A ZRÍNYI MIKLÓS NEMZETVÉDELMI EGYETEM KIADVÁNYA

Kommunikáció 2010
Communications 2010

11

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

SCI-Network Távközlési és Hálózatintegrációs 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.

Zrínyi Miklós Nemzetvédelmi Egyetem

Budapest, 2010. október 06.

A tudományos kiadványt lektorálták:
Prof. Dr. Rajnai Zoltán mk. alezredes, egy. tanár
Dr. habil. Sándor Miklós ny. ezredes, egy. docens
Dr. Fekete Károly mk. alezredes, egy. docens
Dr. Szöllősi Sándor ny. okl. mk. őrgy, egy. docens

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

Anyanyelvi lektor:
Dr. Fregan Beatrix

Felelős kiadó: Dr.Lakatos László ny. okl. mk. vezérőrnagy, a Zrínyi Miklós Nemzetvédelmi Egyetem rektor jogkörében eljáró főtitkár
Megjelent a Zrínyi Miklós Nemzetvédelmi Egyetemi Kiadó gondozásában
Készült a Zrínyi Miklós Nemzetvédelmi Egyetem nyomdájában, 80 példányban
Felelős vezető: Soós Károly
Levelezési cím: 1581, Budapest, Pf.: 15.

ISBN 978-963-7060-21-2

TARTALOMJEGYZÉK

A Nemzetközi szakmai tudományos konferencia kommunikációs partnere:

T-Systems

A tudományos konferencia támogatói:

Alcatel-Lucent Magyarország Kft.

Fercom Kommunikációs Kft.

Hírközlési és Informatikai Tudományos Egyesület

Hungaro DigiTel Kft.

Kapsch Telecom Kft.

Magyar Villamos Művek Zrt.

MH Támogató Dandár

43. Nagy Sándor József Híradó és Vezetéstámogató Ezred

Pro-M Zrt.

SCI-Network Távközlési és Hálózatintegrációs ZRt.

SIEMENS ZRt.

VIDEOTON
VT-Rendszertechnika Kft.

VIDEOTON
VT-Rendszertechnika Kft.

vtsys@rendszertech.videoton.hu

A NEMZETKÖZI KONFERENCIA HÁTTÉR INFORMÁCIÓI

A konferencia fővédnöke:
Halmai Ottó mk. dandártábornok
HM Híradó, Informatikai és Információbiztonsági Főosztály főosztályvezető

A konferencia védnökei:
Dr.Lakatos László ny.okl.mk.vörgy, ZMNE főtitkár
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.
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.
MH Támogató Dandár
43. Nagy Sándor József Híradó és Vezetéstámogató Ezred

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

A szervező bizottság elnöke:
Dr. habil Pándi Erik r. ezredes

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

A szervező bizottság tagjai:
Prof. Dr. Rajani Zoltán mk. ezds.
Dr. habil Sándor Miklós ny. ezds.
Dr. Szöllősi Sándor ny. okl. mk. őrnagy
Farkas Tibor fhdgy.
Jobbágy Szabolcs fhdgy.

BEVEZETŐ

A KOMMUNIKÁCIÓ nemzetközi szakmai-tudományos konferencia-sorozat tizenegyedik évfordulóján tisztelettel köszöntjük Önt, Kedves Kolléga, Tisztelt Olvasó!

A Híradó Tanszék sok évtizedes hagyományokra tekint vissza mind az alapfokú tisztképzés, mind a magasabb parancsnoki tisztképzés, mind pedig a tudományos képzés területén. Szakmai kultúránk kiforrott, stabil alapokon nyugszik, oktatási egységünk kollektívája szeretné ezért egyrészről a szakma zászlóshajójának, másrészről olyan integráló erőnek tekinteni önmagát, amely hatékonyan elősegíti a védelmi szférán belüli, illetőleg a védelmi és civil területek közötti gyümölcsöző szakmai párbeszédet, a tudástranszfert.

Idei rendezvényünkkel ismételten e szerepünket kívánjuk elősegíteni, amely reményeink szerint a résztvevők megelégedésével zárul. Jelen kiadványunk unikális, hiszen e kötetben számot adunk oktatási egységünk által ebben az évben lebonyolított gyakorlatunkról és katonai információbiztonsági rendezvényünkről is.

A gyakorlat mellett oktatási egységünk idén tehát elindult egy új úton is, amellyel célunk, hogy az információbiztonság területét a szakmai berkekben „népszerűsítsük", illetőleg olyan fórumot hozzunk létre, ahol a szereplők közötti információcsere létrejöhet és megvalósulhat. Levonva következtetéseinket úgy ítéljük meg, hogy a felügyeletet ellátó és egyben a szakmai munkát irányító szervezet és a tanszékünk által szervezett első információbiztonsági konferencia elsődleges célját elérte, ezért 2011-ben ismét vállalkozunk arra, hogy a hagyományteremtés rögös útján e szakterületen is előrébb jussunk.

A kiadvány áttekintéséhez jó időtöltést kívánunk, egyúttal kérjük, tekintsük bizakodva az ősi és újonnan kitaposandó ösvényeink elé!

Budapest, 2010. 10. 06.

A szervező bizottság

PÁNDI Erik – FARKAS Tibor – JOBBÁGY Szabolcs1

COMMIT 2010. NEMZETKÖZI, TANINTÉZETI HÍRADÓ ÉS INFORMATIKAI GYAKORLAT2

Absztrakt:
Idén, május 17-20. között ismételten megrendezésre került a COMMIT magyar-francia tanintézeti híradó és informatikai gyakorlat. A gyakorlatot a Zrínyi Miklós Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Kar Híradó Tanszéke tervezte-szervezte a Francia Hadsereg, valamint a Magyar Köztársaság Rendőrsége szerveitől érkezett híradó és informatikai tisztjeivel, tiszthelyetteseivel. A gyakorlat végrehajtása a balatonkenesei honvédüdülőben történt. Jelen közlemény felidézi a gyakorlat főbb elemeit.

Bevezetés

A gyakorlat elsődleges céljaként fogalmazódott meg, hogy a 2009/2010. tanév harmad- és negyedéves híradó tiszti hallgatói kapjanak lehetőséget eddig elsajátított – *többségében elméleti jellegű* –szakmai ismereteinek gyakorlati körülmények között történő próbájára is. A feladat meghatározása a Magyar Honvédség jelenlegi feladatrendszerével összhangban történt, vagyis a magyar-francia tervező részleg a hallgatók számára egy többnemzeti dandár keretében működő magyar békefenntartó zászlóalj kommunikációs rendszerének kialakítását és működtetését szabta meg.

A tervek előirányozták a rendőrség egy részlegének a honi zászlóalj szervezetében történő alkalmazását is. A technikai eszközöket a Híradó Tanszék, az MH Támogató Dandár, az MH 43. Nagysándor József Híradó és Vezetéstámogató Ezred, az ORFK Közép-magyarországi Gazdasági Ellátó Igazgatóság, valamint a

1 Szerzők: Pándi Erik PhD, r. ezds., ZMNE Híradó Tanszék, főiskolai tanár, Farkas Tibor PhD, fhdgy., ZMNE Híradó Tanszék adjunktus, Jobbágy Szabolcs MA, fhdgy., ZMNE Híradó Tanszék tanársegéd

2 Jelen közlemény a Bolyai János Kutatási Ösztöndíj támogatásával készült

Balatoni Vízirendészeti Rendőrkapitányság biztosította. A békeműveletek nemzetközi gyakorlatának megfelelően a tervező részleg külső szolgáltatókat is bevont a feladat végrehajtásába, úgymint Hungaro Digitel Rt.-t, Magyar Villamos Művek Zrt.-t és műszaki partnerét a Microcom Kft.-t, valamint a Pro-M Zrt.-t.

A végrehajtás főbb mozzanatai

A hétfői nap hallgatóink számára szokatlanul korán kezdődött és meglehetősen későn végződött. Igen mostoha időjárási körülmények között kényszerültek telepíteni a zászlóalj vezetési pontját, a katonai műhold antennát és mobil híradó-informatikai komplexumot (HIK) magába foglaló hírközpont elemeket, valamint a harcászati rádiórendszer elemét képező R-142 rádióállomást.

A keddi napon ismét megfeszített munkára került sor – hasonlóan rossz időjárási körülmények közepette – amikor is a beérkező rendőri részleg, illetőleg szolgáltatók segítségével a telepítési és összeköttetés felvételi munkák befejeződhettek. A zászlóalj ekkor már rendelkezett műholdas videokonferencia (VTC) kapcsolattal a francia dandárparancsnokság irányába, rövidhullámú rádiókapcsolattal a nemzeti

elöljáró, vagyis az MH Összhaderőnemi Parancsnoksággal. Mindkét irányt tekintve a kommunikációs igényeket a második műholdas kommunikációs csatornán rendszerbe integrált HICOM távbeszélő alközpont távbeszélő és telefax szolgáltatásai is kielégítették.

A zászlóalj alárendeltségébe tartozó katonai szervezeti elemek, úgymint őrség, vegyi-sugár felderítő és járőrtevékenységet ellátó alegységek kommunikációját kézi és háti MRR rádiók biztosították. A műveletbe bevont rendőri erők belső kommunikációjukat – feltételezve a terület lefedettségét – az EDR szolgáltatásain keresztül bonyolították. A katonai és rendőri erők együttműködését a zászlóalj vezetési pontján, valamint az egyes katonai alegységeknél telepített EDR készülékek biztosították. Újszerű megoldásként a rendőri erők a zászlóalj vezetése számára valós idejű képi információkat biztosítottak a körlet területén őrzés-védelmi célokból felszerelt kamerák, a rendőri közúti és vízi járműre telepített kamera, valamint a légi felderítő repülőre szerelt kamera révén. Mindezt elsősorban a vezetési pont közelében letelepített, Wi-Max technológiára épülő bázis állomás tette lehetővé. Az EDR rendszerbe integrált helymeghatározó megoldás (AVL) révén a zászlóalj vezetése valós idejű térképi információt kaphatott az egyes EDR készülékekkel felszerelt alegységek tartózkodási helyéről. Hallgatóink a zászlóalj vezetési pontján, az egyes vezető személyek részére biztosított PC-ket LAN-ba integrálva a HIK informatikai szolgáltatásainak révén MH intranet kapcsolatot alakítottak ki, amelyen keresztül biztosították az elektronikus levelezés és meghatározott adatbázisokhoz való hozzáférés lehetőségét. A teljes vezetési pontot besugárzó Wi-Fi bázisállomás révén – meghatározott PC-k tekintetében – internet hozzáférés került kialakításra a publikus adatbázisokhoz való csatlakozás érdekében. A rendőri részleg – megfelelő biztonsági elemek felhasználásával – szintén interneten csatlakozott saját központi levelező rendszereihez és adatbázisaihoz.

Szerda délelőtt, a gyakorlat keretében, első ízben került megszervezésre információbiztonsági konferencia magyar, francia és szlovák részvétellel, amelynek fővédnöke Halmai Ottó mk. dandártábornok, a HM Híradó, Informatikai és Információbiztonsági Főosztály vezetője volt. A munkanyelv angol volt, azonban a felmerült egyéb igények alapján a végrehajtásba tolmácstechnikai eszközöket és tolmácsot kellett bevonni, amelyet a Rendőrség biztosított.

A szimpózium a HM, az MH katonai szervezetei által üzemeltetett információbiztonsági rendszerek vezetőinek és munkatársainak, a nemzetközi kapcsolatrendszerben érintett, a társ fegyveres testületeknél és közigazgatásban (ORFK, BVOP, NBSz, NBF) tevékenykedő szakemberek, a Híradó Tanszék oktatóinak, valamint egyes polgári szervek képviselőinek részvételével és meghívása útján került végrehajtásra. A tudományos konferencia célja volt:

- a tudományos konferencia keretein belül vizsgálni az információbiztonság helyzetét a Magyar Honvédség szervezetében, az információbiztonsággal kapcsolatos trendeket és kihívásokat a XXI. században;

- áttekinteni az információvédelem rendszerének lehetséges továbbfejlesztését, a korszerű és perspektivikus eszközök információbiztonságot érintő jellemzőit, alkalmazási, üzemeltetési és fenntartási rendjük, szolgáltatásaik igénybevételére vonatkozó elvek kérdéseit;
- közreadni az akkreditálások, szakfelügyeleti ellenőrzések, a végrehajtás szakmai felügyeletének általánosítható tapasztalatait a számítógépek, számítógépes hálózatok elektronikus biztonságát érintően;
- a honvédelmi érdekből minősített nemzeti, valamint a nemzetközi szerződés alapján átvett, vagy nemzetközi kötelezettségvállalás kapcsolatos jogszabályi háttér vizsgálata, speciális követelmények elemzése;
- erősíteni a szervezett tapasztalatcserét és a rendszeres kapcsolattartást.

A konferenciát – *a nemzetközi együttműködés keretében* – Bertrand Giffault őrnagy, francia híradótiszt vezette le.

Hallgatóink számára mind a kedd késő délután, mind a szerda délelőtt aktív gyakorlással telt, amelynek során mindannyian behatóan megismerték a teljes

hálózat rendszertechnikai felépítését, illetőleg – *az eszközpark többségének tekintetében* – elsajátították az egyes munkahelyeken létesített kommunikációs eszközök használatát, valamint az igénybevehető szolgáltatások fajtáit.

A konferenciát követő ebéd után, délután Horváth Ferenc dandártábornok, az MH Támogató Dandár parancsnokának, Dr. Ujj András ezredes, a ZMNE tudományos rektorhelyettesének, Czirok Ferenc rendőr ezredes, az ORFK igazgatójának, valamint a Francia Köztársaság Budapestre akkreditált katonai attaséjának vezetésével közel száz megjelent vendég tekintette meg hallgatóink háromnegyedórás, angol nyelvű bemutatóját, amelyet Prof. Dr. Rajnai Zoltán mk. ezredes oktatási és minőségbiztosítási dékánhelyettes vezetett fel.

Negyedéves hallgatóink közül Flőgl Attila hallgató, mint parancsnok jelentett a résztvevőknek a zászlóalj helyzetéről, alá-fölérendeltségi viszonyairól és feladatrendszeréről, amelyet követően Giber Attila hallgató, híradó és informatikai főnök jelentett a hír- és informatikai rendszer kiépítésének elvéről és szolgáltatásairól. Giber hallgató a zászlóaljparancsnoknak, a hadműveleti részleg vezetője, Gál Richárd hallgatónak, valamint a vegyi-sugár részleg vezetője, Koncz Bence hallgatónak a bevonásával a gyakorlati példákon keresztül is bemutatta a vezető szervek és az elöljárók, illetve az egyes alegységek közötti kommunikációs fajtákat és megoldásokat, valamint használatukat.

Ezen bemutatóban Szalai Máté hallgató őrparancsnokként, Bodnár István hallgató a vegyi-sugár felderítő járőr parancsnokaként, valamint Szűcs Gergő hallgató a felderítő járőr parancsnokaként jelentett. A prezentáció során, a tábori körülmények között a hagyományos fónikus rádió, valamint távbeszélő kapcsolatokon túlmenően videokonferenciára, telefax és e-mail fogadására, adatbázisok lekérdezésére, illetőleg a harcászati rádiórendszer alkalmazásával képátvitelre is sor került.

A bemutató további részében Lengyel György r. főhadnagy, a rendőri részleg vezetője gyakorlati példákon keresztül mutatta be a békeműveleti tevékenység végrehajtásához biztosított rendőri képességeket. Ennek során légi, vízi, közúti és objektumvédelmi célú, valósidejű videojelek, valamint AVL információk térképi megjelenítése történt meg. A részlegvezető bemutatta továbbá a rendőri részleg és az egyes katonai alegységek közötti, EDR-en megvalósuló együttműködést biztosító rádióhíradást, valamint a rendőri adatbázisokhoz és levelezőrendszerhez történő hozzáférés gyakorlati megoldásait.

A délutáni gyakorlati bemutatót követően a résztvevők megtekinthették a vezetési ponton kívül települt haditechnikai, valamint a rendőrség felsorakoztatott földi, légi és vízi eszközeit, amelynek keretében aktívan kipróbálhatták a vízirendészet motorcsónakját is, illetőleg előadást hallgathattak meg a C2 vezetés-irányítási rendszerekről, valamint a rennesi Híradótiszti Iskola képzési és oktatási rendszeréről.

Hallgatóink számára a közel hetven órás intenzív fizikai és pszichikai terhelést követően szerda este eljöttek a pihenés órái, amelyet a Híradó Tanszék oktatói

állománya részéről testületileg kinyilvánított, a szakmai, emberi és katonai teljesítményüket, hozzáállásukat elismerő, méltató vélemény és köszönet mellett kezdhettek meg.

A gyakorlat utolsó napja a csomagolásé volt, amely során a résztvevő állomány hihetetlen gyorssággal képes volt a híradó és informatikai rendszert lebontani és szállításképes állapotba hozni. Ebédet követően a gyakorlat hivatalosan is véget ért, amelynek eredményét a négynapos, hosszú hétvége méltán koronázta meg.

Összegzés

A Híradó Tanszék több évtizedes gyakorlati tapasztalatokra alapozva szervezte meg a tanintézeti gyakorlatot. Úgy ítéljük meg, hogy az oktatás-kiképzés ezen mozzanata döntő lépés hallgatóink szakmai szocializációjában. Tanintézeti lehetőségeink – *mobilizálható haditechnikai eszközpark tekintetében* – jelenleg szűkre szabottak, azonban szilárd elhatározásunk, hogy e szakmai és hadikultúránkba beépült módszert minden körülmények között fenntartjuk és modernizáljuk.

A gyakorlat mellett oktatási egységünk idén elindult egy új úton is, amellyel célunk, hogy a katonai információbiztonság területét a szakmai berkekben „népszerűsítsük", illetőleg olyan fórumot hozzunk létre, ahol a szereplők közötti tudástranszfer létrejöhet. Nézőpontunk szerint a felügyeletet ellátó és egyben a szakmai munkát irányító szervezet és a tanszékünk által szervezett első információbiztonsági konferencia célját elérte, ezért 2011-ben ismét vállalkozunk arra, hogy a hagyományteremtés rögös útján előre haladjunk.

A rendezvények lebonyolításában nyújtott önzetlen szakmai és emberi segítségükért köszönetet mondunk

1) az MH Támogató Dandár állományából:

Horváth Ferenc dandártábornoknak,

Lédeczi Zoltán mk. főhadnagynak,

Kocsis Zsolt zászlósnak

2) az MH 43. Nagysándor József Híradó és Vezetéstámogató Ezred állományából:

Németh Sándor mk. századosnak,

Káldi Dániel törzsőrmesternek

3) az ORFK GF Közép-magyarországi Gazdasági Ellátó Igazgatóság állományából:

Czirok Ferenc r. ezredesnek,

Lengyel György r. főhadnagynak,

az ITO Rádió és Biztonságtechnikai Alosztály munkatársainak

4) a Budapesti Rendőr-főkapitányság állományából:

Vinczellér Gyula r. alezredesnek

5) a Balatoni Vízirendészeti Rendőrkapitányság állományából:

Dr. Springs József r. alezredesnek,

a Balatonkenesei Vízirendészeti Rendőrörs munkatársainak

6) a Francia Hadsereg tisztjének:

Bertrand Giffault őrnagynak

7) a Zrínyi Miklós Nemzetvédelmi Egyetem állományából:

Kovács István úrnak,

Dr. Németh József úrnak,

valamint a Hungaro Digitel Rt., a Magyar Villamos Művek Zrt. és telekommunikációs partnere a Microcom Kft., illetőleg a Pro-M Zrt. illetékes munkatársainak.

Zoltán RAJNAI

UN PORTRAIT MILITAIRE AU REFLET DE L'INSURRECTION HONGROISE

Cet article a pour but de présenter le colonel András Márton, commandant de l'Académie supérieure militaire hongroise pendant l'insurrection hongroise de 1956.

András Márton, capitaine encore en 1949, est devenu colonel en décembre 1952 à 29 ans à peine. Ce fut une carrière exceptionnelle par rapport à celles de l'époque.

En novembre 1955 le colonel a été nommé commandant adjoint général de l'Académie supérieure militaire Miklós Zrínyi puis commandant le 1e octobre 1956. Cette nomination était évidente pour tout le monde car l'Académie avait besoin d'un nouveau regard pour rafraîchir ses murs anciens. La majorité du corps professoral a accueilli avec sympathie la relève du commandant et a fondé de grandes espérances sur sa personne.

Le crédo militaire du colonel András Márton était alors déjà visible. Il appela à „l'Ordre" ce qui caractérisait tous ses efforts et tous ses consignes pendant la révolution de 1956.

Ses subordonnés ont vite reconnu qu'il assumait toujours la responsabilité de ses hommes ce qui lui a permis de garder la cohésion de l'Académie. Il n'y eut aucune insurrection intérieure ou manifestation extrémiste, bref ses collaborateurs l'écoutaient, à voir la confiance en lui leur donna un certain sens de sécurité.

Deux officiers de Transmissions de l'Académie s'attachèrent étroitement aux activités du commandant. János Haász, chef de transmissions du Passage Corvin devenu un centre important de la résistance, fut l'un de ceux qui étaient affectés dans les rues. Le commandant avait pour ambition de mettre de l'ordre avec ses militaires parmi les „garçons du passage Corvin". Le deuxième officier de Transmissions fut le capitaine Arnóczky, collaborateur proche du commandant de l'Académie. Le 10 novembre 1956 le colonel András Márton a réuni les officiers de l'Académie pour „leur déclarer qu'à l'Académie il fallait avoir de l'ordre." – a-t-il dit. Après la révolution il avait toujours confiance en la direction militaire du nouveau pouvoir mais il fut vite déçu. Les officiers désirant continuer leur carrière militaire dans l'armée ont du signer une déclaration d'officier. Le colonel Márton l'a également signée mais il ne voulait pas que l'Académie perde sa cohésion. Il a préféré choisir de démissionner puis de prendre sa retraite. Les nouveaux décideurs militaires ont laissé partir un chef de qualité ayant gardé son sang froid aux moments les plus chauds.

Le 5 février 1957 le colonel en réserve András Márton fut arrêté pour son rôle pendant la révolution. Qu'est-ce qu'il a fait? Rien. Il n'a voulu que l'ordre dans les rues. Il a affecté des officiers pour ramener l'ordre et donner des consignes aux insurgés encore à l'âge d'enfance.

Le 9 septembre 1958 la condamnation fut déclarée: 10 ans de prison, rétrogradation, confiscation de biens. Le monde extérieur n'en savait rien.

A l'automne 1960 András Márton, colonel privé de son grade menotté, fut amené de Vác à Budapest au procès du colonel Dienes, son ancien subordonné pour être écouté en tant que témoin.

Arrivant dans le couloir du tribunal il était salué par les officiers de l'Académie cités comme témoin se levant l'un après l'autre pour lui souhaiter avec respect du courage et de la santé.

L'acte d'accusation de András Márton est une lecture à analyser surtout sémantiquement. Elle ressemble énormément à celui créée contre Imre Garab à Debrecen sur le plan linguistique et terminologique. Le lecteur ne peut pas se débarrasser de l'idée qu'elle fut le résultat d'un ordre central. Les accusateurs n'ont pas voulu s'en remettre au hasard. 121 personnes ont été interrogées lors du procès de András Márton.

En avril 1962 la porte de sa prison s'est ouverte et il fut libéré après cinq ans et demi avec amnistie.

Après sa libération plusieurs personnes ont voulu le voir mais il n'a rien accepté des représentants du pouvoir. Les années passées en prison ont forgé sa personnalité. Il a souvent déclaré qu'il n'avait pas envie de se venger et qu'il ne se considérait pas comme un héros, au contraire il refusa ce titre. Il assuma tout ce qu'il avait fait à ce temps-là, y compris les huit points d'accusation, mais il ne se sentait jamais coupable et il ne pourra jamais oublier les choses qui lui sont arrivées.

On a écrit beaucoup de choses sur l'histoire de 1956. Cependant quand on s'intéresse aux événements une question se pose: Comment András Márton s'est-il retrouvé au passage Corvin?

colonel András Márton en 1956 et général de corps d'armée aujourd'hui

„Justifiez-vous!" András Márton a entendu cette ordre claire et simple dans la rue en se montrant dans la tourelle d'un char T34. La voix venait d'un enfant qu'il n'a pas vu. Au bout d'un certain temps il a vu un petit garçon. Son faux-nom était petit marmot. András Márton lui répondit: „Mon fils, il ne faut pas s'adresser

comme ça à un colonel." Finalement le petit marmot monta dans le char et amena le colonel à son chef au passage Corvin.

En entrant dans le cinéma Corvin (poste de commandement des résistants) il a entendu dire:

„Mais qu'est-ce qu'un officier communiste fait là? Tuez-le." Les enfants n'ont heureusement pas tiré puis leur commandant Iván Kovács lança: "on n'accepte pas de conseil d'un communiste." Il y eut une dispute après laquelle les garçons choisirent un nouveau commandant.

Le colonel András Márton a ensuite affecté dix jeunes officiers au passage Corvin que les historiens réussirent à identifier.

András Márton a été le commandant de l'Académie pendant quarante-cinq jours, raison pour laquelle il a subi 1884 jours en prison. Pour chaque jour qu'il a passé en tant commandant de l'Académie il „mérita" quarante-cinq jours dans en prison.

Pendant ce court temps de son commandement les officiers l'ont suivi instinctivement, il l'écoutait toujours. Quelques départements parlaient de sa nomination au poste de ministre.

