide range of technologies being used is an operational nightmare for the operations crew
4. the wide range of technologies being used require lots of specialists knowledge, which may not be present in the Hungarian Army

These facts lead to that the efficiency, and simplicity of the network provide direct cost and operations benefit – which results in that, that the overutilization of the IT/network operations crew can be significantly lowered by simplifing the network – and at the same time not using parallel networks for similar purposes.

The network resources not being used appropriately

Since the deployment of the fixed network, both technologies and user habits have significantly changed. The development of data and mobile technologies have made a huge impact on how military personnel use communications equipment. The heavy use of mobile and data technologies have made daily work more efficient both in times of peace, and in times of danger. The fixed communication network of the Hungarian Army – unlike any other NATO nation – was not able to adopt fast enough. The reason for this is often cost related. This results in the fact that military personnel use whatever civil resources (cell phones, Internet etc.) in order to fulfill their job as required by the superiors. It is not a good approach to change completely how military personnel use their networks, it is better to

harmonize the network to daily workneeds of the military personnel. If their job can be more efficiently fulfilled via data networks – they should do so, otherwise present fixed network resources will not be utilized, due to the fact that they are not able to adopt to the needs of the military workforce. So fixed communication network resources are not utilized well – for 2 reasons:

- they are not suitable enough for the job, (eg. They do not support data and mobility)
- cheap solutions are available on the consumer market, which impose a security threat

The main reason against using civil technologies are usually security related , and they have a point. Yes, security is important, it is very important – but one must realize that data network security – as of today – is a well solved subject, not only in theoretical or engineering sense, but we have seen a wide-spread deployment of IT-security equipment in both the civilian networks and military networks. Yes, they requirements are stringent, and real – but they can be fulfilled with the network portfolio from various vendors. IT-Security has become a commodity in the business world, with a wide range of civilian products available – which make it economically feasible to pay attention to the security aspects as well. These aspects must be harmonized.

Fixed communications – as of today being used in the Hungarian Army – do not support mobile applications of the workforce. This makes work inefficient in a number of scenarios, particularly in times of emergency, and danger, when mobility and quick response is crucial. This leads to the scenario that in certain cases military personnel – in fact – do not use their internal communication system – and they are not using it, with a good reason. Because there are better methods available in the civil space to solve similar tasks.

There is a third aspect to that. One must admit, that military personal have a private life also – and the Army should accept that, and support that, because such an open approach makes military life attractive for the youth. The communication between civil and military personal is inevitable, and very important, both in conflict situations and peacetimes. As of today, this view is not reflected in the military eg. For example using the communication equipment of the military to call civils is not encouraged. The point one must realize is that in most cases military personal are doing their job with whatever means of equipment they have. It is a fact, that using civil resources to solve certain tasks is a part of daily life. Of course this must be controlled both in terms of costs, efficiency and security. A more detailed analysis of this problem will be given in a further paper.

The network is not suitable for military IT applications, which require high bandwidth

The following table [táblázat 1: Bandwidth demands of the fixed communication network (all values are in Mbps)] shows the future bandwidth and Quality of services demands of the fixed communication network of the Hungarian Army:

táblázat 1: Bandwidth demands of the fixed communication network (all values are in Mbps)

	Telephely	Telephely2	Telephely3	Telephely4	Telephely5	Telephely(	Telephely
Telephely1	x	110	8000	x	x	x	
Telephely2	1500	x	x	4000	8000	x	x
Telephely3	8000	x		4000	x	x	x
Telephely4	x	4000	4000	x	8000	4000	4000

These are based on future projections – as, as of today bandwidth and quality of service demands are not being measured in the packet network. Based on such network capacity planning should one design a fail-proof networks.

The following table [táblázat 2: Quality of Service requirement patterns of the Hungarian Army]shows the Quality of Service requirement traffic patterns of the fixed communication network of the Hungarian Army:

táblázat 2: Quality of Service requirement patterns of the Hungarian Army

QoS class	Description	Percentage of the traffic
nc	Network protocol, required for operation	5%
EF	Real-time data, voice, video etc.	20%
AF	High priority data (email, internal data, military IT applications)	30%
BE	General data	45%

Historically, the fixed communication system of the Hungarian Army has been built using reliable TDM based network elements. As the demand for data networking and connectivity increased 1st generation enterprise grade network routers have been deployed in environments which require high availability and fail-proof design. At the time being this has been a good answer for the original problems, however times have changed, and next generation routing must be deployed more widespread where reliability is a factor. According to [[1]]), next-gen IP/MPLS routers have the following characteristics:

- Multiple services : support for both voice, data and video – in a point to point and point-to-multi-point fashion,
- Scalability: this has risen the top concerns, as network traffic increase, 1st generation routers tend to break down, as they have not been prepared for the amount of traffic, and services to be deployed in an environment like this. A military network is even more demanding from this aspect
- Features: migration from old generation routing platforms to new generation platforms must be smooth, therefore the platform must be flexible enough to provide services in a mixed TDM – IP/MPLS network, with a smooth transition to all Ethernet/IP/MPLS network
- Security: Security is the topmost concerns for environments that have such a stringent data security requirements as the Military sector. The security architecture is defined by: NATO standards [STANAG5066] among others , the security environment must be scalable and high availability

- IPv6: IPv4 address space is projected to be depleted in 2010-14 timeframe in Europe, so more and more network designers are calling the attention of the decision makers that moving to IPv6 is crucial for for the next generation of applications, this will happen of course smoothly, but more and more Service Providers moving to that direction
- Stability and performance : the 1st generation routing portfolio lags the reliability and high-availability design of next-generation routing platforms. The products are widely available and being used at NATO in the US, Canada, UK, France and Germany – to mention a few.
- Service and support: It has become more and more important to emphasize, that skilled workforce is required to operate such a network. This can be achieved in various forms, (this topic is not the subject of this paper.)

In terms of military requirements it can be clearly stated that the present platform is not able to support the level of reliability required. Critical Information Infrastructure Protection and Providing is a serious concern also in the EU: [CIIP2009]

In terms of capacity, the situation is even worse, as today most of the links provide nx2Mbit/s digital bandwidth. This was sufficient in the past, without data networking but clearly not sufficient at the moment. The military C4ISR applications require high-bandwidth, low-latency, high-availability network in order to support the decision making with real-time, high-accuracy data. This is crucial for the military decision makers, as information superiority result in quicker decisions, which result in decision superiority. Decision superiority has clear advantages in terms of efficiency, and this proves to be crucial in a challenging environment. (Munk Sanyi jegyzet)

As of today, it is possible to reach 100 Gbit/s in an optical fiber and it is under standardization ([IEEE8023ba], to a long distance, but even in Hungary in the Service Provider field, 10 Gbit/s deployments are widespread in the core fixed networks. Using fiber optics it is possible to provide 64-128 different wavelengths so as of today, the bandwidth capacity of fiber optics can be measured in terabits only. Using microwaves it is also possible to achieve 10 Gbit/s over short distance ([NTT-Tech-rev]), approximately 1-2 Gbit/s in a medium distance and several 100 Mbit/s over 50-100 km/s distance(reference).

Due to the lack of high-bandwidth link between the fixed and camp communication networks, the necessary decision support systems can not be implemented

One of the major problems in the military backbone is the lack of high-bandwidth communication links between the fixed and the camp communication network. The camp communication network should be one that supports deployments in the army locally within Hungary, and one that supports missions in various environments. For the former high-bandwidth microwave links are required, for the latter, as of today, the only option is using service provider offerings either based on satellites or any other means of civil architecture. I'll not cover the later here, as they are depending on the conflict region, and the local

possibilities as well, so a long term product/service strategy for this layer can not be developed.

Military decision support systems require high bandwidth , low latency and high availability. In today's TDM based infrastructure, this can not be assured, as they do not provide the necessary bandwidth, and due to the Ethernet to - TDM conversion the latency times are also high. This effects highly the usability of the decision support systems.

Camp network deployments require flexibility, and mobility as the region for the actual deployment may vary. On the access network side (camp network) wireless access technologies are the most feasible options, as they can be deployed quickly and reliable. Security concerns have to considered here.

The only realistic option for the camp and the fixed networks is using high-bandwidth wireless technologies. Ethernet based point to point microwave links are offering the highest bandwidth and the best bandwidth/price ratio, and they are the most suitable for data traffic.

Certain network end-points are not sufficiently connected to the network

The network deployment in the Hungarian Army has been done on an on-demand basis, therefore some network end-points are not connected sufficiently to the fixed network. The result of this – not evolutionary – approach is that the allocation of network resources do not reflect the actual needs. The actual needs of the Hungarian Army is to be studied further, both with respect to quality of service and bandwidth.

The not evolutionary development has resulted in a situation that certain network end-points are not allocated at the right place, and does not have the sufficient bandwidth and connectivity to the information and energy resources. This results in a situation that military personnel use other means of communication, as the technology available in the military does not fulfill their needs. This can be seen all over Europe not only in Hungary. The only real solution to this problem in the long term is to accept the use of the civilian resources, with special military characteristics. This has the effect that the state should be more involved in this as the security concerns are more realistic.

Topology of the network does not reflect the needs

One of the main concern is that energy and information is gaining higher momentum with the changing doctrines, but the present fixed network allocation is reflecting an 2nd wave military network, so the deployment is more focused on transport of material. This has the effect that stationary systems are located where access to mass transportation (eg. railroads) are provided. This is based on the assumption that :

1. Railroad is the best available transport method for transportation needs
2. Quick deployment of people is required to places where railroad is available
3. There is no road access to the areas to be defended
4. Heavy devices should be transported

Current military doctrines do not apply to these doctrines, and Hungarian military traditions do not support these ideas. Due to technological changes :

1. Railroad is not the best available transport method, as both motor vehicle, and air based transport are better suited for military crisis operations

2. Quick deployment is required not only where railroad is available, and the road and air access are much better achievable

3. In Hungary the road access is more available than the railroad access so this is not really true

4. Realistically heavy devices need to be very rarely transported, not in the situations which can be expected (eg. climate change based resource conflicts, floods, etc.)

Due to these using railroad is not the best available method for transportation but means of other transports must also be concerned. If other means of transport must also be concerned this implies that current camp access might not be located where the best infrastructure is available. In order to find the right topology and placement for the camps, we need to identify the:

1. the resources needed

2. the distribution network,

3. where the resources are available

One ideal allocation probably does not exist, the point is to focus on a problem which is there and should be solved. Both Hungarian society and military rely on

1. natural resources (material)

2. human resources

3. energy resources

4. information resources

5. money as a resource (equally)

equally. Current allocation of the camps do not reflect these, as the sufficient access to increasing energy and information resources are not available on the camps; and the most critical infrastructure to be defended is the energy and information distribution network. [[KatInfo]]

Information and energy distribution networks are both considered critical infrastructure elements according to EU Commission official communication document [EUCom2006]. Merging the resources of the energy and information network on a common platform is not only cost-efficient, reliable, but also wise, because the necessary critical infrastructure to be defended can be co-located. This has the immediate effect that response times will be better, services will be better, and there is only one network infrastructure to be defended – the one that is co-located with the energy network. The security requirements of the energy and information distribution networks should also be well understood. Recent studies

show that critical infrastructure protection will be an important development route for the near future [CIPFW-2009].

Energy distribution networks have similar characteristics to that of the Hungarian Army, both in terms of quality of service and high availability. This implies that ideally camps should be placed in cities with good access to energy and information resources and energy and information distribution network topology should be based on the same infrastructure. This is aligned with both EU and NATO requirements [EUCom2006],[2]. Further study of these problems are too broad and out of the scope of this paper.

Summary

In this paper the authors pointed out that the fixed communication network of the Hungarian Army has numerous problems, which imply that the technology being used for building out the network is outdated. Current civilian network technology development in IP/MPLS technology have reached a state which show that high-availability, stable and future-proof networking technology is available at an affordable cost. This paper points out the problems and the direction of the development of the IP networks used in the Hungarian Army.

Bibliography

[NG_in_MH]: Bleier Attila, Uj generációs hálózati megoldások alkalmazása a Magyar Honvédség stacioner hálózatának modernizációjában, 2009
[TrafficGrowth2009-12] ,http://www.mm-online.hu/cikk/Elerkezik_a_zettabajt_korszaka,2009.06.24
[[1]] ,http://voicendata.ciol.com/content/goldbook/goldbook05/105030506.asp ,2009.02.28
[STANAG5066] ,http://whitepapers.zdnet.com/abstract.aspx?docid=396371,2009.06.23
[CIIP2009] ,http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm,2009.06.23
[IEEE8023ba] ,http://www.ieee802.org/3/hssg/index.html,2009.06.24
[NTT-Tech-rev] ,https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr200903sf2.html,2009.06.23
[KatInfo]: Dr. Munk Sándor, Katonai informatika a XXI század elején, 2007
EUCom2006: , ,
[CIPFW-2009]: Manuel Suter, A generic national framework for critical information infrastructure protection , 2007
[EUCom2006] ,http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf,2009.06.24
[2]: Précsényi Zoltán, Solymosi József, TOWARDS EU-NATO COOPERATION IN THEPROTECTION OF EUROPEAN CRITICAL INFRASTRUCTURE, 2007

Attila SEBESTYÉN

WOULD IT BE POSSIBLE TO DECREASE THE DATA SECURITY RISKS RELATED TO SUPERUSERS?

„Never lose sight of the human factor, when it comes to machines"

In my thesis I wish to deal with superusers (including administrators, roots, supervisors, sysadmins, dbadmins, etc.) who, nevertheless having irreplaceable roles in certain systems, possess unlimited „power". Despite all that they still cannot be called a risk factor not even from data security point of view; nor does literature deal with defining standalone security rules influencing their work or activities.

On one hand it is understandable as it is impossible to imagine their "unlimited power" in the system in lack of trust lain in their expertise, loyalty and honesty, but on the other hand owing to their special – exceptional – knowledge it is hard for an "outsider" to determine what and how to keep under control concerning their activities, and how their professional supervision can be established.

Along such thoughts of mine the question is reasonably put: - Is it really an important issue? Is it justified to "detain" the activities of the superusers with "superfluous" administrative and other "artificial" rules? The answer can be given the easiest way by statistics. Three quarters of the successful abuses are committed by the employees.[90]

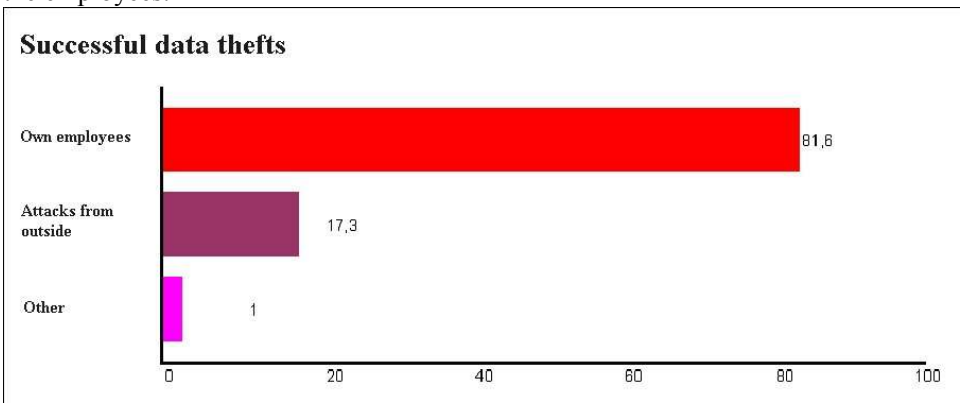


Fig 1.

The "employees" category includes also those who recently left the company and intended to take revenge for a real or alleged injury.

So I do find it necessary to evaluate superusers as risk factors. This intention is flanked by the fact that the IT security policy[91], the IT security rules[92], or the data

[90] Visnyei Aladár – Dr. Vörös Gábor: a számítógépes információ biztonság alapjai – LSI Oktatóközpont – ISBN 963 577 128 2

[91] http://www.bm.hu/proba/bmtvtev.nsf/e59c75bcdbbc3613c1256835004755d5/3b0a71a8b6e30855c1256eed004abee9?OpenDocument&High light =0,informatika* - a Belügyminisztérium Informatikai Biztonsági Politikájának kiadásáról szóló 12/2004. (B.K. 12) BM utasítás

[92] A Határőrség Informatikai Biztonsági Szabályzata – kiadás előtti koordinációs példány

security action system based on it[93], typically elaborates on norms regarding users which analogously go for superusers as well, and which, rising from the role they play in operating the system, may not be satisfactory.

It is not an objective for my thesis to introduce the entire spectrum of IT security, so I only wish to touch upon again the fact that general norms naturally refer to the activities of the superusers, like:

1. as regards basic principles:
   a. credibility
   b. confidence
   c. integrity
   d. disposability and being operational
2. as regards protection measures – rules related to:
   e. the organization
   f. the infrastructure
   g. the devices (hardware)
   h. the applications (software)
   i. documentation
   j. data
   k. data bearers
   l. communications
   m. persons
   n. rules of action.

The literature indicates the human motives on data security as 7-E which abbreviates the English words for them, being[94]

- ego
- embezzlement
- eavesdropping
- enmity
- espionage
- extortion
- error

As human factors one of these or any of these may affect superusers. Let us now put aside the evaluation of the criminal cases, as from the point of view of the recommended solutions it is irrelevant which cause leads to breach or attempted breach of data security; let us instead look more deeply into the categories of ego and error.

Superusers are in an "exceptional" situation from the point of view of the operation and maintenance of the system, as they may take decisions in questions of "existence" or "non-existence", exercise their favor in supporting a user, so a part or the whole of data processing may fall a victim to their personality or deviance.

[93] A Határőrség Adatvédelmi Szabályzatának kiadásáról szóló 47/2001. számú Országos Parancsnoki parancs

[94] http://www.cryptox.hu/crypto02.php - Virasztó Tamás: titkosítás és adatrejtés – NetAcadémia oktatóközpont

The same may occur in case the expertise or the experience of the applicant is not sufficient. The third pillar of this problem is irreplaceability rising from their being "exceptional", meaning a kind of special knowledge piling up in the superusers (and then its storage without sharing it with anyone) that endangers replaceability, so in case they are permanently away the operation of the system is endangered. In all three cases the features of the personality enhances or generates the risks of operation, so the activities of superusers should be established in a way that these factors are minimized in the life-cycle of the system.

What methods are recommended by the literature in order to lower risks (and also standing ground with respect to superusers)?

Separation of jobs[95]:

There exist certain jobs that mutually disqualify one another due to their task system. The developer cannot be the operator – developing cannot be done in a system that is operating. The one who assesses the efficiency of the development may not be employed by the developing company. The security officer may not be the employee of the IT organization, etc. Inconsistent jobs should be indicated in the security rules, and care must be taken that no temporary connection between such jobs could be made even during substitution.

Rotation of jobs:

By this method the persons working in certain positions are rotated after some time (if the period is at random then the efficiency is greater), in our case the job of system administration is replaced. In my opinion the replacement should be made no later than every 1 or 1.5 years.

There are more than one advantages offered by this method. Superusers gain appropriate knowledge about the entire IT system. Using replacement their irreplaceability will cease to exist. Control is made easier by the fact that more than one person may yield sufficient formal and informal data on the system and the condition of the system. The commonly shared "topic" furthermore provides for an innovative opportunity, a competition for gaining professional appreciation. The level of being trouble proof increases as more than one highly qualified expert is involved in the system.

Principle of obligatory freedom:

The unexpected and longer (at minimum 10 workdays) period of "removal" of the superuser from the system results in forced information sharing and counterbalances the gaining of exclusive knowledge by putting the substitute "in the picture".

Documentation:

Documentation is a security system on more than one pillar. First of all, all subsystems are to have a three-level documentation at minimum (technical description or system plan, users guide, administrators booklet or guide). Secondly, a normative rule, operation regulation or order describing the system of tasks and positions

[95] Kő Andrea: információrendszerek auditálása – Budapesti Közgazdaságtudományi- és Államigazgatási Egyetem, Információrendszerek Tanszék – 2003. (címszavak a 15. oldalról)

concerning system operation and maintenance as well as the system of rights and obligations connected to them. Thirdly, the notes or vade-mecum on operation experience and practices (operator logbooks, debugging registers, logs, service books, other work documents), which are to be regularly incorporated into the above mentioned two documents.

Access and rights control:

I do not consider it as an independent security element, as it is part of security policy and the security regulation. As a matter of fact they are to be described in the operation regulation on certain subsystems as lists connected to the systems. The list, referring to certain subsystems, should at minimum contain the identification data of the user, the beginning and expiry date of access, the modular and data access levels within the application. The superuser should apply in the system the rights fixed in these sources both at infrastructure and at application system levels.

The criterion of the principle is securing the needful and sufficient access. The (super)users may be rendered access to the given subsystem only to an extent that is sufficient for them to entirely execute their tasks rising from their jobs. This includes that the Oracle sysadmin does not necessarily require possessing superuser rights for the operating system level working under the Oracle; what is more, the principle of separating jobs even prevents that.

Policy of the empty desktop:

This principle both literally and figuratively comprises the expectation that only those paper documents or opened documents or applications should be left on the "desktop" that are linked to the tasks currently being done. When leaving the office care must be taken so that unauthorized access must be avoided by locking away all paper documents, data bearers in a secure way, and all tasks and sessions must be locked on our computer. Superusers must be required not to leave unattended either any data, computers or terminals.

Disposal of waste:

Irrespective of the material of the data bearer, the disposal of unused data must be ensured. It is not enough to consider using the recycle bin or quick formatting as sufficient form of condemnation. In accordance with the classification of the stored data the regulation must specify the method of condemnation of certain data types and data bearers from chip crushers through burning as far as the "acetic scissors". The work morale of superusers is to be developed from identifying waste to condemning it in accordance with the rules.

Beyond my exploring sources, based upon my 23 years of experience with computers I recommend to amend those above with the following methods:

The necessary extent:

Superuser rights are an instrument of labor rather than a privilege. An instrument to which special tasks are assigned along the life-cycle of the system, such as the installation of a hardware or software element, creation of users, creation, assignment or deletion of user rights, etc. However, it also includes that if the superuser has a job which does not require possessing this sort of privileged right then they should have a "simple" user right or advanced user right to access the system.

The superusers are to be made aware that because the accessing IDs or acting on behalf of other users (e.g. in case of a virus) may utilize the privileges that the accessed rights ensure. There should be a level of access rights assigned to tasks that is necessary but also sufficient to accomplish them.

Log and monitoring system:

The logging at system and application level is an essential condition for the maintenance activities and an accessory in the system of instruments for data security and data protection. We must be aware that logging is not a preventive action rather a follow-up instrument, yet a primary source for monitoring the tendencies of the activities of the system or the users, as well as for monitoring errors and unauthorized access.

In case of logs the superuser access rights must be set to read-only. It may be realized by having the log file created at a central storage area with access only by the local default superuser, and by granting that no further services are run on this device that may be linked to any levels of other user activities.

Superuser personification:

The use of superuser impersonators must be consistently banned in the system. It means that the tasks that require superuser privileges should be carried out with user access rights that are not identified by a superuser name – in systems where it is possible – and which distinctly identify the user of the privilege. I.e. the superuser should work using administrator as user name but e.g. Attila Sebestyén, to which superuser privileges may be assigned. It is necessary that there should be no more than 2 users with superuser privileges in a certain subsystem. In case an unexpected occurrence should require some action and if the acting user has no superuser rights then it must be made possible for them to log in using the default superuser login. This should happen in a preliminarily established regime, for example with the codes locked away at the operator service (in separate envelopes or keycases for each system) and using a password registry. After the application, the range of users with superuser rights should be checked and the password for the default admin user should be changed.

The logging and monitoring of superusers makes sense only in case of private user names.

One-man supervision:

The activities of the superusers are to be supervised by the leader of the organ assigned with operation and maintenance. Besides daily tasking, coordination, checking it also includes supervising the privileges of the default superuser, the password changes, and the maintenance of logbooks. It is a basic principle that along their other activities the leader should use their own user name and password whose privileges should comply with the activities they do.

With my thesis I do not intend to evoke distrust in superusers and particularly not to grade persons doing activities of that sort. I simply wish to draw the attention to the fact that superuser privilege is an instrument of labor and as such, certain requisites and norms must be applied for its beneficiaries as well. According to my experience the norms created for IT systems are supposed to hold the user activities “on a short leash”, yet from the aspect of IT security the superuser is just

another user of the system even though in the possession of some privileged access.

In the framework of normative regulations I find it reasonable to further describe the application system of superuser rights as well.

Bibliography:

[1] Visnyei Aladár – Dr. Vörös Gábor: a számítógépes információ biztonság alapjai – LSI Oktatóközpont – ISBN 963 577 128 2

[2] http://www.bm.hu/proba/bmtvtev.nsf/e59c75bcdbbc3613c1256835004755d5/3b0a71a8b6e 30855c1256eed004abee9?OpenDocument&High light =0,informatika* - a Belügyminisztérium Informatikai Biztonsági Politikájának kiadásáról szóló 12/2004. (B.K. 12) BM utasítás

[3] A Határőrség Informatikai Biztonsági Szabályzata – kiadás előtti koordinációs példány

[4] A Határőrség Adatvédelmi Szabályzatának kiadásáról szóló 47/2001. számú Országos Parancsnoki parancs

[5] http://www.cryptox.hu/crypto02.php - Virasztó Tamás: titkosítás és adatrejtés – NetAcadémia oktatóközpont

[6] Kő Andrea: információrendszerek auditálása – Budapesti Közgazdaságtudományi- és Államigazgatási Egyetem, Információrendszerek Tanszék – 2003.

[7] Pándi Erik: A rendőrségi információtechnológiai szervezet fejlesztésének néhány kérdése, Hadmérnök, III. évf. 3. szám, Budapest, ISSN 1788-1919, pp 154-168., 2008.;

[8] Pándi, Erik: Modernisation process of public administration services, „Communications 2007" international scientific conference, Zrínyi Miklós National Defence University, Budapest, ISBN 978-963-7060-31-1, pp. 90-97., 16.10.2007.

SEBESTYÉN Attila

BÜNTETÉS VÉGREHAJTÁS INFORMATIKAI FEJLESZTÉSI PROJEKT

EKOP-1.1.6

A fejlesztési feladat behatárolása

A feladat összefoglalása

A büntetés-végrehajtási szervezet az 1990-es években egységes, homogén rendszertechnológiára alapuló számítástechnikai rendszert hozott létre, amely a fogvatartottak nyilvántartásával, ellátásával, reszocializációjával kapcsolatos, a törvény által előírt valamennyi nyilvántartási kötelezettséget és az ehhez illeszkedő adminisztratív tevékenységek támogatását biztosította. A célalkalmazás rendszer az akkor korszerűnek számító eszköz-, adatkapcsolati- és operációs rendszerkörnyezetre épült és műholdas táv-adatátviteli összeköttetéssel biztosította egy országos hatáskörben működő programrendszer kiteljesedését.

Az elmúlt másfél évtizedben a célalkalmazás által biztosított nyilvántartási lehetőségek, munkamódszerek a napi feladatvégzés rutinjává váltak, a fogvatartotti rendszer gyökeresen betagozódott az informatikai alapinfrastruktúrába.

A büntetés-végrehajtási szervezet az egyre romló költségvetési- és gazdasági környezeti lehetőségek között érdemben nem tudta megújítani a célalkalmazás rendszert, a sorozatos szervezeti átalakítások következményeként fluktuálódott a rendszer bevezetésében és kiterjesztésében részt vett szakterületi- és informatikai állomány.

Az informatikai költségvetési források felhasználásában egyre meghatározóbbá vált a fogvatartotti rendszer üzemeltetési- és fenntartási tevékenységéhez szorosan köthető források biztosítása, fajlagosan egyre drágult a célalkalmazás rendszer folyamatos működési képességének megőrzése.

Napjainkra a fogvatartotti rendszer minden elemében (eszköz, operációs rendszer környezet, adatbázis kezelés, adatátviteli és on-line adatszolgáltatási képességek, munkafolyamat szervezés és döntéstámogatási képesség stb.) elavult, az egyes rendszerelemek gyártói támogatásának megszűnte következtében rendszertechnológiai „zsákutcává" vált. A fogvatartotti rendszer folyamatos korszerűsítése, az informatikai alapinfrastruktúra következetes megújítása elmaradt az elmúlt évtizedben, így mind az eszköz-, mind az alkalmazás környezetben kialakult az úgynevezett „amortizációs csapda helyzet", amikor is olyan mértékben kell az alapinfrastruktúra- és rendszertechnológiai változtatásokat végrehajtani, amelyre a saját költségvetési forrás már nem elégséges.

Jelenleg a büntetés-végrehajtási szervezetben működő informatikai rendszer az alábbi jellemző tulajdonságokkal működik:

- A fogvatartotti rendszer elavult eszközparkon, korszerűtlen alkalmazás technológián alapul (UnixWare és Recital rendszerkörnyezet; P-I kategóriás vagy korábbi számítógépek és unix terminálok; karakteres, vastag kliens architektúrára alapuló felhasználói alkalmazás felület), közel 400 me-

nüpontban több mint 750 funkció valósul meg, az alkalmazás mérete több százezer kódsor

- A fogvatartotti rendszer és a vele egy időben megvalósított egyéb célalkalmazások (fogvatartottak egészségügyi ellátása, saját állomány személyügyi alapnyilvántartása) korszerűtlen, funkcionalitásában, jogszabálykövetésében idővel elmaradt a jelentkező igényektől
- A fogvatartotti rendszer adatkezelése intézeti szinten elosztott, így országos szinten történő adatgyűjtési, -keresési, -összesítési, statisztikai képesség kizárólag az országos parancsnokságon összesített adatbázisból lehetséges, illetve a fogvatartott intézeti elhelyezésének változásából következő adatmozgatás körülményesen és nem teljes körűen biztosítható
- A fogvatartotti rendszer egészségügyi modulja a minimális nyilvántartási és jelentési kötelezettségeket teljesíti, nem alkalmas a járó- és fekvő beteg ellátás, kórházi betegirányítással kapcsolatos támogatói feladatok ellátására. Az egészségügyi alrendszer jelenleg alkalmatlan a házi orvosi szolgálat alrendszerével együttműködni.
- A személyügyi rendszer elavult rendszertechnológián, elégtelen adatkezelési képességekkel működik, funkcionalitásából teljes egészében hiányoznak releváns nyilvántartási kötelezettségek (állománytábla alapú személyi állomány kezelés, szolgálatszervezési, pótlékszámítási képesség, együttműködés a bérszámfejtő alkalmazással, személyi állomány fizikai- és pszichológiai állapot nyilvántartása, fegyelmi helyzet alapnyilvántartásai)
- 32 intézetből 27-ben nem elégséges, vagy hiányzik a 100Mbit/sec strukturált kábelhálózat (a helyi hálózat alkalmatlan az integrált hang-adatátvitelre, a hálózati aktív eszközök zömében elavultak, hiányzik a hálózati szegmentálás-, távfelügyelet- és távmenedzselhetőség képessége, nem biztosíthatóak hálózat biztonsági rendszabályok)
- a harmadik amortizációs életcikluson túl működő eszközök rendelkezésre állása, biztonságos működése, informatikai biztonsági kritériumoknak való megfelelése alacsony, esetenként minősíthetetlen, jelenleg alkalmatlan új rendszertechnológiai megoldások bevezetésére (grafikus felhasználói felület; böngésző alapú vagy virtuális, vékony kliens architektúra alkalmazása; szünetmentesítés és szükségáramforrás ellátottság; idegen gép csatlakozási védelem stb.).

Az Elektronikus Közigazgatás Operatív Program 2009-2010. évi akciótervében nevesített, a „Felelősen, felkészülten a büntetés-végrehajtási szervezetfejlesztési program" részeként megvalósításra tervezett informatikai rendszerfejlesztés (4. „Konszolidáció" program, 4. Informatikai rendszer fejlesztése, korszerűsítése – EKOP 1.1.6) lehetőséget biztosít a büntetés-végrehajtási szervezetének az informatikai rendszer korszerűsítésére, a törvényben meghatározott szolgálati feladatok maradéktalan és hatékony ellátását biztosító célalkalmazások fejlesztésére.

A fejlesztés során meghatározó szerepet tölt be a fogvatartotti rendszer korszerűsítése, új rendszertechnológiai alapokra helyezése, funkcionális bővítése, illetve a társszervekkel, együttműködőkkel való on-line adatszolgáltatási képesség kialakítása. A célalkalmazás fejlesztés a több életcikluson túl amortizálódott eszközpar-

kon, alacsony hatásfokkal működő helyi hálózati környezetben nem valósítható meg eredményesen, így a fogvatartotti rendszer megújítása az informatikai környezet gyökeres megváltoztatását is feltételezi. (A célalkalmazás tervezett új rendszertechnológiai megoldásai nem alkalmazhatóak a jelenlegi eszközparkon, és operációs rendszerkörnyezetben; viszont a régi célalkalmazás és rendszerkörnyezete sem működtethető a megújított eszközparkon. Az egymásra utaltság következményeként mind az informatikai környezet, mind a célalkalmazás rendszer cseréje szükséges).

Az új informatikai rendszerkörnyezet kialakítása további előnyöket hordoz magában, amelyek túlmutatnak a fogvatartotti rendszer működésén. A fejlesztés első lépcsőjében megteremtődnek az egységes és homogén informatikai rendszer alapjai. Olyan az informatikai működés szempontjából releváns szolgáltatások vezethetőek be, amelyek nem csak az informatikai szolgáltatások minőségét, hanem az informatikai biztonság alapjait is megteremtik.

Új szolgáltatások:

- teljes körű infrastruktúra az integrált hang és adatátviteli szolgáltatásokhoz
- egységes és szabványos iroda-automatizálási környezet
- általános Intranet szolgáltatási képesség szerver és munkaállomás oldalon
- a további fejlesztésekhez szükséges szabványos, rugalmas és skálázható, megoldás szállító független környezet kialakítása
- szerepkör alapú informatikai továbbképzések rendszere (minimálisan felhasználói és rendszergazdai, üzemeltetői és fenntartói szerepkörök)
- dokumentált, a nemzetközi szabványoknak és ajánlásoknak megfelelő alrendszerek (fejlesztői-, teszt-, oktatói- és „éles”, környezet érzékeny online segítségnyújtás – „help” rendszer)
- „tudás megosztáson” alapuló, „egy kapus” informatikai működés, a szakirányítói és szakfelügyeleti tevékenységek erősödése
- vezető tájékoztató, döntés támogató és statisztikai képességek javítása
- szabványos és dokumentált adatcsere képességek kialakítása
- központi címtárak használata (személyi, szervezeti, hálózati működéshez kötődő)
- megújult, korszerű az informatikai környezethez illeszkedő, hatékony célalkalmazások megjelenése (fogvatartotti-, személyügyi alkalmazás)

Informatikai biztonsági kritériumok:

- magas fokú rendelkezésre állás és hibatűrő képesség
- szerepkör alapú differenciált hozzáférés szabályozás
- az adatkezeléshez kötődő tevékenység naplózás
- szabályozott adatkapcsolati rendszer (együttműködési megállapodás, szerződés szintjén)
- illetéktelen behatolás-, szándékos támadás-, programozott károkozás- és idegen gép csatlakoztatás elleni védelmi megoldások kiterjesztése
- távmenedzselhetőség-, távfelügyelet- és távoli segítségnyújtás képességének kialakítása

- reagáló képesség és a helyreállíthatóság körülményeinek javítása (szerver és virtuális környezet, vékony kliens architektúra)
- a hitelesség, a bizalmasság, a sértetlenség, az elérhetőség, a visszaállíthatóság, a bizonyítékbiztosítás és a nyomon követhetőség kritérium rendszer kialakítása az informatikai rendszerszolgáltatásban

A fejlesztést indokoló jogszabályi környezet

- 1995. évi CVII. törvény a büntetés-végrehajtási szervezetről;
- 1996. évi XLIII. törvény a fegyveres szervek hivatásos állományú tagjainak szolgálati viszonyáról
- 1992. évi XXXIII. törvény a közalkalmazottak jogállásáról
- 2006. évi LV. törvény a Magyar Köztársaság minisztériumainak felsorolásáról
- 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról
- 2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól
- 1997. évi CLIV. törvény az egészségügyről
- 1997. évi LXXX. törvény a társadalombiztosítás ellátásaira és a magánnyugdíjra jogosultakról, valamint e szolgáltatások fedezetéről
- 217/1997. (XII. 1.) Korm. rendelet a kötelező egészségbiztosítás ellátásairól szóló 1997. évi LXXXIII. törvény végrehajtásáról
- 9/1993. (IV. 2.) NM rendelet az egészségügyi szakellátás társadalombiztosítási finanszírozásának egyes kérdéseiről
- 43/1999. (III. 3.) Korm. rendelet az egészségügyi szolgáltatások Egészségbiztosítási Alapból történő finanszírozásának részletes szabályairól
- 60/2003. (X. 20.) ESzCsM rendelet az egészségügyi szolgáltatások nyújtásához szükséges szakmai minimum feltételekről
- 1979. évi 11. törvényerejű rendelet a büntetések és az intézkedések végrehajtásáról
- 6/1996. (VII.12.) IM rendelet a szabadságvesztés és az előzetes letartóztatás végrehajtásának szabályairól
- 11/1996. (X.15.) IM rendelet a büntetés-végrehajtási intézetekben fogvatartottak fegyelmi felelősségéről
- 17/1997. (V.9.) IM rendelet a szabadságvesztés kezdő és utolsó napjának megállapításáról
- 5/1998. (III. 6.) IM rendelet a fogvatartottak egészségügyi ellátásáról;
- 50/1998. (III. 27.) Korm. rendelet a zártcélú távközlő hálózatokról;
- 84/2007. (IV. 25.) Korm. rendelet a Központi Elektronikus Szolgáltató Rendszer és a kapcsolódó rendszerek biztonsági követelményeiről.
- 33/1999. (BK.22.) BM utasítás a személyes adatok belügyi igazgatási területen való kezelésének és védelmének egyes szabályairól
- 15/1998. (BK.11.) BM utasítás az emberi erőforrás gazdálkodást támogató információs rendszer alkalmazásáról

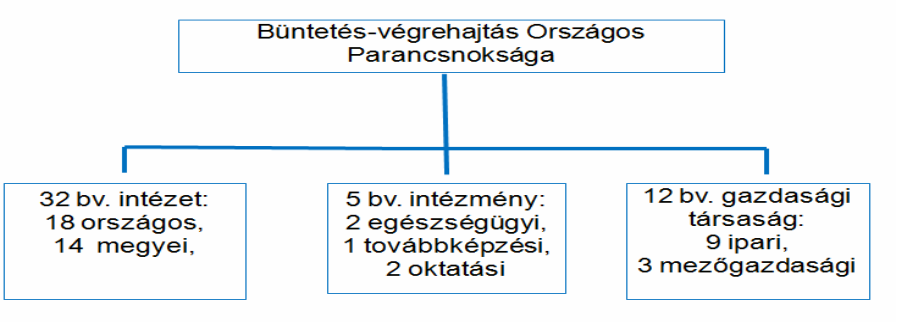
- 53/2007. (XII.7.) EüM rendelet a gyógyszerrendeléshez használandó számítógépes program minősítésének szabályairól
- 50/1999. (XI. 3.) EüM rendelet a képernyő előtti munkavégzés minimális egészségügyi és biztonsági követelményeiről

Egyes az adó-, járulék- és egyéb közteherviseléssel, a büntetés-végrehajtás működésével, a fogvatartással, az egészségügyi ellátással és a humán erőforrás gazdálkodás szabályaival kapcsolatos jogszabályok, amelyek az érintett célalkalmazás fejlesztés működése szempontjából releváns.

Részben elérhetőek a büntetés-végrehajtási jogszabályok jegyzéke, belső normák alapján:

- (http://www.bvop.hu/download/jogszabalyok_200811ho.doc/jogszabalyok_200811ho.doc;
- http://bvop.hu/hopi/full.html)

A működtető szervezet struktúrája



A Büntetés-végrehajtási Szervezet

A büntetés-végrehajtási szervezet a külön törvényben meghatározott szabadságelvonással járó büntetéseket, intézkedéseket, büntetőeljárási kényszerintézkedéseket, a szabálysértés miatt kiszabott pénzbírság átváltoztatása folytán megállapított elzárást, továbbá – törvény által megállapított körben – fegyveres rendészeti szerv. A büntetés-végrehajtási szervezet a feladatainak törvényes ellátásával járul hozzá a közrend és a közbiztonság erősítéséhez.

Büntetés és intézkedés csak a bíróság jogerős határozata alapján, jogszabályban meghatározott módon hajtható végre. Az elítélttel szemben csak az ítéletben és a törvényben meghatározott joghátrányok alkalmazhatók. A szabadságvesztés végrehajtásának célja, hogy az e törvényben meghatározott joghátrány érvényesítése során elősegítse az elítéltnek a szabadulása után a társadalomba történő beilleszkedését, és azt, hogy tartózkodjék újabb bűncselekmény elkövetésétől.

A szabadságvesztést a büntetés-végrehajtási szervezet hajtja végre. A büntetés-végrehajtási feladatok teljesítésében – a jogszabályban meghatározottak szerint – az állami szervek közreműködnek. A büntetés-végrehajtási szervezet a büntetés-végrehajtási feladatainak segítése érdekében más, nem állami szervezetekkel és magánszemélyekkel együttműködik.

A Büntetés-végrehajtás Országos Parancsnoksága (BVOP)

A büntetés-végrehajtási szervezet részére feladatot törvény határozhat meg. A büntetés-végrehajtási szervezet működését a Kormány az igazságügyi és rendészeti

miniszter útján irányítja. A büntetés-végrehajtási szervezet központi vezető szerve a Büntetés-végrehajtás Országos Parancsnoksága, élén a büntetés-végrehajtás országos parancsnokával. Az országos parancsnok a jogszabályok, az állami irányítás egyéb jogi eszközei, és az igazságügy-miniszter törvényben meghatározott jogkörében hozott döntéseinek keretei között vezeti a büntetés-végrehajtási szervezetet. Az országos parancsnok a büntetés-végrehajtási szervezet személyi állományának szolgálati elöljárója, illetve felettese. Az országos parancsnok törvény, illetve az igazságügyi és rendészeti miniszter eltérő rendelkezése hiányában képviseli a büntetés-végrehajtási szervezetet.

A büntetések és az intézkedések végrehajtása felett az ügyészség – külön törvényben meghatározottak szerint – törvényességi felügyeletet gyakorol.

A BVOP központi költségvetési szerv, amely éves költségvetés alapján gazdálkodik, az Igazságügyi és Rendészeti Minisztérium költségvetési fejezetén belül önálló címként (büntetés-végrehajtási szervezet) szerepel. A szervezet az elmúlt évtizedben folyamatosan alulfinanszírozott volt. Ezt a helyzetet a 2009. évi költségvetési megszorítások csak tovább nehezítették.

BVOP szakfeladatai között kiemelt jelentőséggel bír a fogvatartottak nyilvántartási rendszerének működtetése, fejlesztése, és adatok szolgáltatása a szervezeten belül illetve a társszervek felé (a büntetés-végrehajtási szervezetről szóló 1995. évi CVII. törvény, 29.§. (1) bekezdés), mint a bíróságok, ügyészségek, önkormányzatok, Rendőrség, KEKKH, OITH, OEP, ÁNTSZ stb.

A releváns folyamatok

Az informatikai rendszer korszerűsítésének kiemelt feladatai

1. A fogvatartotti rendszer korszerűsítése, újraírása, funkcionális bővítése (letétkezelő-, élelmezési-, foglalkoztatási-, fényképkezelő-, egészségügyi járó- és fekvőbeteg ellátó-, on-line lekérdező-, vezető-irányító és statisztikai alrendszerek)

2. A személyi állomány személyügyi nyilvántartásával kapcsolatos alkalmazás fejlesztése, korszerűsítése, funkcionális bővítése (személyügyi-, fegyelmi-, egészségügyi ellátásokat, egészségi, pszichikai alkalmasság és fizikai állapot felmérést nyilvántartó-, szolgálatszervezési alrendszer)

3. A büntetés-végrehajtás intézetek/intézmények helyi hálózatának (LAN) korszerűsítése, strukturált kábelhálózatok kialakítása (integrált hang-, adatátviteli infrastruktúra megteremtése)

4. Az intézetek szervereinek lecserélése és egységes, egyenszilárd intézeti hálózati operációs rendszer-struktúra létrehozása, integrálása, távfelügyeleti- és központi címtár szolgáltatások bevezetése

5. Intézeti munkaállomások, terminálok korszerűsítése (a karakteres UNIX terminálok cseréje)

6. Felhasználó barát üzemeltetési környezet kialakítása, rendelkezésre állás és hibatűrő képesség javítása, iroda-automatizálási funkcionalitás általánossá tétele

7. intézeti nyomtatók konszolidációja

A büntetés-végrehajtási szervezet az 1990-es évek végén az akkor korszerűnek számító SCO Unix platform alatt Recital adatbázis kezelőre építve országos hálózatban működő, a fogvatartottak ellátásával kapcsolatos valamennyi munkafolyamatot átölelő alkalmazásrendszert állított üzembe, illetve az elmúlt több mint tíz évben folyamatosan naprakészen tartott.

A rendszertechnológiai fejlődés következtében az alkalmazás rendszer futtató környezete (operációs rendszer, adatbázis kezelő, irodai alkalmazás, hálózati erőforrás kezelés és használat stb.), illetve az azt futtatni képes eszközpark elavult, amortizálódott nem ritka a harmadik életciklust is meghaladó eszközök jelenléte.

A fogvatartotti nyilvántartás rendszertechnológiai cseréje mára nemcsak az alkalmazás újraírását, hanem az azt működtető teljes informatikai rendszer (infrastruktúra, eszköz, platform) cseréjét, megújítását is szükségessé teszi korszerű rendszertechnológiai megoldások használatát lehetővé tevő megoldással.

A fogvatartotti rendszer fejlődéstörténete során, a folyamatosan fennálló költségvetési alulfinanszírozás, beruházási elégtelenség mellett, egyre több, a fogvatartottak személyes és különös adatainak kezelésén túlmutató, a büntetés-végrehajtási szervezet működéséhez kapcsolódó egyéb funkciót, nyilvántartási feladatot látott el. Az állandó funkcionális bővítés hatására egyéb, a közvetlen fogvatartotti nyilvántartással össze nem egyeztethető feladat is az alkalmazás részévé vált, így tipikusan a szervezet személyi állományára vonatkozó alapnyilvántartások működtetése. Az alkalmazás fejlesztés célja, profil tiszta, az egyes adatkezeléseket funkcionálisan elválasztó moduláris felépítésű célalkalmazás rendszerek létrehozása.

A felhasználói igények kiszolgálhatóságának alappillére a helyi hálózatok korszerűsége (továbbiakban: LAN). Ez a hálózati rendszer valósítja meg egy telephelyen belül a felhasználók közötti kommunikációt, a központi erőforrások elérhetőségét (levelezés, Internet-, Intranet alkalmazások, telefonközponti szolgáltatás, stb.).

A BVOP 38 telephelyén jelenleg teljesen inhomogén LAN-ok üzemelnek, amelyek nem képesek megfelelni tovább a megnövekedett igények miatt jelentkező jelentős sávszélesség és hálózati biztonsági követelményeknek. Gyakori problémát jelent, hogy a meglévő hálózati rendszer a korábbi évek igényei szerint és akkor fennálló iroda elhelyezési körülményekhez igazodott. Az elmúlt évtizedben az épületek iroda elosztásában bekövetkezett funkcionális változásokat (irodából raktár, raktárból iroda) nem vagy csak részlegesen követte a hálózati topológia. A bővítési lehetőség ezért kizárólag az adatforgalom minőségromlásával együtt járó indokolatlan szegmentálással oldható meg jelenleg (végponti ellátásról tovább switchelt szegmens).

A LAN rendszerek hosszú távra épülnek, ez indokolhatja a ma elérhető legmodernebb technológia bevezetését, ugyanakkor a források optimális felhasználhatósága mellett minimális célként az UTP Cat5e 100 Mbit/sec strukturált kábelezést alakítjuk ki.

A helyi hálózatok korszerűsítése esetén a felhasználók gyorsabban, hatékonyabban tudják végezni a munkájukat. A homogén rendszer, az energiatakarékos

és azonos típusú eszközök (chipset és firmware szintig) beszerzése miatt az üzemeltetési, karbantartási költségek csökkennek, továbbá az informatika gyorsabban, rugalmasabban tudja kiszolgálni a felmerülő igényeket. A homogén, országosan egységes hálózati aktív eszköz park egyszerűbbé teszi a tartalék képzést, csere készülék biztosítását, az újra szegmentálást, üzemeltetési tevékenységek ellátását. Fontos, hogy a helyi hálózatok azonos minőségi szintre hozása megtörténjen, ezzel alkalmassá váljanak a büntetés-végrehajtási szervezet informatikai szolgáltatásainak egyenlő mértékben történő igénybe vételére, ezzel egy időben optimális és hatékony munkavégzést és a jelenlegi kiadásokhoz képest költségmegtakarítást érjünk el.

Egy új, strukturált hálózat kiépítése a korszerű munkaállomások grafikus alkalmazásainak adatátviteli szükségleteinek biztosításán túl, a telefonrendszer korszerűsítési lehetőségét is biztosítja. (Elvárás ehhez a szükséges a hálózati aktív eszközök végpontszámának 30-50%-ában az un. PoE képesség biztosítása, a redundáns működés és moduláris kialakítás.)

A büntetés-végrehajtási szervezet informatikai rendszerének teljes modernizálása programjában a következő és halaszthatatlan lépés a büntetés-végrehajtás intézetek munkaállomásainak, majd nyomtatóinak modernizálása. A cél, hogy az elavult második, harmadik életcikluson túli eszközök amortizációs cseréje megtörténjen, és olyan korszerű eszközpark alakuljon ki, amelyik alkalmas a grafikus felhasználói felületen böngésző és/vagy virtuális célalkalmazás fejlesztések megvalósítására. (Egy életciklus az informatikai eszközök esetén a 33%-al számított értékcsökkenést figyelembe véve 3 év, funkcionális működési képességet figyelembe véve 5-8 év) A helyi hálózati és eszköz konszolidáció végső célja az, hogy a büntetés-végrehajtás intézetei/intézményei az informatikai alrendszerek tekintetében kizárólag mennyiségi mutatóiban különbözzenek egymástól, minőségi eltérés, belső struktúra, működési tulajdonságok közötti különbség ne mutatkozzon. Azaz olyan homogén, egységes és egyenszilárd informatikai rendszer valósuljon meg, amely biztosítja a szolgálati feladatok változásaihoz rendelt erőforrás allokációt, szükséges átcsoportosítások végrehajthatóságát. (Egyenszilárd az informatikai rendszer, ha egyes funkcionális elemei egymáshoz viszonyítva azonos módon és azonos színvonalon teljesítenek, függetlenül a rendszerben való elhelyezkedésüktől. Az egyenszilárdság képessége így jelenti a helyettesíthetőséget, a kapacitás skálázhatóságát, az átcsoportosíthatósággal való manőverezés képességét is.)

A számítógépes rendszer leírása (forrás: 2008. december 31-i fordulónap)

A Büntetés-végrehajtás szerveinek informatikai rendszere jelenleg üzemképes, de a technológia rohamos fejlődése, valamint a felhasználók igényeinek változása, bővülése miatt a jelenleg működő rendszer elérte teljesítő képességének felső határát. Ahhoz, hogy a felhasználók növekvő igényeit az informatikai szolgáltatások jövőbe mutatóan ki tudják szolgálni az alkalmazott rendszertechnológiai megoldásokat rövid időn belül jelentősen fejleszteni szükséges.

A munkaállomások 28%-a csak karakteres üzemmódban képes működni. A fennmaradó PC kategóriás munkaállomások a több évre elhúzódó beszerzések következtében eltérő teljesítményűek, nem bővíthetőek, a korszerű alap és alkalmazói programok működtetésére, egységes rendszerfelügyelet és menedzsment

kialakítására nem alkalmasak. Az egységes grafikus felhasználói felület hiánya akadályozza a központosított nyilvántartások korszerűsítését, a korszerűbb információtechnológiák alkalmazását is, veszélyeztetik az informatikai biztonságot. (ld.: Win95-98. felhasználói hozzáférés kezelése)

Eddig megvalósult korszerűsítések:

1. A büntetés-végrehajtási szervezet távadat-átviteli hálózatának (WAN) és telekommunikációs rendszerének korszerűsítése 2007-ben (EKG, VoIP – jelenleg a büntetés-végrehajtás zárt célú távközlő hálózata gerincirányú összeköttetései 512Kbit/sec – 4Mbit/sec kapacitással rendelkezik a 38 intézet között. Az táv-adatátviteli hálózat logikai csillagpontjában a BVOP működik, haránt irányú kapcsolatok nincsenek kialakítva)

2. Az Országos Parancsnokság helyi hálózatának korszerűsítése 2007-ben. (A BVOP Steindl Imre utcai objektumában mintegy 150 végpontos, strukturált kábelhálózat került kialakítása 100Mbit/sec kapacitással.)

3. Az Országos Parancsnokság szervereinek cseréje (virtuális szerver farm, blade architektúrán) és egységes hálózati operációs rendszer-struktúra létrehozása Microsoft Windows tartományi alapokon (büntetés-végrehajtás infocenter), új szerverterem létrehozása 2007-ben.

4. Büntetés-végrehajtás szintű egységes levelezőrendszer kialakítása. (Exchange 2008 alapú belső és külső levelezési szolgáltatás.)

5. Az Országos Parancsnokság munkaállomásainak, monitorainak, nyomtatóinak cseréje. (2006-tól folyamatosan évi 20-40 db PC és 10 db nyomtató a költségvetési lehetőségek függvényében, összességében közel 100 db számítógép és 30 db nyomtató.)

6. A Központi Nyilvántartó rendszer migrációja 2008-ban. (A Központi Szállítási és Nyilvántartási Főosztály adatszolgáltatásával kapcsolatos tevékenységek támogatására létrehozott központi, Oracle alapú rendszer az elkülönült intézeti adatbázisok összegzésével.)

7. Internet szolgáltatás központi biztosítása a büntetés-végrehajtási szervezet részére 2008-tól. (Mindösszesen 500 főt meg nem haladó Internet jogosultság mellett.)

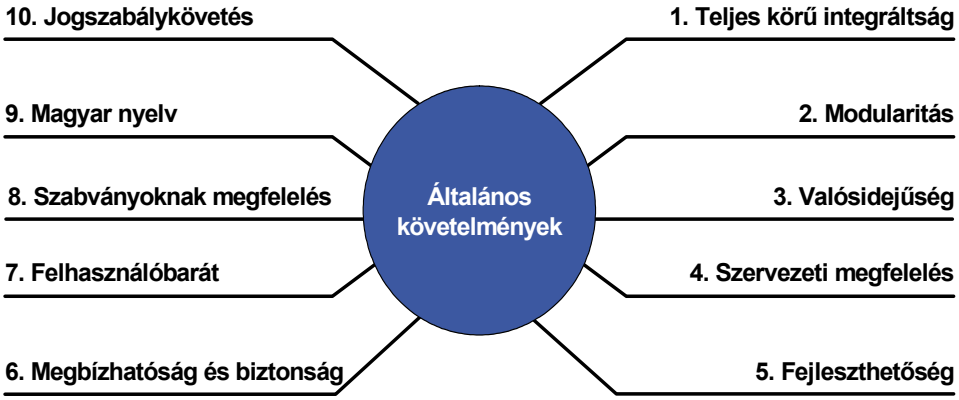
8. Vácon informatikai szempontból adoptálható „minta” intézet kialakítása a jelenlegi célalkalmazások migrációjával. (2007-2008. évben „pilot” rendszerben létrehozott Microsoft Windows tartományi site létrehozása, iroda-automatizálási képességgel, és vékony kliens technológiával kialakított helyi hálózati rendszerben.)

A probléma kezelése

Az elmúlt évtized adottságai miatt (2/e pontban ismertetett fejlesztések) a büntetés-végrehajtás informatikai rendszerének fejlesztésére a jelen projektben vázolt fejlesztés az egyedüli járható út. Olyan mérvű mennyiségi és minőségi torzulások következtek be az informatikai rendszerben, amelyek az egyre szűkülő költségvetési források mellett érdemben nem kezelhetőek. A finanszírozható mértékű beru-

házások az informatikai rendszer egészére vonatkoztatott amortizációs csapdát nem képesek felszámolni, a forrás hiányos ütemezés időbeni elhúzódásából következően a csapda helyzet mélyül, a végrehajtott fejlesztések is eltékozolt forrássá válnak.

Ahhoz, hogy a pályázati forrás megfelelő felhasználásával érdemi beruházás valósulhasson meg, a fejlesztés fókuszában lévő fogvatartotti célalkalmazással szemben általános követelményeket fogalmaztunk meg, úgy a rendszert képező egyes modulokra, mint a rendszer teljes egészére vonatkozóan. A követelményeket az elvárások alapján a következő ábra foglalja össze:



Az alkalmazás fejlesztés részletezéséhez a projekt megvalósítás kezdetén informatikai felmérést tervezünk végrehajtani, amely a nagy bonyolultságú fogvatartotti rendszer és kapcsolatainak szakértő szintű specifikáció létrehozását célozza, még az alkalmazásfejlesztésre vonatkozó közbeszerzési eljárást megelőzően. Jelenleg a követelmények általános meghatározásai, átfogó igényeinek rögzítése történt meg.

Teljes körű integráltság:

Adatbázis konzisztencia. A rendszer moduljai a közös adatbázisból vegyék mind az elemi, mind a származtatott adatokat. Az egymásból egyértelműen, előre definiálható módon következő műveletek — akár modulon belül, akár modulok között — automatikusan menjenek végbe. Az intézeti/intézményi és a központi adatbázis adattartalma ne térjen el egymástól, kizárólag a hozzáférési jogosultság korlátozza a megismerhetőséget, alkalmazást.

Modularitás:

A központi, integrált adatbázis struktúrához illeszkedő célalkalmazás megoldások bevezetése az intézeti elosztott adatbázis architektúra alapelvén működő frissített technikai másolatok jelenléte mellett történjen, az egyes funkcionális bővítések moduláris biztosításával (akár különböző megoldásszállítók bevonásával biztosítható legyen a funkcionális követelmények / igények lefedése). A moduláris kialakítás kövesse a szerepkör alapú delegálás, hozzáférés és tevékenység feladatokat, szolgálja ki a differenciált hozzáférést.

Valósidejűség:

Az egymásból következő műveletek végrehajtása — akár modulon belül, akár modulok között — az elsődleges adatok rögzítését követően azonnal, valós időben történjen. A forrásadatok feldolgozása azok keletkezési helyén és idejében legyen biztosított. Különüljön el az adatrögzítés (a keletkezés helyén) és a származtatott adatokkal történő műveletek tevékenysége olyan módon, hogy az adatok valós időben történő feldolgozása tegye lehetővé az összegző-, elemző-, értékelő tevékenységek naprakész adatokkal való végrehajtását.

Szervezeti felépítésnek való megfelelés:

Több intézményes felhasználás, szervezeti intézményeken belüli szervezeti elem/felhasználó azonosítás, legyen megvalósítható (szerepkör alapú hozzáférés szabályozás). A rendszer kialakítható legyen olyan formában, hogy az intézmények adataiból összevont és intézményenkénti beszámoló, valamint vezetői információs adatszolgáltatás is biztosítható legyen.

Rugalmasság és fejleszthetőség:

A rendszer egyes moduljainak funkciói, a lekérdezési struktúrák, a jelentésformátumok stb. egyrészt legyenek előre (beégetetten) definiáltak a büntetésvégrehajtás specialitásainak és az intézmények igényeinek megfelelően (paraméterezés), másrészt biztosítsák az un. „rugalmas lekérdezést" az előre nem definiálható keresési, adatgyűjtési feladatokhoz illeszkedően. A fejlesztés tegye lehetővé az így beállított értékek egyszerű megváltoztatását, rugalmas kódszótár, mintaokmány kezelést, ezek felhasználói felületen történő megváltoztatását. Rendszertechnológiai megoldásaiban legyen EU-konform.

Megbízhatóság és biztonságosság:

Nyújtson megbízható megoldást az adatbevitel tartalmi és formai (pl. a rendszerben létező adat érvényesség vizsgálata) ellenőrzésére. Jogosultsági rendszere legyen kellően mély, szerepkörökhöz illeszkedő, szükség esetén lekérdezés és/vagy törzsadat típushoz kötött. Biztosítsa a folyamatokon belüli ellenőrzés, engedélyezés lehetőségét. A rögzítési, javítási, megtekintési stb. jogosultságok szintén váljanak szét. A jogosultságok kiadása, megváltoztatása csak központilag történhessen, integrálva a központi címtárhoz. Biztosítson archiválási lehetőséget és gyors hozzáférést az archivált adatokhoz. Tegye lehetővé a személyes- és különös adatok kezelésével kapcsolatos normatívák érvényesítését, a bizonyíték biztosítás és nyomon követhetőség alapelveinek érvényesülését.

Felhasználóbarát kezelhetőség:

Felhasználói felület és kezelési technika legyen egységes, felhasználóbarát az összes modulra kiterjedően. Alkalmazzon korszerű grafikus felületi megoldásokat, éljen a keretrendszer adta szolgáltatásokkal és alkalmazza azokat saját funkcionalitása kiegészítéseként. Kerülje a megszokott és szabványos rendszertechnológiai megoldásoktól eltérő gyakorlatot, közvetlen eszközkezelést.