Il a commandé l'Académie dans une période complexe où la situation changea du jour au lendemain dans les rues. Il savait toujours mener son institut à la baguette. András Márton fut naturellement réhabilité. En tant que général de corps d'armée il répond souvent aux demandes d'invitations. Au centre de son travail social il essaie de conserver le vrai esprit de 1956 en ayant des capacités mentales excellentes.

Il faudra encore beaucoup de temps pour avoir des réponses fiables et objectives aux questions qui demeurent à l'ordre du jour depuis des décennies et surtout depuis la relève du régime et qui sont d'actualité politique quotidienne.

Nous en esquissons quelques unes, dont l'analyse scientifique est en cours.

Voyons qu'au sujet de la demande de pardon qu'est-ce qui pourra s'avérer une solution rassurante?

Une fois la réhabilitation réalisée pourquoi les gens de 1956 sont-ils tout de même déçus?

Du point de vue militaire la question la plus intéressante peut se poser de façon suivante:

Est-ce qu'il y eut une chance? Non, il n'y en eut ni politiquement, ni militairement.

A ce temps-là la politique agressive liée au statut de grande puissance de l'Union Soviétique rendit évident, et non seulement pour les hongrois qu'il n'y avait pas de débouché ou de fuite. Les pays du camp socialiste tombèrent dans leur propre prison eux-même et la force militaire de l'Union Soviétique veillait au maintien du statut quo. L'Occident soutenait les pays socialistes en théorie mais les actions montrèrent autre chose. Le monde occidental trouvait qu'il ne valait pas le coup de prendre des risques pour nous, les Hongrois. Il s'avéra que les dirigeants des Etats-Unies ont même rassuré l'Union Soviétique qu'elle pouvait faire ce qu'elle voulait parce que le système Yalta ne changerait pas. De plus il y avait l'affaire de Suez.

La réaction de l'environnement proche, donc des pays socialistes était fraternelle, du moins des grandes puissances. Les frères de l'Orient lointaine en particulier des chinois se sont exprimés. Le comportement hypocrite de la Yougoslavie pourrait faire l'objet d'une étude spéciale sans parler de la Roumanie „accueillant" le groupe de Imre Nagy. Du point de vue militaire l'armée soviétique stationnait provisoirement dans le pays ce qui a tout expliqué. Dans certains pays amis surtout en Roumanie des divisions soviétiques étaient en réserve avec des unités aériennes aptes au combat. Nous étions entourés d'une force militaire qui aurait pu intervenir contre nous. Tout était prêt à l'échec.

Dans l'armée hongroise il y avait une centaine de militaires qui connaissaient bien la force armée de l'Union Soviétique puisqu'ils y avaient fait leurs études pendant de longues années. Quand on veut soupeser les chances il faut avouer la dure vérité. Nous devons faire la différence entre les insurgés équipés d'un seul fusil appelés garçons de Pest et l'incapacité de prise de décisions des chefs militaires hautement qualifiés. L'enthousiasme des garçons de Pest s'inspirait du manque d'informations et d'organisation militaire dans les situations concrètes car en réalité il s'agissait d'une révolution. L'appréciation d'un commandant disposant de pouvoir se fait sur la base de différentes critères, ce qui peut avoir un point de vue spécial en cas de révolution.

On dit que les Hongrois ne peuvent lutter qu'en cas de supériorité de l'ennemi. Mais il faut reconnaître que le combat contre les soviétiques était désespéré que l'élan sincère des Hongrois n'a pas pu non plus compensé. La période d'après–révolution liée au nom de János Kádár se caractérise par la rétorsion irrationnelle dont les dimensions ont été révélées bien plus tard et se sont incrustées comme l'une des périodes les plus sombres dans la mémoire des gens.

PÁNDI Ferenc – PÁNDI Erik3

KRITIKUS INFRASTRUKTÚRÁK - AZ ÉLELMISZER ELŐÁLLÍTÁS STRATÉGIÁJA, MINT A NEMZETGAZDASÁGI STRATÉGIA RÉSZE4

Absztrakt:
Az elmúlt évtizedben egyre többen foglakoznak a víz- és élelmiszerhiány stratégiai jelentőségével az emberiség életében. [1.2.3]. Jelen közlemény ezzel kapcsolatos gondolatokat foglal össze.
Kulcsszavak: kritikus infrastruktúra, nemzetbiztonsági stratégia

Jelenleg mintegy egymillió embert érint a vízhiány, kb. ugyanannyi ember éhezik, és ennek a duplája pedig éhínségben szenved. A globális felmelegedés következtében növekedhet a vízhiány, amely további élelmiszerválsághoz vezethet.

A megnövekedett kereslet következtében a pénzügyi befektetők figyelme az olaj mellett az élelmiszerek felé fordul. Ez azt is eredményezheti, hogy az élelmiszer stratégia fegyverként szolgálhat különböző államok kezében. Tovább bővítheti a válságot az a kérdés, hogy a mezőgazdasági termékekből élelmiszert, vagy bioüzemanyagot kell-e előállítani, annak ellenére, hogy jelenleg az élelmiszer előállításra felhasználható mezőgazdasági alapanyag termeléséhez szükséges termőterület bioüzemanyag gyártásra fordítandó része elenyésző [4].

Ennek megfelelően pld. Brazília mezőgazdasági területének 2%-án az ország benzin fogyasztását teljes egészében ki lehetne váltani az ott termelt termékekből történő etanol gyártással. Mindazonáltal e probléma legfőbb okának - a fentiek mellett - a túlnépesedés nevezhető, de kétségkívül egyes esetekben a vízkészletek egyenlőtlen eloszlása és az infrastruktúra hiánya is további gondokat okozhat.

A fentiek szellemében, egyesek úgy gondolják, hogy az élelmiszer-, és vízhiány okozta konfliktusok feloldása a gazdasági és politikai megoldásokban rejlik, annak ellenére, hogy az ügynek vannak katonai vonatkozásai is. Sajnálatos módon az ügyet több helyütt marginális kezelik, figyelmen kívül hagyva annak globális vonatkozásait.

Magyarország nemzeti bizottsági stratégiája, amely a veszélyek között megkülönbözteti a globális, regionális, és belső kihívásokat, az azonosítható globális kihívások közé sorolja e természeti civilizáció és egészségügyi veszélyforrásokat [5].

Hazánk nemzeti biztonsági stratégiája egyúttal kihangsúlyozza azt is, hogy a biztonság komplex felfogásának megfelelően a kitűzött célok megvalósításának feladata megoszlik az egyes ágazatok között. Ezért fontos az egyes területeken végzett munka összehangolása, mind a kidolgozás, min az alkalmazás területén.

3 szerzők: Pándi Ferenc CSc, Magyar Élelmiszer-tudományi és Technológiai Egyesület Környezetgazdálkodási Bizottságának Elnöke, Pándi Erik PhD, ZMNE BJKMK Híradó Tanszék vezetője

4 a közlemény a Bolyai János Kutatási Ösztöndíj támogatásával készült

Ennek figyelembevételével a továbbiakban vizsgáljuk meg az élelmiszerágazat jelenlegi helyzetét, lehetőségeit, feladatait és, hogy ezek a kérdések hogyan kapcsolódnak a komplex nemzetbiztonsági stratégiához.

Az elmúlt évtizedek élelmiszer-túltermelése után ismét egyre súlyosabb társadalom-politikai kérdés az élelmiszerellátás biztonsága. Az import függés, a jelenleg zajló válság, az áruk világméretű szabad áramlása, az élelmiszerbiztonsági kockázatok felértékelik a helyi élelmiszer-beszállítókat, akik jobban tudják garantálni a biztonságot.

Ebben a helyzetben az élelmiszer előállítás területén, komparatív előnyökkel rendelkező olyan országoknak, mint amilyen hazánk is, mindent meg kell tenniük annak érdekében, hogy ezt az előnyüket a lehető legjobban kihasználják.

Az élelmiszergazdaság kiemelkedő adottságait úgy kell kihasználni, hogy az korábbi versenyképességét visszanyerve, növelje, és a lehetőségekhez képest járuljon hozzá a nemzetgazdálkodás fejlődéséhez [6].

Az élelmiszeripar mind Magyarországon, mind az Európai Unióban jelentős szerepet játszik a nemzetgazdaságban.

Az Európai Unió élelmiszer-előállítása, illetve gyártása, a közösség feldolgozó iparának a maga 13,5%-kal elsőszámú ágazata is, az itt lévő több mint 300 ezer vállalkozás, mint egy négy millió embert foglalkoztat, és ágazat termelési értéke megközelíti az ezer milliárd eurót.

Magyarországon a 14 ágazatot átfogó feldolgozóiparon belül - stratégiai jelentősége ellenére - az élelmiszeripar részesedése az ipari teljesítményből csökkenő tendenciát mutat. Amíg 2002-ben 14,9 %-os részesedéssel a második volt az ágazatok rangsorában, addig 2008-ra részesedése 9,8 %-ra csökkent (bruttó termelési értéke ekkor mintegy 2082 milliárd Ft volt). Ez az ágazati rangsorban még mindég a harmadik helyet jelenti, mutatva az ágazat továbbra is kiemelkedő jelentőségét.

A magyar élelmiszeripar az élelmiszer-ellátási lánc központi fontos eleme. Élelmiszergazdasági jelentőségére jellemző, hogy még jelenleg is a hazai mezőgazdasági termelés mintegy kétharmadát vásárolja fel tovább-feldolgozás céljából. Ez azt jelenti, hogy az élelmiszeripar által 2008 évben közvetlenül foglalkoztatott mintegy 100 ezer fő mellett több százezer mezőgazdaságból élő állampolgár megélhetése függ az ágazat teljesítményétől.

Stratégiai fontossága ellenére az ágazat súlyos válságban van.

A magyar élelmiszeripar nem tudta kihasználni az EU csatlakozásból adódó lehetőségeket, hazai beszállítói pozíciója csökkent, különösen a többi új csatlakozó tagállamból származó import térnyeréssel szemben. Exportorientáltsága ugyanakkor jelentős, külkereskedelmi mérlege még mindig pozitív, ez a szaldó azonban fokozatosan csökken. Jövedelemtermelő képessége évek óta romlik: adózás előtti eredménye az utóbbi két évben tovább zuhant, jelentősen alulmúlva a hazai mezőgazdaság hasonló mutatóját [7].

Mindezeket figyelembe véve nyilvánvalóvá vált, hogy e területen fel kell tárni a kibontakozás lehetőségét.

Az általános, minden ágazatot befolyásoló gazdasági/szabályozási környezet kedvező megváltoztatásán túl (elvonások jellege, mértéke, jogbiztonság, vállalkozásbarát adminisztráció, stb.) a magyar élelmiszeripar váltságból való kibontakozásához olyan sürgős lépéseket kell tenni mint pld., a forráshoz juttatás, szerkezetát-

alakítás, támogatási feltételek szabályozása, K+F tevékenység fokozása, szakirányú képzés, erősítése, stb. Ezek szükségességére több feltáró dokumentum, tanulmány is rámutatott [8, 9, 10].

Ennek megfelelően miután, – így hazánkban is – az élelmiszert, a fejlett világ szinte minden országában stratégiai termékként kezelik, jelentős fejlesztési programok kezdődtek el. Az is megfigyelhető, hogy az agrárinnovációt, a kutatást, és fejlesztést kiemelten, és gyors ütemben fejlesztik, mivel a versenyképes élelmiszer-előállításnak ez a legalapvetőbb feltétele.

Ugyanakkor mint stratégiai termék az élelmiszer kiemelt figyelmet kap, miután mindennapi életünk egyik legfontosabb előfeltétele.

Az élelmiszer a szállítótól, – forgalmazótól – az élelmiszerláncon keresztül jut el a fogyasztókhoz. Ez egy speciális kapcsolatrendszer, amelynek elődleges eleme a termékek begyűjtése és tárolása, majd a továbbiakban az élelmiszer feldolgozása, forgalomba hozatala és forgalmazása, de ide tudnánk még olyan további elemeket is sorolni, mint például a biztonság, bizalom, etika, környezetvédelem és egyéb kapcsolódó információk.

A rendszer működésének hiányában a biztonságos élelmiszer nem termelődik meg, vagy a biztonságos élelmiszerrel való ellátottság meghiúsul. Ezért a biztonságos élelmiszertermelés, az élelmiszerrel való ellátás biztosítása, valamint az élelmiszerlánc védelme az ú. n. kritikus infrastruktúrák közé sorolható [11], amelyet különböző veszélyek (pl.: szándékosan ártó jellegű, illetve természetes veszélyek, helytelen emberi beavatkozás, stb.) érhetnek. Ezért azt természeti katasztrófáktól, balesettől, terrorcselekményektől védeni kell.

A fenntartható fejlődés egyik elengedhetetlen feltételének az élelmiszerláncnak a biztonsága, elsősorban az ú. n. élelmiszerbiztonsági rendszeren keresztül valósítható meg. Az európai Unió átfogó élelmiszer-biztonsági stratégiát léptett életbe, mely az élelmiszer-biztonságon túlmenően állat- és növényegészségügyi, valamint állatjólléti kérdésekkel is foglalkozik. A stratégiának köszönhetően az élelmiszerek útját a termelőtől a fogyasztóig végig - akár több uniós tagországon keresztül is – nyomon lehet követni.

A fentieket a 178/2002. EK rendelet szabályozza, amelynek következtében létrejött az Európai-biztonsági Hatóság (EFSA), amely Igazgató Tanácsának Elnöki tisztjét 2008 óta magyar szakember (Dr. Bánáti Diána) tölti be.

Ezzel egyetemben megállapították az általános élelmiszerbiztonsági alapelveket:

- ·integrált megközelítés,
- ·az élelmiszerlánc szereplőinek felelőssége,
- ·az elővigyázatosság alapelve,
- ·az elemzési rendszer,
- ·nyomon követhetőség,

Ekkor született döntés arról is, hogy annak érdekében, hogy a károk elhárítására, az élelmiszer-biztonságot fenyegető veszélyek felszámolására az EU sürgősségi risztórendszert (Rapid Alert System for Food and Feed) működtet, amely vészhelyzetben megóvja a fogyasztókat. Az EK rendeletből adódó feladatokat, a rendszer működtetését hazánkban az Élelmiszer-biztonsági Hivatal látja el.

Mint az előzőekben láthattuk az Európai Unió és a NATO egyre inkább fontosnak tartja az egyes tagállamok és a szövetségek által működtetett infrastruktúrák potenciálisan veszélyeztetett kritikus elemeinek védelmét. Ezért a hatékony védelem érdekében minden ez irányú tevékenység szoros együttműködésben, összehangolt, szabályozott módon kell, hogy továbbra is megvalósuljon.

Hazánk nemzetbiztonsági stratégiája által kritikus elemek közé sorolt biztonságos élelmiszerrel való ellátás tekintetében e területen a nemzetközi együttműködés megfelelőnek mondható. A magyar élelmiszeripar, amely az élelmiszerellátási lánc jelentős központi eleme, viszont stratégiai fontossága ellenére jelenleg súlyos válságban van.

Miután a biztonság komplex felfogása szerint a célok megvalósításának feladata megoszlik, az egyes ágazatok között, és fontos az egyes területeken végzett munka összehangolása, ezért a hazai élelmiszergazdaság, egyébként kiváló adottságait, - a megfelelő feltételek kialakítása mellett - úgy kell kihasználni, hogy a korábbi versenyképességét visszanyerje, és ezúttal hozzájáruljon a nemzetgazdálkodás fejlődéséhez, és be tudja tölteni elvárható szerepét a nemzetbiztonsági stratégiában.

Összefoglalás

A szerzők közleményükben az élelmiszer stratégiának nemzetgazdasági stratégiában betöltött szerepével foglalkoznak.

A nemzetközi és hazai helyzetet vizsgálva megállapítják, hogy egyre súlyosabb társadalmi-politikai kérdés az élelmiszerellátás biztonsága, amelyet a nemzetbiztonsági stratégiák a kritikus infrastruktúrák közé sorolnak.

Áttekintve az élelmiszeripar Európai Uniós és hazai helyzetét, megállapítják, hogy az jelentős szerepet tölt be a nemzetgazdálkodásban. Ugyanakkor megállapításra kerül az is, hogy az élelmiszerellátási-lánc - központi fontos eleme az élelmiszeripar - stratégia fontossága ellenére hazánkban jelenleg súlyos válságban van.

Miután az élelmiszerlánc, amelyen keresztül az élelmiszer az előállítóktól a fogyasztókig jut el, biztonsága elsődleges kérdés, ezért az Európai Unióban és hazánkban is ú. n. élelmiszerbiztonsági rendszerek kerültek kialakításra, amelyek jelenleg is hatékonyan működnek.

Ahhoz azonban, hogy az élelmiszeripar, az élelmiszer stratégiában, és így a nemzetgazdasági stratégiában is betölthesse megfelelő szerepét, el kell érnie versenyképességének visszanyerését, természetesen a megfelelő feltételek biztosítása mellett.

Irodalomjegyzék

[1] Kecskeméti József: Nem csak a szükségesség váltja ki az éhséglázadásokat. www.honvedelem.hu 2010. január 8.

[2] A biztonsági kihívások új felfogása., Corvinus Külügyi és Kulturális Egyesület 2009.

[3] Az élelmiszergazdaság a nemzetgazdaság stratégiai ágazata. Agrár Hírek, 2009. július 7.

[4] Washington International Renewable Conference, Washington 2008. március 4.

[5] Magyarország nemzetbiztonsági stratégiája. Corvinus Külügyi és Kulturális Egyesülés, 2008.

[6] A magyar élelmiszeripar stratégiai jelentősége. FVM Élelmiszerlánc-elemzési Főosztály 2009. május 8.
[7] Jelentés az agárgazdaság 2008. évi helyzetéről. FVM 2009. szeptember.
[8] A magyar élelmiszeripar egyesületet innovációs stratégiai terve. (2009-2024) ÉFOSz. 2009.
[9] Élelmiszeripari K+F és innováció. FVM, 2009.
[10] Az Élelmiszeripar Ágazata, Párbeszédbiztonság állásfoglalása a magyar élelmiszeripar válságos helyzetéről 2009.
[11] Négyesi Imre: Az információgyűjtés jövőképe, Hadtudományi Szemle I/3. szám, 96. oldal

KERTI András – PÁNDI Erik – TÖREKI Ákos5

A VEZETÉSI ÉS INFORMÁCIÓS RENDSZEREK ELMÉLETI MEGKÖZELÍTÉSE6

Absztrakt:
Jelen közlemény a vezetési és információs rendszerek néhány elméleti kérdését dolgozza fel.

Kulcsszavak:
kritikus infrastruktúra, nemzetbiztonsági stratégia

Bevezetés

A korszerű hadviselés, a korszerűen felszerelt haderő sikeres tevékenységének egyik legfontosabb eleme, hogy rendelkezzen hatékony, a feladatok végrehajtását biztosító és támogató vezetési és irányítási rendszerrel. Ez a rendszer nem nélkülözheti a hatékony irányítási filozófiákat éppúgy, mint a vezetéshez szükséges technikai eszközök modernségét, fejlettségét, a béke- és a békeállapottól elérő helyzetek gyors változásához szükséges reagálási idő alkalmazkodását a vezetésben.

A XXI. század technikai eszközeinek gyors fejlődése, a nagypontosságú fegyverek jelenléte, a kommunikációs és informatikai, az információs forradalom időszaka új vezetési elveket kíván, melyek szoros összefüggést feltételeznek, harmonizálnak a technikai rendszerek megfelelésével. A Magyar Honvédség a vezetési és információs rendszer üzemeltetésével a haderő alkalmazkodási képességének feltételeit biztosíthatja akkor, amikor a missziós szerepvállalások fokozódásának idején egyrészt a külszolgálaton lévő kontingensek irányítási rendszerét igazítja a vezető nemzet szerepét ellátó parancsnokság rendszeréhez, másrészt a honi területen lévő csapatainak vezetési és irányítási rendszerét saját nemzeti érdekeinek védelme érdekében fenntartja. A két rendszer sok esetben eltérő vonásokat, jellemzőket hordoz, hiszen a missziós tevékenységek országhatárainktól távol folynak, a vezetés és irányítás elvi és technikai feltételei kompatibilitási hiányosságokat nem szenvedhetnek, vagyis a más nemzetek által alkalmazott elveket és módszereket éppúgy kell tudni alkalmazni, mint a kontingens belső működését biztosító, nemzeti szinten begyakorolt és elfogadott irányítási mechanizmust és technikai eszközrendszert. E területeken a rendszerek elsődleges feladataként kell meghatározni, hogy a modern technológián alapuló vezetéstechnikai eszközök biztosítsák a reális idejű információhalmazokat a parancsnok, a döntéshozók részére, másrészt vezetési elveinknek megfelelő technikai eszközpark álljon rendelkezésre a műveletek, missziós tevékenységek, békeműveletek speciális feladatainak végrehajtásához.

Feladataink végrehajtásának nem lehet azonban egyetlen feltétele a technikai eszközpark, a korszerű eszközrendszer, hanem az irányítási mechanizmus helyzetekhez adaptált működtetése is feltételét képezi a sikereknek. A feladatrendszerek

5 szerzők: Kerti András PhD, ZMNE BJKMK Híradó Tanszék adjunktus, Pándi Erik PhD, ZMNE BJKMK Híradó Tanszék főiskolai tanár, Töreki Ákos MA, ZMNE BJKMK Híradó Tanszék tanársegéd

6 a közlemény a Bolyai János Kutatási Ösztöndíj támogatásával készült

változása, a technológia fejlődése maga után vonja a vezetési és irányítási rendszerek változtatását, módosítását, hiszen ez alapfeltételként jelentkezik a korszerűség, a hatékonyság realizálásának szintjén.

Jelen közleményünkben vizsgálat alá vetjük a vezetési és információs rendszerekkel kapcsolatos elméleti tételeket.

1 Vezetési és információs rendszer

Az 1990-es évek első felében és még napjaink általános katonai gondolkodásában is egy le nem zárult paradigmaváltás figyelhető meg, amely érinti a hadsereg társadalomban betöltött szerepét, feladatait, a hadtudományi kutatások irányainak és tartalmának változását, melyet determinánsan a polgári élet kutatási területeihez történő közeledés jellemez. A változás lényegét az alábbi három fő okban látjuk:

- Hadikultúra váltás:

A Varsó Szerződés (VSZ) felbomlása és a kedvező politikai folyamatok eredményeként hazánk NATO-tagsága nem egyszerűen az egyik szervezetből a másikba történő „átállásként" jelent meg. Míg a VSZ-tagállamainak katonái a mozgás centrikus hadikultúra hadművészetét gyakorolták, a NATO katonai gondolkodói az anyag centrikus hadikultúra hívei voltak.

- Terminológiaváltás:

NATO-tagságunkkal a terminológiai, eljárásbeli változások nem csak az új „szövetségi nyelv" változását, hanem egy új kifejezés-rendszer, fogalomértelmezési szükségességet is magukkal hoztak. Az új definíciók jelentéseinek, tartalmának egységes értelmezése, vagy annak hiánya felületesen nem annyira szembetűnő jelenség, hiszen nagyon sok kifejezés hasonló tartalommal bír, azonban a két különböző „iskolán" (szövetségi rendszerben) felnőtt szakembergárda esetében, ha nem is teljesen eltérő, de esetenként nem is egymással azonos fogalmakat ért ugyanazon definíció alatt. Ilyen például a szakterületünkről vett „információtechnológia" amely jelenthet akár információ-feldolgozó eszközt (akár elektronikus akár nem), más számára azonban csak a szűken vett informatikai eszközparkot, eljárási módszert, megvalósítási lehetőséget jelenthet. Vagy másik példaként említhetném a kommunikáció kifejezést, ami technológiai szemléletű egyének számára a kommunikációs rendszert, annak technikai és személyi feltételeit, más számára egy megjelenési lehetőséget jelent a külvilág felé.

- Alapvető feladatváltás:

A rendszerváltás előtt egy „bipoláris" világban éltünk, amelynek alapvető katonapolitikáját a két fél szembenállása határozta meg, amelyben az I. és II. világháborúra is jellemző frontális jellegű hadműveleti és harcászati feladatokat vizionáltunk. Napjaink katonapolitikai, biztonságpolitikai szakértőinek és Magyarország hivatalos álláspontja szerint *„[a] Magyar Köztársaságot belátható időn belül hagyományos jellegű fegyveres támadás veszélye nem fenyegeti, bekövetkezése hosszabb távon is alacsony valószínűségű."*[1]. Ebből következtetve a Magyar Honvédség elsősorban a nemzetközi szerepvállalásra, a különböző missziós feladatokra készül fel.

Megítélésünk szerint tehát a napjainkban a magyar katonai terminológiában keverednek a különböző, a rendszerváltás előtti és utáni fogalmak, definíciók meghatározások és azok értelmezése, nincs letisztult kép, kialakult azonos hivatalos

szemlélet. A vezetési és információs rendszerek tekintetében a tisztánlátást továbbra is nehezítő tényező a folyamatos technikai-technológiai fejlődés, az informatikai és híradó rendszerek között lezajlott konvergencia.