Szabványoknak megfelelés:

Feleljen meg a vonatkozó magyar, európai közösségi (nemzeti és nemzetközi) szabványoknak, ajánlásoknak. Szükség esetén egyes funkcióiban, vagy moduljaira vonatkozóan minősített, auditált legyen a megfelelő törvényi előírások betartására.

Magyar nyelv használata:

A fejlesztett célalkalmazásokra vonatkozóan magyar felhasználói felület, magyar nyelvű súgó (= „help") funkció és minimálisan rendszer üzemeltetői-, valamint felhasználói kézikönyv biztosítása szükséges.

Jogszabálykövetés:

Biztosítsa a törvényben és rendeletekben előírt külső és belső adatszolgáltatásokat. A jogszabályi változások implementálása a jogszabályban rögzített hatályba lépésre történjen meg, auditált módon. A büntetés-végrehajtáshoz kapcsolódó összes jogszabály követését garanciával biztosítsa. Folyamat-specifikus követelményeknek tegyen eleget, lehetőség szerint a felhasználó számára hozzáférhető módon (un. paraméter lista, kódszótár használatával). Tegye lehetővé a jogszabály követés célalkalmazás fejlesztés nélküli megvalósítását. A jogszabálykövetés kötelme a megvalósítás teljes időintervallumában kötelezettség (2011. december 31-ig külön szerződés nélküli elvárás).

A választott megoldás áttekintő ismertetése

(jogszabályi megfelelőség, hatékonyság, gazdaságosság, műszaki indokoltság)

Összhangban az EKOP 1. prioritási tengely céljával jelen fejlesztés hozzájárul a közigazgatás működésében az elektronikus szolgáltatások nyújtásának képességéhez szükséges belső fejlesztések végrehajtásához, mely által biztosíthatók a közigazgatáson belüli (G2G) informatikai szolgáltatások.

A fejlesztés tervezése során figyelembe vettük a büntetés-végrehajtási intézetek jelenlegi informatikai felszereltségét, valamint a rendelkezésre álló erőforrásokat és a projekt tevékenységeit valamint a tervezett informatikai beszerzéseket - hálózat kiépítése, hardver és szoftver - azokhoz illesztettük.

A büntetés-végrehajtási intézetek, intézmények és az országos parancsnokság speciális feladatainak ellátásához szükséges adatok – így különösen a fogvatartottak elhelyezésére, egészségügyi ellátására, foglalkoztatására, elítélésére, várható szabadulására vonatkozó adatok - nyilvántartására egységes Fogvatartotti Programrendszer került kifejlesztésre 1992-1996-ban.

A büntetés-végrehajtás törvényben meghatározott feladatai végrehajtásához szervesen kapcsolódik a fogvatartottak különböző adatainak gyűjtése, rögzítése, rendszerezése, továbbítása. Számos funkció esetében elengedhetetlen, hogy az egész döntési mechanizmus számítógépen történjen (pl.: fogvatartotti kérelmek esetén). Az információ-technológiai támogatás minősége közvetlenül hat a fogvatartottak jogainak érvényesülésére, hiszen az ügyintézés a rendelkezésre álló információk pontosságától és az elérés idejétől is függ.

A büntetés-végrehajtási szervezet a büntető igazságszolgáltatás szerves részét képezi, amely többek között abban is megnyilvánul, hogy más szervek felé nagy tömegű adatot szolgáltat. Ilyen formában hozzájárul a rendőrség, az ügyészség, a bíróságok és más államigazgatási szervek törvényes és szakszerű működéséhez.

(Az adatszolgáltatást a Központi Szállítási és Nyilvántartási Főosztály végzi, napi rendszerességgel folyamatosan 6-7 fő telefonos adatszolgáltatást végez, havi szinten átlagosan 9-10000 db papír alapú, valamint 1500 db telefax megkeresés érkezik). A biztonságos összeköttetés biztosítása mellett egyes társszervek (ügyészség, bíróság, Rendőrség stb.) közvetlen on-line lekérdezésének biztosításával az ügyiratforgalom és a személyi állomány leterheltsége a várakozás szerint mintegy 60%-al csökkenthető.

Jelenleg a kilencvenes évek elején rendszerbe állított információ-technológia hivatott mindezen feladatok ellátására. Ennek technikai színvonala teljes mértékben elavultnak tekinthető, kapacitása egyre komolyabb működési zavarokat okoz.

A tervezett fejlesztés célja alapvetően öt gondolatkörben összegezhető:

1. Az elavult rendszertechnológián működő alkalmazásrendszerek cseréje, korszerű programtechnikai megoldásokkal és megújított eszközparkon, amely lehetővé teszi már a rendszerintegrálást követően az irodaautomatizálást, a távfelügyeleti-, távmenedzselési- és távsegítség nyújtási funkcionalitást, biztonságos informatikai környezetben történő kialakítással.

2. Az intézetek helyi hálózati- és az országos parancsnokság közötti adatforgalom megfelelő kapacitásának, biztonságának, gyorsaságának biztosítása.

3. A különböző társszervek (Igazságügyi Minisztérium, Legfőbb Ügyészség, Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala, ORFK stb.) felé történő adatszolgáltatás on-line támogatása, a jelenlegi papír alapú ügyintézés időszükségletének csökkentése. (A 10 nap adminisztratív válaszidő, azonnali közvetlen lekérdezéssel való kiváltása.)

4. A rendszer alkalmassá tétele a jelenleginél szélesebb körű statisztikai elemzések elvégzésére, döntés előkészítő-, döntés támogató képességek javítására. (Az Európa Tanács a magyar statisztikai rendszertől eltérő bontású adatokat kér.)

5. Korszerű, magas rendelkezésre állású, hibatűrő rendszertechnológia bevezetése, figyelemmel járulékos környezeti előnyök érvényesítésére (pl.: környezetkímélő, alacsony fogyasztású megoldások preferálása.)

Ilyen módon a tervezett korszerűsítés önállóan is jelentős eredményeket biztosít, hozzájárul mind a büntetés-végrehajtási szervezet, mind az igazságszolgáltatási rendszer törvényes és szakszerű működéséhez, a társszervek igényéhez kapcsolódó adatszolgáltatás felgyorsításával a hatósági tevékenység, a közigazgatás hatékonyságának javításához.

A büntetés-végrehajtási szervezet informatikai rendszere jelenleg nem megfelelően támogat több szakmai területet. A projekt célja, hogy a büntetés-végrehajtás intézetekben használt egységes, a fogvatartáshoz kötődő (SCO UnixWare/Recital rendszerek) célalkalmazások:

1. Fogvatartotti Alrendszer,

2. Egészségügyi Alrendszer,

3. Fogvatartottak telefonhasználata

mellett, a jelenleg nem egységes (nem SCO UnixWare/Recital) célalkalmazások:

1. Fogvatartottak fényképezése,

2. Fogvatartottak letétjeinek nyilvántartása,

3. Fogvatartottak élelmezése,

4. Fogvatartottak bérének számfejtése

helyett, egységes szerkezetű és felhasználói felületű megújult fogvatartotti alkalmazói rendszer (vagy modulárisan önálló, de egyként működő alrendszer együttes) kerüljön kialakításra.

Az új célalkalmazások fejlesztésével kialakítandó szoftver környezet, a fogvatartotti rendszerhez illeszkedően:

- Fogvatartottak nyilvántartási rendszerének korszerűsítése, újra programozása
- Letétkezelő alrendszer (ide értve a virtuális pénzletét kezelését is)
- Élelmezési alrendszer
- Foglalkoztatási alrendszer
- Fényképkezelő alrendszer
- Befogadási eljárás biometrikus adatcseréje
- Egészségügyi alrendszer (járó-, fekvőbeteg ellátás az 5/1998. (III. 6.) IM rendelet alapján)
- Társszervek on-line lekérdezése
- Statisztikai és vezető-irányító funkcionalitás bővítése
- Adatmigrálás és rendszerintegráció

A büntetés-végrehajtás személyi állományára vonatkozóan:

- Személyügyi alapnyilvántartás
- Szolgálatszervezés
- Fegyelmi alrendszer
- Egészségi-, pszichikai- és fizikai állapot felmérés nyilvántartása (Hszt. 68.§. (1) e.)
- Adatmigrálás és rendszerintegráció

A projekt tervezése során az alábbiakat vettük figyelembe:

- jogszabályban meghatározott feladatok végrehajtásához szükséges fejlesztések;
- meglévő informatikai rendszer fejlesztési lehetőségei, és a fejlesztést befolyásoló tulajdonságai
- hiányzó eszközök beszerzési, pótlási költségei;
- költséghatékonyság, célszerűség, egységes és egyenszilárd informatikai környezet kialakítása.
- Informatikai szakállomány és felhasználói szintű differenciált képzések

A projekt megvalósítás során további az informatikai környezetre vonatkozó fejlesztési célokat is megvalósítunk:

- Integrált hang- és adatátvitelre képes strukturált minimálisan 100Mbit/sec kapacitású helyi hálózati szolgáltatás kialakítása
- Szerver-, munkaállomás és nyomtató konszolidáció (amortizációs csere)
- Rendelkezésre állás és hibatűrő képesség javítása
- Rendszerüzemeltetői és felhasználói képzés

A projekt megvalósításához szükséges feltételezések

A felhasználói igények kiszolgálhatóságának alappillére a lokális hálózatok korszerűsége. Ez a hálózati rendszer valósítja meg egy telephelyen belül a felhasználók közötti kommunikációt, a központi erőforrások elérhetőségét (levelezés, Internet, alkalmazások, telefon, stb.). A kiegyensúlyozottan és folyamatos megbízhatóság mellett működő hálózati szolgáltatásokra alapozva célszerű a munkaállomás oldali erőforrásokat kímélő böngésző alapú és/vagy vékony kliens (pl.: RDP/virtuális) technológiát meghonosítani. A felhasználói igények valósidejű kiszolgálása érdekében a WAN hálózati kapacitások és rendelkezésre állás minősége okán az intézeti elosztott adatbázis struktúra kialakítása látszik célszerűnek nemcsak a tartományi- és helyi hálózati szolgáltatások kiterjesztésével, hanem az adatbázis struktúra szintjén is. A felhasználók az egységes felhasználói felületnek köszönhetően kedvezően fogadhatják a rendszertechnológiai újítást, ugyanakkor az újtól való idegenkedés, az átállással járó nehézség, stressz, így kockázat, megfelelő, az egyes szerepkörökhöz illeszkedő célképzésekkel csökkenthető (ügyintéző, vezető, rendszergazda stb.). A képzés során a célalkalmazások kezelésén túl, alapvető informatikai szolgáltatásokra vonatkozó képzést is nyújtani kell a hibatűrő képesség és a hibaeseményt követő helyreállítás, kárenyhítés munkálatainak gyorsítására. A célalkalmazás használatára vonatkozó képzés hatékonyságát növeli az alap infrastrukturális szolgáltatások megelőző bevezetése, az új grafikus felhasználói környezet, iroda-automatizálás bevezetése, működtetési tapasztalatok értékelő feldolgozása.

A fejlesztés célja, a tervezett eredmény

A fejlesztéstől elvárt eredmények

Összhangban az EKOP 1. prioritási tengely céljával, jelen fejlesztés hozzájárul a közigazgatás működésében az elektronikus szolgáltatások nyújtásának képességéhez szükséges belső fejlesztések végrehajtásához, mely által biztosíthatók a közigazgatáson belüli (G2G) informatikai szolgáltatások.

A projekt célja az, hogy a büntetés-végrehajtás korszerű rendszertechnológiai megoldással váltsa ki a jelenleg magas működési kockázattal és indokolatlanul magas üzemeltetési-fenntartási költséggel működő elavult alkalmazásrendszereit, illetve az intézetek/intézmények az informatikai rendszerek tekintetében csak mennyiségben különbözzenek egymástól, minőségi, funkcionális teljesítménybeli eltérés ne legyen. A fejlesztés során kialakítandó programrendszer általános követelményei az alábbiak szerint összegezhetőek.

A büntetés-végrehajtás 2004. évben határozott a Microsoft Windows platform bevezetése mellett, első sorban a felhasználóbarát, grafikus operációs rendszer

felület, és az iroda-automatizálási képességek miatt, figyelemmel arra, hogy a Világon működtetett munkaállomások 90%-án Microsoft Windows termék fut. A 2007. évi Büntetés-végrehajtás Informatikai Stratégiája rögzíti a Microsoft Windows alapú szoftver infrastruktúra homogén módon történő bevezetését, amely koncepció eredményeként valósult meg a központi Microsoft Exchange belső- és külső elektronikus levelező rendszer, munkacsoportos feladatütemezés és határidő naplózás. A központi kiszolgálók tekintetében tartományi rendszer alapú állomány és nyomtató megosztás, központi címtár szolgáltatás, egységes helyi hálózat oldali DNS és DHCP szolgáltatás alakult ki. A központi kiszolgálók Microsoft Windows Server 2008-ra alapulnak, az SCO UnixWare/Recital alapú Fogvatartotti Alrendszer működtetése terminál emuláció virtuális megoldásával valósul meg. A Váci Fegyház és Börtönben Microsoft Windows alapú mintarendszer került bevezetésre 2007-2008. fordulóján. A kialakított rendszer, mint minta intézet valósult meg olyan módon, hogy a teljes munkafolyamat támogatás Microsoft Windows tartományi környezetre alapul, munkaállomás oldalon homogén Microsoft Windows Vista operációs rendszer fut. A leendő fejlesztés eredményeként, mint alternatív lehetőség, számolunk a Windows 7 munkaállomás oldali operációs rendszer megjelenésével, de nem zárjuk ki a nyílt forráskódú (un. Open Source) rendszer átfogó bevezetését. (A rendszertechnológiai megoldás kiválasztása esetén előnyben részesül az átfogó, homogén rendszertechnológiai megoldást megvalósító megoldás.)

A megkezdett és rövid távon, koncepcionálisan követett informatikai fejlesztés részeként a szoftverfejlesztéseket a jelenleg működő tartományi rendszerrel, központi címtárszolgáltatással együttműködni képes megoldással tervezzük megvalósítani olyan módon, hogy az alkalmazás rendszerek a folyamatos rendelkezésre állás követelményét központosított adatbázis modellel, de backup-ként helyben is működő tükör replika struktúrára alapozzák. Az elosztott adatbázis infrastruktúra licensz költségeinek csökkentése érdekében az intézményi telephelyeken homogén adatbázis kezelői architektúrát kívánunk megvalósítani, nem számolunk eltérő adatbázis kezelő megoldások párhuzamos kiterjesztésével. Az alkalmazás fejlesztések során a hardver környezet beszerzése nem része az alkalmazásfejlesztésnek, ugyanakkor a megoldásszállítónak ajánlást kell tennie a fejlesztett rendszer minimális és optimális hardver és szoftver feltételeire. Amennyiben az ajánlott rendszertechnológiai megoldás új platform környezetet feltételez, úgy a megoldásszállítónak a célalkalmazás kifejlesztésének árában kalkulálnia kell az új platformhoz szükséges licenszek biztosítását is.

A működő tartományi környezetből következően az újonnan bevezetésre kerülő alkalmazások, szolgáltatások authentikációját, szerepkör alapú jogosultsági rendszerét első sorban a tartományi központi címtárra alapozva tervezzük megvalósítani. (A leendő megvalósítási ajánlatok elbírálásánál előnyt jelent a teljes címtár integráltság, a humán rendszer esetében a személyügyi nyilvántartás és a címtárszolgáltatás valós idejű összekapcsolását.)

A táv-adatátviteli hálózat kapacitására érzékeny módon vékony kliens technológia alkalmazását (terminál-szerver kliens, egyéb virtuális megoldás), vagy szerver oldalon futó böngésző alapú célalkalmazás fejlesztését várjuk el. A célalkalmazásnak úgy kell futnia a munkaállomás oldalon, hogy működése során átmeneti állományokat kizárólag a felhasználói jogosultság birtokában, a felhasználó számá-

ra operációs rendszer szinten biztosított alkönyvtár és jogosultsági struktúrában képezhet, és ennek kapacitása nem haladhatja meg az 50Mb méretet, ide értve például a Java futtató környezet jelenlétét is. A munkaállomás oldalon nem megengedett olyan rendszertechnológiai megoldás alkalmazása, amely helyi rendszergazdai jogosultságot feltételez, vagy használ, illetve amely az alkalmazás futtatása során rendszer területen írási jogosultságot igényel. (Változó konfigurációs állomány, futtató környezet aktualizálása, változó kódszótár stb.). A terminálszerver- és a böngésző használatot 16 bites színmélység mellett 1024*768-as felbontásra kell optimalizálni, 256 Kbit/sec sávszélesség mellett, Internet Explorer 7.x, vagy magasabb verziószámú böngészőre.

A célalkalmazásnak a rendszertechnológiai megoldásnak megfelelő operációs rendszer szabványos szolgáltatásaira kell alapulnia, azaz nem tartalmazhatnak operációs rendszer szolgáltatásokat megkerülő közvetlen I/O műveleteket. Így különösen fájl- és nyomtatási műveletek, képernyőkezelés, karakterkészlet tekintetében, nem alkalmazhatnak közvetlen IP cím hivatkozást (elvárás a teljes körű DNS használat), programkódba beágyazott, rögzített jogosultság kezeléssel adatbázis-, szolgáltatás elérést stb. A táv-adatátviteli hálózati környezetre alapulva a célalkalmazásnak előre definiált és meghatározott cél IP cím, port és protokoll kapcsolatokkal kell kommunikálnia a munkaállomás oldalról kezdeményezve.

Amennyiben az alkalmazás valamilyen korábban fejlesztett-, vagy un. dobozos termék testre szabásával kerül módosításra, kifejlesztésre, fenti követelményeket a lehető legnagyobb mértékben figyelembe véve kell alkalmaznia. Vastag kliens megoldás esetében a cél-alkalmazás nem tartalmazhat táv-adatátviteli hálózatban működő program funkciót, illetve ilyen funkcionalitás kialakítása esetén azt már a fentiekben rögzített rendszertechnológiai megoldással kell biztosítania. Amennyiben a vastag kliens környezet frissítése a célalkalmazás indítását megelőző verzió ellenőrzésen alapulva, automatikusan történik a munkaállomás oldalon, úgy annak terítését, frissítését kizárólag helyi hálózati környezetben terített módon lehet megvalósítani. A frissítendő futtatási környezet táv-adatátviteli hálózatban való terítését szabványos rendszer megoldásokkal kell kialakítani (jogosultsági rendszer figyelembe vétele, szolgáltatás vagy policy alapú ellenőrzés és terítés, fájl megosztás, vagy FTP stb.).

A büntetés-végrehajtás az alkalmazás rendszerek fejlesztése során keletkező termék használati jogát a szervezetén belüli korlátlan használatra várja el, amely jelenti a szerver oldali megoldások korlátlan számú reprodukálását, illetve a munkaállomás oldali alkalmazás korlátlan számú egyidejű használatát is. (Amennyiben a megoldásszállító licensz politikája nem teszi lehetővé a szervezeten belüli „korlátlan" felhasználási jogot, úgy azt 5000 darabban kell maximálni, figyelemmel a büntetés-végrehajtás jelenlegi és prognosztizálható maximális munkaállomás, illetve felhasználói számára.) A szervezeten belüli korlátlan felhasználási jog magában hordozza az alkalmazással együtt szállítandó telepítési és üzembe helyezési leírás, üzemeltetői kézikönyv, felhasználói leírás és egyéb műszaki dokumentációk elektronikus példányainak szervezeten belüli korlátlan reprodukálásának lehetőségét is, illetve annak részei, egésze tekintetében felhasználhatóságát a saját állomány képzésében, a rendszerek harmadik félnek való bemutatásában azok egészének, vagy részeinek átadási engedélye nélkül.

A fejlesztett alkalmazás un. „master” példányát a teljesítési jegyzőkönyvvel egy időben át kell adni a büntetés-végrehajtási szervezetnek, amely termékre szintén vonatkozik a saját szervezeten belüli korlátlan felhasználás, reprodukálás lehetősége. A „master” példánynak tartalmaznia kell a rendszertervet (minimálisan funkcionális leírás és adatbázis kapcsolatok szintjén), illetve a forráskódot és a metanyelvű leírást, a független továbbfejleszthetőség és bővíthetőség érdekében szükséges minden dokumentumot.

A fejlesztett célalkalmazások esetén nem elegendő a „működő” célalkalmazás telepítése és bevezetése, szükséges az „éles” alkalmazásrendszertől független, önállóan működő fejlesztői-, teszt- és oktató- környezet (verzió) reprodukálható központi létesítése is.

A létrehozandó fejlesztés célja

1. Homogén, korszerű helyi hálózatok, biztonságos hálózati adatátvitel és munkavégzés feltételeinek megteremtése.
2. Korszerű, környezetkímélő és alacsony üzemeltetési költségű eszközök alkalmazása, egyenszilárd szerver és munkaállomás oldali informatikai rendszer létrehozása.
3. Korszerűsített, funkcionálisan bővített célalkalmazások bevezetése a fogvatartotti- és a saját személyi állomány nyilvántartásaira vonatkozóan.
4. Új informatikai szolgáltatások bevezetésének rendszertechnológiai megalapozása (IP telefónia, video tárgyalás, központi elektronikus iratkezelés, e-learning, fogvatartotti Internet használat stb.).
5. Magas rendelkezésre állás képességének kialakítása, hibatűrő rendszerek általános bevezetése.
6. Rendszertechnológiai alapú távfelügyeleti, táv-menedzselhető, biztonságos informatikai környezet kialakítása, a felhasználói támogatás színvonalának emelése.
7. Gazdaságosabb, költséghatékonyabb információ-technológiai megoldások alkalmazása, hatékonyabb szakterületi működés biztosítása.
8. Probléma érzékeny, a jelentkező szakterületi igényekre dinamikusan és eredményesen reagálni képes informatikai szolgáltatási rendszer megalapozása.
9. Intézeti nyomtatók alacsony működtetési költségű eszközökkel történő részbeni kiváltása.
10. A jelenlegi „felügyelő” informatikai működés helyett továbbképzésekkel „végrehajtó” szemléletű informatikai támogatás kialakítása.

A javasolt fejlesztés menete

A fejlesztés menetének összefoglalása és tevékenységenkénti bemutatása

A felhasználói igények kiszolgálhatóságának alappillére a lokális kábel hálózatok korszerűsége. Ez a hálózati rendszer valósítja meg egy telephelyen belül a

felhasználók közötti kommunikációt, a központi erőforrások elérhetőségét (levelezés, Internet-, Intranet alkalmazások, telefon szolgáltatás, stb.).

A helyi hálózati rendszerek második alkotóeleme a hálózati aktív eszközök. Az aktív eszközök korszerűsítése során minden felhasználó azonos sebességű (100 Mbps) kapcsolattal rendelkezik.. A kritikus rendszerek 1000 Mbps-os sávszélességgel kapcsolódnak, így a felhasználók gyorsabban érhetik el a központi alkalmazásokat. A LAN eszközök egyik legfontosabb követelménye az üzembiztonság, a moduláris felépítés és a redundáns működés. Az aktív eszközöknek meg kell felelniük a strukturált hálózatból következő integrált hang-adatátviteli követelménynek (PoE képesnek kell lenniük).

A büntetés-végrehajtási szervezet informatikai rendszerének teljes modernizálása programjában a következő és halaszthatatlan lépés a büntetés-végrehajtás intézetek szerver- és munkaállomásainak modernizálása. A cél, hogy az elavult második, harmadik életcikluson túli eszközök amortizációs cseréje megtörténjen és olyan korszerű eszközpark alakuljon ki, amelyik alkalmas a grafikus felhasználói felületen böngésző és/vagy virtuális célalkalmazás fejlesztések megvalósítására (egy életciklus az informatikai eszközök esetén a 33%-al számított értékcsökkenést figyelembe véve 3 év, funkcionális működési képességet figyelembe véve 5-8 év). Végső cél, hogy a büntetés-végrehajtás intézetei/intézményei az informatikai alrendszerek tekintetében kizárólag mennyiségi mutatóiban különbözzenek egymástól, minőségi eltérés, belső struktúra, működési tulajdonságok közötti különbség ne mutatkozzon. Azaz olyan homogén, egységes és egyenszilárd informatikai rendszer valósuljon meg, amely biztosítja a szolgálati feladatok változásaihoz rendelt erőforrás allokációt, szükséges átcsoportosítások végrehajthatóságát. A rendelkezésre álló források mértékében törekedni kell a nagy teljesítményű hálózati nyomtatók bevezetésére, a kis teljesítményű, magas működési költségű, egyedi gépekhez kötött nyomtatók helyett.

A projekt célja továbbá, hogy a büntetés-végrehajtás intézetekben használt egységes, a fogvatartáshoz kötődő SCO UnixWare/Recital alrendszerek (Fogvatartotti Alrendszer, Egészségügyi Alrendszer) mellett, a jelenleg nem egységes alkalmazások (Fogvatartottak fényképezése, Fogvatartottak letétjeinek nyilvántartása, Fogvatartottak élelmezése, Fogvatartottak bérének számfejtése stb.) helyett, egységes szerkezetű fogvatartotti alkalmazói rendszer kerüljön kialakításra. A kialakítás során a központi, integrált adatbázis struktúrához illeszkedő célalkalmazás megoldások bevezetését tervezzük intézeti elosztott adatbázis architektúra alapelvén működő frissített technikai másolatok jelenléte mellett, ahol az egyes funkcionális bővítések modulárisan biztosítottak (akár különböző megoldásszállítók bevonásával fejlesztett funkcionális modulok).

A projekt lebonyolítás – EU, hazai előírásaihoz kapcsolódó – tevékenységei:

- a teljes projekt folyamatot végig kíséri a projekt menedzsmentje, a projekt adminisztrációja (pénzügyi, számviteli, egyéb)
- közbeszerzések (hálózat kiépítéséhez, hardver és szoftver beszerzéshez kapcsolódó) a tanácsadással és hirdetéssel együtt
- nyilvánossági követelmények teljesítésére irányuló tevékenységek
- könyvvizsgálói, projekt felügyeleti és minőségbiztosítási tevékenység

- Informatikai szakállományi- és felhasználói célalkalmazáshoz kötött képzések

A tevékenység időzítése, függőségei

A projekt megvalósítás kezdő időpontja: ~2009. szeptember 1.
A projekt fizikai megvalósítás határideje (24 hónap): 2011. július 31.
Függőségek:

- Kormány döntés (kormány határozat),
- kiemelt projekt pályázati felhívás megjelenése,
- közbeszerzési eljárás elhúzódása, esetlegesen induló jogorvoslati eljárások,
- központosított közbeszerzés keretmegállapodása szerint lehívható keretek kimerülése

A tevékenység minőségbiztosításának módja

A projekt a bevonni kívánt informatikai szakértő(k) és a BVOP Információtechnológiai Főosztályának folyamatos szakmai felügyelete mellett valósul meg. E mellett a projekt költségek terhére független minőségbiztosítási szakember (társaság) alkalmazását tervezzük, illetőleg a célalkalmazás fejlesztések esetében a megoldásszállító kötelezettségeként írjuk elő a minőségbiztosítás követelményrendszerének biztosítását.

A SCI-NETWORK KOMPLEX HP PROCURVE WLAN (WI-FI) RENDSZERE

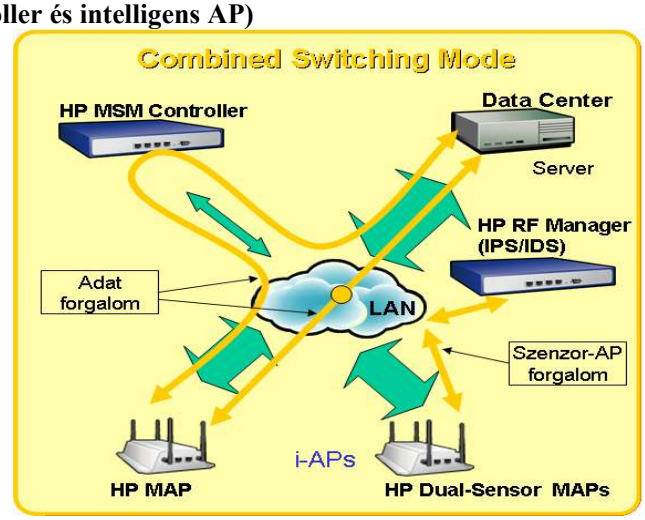
A hordozható kommunikációs eszközök elterjedésével felhasználói oldalról egyre nagyobb igény mutatkozik a hálózatok mobilitásának növelésére. A vezeték nélküli hálózatok az utóbbi időben óriási népszerűségre tettek szert, így szinte valamennyi felhasználói készülék támogatja a vezeték nélküli hálózati szabványokat. Napjainkban a WLAN technológia egyre biztonságosabbá válik, valamint nagy sebességű adatátvitelt biztosít (802.11n szabvány). Teljesítményét illetően ma a Wi-Fi hálózatok már költséghatékony alternatívát nyújtanak az Ethernet hálózatok számára, hiszen valós átviteli kapacitásuk több, mint 180 Mbps is lehet. Ennek köszönhetően a szolgáltatók és az intézmények hálózatukba integrálják a Wi-Fi rendszereket, ezzel bővítve minőségi szolgáltatásaik körét.

A SCI-Network által kínált HP ProCurve MSM (volt Colubris) WLAN rendszer az egyszerű hálózati hozzáférésen túl gondoskodik a különböző típusú felhasználói alkalmazások forgalmainak biztonságos, struktúrált és priorizált kezeléséről, beleértve a speciális alkalmazásokat is, mint Voice over WLAN, video megfigyelő rendszerek elemeinek vezeték nélküli hozzáférése, helymeghatározó rendszer, stb. A HP MSM megoldás olyan kulcsrakész, biztonságosan üzemeltethető rendszer, amely rugalmasan beépíthető a fix és mobil szolgáltatói, valamint a vállalati és intézményi hálózatokba is.

Ezen felül a SCI-Network az MTA SZTAKI közreműködésével olyan komplex számlázási szoftvert fejlesztett ki a HP Procurve MSM Wi-Fi rendszerekhez, amely testre szabható az üzemeltető igényeinek megfelelően.