2. A vezetési és információs rendszer

Alapproblémaként kezeljük tehát a fogalmi egység hiányát. A vezetési és információs rendszer vizsgálata megköveteli néhány alapfogalom tisztázását. A *„**katonai vezetés** az adott időszakban érvényben lévő, az ország védelmi helyzetére vonatkozó törvényi szabályozás, és a bevezetett rendszabályok alapján megvalósuló békevezetés, vagy háborús vezetés, az alárendeltek befolyásolásának folyamata a feladat eredményes végrehajtása érdekében. Lényege a parancsnoki akarat és szándék megvalósítása."*[2]. A parancsnok az alárendeltek „befolyásolását"a vezetési rendszerrel teszi, amely: *„egy szervezeten belül a vezetés folyamatai, a vezetési módszerek és vezetési eszközök együttese"*[3]. A vezetési rendszer felépítése tehát a parancsnok feladata, amelynek kialakítását vezetési ismereteire, a vezetési módszerére vonatkozó elképzelések alapján határoz meg.

A katonai vezetés akkor tölti be szerepét, ha azt felkészült és az egyszemélyi felelősséget vállaló parancsnokok (vezetők) gyakorolják, akik a módszerek, eljárások, vezetési stílusuk megválasztását, a végrehajtók motiválását a körülményekhez igazítják [3]. Ezen megállapítást figyelembe véve meghatározhatjuk a vezetés részterületeit is, amelyek a következők:

- információgyűjtés,
- információ szelektálás,
- szintetizálás,
- célkitűzés,
- tervezés,
- döntés,
- szervezés,
- irányítás,
- ellenőrzés,
- eredménymérés (értékelés).

Alapvetően megfelelőnek tartjuk fenti gondolatmenetet, azonban véleményünk szerint két fontos tulajdonság nem azonosítható be, úgymint a *feladatorientált jelleg*, vagyis a tevékenység meghatározásának feladata, joga, amit vagy az elöljáró szab meg a parancsnok részére (mint például egy harcászati feladat), vagy éppenséggel az alaprendeltetéséből fakadóan kell megoldania (kiképzési, vagy fenntartási feladatok). Másrészről az előbbiekben bemutatott részterületek teljesen lineárisnak mutatják be a folyamatot, pedig a résztevékenységek egymásra hatása és visszahatása jelentős szerepet tölt be a vezetés folyamatában. Példaképpen hozhatók olyan gátló tényezők is, amelyek lehetetlenné teszik, vagy csak aránytalanul nagy áldozatok révén tehetik vállalhatóvá a célkitűzés megvalósítását, amikor is az egész vezetési folyamatot át kell tekinteni, és új célkitűzéseket, terveket, elgondolásokat kell készíteni. E résztémakörben másik példaként hozhatjuk fel az ellenőrzés és eredmény-mérés eseteit, amikor az észlelt negatív információk alapján lehet, hogy a szervezési és a tervezési folyamatot kell korrigálni. Az egész folyamat mozgatórugója megítélésünk szerint az **információáramlás.**

A vezetői folyamat tehát felfogható a különböző információk továbbításának is, amikor tervek, utasítások, intézkedések eljuttatása valósul meg az érintett feleknek, másrészről a végrehajtásról történő visszacsatolás, a tervezés és a szervezés is különböző információkkal kerül alátámasztásra.

Ugyancsak fontosnak tartjuk megvizsgálni, hogy mely információk gyűjtése szükséges, illetőleg melyeket kell szelektálni és szintetizálni. Erre a kérdésre a parancsnok információs igényei adják meg a választ. Fontos megválaszolni tehát azt a kérdést, hogy a szükséges információkat ki és milyen módon fogja szolgáltatni a vezetési rendszer számára.

Vizsgálódásaink alapján úgy ítéljük meg, hogy a parancsnok számára a különböző információkat alapvetően az elöljáró és alárendeltjei, valamint a törzs különböző beosztású tagjai saját adatbázisaikra és információs kapcsolataikra támaszkodva szolgáltatják. Az ellenségre és a környezetre vonatkozó adatokat a felderítési rendszer, a saját erőkre vonatkozó adatokat a hadműveleti, logisztikai, és személyügyi rendszer, a saját csapatok vezetését a híradó és informatikai rendszer biztosítja

Természetesen ezek az alrendszerek akár még kisebb alrendszerekre is bonthatók, attól függően, hogy milyen mélységben és céllal kívánjuk vizsgálni a rendszert. Az, hogy ezeknek az információs alrendszereknek mi az adattartalma, nagy részben függ a feladat jellegétől, a parancsnok szándékától és a törzs szervezetétől. A törzs szervezete függ az alegység, illetve egység alaprendeltetésétől és nagyságától, valamint attól, hogy a különböző szervezeti elemeket a kötelék vezetése mely szervezetei elemben tervezi alkalmazni.

Fenti gondolatok működésmechanizmusát egyszerű belátni, amennyiben összevetjük egy század vezetési rendszerét a dandár vezetési rendszerével, vagy ha éppen a frekvencia menedzsment feladatainak változását vizsgáljuk a különböző szervezetek között. Egyértelműnek tűnik tehát azon tény, amely szerint minél magasabban helyezkedik el a parancsnok a vezetési struktúrában, annál több információra van szüksége előírt feladata megfelelő végrehajtásához. Azt viszont már nehezebb belátni, hogy a különböző szinteken elhelyezkedő parancsnoknak ugyanolyan fajta információkra van szüksége csak más –*esetlegesen több, vagy kevesebb* – adattartalommal.

Abban az esetben, amikor a szakaszparancsnok parancsot kap elöljárójától az egyértelműen vezetési és irányítási információnak minősül, amikor viszont figyelembe veszi alegysége lőszerkészletét, az már logisztikai információ, ha azonban az ellenségről megfigyeléseket gyűjt, az felderítési információ. Természetesen ezen információk nagysága egység és magasabb egység szinten már azt eredményezheti, hogy nem elég egyetlen ember a feldolgozásukhoz, hanem több emberből álló törzs összehangolt munkájára van szüksége a parancsnoknak az információk szakszerű szolgáltatása érdekében. Bármilyen nagy is a törzs, annak feladata, hogy a parancsnok számára a szükséges információkat előállítsa a feladat eredményes végrehajtása érdekében. Megállapíthatjuk, hogy az információt szolgáltató alrendszer a törzs szakbeosztású személyzete (felderítő, kiképző, hadműveleti, humán stb.) [4].

Kérdésként merülhet fel, az információk megfelelő entitásokhoz való eljutása. A jelentések, adatok, üzenetek címzettekhez történő eljuttatását és megfelelő feldolgozását a vezetési és információs rendszer számára szolgáltatást nyújtó ***híradó***

és informatikai rendszer feladata. Más szóval **a híradó és informatikai rendszer a vezetés és információs rendszer technikai alrendszere**.

Összegezve az eddigi definícióhalmazt megállapítható, hogy a vezetési és információs rendszer elemei közé sorolható az annak működtetésére vonatkozó **elvek, elgondolások**, az **információkat szolgáltató alrendszer**, valamint az információk áramlását, feldolgozását és tárolását biztosító **technikai alrendszer**.

3. A vezetési és információs rendszer technikai alrendszerének feladatai

Az információs társadalom és így az információs társadalom hadseregének egyik legnagyobb kihívása az információk biztonságának egy, a költségek és a lehetséges károk közötti arányos megvalósítása.

Az információvédelmi mechanizmusok az információs infrastruktúra minden területére beépülve, egymással együttműködve fejtik ki hatásukat. Az információforrás a rendszer legkevésbé meghatározható eleme, amely minden egyes esetben más és más lehet, úgymint lehet egy szenzor adata, egy felderítő jelentés, vagy éppen lehet egy másik információs rendszer. Fontos kérdés viszont, hogy ezek az információforrások mennyire vannak az ellenőrzésünk alatt. Előfordulhatnak olyan esetek, amikor teljesen, részben, illetve teljesen független tőlünk. Éppen ezért csak olyan mértékben garantálhatjuk az információforrás információinak biztonságát és megbízhatóságát, amilyen mértékben ellenőrzésünk alatt tartjuk magát a forrást.

Az információforrások az általuk szolgáltatott adatok jellegét tekintve a vezetés és információs rendszer technikai alrendszere szempontjából alapvetően kétfélék lehetnek:

- analóg;
- digitális jeleket szolgáltatók.

Az analóg jelek lehetnek, mozgó- és állóképek, beszéd, írás. A digitális jeleket szolgáltató információs források lehetnek különböző szenzorok, illetve egy másik információs rendszer adatai is.

A vezetési és információs rendszereket kiszolgáló technikai alrendszer általános elfogadott megnevezése jelenleg Híradó és Informatikai Rendszer. Megítélésünk azonban az, hogy a vezetési és információs rendszer technikai alrendszere *a vezetés és az információ szolgáltatás érdekében telepített információ és adat továbbító, feldolgozó és tároló eszközök (hardver és szoftver) és az őket telepítő és üzemeltető személyi állomány összességét* jelenti. Az információtovábbítás, valamint a feldolgozást-tárolást végrehajtó egységek feladatai – *véleményünk szerint a szakmai közösség által elfogadottan* – a következőképpen került megfogalmazásra: *„Az a tudomány, amely az információk keletkezésének, kezelésének és felhasználásának elméleti és gyakorlati megvalósításával és eszközrendszerével foglalkozik nem más mint az informatika. Az információs rendszer „nyersanyagait" azonban nemcsak felhasználni – feldolgozás, tárolás, megjelenítés, elosztás, stb. – , hanem továbbítani is kell. A rendszer, amely a különböző formában megjelenő híreket, adatokat, stb. továbbítja a híradó rendszer."* [5].

Ezen elgondolásból kiindulva megállapíthatjuk, hogy a faxberendezések (papíralapú dokumentumok átalakítása elektronikus jelekké) és telefonok (szóbeli közlések átalakítása) ugyan olyan végberendezések, mint a számítógépek. Tapasztalataink szerint a telefon és a fax berendezéseket, valamint az őket összekötő há-

lózatokat jelenleg a híradó rendszer részeihez sorolják a Magyar Honvédségben, amíg a számítógépek, a hozzájuk tartozó szoftverek és az őket összekötő hálózatok pedig az informatikai rendszer részeit képezik. Véleményünk szerint ezen, egységesnek nem tekinthető álláspont a haditechnikai rendszerek eltérő fejlettségi viszonyaiban keresendő. Meglátásunk szerint a nem katonai szférában az évek során sokat emlegetett informatikai és híradó rendszerek konvergenciája befejeződni látszik. A polgári rendszerekben a különböző szolgáltatók egymással versenyezve ajánlanak komplex szolgáltatásokat, amelyekben beletartozik mind az infrastruktúra, mind a tartalom is. A legújabb mobil készülékekkel pedig már képesek lehetünk az internetezésre és tévénézésre is a telefonáláson túlmenően. Hazánkban sajnálatosan megfordult azon trend, amely szerint a katonai fejlesztést követi a civil fejlesztés, előzőekben ismertetett folyamat – *akár* – mérvadónak is tekinthető.

A magyar katonai híradó és informatikai rendszerek konvergenciájára kettő, alapvetően különböző modellt találtunk vizsgálódásaink során. Az egyik szerint mindig is megmarad valamiféle különállás a két rendszer között, a másik teljes összeolvadást ígér. Véleményünk szerint jelenleg három különböző szintű rendszerről beszélhetünk a Magyar Honvédség tekintetében.

Az első az állandó telepítésű technikai alrendszer, amely a legfejlettebbnek tekinthető, összeköttetésben van a többi kormányzati rendszerrel. Esetükben már a tartalomszolgáltatás is kialakulóban van.

A harmadik fejlettségi szinten a tábori rendszer található, amely a végbement politikai és gazdasági változások hatására megrekedt az 1980-as évek technológiai szintjén. Ezen megállapítást még akkor is reálisnak tartjuk, ha figyelembe vesszük az új URH rádiókat és az egyéb úton (támogatásként) beérkezett RH eszközöket. Hiába érkeztek meg ezek az eszközök, hiszen lényegében véve nem illeszthetők a saját rendszerünkhöz, attól mintegy elkülönülve léteznek. Ebből adódóan nem létezik egy teljes, a mai kornak megfelelő komplex tábori rendszer, amely a vezetés és irányítási rendszerek technikai alrendszereként működhetne.

A második fejlettségi szint egy kis magyarázatra szorul. Az 1990-es évek közepétől hazánk is részt vesz különböző missziókban. Nagy valószínűséggel a missziókat nem lehetett volna sikeresen végrehajtani megfelelő vezetési és irányítási rendszer nélkül, azonban a missziók vezetés és információs rendszerének technikai alrendszere szerintünk nem tekinthető sem állandó rendszernek, sem tábori rendszernek. Egyértelműnek tűnik számunkra, hogy állandó rendszernek azért nem, mert hazánktól távol, ideiglenesen üzemeltették, üzemeltetik, tábori rendszernek viszont azért nem, mert ezek a híradó és informatikai központok a misszió kezdetén letelepítésre és a misszió végén pedig elbontásra kerültek, közben nem kellett őket úgy mozgatni, áttelepíteni mint egy hagyományos katonai hadművelet során. Ennek következtében, megítélésünk szerint a fejlettségük is a kettő szint között helyezkedik el.

Leszögezhető, hogy a legjobb minőségű tábori eszközök kerültek összeépítésre a kereskedelemben kapható berendezésekkel. Természetesen, minél előrehaladottabb a rendszerek fejlettsége, annál nehezebb elkülöníteni az „informatikai rendszert" a „híradó rendszertől". Véleményünk szerint a vezetés és irányítás technikai alrendszerének fogalmát mint híradó és informatikai rendszer korszerű fogalmát az Összhaderőnemi Doktrína tartalmazza, hiszen leszögezi, hogy *„a híradó és infor-*

matikai rendszer magába foglalja a híradó és informatikai eszközállományt (hardver), az eszközöket működtető rendszer- és az alkalmazói feladatok ellátását elősegítő alkalmazói szoftvereket, az üzemeltetési és alkalmazási eljárásokat, a rendszerben rögzített, illetve továbbított adatokat, valamint az üzemeltető személyi állományt." [6]. Fentiekből látható, hogy a híradó és informatikai rendszer egymástól elválaszthatatlan.

4. A vezetési és információs rendszere technikai alrendszerének felépítése

Az 1990-s évek elejétől a katonai munka területén is megjelentek a személyi számítógépek, amelyeket az ezredforduló idején elkezdtünk helyi hálózatokba szervezni és jelenleg a legtöbb helyen a helyi hálózatok egy egységes országos hálózatban tudnak működni. Összegzésképpen megállapítható, hogy a katonai rendszerekben a híradás és az informatika konvergenciája még biztosan nem fejeződött be, ami kettőséget mutat minden rendszerelem tekintetében.

4.1. A VIRTAR vezetése

Bár a vezető szervek feladata és felelőssége, ezzel együtt eszközparkja is kibővült, de ezzel nem változott alapvetően a híradás vezetési rendszere, a szakmai irányítás továbbra is meghatározza a rendszer alkalmazhatóságát.

4.2. Vezetési pontok belső struktúrája

A végberendezések és a külső összeköttetések biztosítása a nyolcvanas években teljesen homogén volt. Jelenlegi rendszereinkben külön híradó és külön informatikai alrendszereket különböztetünk meg, amelyek felesleges redundanciát okoznak, hiszen külön-külön ki kell építeni mindkét rendszer hálózatát és a szolgáltatások igénybevételét lehetővé tevő eszközöket.

Úgy ítéljük meg, hogy a tábori rendszerek híradó eszközei megmaradtak a nyolcvanas évek szintjén, egyúttal jelenleg nincs a rendszerünkben kifejezetten tábori informatikai eszköz sem. Tapasztalataink azt mutatják, hogy a törzsek állománya az információtovábbítás céljára saját tulajdonú, illetőleg szolgálati mobiltelefonjaikat használják. A jelenlevő kontraszt miatt az állomány nem érez késztetést a nehézkesen működő és gyenge minőségi mutatókkal rendelkező tábori híradó eszközök használatára. Talán ennek okán sokan (nem híradó és informatikai szakállomány) megkérdőjelezi a tábori eszközök fejlesztésének szükségességét.

Az informatikai hálózatok kiépítésére a katonai szervezetek informatikai beosztottjai a meglévő, általában asztali számítógépeket telepítik, amelyek alapvetően nem a katonai elvárásoknak megfelelően kerültek kialakításra, amelyeknek velejárói a gyakori meghibásodások is.

Gyakori a meghibásodás.

4.3. A VIRTAR területlefedő rácsrendszere (alaphírhálózatok)

Az állandó VIRTAR nagytávolságú összeköttetéseit, a különböző stacioner gerinchálózatok képezik, amelynél szintén jelentkezik a híradó és informatikai kettősség. A tábori területlefedő hírrendszer elemei jelenleg megtalálhatók az MH 43. Nagysándor József Híradó és Vezetéstámogató Ezred kötelékében, azonban ezekhez informatikai eszköz hatásosan nem csatlakoztatható, vagyis a országos informatikai hálózat képzésére nem alkalmasak.

A legszembetűnőbb változás az állandó telepítésű rendszerek esetében látható. Napjainkban megmaradt ugyan a Magyar Honvédség zártcélú hálózata, azonban a jogszabályilag előírt különböző feladatok, mint például az ügyfélkapu működtetése miatt egyre több szállal kapcsolódik az elektronikus kormányzati gerinchálózathoz. Nem tartjuk elképzelhetetlennek, hogy a jövőben integrációra is sor kerülhet az EKG és a HM állandó híradó és informatikai hálózatát tekintve [7].

Az viszont már technológiai kérdés, hogy a meglévő nemzeti hálózatunkhoz hogyan tudunk csatlakozást biztosítani a szövetséges katonai szervezetek részére, mint a befogadó nemzeti támogatás egyik része, amennyiben a NATO csapatoknak feladatukat hazánk területén kell végrehajtaniuk.

A tábori alaphírhálózatok tekintetében napjainkra megváltozott a hadműveletei helyzet. A jelenlegi missziók tapasztalata az, hogy a különböző szomszédos egységek, alegységek egymástól több tíz kilométerre levő bázisokon állomásoznak és onnan kiindulva végzik a feladatukat. A terület lefedő hírrendszereknek előnyük, hogy a csomópontjaikhoz több vezetési pont is tud csatlakozni, ezáltal elkerülhetjük a híradó vonalak újólagos telepítését csapatmozgások esetén. Ez az előny azonban akkor, ha vezetési pontok nem folyamatosan, hanem szigetszerűen, egymástól nagy távolságra helyezkednek el hátránnyá válhat, ha csak azért kell fenntartani a csomópontokat, hogy a távolabbi csomópontok számára biztosítsák az összeköttetést, ugyanakkor azokhoz szervezet nem csatlakozik, Könnyen belátható, hogy ez gazdaságtalan erőforráskezelést jelent. A felvetett probléma megnyugtató rendezéséhez megítélésünk szerint katonai felsővezetői szintű, vagy kormányzati döntés szükséges, amely nem is kifejezetten a híradásra, hanem sokkal inkább a Magyar Honvédség feladataira vonatkozik.

4.4. Közvetlen összeköttetések

Az elmúlt egy évtizedben kevés gyakorlat került végrehajtásra, ahol az alaphírhálózatok telepítésre kerültek, vagyis a vezetési pontok hírközpontjai közvetlen összeköttetések felhasználásával biztosították volna az összeköttetést. A technikai színvonalukra jellemző, hogy informatikai szolgáltatások alapját képező felületek kialakítására nem alkalmasak. Az informatika hálózatok összekapcsolását a szakállomány a meglévő stacioner központok felhasználásával oldja meg. A közvetlen összeköttetéseket megvalósító rádiórendszerek az MRR rádiók kivételével elavultaknak tekinthetők, hálózatképzésben szintén nem játszanak szerepet.

4.5. Futár és tábori posta hírrendszer

Béke időszakban a futárszolgálat feladatait országosan a BM látja el, a misszióknál ezt a feladatot egyedi futárok veszik át. Vélhetően e szolgáltatásfajta szerepe a jövőben csökkeni fog, főleg akkor, amennyiben megvalósul az elektronikus küldemények hitelesítése. Mindenképpen kijelenthető, hogy mindig lesznek olyan küldemények, amelyeket eredeti formában kell továbbítani a felhasználók részére.

4.6. Anyagi technikai biztosítás rendszere

A híradó és informatikai anyagi-technikai biztosítás rendszere jelenleg a logisztikai szervezetek feladatkörébe tartozik, mely azonban csak akkor működhet a

rendeltetésének megfelelően, ha szoros együttműködés alakul ki a híradó és informatika vezetési rendszer és a logisztika vezetési rendszere között.

5. NATO hálózat nyújtotta képességek (NNEC)

2002 novemberében a NC3B ülésén a NC3B tagjai egyetértettek abban, hogy szükség van kifejleszteni egy NATO vonatkozású koncepciót, amely olyan nemzeti kezdeményezésekre épül, mint az USA hálózatközpontú hadviselés és az UK hálózat alapú képességek. A NATO kommunikációs és információs infrastruktúráját meghatározó NC3B 2002 óta megkezdte a hálózatos rendszer kiépítésének tervező és szervező munkáját. Az ezzel kapcsolatos eredmények nem mindegyike kerül publikálásra, ezért a nagyközönség számára „láthatatlan" marad. A látható rész az interneten is közzétett „Allied Data Publication (ADatP-34) NATO C3 Technical Architecture Implementation Handbook". Maga a kézikönyv több kötetből áll, és folyamatosan előírt időrend szerint fejlesztik. A NATO hivatalos megfogalmazásában a NNEC a következő [8]: *„A NATO hálózat nyújtotta képességek (NNEC) a szövetség észlelő és technikai képessége, amely egyesítse a műveleti környezet alkotóelemeit a stratégiai szinttől (beleértve a NATO parancsnokságot is) a taktikai szintig a hálózati és információs infrastruktúrán keresztül."*

A NNEC megvalósítása nem csak technológiai feladat. A technológia feladata, hogy támogassa a NNEC kialakítását, elősegítse az információkról, a döntésekről, a folyamatok gyorsaságáról szóló nézeteink fejlődését, szükséges továbbá az együttműködés és valósidejű információközlés megvalósításához [9].

Ahhoz, hogy a törzsben dolgozó tiszt el tudja látni a feladatát szüksége van saját eszközre, nevezzük ezt **felhasználói eszköz**nek**.** Ahhoz, hogy ezeket az egy vezetési ponton levő felhasználói eszközöket hatékonyan ki lehessen használni célszerű őket hálózatba kötni. A vezetési pont hálózatát megvalósító eszközöket nevezzük **belső hálózatképző eszközök**nek. A vezetési pontok is csak akkor tudnak hatékonyan működni, ha egymással összeköttetésben állnak, e cél megvalósítására legjobb, ha egy mindent felölelő hálózatot használunk. Diffúzió szintjén ezt tekintjük **transzport hálózatnak**, harcászati hálózatnak vagy országos hálózatnak, attól függően, hogy béke elhelyezési körletben, vagy feladat végrehajtáson vesz részt a katonai szervezet.

Ebben az időszakban ez a rendszer nem különbözik a NATO-leírástól, mert a felhasználói eszközök és a belső hálózatképző eszközök megfelelnek az „User domain", a harcászati hálózat pedig a „Network domain" szintjének. Azonban, hogy a rendszerünk működőképes legyen, szükség van két fontos elemre, a **hálózat független eszközök**re és a VIRTAR **vezetési rendszer**re.

A jövőbeni rendszer technológiai kiépítésének kérdése túlmutat e közlemény keretein, hiszen e területen a polgári technológia térnyerése hazánkban jelentős. Igaz ez a megállapítás a szabványosításra is, amely a technológia fejlődése után „kullog". A hálózati technológia szabványosítási törekvéseit és buktatóit például Andrew S. Tanenbaum is bemutatja könyvében [10].

Összegzés, következtetések

A katonai hivatás célja a különféle, akár béke, akár missziós feladatok eredményes végrehajtása. A parancsnok döntéseihez megfelelő minőségű és mennyiségű információ szükséges. Ezeket az információkat a parancsnok számára az elöljáró,

az alárendeltjei, valamint a törzsének különböző beosztású tagjai, a saját adatbázisaikra és információs kapcsolataikra támaszkodva szolgáltatják. Az ellenségre és a környezetre vonatkozó adatokat a felderítési rendszer, a saját erőkre vonatkozó adatokat a hadműveleti, logisztikai, és személyügyi rendszer, a saját csapatok vezetését a híradó és informatikai rendszer biztosítja. Természetesen ezek az alrendszerek akár még kisebb alrendszerekre is bonthatók, attól függően, hogy milyen mélységben és céllal kívánjuk vizsgálni a rendszert. Az, hogy ezekben az információs alrendszereknek mi az adattartalma, függ a parancsnok szándékától és a törzs szervezetétől. A törzs szervezete függ az alegység, illetve egység alaprendeltetésétől és nagyságától, valamint attól, hogy a különböző szervezeti elemeket a kötelék vezetése hogyan kívánja egymáshoz rendelni.

Jelenleg a katonai infokommunikációs terminológiánkban nincs egységesen kialakult és letisztult fogalom rendszerünk, amely formálisan vagy informálisan, de egységesen értelmezne a szakma. A különböző értelmezésbeli problémák elkerülése okán a közleményben a híradó és informatika rendszert a feladatából adódóan Vezetési és Információs Rendszer Technikai Alrendszereként (VIRTAR) neveztük el. A VIRTAR tehát a vezetés és az információszolgáltatás érdekében telepített információ- és adattovábbító, feldolgozó és tároló eszközök (hardver és szoftver) és az őket telepítő és üzemeltető személyi állomány összessége.