A HP Procurve MultiService Mobility (MSM) rendszer főbb előnyei:

Elosztott intelligenciájú WLAN architektúra (Multiservice WLAN Kontroller és intelligens AP)



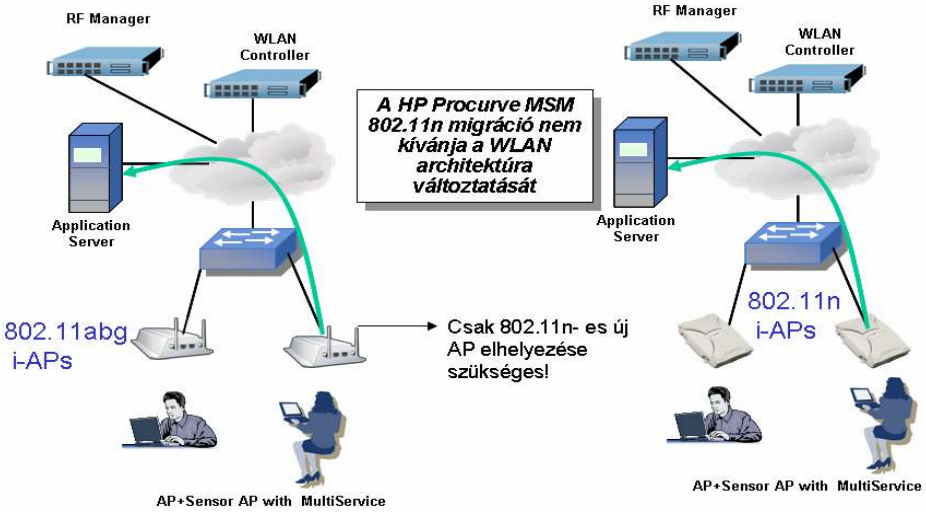
- Az intelligens AP-k adatforgalma kombinált módon a kontrolleren át (pl. HTTP-redirect esetén), vagy közvetlenül a szerver erő-források felé irányulhat (tipikus megoszlás a működő hálózatokban 10% / 90%), míg a Sensor-AP forgalom kizárólag az RF Ma-nagerhez tart.

Kapacitás optimalizált kialakítás

- A hálózat aktív eszközeinek (tipikusan L2/L3 switchek, routerek) kisebb forgalmat kell átvinniük, mert viszonylag kevés forga-lom halad át a kontrolleren. Ez a 802.11n-es migrációnál jelentős beruházás megtakarítást eredményez, mivel nem szüksé-ges az aktív elemek cseréje ahhoz, hogy a hálózat elbírja a megnövekedett forgalmat.

Zavartalan és egyszerű 802.11n migráció

- Az adott konfigurációban vezérelhető HP ProCurve intelligens hozzáférési pontok száma független az egyes AP-k típusától. Tehát a központi vezérlőegységek által kezelt hozzáférési pontok száma nem függ attól, hogy az adott hálózat milyen összetételben tartalmaz egy-, kettő illetve három rádiós felépítésű, valamint 802.11 a/b/g illetve 802.11/n képes eszközöket. Így a rendszer a legkorszerűbb, nagy sávszélességet biztosító 802.11/n módú eszközökkel is könnyen és költség hatékonyan bővíthető.



- A 802.11/n mód biztosítása a HP ProCurve MSM422 NA intelligens hozzáférési pontokkal melyek PoE távtáplálással is üzemeltethetők.

Jól skálázható rendszer a hozzáférési pontokba kihelyezett intelligenciának köszönhetően

- Az egyes AP-kon 16 különböző SSID (virtuális AP) hozható létre, amelyek mindegyikén egye-dileg konfigurálhatóak a QoS paraméterek, a security policy (titkosítás, szűrőlista, authen-tikáció), a VLAN és az elérhető maximális sávszélesség.
- Egyazon AP-n biztosítható, hogy a virtuális hozzáférési pontok egy része a központi vezérlőegységen áthaladó és felügyelt forgalmat továbbítsa,

míg más virtuális hozzáférési pontok forgalma közvetlenül a helyi szerver és az adott AP között bonyolódjon. A direkt forgalom nem terheli a központi vezérlő(ke)t és mivel a forgalom kevesebbet utazik a hálózaton, így annak erőforrásait is kevésbé terheli. Ilyen esetben a központi vezérlő(k)re a hozzájuk kapcsolódó hozzáférési pontok menedzselése és a bejelentkező felhasználók authentikációja és authorizációja hárul.

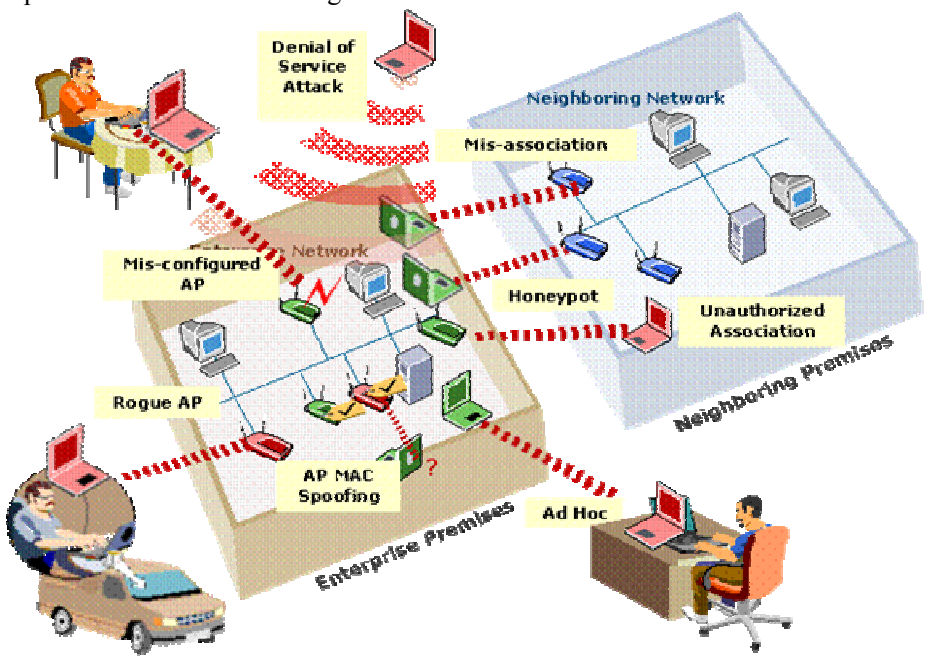
- A QoS, valamint a biztonsági szabályok betartatása már a hozzáférési pontoknál megtörténik. A kiemelt fontosságú alkalmazások biztonságának érdekében az eszközök a kliensek felé támogatják valamennyi jelenleg használt rádiós titkosítási lehetőséget (WEP, WPA, 802.1x tanúsítványok használata). A hálózati oldalon tűzfalas védelem, IPSec kliens és GRE tunnelling áll rendelkezésre.

Valós idejű mobilitás

- Az intelligens access pontok (MAP) a központi vezérlő(k) (MSC) koordinálásával támogatják a valós idejű (real-time) mobilitást. A vezeték nélküli ügyfelek szabadon mozoghatnak az access pontok között fenntartva a biztonságos, szakadásmentes kapcsolatot miközben az inter- és intra-subnet handover értéke a kívánt 50 ms alatt marad. A csomagvesztés nélküli roaming funkció Mobility upgrade-del a kontrollerekre utólagosan is rátölthető.

Hálózat védelem

A hálózatok védelme a rádiós hálózatok tervezésének és üzemeltetésének kritikus pontja. A HP piacvezető megoldása nemcsak detektálni, hanem elhárítani is képes az alábbi ábrán összefoglalt különböző rádiós hálózatot érő támadásokat.



- Legmagasabb három szintű védelem a HP MSM WLAN rendszerben.

1. Fizikai szintű adatfolyam titkosítás (WEP, WPA, WPA2), VLAN és L2 izoláció.

2. Hálózati hozzáférési réteg kontroll 802.1x és Radius segítségével.

- Az MSM 700-as sorozatú kontrollerekben beépített RADIUS szerver biztosítja a költséghatékony authentikációt
- Biztonságos Guest User lehetőség (pl. HotSpot alkalmazásoknál) a kontroller-ben található alap hozzáférést biztosító web-szerverrel
- Vezetékes és Wi-Fi hozzáférés integráció

3. Wi-Fi behatolás detektálás és megelőzés RF Managerrel és MAP AP/Szenzorral.

- 20 egyidejű WLAN biztonsági támadás blokkolása minden szenzor AP-ban
- 1+1-es tartalékolás megvalósítása RF Managerrel (24/7 konfiguráció)

Központosított WLAN menedzsment a Multiservice kontrollerben

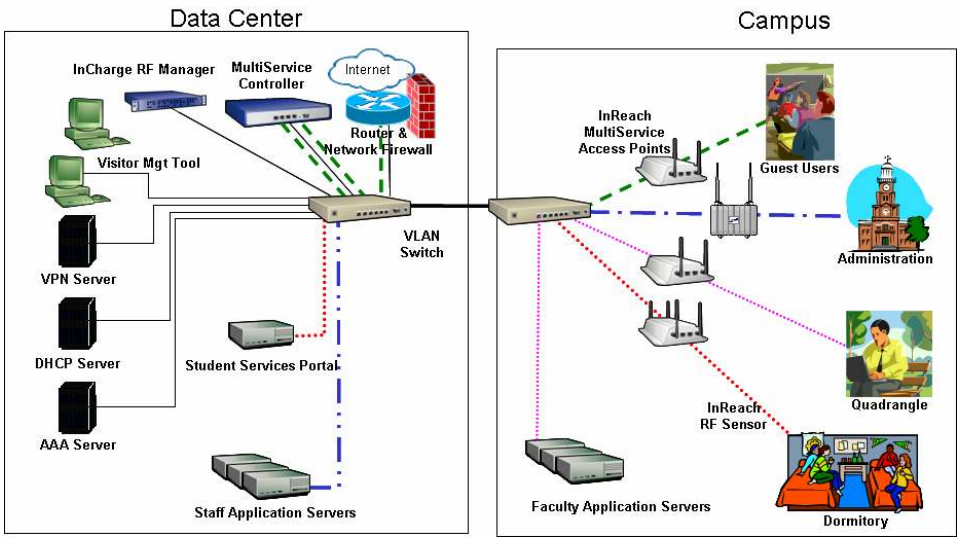
- A központi vezérlő felügyeli a telepített hozzáférési pontokat, gondoskodik azok konfiguráció és firmware menedzsmentjéről is. Az eszközök konfigurációja lehet eszközönként külön-külön egyéni, vagy csoportonként különböző, illetve a hálózat összes elemére kiterjedően közös is. Lehetőség van auto provisioning használatára is, azaz a hálózathoz újonnan csatlakoztatott MAP hozzáférési pontokat a kontroller megfelelő firmware verzióra frissíti és automatikusan beállítja az ügyfél által megadott alapértelmezett konfigurációt.
- A rendszer konfigurálása történhet parancssoros felületen (CLI), vagy egy rendkívül könnyen kezelhető és áttekinthető, webes, grafikus felületen is. A rendszer biztosít SNMP és SOAP felü-letet is.

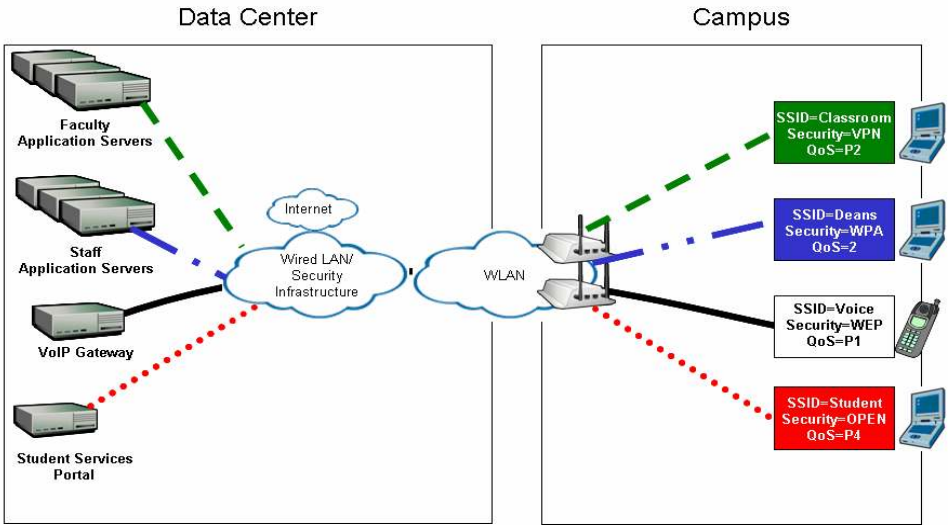
Alkalmazási példák privát és a nyilvános WLAN szolgáltatásra

Egyetemi WLAN megoldás – differenciált és priorizált hozzáférések a hálózati szolgáltatásokhoz, szerverekhez

A SCI-Network által kínált HP ProCurve MSM rendszer egységes rádiós lefedettséget és vezeték nélküli differenciált és biztonságos hozzáférési lehetőséget biztosít a felsőoktatási intézmény vala-mennyi épületében.

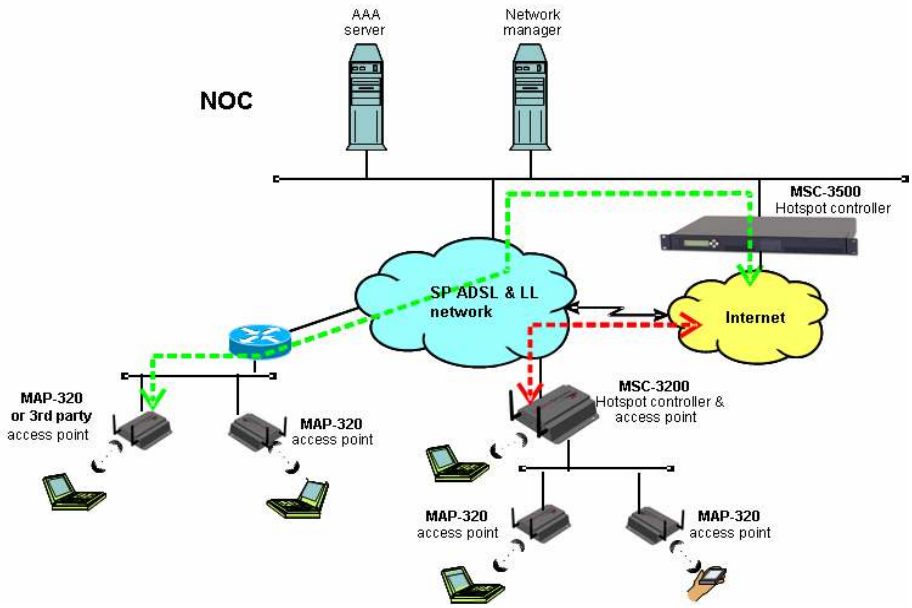
A rendszer különböző szolgáltatásait az egyes karok vagy szervezeti egységek hallgatói és oktatói szabályozottan (pl. helyszín szerint és időben differenciáltan) érhetik el különböző prioritási és biztonsági szintű hozzáféréssel.





A többszörös, virtuális AP technológia alapján a szervezeti egységek rádiós hálózatai egymástól elkülönítve, de a teljes campusban meglévő lefedettséggel jelennek meg. (VLAN wireless környe-zetben)

Távközlési szolgáltatók nyilvános Hot Spot szolgáltatása HP MSM WLAN rendszeren



A megoldás központi eleme az HP ProCurve MSM központi kontroller, ami fogadja és felü-gyeli az alárendelt rádiós access pontok felőli forgalmat.

Az Internet elérést mindaddig blokkolja, amíg a végfelhasználó sikeresen be nem jelentkezett. A bejelentkezés helyétől, a felhasználói azono-sítótól függően – az AAA szerverrel kommuni-kálva – meghatározza a felhasználó lehetősé-geit az alábbiak szerint:

- időkorlátot állíthat be az adott kapcsolatra (session-re) vagy egy meghatá-rozott havi időlimit esetén a felhasznált időt méri
- adatforgalmi kvótákat állíthat be a le- és feltöltési irányokban (szintén adott session-re, vagy egy időszakra vonatkoztatva)
- sebesség és prioritási korlátozásokat érvényesíthet (sávszélesség me-nedzsment az egyes access pontok vagy az egyes felhasználói session-ök számára)

A felhasználói bejelentkezés web böngészőn keresztül történhet. Az internet el-érésének kezdeménye-zésekor egy testre szabható login ablak jelenik meg. A sike-res bejelentkezés után egy tájékoztató ablak

ismerteti a felhasználó idő- és forgalmi korlátait. Ez az ablak periodikusan fris-sül, azaz a felhasználó folyamatosan követheti a kvóták alakulását. A támogatott felhasználói eszköz lehet tetszőleges Wi-Fi-képes notebook, PDA vagy Wi-Fi telefon.

WLAN technológia további felhasználási területei

- Kórházak – helymeghatározó rendszer Wi-Fi technológiával
- Logisztikai központok – Voice over Wi-Fi, helymeghatározás, adattovábbítás
- Térfigyelő rendszerek közterületeken, magán területeken
- Kistérségi internet szolgáltatás, Hot Spotok
- Vállalati alkalmazások (vendég és dolgozói hozzáférések)
- Közlekedési eszközök

és a jövő alkalmazási lehetőségei…..

A HP ProCurve MSM WLAN rendszereit több ezer meghatározó vállalat és intézmény használja világszerte

Beatrix FREGAN

LA CONTRIBUTION DU COLLÈGE EUROPÉEN DE SÉCURITÉ ET DE DÉFENSE À LA CULTURE MILITAIRE EUROPÉENNE

Un rôle majeur a été dévolu au Collège européen de sécurité et de défense (CESD) dans la mise en oeuvre de l'initiative Erasmus militaire.

A l'origine de ce Collège, on trouve la proposition faite en octobre 1991 au Président du Conseil européen par le Président français François Mitterrand et le Chancelier allemand Helmut Kohl de transformer l'Institut de l'Union de l'Europe occidentale en Académie européenne de sécurité et de défense, formulation reprise dans le Traité sur l'Union européenne de 1992.

Il faudra pourtant attendre encore quatorze ans pour voir fonctionner un Collège européen de sécurité et de défense. Pendant ce temps, l'Institut de l'UEO, créé en 1990, sera en fait devenu l'Institut d'études de sécurité de l'Union européenne (IES) et s'inscrira dans le réseau d'instituts, de collèges, d'académies et d'institutions des pays membres de l'UE, géré précisément par le CESD.

On peut décrire le CESD comme un collège virtuel dont la mission est de fournir une formation dans le domaine de la PESD au niveau stratégique, afin de mettre en place et de promouvoir une compréhension commune de la PESD parmi le personnel civil et militaire et de recenser et de diffuser, au moyen de ses activités de formation, les meilleures pratiques en rapport avec diverses questions relevant de la PESD. Il s'agit de renforcer la culture européenne de sécurité dans la PESC et d'offrir aux différentes instances de l'Union européenne ou aux administrations et états-majors des Etats membres un personnel qualifié et efficace, au fait des développements de la PESD.

Le CESD est une construction originale mais encore fragile. Il est le fruit d'un compromis l'ayant privé de toute structure permanente: il est en quelque sorte sans domicile fixe, intermittent (une dizaine de semaines par an), itinérant (accueilli successivement dans des villes européennes différentes) et modulaire (organisé selon plusieurs sessions thématiques). Il dispose d'un secrétariat basé à Bruxelles, dont le noyau comprenait à l'origine quatre personnes, qui sont passées à onze avec le projet Erasmus et dont la mission est de coordonner les initiatives, puis de les diffuser aux différents destinataires.

Les activités de formation du CESD incluent deux types de cours: un cours de haut niveau dans le domaine de la PESD (une fois par an, organisé en cinq modules d'une semaine à travers l'Europe) et un cours d'orientation à vocation plus généraliste (à raison de quatre ou cinq sessions chaque année, soit à Bruxelles soit dans l'une des capitales des Etats membres). La soixantaine de participants retenus pour chacun de ces cours occupent un poste de responsabilité (niveau officier supérieur ou équivalent civil pour le cours d'orientation, niveau colonel ou équivalent civil – haut fonctionnaire – pour le cours de haut niveau).

En outre, le Collège a multiplié les cours spécifiques pour des auditoires spécialisés :

- cours « Press and Public Information »,
- cours pilote sur la réforme des systèmes de sécurité,
- cours sur les processus de planification des opérations militaires de l'Union européenne, etc.

Depuis peu, le Collège prend en charge de nouvelles activités de formation : réunions d'anciens participants et séminaires de haut niveau pour des participants exerçant de très hautes responsabilités dans le domaine de la PESD (niveau Général ou Ambassadeur).

On a considéré qu'il était essentiel que les responsables européens connaissent les mécanismes de la PESD et réfléchissent ensemble au moyen d'améliorer cette politique. Des activités de formation du CESD sont ouvertes par ailleurs aux ressortissants des pays candidats à l'UE et de pays tiers (y compris aux Etats-Unis et à la Chine), voire à certains représentants d'organisations internationales (de l'OTAN à la Ligue arabe).

Ces activités peuvent également accueillir la participation de représentants du monde des affaires, d'organisations non gouvernementales ainsi que des universitaires et des journalistes.

De manière générale, le CESD a permis de rapprocher les instituts nationaux des institutions de l'Union européenne. Ce faisant, il a favorisé une certaine osmose entre ces différents instituts, notamment pour rendre compte de la complexité des problématiques de crise et de leur gestion dans le cadre de la PESD. Il est important de noter en effet qu'une grande partie de ces enseignements concernent les aspects civils de la PESD et leur imbrication avec les compétences militaires. C'est l'une des principales valeurs ajoutées de ce Collège, à la différence du Collège de Défense de l'OTAN (NDC), créé en 1951 et qui a fortement contribué à forger la culture otanienne.

Les formations du CESD peuvent être complétées le cas échéant par d'autres institutions, Etats membres ou instituts communautaires comme le Collège européen de police (CEPOL). Le CESD peut en outre faire autorité pour certifier la qualité des formations délivrées par un Etat membre seul. L'idée d'enseigner la PESD au sein des écoles de formation initiale a toutefois été longtemps négligée.

Jusqu'au lancement de l'initiative militaire inspirée d'Erasmus, les missions du CESD ne concernaient pas le niveau de base de la formation des officiers. Ces derniers sont pourtant appelés à exercer des responsabilités charnières entre les forces et les échelons supérieurs militaires et politiques. Ils sont au coeur de cette compréhension mutuelle qui fonde l'interopérabilité. Désormais, l'Europe devrait veiller à ce qu'un maximum de jeunes officiers puisse recevoir une formation dans le domaine de la PESD.

Programme des cours du CESD

Date et lieu	Module	Institut hôte / Nation
6-10 octobre 2008, Bruxelles	**Module 1 – « Fondamentaux »** • les évolutions récentes de la PESD • les outils communautaires et processus de décision au sein de l'Union européenne • le concept européen de gestion des crises • les organes de la PESD • la PESC • les relations de l'UE avec ses principaux partenaires • les programmes de coopération	*Institut Royal Supérieur de Défense / Koninklijk Hoger Instituut voor Defensie, Belgique*
8-12 décembre 2008, Paris	**Module 2 – « Capacité en matière de gestion des crises »** • la capacité civilo-militaires de la PESD (Civilian Headline Goal 2008 and 2010) • les activités de l'agence européenne de défense • la politique spatiale	*Institut des Hautes Études de Défense Nationale, France*
19-23 janvier 2009, Vienne	**Module 3 – « Contextes régionaux de La PESD »** • les régions d'intérêt stratégique pour l'UE	*Defence Academy, Autriche*
9-13 mars 2009, Rome	**Module 4 – « Les opérations de gestion des crises »** • les opérations civiles et militaires de gestion des crises • les leçons tirées de l'expérience • le rôle du centre d'opération	*ISSMI et Bundesakademie für Sicherungspolitik, Italie*
8-12 juin 2009, Helsinki	**Module 5 – « Perspectives futures pour la PESD »** • l'avenir du concept de gestion des crises • réflexion avec l'ensemble des participants	*National Defence of Poland, Pologne*

Il est rappelé dans la nouvelle Action commune instituant un CESD que le CESD veille à soutenir des programmes d'échange dans le domaine de la PESD

entre les instituts de formation des Etats membres. Aux termes de la Déclaration des Ministres de la défense du 10 novembre 2008, le CESD est appelé à remplir entre autres les missions suivantes en vue de la mise en oeuvre de l'initiative inspirée d'Erasmus:

– procéder à un état des lieux des échanges existants entre écoles nationales de formation initiale des officiers (base de données informatique) ;
– élaborer le module commun de formation sur la PESD ainsi que plusieurs modules traitant d'autres thèmes relatifs aux affaires internationales et les mettre à la disposition des institutions nationales de formation militaire initiale;
– mettre également à leur disposition l'Internet Distance Learning » (IDL) et d'autres outils appropriés pour élargir le champ des supports pédagogiques ;
– constituer, dans le cadre du Conseil académique exécutif, un Groupe de mise en oeuvre, l'IWG (Implementation Working Group). Ce groupe a été effectivement mis sur pied le 5 février2009; il rassemble des représentants d'Etats membres intéressés et s'est réuni pour la première fois le 19 février dernier.

Le Collège est donc appelé à remplir plusieurs fonctions. Outre un rôle d'élaboration et de mise à disposition de différents modules de formation relatifs aux affaires internationales (dont le module PESD, déjà disponible), le Collège est chargé d'administrer une plate-forme d'échange informatique. Cette base de données recense les différentes initiatives venant d'établissements de formation initiale et entrant dans le cadre de l'Erasmus militaire: programmes de formation développés par les écoles militaires de formation initiale, et liste des différentes offres et des demandes de places pour des échanges d'officiers. Enfin, le Collège assure le suivi de la mise en oeuvre générale du projet d'Erasmus militaire dans le cadre de son Conseil académique exécutif.

Un aspect important du travail du Groupe de mise en oeuvre (IWG) consiste à développer un système d'équivalences pour le volet militaire de la formation initiale des officiers en examinant les possibilités de l'actuel système de transfert et d'accumulation de crédits (ECTS). Le Secrétaire général/ Haut représentant pour l'Union européenne rendra un rapport dans le courant de l'année sur la base de l'évaluation et de la réflexion de l'IWG. Ce rapport devrait formuler des propositions visant à supprimer les obstacles administratifs, juridiques et d'autre nature aux échanges, et à prévoir des mécanismes incitatifs inspirés du programme Erasmus. Lors de la réunion du 19 février 2009, des solutions rapidement applicables, ont été définies : tout d'abord la mise en oeuvre du module d'étude sur la PESD, déjà existant, avec l'organisation d'un séminaire consacré aux formateurs; ensuite, la mise en commun des données informatiques avec accès sécurisé aux données relatives aux résultats des questionnaires diffusés, la création d'un forum informatique d'échange d'expérience mis à la disposition des élèves des académies et enfin l'élaboration d'un modèle de convention juridique et administrative pour l'adhésion au programme Erasmus.

Dans les textes, il est prévu que le secrétariat du CESD est assuré par le secrétariat du Conseil de l'UE, les Etats membres et les instituts qui constituent le réseau du CESD; mais dans les faits le CESD manque de soutien administratif.

Le 23 juin 2008, le Conseil, sur la base du rapport soumis en décembre 2007 par le Comité directeur du Collège, a révisé l'Action commune instituant le CESD.

Il s'agissait notamment de conférer au Collège la capacité juridique nécessaire pour conclure des contrats et arrangements administratifs.

Toutefois, ces nouvelles dispositions ne traitent pas tous les aspects liés à la hausse de la demande des Etats membres et aux besoins croissants des personnels et des missions de la PESD. Un nouvel article 13 prévoit donc : « une révision de l'action commune le cas échéant à la lumière d'une étude sur les perspectives du CESD et leurs incidences éventuelles. L'étude porte également sur des points comme le secrétariat, les effectifs, l'exploitation du système IDL, les services de conférence, les arrangements financiers, la gestion et la coordination de la formation dans le domaine de la PESD au niveau de l'Union européenne et l'équilibre civilo-militaire au sein du réseau du CESD; cette étude est réalisée par le Secrétariat général du Conseil et présentée au Conseil par la présidence française.

Ledit rapport d'étude devait être établi en novembre 2008. Il a en fait été rédigé par le secrétariat du CESD et a servi de fondement pour élaborer des recommandations concrètes concernant le Collège. Une version finale du rapport a été diffusée le 1er décembre 2008. S'agissant de l'initiative inspirée d'Erasmus, l'étude reconnaît que la participation du Collège à sa mise en oeuvre ne nécessite pas de ressources supplémentaires: le soutien administratif du Conseil académique exécutif, spécialement configuré pour ce projet, et la gestion d'une base de données peuvent être considérés comme des tâches de secrétariat courantes pouvant être exécutées avec les ressources existantes.

En revanche, l'étude constate de manière plus générale le décalage grandissant entre le développement des activités du Collège et le cadre existant. Ce décalage serait dû au rôle clé joué par les instituts nationaux et au besoin d'équilibrer l'engagement des instituts militaires et civils, à l'accès aux infrastructures de conférence, à l'insuffisance des ressources en personnel, à l'emplacement actuel du secrétariat du Collège.

Le CESD devra disposer dans le futur:

– d'un personnel plus important;
– d'un budget propre financé sur la ligne PESD du budget communautaire qui permettra de couvrir les dépenses prévues pour le fonctionnement du collège ;
– d'une personnalité juridique qui lui permettra de recruter du personnel, de conclure des contrats, d'acquérir des équipements, notamment pédagogiques, ou de détenir un compte bancaire.

Il convient de préciser que le principe de la contribution volontaire des Etats membres n'est pas remis en cause, ce qui permet d'envisager un soutien financier pour des projets spécifiques non couverts par le budget du Collège.

Károly FEKETE

SEVERAL ASPECTS OF DISASTER RECOVERY IN STATIONARY MILITARY COMMUNICATION SYSTEM

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
Strategic networks in military communications system mainly based on microwave, landline, copper and fiber connections. In emergency situations disaster recovery and response require a timely coordination of the emergency services. In this paper we describe several aspects for an integrated military communication and information system, particularly addressing in kind of risks, disasters, connectivity, networking and physical medium issues.

Keywords: Disaster, stationary, communication system, military, recovery, restore, management policy.

Introduction

Shutdowns may be classified as disasters, catastrophes or malfunctions. However, more likely events, including electrical problems, storms, fires, snowstorms, and flooding occur less frequently than hardware failures. The probability of shutdowns occurring regularly is quite significant. In fact, most communication hardware, in consistent use over a period of some years, stands a good chance of having a catastrophic hardware failure. It is typical of military support purchase commercial off the shelf (COTS) and sometime non-brand computers. Most use CD- DVD disks, an inexpensive file server, or a cheap hard drive for backup. Rarely are the backups[96] tested to determine if a system can be rebuilt from scratch, and many times, the backups fail to restore critical data.

Dealing with disasters in stationary military communications system such as natural events, human and technology risks there is a big challenge to military emergency communication services. Up-to-date information needs to be available in real-time for the decisions makers of high level. An integrated military communication and information system for easy plug-in into other systems will establish a good disaster platform for the reliable and secure exchange and processing of information flow.