A jövő katonai konfliktusainak az információ áramlását, az információk minőségét mennyiségét és elosztását a „NATO hálózat nyújtotta képességek NNEC” koncepciója fogja meghatározni.

A NATO hálózat nyújtotta képességek (NNEC) a szövetség észlelő és technikai képessége, amely egyesítse a műveleti környezet alkotóelemeit a stratégiai szinttől (beleértve a NATO parancsnokságot is) a taktikai szintig a hálózati és információs infrastruktúrán keresztül. Egyszerűbben fogalmazva, az információk hatásos és hatékony megosztásának a képessége, a missziók (feladatok) sikeres végrehajtása érdekében, a NATO-t alkotó nemzetek és a szervezetek között.

A VIRTAR tervezésében, üzemeltetésében résztvevők számára az a legfontosabb kérdés, hogy a NNEC megvalósításához szükséges rendszer hogyan fog a jövőben felépülni. Ezek mellett napjaink talán egyik fontos kihívása a biztonságos infokommunikáció, amely szakterületen a biztonságos átviteli utak területét sokan keverik a minősített adatokat feldolgozó rendszerekkel. E területek megkülönböztetése igen fontos, mert minden egyes rendszernek és hálózatnak vannak, illetőleg kell, hogy legyenek biztonsági funkciói, amelyek „szigorúsága” függ a feldolgozott adatok minősítési szintjétől. Belátható, hogy ebben az esetben minden olyan munkahelyre ahol, több hálózatot is használnak, a használt hálózatok számának megfelelő külön számítógépet és a hálózatokhoz tartozó aktív és passzív elemeket kell rendszeresíteni. Ezen módszer még akkor is hatalmas kiadást jelenthet, amennyiben korlátozzuk a felhasználók számát a hálózatokban. Éppen ezért, főként a hadműveleti területen, ahol a kiépítésnek nem csak anyagi, de idő korlátjai is vannak, lehetőség szerint egy hálózaton kell kiépíteni és a felhasználónak egyetlen gépen biztosítani az összes használni kívánt szolgáltatást.

A közleményben foglaltakat mérlegelve az alábbi következtetéseket vonjuk le:

1) A vezetési funkció nem választható el a vezetés technikai alrendszerétől, amelyből következik, hogy az információt szolgáltató alrendszer és a technikai alrendszer egymástól szintén elválaszthatatlan;

2) A NATO és így a Magyar Honvédség előtt álló fontos feladat a hálózat nyújtotta képességek megteremtése;

3) A Hálózat nyújtotta képességek kialakítása nem elsősorban technikai feladat, de a jelenlegi VIRTAR átalakítása szükséges. A VIRTAR felépítése tartalmazza a felhasználói eszközöket (végberendezéseket) belső hálózat képző eszközöket, harcászati vagy országos hálózatot, hálózatfüggetlen eszközöket, VIRTAR vezetési rendszerét.

4) A VIRTAR személyi állománya előtt álló egyik legnagyobb kihívás a biztonságos rendszer megteremtése, azonban szakítani kell a meglévő hagyományokkal és lehetőség szerint egy munkahelyhez csak egy felhasználói eszközt kell rendelni, amelyen biztosítható a legkülönbözőbb hálózat szolgáltatásainak biztonságos elérése.

Felhasznált irodalom:

[1] 1009/2009. (I. 30.) Korm. határozat A Magyar Köztársaság Nemzeti Katonai Stratégiájáról 41 pont.

[2] Magyar Honvédség Összhaderőnemi Doktrina 3. kiadás 53. oldal

[3] ÁLT 27 Magyar Honvédség Összhaderőnemi Doktrína 2. kiadás 2007 80. oldal

[4] Négyesi Imre: Az Információ szerepe a Katonai-Vezetői Információs Rendszerekben (Hadtudományi szemle on-line, II. évfolyam (2009) 1. szám, 119-125. oldal)

[5] A honvédelmi minisztérium szervezeti és működési szabályzata 16. oldal

[6] ÁLT 27 Magyar Honvédség Összhaderőnemi Doktrína 2. kiadás 2007 98. oldal

[7] Négyesi Imre: Az elektronikus aláírás lehetőségei a Magyar Honvédségben I. (Nemzetvédelmi Egyetemi Közlemények, 11. évfolyam/3. szám (2007), 110-121. oldal)

[8] ACT Transformation Network Portal

[9] Négyesi Imre: TRAGBARE UND FELDINFORMATIK-GERÄTE II. (Tábori és hordozható informatikai eszközök II.) (Hadmérnök on-line, IV. évfolyam (2009) 3. szám, 355-362. oldal, ISSN 1788-1919)

[10] Andrew S. Tanenbaum: Számítógép hálózatok 97-101. oldal.

KERTI, András – PÁNDI, Erik – RAJNAI, Zoltán – TÖREKI, Ákos7

NEW AREAS OF IT AND INFORMATION SYSTEMS OF THE HDF8

Abstract:
The article provides an overview of requirements currently set out for the national military communications systems.

Keywords:
CIS, IT, Information Systems

1. Introduction

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

2. Change of paradigms

Before the 1990s and in present time an unfinished change of paradigms in general military thinking has become noticeable, which has three main factors:

- Change of military culture;
- Change of terminology;
- The change of basic role.

2.1. Change of military culture

The end of the Warsaw Pact (WP) and our NATO membership as a result of a long political process was not merely "switching" to another organisation. While members of the WP practiced the military art of the movement-centric military culture, NATO strategists are the followers of the material-centric military culture.

7 Authors: András KERTI PhD, assistant professor, ZMNDU Signal Department, Erik PÁNDI PhD, associate professor, ZMNDU Signal Department, Zoltán RAJNAI PhD, professor, ZMNDU Signal Department, Ákos TÖREKI MA, lecturer, ZMNDU Signal Department

8 This paper was supported by the Bolyai János research scholarship of the Hungarian Academy of Sciences

2.2. Change of terminology

The changes have not only brought about the change of the language of the organisation, but also the change of the terminology. This might not as apparent because many of the terms have similar meanings. However experts growing up on the two different schools have different meanings for the same term.

2.3. Change of basic role

Before the change in the political system we lived in a "bi-polar" world, where military strategy has been mainly determined by the conflict of the two sides, in which frontal tactical and operational tasks typical to WWI and WWII were envisioned.

According to our current ideas however: The Hungarian Republic is not threatened by an attack using conventional warfare within the foreseeable future, and the occurrence of event is also less likely on the longer term.. In our opinion in the current situation Hungarian military terminology is a mixture of terminologies from before and after the change of the political system, there is no clear picture, or common concept developed.

Another factor impairing clarity is the development in technology, the convergence between communications and information systems. The emergence of terminology regarding Command and Information in the current situation however there is no clear standardized terminology that the experts of this field interpret formally or informally the same way. There has been many occasions where the reason for disagreement between experts was only that they had different interpretations for the same term. This viewpoint is also confirmed by a statement from Hungarian researches regarding information security: terminological confusion can also be found in the military lexicon, the reasons for which are the merging of old and new terms and the intention of translating or localising English terms.

Furthermore particular terms change over time, thus the NATO practice of yearly revision of important terms, and yearly new edition of collection of terms and abbreviations gains more interest. In order to make any kind of examination regarding the Command and Information System, we first need to define the concept of the Command and Information System. As a first approach we can interpret it as the assembly of data-processing, data-transfer, and data-storage technical equipment.

In a deeper analysis of the situation it can be found that the described system is only the subsystem providing technical implementation of facilities for the Command and Information System. In our opinion the *Command and Information System* has two more important components, the *system of concepts and notions* regarding the operation of the Command and Information System, and the *operating personnel*.

Staffs operating the Command and Information System are not to be confused with personnel operating the technical subsystem of the Command and Information System, they are the users of the technical subsystem, the information technology experts of the particular military units.

The structure of Command and Information Systems in NATO terminology is: *Command and Control Systems / C2S an assembly of equipment, methods and*

procedures and, if necessary, personnel, that enables commanders and their staffs to exercise command and control [4].

Technical subsystem of the Command and Information System Concepts and notions regarding the Command and Information System. Although it's true that the above definition only applies to Command and Control Systems, and that Command and Information Systems have more components, still this statement is a good demonstration of the relationship between the particular components.

In our opinion the most important component of the Command and Information System is the commander. In order that the commander can from an opinion the commander needs a lot of information and many kind of information. This information is produced the specific specialists of the commanders' unit, by collecting and processing information through their own sources. The commander based on his / her concepts regarding commanding and command systems determines who, when, in what form and with what content should report and transfer messages, reports and data.

The purpose of the technical subsystem of the Command and Information System is to transfer reports, data, messages to the recipients so that they can be processed. The Command System is: the assembly of control processes, control methods and control tools within an organization. Thus the command function cannot be separated from the technical subsystem. Despite this the joint-forces doctrine of the Hungarian Army discusses topic of Communications and Information Systems (as the technical subsystem of the Command System) in the chapter of combat support.

So the question arises, why Communications and Information Systems cannot be thought of as support systems. For this, first lets overview the concept of support: Support is basically an activity during, which the coordinating commander using the forces and equipment under his / her command helps the forces performing the operation in successfully accomplishing the military operation, without *even* temporarily submitting the supporting forces and equipment to their command.

In our opinion the two systems are inseparable. The commanding function cannot be conceived, if the commands, orders, and supporting information cannot be transferred from the sender to the recipient. The problem with judgement is caused by the fact that the technical equipment is not installed by the users, but by a separate subunit, which is however under the command of the commanding organisation. The basic tasks of the technical subsystem are shown on one of the greatest challenges of the information society and thus the army of the information society is to implement information security at a level proportionate to the costs and potential damage.

We don't find it practical that the joint-forces doctrine discusses information security in the information operations chapter separately from the chapter of Command and Control and the chapter of Communications and Information Systems. Information security cannot be implemented at only one place or only using one method, the information security has to be deliberately implemented at every point throughout the Command and Information System.

This is even more important regarding the technical subsystem. In order to implement information security throughout the whole information processing procedure, various tasks have to be performed depending on locations (geographical or logical) and roles. Information security mechanisms reach their goal by being applied at every area of the information infrastructure cooperating with each other.

The part of the figure marked by us as information source is the least defined part of the system, which can vary from case to case from sensory data, recognisance reports to other information systems. The level of control we have over the information source is however important. It can be partially, or complete independent from us. Based on this as it can be seen in the figure, information security does not entirely cover the information source. We can only guarantee the security and validity of the information source at a level proportionate to the level of control we have over it [5]. The networks connecting the mentioned devices form the Communications System, the computers and their connecting networks form the Information System. In our opinion the above distinction is made because of the differences in the level of technological development in the systems of local military equipment.

Two different kind of models can be found in military publications regarding the convergence of the Communication and Information Systems of the HDF. According to the first there the two systems will always remain separated to one point, the other one promises the complete integration of the two systems.

Currently we can speak of three systems with different levels of development. The first is the stationary technical subsystem, which can be thought of as the most advanced system, which is connected to the other governmental systems. The system at the least advanced level is the field communication system, which is virtually still on the technological level of the 80s. There is no modern field system that can serve as the subsystem for the Command and Information System.

The second level of technological development requires some explanation. From the second half of the 1990s our nation is involved in various missions, and these missions could not have been successfully achieved without a Command and Information System. However the technical subsystem of the Command and Information System of the missions cannot bethought of as part of either the stationary system or the field system. It's not part of the stationary because it's operated temporarily, far from the homeland. It's not part of the field system as it was assembled at the start of the missions and disassembled at the end of the missions and did not have to be moved during the missions like in a "classical" military operation.

The Command and Information Systems of the missions consisted of modern field equipment introduced to the HDF assembled with high quality commercial devices.

3. Summary

Our nation unfortunately only came to realize during cooperation in NATO operations, the necessity and the difficulties of introducing modern military communications networks. The Hungarian Army still does not have a modern field communications system, hence the modernization processes, in other words the equip-

ment and system purchases, will have to consider the requirements also pointed out in this publication.

In our opinion, according to the studied publications the concept of the Command and Information System as a Communication and Information System is best defined by the joint forces doctrine: The Communication and Information System consist of the communications and information equipment (hardware), the system software operating the equipment, the client software providing user functions, maintenance and application procedures, the data-stored and transmitted by the system, and the operating personnel.

It can be concluded from the above mentioned that the communication and information system is inseparable, however in practice the only information systems are represented by a separate department within the structure of the Ministry of Defence, the department of Information technology and information security.

References

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

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

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

[4] Négyesi Imre: A megfigyelés és információgyűjtés múltja, jelene és jövője (MK KBH Szakmai Szemle 2009. 3. szám, 35-50. oldal, ISSN 1785-1181)

[5] Négyesi Imre: Informatikai rendszerek és alkalmazások a védelmi szférában (DUF Konferencia kiadvány, 2010.03.05.-06.)

KERTI András[9]

A MINŐSÉGBIZTOSÍTÁS ÉS ÁTVITELBIZTONSÁG KÉRDÉSEI A VEZETÉSI ÉS INFORMÁCIÓS RENDSZER TECHNIKAI ALRENDSZERÉBEN

Absztrakt:
Jelen közlemény a Hadtudományi Doktori Iskolában elvégzett kutatásokat mutatja be.

Kulcsszavak: átvitelbiztonság, híradó és informatikai rendszer, minőségbiztosítás, VIRTAR (vezetési és információs rendszer technikai alrendszere),

Bevezetés

A Magyar Honvédségben 1993-ban lépett hatályba az Informatikai szabályzat (ÁLT/210), melyben az informatika - *mint az infokommunikáció különálló részterülete* – feladatait a kor technikai színvonalán rögzítette. Az azóta eltelt időszakra azonban a konvergencia meghatározó vonásai lettek jellemzőek, és a katonai infokommunikáció szabályozása nem volt képes követni az elmúlt több mint tizenöt évben végbement társadalmi, katonapolitikai és főleg technikai változásokat. A tudományos igényű publikációk, cikkek, tanulmányok, doktori értekezések többsége is általában csak a technikai megvalósításra, a technikai fejlődésre fordítottak figyelmet, nem kaptak a kérdés fontosságának megfelelő hangsúlyt a vezetési és információs rendszerek technikai alrendszerének területei (híradás, informatika, információbiztonság) és azok tervezési-szervezési kérdései.

1. Elvégzett munka

Az értekezésemben a kapcsolódó nemzeti és NATO-dokumentumokra alapozva megvizsgáltam, a vezetési és információs rendszer, valamint a híradó és informatikai rendszerek közötti összefüggéseket és viszonyrendszereket azok kölcsönhatásait.

Kutatásiam során megállapítottam, hogy a vezetési és információs rendszer (VIR) a parancsnok elgondolásának megfelelően, a feladat eredményes végrehajtása érdekében létrehozott szervezet és kapcsolatrendszer, amelynek legfontosabb feladata, hogy megfelelő információkkal lássa el a parancsnokot döntési mechanizmusának segítése érdekében. A VIR megállapításaim szerint nem más, mint a parancsnokságok és törzsek különböző szakbeosztású tisztjeinek összessége. Azonban ahhoz, hogy a törzsben dolgozó egyének munkájukat a parancsnok által elvárt szinten tudják végrehajtani szükségük van információfeldolgozó és tároló- (informatikai), valamint információt továbbító (híradó) rendszerekre, eszközökre és kapacitásokra.

A teljes információs rendszer minőségi mutatói nem hagyhatják figyelmen kívül a megfelelő információbiztonsági szintek megvalósítását. Vizsgálataim alapján bebizonyítottam, hogy az említett eszközrendszer nem más, mint a VIR technikai alrendszere (VIRTAR).

[9] Szerző: Kerti András PhD, ZMNE Híradó Tanszék, adjunktus

Úgy ítéltem meg, hogy a híradás és informatika konvergenciája a polgári életben napjainkra befejezettnek tekinthető, ezért fontosnak tartottam a VIRTAR felépítésének, elemeinek és viszonyrendszerének vizsgálatát a felkutatott dokumentumok révén. Megállapítottam, hogy jelenleg nincs egységes nézőpont a rendszer felépítésére, a tudományos publikációk szerzői gyakorlatilag a polgári életben végbement konvergencia eredményeit nem rendszerben elemezték, hanem az informatika, vagy az átvitelt biztosító hírrendszer oldaláról. Ezen túlmenően megállapítottam, hogy a NATO-ban sincs egységes elfogadott álláspont a rendszer egészéről, az üzemeltett rendszert több (különböző) nézőpontból vizsgálják.

A meglévő, illetve a továbbfejlesztendő rendszert legjobban leíró modellt egy 2001-ben készített doktori értekezésében találtam meg, azonban ekkor még a konvergenciát nem lehetett befejezett tényként kezelni. Az eddig elért kutatási eredményekre alapozva dolgozatomban bemutattam a VIRTAR célszerű felépítését és elemeinek feladatrendszerét a Magyar Honvédség hálózat nyújtotta képességének elérése utáni időszakra.

Kimutattam, hogy a VIRTAR fő területeinek nincs egységes szabályozási rendszere, ezért a hiány pótlására irányuló feladatot alapvetően vezetési feladatként kell kezelni, amelynek egyúttal illeszkednie kell a meglévő katonai vezetési funkcionális rendszerhez. Ennek érdekében értekezésem második részében megvizsgáltam, hogy napjainkban milyen metodikák alapján, milyen eszközrendszerrel irányítják a vezetők, a parancsnokok a Magyar Honvédség tevékenységét. Megállapítottam, hogy amíg a parancsnoki munka viszonylag jól szabályozott addig a szakmai munka nyílt forrásokra támaszkodva nem követhető. Bizonyítottam, hogy a Magyar Honvédségben keveredik az öröklött szabályzati struktúra a NATO szerinti policy-directive-guideline szisztémával, illetőleg tovább bonyolítja a helyzetet a polgári szférából érkező szabályozási rendszer is, melyet a vezetési és információs rendszer, mint külső tényezői halmazt nem hagyhat figyelmen kívül.

Ez a keveredés jellemző a VIRTAR irányítására is, mert bár egységes szabályozás nincs, jogilag (jogszabályokkal és az állam irányítás egyéb jogi eszközeivel) azonban néhány részterület, úgymint frekvenciagazdálkodás vagy az EDR hálózat szabályozásra került.

Annak érdekében, hogy javaslatot tehessek a VIRTAR irányítására szükségszerűnek mutatkozott előzetesen megvizsgálni a vezetés érdekében ellátandó feladatok körét. Megállapítottam, hogy vezetési feladatokat egyrészt tervezési-szervezési feladatokra, valamint a mindennapi élet irányítására lehet felbontani. Mindkét részfeladatot további részekre osztottam fel, így meghatároztam az állandó és ideiglenes rendszerek tervezési és szervezési elemeit. A napi élet irányítását a hálózatfelügyeleti munka feladataira, illetve a számítógépes incidenskezelő központ feladataira bontottam fel, és értekezésem ezen részében összehasonlítottam a napi élet irányításának e két részterületét.

Korunk társadalmi elvárása, hogy a hadsereg ne állam legyen az államban, hanem a társadalom szerves, integrált része. E gondolatból kiindulva megvizsgáltam annak lehetőségét, hogy a VIRTAR vezetési rendszerében milyen eljárásrend szerint lehetséges alkalmazni a polgári életben már elfogadott minőségirányítási szabvány előírásait. Megállapítottam, hogy a VIRTAR irányításának megszervezése a minőségirányítási szabvány alapján kimutatható előnnyel jár abban az esetben,

amennyiben egyrészről a szakmai vezetés elfogadja annak mechanizmusát, másrészről a beosztott állománnyal sikerül a kitűzött célokat megértetni és megvalósíttatni.

Amennyiben a minőségirányítási rendszer nem fogja elősegíteni a hatékonyság növelését, várhatóan a kvantitatív és kvalitatív mutatók csökkenésére kell számítani.

Kimutattam, hogy az információs rendszerek bármelyikéről is legyen szó, a legfontosabb feladat az információbiztonság megfelelő, az adott rendszerre jellemző megteremtése. Ebből eredően a NATO minősített információbiztonságának alapdokumentumára alapozva, a polgári életben meglevő szabványosítási törekvéseket szem előtt tartva a kutatások végrehajtása során áttekintettem a VIRTAR biztonsági kérdéseit.

A biztonsági kérdések elemzését követően megállapítottam, hogy a technikai információbiztonsági kérdéskörből az átviteli út biztonság vagy másképpen az átvitel biztonság, amely leginkább katonai szakterülete a biztonságnak, sem a polgári életet, sem a katonai rendszereket tekintve nem került teljes egészében kidolgozásra.

Feltártam a kidolgozatlanság okait, és kutatásaimat az átviteli út meghatározására és a biztonságának megvalósítására fókuszáltam a Magyarországon is elfogadott nemzetközi szabványokra alapozva. A vonatkozó szabvány alapján bemutattam, hogyan lehet meghatározni az átviteli utat és struktúráit. Bizonyítottam a biztonsági intézkedések szükségességét, melyet a szakértők igazoltnak látnak, azonban a költségek és a szabad információ áramlás gátjai miatt az elfogadás alacsony szintű. Ezek miatt a fenyegetésekkel és a védendő információkkal arányos védelem megvalósításának leginkább járható útja és eszköze a kockázatok felmérése.

Az idevágó szabvány módszereit alkalmazva bemutattam hogyan célszerű az átviteli út tekintetében végrehajtani a kockázatok felmérését. Megfogalmaztam, hogy a biztonság egy olyan állapot, amely csak egy bizonyos időpillanatra értelmezhető, ezért ha kidolgozásra kerül egy rendszer biztonsági intézkedéscsomagja, akkor a figyelmet a biztonságot befolyásoló eseményekre és az azokra adandó válaszintézkedésekre kell fordítani.

A válaszintézkedések életbeléptetésére már előre fel kell készülni, amely a Magyar Honvédség tekintetében két fő feladat köré csoportosítható, egyrészről az információbiztonsági incidenskezelés, másrészről a vezetésfolytonosság köré.

Az értekezés utolsó részében bemutattam mindazon feladatokat, amelyeket az incidenskezelés és a vezetésfolytonosság megfelelő tervezése érdekében kell végrehajtani.

2. Végkövetkeztetések

Az értekezésben foglaltakat mérlegelve az alábbi végkövetkeztetéseket vontam le:

- A vezetési funkció nem választható el a vezetés technikai alrendszerétől, amelyből következik, hogy az információt szolgáltató alrendszer és a technikai alrendszer egymástól szintén elválaszthatatlan, szerves egységet

alkot. A VIRTAR leírását és megalkotását a nemzeti modell módszertana alapján célszerű végrehajtani.

- Az információs társadalomban a haderő előtt álló egyik legnagyobb kihívás az információk biztonságának megvalósítása. A részterületek kidolgozottsági foka megfelelő az átvitelbiztonság kérdéskörének kivételével.
- A vizsgálat időszakát tekintve kijelenthető, hogy a VIRTAR három alapvető szakterületét illetően a vezetés egységessége nem valósult meg, a szakterületi viszonyrendszer korrekt rendezése nem teljesült. A VIRTAR kialakítását újabb megoldások keresése helyett célszerű a megfelelő szabványcsaládra, valamint a bevált gyakorlatokra alapozva végrehajtani.
- Az átvitelbiztonság feladatrendszerét a nemzetközi szabványok adaptálása révén célszerű meghatározni. A VIRTAR biztonságának fokozása érdekében incidenskezelési és vezetésfolytonossági tervet szükséges készíteni.

3. Tudományos eredmények

- Tudományos módszerekkel feldolgoztam, elemeztem és értékeltem - *mindazon dokumentumot, jogszabályt, amely alapján meghatározhatóvá vált* - a vezetési és információs rendszerrel és annak technikai alrendszerével szemben a hálózat nyújtotta képességek megvalósulása érdekében támasztható követelmények.
- Kritikai szempontból elemezve a VIRTAR Magyar Honvédség szintű szakmai vezetését, a hazai és nemzetközi szinten kidolgozott eljárások adaptációja révén meghatároztam a VIRTAR minőségbiztosításra épülő vezetési elveit.
- A kockázatelemzés módszerének felhasználásával kidolgoztam az információbiztonság átvitel-biztonsági részterületének feladatrendszerét.

FARKAS Tibor10

A HÍRADÓ ÉS INFORMATIKAI RENDSZEREK MISSZIÓS KÖVETELMÉNYEKEN ALAPULÓ MEGSZERVEZÉSÉNEK KÉRDÉSEI

Absztrakt:
Jelen közlemény a Hadtudományi Doktori Iskolában elvégzett kutatásokat mutatja be.

Kulcsszavak:
híradó és informatikai rendszer, tábori hírrendszer, többnemzeti műveletek

Bevezetés

A pontos, megbízható és időbeni információtovábbítás és feldolgozás elengedhetetlen követelmény a modern hadműveleti vezetés- és irányítás megvalósítása érdekében. A nemzetközi tapasztalatok – és a vonatkozó szövetségi dokumentumok – alátámasztják, hogy egyes követelmények csak a Magyar Honvédség számára tekinthetők új kihívásoknak, mivel a tábori infokommunikációs eszközeink fejlettségi szintje messze eltér azoktól, amelyeket a fejlett NATO tagországok hadseregei alkalmaznak. A többnemzeti válságreagáló műveletek parancsnokai vezetési tevékenységének korszerű infokommunikációs eszközökkel történő támogatása során nagy hangsúlyt kell fektetni a szervezési eljárásokra, tervezési metódusokra, amelyek együttes alkalmazása biztosítja a rendszer megfelelő szintű képességét. A rendszer funkcióinak teljes kihasználása csak és kizárólag egységes szervezési eljárások alkalmazásával, korszerű infokommunikációs eszközök felhasználásával és a szakállomány magas szintű kiképzésével és felkészítésével érhető el.

1. Elvégzett munka

Értekezésemben olyan témakör elemzését és összegzését kíséreltem meg, amely a jelen- és jövőbeni többnemzeti válságreagáló műveletek vezetés- és irányítását nagymértékben meghatározza. A Magyar Honvédség stacioner híradó- és informatikai rendszere korszerűsítését nem követte a tábori körülmények között alkalmazott infokommunikációs rendszer fejlesztése, amely komoly szervezési és technikai problémákat eredményez a tervezéssel, szervezéssel megbízott szakembereknek, és a missziós környezetben szolgálatot teljesítő végrehajtó szakállománynak.

A széleskörű, minden területet felölelő szervezési eljárások alkalmazása érdekében vizsgáltam meg a vonatkozó nemzeti- és nemzetközi dokumentumokat, szabályzókat, követelményeket, fejlesztéseket és tapasztalatokat. A következtetésem alapján meghatároztam a válságreagáló műveleteket támogató híradó- és informatikai rendszer fogalmát, a szervezést befolyásoló követelményeket, képességeket és egyéb tényezőket, amelyeket figyelembe kell venni a tervezési és alkalmazási eljárásrend során.

[10] Szerző: Farkas Tibor PhD, ZMNE Híradó Tanszék, adjunktus

2. Végkövetkeztetések

- A nemzetközi- és hazai missziós tapasztalatok alapján megállapítottam, hogy kisméretű, többfunkciós képességekkel rendelkező, korszerű haditechnikai eszközökkel felszerelt katonai erőket (civil képességek kiegészítésével) kell létrehozni, amelyek a komplex hadműveleti elvárásoknak és vezetői igényeknek megfelelnek. A kor követelményeinek megfelelően és az elvárásokhoz igazítva viszonylag kis anyagi ráfordítással továbbfejleszthetők, valamint a jellegükből adódóan képesek a konfliktusok felszámolására és hazai alkalmazásra egyaránt.
- Az általános hadműveleti képességek és igények alapján konstatáltam, hogy az MH által jelenleg alkalmazott híradó- és informatikai rendszer definíció nem tartalmazza azokat az összetett jellemvonásokat (a jelenleg rendszerbe állított technikai eszközök és azok képességei következtében), amelyeket a válságreagáló műveletek infokommunikációs rendszere ölel fel.
- A megvizsgált és bemutatott MH többnemzeti missziós tevékenységei híradó és informatikai támogatásának elemzése során arra a következtetésre jutottam, hogy a rendszer megtervezése és megszervezése szerteágazó, összetett folyamatot foglal magába, amelynek figyelembe kell vennie a mindenkori, az adott térségre, az együttműködők összetételére és a speciális feladatokra jellemző tényezőket.
- A parancsnoki vezetés támogatása érdekében biztosítani kell az optimális mennyiségű, minden területre és részfeladatra kiterjedő információkkal történő ellátását, a megszerzett információk feldolgozását és azok továbbítását. Ennek érdekében kiemeltem mindazon követelményeket, képességeket és egyéb hatást gyakorló tényezőket, amelyek specifikusan jelennek meg a nemzetközi műveleti területen.
- A részeredmények alapján sikerült megfogalmaznom és kialakítanom azt a struktúrát, amely alapján az információk feldolgozása és cseréje érdekében létrehozott komplex, NATO követelményeknek megfelelő, többnemzeti együttműködésre alkalmas híradó- és informatikai rendszer megszervezhető. A tervezést a hadműveleti igények, a rendszerkövetelmények és a technikai megvalósítás lehetősége alapján kell meghatározni. Ezen hármas tényező minden esetben a folyamatos ellenőrzés és visszacsatolás alapelve szerint jelenik meg a munkasorrend, munkafolyamat során.
- A tapasztalataim és az értekezésben leírtak alapján a jelenlegi tábori hírrendszer nem alkot egységes rendszert és nem felel meg a modern hadműveleti kihívásoknak, ezért javaslom egy olyan korszerű és komplex tábori CIS rendszer alkalmazását (megvásárlását), amely egyaránt támogatja a hagyományos- és a válságreagáló műveletek vezetését. A missziós műveletek hadműveleti híradásának biztosítására nem tartom célszerűnek felhasználni a (teljes) csomóponti hírrendszert, mivel a tábori alaphírközpontok védelme megkövetelné a műveletet végrehajtó erők létszámának, technikai eszközeinek, logisztikai biztosításának növekedését. Hasonló

elvek alapján a bázisállomások telepítését igénylő EDR rendszer alkalmazását sem látom megfelelőnek. A hadműveleti feladatok ellátását kiválóan (a tapasztalatok alapján) támogató Harris PRC-117/F típusú rádiókészülékek rendszerbe állítását jelentős képességnövekedésnek tartanám, mivel biztonságos, műholdas összeköttetés létesítésére is alkalmas, hang- és adatátvitelt biztosító, a katonai szabványoknak eleget tevő rádiókészülékek.

3. Tudományos eredmények

- Az értekezés témájához kapcsolódó dokumentumok (jogszabályok, normák, doktrínák) elemezésével és értékelésével meghatároztam a válságreagáló műveletek híradó- és informatikai támogatásának képességeit és követelményeit, valamint vezetés-irányítását támogató híradó- és informatikai rendszer újszerű definícióját.
- Összevetve a nemzetközi szerepvállalásból szerzett tapasztalatokat és a hadműveleti-harcászati képességeket meghatároztam a válságreagáló műveleteket támogató híradó- és informatikai rendszerrel szembeni követelményeket, valamint a híradó- és informatikai rendszerek szervezését, tervezését befolyásoló tényezőket.
- Meghatároztam az egységes és komplex támogatási igényeket kiszolgáló, mind a hagyományos, mind a válságreagáló műveletek vezetés-irányításának elemeként működtetett tábori híradó- és informatikai rendszer (CIS) elemeit.

4. Ajánlások

Megítélésem szerint jelen értekezésemben összefoglalt kutatási eredményeim egyrészről a válságreagáló műveletek híradó- és informatikai támogatásának megszervezése során válhat hasznosíthatóvá, másrészről integrálhatók a Zrínyi Miklós Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Kar szakmaspecifikus BSc és MSc, valamint szakmai továbbképzések oktatási tananyagaiba.

Az anyagban leírt és meghatározott szervezési elvek jó alapot nyújthatnak a téma további, speciális területeinek (információvédelem; technikai eszközök; informatika; hálózat nyújtotta képesség) vizsgálatához és új PhD értekezések megírásához.

FREGAN Beatrix-FÁBIÁN Éva

THE SPECIAL RELATIONSHIP FOR EUROPEAN INTEGRATION

During research, when people look back to the European history after the Second World War unavoidably can meet the relations between the French and the German state. This fact and the history of these European countries full of contrasts gave me inspiration to make a comprehensive picture in my writing. It's also an important reason that France and Germany are until now the engine of the European integration, the correlation of their interests are influencing the future of the other member states.

After the Second World War, in the Cold War period the most successful European event was the integration organization, which nowadays people call the European Union. The most important engine of this European alliance was France and Germany and the situation has not changed yet. However in the development of their relations has always had bad moments both during the bipolar and the post-bipolar world. These depressions have historical roots, which can be felt in today's international relations too. Concerning the French and the German interests, we have to point out the relations with Central and Eastern Europe. With these small countries Germany has always had good relationship, while French traditional interests were connected mostly to the southern and Mediterranean area, to the Maghreb countries, but the Anglo-Saxon world also was not so far from its borderlines.

After the 90s changing, during the period of Jacques Chirac only few positive events happened indeed during the conservative president's term was the deepest point in the formation of the French-German relations. The presidential elections of the year 2007 brought the wind of a new period in France, more exactly everyone hoped it both in the homeland and in the international political life. However, the Germany-policy of Nicolas Sarkozy has shown us an ambiguous balance so far: it seems that the actually first person of the France sometimes meet the British prime minister to prefer visit Angela Merkel.

The central element of the French policy: Europe

For France the European policy represent an important dimension. It is an obvious fact, which has some simple and some complex reasons: the country's location, possession of a middle-power status, a continuous self-determination, abundant ambitions of power. I start my work with the history of the French-German relations after the Second World War emphatically their roles of overriding importance in the European integration. TAMÁS SZEMLÉR's dissertation[i] and FERENC GAZDAG's article[ii] gave me a lot of useful information to write this chapter[11].

In the Cold War's ages – where the international tensions were almost daily – all the states of Western Europe understood slowly that their (primarly economic)

[11] The endnotes of this paper you may find at the end of proceedings.

security would be guaranteed through an European institution. In this situation – among the western European countries – France and Germany were interesting phenomenon because their affairs were cloudy but this couple launched and developed the European integration. Independently of this incidence everyone knew that the great world political decisions were made in the tables of Russia and the United States of America. The two latters had only adequate abilities for enforcing their interests on the contrary with the French and the German states. The Gauls was one of the winner countries after the war but their ability did not allow it to recover its former power status and to return to the high politics. While Germans suffered a totally defeat and became weak. The winners divided its territory into two parts and in its west part – mostly France – made an effort to restrict its political and military movement. So the west German politics was interested in the slowly and cautious enlargement of its possibilities. Its objective for the future was naturally the reunion of the Germans's home country. Because of the above reasons – in spite of their historical injuries – these two countries were able to commit themselves to the cooperation for Europe's future.[iii]

France's interest increased due to the foundation of the North Atlantic Treaty Organization (NATO)[iv] and to the birth of the two German states. They knew very well that the decrease of Europe's role in the world politics and the dissolution of their enormous colonial empire would also reduce both its internal and international prestige. So Paris tried to become independent of the United States of America and to become a leader in the European project.[v]

A strange marriage became official

In the formation of the relations 22 January 1963 was an important station. This day Germany and France signed the Elysée treatment, which seemed and treated like the strangest marriage of Europe. In different power position,[vi] the continent's two big opponents had to integrate after the Second World War into a system where they were who had to make a new Europe. The actual French foreign policy – named Charles de Gaulle – saw the possibility to restore its former power in their permanent rival. Nevertheless, due to the strongly technically agreement – signed by Konrad Adenauer and Charles de Gaulle – the French-German tandem proved to be a stable framework for the young European alliance despite the fact that their relationship did not become well-balanced then.

Both states celebrated the 40th anniversary of the treatment with monumental ceremonies. On the occasion of this long-term cooperation a political declaration was accepted, where the alliance was raised to European dimension and concerning its content, it spoke about the foreign and security politics of the integration, some questions of the defense politics, the possibility of a cooperation in the war industry and strategies concerning the third countries. The questions about Iraq they tried to show an united stand and emphasized the primacity of the UN's Security Council. After all they were against the war and they emphasized the importance of that opinion with few small member countries.[vii] The rapprochement in January 2003 was a new phenomenon but was burdened with the incompatibility of Schröder's electoral pacifism and Chirac's neogallism.[viii]

The Elysée-treatment can be taken successful. Its background is France and Germany's long-term interests, mostly the end of the tensions because of de German question. In the bipolar war's ages continously happened a few differences of opinions between them but they knew well that they could not get out of the way of each other concerning mainly the important questions of the new European integration. However, the balance reached[ix] was so quite fragile that people could not be surprised in the 90s.[x]

Nicolas Sarkozy – new winds in French

With Nicolas Sarkozy a new style appeared in the right wing. The new president of the republic – who was elected in 2007 – was already very charismatic during his campaign, where he was almost declaring his love to French and to its nation in every speeches and always emphasized that he would make his country great again.[xi] One of the secret of his success was that he chose skilfully the ideas both from the right and from the left wing, while his opponent lost – in DOMINIQUE MOIS's opinion – not because of but against that she was a women.[xii]

The new president began his work in 16 May 2007. Everybody hoped a lot from the Gualliste Right and from Sarkozy both in the field of internal politics and the international political life. For example, an average French voter would be the resolution for the economic problems[xiii] and for the countinously increasing unemployment.[xiv] In the 90s and after the Gallic country became more and more restless, its inhabitants wanted to have reforms and an other state-model.[xv] With relation to this, there was a high chance of the reinforcement of the French diplomatic activity.

In recent years some controversial changes happened in the French international situation. So it is no wonder that the participants of the international life hoped for considerable improvements from the new French president – as FRÉDÉRIC CHARILLON wrote on his essay's 140th page: „From Berlin to Beirut, from Washington to Cairo, from Moscow to Abidjan."[xvi] – and they saw the answer and the willingness in the person of Nicolas Sarkozy. The young president's aim was to move his home from its sluggish place. In his official statement – presented in *Politique International* in spring 2007[xvii] – he emphasized the importance of the break with the former ages and with the Chirac's period. He said that the most important task is to put the internal affairs in order and then it could be continued with the also unstable – due to for example the international Iraq debate – European policy.[xviii] In connection with the problem of this state in the Middle East the French manifestations caused itself more losses in Europe than popularity in the Arab countries. Its prestige was also reduced with the rough French critism against the new member states.[xix]

The elected president of the republic represent the „rupture" namely the break with the previous policy. It has been realized since 2007 naturally specifically in French style and people could see its several results: for example opening to Central and Eastern Europe.[xx]

From the year 2007 – mainly in European medium – everyone was waiting for the renascence of the alliance between the two founder of the European integration. Since the 90s – especially with the enlargements in 2004, 2007 and in the future –

the European Union has been in crisis and the Europeans were waiting for a wonder. As a result, almost all European political leaders hoped for the French-German tandem re-assemble.[xxi] Nevertheless, the relation between Nicolas Sarkozy and Angela Merkel were filled with contradictions so far, mostly because of the personality of the new French president but also because of the different interests of the two big countries in certain (not only European) political questions.

During the year 2007 and 2008 promising events happened[xxii] but during the second semester of 2008 the French European Union Presidency brought interesting developments in their relations. The end of 2008 the French press wrote about Mr. Sarkozy's preferred British relations[xxiii] against the neglected German strings.

As conclusion

I think it is a true statement that the French-German relations resemble an old couple who has a lot of common interests that they can not have different interests. Following Hubert Védrine's words – ex-minister of Foreign Affairs – the Franco-German alliance is necessary but today is not enough to create a new European system.[xxiv]

The Elysée treatment was 40 years old in 2003. Since this year the two European states organize twice a year common sessions, they call it French-German common ministerial council. Moreover, both the German and the Gallic countries appoint a commissioner for the cooperation and these two persons – as a Minister of the State and as a Secretary of the State – are also responsible for the European affairs. The two appointed – with continuous coordinations – work on approaching the civil societies.

Today there are good examples for the activity of the Merkel-Sarkozy couple. 18 October 2010 the French-German-Russian summit in France, Deauville started, where the two European middle-powers negotiated with Moscow about the future of the European security and about the relations betveen the European Union and Russia. I note that both the United Satetes of America and the Western European member states did not like the arrangement of the appointment. The balance show an ambiguous result: the Russian president was essentially cooperative but he promised not too much and which was even more worrying for the European politicians that, among others, Catherine Ashton – actual high-representative of the Foreign and Security Policy in the European Union – was not invited.[xxv] Additionally, Paris and Berlin organized an other meeting where – according to French presses – they agreed on one hand on a common action to decrease the budget deficit of the EU members. On the other hand they also agreed on the Lisbon treatment but both steps evoked similar reactions as it happened in connection with Deauville.[xxvi]

After all, we can not end up with the colorful history of the French-German relations but – as I proved for the reader earlier – nobody knows how it could harmonize. It is difficult to realize it mainly because of the unpredictability of the international environment and because of the still existing French exceptionalism.

András TÓTH

THE SIGNAL PROVIDING OF THE HUNGARIAN NATO RESPONSE FORCES

Abstract:
The NATO Response Force was established with a view to any crisis quickly and effectively be able to assist. The nations participating in the service available to modern technology and military forces trained extensively to ensure that NATO is anywhere in the world within a very short period of time reflected and carry out tasks either at the joint effects-based operations and network requirements.

Keywords:
NATO Response Forces (NRF), C2 system, satellite communication, GSM communication

Introduction

After 11 September 2001 the USA, to identify the changing of the operational character of the military wars and conflict, made a plan for establishing a new military unit. In November 2002 at the Prague Summit they made a proposal for a new NATO Quick Reaction Force, and it was voted during the conference. Therefore NATO Response Force (in the following: NRF) was formed in 2002.

The NRF is a high-readiness force with up-to-date equipment, which accomplishes its activity in joint environment. It is a flexible, rapid operational, interoperable, and includes NATO's land forces, air forces, navy and special forces. After the order of the deployment it is able to fulfill its tasks quickly, all over the world in the full spectrum of operations.

The possible mission of the NRF:

- collective security duties according the Article V;
- crises response tasks, evacuation operations, elimination of the disasters' effect, humanitarian assistance, war against terror, non Article V activities;
- preparation tasks of the theatre, to ensure the march of the main forces
- to show force to prevent the crisis, or to deter

The NRF duty works in a rotation principle: after the 6-month training, preparation and the check of compliance with the requirements a 6-month readiness duty begins. After the end of all of the rotations the units are changed for a new, up-to-date troop, which successfully carried out the training, the check and suited the requirements.

The Hungarian Defense Forces (in the following: HDF) since 2003 provided companies for the NRF duties. In this year the NRF-14 and NRF-15 is on 6-month duty in the bonds of HDF.

The NRF is due to the modern, technically advanced assets meets demand of the network centric warfare and the effects-based operations, that's why its command- and control-supported communication and information systems have to be

planed and established in that wise, and it will be able to attend the communication needs of the units, subunits.

The communication and information system has to ensure:

- The conditions of the superior command's contacts at the operation area for the operational management;
- Liaison with the national (domestic) headquarters and organizations to send the reports of the contingent's activities, the requests of the assets' improving and the means' reinforcements;
- The internal communication among the subunits.
- The plan, the organization and the operation of the contingent's communication and information system in camp housing conditions;
- The conditions of the non-duty services to keep the contact between the soldiers and their family members;
- Courier and mail service.

The communication system of the NRF

After the ordering of the tasks' execution the offered forces of the Republic of Hungary belong to a superior battalion, which is leaded by a multinational brigade, and the area of its tasks is the battalion's area of responsibility. The operational communication net between the battalion and the Hungarian infantry company is planned and organized by the TOC12 of the battalion, and it is established with the Hungarian equipments. If it is necessary the superior command ensures materials for the contingent. If the application requires the company can send 1 liaison officer to the superior TOC, who can be equipped with GSM telephone and/or IRIDIUM satellite phone, or the superior can send 1 liaison officer to the NRF company.

Radio communication

When the NRF starts its mission the signal officer has to make the contact with the communication and information department of the battalion because of the access of the superior command's services, and he has to prepare the users for the installation and operation of the terminals and facilities.

The communication between the contingent and the homeland command (HDF JFC13) is organized primarily with national mobile phones, secondarily with IRIDIUM satellite phone. The command net is planned and established by the TOC of the superior command, and they can use HF14 radios, satellite or mobile phones to keep the contact.

The signal officer of the contingent is responsible for the inner communication of the Hungarian NRF. A long-range HF radio net will be organized for the contact between the contingent command and the company HQ15. This radio can be a HARRIS radio, which is not designed just for voice forwarding it is also able to

[12] Tactical operations center
[13] The Joint Forces Command of the Hungarian Defense Forces
[14] high frequency
[15] headquarters

push data trough as well. These nets are not secured that's why the soldiers always have to use the TDR and the leading tables. Against the enemy's radio detection and interference activity the radios are usable just as long as needful and with the necessary output power.

The inner communication of the company is ensured with VHF16 radios which are mounted into armored personnel carrier (for example: BTR-80, BTR-80/AM) and these might be R-173, MRR MV-30017 and PRC-150 HF/VHF HARRIS radios. When the soldiers get out of the vehicles they can use portable radios as MRR MP-30018 and/or MRR MH-30019.

People, who are serving at the Hungarian NSE20, also can use MRR MP-300 and/or MRR MH-300 radios to keep contact with each other. The commander of the NSE is responsible for the allocation of the devices and the keeping of the communication-rules.

When the changing of the radio net is necessary it can be changed just with the contingent commander's order. After the commander's order the NRF signal officer has to plan and organize the new networks according to the commander's conception.

The signal officer has to make the frequency requests for all units. The officer has to send this document through the CRONOS to the superior command. The S-6 officer gets a document with the usable and spare frequencies. If they need more he can require new frequencies for the units.

The units have to check the radio stations before leaving the base. The unit commander is responsible for this procedure. If one or more devices do not work the users have to change to the spare frequency or they have to change these equipments.

On the operation area the superior command ensure the MEDEVAC data. The commander of the entry forces have to deliver this information for every subordinate. The MEDEVAC frequencies must be programmed into the memory of all of the radios.

During the operation there are two ways for MEDEVAC request:

- indirectly from the unit who is on MEDEVAC duty with the established radio, GSM, wired or satellite nets;
- directly from the superior TOC at CRONOS21.

Wired, satellite, GSM communication

Wired communication will be established by the superior TOC to ensure the contact with the operational command post of the battalion. If the Hungarian contingent gets more than one line the signal officer has to plan one of them directly to the commander.

[16] very high frequency
[17] Multi Role Radio Vehicle-mounted version
[18] Multi Role Radio Portable version
[19] Multi Role Radio Handhold version
[20] National Support Element
[21] Crisis Response Operations in NATO Operating Systems

Every NRF rotation has IRIDIUM satellite phone to keep the contact with the homeland, or they can use these when they do not have any other possibility to keep the inner communication of the contingent. These are the secondary devices for the communication between the contingent and the homeland, it can be used if the GSM system is not working. It is prohibited to use these equipments for private conversation, just for voice service (login, short report and so on), or at that case when immediately measure is requisite.

Due to the order of the Commander of The Joint Forces Command of the Hungarian Defense Forces the contact with the homeland command primarily is executed with 3 norm national mobile phones with Hungarian SIM cards, in order to ensure the link between the operation area and the homeland.

Summary

The NRF is a highly ready and technologically advanced force, which meets the modern operational requirements and it is appropriate to serve a network centric or effects-base operation. The Hungarian rotations were designed according to these technical challenges, equipped with the necessary materials, and reinforced with the needful module elements. It is the reason, because it is necessary to translate big attention for the training of the strength, the instruction of the new command and control system.

When the NRF has to start its mission anywhere in the world, it would belong to a common battalion of a multinational brigade, which is the basic element of the communication system planning of the mission. With a big probability the contingent can ensure just the inner communication and the national networks with the homeland with its equipments because of the compatibility problems.

The contingent's organizational elements are capable of voice and data transfer with its modern equipments, which make shorter the reconnaissance, the decision and the preparation and execution of the strike.

Literature

[1] Koós Gábor - Szternák György: Gondolatok a hatásalapú- és a hálózatközpontú katonai műveletekről, FELDERÍTŐ SZEMLE, ISSN 1588-242X, Budapest, 2009

[2] http://www.nato.int/cps/en/natolive/topics_49755.htm

[3] Dr. Munk Sándor ezredes: KATONAI INFORMATIKA II., Katonai informatikai rendszerek, alkalmazások, Egyetemi jegyzet, ZMNE, Budapest, 2006.

[4] Berzsenyi Dániel: A hálózatközpontú hadviselés és a hálózatközpontú harc megvívására képes hadsereg, Tanulmány, ZMNE Biztonság és védelempolitikai szak, 2008. november 12.

[5] Kiss Álmos Péter: Generációk a hadviselésben − a negyedik generáció. Zrínyi Miklós Nemzetvédelmi Egyetem Hadtudományi Doktori Iskola, Tanulmány, 2008.

András TÓTH

A MAGYAR HONVÉDSÉG TARTOMÁNYI ÚJJÁÉPÍTÉSI CSOPORT KOMMUNIKÁCIÓS RENDSZERE, ÉS ANNAK ALAPVETŐ PROBLÉMÁI

Absztrakt

A szerző a hazai és az afganisztáni gyakorlati tapasztalatai, valamint korábbi tanulmányai alapján elemezi a Magyar Honvédség Tartományi Újjáépítési Csoport kommunikációs hálózatát nemzeti és nemzetközi viszonylatban, és összegzi a Magyar Honvédség által végrehajtandó fejlesztési feladatokat.

The writer analyses the communication network of the Hungarian Defence Forces Provincial Reconstruction Team to lean on his national and afghan practical experience in national and international circumstances, and summarises the necessary development activities of the Hungarian Defence Forces.

Kulcsszavak:

Tartományi Újjáépítési Csoport, missziós híradás, konvoj-híradás, NATO C2 rendszer.

A Tartományi Újjáépítési Csoport, (angolul Provincial Reconstruction Team – PRT) alapvetően katonai személyek és csoportok (kiegészítve néhány polgári személlyel) olyan egysége, amely Afganisztán minden tartományában újjáépítési, segélyezési, fejlesztési, valamint humanitárius tevékenységet hajt végre, azzal a céllal, hogy egy afganisztáni viszonylatban biztonságos környezetet teremtsen. Magyarország 2003 óta vállal szerepet az afganisztáni nemzetközi missziós feladatokban. A katonai feladatok mellett úgy, mint őrzés – védelem, konvoj és VIP kísérés, a lakosság életkörülményeinek javítását is elősegítő CIMIC22 projektek végrehajtása az elsődleges tevékenység. A CIMIC csoportok a számukra meghatározott feladatokat szakértőkből álló összekötő csoportok (úgynevezett Liaison Team-ek) segítségével hajtják végre. Az összekötő csoportok tartják a kapcsolatot a járások, települések vezetőivel, a rendőrfőnökökkel, kórházakkal, helyi vállalkozókkal és a segélyügynökségekkel (például: US AID United States Agency International Development – Egyesült Államok Nemzetközi Fejlesztési Segélyügynökség) [1].