[96] A copy of files and programs made to facilitate recovery if necessary.

One of the findings was that maintaining communications is the "primary challenge" during a disaster and with the following major requirements we should meet in a satisfactory way:

- Fast data access;
- Timeliness and updating of information;
- Availability of communication, redundancy of links;
- Integration and linking of information;
- Standardization of information.

The main goal is to save resources and to preserve wealth. Other benefits include:

- Developing an appreciation of the military procedures continuation plan as an integral part of the operation plan;
- Closely examining processes, policies, and procedures to ensure requirements are met;
- Developing an awareness of what processes actually impact the operation;

Risks generally fall into three major categories:

- Human[97];
- Technology[98];
- Natural events[99].

The potential Communications Technology disasters and their types among others may be:

- Electrical power failure

[97] Human risks range from “human error” to someone “going postal.” These are the hardest to avoid and sometimes the most expensive to mitigate.

[98] Technology risks run the gamut from a loose connection to a failed system. Technology risks usually can be avoided by redundancy, but that is an expensive option.

[99] Natural events include flooding, the most common risk, and other weather and geological events. Many of these events can be predicted with fairly good accuracy, some of them not.

- Communications services breakdown
- Equipment or System Failure,
- Internal power failure,
- Air conditioning failure
- Production line failure,
- Equipment failure (excluding IT hardware)
- Serious Information Security Incidents
- Cyber crime, Loss of records or data
- Disclosure of sensitive information
- IT system failure

Critical IT Resources

We should identify the following resources as critical, meaning that they support critical military communication processes:

- Optical and copper connections;
- Microwave networks;
- Satellite links;
- Telecommunications management networks;
- General support system[100];
- Authentication/network operating system server (required for military users to have LAN access)
- Database server;
- E-mail, Web, Voice servers and application;
- Desktop computers

[100] An interconnected information resource under the same direct management control, that shares common functionality. It usually includes hardware, software, information, data, applications, communications, facilities, and military users and provides support for a variety of users and/or applications. Individual applications support different mission or operation-related functions. Users may be from the same or different military organizations.

- Switches, routers, gateways;
- Network cabling;
- Electric power;
- Heating, Ventilation, and Air Conditioning system
- Physical security
- Facility.

Connectivity Loss

There is one permanent fact about the network connection in stationary military communication system. It probably will go down. The length of time depends on the main time between failures (MTBF) of communications equipments, stations, complexes.

There are a lot of factors sometimes outside the control of the military service providers that cause the network to go down, including cut cables, backbone outages. With the uncertainty of the telecommunications industry, many military service providers or communication backbone service providers notified military users that within ours, sometime days. Consequently it is critical to have a backup strategy and a contingency plan101 if our operation depends on network connectivity.

Most of military communication professionals think is that wireless microwave networks are inherently more vulnerable and less reliable than parallel landline network counterparts. Given that cable of any type even the fiber optic line is a solid medium, landline military networks must be continuously connected between termination points. Consequently, they are extremely vulnerable to the extreme conditions of ground movement, wind, flooding, snowing, and rain.

Microwave backhaul is preferred for its extended range and high bandwidth, making it capable of supporting both voice and broadband data communications. Microwave backhaul equipment is straightforward to install and configure and, without dependencies on physical infrastructure, there are no obstacles to deployment. First action of disaster recovery of communication lines can be turn to microwave to restore communications because it can be installed within hours, fully restoring communications capabilities, voice, video and data communications.

[101] Management policy and procedures designed to maintain or restore military operations, including communications and computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster.

Digital communications data systems include both internal and external networking, as well as VPN102 systems and other transit communications tools. This category covers different methodologies such as ensuring more than one connection to the outside communication world and making sure that VPN connections can interact with any location that might contain viable data systems.

Physical communications are also important to a successful disaster recovery plan. For example it would be a good solution to use mobile phone systems for backup. Counting on land lines as secondary communication systems is often an option. But we may consider that during large-scale disasters such as terrorist activity, fire, and flood such systems can easily fail.

The other factor what we might take into consideration is that mobile service providers can rapidly restore their critical infrastructures, cell sites and backhaul traffic from these mobile sites103 to the nearest surviving link in the Public Switched Telephone Network, connected to Closed Military Network. An ad-hoc Wi-Fi or WiMAX network can be set up to give everyone in the nearest temporary Internet access.

Of course, nearly every military communication system can fail. That's why using multiple systems offers the highest probability that communications and alerts will get through in an operation.

Conclusions

To decrease of primer impact of future disasters for the survivability of stationary military communication system, there is the way organizations can become better prepared. The most obvious preparatory step is to arrange for ready access to a sufficient inventory of equipment that will be required in the recovery effort, including spare parts, equipments, antennas, mounting hardware and generators.

Most of military organisation with special regards to stationary segment should afford partial or completely redundant connectivity--multiple, high-speed links. However, some form of additional connectivity can almost always be feasible within our expense limits even within defence sphere.

Another aspect that military organizations intended to support communications should often overlook in their planning is communication systems. Military data systems require communication systems to work properly, but organizations rarely neglect to protect them.

[102] Virtual Private Network

[103] A self-contained, transportable shell custom-fitted with the specific IT equipment and telecommunications necessary to provide full recovery capabilities upon notice of a significant disruption.

References

[1] Guttman, E. Autoconfiguration for IP Networking: Enabling, Local Communication, IEEE Internet Computing, May/June 2001.

[2] Mobile Broadband for Emergency and Safety Applications: MESA Project, www.projectmesa.org.

[3] A guide to the perplexed business owner helping your business survive the unexpected shutdown Edited By Eric L. Beser, CEO, ennovate inc.

[4] Augustine, N. Managing the Crisis You Tried to Prevent. Harvard Business Review on Crisis Management, 2000 Harvard Business School Press, Boston.

Formázott: Angol (királysági)

FREGAN Beatrix- FÁBIÁN Éva

A FRANCIA KATONAPOLITIKA VÁLTOZÁSAI

A Francia Köztársaság védelempolitikai elvei között napjainkban az összeurópai közös biztonság és védelempolitikai szempontok kerülnek előtérbe. Mindezek mellett – sajátos szereppel – a NATO politikai szervezetének tagjaként minden szinten törekszik a szövetség eljárásaival, módszereivel, alkalmazási képességeivel a maximális interoperabilitás megvalósítására.

A II. világháborút követően Franciaország védelempolitikáját a hagyományos, világosan behatárolható, masszív és viszonylag kiszámítható fenyegetettség, valamint ellenségkép, azaz a keleti szovjet tömb határozta meg. A '90-es évektől azonban a fenyegetések természete megváltozott, váratlan és hihetetlenül széles skálán mozgó válságok, konfliktusok követték egymást. Bár a fenyegetések egy része hagyományos katonai eszközökkel leküzdhető etatikus jellegű maradt, azonban mára már nyilvánvalóvá vált, hogy a konfliktusok nem pusztán katonai jellegűek.

A francia katonapolitikát átszövő, a nemzetközi kapcsolatokban sajátos színfoltot jelentő kivételesség tudata lépten-nyomon tapasztalható. A második világháborút követően, de legfőképpen Charles de Gaulle tábornok 1958-as elnökké választásával ez a tendencia még inkább erősödött. Franciaország kapcsolatai a világban, az angolszász globalizációt érintően tett lépései és megnyilvánulásai ezt több alkalommal igazolták.

Nicolas Sarkozy köztársasági elnökké választásával új stílus jelent meg a francia jobboldalon. Az V. Köztársaság történelme folyamán eddig még nem fordult elő, hogy alig egy hónappal a sorsdöntő szavazások előtt kormányzati pozícióban lévő államfőjelölt vezesse a népszerűségi listát. HERVÉ COUTAU-BÉGARIE[104] arra hívta fel a figyelmet Nicolas Sarkozy személye kapcsán, hogy a francia nemzetvédelmi politika már korábban körvonalazódott alapjai nem kérdőjeleződnek meg. Ezt a legújabb kiadású Fehér Könyv a Honvédelemről is alátámasztja.

A francia nemzetvédelmi politika prioritásait az alábbiakban foglalhatjuk össze. Az első a nemzeti terület védelme, melynek elsődleges eszköze az elrettentés. E cél elérése érdekében Franciaország önálló, független eszközöket használ, melyeket nem rendel alá semmilyen szövetségi politikának.

A nukleáris csapásmérő erők jelentette reagálási képesség képezi Franciaország függetlenségének és biztonságának végső eszközét, stratégiai önállóságát. Értékelésük szerint ez egyben a nemzet túlélésének alapgaranciája, amely a konfliktus tétjével arányban nem álló veszteségeket helyez kilátásba a Franciaországot, vagy

[104] A politikatudományok és a stratégiai tanulmányok doktora, a katonai gondolkodás fejlődéstörténetének legnagyobb szakértője, számos francia szaklap vezető szerkesztője és igazgatója, a Francia Katonai Akadémia Stratégiai Tanulmányok tanszékének tanszékvezetője, a Sorbonne Egyetem kutatásvezetője.

érdekeit ért agresszió esetén az elégségesség elve alapján. Ennek érdekében az atomütőerő megfelelő szinten tartása ma is kiemelt célt és feladatot jelent, ami egyben hozzájárul Európa biztonságához és a világban kialakult egyensúly fenntartásához. A francia politikai vezetők nyilatkozataikban gyakran hivatkoznak a de Gaulle-i örökségre, amelynek érvényességét ma sem kérdőjelezik meg nukleáris vonatkozásban, bár a nemzetközi környezet átalakulása az atom-ütőerő szerepének rugalmas adaptálását követelte meg az új viszonyokhoz.

A francia védelmi politika másik prioritása a nemzetközi szolidaritás, amelytől minden, a nemzetközi jog tiszteletén alapuló stabilitási politika sikere függ. E tekintetben a francia védelmi diplomácia nagyon intenzív tevékenységére kell utalni, ugyanis Párizs számára a két- illetve többoldalú megállapodások megkötése az afrikai államokkal és az új közép- és kelet-európai demokráciákkal fontos befolyás-érvényesítő eszköznek tekinthető.

Az európai dimenzió, mint prioritás, szervesen kapcsolódik a szolidaritási célkitűzésekhez. Az európai biztonság- és védelempolitika ma már a francia védelempolitika strukturális keretét képezi. Az európai védelmi integráció megvalósítása realitás, a NATO-együttműködés fenntartása mellett a párhuzamosságok elkerülésével céljuk az önálló európai cselekvési képességek létrehozása és kiszélesítése.

A parancsnoki, felderítő és helyzetértékelő eszközök szerepét jelentős megerősítés és fejlesztés jellemzi. Ez egyben az európai szerepvállalás megjelenésének egyik formájaként fogadható el, hiszen a haderőképesség-növelés ezzel megfelel az Európai Tanács 1999. decemberben Helsinkiben elfogadott fő irányelveinek, melyekben meghatározták az európai haderő felállítására vonatkozó direktívákat. A parancsnoki eszközök fejlesztése során a vezetési pontok már nem csak a nemzeti szintű alkalmazásban kapnak szerepet, hanem prioritást kap ezek hadászati, hadműveleti és harcászati szintű multinacionális keretekbe történő integrálása is. A hadműveleti terület digitalizálása (egészen az alegységek szintjéig) kiterjed az informatikai eszközök és rendszerek elleni támadások, illetve azok támadás elleni védelmének biztosítására, a szituációs helyzetek kiértékelésére. A felderítő és helyzetértékelő eszközök fejlesztése területén kiemelt szerepet kap a képi információk megjelenítése és továbbítása; valós idejű, nagy felbontású műholdas (képi) adattovábbítás és fogadás képességének kialakítása; a pilóta nélküli felderítő repülőgépek (dronok) alkalmazása. Ezen a területen a pilóta nélküli francia felderítő repülőeszközök rendszerbe állítása, a nagyfelbontású műholdas felderítő eszközök (HELIOS) telepítése és a GALILEO (független európai kereskedelmi és polgári) navigációs műholdszolgáltatás biztonsági komponensének üzemeltetésében való részvétel fémjelzi a franciák szerepvállalását.

Az erő-áttelepítés és mobilitás-képesség javítása érdekében a haderőfejlesztés során javítani szükséges a légi szállítási képességeket az időszak végére az AIRBUS A-310 és a CASA szállító repülőgépek rendszerbe állításával. A többrendeltetésű szállító repülőgépek között a nagy hatótávolságú és a légi utántöltési képességekkel rendelkező gépek prioritása biztosíthatja a képességek növelését a

kívánt szintre. A haditengerészetnél ezt a képességet a vezetési-, és az egészségügyi kiszolgáló képességek hozzáadásával szükséges elérni.

A megelőzés a védelmi stratégia megvalósításának első szakasza, amelyet az aszimmetrikus fenyegetések megjelenése tett szükségessé. Ez nyújtja továbbá a nemzetközi béke és stabilitás megteremtésére irányuló francia külpolitika eszközét. A közvetett és közvetlen nagykiterjedésű fenyegetések kiújulása elleni állandó készenléthez szükséges a francia, az EU és a NATO-tagországok érdekeit, illetve biztonságát megkérdőjelező válság- és konfliktus helyzetek megelőzése, ezért hatékony felderítésre, önálló helyzetértékelő-képességre van szükség. További erőfeszítések várhatók a humán-, illetve technikai felderítés területén a hadászati és hadműveleti szintű adatok megszerzésére képes eszközök esetében is. A terrorizmus elleni küzdelem területén folytatódik a kormányközi egyeztetés, összehangolják a készenléti és riasztási képességeket európai szinten, különös tekintettel az információk kölcsönös cseréjére, hogy ellenőrizhessék a transznacionális hálózatokat.

A védelmi diplomácia a külföldi partnerekkel a védelmi és biztonságerősítő kapcsolatok fejlesztése révén valósul meg megelőző védelmi diplomácia keretében (kölcsönös katonai együttműködés a partnerországokkal, segítségnyújtás, információcsere). Az előretolt összhaderőnemi erők fenntartása, állomásoztatása megkönnyíti a felderítési adatok megszerzését, a közvetlen és gyorsreagálási képesség fenntartását az érintett térségekben. Erőfeszítések történnek a műholdas megfigyelő és felderítő eszközök fejlesztése érdekében is (pl.:C3R[105] rendszerek, programok folytatása).

[105] Commandement, Conduite Communication et Renseignement – Vezetés, irányítás, kommunikáció és felderítés

SZÖLLŐSI Sándor

TÁBORI HÍRRENDSZEREK POWERLINE[106] ÉS 802.11N TÍPUSÚ WIFI HÁLÓZATOK KOMBINÁLT ALKALMAZÁSI LEHETŐSÉGEI

Napjaink szűkös pénzügyi lehetőségei rákényszerítenek bennünket arra, hogy a meglévő kevésbé korszerű (vagy már eleve korszerűtlen) eszközeink teljes lecserélése helyett megpróbáljunk ***alacsony beruházási igényű, a rendszerben tarthatóság idejét kiterjesztő megoldásokat*** is keresni. Ezen esetekben azonban nem elhanyagolható kérdés az sem, hogy a korszerűtlen technika esetleges cseréje/kivonása esetén ***az új kiegészítő rendszerelemek*** korszerű módon ***továbbra is felhasználhatók legyenek***, ne kerüljenek a felesleges beruházások soraiba. Ennek a fajta beruházási módnak természetesen nem szabad öncélúnak lennie. Csak abban az esetben szabad és kell belekezdeni, ha a korszerűtlen jelenlegi technikai háttér képességeit ki tudjuk terjeszteni, a vezetés támogatottsági szintjét magasabb és megbízhatóbb műszaki szintre tudjuk emelni úgy, hogy perspektivikusan, a technikai fejlődés/fejlesztés során megőrizze értékeit, az új eszközparkhoz és megoldásokhoz illeszthető legyen, valamint műszakilag feleljen meg napjaink (és várhatóan a jövőbeli) biztonsági, katonai kihívásoknak, szövetségi elvárásoknak, együttműködési igényeknek.

A Magyar Honvédség jelenlegi mobil és stabil rendszereit tekintve azt mondhatjuk, hogy a híradást tekintve a ***tábori rendszereink területén több évtizedes műszaki elmaradásunk*** *v*an[107] a fejlett világ katonai és civil műszaki infokommunikációs színvonalát tekintve. Eszközeink túlnyomó része a ’60-as, ’70-es évek terméke, nem kívánom részletesen felsorolni a rendszerben lévő híradó eszközöket és azok gyártási évét. Ez a tény már önmagában is komoly biztonsági kockázatot jelent az országra nézve, mert a vezetés ilyen irányú támogatottságának alacsony szintje bizonytalanná, kétségessé teszi ***valóságos harci körülmények között*** katonai sikerek elérését, megtartását, vagy akár a csapatok megóvását. Az a vezető, aki nem rendelkezik valós idejű és hiteles információkkal, nagy valószínűséggel hoz rossz, az ellenség számára kedvező döntéseket. Az a harcot végrehajtó katona, akit nem vezetnek, vagy látja a rossz döntéseket, de nem tehet annak érdekében semmit, hogy tájékoztatni tudja vezetőit a valós eseményekről, nem katona, csak áldozat, vagy esetleg „hős”, aki elszigetelve kitart az utolsó lőszerig. A mi kis létszámú hadseregünk ilyen helyzetet nem engedhet meg magának, mert az hazardírozást jelentene az embereink életével és következményként az ország biztonságával. A probléma másik oldala az, hogy katonáink látják a civil környezetben elérhető és naponta használt műszaki megoldásokat, vele élnek, így nehezen elfogadtatható a munkájuk során kezükbe kerülő technikai eszközök alacsony műszaki

[106]PowerLine távközlési technológia: Power Line Communications - PLC

[107]A 2014-ig tervezett digitalizálást célzó fejlesztések tényleges befejezése nem valószínűsíthető.

és erkölcsi értéke. Ők is nagyon jól tudják, hogy alkalomadtán a hatékony kommunikáción múlhat akár az életük is.

Jelenleg döntően financiális okok miatt a fenti szempontok háttérbe szorulnak, csak a külföldi szerepvállalásainkban van kimutatható minőségi ugrás. Ezért úgy gondolom, hogy erkölcsi és szakmai kihívás minden olyan lehetőségre felhívni a katonai döntéshozók figyelmét, mely viszonylag olcsón, rövid időn belül megvalósíthatóan ad jelentős többlet lehetőséget a katonai vezetők kezébe tábori körülmények között, akár Magyarországon is.

Megvizsgálva a tábori vezetési pontok rendszerének jelenlegi struktúráját és figyelembe véve a korábbi híradó- és informatikai koncepcionális elgondolásokat, valamint ismerve az infokommunikációs rendszerek várható fejlődési trendjeit úgy gondolom, hogy a vezetékes rendszerek kora a tábori vezetési struktúrákban lejárt. Ma már alkalmatlanok és képtelenek alkalmazkodni az új típusú biztonsági kihívásokból adódó és elvárható dinamikus, igen nagy műszaki rugalmasságot igénylő harctevékenység biztosítására. Nem várható – és értelmetlen lenne – nagytávolságú vezetékes gerinchálózatok kiépítése, hiszen sem létszámviszonyaink, sem műszaki eszközeink, sem a harctevékenységek során megvalósuló gyors térbeli és időbeli változások nem adnak lehetőséget és módot ilyen jellegű feladatok végrehajtására. Más részről külföldi katonai feladataink során fel sem merül ezek használata, hazai környezetben pedig támaszkodhatunk a saját állandó telepítésű zártcélú hálózatainkra és a polgári szolgáltatók rendszereire is. A kérdést tovább boncolgatva és a korábbi fejlesztési elgondolásokat átnézve azt láthatjuk, hogy a kisebb távolságokra telepített – vezetési pontok belső struktúráját kiszolgáló – vezetékes rendszerek kérdése nyitott, annak lehetséges műszaki kialakításaival, korszerű vezetékes, vagy vezeték nélküli megoldásokkal (UTP, STP, optikai kábelek, WiMAX és WiFi megoldások, stb.) már több kollégámmal együtt részleteiben is foglalkoztunk.

Az újabb kérdés az, hogy van-e olyan megbízható és lehetőleg olcsó műszaki lehetőség, mellyel az analóg tábori rendszereinkben jelenleg alkalmazott, kiépítésre kerülő vezetékes rendszerek teljesen, vagy jelentős részben kiválthatóak lennének. Az sem lenne baj, ha a jelenlegi, alapvetően távbeszélő funkciót biztosító analóg vezetékes rendszereket helyettesítő megoldás valamilyen módon a beszéd mellett a minél gyorsabb[108] adatátvitelt is támogatná. A legjobb pedig az lenne, ha ez ráadásul IP alapú lenne[109]. Az IP képesség azért is szempont, mert az állandó rendszereinknél folyamatban van az ISDN-től az IP felé történő elmozdulás[110] és természetesen a tábori rendszerek felkapcsolódását az állandó rendszerek felé biztosítani kell a jövőben is, lehetőleg műszakilag minél egyszerűbben. Ezt az IP-IP struktúra

[108]Az analóg géptávíró, esetleg modemes átvitelnél, de az ISDN BRA és PRA lehetőségekhez képest is mindenképpen gyorsabb esetben indokolt a beruházás, mert ekkor „informatikai igényeket" is képes lehet kiszolgálni.

[109]Számolva azzal, hogy az infokommunikációs rendszerekben várhatóan egyeduralkodóvá fog válni ez az átviteli mód, így hosszú távon perspektivikus rendszerelemeket vehetünk figyelembe.

[110]pld.: HICOM-HIPATH evolúció.

feltétel nélkül képes megtenni, önmagával általában minden rendszer kompatibilis… Ebben az esetben lehetne a mostani analóg tábori rendszerünk olcsón ***„kvázi-digitális[111]", elsősorban a vezetési pontokon és környezetükben.*** Ráadásul ez a megoldás, gazdaságossági szempontok szerint is – eszköz sokféleség csökkenése, kevesebb a speciális, a különböző típusú rendszerek közti átjárást biztosító interfész iránti igény, ebből is következően a korábbiakhoz képest kevesebb raktározási, logisztikai probléma – kifizetődőnek látszik.

Ha a felsorolt feltételek szerint ki tudunk váltani eddigi vezetékes telepítési feladatokat, vagy akár a híradó járművek közötti kommunikációs (jelenleg elsősorban beszédalapú) kapcsolatrendszert támogató vezetékek kiépítését, akkor akár a rendszerek le- és áttelepítésére fordított idő is csökkenthetővé válna, ráadásul a már döntően elavult vezetékes anyagok és eszközök kivonásra kerülhetnének, a hozzá rendszeresített állomány más irányú (gyors!) átképzésével pedig az új eszközök telepítése, üzemeltetése megoldhatóvá válik. Az alkalmazandó eszközök kis mérete a járműpark csökkentését is magával hozza.

Láthatóan nagyon szépen hangzó lehetőségeket lehetne ráépíteni a meglévő tábori struktúráinkra, ha valóban létezik rá jó megoldás. Áttekintve a napjainkban fellelhető legújabb távközlési és informatikai eljárásokat, egy mostanra már egyre inkább kiforrott néhány éves technológia (PowerLine) és az egyik legújabb, elterjedőben lévő 802.11n WiFi szabványú hálózati megoldás kombinált és több elemében az általános felhasználói eljárásoktól eltérő együttes alkalmazása tűnik a leghasználhatóbb megoldásnak. A továbbiakban ezen együttes alkalmazhatóság kérdéseivel kívánok foglalkozni.

PowerLine hálózati elv lényegi elemei, sajátosságai

A PowerLine hálózatok alaplényege az, hogy az elektromos (villamos-energia továbbító) hálózaton biztosít adatátvitelt. Napjainkra a technológiák és gyártói csoportok is kialakultak. Az eszközök valódi és neves gyártókhoz kötöttek. Pld. már 2002-ben a HomePlug Powerline Alliance szervezetnek több száz cég volt a tagja, többek között a Compaq, az Intel, a Motorola, a Cisco Systems, a 3Com, stb., így a piacon ma már ennek megfelelően igen széles a választék. Viszonylag friss a kapcsolódó szabvány (IEEE P1901), hiszen 2009 júliusában ratifikálták [1][2]. A legismertebb változatai (mely sorrend a fejlődési lépcsőket is mutatja) a következők:

1. HomePlug 1.0
2. HomePlug 1.0 Turbo
3. ***HomePlug AV[112]***

[111] A rendszerben eddig is meglévő analóg rádiók cseréje lassan folyamatban van, miközben az analóg rádiórelé eszközök egyelőre nem változnak és a „belső" kistávolságú műszaki struktúra radikális átalakításon megy keresztül.

[112] A ma elérhető legfrissebb változathoz is léteznek már valós fizikai eszközök.

4. HomePlug AV2 (még csak tervezet, 2010-2011 körül várható ilyen eszközök megjelenése, Gbit/s átviteli sebességű hálózatokhoz)

A ma elérhető típusok esetén 14 Mbit/s, 85 Mbit/s és 200 Mbit/s ***elméleti*** átviteli sebességet adnak meg a gyártók***, a legutóbbi változatot (AV) VoIP[113] és videó átvitelre[114] is*** ajánlják. Az eszközök felülről kompatibilisek. A leírások alapján általában max. 200 m-es fizikai távolság lehet két adapter között repeater eszköz nélkül és ugyanazon a hálózaton (fázison) legfeljebb 16 eszköz működhet egy időben. Tipikusan 128 bites AES[115] kódolással lehet védeni a hálózatot az illetéktelen behatolók ellen. A hálózati frekvencia (50 Hz) fölötti tartományban történik az adatátvitel. A legújabb verziók többnyire rendelkeznek beépített hálózati interferencia-szűrővel, az elektromos fogyasztók által okozott káros hatások kivédése érdekében. A sok elektromos elosztón történő vezetékes kapcsolat átviteli sebesség csökkenést eredményez, továbbá a villanyórák (árammérők), transzformátorok a legtöbb esetben fizikai gátat szabnak, vagy jelentős szint csökkenést okoznak a továbbítása során. Szerencsére lehetőség van OFDM[116] eljárással, vagy bridge-ek alkalmazásával a problémás áramköri részeknél is átvitelre (transzformátorok), vagy az árammérők esetén is a jel átvezetésére [3]. Alapesetben csak az azonos fázison lévő eszközök képesek az együttműködésre.

A 802.11n WiFi hálózatok lényegi elemei, sajátosságai

Az új WiFi szabvány annyira friss, hogy 2009. szeptemberében került jóváhagyásra az utolsó, 11.0-ás tervezet (7 évi vita és egyezkedés után...). Elméleti legnagyobb átviteli sebessége 600 Mbit/s, amit 4 adó és 4 vevőantennával, egyidejűleg 4 rádiócsatorna alkalmazásával érhető el (MIMO[117]). Ezen eszközök is ismerik az AES titkosítást, felülről kompatibilisek a korábbi 802.11 a/b/g szabványú eszközökkel. A hálózati eszköz gyártók jelentős része már közel két éve forgalmazza a még szabványosítás előtti, 2.0-ás, a végleges szabványverzióhoz közel álló berendezéseit, így egyre több tapasztalattal és egyre megbízhatóbb minőségű eszközökkel rendelkeznek. A tervezet szerint a már legyártott eszközök szoftverének frissítése (firmware) biztosítja a végleges szabványnak való megfeleltetést. A csatornák dinamikus váltogatásával (DFS2[118]) egyszerre használja a jelentősen túlterhelt 2,4 GHz-es és a jelenleg alig kihasznált 5 GHz-es sávokat. Szabadtéri (kültéri) akadálymentes terjedés esetén a hatótávolság kb. 250 m, de ezt természetesen a beépített (körsugárzó) botantennák segítségével éri el. Léteznek már olyan berendezések is, hogy ***szektorsugárzást*** biztosító, mindkét frekvenciát kihasználó antenna típus rákötését is támogatják, melyek így gyártói adat szerint 400-450 m körüli hatótávolság elérését teszik lehetővé.

[113] Gond nélkül kiválthatja az eddigi analóg távbeszélő funkciókat is.
[114] Valós idejű videojel továbbításához is ideális eszköznek tűnik.
[115] Advanced Encryption Standard
[116] Orthogonal Frequency Division Multiplexing
[117] Multiple Input, Multiple Output
[118] Dynamic Frequency Selection

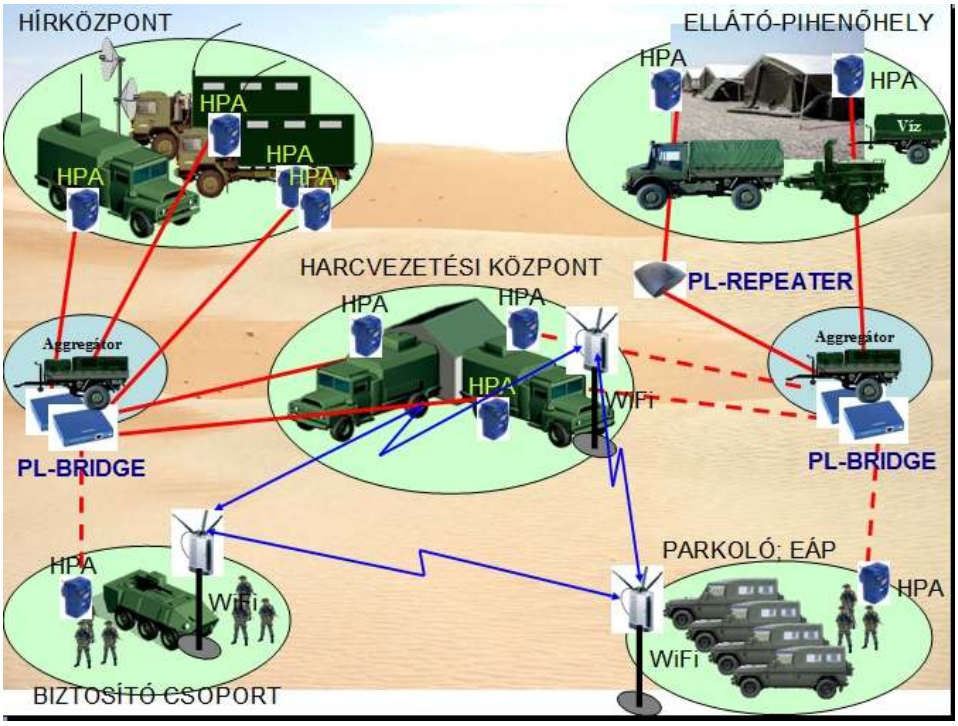
1. ábra Példa irányított, 6-8 dBi nyereségű 802.11n hálózathoz illeszthető antennára (Level One WAN-1160 irányított antenna; CP Technologies)[4]

A technológia alkalmazhatósága katonai, tábori körülmények között

A korábbi megfontolások és a tömör technikai ismertető után az a kérdés, hogy az elvárások és a technikai-technológiai fejlettségből adódó képességek megfeleltethetőek-e egymásnak. Ahhoz, hogy erre korrekt választ tudjunk adni, meg kell vizsgálni az alkalmazási környezetet, amihez egy hipotetikus vezetési pont rendszert vegyünk modellnek.

Kiindulásként, mint általános szervezési elvet figyelembe kell venni azt, hogy milyen csoportokat kell létrehozni egy ***általános analóg vezetési pont technikai rendszerében***. Általános elvnek kell tekinteni, hogy szükség van vezetési, híradó, valamint biztosító és kiszolgáló csoportok létrehozására, azokat működtetni kell, miközben köztük is meg kell oldani az információáramlást. A feladataik ellátására villamos energiára is szükségük van attól függetlenül, hogy járművekre, sátrakba, vagy konténerekbe települnek. Ez már önmagában egy viszonylag kis területre koncentrálódó elektromos hálózat kiépítési kényszerét hozza magával, mely a korábbi megfontolások szerint infokommunikációs hálózattá is alakítható. A következő elvi vázlat egy ilyen jellegű rendszer aggregátoros tápellátó megoldás esetén történő megvalósíthatóságát mutatja be. Ezen ábrán – hely hiányában – nem részleteztem a HomePLugAdapterek (HPA) esetén az eszközök szabványos Fast-Ethernet portjára felfűzhető routereket (amik természetesen WiFi eszközök is lehetnek, pld. 802.11n típusúak is), vagy más elképzelhető hálózati elemeket.

Az aggregátorok esetén PowerLine Bridge (PL-BRIDGE) eszközök segítségével (is) oldható meg a korábban jelzett, az áramellátó csomópontok esetén fellépő jelszint csökkenés vagy megszakadás elhárítása, valamint az eltérő fázisokra felfűzött adatátviteli vonalak közti átjárás. Hosszabb áramellátó vonalak esetén szükség lehet a jelfolyamba regeneráló eszközök (PL-REPEATER) beiktatására, figyelembe véve a jelenlegi 200 m-es távolságkorlátot.



2. ábra Példa egy eredetileg analóg vezetési struktúra „kvázi-digitális” átalakítására

Azon esetekben, ahol nem áll rendelkezésre, vagy nem indokolt az áramellátást központi rendszerből megoldani (a példaábrán ilyennek tüntettem fel a biztosító csoportot és a parkolót az ellenőrző-áteresztő ponttal), szükség esetén lehetőség van akár valós idejű videokapcsolat kialakítására is az új típusú 802.11n típusú WiFi hálózattal, irányított, nagy nyereségű antennák[119] alkalmazása mellett (max. 100 mW kimenő teljesítmény esetén, az általános előírás szerint [5]). Az antennát magával a készülékkel egy egyszerű, nem túl magas antennaárbocra (vagy gépkocsi tetejére, szükség esetén onnan kiemelve) telepítve, a láthatóság biztosítása mellet akár 1-2 km hatótávolság is elérhető lehet. A megoldás a példaábrán feltüntetett csoportokon belüli kis távolságú adatátviteli rendszer kialakítására is biztonsággal alkalmazható, hiszen a területlefedő jelleg esetén elég közel kellene jutni hozzá, hogy lehallgathatóvá és esetleg feltörhetővé váljon, miközben a csatornák önmagukban is titkosítottak (AES) és a végkészülékek is rendelkezhetnek információvédelmi megoldásokkal. Ez akár egy zászlóalj szint esetén sem tűnik túl életszerűnek, figyelembe véve a vezetési pontok körül kialakítható védelmi zónákat. A csatornák ilyen jellegű többszörözése (vezetékes és vezeték nélküli) még ledobott automata

[119] Pld. panel antenna, parabola antenna, Yagi antenna, stb.

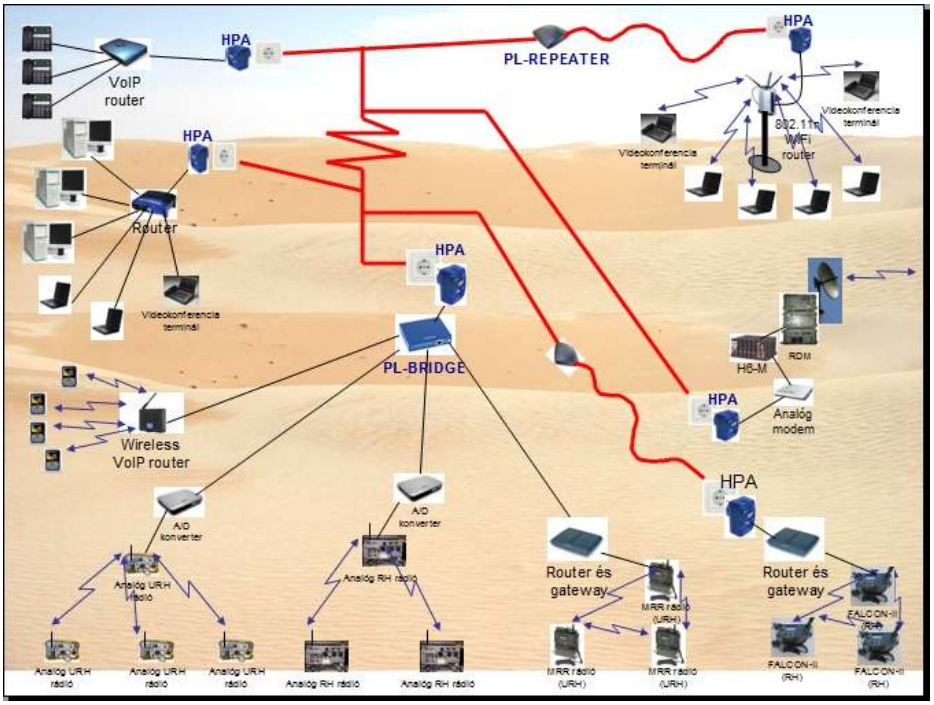
zavaró eszközökkel történő zavarás esetén is jelentősen növelheti a rendszer megbízhatósági szintjét.

A jelenleg már több gyakorlaton alkalmazott informatikai rendszergépkocsi – az áramellátó csomópont problémaköre miatt – átcsoportosítása az aggregátorcsoport közelébe indokoltnak látszik, ezzel a gyors beavatkozás feltételei adottak lehetnek. Az eddigi analóg (tipikusan 40 vonalas) távbeszélő központ gépkocsik kiváltása csak úgy lehetséges, ha a (belső) rendszerből való „kilépés" a nagytávolságú vonalak felé routerekkel támogatott. Ezt az indokolja, hogy a belső hálózat az új elképzelésekben IP eszközökre támaszkodik, így azok elérése (megcímzése) közvetlen módon máshogy nem megvalósítható. Ezen routereket az informatikai rendszergépkocsi készletében célszerű tartani, beállításuk is az ottani kezelői szakállomány feladata lehet. Egyben ide koncentrálható a digitalizált tábori infokommunikációs rendszer-rész hálózatfelügyelete is, hiszen pld. a beépítendő routerek egyszerű felületen keresztül távmenedzselhetők is.

A nagysebességű digitális rendszerből történő kilépés az analóg gerinchálózatok felé sajnos csak megfelelő, pld. IP/FDM[120] átalakító eszközök beiktatásával oldhatók meg. Itt is a legkisebb (szűk) keresztmetszet adja a „külső" hálózat áteresztő kapacitását, ami elméletileg legfeljebb 12 kHz-es „szélessávú" csatornát jelenthet, elméleti (PCM) 192 kbit/s sebességgel. Ilyen képességű katonai modemes eszköz létéről nincs ismeretem, de esetleg célszerű lenne kialakítani, miáltal analóg modemes technikával lehetőség lenne a mostaninál hatékonyabb analóg reléstruktúra kialakítására, az eszközök alkalmazhatósági idejének és a műszaki képességek növelése érdekében (a tábori analóg rádiórelék lecserélésének ütemezéséről nincs új információm).

A rádiókat tekintve erőltetni kell az új típusú eszközök alkalmazását, hiszen mind az MRR, mind a FALCON-II. család alkalmas adatátvitelre, minimális műszaki beruházással (pld. IP/X.25 GATEWAY) bekapcsolhatóvá válik az új struktúrához. A régi eszközökhöz is lehet speciális A/D átalakítókat alkalmazni, de megítélésem szerint felesleges beruházást jelent, tekintve ezen analóg rádiók alacsony katonai-műszaki értékét, csekély zavarállóságát, zavarérzékenységét, műszaki elavultságát. A következő ábrán a teljes rendszer elvi csatlakozási felületeit ábrázoltam egy változatban, a mögöttes kiszolgálandó felhasználói csoportok feltüntetése nélkül, egyfajta általános technikai vázlatként, tipikus kapcsolódási módokkal.

[120] H-6M távbeszélő vivőző berendezés pld. a relécsatornák felé.



3. ábra Egy elvi rendszervázlat az alapvető rendszerelemek feltüntetésével

Összességében – megítélésem szerint – a felvázolt új struktúra viszonylag olcsón megvalósítható, a rendszer képességei pozitív választ adnak a korábban ismertetett kérdéseimre. A technikai fejlődés IP felé történő elmozdulása ebben az esetben „alulról felfelé" történik, viszonylag alacsony beruházási költségek mellett, akár teljesen kommersz[121] eszközökkel. Lényegesen kisebb tételt jelentene, mint a korábbi híradó és informatikai fejlesztési tervekben szereplő tábori rácsponti hálózat komplex megvalósítása, de természetesen a nagytávolságú vezetési rendszer és műszaki megoldások alapvető változtatása nélkül. Az alapvetően analóg gerinchálózati eszközparkhoz az illesztés műszakilag megvalósítható, de kiegészítő (eszközszintű) elemeket igényel. Sajnos ezen elemek egy része esetleges rendszerfejlesztés (digitalizálás) esetén nem használhatók tovább, hiszen eszközspecifikusak (pld. "relé-modem", vagy esetleges analóg rádiók illesztését biztosító A/D átalakítók, stb.).

A leírt eljárásokkal kapcsolatban „otthoni" és „irodai" környezetben történő néhány alkalmazási módot, valamint – főleg az átviteli sebességre vonatkozó – méréseket és teszteket lehet találni számítógépes szakfolyóiratokban, vagy akár az interneten, pld. fórumokon is. Ezekből sajnos a sajátos katonai körülményekre vonatkozóan csak nem tudunk leszűrni konkrét következtetéseket. Ebből is adódóan – az elvi megfontolások mellett – az elképzelés további gyakorlati vizsgálatokat

[121] Itt nem katonai, hanem köznapi, civil kivitel értendő alatta

igényel a tábori katonai specifikumok figyelembevétele mellet, hiszen nem tisztázott, hogy pld. a jelenleg nem túl korszerű és jelentős interferenciát is létrehozó aggregátoraink hatásait mennyire képesek az eszközök kiszűrni, vagy az, hogy a híradó állomásokon a Magyar Katonai Szabványban kötelezően és gyakorlatban alkalmazott életvédelmi berendezések milyen mértékben befolyásolják az adatátvitelt. Az ilyen és ehhez hasonló kapcsolódó problémakör tisztázása, a nyitott kérdésekre történő válaszadás után lehet csak egyértelmű választ adni a gyakorlati megvalósítás tényleges lehetőségeire és reményeim szerint a rendszer bevezetésére, ami nagy lépés lehetne a Magyar Honvédség számára egy digitális tábori rendszer kialakítása felé.

Irodalomjegyzék

[1] http://www.homeplug.org/home; 2009. 09. 23

[2] http://en.wikipedia.org/wiki/HomePlug_Powerline_Alliance#1.0; 2009. 09. 23

[3] Telbisz Ferenc (KFKI RMKI Számítógép Hálózati Központ és Magyar Telekom PKI-FI): Új szélessávú kommunikációs közeg: az erősáramú tápvezeték; Networkshop 2008; https://nws.niif.hu/ncd2008/docs/phu/026.pdf; 2009.09. 21

[4] http://www.cptechusa.com/cpt/index.php?page=shop.product_details&flypage=flypage.tpl&product_id=109&category_id=99&option=com_virtuemart&Itemid=10080; 2009. 09. 23

[5] Nemzeti Hírközlési Hatóság: Tájékoztató: Szélessávú adatátvitel rádiós hozzáférési eszközökkel (RLAN, WiFi, WMAN, WiMAX ...); 2007. 03. 09.

SCI-Network Távközlési és Hálózat-integrációs zRt.

http://www.scinetwork.hu/

info@scinetwork.hu

A SCI-Network Távközlési és Hálózatintegrációs zRt. hálózati rendszerintegrációval foglalkozó szakértő vállalkozás. A szűkebb értelemben vett hálózati rendszerek mellett a cég alaptevékenységébe tartozik a mikrohullámú átvitel, a hálózati biztonság és a rendszerfelügyelet is. A SCI-Network teljeskörű szolgáltatást nyújt ügyfeleinek a hálózatok terén a feladat felmérésétől kezdve, a tervezésen, eszközszállításon, üzembehelyezésen, oktatáson keresztül a garanciális és garancián túli szolgáltatásokig. A folyamatosan gyarapodó létszámmal, bővülő ügyfélkörrel és növekvő forgalommal rendelkező vállalat az informatikai vállalkozások felső harmadába tartozik.

A SCI-Network célja, hogy ügyfelei számára magas színvonalú megoldásokat biztosítson, valamint megismertesse kiváló minőségű termékeit és szolgáltatásait leendő ügyfeleivel.

A vállalat kiemelt figyelmet fordít a minőségbiztosításra, melyet ISO 9001 és AQAP2110 minősítése is tükröz.

EMCOM 2009
III. Veszélyhelyzeti Kommunikáció Nemzetközi Konferencia
2009. november 11-13., Hévíz

A Budapesti Műszaki Főiskola Kandó Kálmán Villamosmérnöki Kar és a Hírközlési és Informatikai Tudományos Egyesület közös szervezésében idén is megrendezésre kerül a Veszélyhelyzeti Kommunikáció (EMCOM'2009) konferencia. Az immár nemzetközi rangúvá emelt szakmai fórumon neves meghívott magyar és külföldi előadók tartanak előadásokat. A rendezvény fő támogatója a Nemzeti Hírközlési Hatóság.

TERVEZETT ELŐADÁSOK:

1. Szabó András (igazgató, fejlesztésvezető, HUNGAROCOM)
   Centralizált kommunikáció rögzítés az EDR-ben. A pilot rendszer tapasztalatai
2. Vereckei Béla (NHH Biztonsági Igazgatóság)
   Kormányzati feladatok (szabályozás, EU és NATO feladatok harmonizációja, végrehajtása)
3. Dr. Kladek András (NHH Biztonsági Igazgatóság)
   Elektronikus hírközlési szolgáltatók veszélyhelyzeti felkészítése
4. Győrbíró László (NHH Azonosító Szabályozási és Gazdálkodási Osztály)
   Lakossági segélykérő rendszerek helyzete, fejlesztése különös tekintettel a 112-es európai segélyhívó rendszerre
5. Pintér István (NHH Biztonsági Igazgatóság)
   Lakossági riasztási rendszerek műsorszóró és egyéb hírközlési hálózatokon keresztül (mobil, Internet)
6. Dr. Maros Dóra, (dékánhelyettes, BMF- KVK)
   Kritikus infrastruktúrák felügyeleti rendszermérnök master képzés kidolgozásának kérdései a BMF Kandó Kálmán Villamosmérnöki Karon
7. Jamrik Péter (vezérigazgató, NOVOFER Távközlési Innovációs ZRt.)
   Legyen a Balaton Európa legbiztonságosabb tava, a Balaton Fejlesztési Tanács Komplex Vízbiztonsági Programjának infokommunikációs fejlesztései
8. Lázár János (kereskedelmi igazgató), Zautasvili Péter (fejlesztési igazgató, Hungaro DigiTel Kft.)
   A műholdas kommunikáció szerepe a védelmi szektorban
9. Manfred Blaha (technology advisor, National Crisis and Disaster Prevention Management, Federal Ministry of Interior, Austria)
   Austria's Public safety- networked for crisis and disaster management
10. Manfred Blaha (technology advisor, National Crisis and Disaster Prevention Management, Federal Ministry of Interior, Austria)
    The role of Public Safety Communication Europe (PSCE) Forum in emergency communications
11. Tóth Csaba (osztályvezető, KeKKH)
    Veszélyhelyzeti kommunikáció a készenléti szervezetek között, EDR tapasztalatok
12. Prajczer Tamás (ügyvezető igazgató, GeoX Kft.)

Digitális térképek a védelmi és segítségnyújtási alkalmazásokban

13. Illési Zsolt (ügyvezető, Proteus Consulting Kft.)
Mobil telefonok igazságügyi szakértői vizsgálata
14. Varga Péter János (tudományos szakértő, BMF-KVK)
A kritikus infrastruktúrák és a vezeték nélküli hálózat kapcsolata
15. Szekeres Balázs (műszaki igazgató, PTA CERT-Hungary)
A PTA CERT-Hungary Központ szerepe a magyar kritikus informatikai infrastruktúra védelemben
16. Dr. Suba Ferenc (testületi elnök, PTA CERT-Hungary)
Nemzetközi és hazai szabályozás, együttműködés a kritikus infrastruktúra védelem területén
17. Dr Bognár Zoltán (ügyvezető, Hírközlési Mérő és Szolgáltató Kft)
Segélyhívás - az állam részvétele
18. Gyányi Sándor (adjunktus, BMF-KVK)
Botnetek felderítése és lokalizálása
19. Dr. Wührl Tibor (docens, BMF-KVK)
Előfizetői hozzáférési pontok működés folytonossága
20. Dr. Muha Lajos (főiskolai tanár, tanszékvezető, ZMNE, Bolyai János Katonai Műszaki Kar)
A kritikus információs infrastruktúrák azonosítása
21. Dr. Takács Márta (főiskolai tanár, BMF-NIK):
Soft computing technológiák a vészhelyzeti kommunikációban
22. Breitner Gábor (ügyvezető, GPSCOM Kft.)
Mobil műholdas távközlés alkalmazása a vészhelyzeti kommunikációban
ZETRON DCS5020 digitális diszpécseri munkaállomás TETRA hálózathoz
23. Dr. Rajnai Zoltán (egyetemi docens, tanszékvezető, ZMNE)
A védelmi szféra fejlesztéseinek technológiai és frekvenciabiztosítási kérdései
24. Dr. univ. Dsupin Ottó (c. egyetemi docens, titkárságvezető, Önkormányzati Minisztérium)
A kritikus infrastruktúra védelme – mint a védelmi igazgatás új aspektusa
25. Kneisz Ferenc (Stratégia referens, MeH, Infokommunikációért és E-közigazgatásért Felelős Szakállamtitkárság)
A kritikus információs infrastruktúra védelem (CIIP) és hálózat- és információ biztonság (NIS) Európai Uniós megközelítési gyakorlata

Részvételi díj szállásköltség nélkül 64.000,-Ft+ÁFA, HTE tagok vagy HTE jogi tagok munkatársai részére 58.000,-Ft+ÁFA.

Szállást a rendezvény helyszínén, a Hotel Európa Fit**** szállodában biztosítunk igény esetén az alábbiak szerint: egyágyas szoba 36.000,-Ft+ÁFA /fő/2éj, kétágyas szoba 26.000,-Ft+ÁFA/fő/2éj.

A jelentkezési lap letölthető a rendezvény honlapjáról, http://kvk.bmf.hu/emcom2009 ahol további hasznos információkat is talál a rendezvényhez kapcsolódóan.

CSÁSZÁR János – DUDÁS Levente

KOMMUNIKÁCIÓS KAPCSOLAT A NEMZETKÖZI ŰRÁLLOMÁSSAL

Nemzetközi űrállomás (ISS)

- Operátor:
  Simonyi Károly
- Hívójel: HA 5 SIK
- Kommunikáció nyelve:
  <<< magyar >>>
- Üzemi frekvencia:144 MHz
- Üzemmód: FM
- Forgalmazási periódus: 8-10 perc

2009.09.27. 3

Mozgó állomás (hőlégballon)

- Operátor: Császár János
- Hívójel: HA5PA / AM
- Utazási magasság: 1200 m
- Repülés helye: Velencei-tó

Hőlégballon

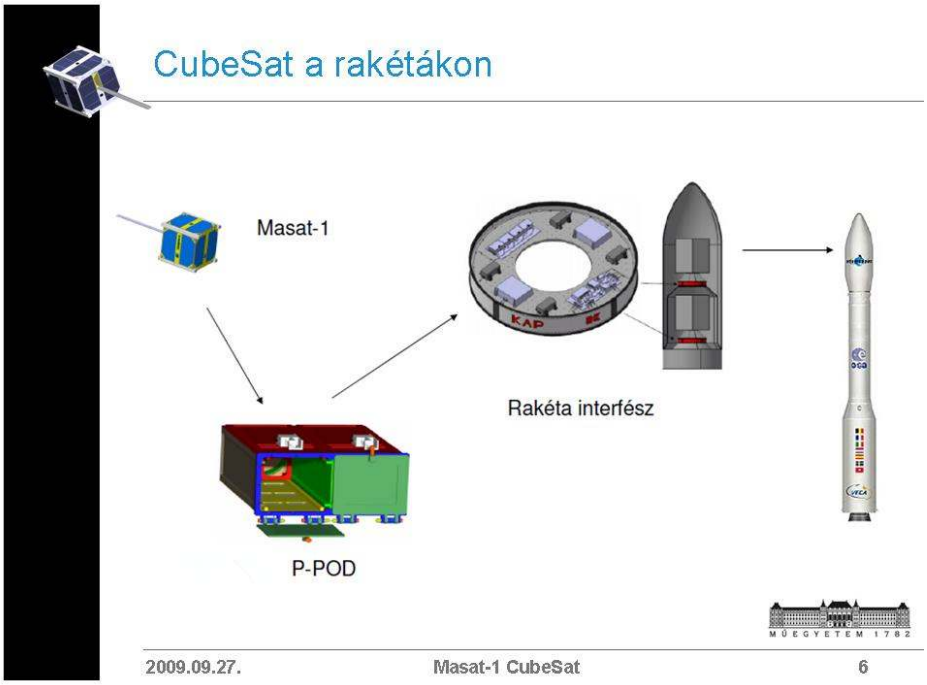
- Kiegészítő tevékenység:
  - Helikális antenna készítés
  - IP kamera on-line üzemeltetése
  - Masat-1 kommunikációs teszt

Adó-vevő

Helikális antenna

2009.09.27. 4


MaSat -1
http://cubesat.bme.hu
Az első magyar műhold
Dudás Levente
okl. villamosmérnök
MaSat-1 Fejlesztői Csoport
2009.09.27.


CubeSat a rakétákon
Masat-1
Rakéta interfész
P-POD
MŰEGYETEM 1782
2009.09.27.
Masat-1 CubeSat
6

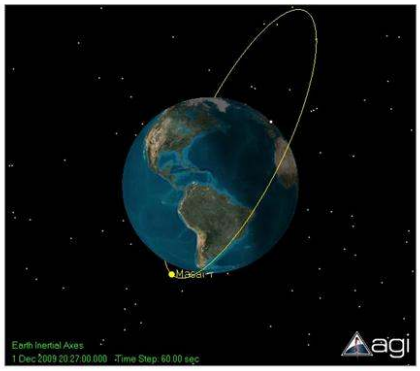
Hordozóeszközök

- VEGA
- Kosmos-3M
- Rockot
- PSLV
- M-V
- Dnepr
- Falcon-1

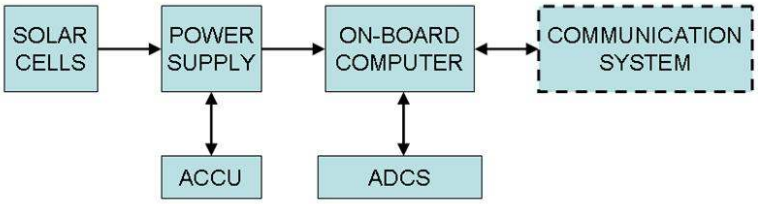



A Masat-1 pályája

- Optimális: 600-800km, napszinkron poláris pálya
- Fényviszonyok:
  - napsütés: 64%
  - árnyék: 36%
- Láthatóság a BME-ről (10 fokos eleváció fölött):
  - Minimum: 1,38 perc
  - Maximum: 8,62 perc
  - Átlagosan: 6,80 perc
  - 10 napra vetítve: 244,86 perc

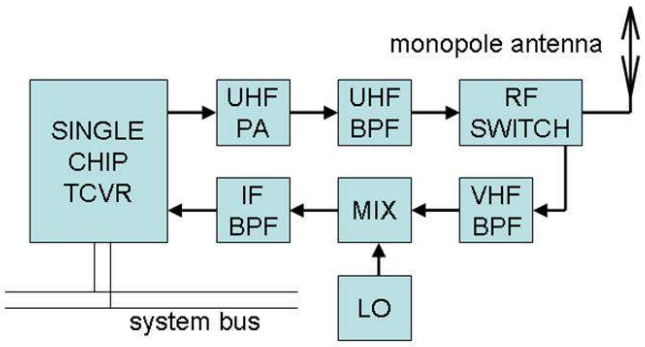


A Masat-1 alrendszerei



- energiaellátó rendszer: 1..3 W bemenő teljesítmény
- fedélzeti számítógép
- kommunikációs rendszer
- félaktív mágneses stabilizáló rendszer
- **redundancia!!!**

A kommunikációs rendszer



- hidegtartalékolt
- 2,5 szeres redundancia

HA5MASAT

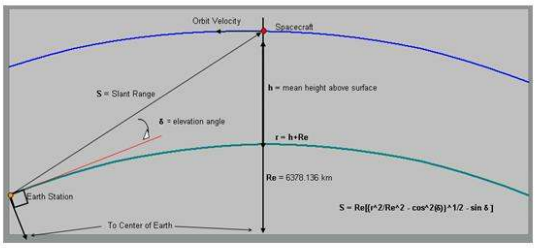
- Felmenő: 145 MHz, lejövő: 437 MHz
- Adatsebesség: 1200 bit/sec
- Moduláció: OOK, 2FSK
- Sávszélesség: 12 kHz
- RF kimeneti teljesítmény: > 0,1 W
- Antenna: negyedhullámú monopól

Doppler-hatás

437 MHz:

6..800 km 90 fok

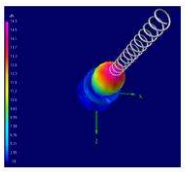
2000 km 10 fok



152 dB
szakaszcsillapítás

A sikerhez kell egy vevőállomás is…

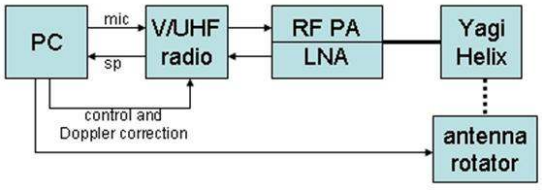
- **HA5MRC**
  - Antennapark a V2 épület tetején
  - Saját fejlesztésű antennaforgató elektronika és
  - Vezérlő szoftver: Doppler, antenna…



BME földi állomása

2009.09.27. Masat-1 CubeSat 13

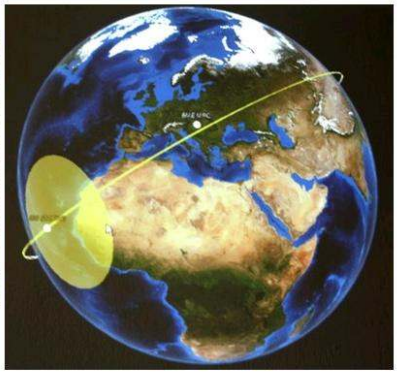
Teszt: HA5SIK – HA5MRC

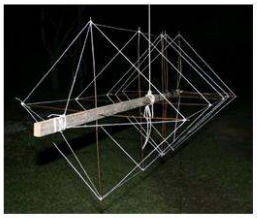


2009.03.29.
Budapest

2009.09.27. Masat-1 CubeSat 14

Teszt: HA5SIK – HA7WEN





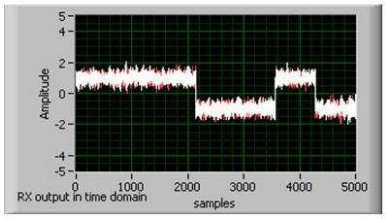
2009.03.31.

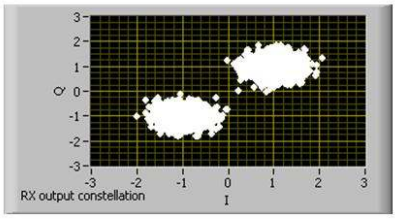
Érd

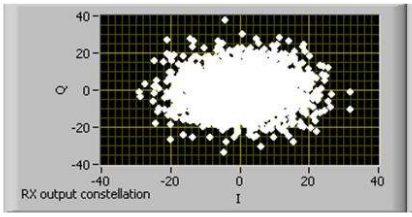
Forgató: R1

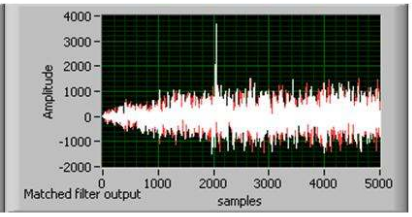
5 el cross-Yagi (10dBi)

Detektálás kézirádióval!









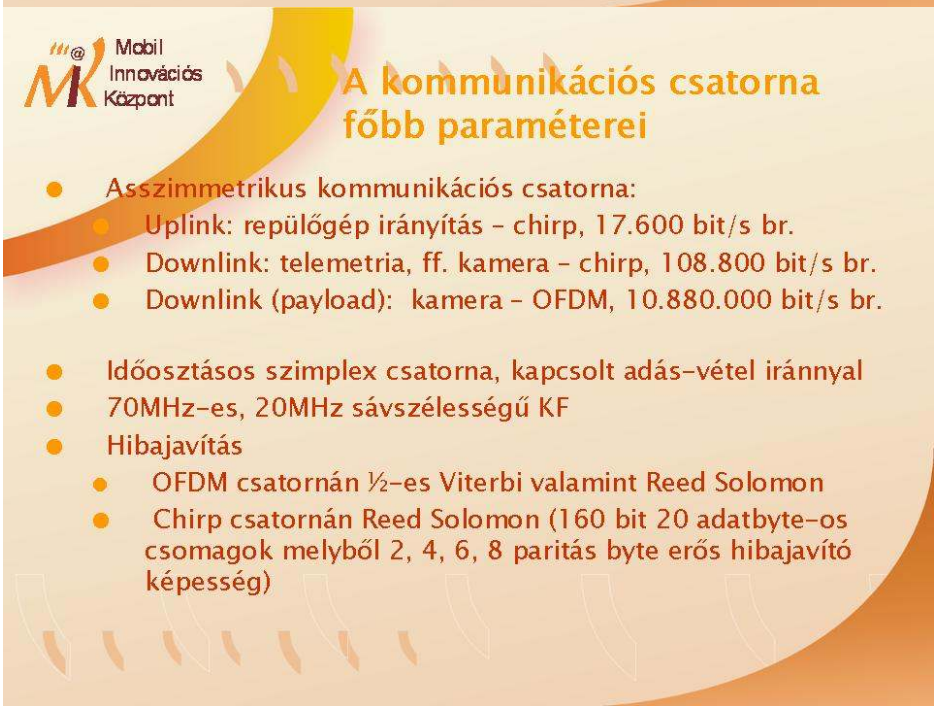
512 hosszú kód → 25 dB nyereség!