A Magyar Honvédség Tartományi Újjáépítési Csoport (továbbiakban MH TUCS) híradó és informatikai, információvédelmi rendszerének alaprendeltetése, hogy biztosítsa a kontingens belső híradását, annak tervezését, szervezését és üzemeltetését tábori elhelyezési viszonyok között, a szakmai alárendeltségébe tartozó híradó, informatikai és információvédelmi beosztottak tevékenységének irányítását [2]. Biztosítania kell a kapcsolatot a nemzeti rangidős-, nemzeti (hazai) parancsnoksággal és szervezetekkel az MH TUCS tevékenységéről történő folyamatos tájékoztatás, valamint az eszközök és anyagok saját kapacitást meghaladó javítása, utánpótlása érdekében, valamint az elöljáró ISAF REGIONAL COMMAND – NORTH (a továbbiakban: ISAF RC – N) parancsnoksággal, az ISAF RC – N nyílt

[22] Civil-Military-Cooperation, civil-katonai együttműködés

és titkos híradó és információs rendszerébe történő bekapcsolódással. A táborban szolgálatot teljesítők számára kiépítésre került egy nem szolgálati célú hálózat, amely a személyi állomány és családtagjaik közötti kapcsolattartást biztosítja.

Az elöljáróval történő kapcsolattartás

A műveleti elöljáró szervezettel (ISAF RC-N) – a NATO nyílt és védett híradó és informatikai rendszerében – történő kapcsolattartást, az ISAF Parancsnokság (ISAF HEADQUARTERS továbbiakban: ISAF HQ) biztosítja. Az összeköttetés megvalósítása vezetékes és vezeték nélküli rendszereken egyaránt kiépítésre került. Amikor csak a helyzet azt lehetővé teszi, a vezetékes összeköttetés az elsődleges összeköttetési forma. Alapvetően az ISAF – NATO-val nyílt és bizonyos esetekben zárt összeköttetés biztosítására, és a hazai kapcsolattartásra használják ezt a módszert.

A rádióösszeköttetés PRC-117/F (TACSAT23) rádiók alkalmazásával kerül végrehajtásra. Az eszköz nyílt és zárt rendszereken alkalmas hang és adat üzenetek küldésére, fogadására. Magas technológiai követelményekkel készült többsávos berendezés, amely szinte minden típusú küldetésnek megfelel, képes együttműködni mind katonai, mind civil rendszerekkel.

A vezetékes összeköttetés alapját a THALES cég által kiépített kommunikációs hálózat alkotja. A rendszer a NATO legnagyobb híradó és informatikai projektje, amely egy nagy távolságú és teljes körű hadműveleti képességekkel bíró (Full Operational Capability: FOC) kommunikációs rendszert biztosít az ISAF részére. Az FOC rendszer célja, hogy a területen állomásozó csapatok vezetési pontjait egy rendszerbe foglalja, és részükre egy mindenki által elérhető nyílt és titkos összeköttetést biztosítson. A Pol-e-Khomriban (továbbiakban: PeK) állomásozó magyar erők részére az ISAF HQ egyaránt biztosított, és a mai napig biztosít nyílt NATO IVSN24 távbeszélő kapcsolatokat, titkos vonalakat NATO IVSN távbeszélő kapcsolatra telepített STU II B végtitkosító berendezésekkel, valamint internet protokoll alapú (VoIP) telefonos összeköttetést. A fenti szolgáltatások igénybevételét mikrohullámú állomások biztosítják. Fenntartásukért az elöljáró parancsnokság a felelős ugyanakkor a híradó és informatikai szakállomány közreműködik a különböző feladatok végrehajtásában.

További lehetőségek, amelyek biztosítják az információcserét a MH TUCS és az ISAF RC – N között, a GSM és a műholdas kapcsolatok. Mobil és műholdas telefonos összeköttetést akkor használnak, amikor a vezetékes kapcsolat nem áll rendelkezésre, vagy a rádiókapcsolat megszakadt. Ennél az összeköttetési formánál elsődleges a mobiltelefon (Roshan, AWCC, nemzeti T-MOBILE) másodlagos az IRIDIUM műholdas telefon, harmadlagos az INMARSAT műholdas telefon. IRIDIUM és INMARSAT készülékekkel nyílt összeköttetés valósítható meg, míg egy STU II B végbiztosító eszköz INMARSAT-hoz történő csatlakoztatásával zárt hálót hozhatunk létre, amelyen már minősített információ is továbbítható.

[23] Tactical Satellite
[24] Initial Voice Switched Network

Nemzeti híradás

Az MH TUCS és Magyarország közötti átviteli út elsődlegesen VSAT[25] műholdas rendszeren keresztüli bérelt szolgáltatás keretében az MH távhívó rendszerén HICOM távbeszélő központ alkalmazásával kiépített összeköttetéssel, INTRANET és INTERNET kapcsolatokkal került kiépítésre. Másodlagosan NATO IVSN kapcsolattal (NATO minősített munkaállomás, NATO IVSN távbeszélő kapcsolatra telepített STU II B végtitkosító berendezés), továbbá helyi és hazai GSM telefonokkal, IRIDIUM és INMARSAT egyedi műholdas eszközökön kezdeményezett hívással, valamint rövidhullámú (a továbbiakban RH) rádióforgalmi rendszeren keresztüli összeköttetés felvételével valósul meg. Az összeköttetés egy HARRIS RF-5800 rádióállomással kerül szükség esetén kiépítésre [3].

A hazai irányú telefax kapcsolat elsődlegesen az MH távhívó rendszerén, illetve kerülő irányon, a NATO IVSN hálózaton keresztül biztosított. Ezen rendszerek teljes kiesése esetén a híradó központ konténerben lévő INMARSAT egyedi műholdas eszközre telepített telefax berendezés kerülhet alkalmazásra.

Az MH TUCS helyi kapcsolati rendszere

Az MH TUCS települési helyén a belső összeköttetés vezetékes – távbeszélő, informatikai és kisteljesítményű ultrarövid hullámú (továbbiakban: URH) rádió eszközökkel valósul meg. Elsődlegesen a holland kontingenstől átvett távközlési alhálózatokat használják a táboron belüli kommunikációra.

Az MH PRT belső kapcsolati rendszerének biztosítása a táboron belül:

- HICOM távbeszélő központ mellékeivel,
- Számítógépes – levelező informatikai hálózat szolgáltatásaival,
- Őrhelyek és EÁP- ok26 részére telepített kisközponttal (Panasonic),
- Kis teljesítményű, kézi URH adó- vevőkkel.
- Helyi SIM kártyával ellátott GSM rádiótelefonok felhasználása, eseti lehetőségként szabályozva.

Az MH TUCS kapcsolattartási rendje műveleti feladat végrehajtásakor

Feladat végrehajtás idején az elsődleges kommunikáció a rádió híradás. Az összeköttetés az MH TUCS híradó és informatikai részlege által tervezett és szervezett RH, URH és RH/ URH rádióforgalmi rendszerek és eszközök alkalmazásával valósul meg. Amennyiben a környezeti viszonyok (távolság, hegyek időjárás) ezt nem teszik lehetővé a helyi SIM kártyával ellátott rádiótelefonok alkalmazása kerül bevezetésre. Afganisztán területén az mobiltelefon lefedettség még csak a forgalmasabb útszakaszok, illetve lakott területek környékén megfelelő, ezért sok esetben szükséges a fentiekben már említett műholdas eszközök (IRIDIUM, INMARSAT) alkalmazása. Sajnálatos dolog, hogy a helyi sajátosságok miatt sok esetben előfordul, hogy egy feladatot végrehajtó konvojjal hosszabb időre is megszakad az összeköttetés (Volt már rá példa, hogy ez egy-két órát is jelentett) [4].

[25] Very Small Aperture Terminal
[26] Ellenőrző Áteresztő Pont

Azfállomány magánbeszélgetése

VSAT műholdas berendezésen keresztül biztosított „nyilvános állomás”-ok/ mellékek felhasználásával, a Budapest (a továbbiakban: Bp.) HM - II. központtal létesített „visszahívásos” eljárással.

Az MH TUCS parancsnokának engedélye alapján – rendkívüli esetben – a meglévő egyéb, szolgálati feladatokra fenntartott eszközökkel és szolgáltatásokkal.

Informatikai hálózatok

Az informatika elengedhetetlen a kommunikáció, adatfeldolgozás, adattárolás döntés-előkészítés, és döntéshozatal szempontjából, nélkülözhetetlen eszköz a vezetés és a felhasználók számára.

Az informatikai biztosítás célja:

- Az elöljáró ISAF parancsnoksággal történő kapcsolattartás
- Az elöljáró nemzeti parancsnoksággal történő kapcsolattartás VTC-n[27] és a HM INTRANET-en keresztül
- A belső informatikai, információs rendszer működtetése
- Szolgálati és nem szolgálati informatikai (Internet) támogatás az állomány részére

Az MH TUCS informatikai biztosítása két fő információtovábbító rendszerre épül. A tábor nemzeti informatikai hálózata műholdas összeköttetésen keresztül kapcsolódik a Magyar Honvédség informatikai hálózatához, amely biztosítja a tábor részére az INTERNET és az INTRANET hozzáférést. Az INTERNET kapcsolattal ellátott munkaállomások a híradó központ konténerben elhelyezett routeren és a VSAT-on keresztül csatlakoznak az MH INTERNET szerveréhez. Az INTRANET kapcsolattal ellátott munkaállomások közvetett módon, a híradó központkonténerben elhelyezett kettő szerveren (fájl kezelő, levelező), routeren és VSAT-on keresztül csatlakozik az MH INTRANET-hez. Ez a két szerver biztosítja a tábor felhasználóinak bizonyos szintű felügyeletét, a felhasználók adatainak korlátozott mennyiségben történő tárolását, az MH INTRANET-en belüli levelezést, valamint a heti egyszeri videokonferenciát. A személyi állomány részére elsősorban hazai kapcsolattartás céljából polgári szolgáltatótól INTERNET szolgáltatás került bérlésre.

Az ISAF RC – N által telepített a tábor területén működő ISAF SECRET és NATO SECRET informatikai hálózat rejtjeles műholdas összeköttetésen keresztül kapcsolódik az ISAF és a NATO informatikai hálózatához, amely biztosítja az arra jogosult felhasználók részére a minősített információk küldését, fogadását. Ezeket a hálózatokat az ISAF RC – N telepítette és kizárólagos joggal teljes körűen üzemelteti és felügyeli.

Fejlesztési irányok

Az MH TUCS működése és tevékenységének híradó és informatikai biztosítása megfelelőnek mondható. A kommunikáció fejlesztéséhez, és az összeköttetés biztonságának növeléséhez véleményem szerint a kontingens részére szükséges lenne még több készlet TACSAT rádió kiutalására a nagy távolságú feladatok zárt csatornán történő vezetésének biztosításához. Baghlan tartomány területén vannak

[27] Video Teleconferencing

olyan járások, amelyek olyan távolságokra helyezkednek el Camp Pannoniától[28], hogy az összeköttetés RH/URH eszközök alkalmazásával nem lehetséges. Személyes tapasztalatok alapján – a területek hegyvidékes jellege, valamint e területek népsűrűségének alacsony szintje miatt a mobil telefon lefedettség sem megfelelő – az ilyen feladatok végrehajtásánál szükséges a műholdas összeköttetés. Az IRIDIUM és INMARSAT eszközök használata nagyon költséges, ezért lenne célszerű minden olyan csoportot PRC-117/F műholdas eszközzel ellátni, amelyik nagy távolságú feladatot lát el. Amennyiben ezeket az eszközöket használnák a konvojok az eszköz az ISAF műholdakra csatlakoznának fel, amely jelentős mértékben csökkentené a kommunikáció anyagi vonzatát. Egy másik nagy előnye az ilyen típusú kommunikációnak, hogy zárt háló felépítésére alkalmas. A magyar fél részére, mint a teljes ISAF részére a kulcsokat az ISAF HQ generálja és osztja. Ennek tükrében az együttműködés más PRT-k hasonló csoportjaival egyszerű módon megvalósítható az eszközök, valamint a kulcsok kompatibilitása miatt [5].

A konvojon belüli híradásnál problémát jelent, hogy a Magyar Honvédség nem rendelkezik olyan eszközzel, amely minden körülmények között képes lenne egy nagyobb – 6-7, vagy annál több gépjárművet, harcjárművet tartalmazó – oszlop áthidalására. Az új típusú URH eszközeink (Kongsberg MRR MH-300[29]) 1 W-os maximális kimenő antenna teljesítményt nyújtanak, ami nem elegendő ekkora távolság áthidalására, főleg olyan esetben, amikor páncélozott eszközök alkotják a konvojt. A megfelelő teljesítményt biztosító rádióknál (MOTOROLA MTS2000) az a probléma, hogy a frekvenciatartomány teljes mértékben beleesik a jammer[30] által lefogott tartományba, amely a távirányítású robbanóeszközök ellen védi az oszlopot. Ahhoz, hogy a belső híradás teljes mértékben biztosított legyen a feladatok során egy olyan eszköz beszerzésére, illetve kiutalására lenne szükség, amely alkalmas a fenti körülmények között a megbízható összeköttetés fenntartására.

A tábor területén üzemelő informatikai hálózat alapját a hollandok által kiépített optikai gerinchálózat képezi. A gyűrű topológiával kiépített rendszer a kontingens vezetéséhez szükséges informatikai hátteret megfelelően biztosítja. A tábor területén dolgozó alegységek számának növekedése megkövetelné az optikai hálózatok kibővítését az újonnan felépített konténerek irányába, ahol egy UTP hálózattal minden irodába behúzható lenne az INTRANET, INTERNET szolgáltatás a munka folyamatos biztosítása érdekében. A munkavégzést nagymértékben könnyítené egy esetleges sávszélesség növelés a VSAT rendszeren hazai irányba. Ezáltal az adatok küldésének, fogadásának, letöltésének ideje csökkenne így hatékonyabbá válna az MH TUCS tevékenysége.

Hivatkozások

[1] Szabó László: A Tartományi Újjáépítési Csoport, mint a terrorizmus elleni küzdelem közvetett formája, Hadtudományi Szemle 2. évfolyam 2. szám, Budapest, ISSN: HU ISSN 2060-0437, 2009

[2] Dr. Rajnai Zoltán – Takács Péter: Az afganisztáni missziós híradás tapasztalatai, Kard és Toll, Budapest, ISSN 1587-558X, 2006/3. szám, 27-32. oldal, 2006.

[28] az MH TUCS tábora PeK-ben

[29] Multi Role Radio – többfunkciós rádió kézi kivitel

[30] zavaró állomás

[3] Magyar Sándor mk. őrnagy: Katonai kommunikációs igények, lehetőségek a békefenntartás vezetésének támogatásában, Doktori (PhD) értekezés, ZMNE, Budapest, 2008.
[4] Tóth András: A béketámogató és békefenntartó műveletek híradása, Diplomamunka, ZMNE, Budapest, 2004.
[5] Haris Károly: A béketámogatás híradó és informatikai támogatásának újszerű megközelítése, Diplomamunka, ZMNE, Budapest, 2009.

JOBBÁGY Szabolcs - SÁNDOR Miklós

A MINŐSÍTETT ADATOK VÉDELMÉRŐL SZÓLÓ 2009. ÉVI CLV. TÖRVÉNY

Act no. CLV of 2009 on the protection of qualified data

Zrínyi Miklós Nemzetvédelmi Egyetem

jobbagy.szabolcs@zmne.hu – sandor.miklos@zmne.hu

Absztrakt

Mindenki számára köztudott, hogy a saját maga határait feszegető, a lehetetlent nem ismerő, megállíthatatlanul dübörgő információs társadalom mindennapjainak a szerves, tudatos és aktív részesei vagyunk. Az ezt átívelő információs szupersztráda alappilléreit megtestesítő információ nélkül elképzelhetetlen ennek a pillanatról-pillanatra megújuló infokommunikációs forradalomnak a léte. Lényegi mivolta abban gyökerezik, hogy az információ mindenki számára a megfelelő módon, a megfelelő mennyiségben és minőségben, a szükséges mértékben, a kellő időben és helyen a rendelkezésére álljon. Ebben a milieu-ben az információt a felfokozott jellegéből adódóan azonban nem szabad magára hagyni, védeni kell a rosszakaratú támadások, az illetéktelen és jogosulatlan hozzáférésekkel szemben.

A szerzők a cikkben alapul véve és elemezve a „Minősített adatok védelméről szóló 2009. évi CLV. törvényt" röviden általános kitekintést próbálnak nyújtani az információbiztonságnak, az információvédelemnek, mint egyre markánsabban megjelenő és érvényesülni kívánó, a híradást és informatikát vagy komplex értelemben az új keletű megnevezéssel illetett infokommunikációt és ennek a technológiai alapját megtestesítő infokommunikációs rendszereket-hálózatokat egyaránt akarva-akaratlan és nélkülözhetetlenül átható szakterületnek a hazai szabályozására.

Abstract

It is common knowledge that we all are integral, conscious and active participants in the everyday life of unstoppably booming information society, which keeps trying to go beyond its limits and for which nothing is impossible. Information, embodying the base of the information superhighway spanning over it, is indispensable for the existence of this infocommunication revolution, renewing itself every single moment. Its essence is that information should be made available for everyone in the proper way, in the proper amount and quality, to the desired extent and at the proper place and time. In this environment, due to its intense nature, information must not be left alone but should be protected against any ill-meant attacks or unauthorised and illegal access.

Taking 'Act No. CLV of 2009 on the protection of qualified data' as their starting-point and analysing it in their article, the authors strive to give a brief and general overview of the national regulation of information security or protection as a more and more markedly present and prevalent field, unavoidably and indispensably penetrating both telecommunications and IT, or in a complex sense and with their

newly-coined common name, infocommunication, as well as the infocommunication systems and networks providing the technological base of the former.

Kulcsszavak:
információs társadalom, infokommunikáció, információ, információbiztonság, minősített adat, bizalmasság, sértetlenség, rendelkezésre állás, elektronikus információbiztonság.

Keywords:
information society, infocommunication, information, information security, classified data, confidentiality, integrity, availability, electronic information security

Előszó

Napjainkban a társadalmi fejlődés fokozatainak harmadik nagy szignifikáns korszakát, ciklusát éljük, melyet az információs társadalom31 kifejezéssel illet a releváns szakirodalom. Ennek a típusú társadalmi szerveződésnek az alapvető alkotóeleme, legfontosabb lényegi meghatározója az információ32, mely egy óriási jelentőséggel bíró „érték", mellyel rendelkezni, melynek birtokosának lenni, pedig „hatalom". [1][2][3][4]

Ezen egyszerű okból kifolyólag azonban nem csak az információ értékének, jelentőségének a súlya, hanem a vele szemben megnyilvánuló támadások száma is ugrásszerűen megnőtt és folyamatosan növekvő tendenciát mutat napjainkban is, mely támadások, illetéktelen információszerzések-hozzáférések, a jogosulatlan behatolások változatos formáinak, minden lehetőséget kiaknázó módjainak tárháza határokat nem ismer. Ugyanakkor a fent említett tevékenységek negatív, destruktív hatásai, az általuk okozott károk volumene is egyre súlyosabb következményekkel jár az egyes személyek, az ország, az információt kezelő rendszerek, ezáltal a katonai infokommunikációs rendszerek biztonságának vonatkozásában is.

Ez egyértelműen megköveteli az információ fokozottabb védelmét, a továbbítására, feldolgozására, tárolására, kezelésére szolgáló infokommunikációs hálózatok33 [5] biztonsági szintjének fokozását, az információ és az átvitelére szolgáló rendszerek védelmére, a biztonságos továbbításnak a lehetővé tételére predesztinált egyre kifinomultabb, megbízhatóbb és biztonságosabb módszerek, eljárások, technológiák, eszközök és berendezések életre hívását és rendszerbeállítását, a szüksé-

[31] *Információs társadalom:* Egy viszonylag új keletű dolog, mely az informatika és a távközlés konvergenciáján, az információ és a tudás szabad létrehozásán, forgalmazásán, hozzáférésén és felhasználásán alapuló társadalmi struktúra kialakításán nyugszik. Legfőbb mozgatórugója az informatikai, a távközlés, a szórakoztató elektronika, és a média külön – külön is hatalmas ütemű fejlődése. A Hadtudományi Lexikon értelmezésében az ipari társadalmak utáni társadalmi formáció, a XXI. századi úgynevezett információs korszak társadalma.

[32] *Információ:* Átvitelre, tárolásra vagy feldolgozásra alkalmas formában kifejezhető hír, ismeretanyag. Az információ lehet jel, adat, szimbólum, kép, hang, stb.

[33] *Infokommunikációs hálózat:* Az infokommunikáció az informatika és a kommunikáció (híradás) integrációja. Az infokommunikációs (híradó-informatikai) rendszer magába foglalja az információ előállítását, gyűjtését, felvételét, tárolását, feldolgozását, törlését, és továbbítását, továbbá az ehhez szükséges berendezéseket, elektronikus eszközöket, üzemeltető és felhasználó személyeket az információ bármely típusát tekintve.

ges információk-adatok különböző szintű minősítését, az információbiztonság34 [6], az információvédelem35, a minősített adatok36 [7] kezelésével kapcsolatos eljárások, szabályzó intézkedések, törvények, jogszabályok komplex egységének és az információbiztonság-politikának37 [6] az előtérbe kerülését.

Az egyre fokozottabb veszélynek kitett infokommunikációs rendszerek-hálózatok, a rajtuk keresztül továbbított információk, minősített adatok azonban nem csak a „polgári-civil" szférában vannak jelen az egyre inkább növekvő „információéhség" és az újabbnál-újabb felhasználói igények kiszolgálásának érdekében, hanem a fegyveres erők, a haderők szektorában, mint egyfajta speciális felhasználási szegmensek területén is aktívan képviseltetik magukat a vezetés és irányítási rendszerek, a csapatok vezetésének legfontosabb és alapvető eszközeiként. Ezen elméleti megfontolás alapján érthető, hogy a katonai kommunikációs rendszerek információbiztonságának kérdése is halaszthatatlan és folyamatos megújulást igénylő és egyben megkövetelő kérdéskör. Különösen igaz ez a mai kor modern hadseregeire, hadviselési módjaira, digitális hadszíntereire38 [8][9][10]. Ebben a speciális, új típusú környezetben az információ, a különféle katonai infokommunikációs hálózatok óriási jelentőséggel bírnak. A digitális hadviselés39, a

[34] *Információbiztonság:* „Az információbiztonság a katonai szervezetek vezetésének, működésének sikere érdekében az adatok bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint az adatkezelő képességek megfelelő szintű védettsége."

[35] *Információvédelem:* Az információvédelem fogalmára nagyon egyszerű magyarázattal szolgálhatunk a hozzá szorosan kapcsolódó fogalom, az információbiztonság alappillélére építkezve. E gondolatmenetet végigfuttatva azzal a triviális megfogalmazással élhetünk miszerint, ha az információbiztonságot egy állapotnak tételezzük fel, akkor az információvédelem ennek az állapotnak a megteremtésére, fenntartására és fokozására irányuló tevékenységek és eszközök összessége.

[36] *Minősített adat:* A 2009. évi CLV. a minősített adatok védelméről szóló törvény értelmében megkülönböztethetünk nemzeti és külföldi minősített adatot. A nemzeti minősített adat „…olyan adat, amelyről – a megjelenési formájától függetlenül – a minősítő a minősítési eljárás során megállapította, hogy az érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele a minősítéssel védhető közérdekek közül bármelyiket közvetlenül sérti vagy veszélyezteti…és tartalmára tekintettel annak nyilvánosságát és megismerhetőségét a minősítés keretében korlátozza." A külföldi minősített adat fogalma, pedig „Az Európai Unió valamennyi intézménye és szerve, továbbá az Európai Unió képviseletében eljáró tagállam, a külföldi részes fél vagy nemzetközi szervezet által készített és törvényben kihirdetett nemzetközi szerződés vagy megállapodás alapján átadott olyan adat, amelyhez történő hozzáférést az Európai Unió intézményei és szervei, az Európai Unió képviseletében eljáró tagállam, más állam vagy külföldi részes fél, illetve nemzetközi szervezet minősítés keretében korlátozza."

[37] *Információbiztonsági politika:* Az információbiztonsághoz szorosan kapcsolódó fogalom. Tulajdonképpen „Az általa meghatározott felelősségi rend és hierarchizált szabályozás, a saját erőkre, képességekre, környezetre, ellenséges erőkre vonatkozó adatok biztonsági alapelvek szerinti kockázatokkal arányos védelme, valamint a rendszabályok folyamatos pontosítása, hatékonyságuk ellenőrzése, a biztonsági eseményekre való gyors és hatékony reagálás képezi az információbiztonság alapját."