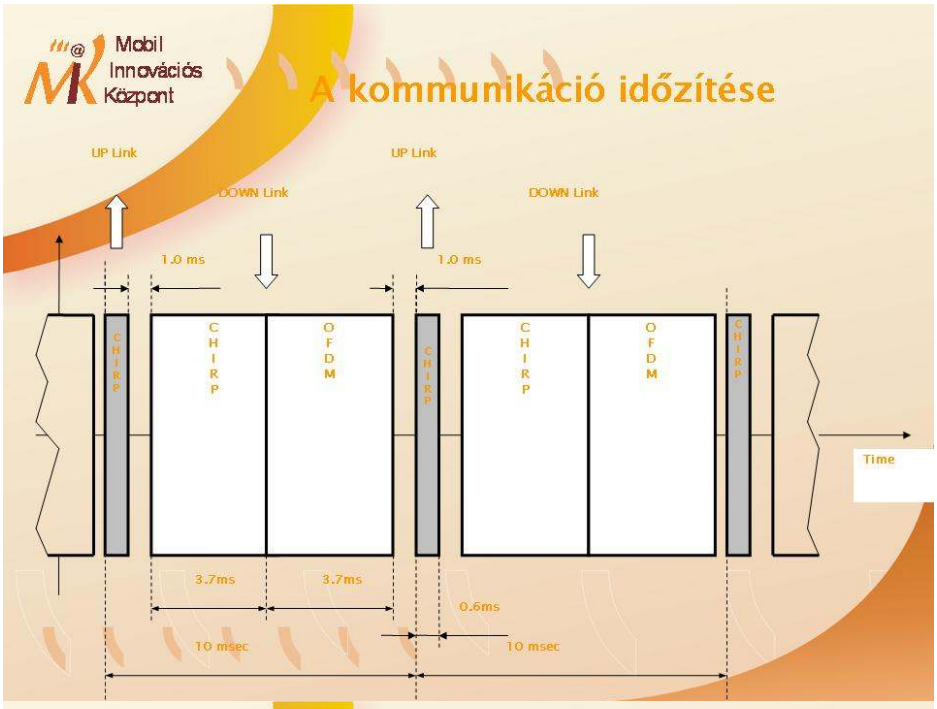
Hőlégballonos repülés

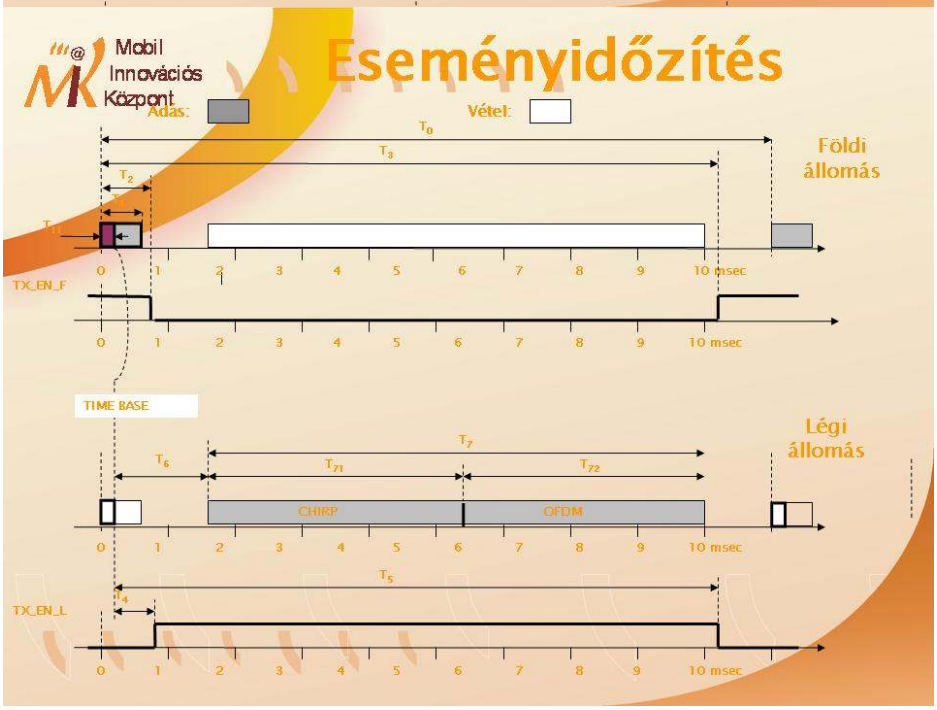
KOLLER István – IMRE Sándor

UAV – FÖLDI ÁLLOMÁS KOMMUNIKÁCIÓS CSATORNA FEJLESZTÉSE


Mobil
Innovációs
Központ
A feladat
Nagysebességű, nagy megbízhatóságú, digitális modulációs eljárások kidolgozása és implementálása
földi állomás – légi jármű (up link)
Légi jármű – földi állomás (down link) irányában
A rádióösszeköttetés mindkét irányban ugyanazon frekvencián – 5 GHz-es sávban

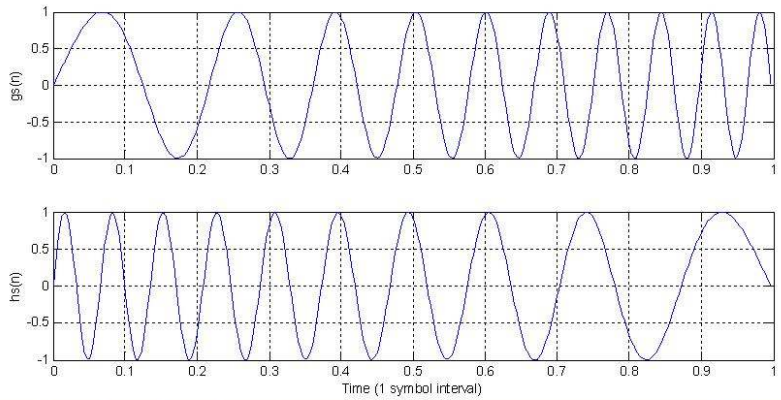

Mobil
Innovációs
Központ
A kommunikációs csatorna főbb paraméterei
Asszimmetrikus kommunikációs csatorna:
Uplink: repülőgép irányítás – chirp, 17.600 bit/s br.
Downlink: telemetria, ff. kamera – chirp, 108.800 bit/s br.
Downlink (payload): kamera – OFDM, 10.880.000 bit/s br.
Időosztásos szimplex csatorna, kapcsolt adás-vétel iránnyal
70MHz-es, 20MHz sávszélességű KF
Hibajavítás
OFDM csatornán ½-es Viterbi valamint Reed Solomon
Chirp csatornán Reed Solomon (160 bit 20 adatbyte-os csomagok melyből 2, 4, 6, 8 paritás byte erős hibajavító képesség)


Mobil Innovációs Központ
A kommunikáció időzítése
UP Link
DOWN Link
UP Link
DOWN Link
1.0 ms
1.0 ms
CHIRP
OFDM
CHIRP
CHIRP
OFDM
CHIRP
Time
3.7ms
3.7ms
0.6ms
10 msec
10 msec


Mobil Innovációs Központ
Eseményidőzítés
Adás:
Vétel:
Földi állomás
TX_EN_F
TIME BASE
Légi állomás
CHIRP
OFDM
TX_EN_L
0 1 2 3 4 5 6 7 8 9 10 msec

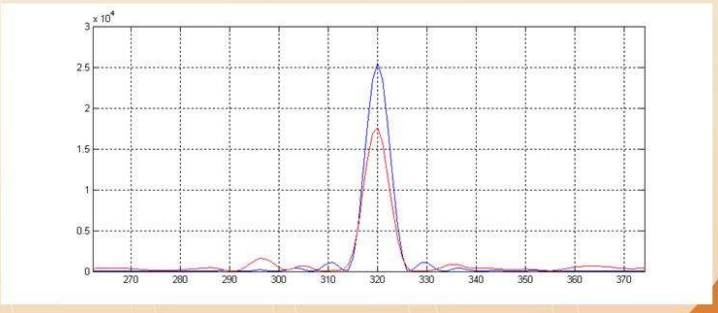
Mobil Innovációs Központ

A chirp moduláció



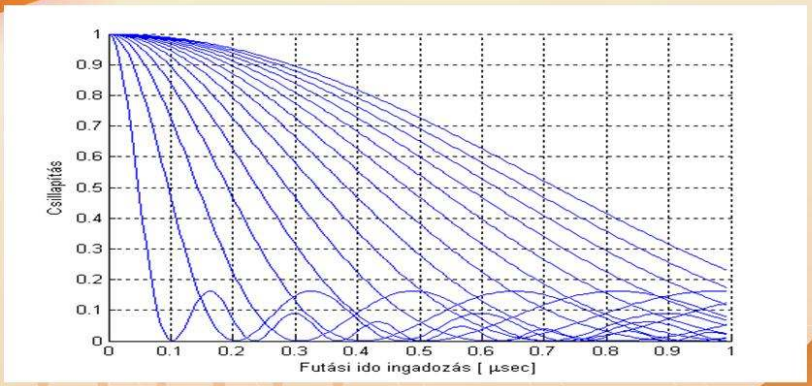
Mobil Innovációs Központ

A detektor kimenőjele zajmentes és 0 dB-es jel zaj viszonyú esetben



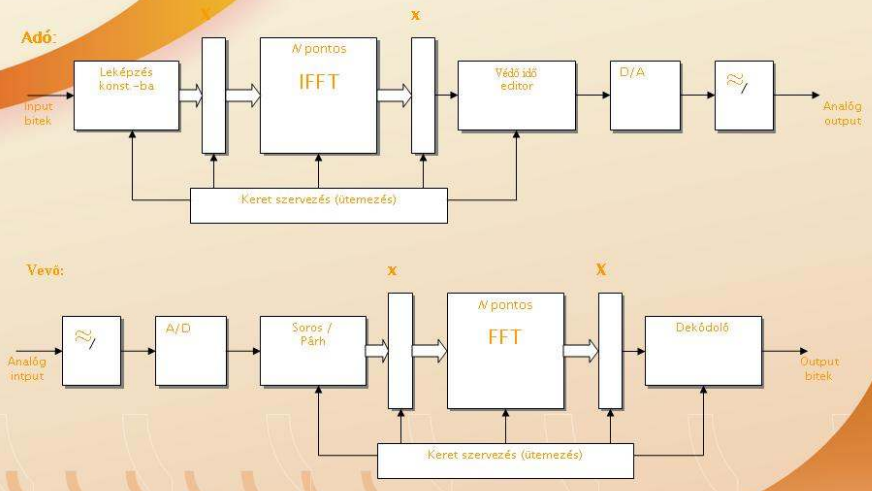
Mobil Innovációs Központ

A chirp detekciós csúcsának változása a futási idő ingadozás függvényében



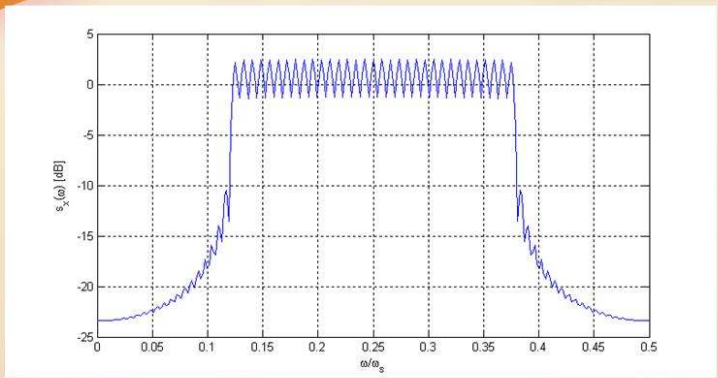
Mobil Innovációs Központ

Az OFDM rendszerek elvi felépítése



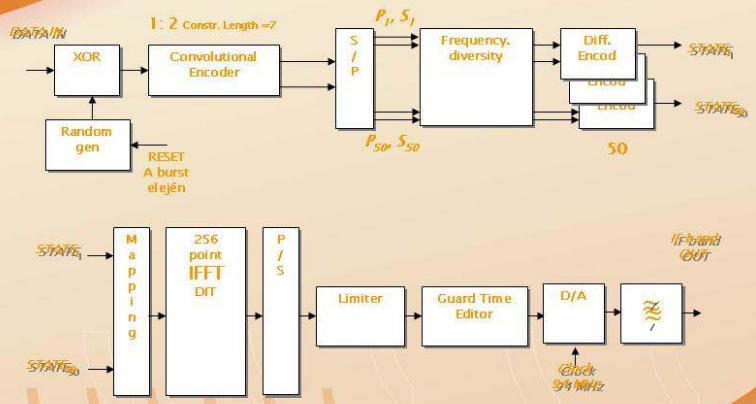
Mobil Innovációs Központ

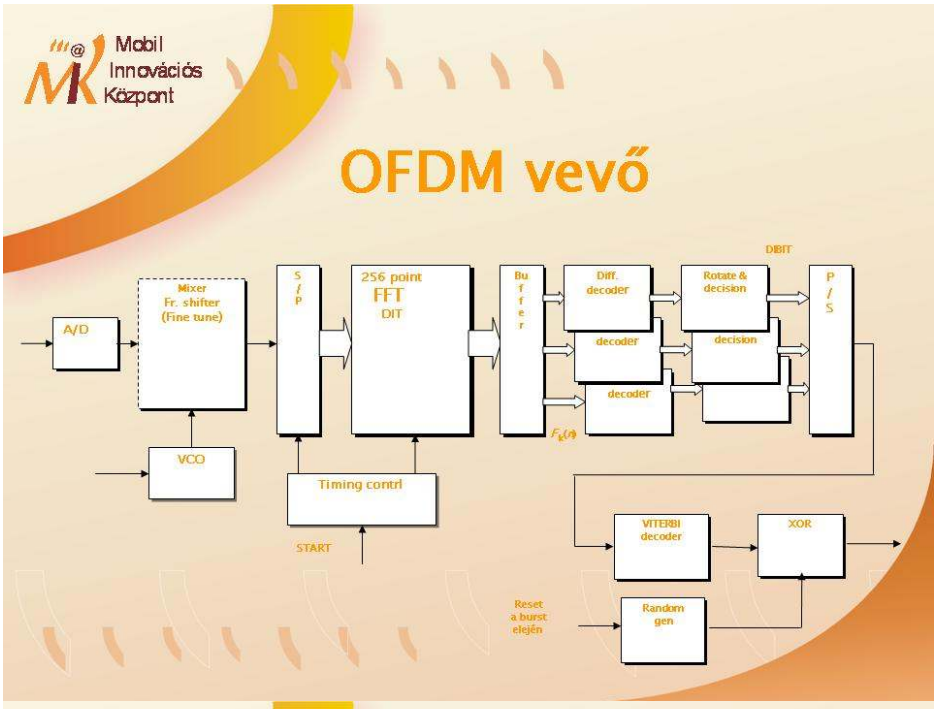
Az OFDM jel spektruma

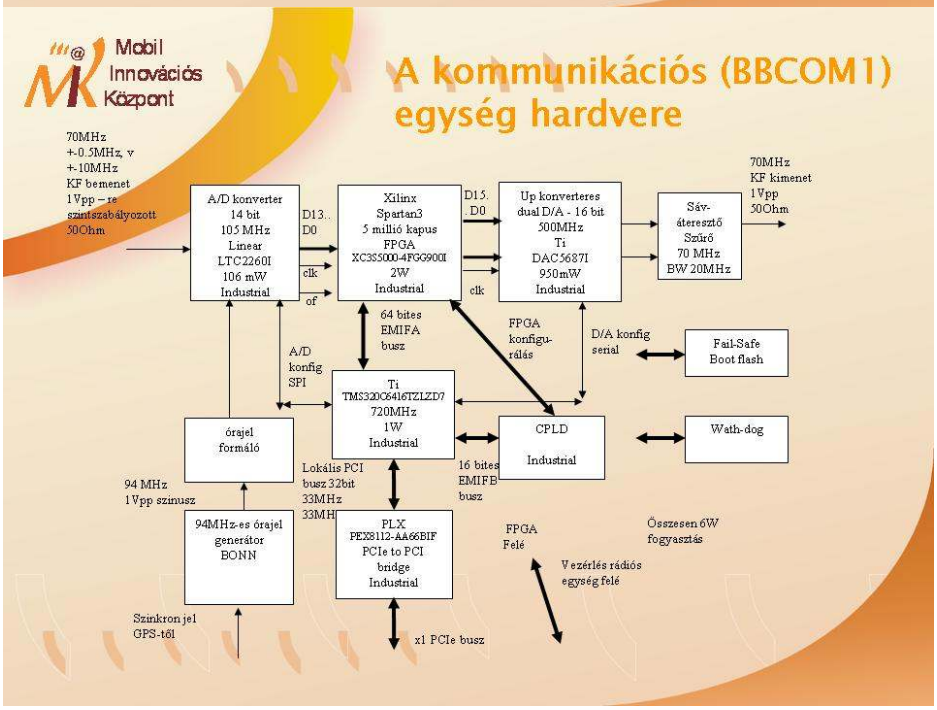


Mobil Innovációs Központ

OFDM adó

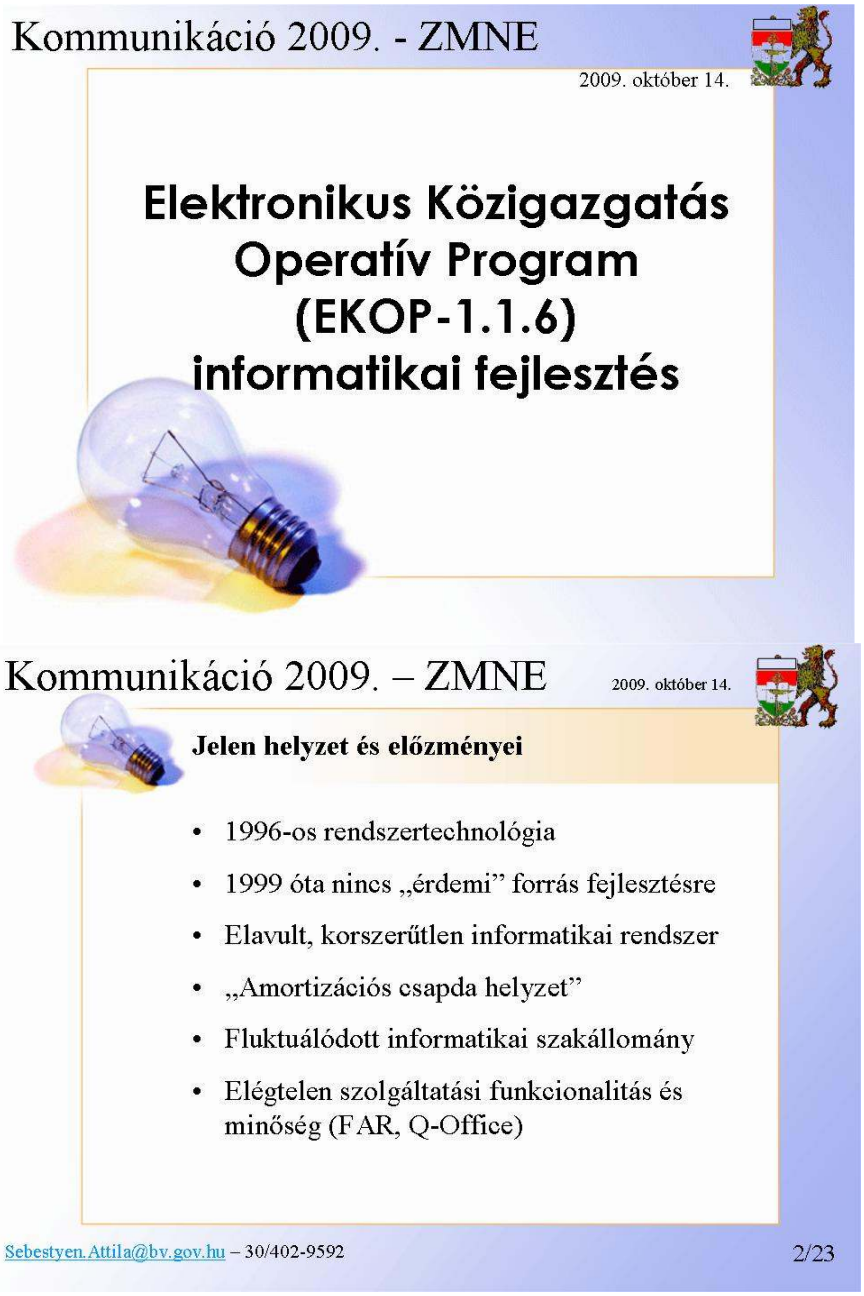



Mobil Innovációs Központ
OFDM vevő
A/D
Mixer
Fr. shifter
(Fine tune)
VCO
S / P
256 point
FFT
DIT
Timing contrl
START
Bu f f e r
Diff. decoder
decoder
decoder
DBIT
Rotate & decision
decision
P / S
VITERBI decoder
XOR
Reset a burst elején
Random gen


Mobil Innovációs Központ
A kommunikációs (BBCOM1) egység hardvere
70MHz
+-0.5MHz, v
+-10MHz
KF bemenet
1Vpp – re szintszabályozott
50Ohm
A/D konverter
14 bit
105 MHz
Linear
LTC2260I
106 mW
Industrial
D13..
D0
clk
of
Xilinx
Spartan3
5 millió kapus
FPGA
XC3S5000-4FGG900I
2W
Industrial
D15.
..D0
clk
Up konverteres
dual D/A - 16 bit
500MHz
Ti
DAC5687I
950mW
Industrial
Sáv-áteresztő
Szűrő
70 MHz
BW 20MHz
70MHz
KF kimenet
1Vpp
50Ohm
64 bites
EMIFA
busz
FPGA
konfigu-
rálás
D/A konfig
serial
Fail-Safe
Boot flash
A/D
konfig
SPI
Ti
TMS320C6416TZLZD7
720MHz
1W
Industrial
órajel
formáló
CPLD
Industrial
Wath-dog
94 MHz
1Vpp szinusz
Lokális PCI
buez 32bit
33MHz
33MH
16 bites
EMIFB
busz
94MHz-es órajel
generátor
BONN
PLX
PEX8112-AA66BIF
PCIe to PCI
bridge
Industrial
FPGA
Felé
Összesen 6W
fogyasztás
Vezérlés rádiós
egység felé
Szinkron jel
GPS-től
x1 PCIe busz

SEBESTYÉN Attila

ELEKTRONIKUS KÖZIGAZGATÁS OPERATÍV PROGRAM INFORMATIKAI FEJLESZTÉS



Korszerűtlen rendszertechnológia

- SCO Unix/Recital
- Karakteres felület
- Nem szabványos adatbázis kezelő
- Elszigetelten elosztott adatstruktúra
- Egységes fejlesztések elmaradása
- Nem szabványos környezet (Q-Office)
- Eszköz szintű problémák (pl.: nyomtatás)

Kommunikáció 2009. – ZMNE 2009. október 14.

„Amortizációs csapda helyzet”

- Harmadik életciklus eszköz szinten
  - Drága üzemeltetés és fenntartás
  - Korszerűtlen rendszertechnológia megoldások
  - Alacsony szolgáltatási szinvonal
- Kiszolgáltatottság a megoldásszállítóknak
- Öninduktív, kontrollálhatatlan működés
- Folyó költségvetésből megoldhatatlan fejlesztés
- Kilátástalan jövőkép (forrás hiány)

Fluktuálódott állomány

- Nincs rendszertechnológiai szakértelem
  - Informatikai szakterületen
  - Szakmai területeken (FAR megoldása a „jó")
- Elszigeteltség, munkaerő piaci hiány (tudás)
- Teljes munkafolyamat ellátás
- Out-sourcing kényszer
- Erős monopol helyzet – kiszolgáltatottság

Sebestyen.Attila@bv.gov.hu – 30/402-9592

Kommunikáció 2009. – ZMNE 2009. október 14.

Elégtelen szolgáltatási szint

- Belső-külső kapcsolattartás nehézkes
- Szabványosítás akadálya a korszerűtlenség
- Új eszközök bevezetése nehézkes:
  - A FAR-t illeszteni kell (pl.: nyomtató)
  - Az új eszköz emulációval butított
  - Az új eszköz kizárja a FAR használatát
- Elektronikus adatcsere nehézkes:
  - Társszervekkel
  - Együttműködőkkel

Sebestyen.Attila@bv.gov.hu – 30/402-9592

Probléma azonosítás

- Elavult rendszertechnológia
- Amortizálódott eszközpark
- Korszerűtlen alap infrastruktúra
- Out-souncing kiszolgáltatottság
- Fejlesztési, bővítési „zsákutca”
- „Elszigeteltség”
- Magas folyó működési költség

Megoldási javaslat

- Korszerű szabványos rendszertechnológia
  - Böngésző alapú vagy virtualizált működés
  - Szabványos adatbázis kezelő
  - Homogén szerver/kliens platform
- LAN, szerver és munkaállomás konszolidáció
- A „felügyelő” informatika helyett „végrehajtó”
  - Saját állománnyal kiterjesztett
  - Saját állománnyal működtetett (In-sourcing)
  - Informatikai biztonság erősítése
- Elszigeteltség és kiszolgáltatottság felszámolása
  - Szabványos, korszerű rendszertechnológia
  - Megoldásszállítók váltása, bővítése

EKOP, mint megoldás

- Európai Uniós forrásból 1.3 MFT beruházás
- Struktúrált intézeti helyi hálózatok kialakítása
- Intézeti és központi szerver parkok létrehozása
- Amortizálódott munkaállomások (részbeni) cseréje
- Fogvatartotti rendszer újraírása
- Személyügyi rendszer újraírása
- Működési környezet feltételeinek javítása (office)
- Rendszertechnológiai környezet korszerűsítése (XXL szd.)

Kommunikáció 2009. – ZMNE 2009. október 14.

EKOP informatikai projekt

- 1.3 MFT beruházás 2009. május – 2011. május
- Tudomásunk szerint a pályázat elbírálása október ???
- Pályázati anyag, egy megvalósíthatósági tanulmányban elkészült (62 oldal)
- Projekt megvalósulás 24 hónap (fenntartási időszak 5 év)
- Projekt szinten nem kezelt informatikai problémák:
  - Erősáramú betáp rendszer
  - Elektronikus ügykezelő rendszer
  - Teljes amortizációs eszköz csere (800-1000 munkaállomás)
  - Nyomtató konszolidáció névleges
  - Analóg telefonok felszámolása elmarad
  - Teljes EDR készülék feltöltés (350 kézi, 50 mobil) elmarad
  - Saját tulajdonú határvédelmi rendszer kialakítása (pl:VPN) elmarad
  - Intranet szolgáltatások bővítése elmarad

LAN konszolidáció (~170 mFt)

- Objektumon belüli, objektumok és épületek közötti helyi struktúrált hálózat kialakítása
- Tartalma:
  - Struktúrált kábelezés (~5000 végpont)
  - Aktív eszközök (48p/24p/receiver – 40/50/50)
  - Központi kábelrendezők, végződtetések, RACK
- 2009. december 31-ig (legkésőbb 2010. május 30-ig)
- Rendező patch- és munkaállomások lengő kábeleit helyben kell biztosítani
- A LAN aktív eszközök konfigurálására képzést várunk el
- Szándék szerint egységes platform, homogén hálózat kerül kialakításra (pl.: PoE és PortSecurity képességgel)

Kommunikáció 2009. – ZMNE 2009. október 14.

Szerver park, munkaállomások (~580 mFt)

- Intézeti a Windows alap infrastruktúra RACK szerverei:
  - AD/DNS/DHCP
  - Fájl- és nyomtató megosztás
  - Alkalmazás szerver (terminál vagy virtuál szerver)
  - MS Sql
  - (Management szerver?)
- Szerver park szünetmentes védelme
- Napi (szalagos/HDD backup) mentési rendszer
- ~ 1200 db vékony kliens és 400 db asztali munkaállomás
- 1-3 db nagy teljesítményű intézeti nyomtató (900 eFt)
- Központi szerver farm (redundáns blade) és aggregátor
- 2009. december 31-ig (legkésőbb 2010. május 30-ig)

Fogvatartotti Rendszer újraírása (~340 mFt)

- Rendszertechnológiai szintű újra írása
  - Szabványos adatbázis kezelő (MS Sql/Oracle)
  - Böngésző alapú és/vagy virtualizált alkalmazás
- Funkcionális bővítés
  - Letétkezelő alrendszer
  - Élelmezési alrendszer
  - Foglalkoztatási alrendszer
  - Fényképkezelő alrendszer
  - Egészségügyi alrendszer (járó és fekvő beteg ellátás)
  - Társzervek on-line lekérdezése
  - Statisztikai és vezetői funkcionalitás bővítése
- Adatmigrálás és rendszerintegráció
- 2010. december 31-ig (legkésőbb 2011. május 30-ig)

Kommunikáció 2009. – ZMNE 2009. október 14.

Személyügyi Rendszer újraírása (~100 mFt)

- Rendszertechnológiai szintű újra írása
  - Szabványos adatbázis kezelő (MS Sql/Oracle)
  - Böngésző alapú és/vagy virtualizált alkalmazás
- Funkcionális bővítés
  - Személyügyi alrendszer (Ht., Ktv., Kjt., egyéb)
  - Szolgálatszervezési alrendszer
  - Fegyelmi alrendszer
  - Egészségügyi,fizikai állapot felmérés nyilvántartása
- Adatmigrálás és rendszerintegráció
- 2010. december 31-ig (legkésőbb 2010. május 30-ig)
  - Személyügyi és szolgálatszervezési alrendszer 2009. december 31.
  - Fegyelmi és EÜ. 2010. december 31.

Informatikai környezet korszerűsítés (~40 mFt)

- MS Windows tartományi rendszer kiterjesztés
  - Szakember képzés
  - Saját állománnyal való kiterjesztés
  - OU rendszergazdaság delegálása
  - Irodai alkalmazások bevezetése szabványosítása
- Informatikai rezsim
  - Egységes, központilag szabályozott informatika
  - MS Windows tartományi környezetre szabott biztonsái, üzemeltetési szabályzói környezet
- 2010. május 31. (funkcionálisan 2010. december 31.)
- Rezsim kialakítása a bevezetésekkel párhuzamos, azokat követő

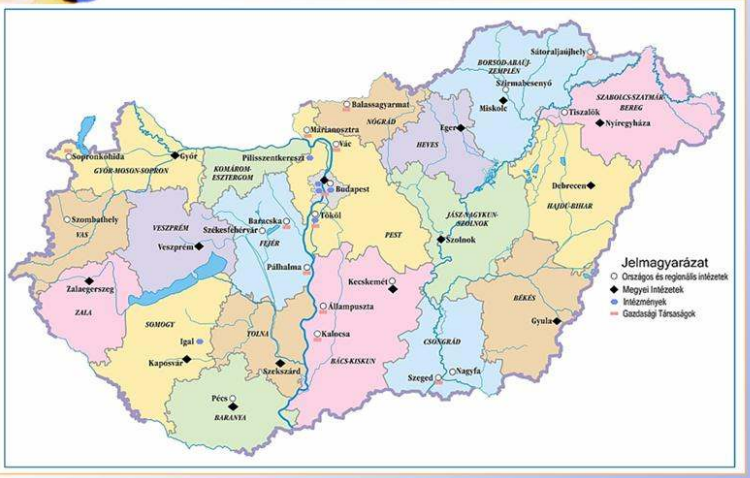
Kommunikáció 2009. – ZMNE 2009. október 14.

Egyéb érvényesítendő elv

- „éles”, teszt és oktató rendszer funkcionális elkülönítése
- Tanintézeti képzés feltételeinek megteremtése, biztosítása
- Pilot, majd országos szintű fejlesztés és tesztelés (min. 6 hó)
- Párhuzamos, elszegényedő működés (FAR és új FAR)
- Teljesen új alapon szervezett MS tartományi kiterjesztés
- Fejlesztéssel együtt kialakított központi HelpDesk rendszer
- E-learning keret bevezetése tudás menedzsment eszközként
- „informatikai szolgáltatások az informatikai szolgáltatásért”
- Új eszköz, magasabb szintű szolgáltatás, korlátozások mellett
- Váltás a „felügyelő” informatikáról a „végrehajtó” felé

Kommunikáció 2009. – ZMNE 2009. október 14.

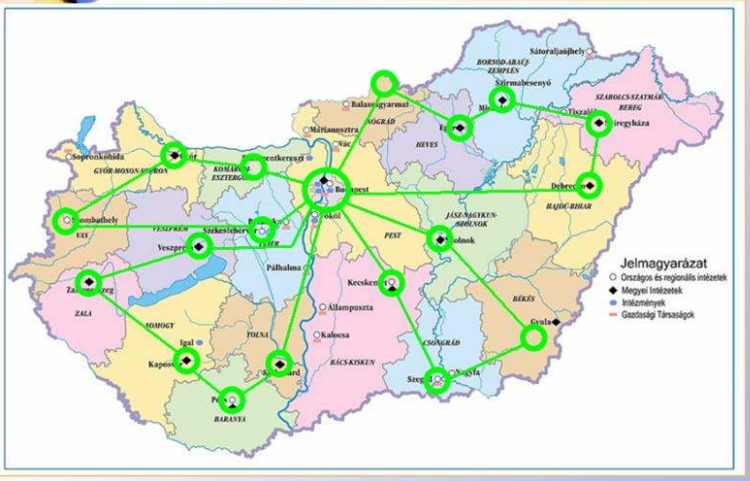
Informatikai rendszer tulajdonságai I.



Sebestyen.Attila@bv.gov.hu – 30/402-9592

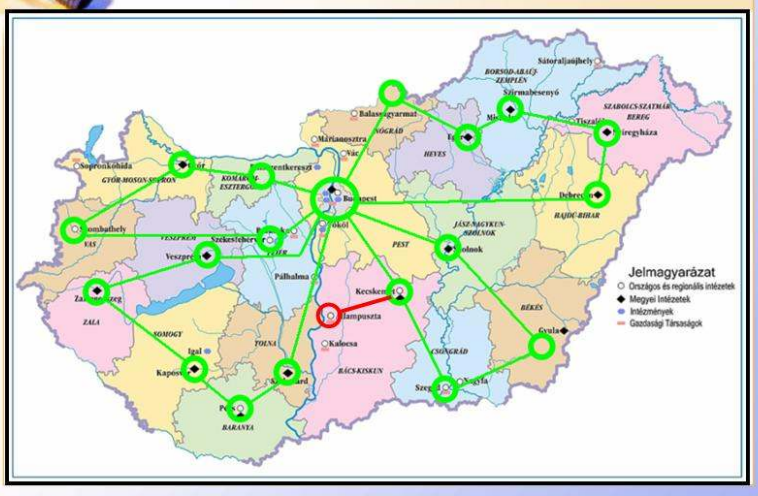
Kommunikáció 2009. – ZMNE 2009. október 14.

Informatikai rendszer tulajdonságai I.



Sebestyen.Attila@bv.gov.hu – 30/402-9592

Informatikai rendszer tulajdonságai I.



Informatikai rendszer tulajdonságai II.

- Drága üzemeltetés és fenntartás
  - EKG 330 millió forint/év (minden telephely)
  - FAR 100 + 30 millió forint/év
  - MS Windows 100 millió forint/év
  - Központi rendszerek támogatása 80 millió forint/év
- Nagy teljesítményű nyomtatók helyett munkaállomáshoz kötöttek (2 Ft/lap kontra 8,- Ft/lap fajlagos költség)
- Vagyon védelmi megoldások (hardware lock) 4000,- Ft/gép
- IP telefon használata belső forgalomban ingyenes, de a telefax szolgáltatás kizárólag a BVOP-n meghaladja a havi 300000,- Ft-ot

Informatikai rendszer tulajdonságai III.

- „Pazarló” humán erőforrás felhasználás
  - Mérnökök látnak el nyomdai kisegítő munkát
  - Out-sourcing a „saját erő” helyett (>napi 100 eFt)
  - Felhasználói ismeretek hiánya, „kényelem érzet”
- Többszörösen alacsony minőségű rendelkezésre állás
  - Aggregátor hiánya
  - Telefon központ rendszer backup hiánya
  - Gépterem, technikai helyiség, raktár, iroda egyben
  - Üzemeltetési környezet out-sourcing felügyelete
- Alacsony szintű általános informatikai kultúra, informatikai biztonság

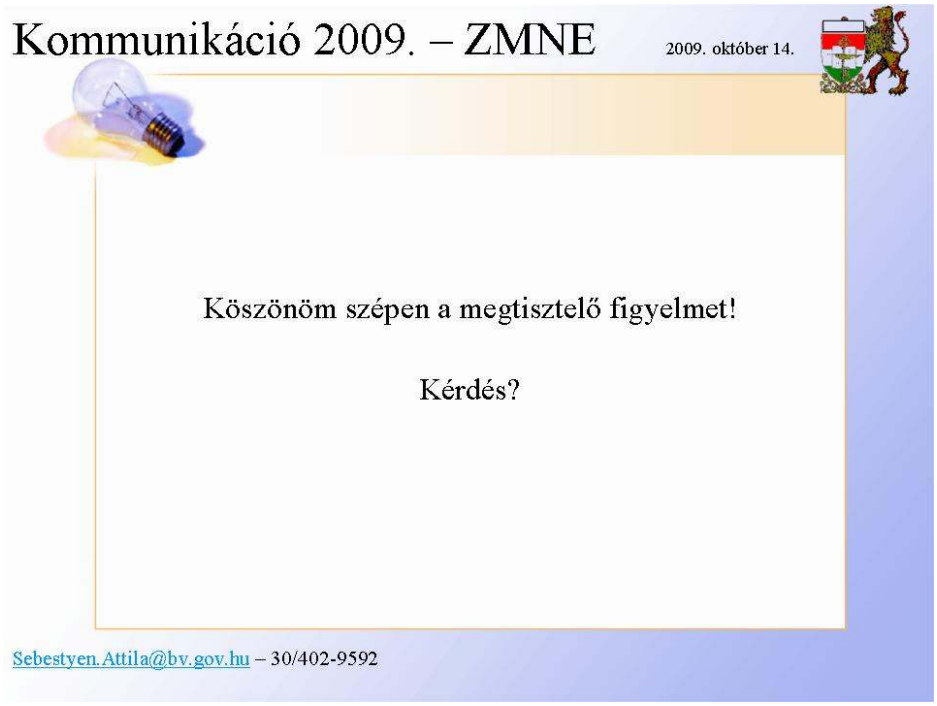
Sebestyen.Attila@bv.gov.hu – 30/402-9592

Kommunikáció 2009. – ZMNE 2009. október 14.

Megvalósítás ütemterve

- 1. fázis 2010. június 30-ig
  - Helyi hálózat konszolidáció
  - Központi és intézeti szerver konszolidáció
  - Munkaállomások kiváltásának megkezdése
  - Kórházi beteg irányító rendszer
  - Humán erőforrás nyilvántartás
  - Szolgálatszervezés
  - Szünetmentesítés, központi alrendszerek
- 2. fázis 2010. december 31-ig
  - Szünetmentesítés, intézeti alrendszerek
  - Fogvatartotti rendszer rendszertechnológiai váltás
  - Teszt és oktató alrendszer bevezetése
- 3. fázis 2011. május 31-ig
  - Fogvatartotti- és egészségügyi alrendszer
  - Nyomtató- és mentő-archiváló alrendszer

Sebestyen.Attila@bv.gov.hu – 30/402-9592

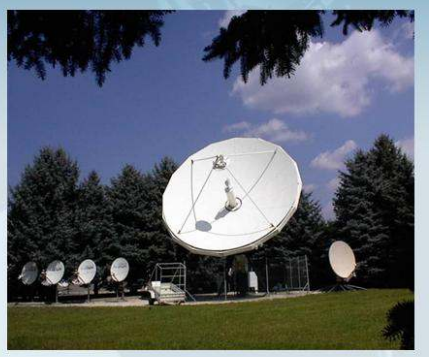

Kommunikáció 2009. – ZMNE
2009. október 14.
Köszönöm szépen a megtisztelő figyelmet!
Kérdés?
Sebestyen.Attila@bv.gov.hu – 30/402-9592

Hungaro DigiTel

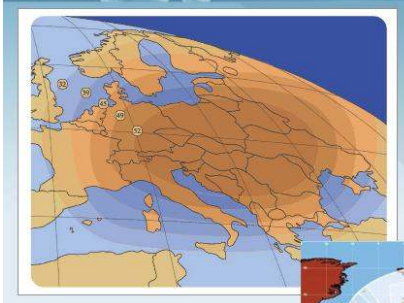
MŰHOLDAS TÁVKÖZLÉS

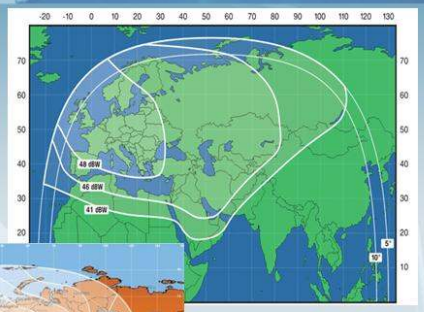
Főbb referenciáink

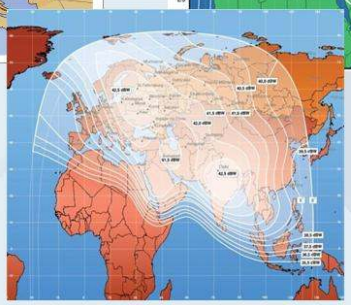
- OTP Bank
- Agip Hungária
- Lukoil Hungary
- MOL
- OMV Hungária
- OMV Serbia
- Shell Hungary
- Shell Bulgaria
- Külügyminisztérium
- Magyar Honvédség
- További Kormányzati Felhasználók
- Miniszterelnöki Hivatal
- Antenna Hungária
- Magyar Telekom
- Invitel



Lefedettség és nemzetközi jelenlét







A VSAT hálózat előnyei

Előnyök a földi megoldásokhoz képest:

- Rugalmas, gyors telepíthetőség
- Ország →régió teljes lefedése
- Azonnali kommunikáció lehetősége
- Földi infrastruktúrától független
  - fejletlen területek kiszolgálása
- Magas rendelkezésre állás
- Távolságtól független díjazás
- Állandó 365/24/7 órás ügyfélszolgálat
- Proaktív hibakezelés

Műholdas szolgáltatások

Nemzetközi adathálózati megoldások

- **Dedikált vagy dinamikus (ügyfél hálózatán belüli) nagysebességű IP összeköttetések**
- **Magyarországi és külföldi telephelyek összeköttetése**
  - Telefonközpont kihelyezés
  - Központi szerverek (pl. központi adattárak) bekötése
  - Intranet elérés
  - Szélessávú Internet elérés
  - Videokonferencia
- **Nemzetközi viszonylatban versenyképes ár**

Mobil műholdas megoldások

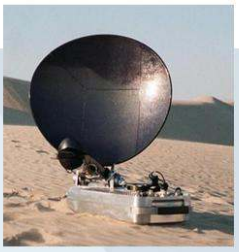
- 1 gombnyomásra üzemképes
- Automatikus műholdra állás
- Gyors műholdra állás (kb. 5 perc)
- Könnyen szállítható
- Nem kell minden helyszínen
  - összeszerelni
  - szétszerelni
- Nem igényel szakértelmet
- Nem igényel fizikai munkát
- Tömege kompletten: <100kg

Mobil műholdas megoldások – Fontosabb műszaki paraméterek

- Automatikus antenna pozícionálás GPS alkalmazásával, beépített elektronikus iránytű és dőlésszögmérő;
- Szigetelési szabvány: IP 65 (por-, és vízálló kivitel);
- Tömege: 40-50kg (kiépítés függően)
- Működési hőmérséklet: -32°C - +50°C;
- Működési szélerősség: max. 72 km/h;
- Működési magasság: max. 3000 m;
- Működési páratartalom: max. 95%;
- Áramfelvétel: 110-240VAC, 1 fázis, 50/60 Hz
  max. 6/3 A csúcs,
  max. 1 A folyamatos

Mobil műholdas megoldások - Hordozható (aktatáska jellegű) megoldások

- Kis méretű, egy dobozos csomagolás, akár repülőgépen is szállítható,
- Háromféle antenna nagyság (90, 120, 150 cm),
- Moduláris felépítés,
- Motorizált, teljesen automatikus változatban is,
- Könnyű telepíthetőség, működőképesség 5 perc alatt,
- A legtöbb műholdon használható,
- A katonai szabványoknak megfelelő,
- Szénszálas anyagból készült, szélsőséges körülmények között tesztelt, masszív kivitel.



Gépjárműre szerelhető megoldások

- Áramvonalas, elegáns, könnyű felépítés,
- Bármilyen járműre telepíthető,
- Ideiglenes, vagy végleges tetőrögzítés,
- 120 cm-es, teljesen motorizált antenna,
- Szélessávú adatátvitel,
- Működőképesség 5 perc alatt,
- Kifejezetten honvédségi célokra tervezett,
- Szélsőséges körülmények között tesztelt, masszív kivitel,

Egyszerűen szállítható, kis méretű megoldás

- Könnyen szállítható (akár helikopteren is), könnyű súlyú, gyorsan telepíthető megoldás,
- A világ legkisebb DISA (Defense Information Systems Agency) igazolással rendelkező műholdas terminálja,
- 10 percen belül telepíthető,
- Robosztus, masszív felépítés, stabil működés erős szélviszonyok között is,
- Kompakt csomagolás.

Egyéb mobil megoldások – Mozgás közbeni kommunikáció

Hajózás, szárazföld

•Használat mozgás közben,

•Szélessávú adatkommunikáció akár 4 Mbps sávszélességgel.

•Hang és fax szolgáltatások,

•Lefedettség világszerte.

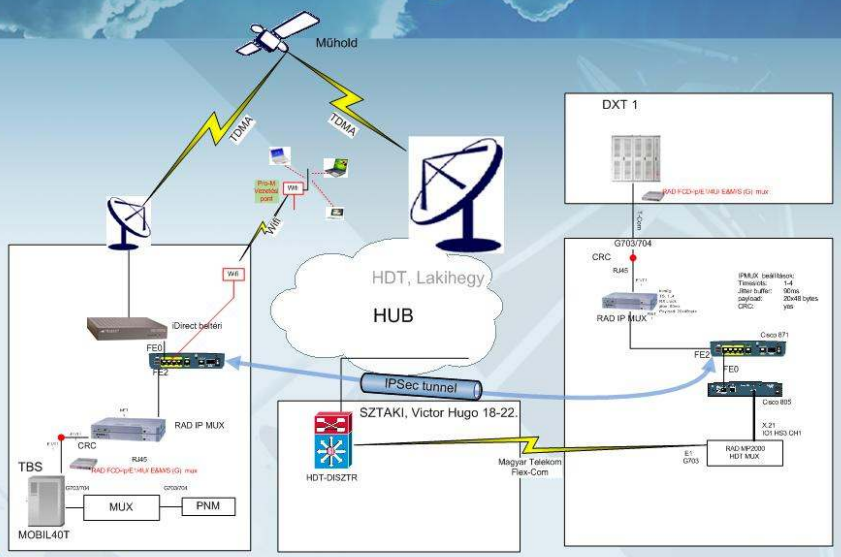
•Azonnali kommunikáció-helyreállás a műholdra való kilátás blokkolásának megszűnése után.

•Tömege: kb. 120 kg

Mobil műholdas megoldások – Felhasználási példák

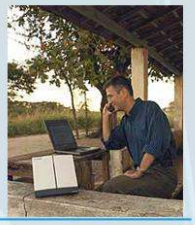
- Mobil ellenőrzési pont felállítása
- Parancsnoki gépjárművek bekötése a belső hálózatba
- Katasztrófavédelmi feladatok szervezése a helyszínről
- Video jel továbbítás a helyszínről/helyszínekre
- Hang továbbítás a helyszínről
- Központi adatbázisok elérése változó helyszínekről

EDR kihosszabbítás



Inmarsat és BGAN szolgáltatások

- A Hungaro DigiTel Kft. a Thrane & Thrane cég termékeinek hivatalos viszonteladója Magyarországon,
- A teljes termékskála forgalmazása, amely többek között magában foglalja az egyszerűbb, belépő szintű Inmarsat eszközöket, de a professzionális BGAN megoldások szállítását is.



Inmarsat teljes lefedettsége

Előfizetési lehetőségek:

- Havi előfizetéses
- Feltöltős (Pre-paid)

Egyéb lehetőségek:

- Mozgás közben működő megoldás;
- Publikus Internet és hanghívás szolgáltatás;
- Hang és Adat (streaming max. 256kbps, burst-ös IP forgalom max. 492kbps) integráció.

Köszönjük megtisztelő figyelmüket!

Továbbiakban is szívesen áll rendelkezésükre:

Lázár János
Kereskedelmi igazgató
E-mail: lazar@hdt.hu

2310 Szigetszentmiklós-Lakihegy, Komp u.2.
Tel: +36 1 4888 500
Fax: +36 1 4888 501
www.hdt.hu

MIHÁLYI Gábor (Pro-M Zrt)

EDR FEJLESZTÉSEK

Pro-M Zrt.
A Magyar Telekom Csoport tagja

EDR Fejlesztések

Mihályi Gábor
Műszaki és Üzletfejlesztési Igazgató
Pro-M Zrt.

2009. október 14.

A fejlesztések motivációi

- Felhasználói igények változásainak követése, az elégedettség növelése
- Lépéstartás a fejlődéssel
- Az EDR rendszer „készenléti" jellegének fokozása
- A 109/2007 (V.15) kormányrendeletben szereplő bővítésre való felkészülés

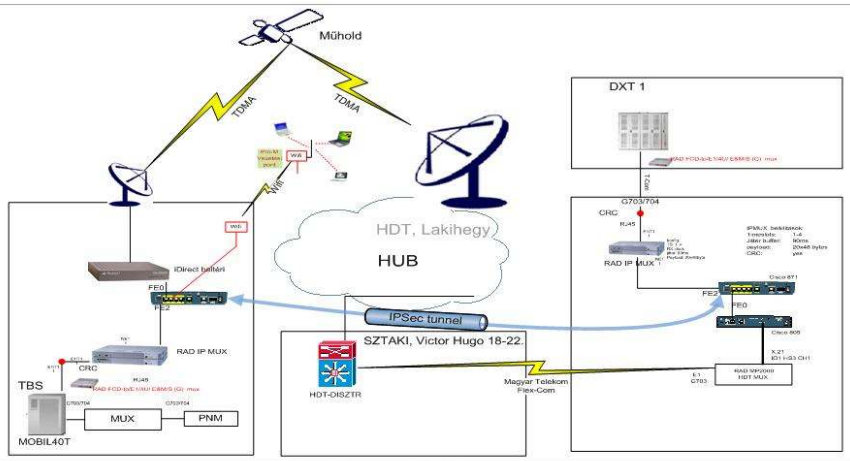
Jelentősebb fejlesztéseink

- Műholdas mobil TBS
- Pro-Mobil Járműkövető rendszer
- e-Learning oktatási rendszer

A műholdas mobil TBS előnyei

- Gyors telepíthetőség
  - Automata gépjárműre szerelhető antenna, amelynek használata nem igényel szakértelmet
  - Telepítési idő 2 óra (műholdas kapcsolat 5 perc)
  - Bárhol települhet ahonnét látszik a műhold (nincs szükség a földi átviteli hálózatra történő rálátásra)
- Multifunkcionális átviteli lehetőség

A műholdas mobil TBS rendszervázlata



A műholdas mobil TBS átviteli lehetőségei

- A kapcsolat kiépülése után ugyanazon az eszközön lehetőség van:
  - G.703 E1-es bittranszparens és titkosított átvitelére
  - 10/100 Base-T interfészen IP adatforgalom bonyolítására (pl. AVL)
  - Különböző IP forgalmak egymástól VLAN-nal történő szétválasztására (8 Ethernet port)
  - Videó konferencia hívásokra vagy egyéb képátvitelre

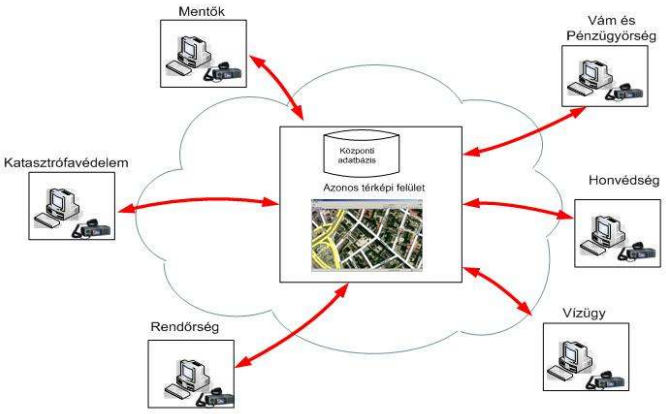
A telepített állomás

Tervezett

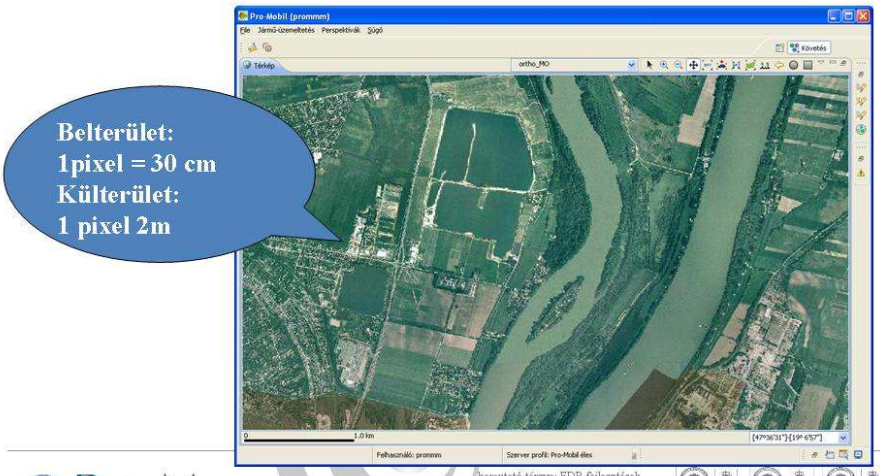
Pro-Mobil Járműkövető rendszer

- Az AVL rendszer továbbfejlesztett változata
- Előnyei:
  - Közös adatbázis
  - Részletes vektor, ortófotó és vektor-ortofotó térképek
  - Saját felületek, ikonok létrehozása
  - POI-k alkalmzása
  - Térképek negyedéves frissítése
  - Archiválás (valamennyi adat 1 évig visszakereshető pl. egy objektum mozgásának filmszerű visszajátszása)
  - Védett hozzáférés

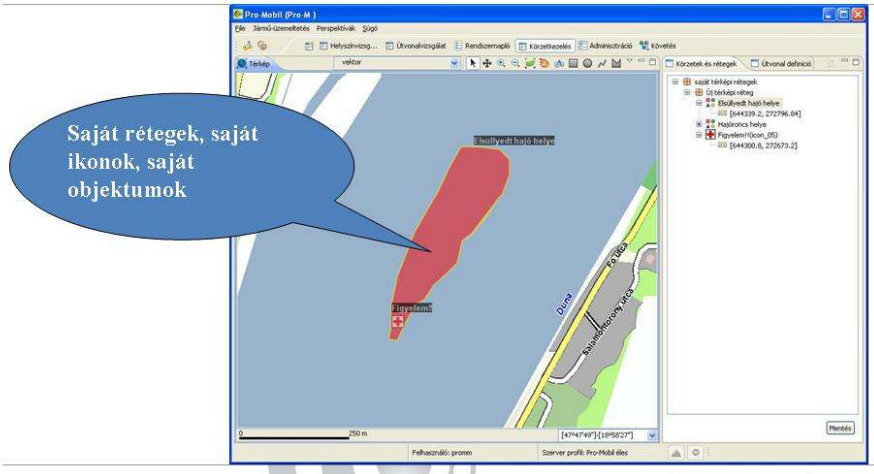
Pro-Mobil Járműkövető rendszer közös adatbázis



Ortofotó felbontása

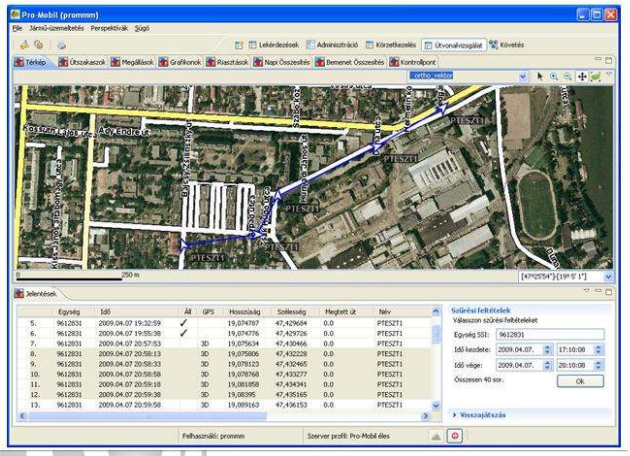


Saját réteg alkalmazása



Útvonal nyilvántartás

- Grafikonok
- Könnyű kezelhetőség
- Filmszerű lejátszás
- Valamennyi adat 1 évig online visszakereshető
- Dokumentum készítés támogatása



Távoktatás

- Kezdeti oktatási feltételek biztosítása
  - A Szolgáltatási szerződés szerint 13 db oktató termet rendeztünk be a Megrendelő által kijelölt objektumokban
  - Írott oktatási segédleteket készítettünk az EDR minden felhasználói elemére
  - Szimulátor programokat telepítettünk az oktató termekben
- Fejlesztés
  - Kapacitás növelés
  - Idő és „helyfüggetlen” oktatási lehetőség biztosítása
- Eredmény: az EDR szakszerű használata

Elektronikus távoktatás: e-Learning

Előnyei:

- Az EDR rendszer és az abban használt eszközök, alkalmazások részletes bemutatása
- Internet segítségével könnyen elérhető
- Gyors, hatékony tanulási lehetőség
- 0-24 órás rendelkezésre állás
- A készenléti felhasználók számára ingyenes

Kurzusok

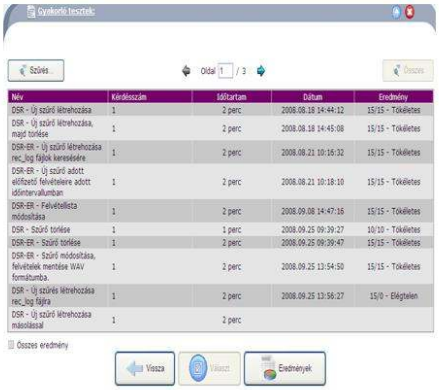
- A témák kurzus formájában sajátíthatók el

- 15 kurzus:
  - Általános EDR rendszer ismertető
  - Diszpécser állomás kezelés (DWS-C, DWS-M)
  - AVL (Automatikus járműkövető rendszer)
  - Hangrögzítő: (DSR: Solidbank 601, Hungarocom: CRU-1)
  - Készülékek (EADS THR880, TMR880, Sepura: SRH3800, SRG3500 Motorola:MTM800)
  - Programozó szoftverek (EADS: ITSI Tool, Phoenix, Sepura: Radio Manager Motorola: Tetra CPS)

Tanulási folyamat

- 1 kurzus 3 részből áll:
  - Tananyagok
  - Tesztek
  - Vizsga (csak 1-szer tehető le)

- Gyakorlás
  - Felelet választós tesztsorok
  - Interaktív (flash alapú) feladatok



Kurzus zárása

- Egy kurzus a sikeres vizsga letételével zárul
  (vizsga csak egyszer kísérelhető meg, ha nem sikerült, új hozzáférést kell igényelni)
- A sikeresen elvégzett kurzusokról, igazoló dokumentum készül

EDR Pro-M Zrt.

Oklevél

e-LEARNING TANULÓ

PRO-M Zrt.

KOZMA BÉLA

e-Learning eredmények

KURZUS	Vizsgázott	Sikeres vizsga
AVL	412	389
DWS-C	417	414
DWS-M	37	36
EADS ITSI Tool	12	7
EADS Phoenix	6	5
THR880i készülék	303	297
TMR880 készülék	384	379
Solidbank 601 hangrögzítő (DSR)	89	86
CRU-1 hangrögzítő (Hungarocom)	118	115
Motorola MTM800 készülék	464	453
Motorola progrqamozás	4	3
Sepura SRH3800 készülék	770	742
Sepura SRG3500 készülék	481	476
Sepura programozás	4	1
Összesen (kurzusszám)	**3501**	**3403**

Köszönöm a figyelmet!