[38] *Digitális hadszíntér:* Egy többdimenziós, digitalizált hadszíntér, ahol magas fokon elektronizált, tudás alapú (knowledge based army), nagy találati pontosságú precíziós (hightech) fegyverzetű hadseregek, digitális katonák, információs harcosok harcolnak. Alapvetően infokommunikációs, multimédiás szolgáltatásokat biztosító harci hálózatokon nyugszik, helyet biztosít a támadó és védelmi információs műveleteknek. „Digitális hadszíntér alatt azt a virtuális teret ért(het)jük, amely magába foglalja a fegyveres küzdelem rendszerének informális elemeit (az elektronikus információszerzés, -továbbítás, -feldolgozás illetve az ennek bénítására és lefogására alkalmazott eszközöket és eljárásokat)."

[39] *Digitális hadviselés:* Napjainkban a harmadik hullámú vagy negyedik generációs hadviselés korszakát éljük, mely a 21. század jellemző hadviselési módja. Legfontosabb jellemzője a globalitás, a

hatásalapú műveletek40 [10], a hálózatközpontú hadviselés41 [11], mint az „új típusú küzdelem” alapvető alkotóelemeit testesítik meg az ellenség legyőzése, az információs fölény-uralom megszerzése-kivívása, a kitűzött cél, a meghatározott feladat elérése és véghezvitele céljából többek között digitális katonák42 [12] és információs harcosok43[10] bevetése, alkalmazása révén.

Mielőtt hozzálátnánk a címben megnevezett törvény boncolgatásához, fontosnak tartom összegezvén a fent elhangzottakat tisztázni azt a kérdést, hogy hogyan is kapcsolódik össze az információ, az infokommunikációs hálózat az információbiztonság és a minősített adatok védelmének a kérdésével. A közös csatlakozási pont evidens, hiszen mint azt korábban említettük volt egy fogalmi kitekintő keretében, az információ számtalon formában van jelen az őt továbbítani, feldolgozni, tárolni predesztinált infokommunikációs rendszerben, mint például hang, kép, jelzés és a számunkra, a cikk szempontjából meghatározó jelentőséggel bíró adat formájában. Tehát az adat tekinthető úgy is, mint egy ismeretelem, egy valamilyen információt magában hordozó, az információ, mint értelemmel bíró adat, „infokommunikációs elem”, melyet tartalmának függvényében minősíteni, az adathoz

dinamikus hadműveletek, a vezetés-irányítási rendszerek (C2-Command and Control) pusztítása, precíziós csapások, digitális és hálózatos hadseregek. Alkalmazására elsőként az I. Öböl háborúban került sor a nemzeti kommunikációs és államigazgatási infrastruktúra ellen intézett digitális, infokommunikációs támadások végrehajtása által.

[40] *Hatáslapú műveletek (effects-based operations):* „A katonai műveletekben alkalmazott hatásalapú megközelítés (effects-based approach) elve szerint a hadszíntéren egymással hálózatba kapcsolt objektumok vannak. Egy kiválasztott központ és a benne található nagyfontosságú célpontok elleni támadás, különböző hatásokat eredményezhet a többi, hozzájuk kapcsolt objektumok működésében is….A hatásalapú műveletekben a korábbi felfogáshoz képest komolyan figyelembe veszik azt a láncreakcióhoz hasonlító elvet, miszerint a kezdeti közvetlen hatással –első csapással- törvényszerűen további közvetett károsító, korlátozó hatásokat lehet elérni, amely a teljes rendszerre különböző mértékű negatív hatást fejt ki. Az előidézett hatások eredőjének, vagyis az összhatás eredményének elemzése és értékelése képezi a hatásalapú műveletek lényegét….A közvetlen és közvetett hatások elve szerint egy rendszer belső – kulcsszerepet játszó – elemeire mért pusztító vagy korlátozó jellegű csapás mind a rendszeren belül, mind, pedig a rendszerek közötti kapcsolatokban másod, harmad és n-edik típusú és erősségű hatásokat vált ki.”

[41] *Hálózatközpontú hadviselés:* „A hálózatközpontú hadviselés (NEC- Network Centric Warfare) legfontosabb eleme az információk megszerzésének és felhasználásának radikálisan új módja, amely gyökeresen átalakítja a haderő vezetési rendszerét is, hiszen lehetővé teszi, hogy minden információ a vezetés minden szintjén egy időben álljon rendelkezésre, és ennek megfelelően a döntések mindig a lehető leggyorsabban és a döntés szempontjából optimális szinten szülessenek. A NEC lényege, hogy egyetlen integrált rendszerbe foglalja az érzékelőket, a döntéshozókat és a fegyverrendszereket. Alkalmazása során kiemelkedő jelentőségű a koalíciós partnerek közötti minél jobb információ-megosztás, a döntéshozatal felgyorsítása, illetve az, hogy a megfelelő időben a megfelelő katonai eszköz kerüljön bevetésre. Az NEC sokkal több, mint többletfelszerelés: optimalizált parancsnokságra, vezetési struktúrára, illetve átalakított kiképzési rendszerre helyezi a hangsúlyt, hogy a válasz gyors és a körülményeknek megfelelő legyen.”

[42] *Digitális katona:* „A digitális katonák (vagyis összfegyvernemi manőverező erők) a digitalizált harcmezőn, elektronizált és informatizált fegyverrel, digitális vezérlésű, igen nagy találati pontosságú ún. precíziós fegyverrel harcolnak az általános hadműveleti terv alapján. Kiképzésükbe és felkészítésükbe beletartozik a számukra rendszeresített számítógépek (palmtopok, laptopok, törzsmunkaállomások, digitálisan vezérlet híradó eszközök, ellenőrző és felderítő eszközök, fegyverek és fegyverrendszerek, stb.) kezelésének mesterfokú elsajátítása.

[43] *Információs harcos:* „Az információs hadszíntéren az információs műveleti terv szerint digitális adatszerző, feldolgozó, továbbító, valamint támadó és védő információs műveleti eszközökkel (fegyverekkel), eljárásokkal harcolnak.”

való hozzáférést a szükséges és elégséges mértékben korlátozni kell, az adatot védeni kell, és biztosítani kell a bizalmasságát44, sértetlenségét45 és rendelkezésre állását46. [7][10]

2009. évi CLV. törvény a minősített adatok védelméről

Létrejöttének okai

A Sólyom László Köztársasági Elnök Úr és a Dr. Katona Béla Úr az Országgyűlés elnöke által aláírt, a minősített adat védelméről szóló törvényt, mely 2010. április 1.-jén lépett hatályba, alapvetően az állami és közfeladatok zökkenőmentes, zavartalan biztosítása érdekében, a közérdekű adatok megismerésének alkotmányos jogából, valamint ennek a jognak a kizárólag szükséges és arányos mértékű korlátozásából kiindulva alkotta meg az Országgyűlés. A törvény megalkotása időszerű volt több szempontból is, értendő ez alatt az idejétmúlt korábbi szabályozás aktualizálása, egyértelművé tétele, a hiányzó szabályozási részelemek, részterületek, a minősített adatok kezelésével foglalkozó nélkülözhetetlen új intézmények, szervezeti elemek felállítása, létalapjuk és intézményrendszerük megteremtése, a hazai szabályozásnak a szövetségesi rendszerekben működő szabályozásnak és gyakorlatnak való megfeleltetése.

Ennek az új törvénynek a megalkotását az államtitokról és szolgálati titokról szóló 1995. évi LXV. törvény szükségessé vált átfogó felülvizsgálata során feltárt hiányosságok tették indokolttá. A felülvizsgálat alkalmával megállapítást nyert többek között, hogy kifejezetten sok a „Szigorúan titkos" és a „Titkos" minősítési jelzéssel ellátott nemzeti minősített adat. Ugyanakkor problémát jelentett bizonyos jogintézmények hiánya is, mint a nemzeti személyi és telephely biztonsági tanúsítványok és a nemzeti iparbiztonsági rendszer, melynek következtében például EU Telephely Biztonsági Tanúsítvány hiányában magyar gazdálkodó szervezetek nem vehettek részt az EU adatok megismerését indokolttá tevő tenderekben. Továbbá a különböző nemzetközi szervezetekben történő szerepvállalásunk, az Euroatlanti régióban elfoglalt helyünk is újabb problémákat, végrehajtandó feladatokat, és megoldásra váró szabályozási kérdéseket vetett fel ezen a téren. Ennek következtében a revízió rávilágított a külföldi, elsősorban NATO és EU, valamint a nemzeti minősített adatok védelmére vonatkozó követelményrendszerek közötti markáns különbözőségekre, mint például az elektronikus információbiztonságra47 vonatko-

[44] *Bizalmasság:* A minősített adatot csak az arra jogosult személy ismerheti meg, csak ő férhet hozzá. Nem fordulhat elő illetéktelen, jogosulatlan információszerzés vagy a minősített adat nyilvánosságra kerülése.

[45] *Sértetlenség:* A minősített adat tartalmát csak az arra jogosult személy változtathatja meg, illetve az adatot csak ő törölheti. Kiküszöböli annak a lehetőségét, hogy a minősített adatot észrevétlenül módosítsák.

[46] *Rendelkezésre állás:* Lehetővé teszi, hogy az arra jogosult személy számára a minősített adat elérhető, hozzáférhető legyen, egyáltalán, hogy használni tudja azt.

[47] *Elektronikus információbiztonság:* INFOSEC – Information security (Electronic information security). „A távközlési és informatikai, valamint egyéb elektronikus rendszerekben és támogató infrastruktúráiban alkalmazott rendszabályok összessége amelyek védelmet nyújtanak az előállított, feldolgozott, tárolt, továbbított és megjelenített információk, bizalmasságának, sértetlenségének és rendelkezésre állásának véletlen vagy szándékos csökkenése ellen.

zó szabályok hiányára, a nemzetközi szervezetek minősített adatok kezelésére vonatkozó szabályrendszereiben bekövetkezett változások (EU) hazai szabályozásba való integrációjának, átültetésének elmaradására. Az új titokvédelmi törvény hiányában jelentős nehézségekbe ütközött többek között a minősített adatok cseréjével járó két vagy többoldalú biztonsági megállapodások megkötése is, nem volt megfeleltetés a nemzetközi szervezetek gyakorlatában alkalmazott és a nemzeti minősítési szintek vonatkozásában, valamint a Bűntető Törvénykönyv állam és szolgálati titok megsértésére vonatkozó paragrafusai ugyancsak nem álltak összhangban a NATO szabályozással. [7][13][[14]

Alapvető célok

A törvény megalkotásával alapvető célul tűzték ki többek között a jogállamiság intézményének alappillérét megtestesítő alapvető jogok tiszteletben tartása, az ország érdekeinek védelme és a nemzetközi kötelezettségvállalásainak maradéktalan teljesítése érdekében, a minősített adatok létrejöttével, kezelésével, a minősítési eljárással, a nemzeti minősített adatok felülvizsgálatával kapcsolatos rendszabályok, a minősített adatok védelme általános szabályainak, az ezt megvalósító személyek és szervezetek körének, a nemzeti iparbiztonsági rendszer főbb eleminek a meghatározását. Szükségessé vált tehát egy egységes követelményrendszer megfogalmazása mind a nemzeti mind a külföldi minősített adatok védelmével kapcsolatban. A törvény megalkotásának indokai között felvonultatott probléma okán, mely a nagyszámú nemzeti minősített adat létére utal, egyértelműen következik, hogy a törvényalkotás egyik alapvető célját testesítette meg ezen adatok volumenének a redukálása. Célként fogalmazható meg többek között a széttagolt szakmai felügyeleti rendszer egységesítése is. [7]

A törvényalkotó természetesen alapul vette a minősített adat kezelésére vonatkozó alapvető kritériumokat, mint a bizalmasság, a sértetlenség és a rendelkezésre állás elvét párhuzamban a szükségesség és arányosság48, valamint a szükséges ismeret49 elvének figyelembevételével. [7][10]

Értelmező rendelkezések

Mint a törvények nagy többségében, és mint az a korábbi 1995. évi LXV. az államtitokról és szolgálati titokról szóló törvényben is tapasztalható volt, ebben az esetben is sor került az egységes értelmezéshez, közös nyelvezethez elengedhetetlenül szükséges fogalomcsokor meghatározására és kifejtésére. Ennek keretében a törvény vonatkozó paragrafusa és annak alpontjai magukba foglalják a minősített adat és az ahhoz szorosan kapcsolódó fogalomtár definiálását, egységes keretbe integrálva a minősített adat kezeléséhez fűződő eljárásokkal, személyekkel, szervezetekkel kapcsolatos definíciókat.

Az információs társdalom „elektronikus íróasztalán" egymás mellé fektetvén a korábbi törvényt és annak utódját, első látásra szembeötlővé válik az a nagyon

[48] *Szükségesség és arányosság elve:* A közérdekű adatok nyilvánosságának korlátozásával foglalkozik, melynek értelmében az adat nyilvánossághoz fűződő jogát csak a törvényi feltételek teljesülése esetén, a védelméhez szükséges mértékű minősítési szinttel és csak a feltétlenül szükséges ideig lehet korlátozni.

[49] *Szükséges ismeret elve:* Az elv a minősített adat megismeréséről rendelkezik, melyet azon személyek részére tesz lehetővé, akiknek az állami vagy közfeladataik ellátásához feltétlenül szükséges.

fontos észrevétel, hogy az aktuális passzus szól, illetve rendelkezik a megértés alapját képező olyan új definíciókról, mint a személyi biztonsági tanúsítványról50, a telephely biztonsági tanúsítványról51, és az elektronikus adatkezelő rendszerről52, mely fogalmak törvényi meghatározása, leszabályozása kvázi az új törvény megalkotása indokainak tárházában jelesen képviseltetik magukat, mint azt korábban említettük volt. Véleményem szerint megemlítendő jelentős különbözősége az értelmező rendelkezéseknek az is, hogy a titokbirtokos53 fogalmát szétbontva az új törvény vonatkozó paragrafusai különbséget tesznek a minősítő54, a felhasználó55 és a közreműködő személye56 között is. [7][14]

A minősítők és a minősítési eljárás szabályai

A törvény vonatkozó paragrafusa szabályozza, és egyértelműen meghatározza azon személyek körét, akik feladat és hatáskörükben egy adat vonatkozásában minősítő jogkörrel rendelkeznek. Ezzel párhuzamosan szabályozza magát a minősítés tevékenységét is, beleértve a minősítéssel védhető közérdekek körének meghatározását, az adat minősítésének egyes eseteit, az alkalmazható minősítési szintek megjelölését és a nemzeti minősített adat felülvizsgálatának és felülbírálatának egyes eseteit.

Itt fontos megemlítenünk a törvény hordozta legjelentősebb változások közül néhányat, melyeket a fent nevezett cím alatt csoportosuló vonatkozó paragrafusok hordoznak magukban. Egyik ilyen változás, hogy a minősítők körében a Legfelsőbb Bíróság elnöke mellett az Országgyűlés Igazságszolgáltatási Tanácsának az elnökét is megjeleníti, ebbe a körbe sorolja továbbá a Nemzeti Biztonsági Felügyelet vezetőjét is, ugyanakkor olyan, az 1995. évi LXV. törvényben meghatározott személyek, mint az Országos Egészségbiztosítási Pénztár elnöke vagy az Országos Nyugdíjbiztosítási Főigazgatóság főigazgatója, a jelen törvényben nem kerülnek a minősítők körébe sorolásra.

Ugyancsak markáns eltérés a két törvény között, hogy az utóbbi esetében az egyes minősítési szinteket az adat nyilvánosságra hozatala, jogosulatlan megszer-

[50] *Személyi biztonsági tanúsítvány:* A 2009. évi CLV. törvény értelmező rendelkezések részében foglaltak értelmében „az a tanúsítvány, amely érvényességi idejének lejártáig meghatározza, hogy valamely természetes személy milyen legmagasabb minősítési szintű adat felhasználására kaphat felhasználási engedélyt."

[51] *Telephely biztonsági tanúsítvány:* A 2009. évi CLV. törvény értelmező rendelkezések részében foglaltak értelmében „az a tanúsítvány, amely meghatározza, hogy a gazdálkodó szervezet milyen legmagasabb minősítésű szintű minősített adat kezelésére alkalmas".

[52] *Elektronikus rendszer:* Az elektronikus adatkezelő rendszer a 2009. évi CLV. törvény értelmező rendelkezések részében foglaltak értelmében „minősített adat elektronikus, elektromagnetikus vagy optikai úton történő kezelésére alkalmas berendezés, módszer és eljárás együttese".

[53] *Titokbirtokos:* Az 1995. évi LXV. törvény általános rendelkezések értelmében „a minősítő, valamint az a személy vagy szerv, akinek vagy amelynek a minősített adatot … továbbították".

[54] *Minősítő:* A 2009. évi CLV. törvény értelmező rendelkezések részének értelmében „feladat és hatáskörében minősítésre jogosult személy".

[55] *Felhasználó:* A 2009. évi CLV. törvény értelmező rendelkezések részének értelmében „az a személy, akinek állami vagy közfeladat végrehajtása céljából a felhasználói engedély kiadására jogosult vezető a minősített adatra vonatkozóan a felhasználói engedélyben rendelkezési jogosultságokat biztosít".

[56] *Közreműködő személy:* A 2009. évi CLV. törvény értelmező rendelkezések részének értelmében „az a természetes személy, aki az állami vagy közfeladatot ellátó szerv feladat- és hatáskörébe tartozó ügyben segítséget nyújt, és ehhez minősített adat felhasználása is szükséges."

zése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele által okozható kár mértéke határozza meg. Ennek megfelelően „Szigorúan titkos", „Titkos", „Bizalmas" és „Korlátozott terjesztésű" minősítési szintekről szól, mely szintek már teljes harmóniát mutatnak többek között a NATO-ban alkalmazott minősítési szintekkel57. Ugyanakkor ennek folyamodványaként megszűnik az „Államtitok" és „Szolgálati" titok, mint minősítési szint kategória, melyről a korábbi törvény még aktívan rendelkezett, és ezzel egyetemben módosításra kerültek a különböző minősítési szintek érvényességi ideje is. Az 1995. évi LXV. törvény értelmében az akkor megfogalmazott „Államtitok" kategória maximális érvényességi idejét 90 évben, a „Szolgálati titok" kategória érvényességi idejét, pedig 20 évben limitálta a törvényalkotó. Jelen esetben ez oly módon változott meg, hogy a „Szigorúan titkos" és „Titkos" minősítési szint esetén 30 évben, a „Bizalmas" minősítéssel ellátott adat esetén 20 évben, a „Korlátozott terjesztésű" minősítési szinttel védett adat esetén, pedig legfeljebb 10 évben állapította meg az érvényesség idejét a törvényalkotó. Természetesen meghatározott módon, korlátozott formában, de mind a két törvény lehetőséget biztosított és biztosít a különböző minősítési szintek érvényességi idejének a meghosszabbítására. Továbbá az új törvény azonosítja az új minősítési szinteknek megfelelő típusú nemzetbiztonsági ellenőrzések szintjét is, mely „Szigorúan titkos" minősítés esetén „C", „Titkos" minősítés esetén „B", „Bizalmas" minősítés esetén „A" típusú nemzetbiztonsági átvilágítást követel meg. A „Korlátozott terjesztésű" minősítési szint esetén a törvény nem rendelkezik nemzetbiztonsági kérdőív kitöltéséről. [7][14]

Külföldi minősített adat

A 2009. évi CLV. törvény vonatkozó paragrafusai kifejezetten a külföldi minősített adatok kezelésére helyezik a hangsúlyt, melyre a korábbi törvényben nem történt intézkedés.

A 2009. évi törvény a 2. számú mellékletében összefoglalja, rendszerezi a különböző nemzetközi szervezetek, mint a NATO, EU, NYEU, EURATOM58, EUROPOL59, EUROJUST60 által alkalmazott minősítési szinteket, és azonosítja az ezeknek megfelelő nemzeti minősítési szinteket. Ha visszagondolunk a korábban említett, a törvény megalkotását szorgalmazó indokokra, célokra, a nemzeti és

[57] *NATO-ban alkalmazott minősítési szintek:* „NATO Cosmic Top Secret", „NATO Top Secret", „NATO Confidential", „NATO Restricted"

[58] *EURATOM:* The European Atomic Energy Community - Európai Atomenergia Közösség. Egy nemzetközi szervezet, melyet 1957.-ben alapítottak a második római szerződéssel. A közösség lényege abban áll, hogy a szerződés aláírói egyértelmű szándékukat fejezték ki az atomenergia békés célú felhasználásával kapcsolatban és az atomenergia-iparban történő készséges együttműködésük iránt. Több ügynöksége létezik, többek között Spanyolországban.

[59] *EUROPOL:* The European Police Office - Európai Rendőrségi Hivatal. Az Európai Unió rendvédelmi ügynöksége, melynek legfontosabb célkitűzése egy biztonságosabb Európa megteremtése, segítségnyújtás az Európai Unió tagállamai rendvédelmi szervei részére a nemzetközi bűnözés és terrorizmus visszaszorítása érdekében. Székhelye Hollandia.

[60] *EUROJUST:* The European Union's Judicial Cooperation Unit - Európai Igazságügyi Együttműködési Egység. A szervezet 2002-ben lett létrehozva az EU által azzal a céllal, hogy előmozdítsák az együttműködést az uniós tagállamok igazságügyi hatóságai között a két vagy több uniós tagállamot érintő nyomozati és büntetőeljárások keretében. Székhelye Hollandia.

külföldi minősített adatok jelölésére szolgáló, a hazai és nemzetközi szervezetek gyakorlatában alkalmazott egyes minősítési szintek egymáshoz illesztése, egymásnak való megfeleltetése, harmonizációja ugyancsak időszerű és halasztást nem tűrő ok volt.

Nagyon fontos kiemelni, hogy a törvény rendelkezése értelmében, abban az esetben, ha a nemzeti minősített adat külföldi minősített adatot is tartalmaz, akkor annak minősítési szintje és a minősítés érvényességi ideje nem lehet kisebb és rövidebb, mint a külföldi minősített adat minősítési szintje és annak érvényességi ideje. [7][14]

A minősített adat biztonságára vonatkozó szabályok

A minősített adatok védelméről szóló törvény a minősített adatok biztonságára vonatkozó szabályok részének első, 10 §-a egy jelentős kritériumot fogalmaz meg a minősített adatok kezelésével kapcsolatban, melynek értelmében minősített adatot kezelni csak a Nemzeti Biztonsági Felügyelet által kiadott engedély alapján lehet, mely szerv új elemként jelent meg korábban a törvénynek a minősítők körét meghatározó paragrafusa alatt. Ezt megelőzően az államtitokról és szolgálati titokról szóló törvény vonatkozó rendelkezése a belügyminiszter felügyeleti jogkörének keretébe helyezte a minősített adatok védelmének szakmai felügyeletét.

A minősített adatokhoz való hozzáférést kizárólagosan a személyi biztonsági tanúsítvány és titoktartási nyilatkozat meglétéhez köti. A személyi biztonsági tanúsítvány kiadása a Nemzeti Biztonsági Felügyelet hatáskörébe tartozó feladat. A minősített adat megismerésével kapcsolatban továbbra is megmarad a megismerési engedély és titoktartási nyilatkozat intézménye mondhatni a személyi biztonsági tanúsítvány intézményén belül, leszabályozva azokat az eseteket a megismeréssel és felhasználással kapcsolatosan, amikor az érintettnek nem kell rendelkeznie a nevezett tanúsítvánnyal.

Továbbá előírja, hogy minden olyan szervnél, ahol minősített adatot kezelnek, meg kell teremteni a személyi61, fizikai62, adminisztratív63 és elektronikus biztonság [10] feltételeket is. Ez önmagában véve nem jelentene merőben új szabályozást, hiszen az előző törvény a titokbirtokos szerv vezetőjének feladat és hatásköre keretében rendelkezik a minősített adatok védelmi rendszerének biztonsági elemeiről, beleértve az imént felvázolt biztonsági feltételeket is, de az új törvény már külön rendelkezik az elektronikus rendszereken kezelt minősített adat és az elektronikus rendszer bizalmasságának, sértetlenségének és rendelkezésre állásá-

[61] *Személyi biztonság:* „…a minősített információ csak olyan személynek juthat birtokába, aki megfelelő szintű személyi biztonsági követelményeknek igazoltan megfelel, illetve az adott minősítésű információ megismerése számára hivatalos célból szükséges. A személyi biztonság megteremtésének egyik legfontosabb eljárása a nemzetbiztonsági ellenőrzés."

[62] *Fizikai biztonság:* „Azon rendszabályok és tényleges akadályok - …falak,…behatolás jelzők, beléptető rendszerek, stb. – összessége, melyek megfosztják az illetékteleneket a minősített, kritikus információkhoz, dokumentumokhoz, eszközökhöz való hozzáféréstől… és meghiúsítják vagy megakadályozzák a fizikai támadást."

[63] *Dokumentumbiztonság:* „ A titokvédelem tágabb értelmezése, amely azt jelenti, hogy az összes dokumentumot a minősítésének, az érzékenységének, vagyis a titkossági osztályba sorolásának megfelelően kell védeni….A dokumentumbiztonság közvetlenül kapcsolódik az elektronikus információbiztonsághoz, hiszen valamennyi elektronikus adathordozó egyben dokumentumnak is minősül."

nak kérdésében is, melyről az 1995. évi LXV. törvényben még nem találunk említést.

Ugyancsak új rendelkezése a törvénynek a személyi biztonsági tanúsítvány intézménye mellett a telephely biztonsági tanúsítvány intézménye is a gazdálkodó szervezetek vonatkozásában, melynek kibocsátását a Nemzeti Biztonsági Felügyelet hatáskörébe utalja. A telephely biztonsági tanúsítvány kibocsátása az iparbiztonsági ellenőrzés lefolytatását követően válik indokolttá abban az esetben, - természetesen, ha kockázati tényezők nem merülnek fel - amikor a minősített adatot kezelő szervnek az állami vagy közfeladata ellátása érdekében gazdálkodó szervezet közreműködését veszi igénybe. [7][13][[14]

A minősített adat védelmét ellátó szervezetek és személyek

A 2009. évi CLV. törvény soron következő V. nagy fejezetében kerülnek meghatározásra a minősített adatok kezelésével kapcsolatban érintett személyek és szervezetek, többek között a már oly sokat emlegetett Nemzeti Biztonsági Felügyelet is. A törvény részletekbe menően szabályozza az érintett szervezet tevékenységi körét, legfőbb feladatát, mely többek között nem más, mint a minősített adat védelmének hatósági felügyelete, a minősített adat kezelésének hatósági engedélyezése és felügyelete, továbbá a nemzeti iparbiztonsági hatósági feladatok ellátása. Korábban az 1995. évi LXV. az államtitokról és szolgálati titokról szóló törvény értelmében a titokbirtokos szerv vezetőjének hatás és feladatkörébe tartozó tevékenység volt a minősített adatok védelméről szóló jogszabályok végrehajtásáról, illetve a hatáskörében keletkezett vagy más szervek által átadott minősített adatok védelmi rendszerének különböző biztonsági elemekkel való kiépítettségéről és működtetéséről történő gondoskodás, mint azt korábban említettük volt.

A felügyelet feladat és tevékenységi körének legfontosabb részét képezi az új törvény által életre hívott személyi biztonsági tanúsítvány, telephely biztonsági tanúsítvány kiadása, a minősített adatok kezelésére szolgáló elektronikus rendszerek használatbavételének engedélyezése, a rejtjeltevékenység hatósági engedélyezésének és felügyeletének biztosítása, a minősített adatok védelmével kapcsolatos bejelentések kivizsgálása, csakhogy néhányat említsünk a legfontosabbak közül. Továbbá korábban említettük volt, hogy az új törvény megalkotásának egyik fontos indokaként jelenik meg a nemzetközi szervezetekkel, szabályozással való harmonizáció, ebből kifolyólag a törvényalkotó a felügyelet tevékenységi körébe utalta a különböző nemzetközi szervezetek vonatkozó szabályzataiban, illetve a minősített adatok védelme tárgyában kötött nemzetközi szerződésekben a nemzeti biztonsági hatóságok számára előírt feladatok ellátását is. [7][14]

Módosuló rendelkezések

Mivel a 2009. évi CLV. törvény a minősített adatok védelméről jelentős változást hoz a korábbi 1995. évi LXV. törvény az államtitokról és szolgálati titokról törvény vonatkozásban, ha már csak az új megnevezésekre, tanúsítványokra vagy szervezetekre gondolunk is, ezért elengedhetetlenül szükséges mindazon releváns törvényekről és az őket kő keményen érintő módosító rendelkezésekről megemlékezni, melyeket maradéktalanul harmonizálni szükséges az új törvény tükrében. Részletekbe menően nem kívánunk kitérni e módosító rendelkezések hosszas felsorolására, csupán címszavakban kívánjuk megemlíteni az érintett törvényeket.

A 2009. évi törvény alkotta szabályozás szorosan érinti tehát többek között a „Büntető Törvénykönyvről szóló 1978. évi IV. törvény", „A csődeljárásról és felszámolási eljárásról szóló 1991. évi XLIX. törvény", „Az Európai Unió bűnüldözési információs rendszere és a Nemzetközi Bűnügyi Rendőrség Szervezete keretében megvalósuló együttműködésről és információcseréről szóló 1999. évi LIV. törvény", „A szervezett bűnözés, valamint az azzal összefüggő egyes jelenségek elleni fellépés szabályairól és az ehhez kapcsolódó törvénymódosításokról szóló 1999. évi LXXV. törvény", „Az elektronikus hírközlésről szóló 2003. évi C. törvény", „Az Európai Parlament magyarországi képviselőinek jogállásáról szóló 2004. évi LVII. törvény", „A légi-, a vasúti és a vízi-közlekedési balesetek és egyéb közlekedési események szakmai vizsgálatáról szóló 2005. évi CLXXXIV. törvény", „Az elektronikus közszolgáltatásokról szóló 2009. évi LX. törvény", „Az országgyűlési képviselők jogállásáról szóló 1990. évi LV. törvény", „A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény", „Az állampolgári jogok országgyűlési biztosáról szóló 1993. évi LIX. törvény", „A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény", valamint „A honvédelemről és a Magyar Honvédségről szóló 2004. évi CV. törvény" releváns paragrafusait. [7][14]

Felhatalmazás

A törvényalkotó felhatalmazza a Kormányt, hogy rendelettel szabályozza a törvényben megjelenő, a korábbi törvényhez képest végbemenő legfontosabb változásokat, értendő ezalatt, hogy a Kormány állapítsa meg többek között a Nemzeti Biztonsági Felügyelet részletes feladatait, eljárás és működési rendjét, a minősített adatok kezelésének rendjét, a minősített adat elektronikus kezelésének részletes szabályait, a rejtjeltevékenység engedélyezésének rendjét és a hatósági felügyeletének részletes szabályait, valamint az iparbiztonsági ellenőrzés és a telephely biztonsági tanúsítvány kiadásának részletes szabályait. [7]

Záró rendelkezések

A jogharmonizáció elősegítése érdekében a 2009. évi CLV. törvény a záró fejezetében rendelkezik a két törvény közötti átmeneti időszakban végrehajtandó intézkedésekről, elindított folyamatokról és határidőkről, megszűnő törvényekről és újabb, esetenként minősített többséget igénylő módosító rendelkezésekről is úgy, mint a személyi biztonsági tanúsítvány beszerzésének, a minősített adatok védelmére vonatkozó fizikai és elektronikus biztonsági feltételek megteremtésének a határidejéről, az 1995. évi LXV. törvény az államtitokról és a szolgálati titokról hatályát vesztéséről, és olyan már korábban is említett esetekről, melyek az új törvény megszületése és hatályba lépése következtében módosulásokon kell, hogy átessenek. [7][14]

Rezümé

Összegezvén a minősített adatok védelméről szóló 2009. évi CLV. törvény legfontosabb passzusait, dióhéjban az alábbi gondolatokat kell felelevenítenünk. Leszögezhetjük, hogy a törvény megalkotása a korábbi szabályozás hiányossága, idejétmúlt volta, a nemzetközi szabályozásban végbemenő változások, a szabályozási rendszerek és törvényi hátterek harmonizációjának szükségessége okán indo-

kolt volt. Olyan új változások következtek be, mint például a különböző minősítési szinteknek az adat nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele által okozható kár mértéke által történő meghatározása, az „Államtitok" és „Szolgáti titok" minősítési szintek megszűntetése, a „Szigorúan titkos", „Titkos", „Bizalmas" és „Korlátozott terjesztésű" minősítési szintek meghatározása, az egyes szintek maximális érvényességi idejének újralimitálása, a hozzájuk szükséges nemzetbiztonsági átvizsgálási szintek újradefiniálása, a Nemzeti Biztonsági Felügyelet felállítása, hatás, feladat és tevékenységi körének meghatározása, a személyi és telephely biztonsági tanúsítvány fogalmi kategória megalkotása, az elektronikus információbiztonságra vonatkozó szabályok életre hívása, az iparbiztonsági ellenőrzés intézményének megteremtése, csakhogy a legfontosabbakat említsük a teljesség igénye nélkül.

Hivatkozások

[1] „Zöld Könyv" A távközlési, média és információ-technológiai szektorok konvergenciájáról és ennek szabályozási kihatásairól. European Comission, Brüsszel, 1997. december 03. (Forrás: http://www.itb.hu/dokumentumok/zold_konyv/index.html#toc /letöltés ideje: 2009.11.10./)

[2] Jobbágy Szabolcs: Az információs társadalom, az informatika és a távközlés konvergenciája. Múlt, jelen, jövő. – In: Hadmérnök A ZMNE Bolyai János Hadtudományi Kar és a Katonai Műszaki Doktori Iskola On - line Tudományos Kiadványa, 2009. március, IV. évfolyam 1. szám (elektronikus) – p. 184-196. (Forrás: http://www.hadmernok.hu/2009_1_jobbagy.pdf /letöltés ideje: 2009.11.10./)

[3] Magyar Hadtudományi Társaság: Hadtudományi Lexikon I. kötet. Szabó József (főszerk.) – Budapest, 1995 – ISBN 963 04 5227 8

[4] Dr. habil Sándor Miklós nyá. ezds – Farkas Tibor fhdgy. – Jobbágy Szabolcs fhdgy.: Híradásszervezés jegyzet a BJKMK Híradó Tanszék BSc, MSc és PhD hallgatói számára – Budapest, ZMNE EEK, 2009 – 109 p.

[5] Muha Lajos: Infokommunikációs biztonsági stratégia. – In: Hadmérnök A ZMNE Bolyai János Hadtudományi Kar és a Katonai Műszaki Doktori Iskola On - line Tudományos Kiadványa, 2009. március, IV. évfolyam 1. szám (elektronikus) – p. 214-224. (Forrás: http://hadmernok.hu/2009_1_muha.pdf - /letöltés ideje: 2009.11.14./)

[6] Magyar Honvédség Öszhaderőnemi Doktrína 3. kiadás (ÁLT/27) – Honvédelmi Minisztérium kiadványa, 2010.

[7] 2009. évi CLV. törvény a minősített adat védelméről – Magyar Közlöny a Magyar Köztársaság Hivatalos Lapja, 2009. december 29. kedd, 194. szám (Forrás: www.nbf.hu/anyagok/jogszabaly/09CLV.doc - /Letöltés ideje: 2010.04.14./)

[8] Dr. Seres György: A digitális hadszíntér határai. – Előadás a Robothadviselés I Konferencián (elektronikus változat), 2001 – 11 p. (Forrás: http://drseres.com/publik/pdf/digit_hun.pdf - /letöltés ideje: 2010.04.06./)

[9] Gácser Zoltán mk. őrgy.: A katona harci képességét növelő korszerű, hálózatba integrált egyéni felszerelésrendszerének kialakítási lehetőségei a Magyar Honvédségben. – Doktori PhD értekezés, Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, 2008.

[10] Dr. Haig Zsolt mk. alez.: Az információs társadalom információbiztonsága Egyetemi jegyzet. – Budapest, ZMNE EKK, 2009 – 179 p.

[11] Nagy Zoltán: A 21. század fegyveres küzdelmeinek irányai és kihívásai a NATO szemszögéből. –In: Hadtudomány. A Magyar Hadtudományi Társaság folyóirata, 2005. december, XV. Évfolyam, 4. szám (elektronikus) (Forrás: http://www.zmne.hu/kulso/mhtt/hadtudomany/2005/4/2005_4_4.html /letöltés ideje: 2010.04.06./)
[12] Várhegyi István – Makkay Imre. Információs korszak, információs háború, biztonságkultúra. – Budapest, OMIKK, 2000 – 296 p. – ISBN 963593 238-3
[13] Zala Mihály: Az új információvédelmi törvény és kihatásai. – Innovációval a Védelemért és a Biztonságért Társaság Innovációs Klub klubnapján elhangzott előadás anyaga, 2010. január 20. (Forrás: http://www.ivb.org.hu/IC-Download.php - /letöltés ideje: 2010.04.17./)
[14] 1995. évi LXV. törvény az államtitokról és a szolgálati titokról – A Magyar Köztársaság Információs Hivatala – (Forrás: http://www.mkih.hu/torvenyek/t9500065/t9500065.htm#kagy1 /letöltés ideje: 2010.04.21./)

VÁNYA László

A HT-28 SAJ INTERJAM PROJEKT

Absztrakt

2007-ben egy kutatás-fejlesztési-innovációs projekt gondolata körvonalazódott, amely egy minőségileg, technológiailag nagy ugrást jelentett a harcászati rádiófelderítés és elektronikai hadviselés 80-90-es években megtorpant technikai eszközparkjához képest. Egy négytagú konzorcium nyerte el a pályázati támogatást és a három éves futamidő végére elérte a kitűzött célokat. Olyan szoftverrádió technológián alapuló berendezéseket fejlesztett, amelyek felhasználva a magyar elektronikai hadiipar legjobb hagyományait, eredményeit, a kor színvonalán valósítják meg az aszimmetrikus hadviselés és a missziókban velük szemben felmerülő követelményeket.

Jelen írás a projekt célkitűzéseit, fő vonalait és az eredményeit mutatja be.

1. A Jedlik Ányos program meghirdetése és fő célkitűzései

A Nemzeti Kutatási és Technológiai Hivatal nevében a Kutatás-fejlesztési Pályázati és Kutatáshasznosítási Iroda felhasználás-orientált kutatásfejlesztések támogatására 2007-ben pályázatot hirdetett **Jedlik Ányos Program** címen. [1]

A program a gazdaság versenyképességének növelését és a fejlődés fenntarthatóságát kívánta elősegíteni korszerű technológiák területén végzett középtávú, felhasználás orientált stratégiai kutatás-fejlesztéssel.

Célja az innováció ösztönzése volt, a magyar K+F stratégiai szempontok figyelembevételével. A program keretében benyújtott projektjavaslatoknak egyértelmű, világos célkitűzéssel kellett rendelkezniük.

2. A pályázatot életre hívó igények és feltételek

A pályázóknak meg kellett fogalmazniuk azokat a legfontosabb tényezőket, amelyek megindokolják a benyújtott elgondolást **úgy műszakilag**, mint a **gyakorlati alkalmazást** illetően. A legfontosabb szempontok az alábbiak voltak:

- a 90-es évektől a polgári hírközlésben, és a modern hadseregekben is uralkodóvá váltak a digitális adás-, vétel- és jelfeldolgozási technológiák;
- a korábbi fejlesztések eredményeképpen létrehozott analóg elektronikai felderítő, zavaró és mérő-ellenőrző rendszerek, a többségében számítógépes vezérlés ellenére napjainkra erkölcsileg és technológiailag teljesen elavultak;
- a hadseregben alkalmazott analóg berendezéseket kivonták a rendszerből, de pótlásukra mindezidáig egyrészt anyagi, másrészt technológiai okokból nem került sor;
- korszerű harcászati és műszaki követelményeknek megfelelő elektronikai (rádió, rádiótechnikai) felderítő és zavaró rendszerekkel a Magyar Honvédség jelenleg nem rendelkezik;
- a NATO Force Protection feladataiban, a missziós feladatokban, illetve a tagországok által vállalt ISTAR (Intelligence, Surveillance, Target Acquisition and Reconnaissance) képességcsomag megteremtésében ezen berendezésekre égető szükség van.

Az igények megfogalmazása mellett ki kellett térnünk annak bemutatására is, hogy mik azok **a jelenleg elérhető technológiai eredmények, műszaki előfeltételek**, amelyek jó esélyt adnak a pályázatban vállalt tevékenységek **reális megvalósítására**. [2] Ezek egy része valóban technológiai jellegű feltétel, másik része pedig a hazai környezetben való megvalósítást indokolta. Ezek az alábbiak voltak:

- napjainkra a korszerű vétel- és adástechnikai rendszerelemek, a digitális jelfeldolgozó áramkörök (DSP) és a számítógép-vezérlésű berendezések olyan technológiai alapot biztosítanak, hogy a szoftvervezérelt komplex mérő-, lehallgató-, jelanalizáló-, helymeghatározó- és zavaró berendezések létrehozásának elvi akadálya nincs;
- a kifejlesztésre ajánlott integrált rendszer az ún. „Software Defined Radio — SDR" technológiára épül, vagyis a működtető program határozza meg, hogy az adott üzemmódban mely részegységek milyen funkciót látnak el. A rádiófrekvenciás jelszintézis, jelanalízis, a különféle modulációs és demodulációs módok nem áramkörökben, hanem a működtető szoftverekben realizálódnak, így a későbbiekben is bármikor ráfejleszthető egy-egy újabb modulációs mód, mérési algoritmus, vagy zavarási elv;
- hasonló, illetve ezzel azonos rendeltetésű külföldi rendszerelemek léteznek, azonban megépített komplex rendszerek nem, vagy csak óriási költségekkel és komoly korlátozásokkal szerezhetők be, miközben minden ország igyekszik a saját korszerű rendszereit a nyilvánosságtól, de még a koalíciós partnereitől is titokban tartani.

3. A hazai fejlesztés indoklása

Az elmúlt évek jelenleg is folyó haditechnikai beszerzéseinek tapasztalatai rámutattak, hogy milyen **nagy költségekkel jár az állomány külföldi felkészítése**, az utaztatásuk, a tanfolyamok megszervezése, a gyakorlati felkészítés a másik, vagy egy harmadik ország bázisain, a menet közben felmerülő technikai problémák elhárításához kapcsolódó eszközszállítási, utaztatási, szállás és egyéb költségek, nem is beszélve az országok között szinte áthatolhatatlan titokvédelmi és rezsimrendszabályok betartása.

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, az tovább csökkenti az egyes rendszerekre eső fajlagos fejlesztési költséget, gazdaságosabban alakítható ki a logisztikai és szervizháttér.

4. Integrált elektronikai felderítő és zavaró rendszer fejlesztése – HT-28 SAJ Interjam projekt

Az Interjam projektet egy négy tagból álló **konzorciumban** adta be, amelynek 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 volt.

5. Az Interjam kutatás-fejlesztési projekt fő célkitűzései [2]

A projektdokumentumban az alábbi célok kerültek megfogalmazásra:

- 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 többrendeltetésű, 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 állomás mintapéldányát megépíteni.

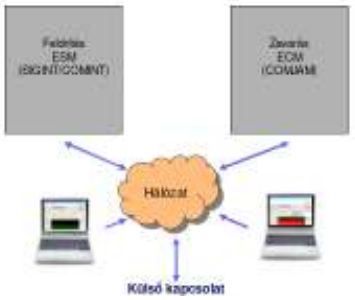
Perspektivikusan kidolgozható többféle hordozó platformra optimalizált rendszerváltozat is, amely pl. könnyű terepjáróba, páncélosba, helikopterbe vagy szállító repülőgépbe is beépíthető a megfelelő tápellátási feltételek és antennakonstrukciók kialakítása mellett.

Ezek előnye, hogy platformtól függetlenül a rendszerfelépítés azonos lehet, közöttük távvezérlési, együttműködési, centralizált irányítási kapcsolatok is kiépíthetők, azonos adatformátumokat és kommunikációs kapcsolatokat alkalmazva. 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 ezen belül még azt is lehetővé teszi, hogy többrendeltetésű, pl. rádiófelderítő-zavaró, radarfelderítő-zavaró, GSM felderítő-zavaró, GPS zavaró, vagy rádió-

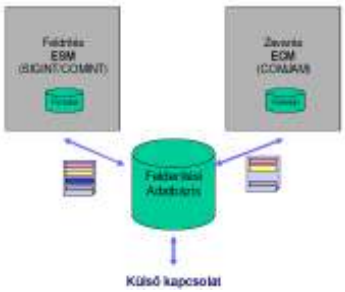
kommunikációs célú feladatban alkalmazzuk ugyanazt az állomást, illetve az egyes üzemmódok közötti gyors átkapcsolást egy másik szoftver futtatásával oldjuk meg.

6. Az Interjam projekt eredményei

A három éves terminus végére az alábbi eredmény született.



1. ábra. Az Interjam rendszer fő elemei



2. ábra. Az Interjam rendszer adatkapcsolata

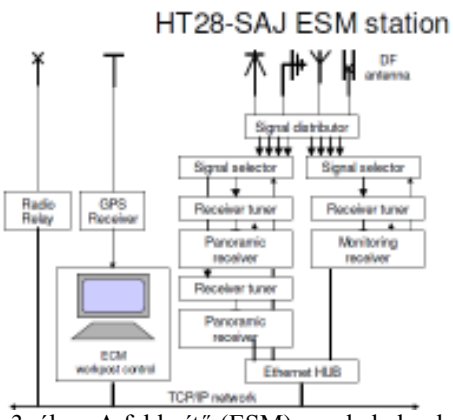
A rendszer két önálló működtetésre is alkalmas munkahelyből, a felderítő (ESM) és a zavaró (ECM) munkahelyből áll. (1. ábra) Ezek kezelhetők azonos helyen (pl. egy gépjárműben) együtt, vagy TCP/IP kommunikációs kapcsolatokon keresztül tetszőleges távolságra széttelepülve egymástól. (A TCP/IP kapcsolatot biztosító kommunikációs eszközök nem részei a projektnek.)

A felderítő (ESM) és a zavaró (ECM) munkahely berendezései egy-egy szállítási egységet képező rack szekrénybe kerültek beépítésre, amelyeket 2 ember tud mozgatni. Ezek kiegészülnek a kezelésüket biztosító 1-1 terepi kivitelű lap-top számítógéppel, az antennákkal és az energiaellátást biztosító aggregátorokkal. Adatkapcsolati szempontból a rendszer mindkét munkahelye egy közös adatbázisba dolgozik, de rendelkezik sajáttal is, ha önálló feladat-végrehajtásra függetlenül telepítik őket.

7. A felderítő (ESM) munkahely

A felderítő munkahely egy lehetséges konfigurációja a 3. ábrán látható. A vevőhöz telepített antennák egy antenna fogadóegységre csatlakoznak. A kimenetről a jelosztókon keresztül jut a kiválasztott antennajel a megfelelő vevőkészülékekhez. A teljes frekvenciasáv (20-3000 MHz) átfogását a vevő tuner biztosítja, amelynek a kimenete a max. 40 MHz sávszélességű panoráma vevőre jut. Az áttekintett frekvenciatartomány egy időben megjeleníthető legnagyobb értéke tehát 40 MHz. A panorámavevő által megfigyelt jelek további analízisre, demodulációra, rögzítésre átadhatók az alapkiépítésben 16 csatornás monitoring vevőre, amely igény szerint többszörösre is bővíthető. Ez azt jelenti, hogy kiépítéstől függően n x 16 csatorna egyidejű feldolgozása biztosítható.

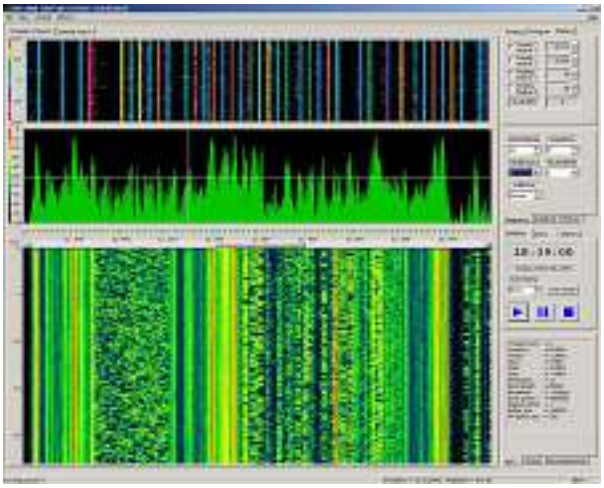
A felderítő (ESM) munkahely vezérlőprogramja egy számítógépen fut, amely valamennyi egységgel TCP/IP hálózaton tart kapcsolatot. A saját települési hely pontos meghatározása céljából egy GPS vevőmodul is tartozik a munkahelyhez. A TCP/IP kommunikáció rádiórelével biztosítható, amely az állványon kívül építhető be.



3. ábra. A felderítő (ESM) munkahely elvi felépítése

1. kép. A kész munkahely

A fejlesztés alapját a SAGAX Kft. **SRS-3000** panoráma vevőkészüléke és az **SRM-3000** monitoring vevőkészüléke képezte. A továbbfejlesztés eredményeképpen **a szoftverrádió technológiának köszönhetően** implementálásra került egy gyors iránymérési eljárás, így a vevőkészülék minden egyes méréshez **a rádióhullám beérkezési irányát is képes szolgáltatni**. A vételi, jelfeldolgozási eljárás digitalizálása eredményeképpen a vevők mérési rekordokat szolgáltatnak, amelyek a merevlemezen letárolódnak, később adatbáziskezelő programokkal feldolgozhatók.



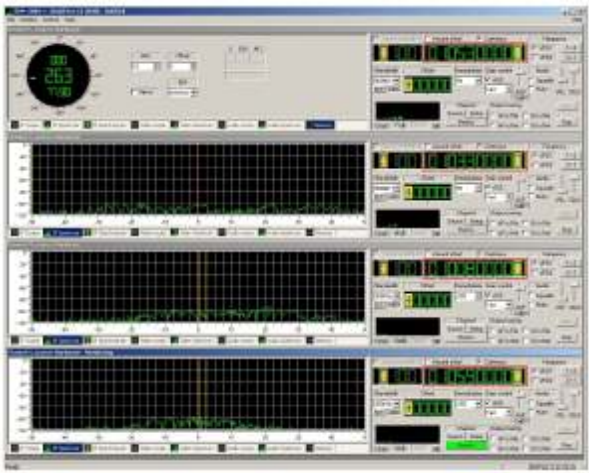
2. kép. Az SRS-3000 panorámavevő képernyőképe

A munkahely feladata továbbá a zavaró (ECM) munkahely számára felderítési adatokat és az azokhoz rendelt zavarási paramétereket előállítani. Együttműködés esetén ezek az adatok a hálózaton átkerülnek a zavaró (ECM) munkahelyre és a megfelelő működésmód esetén ezek képezik a zavaró tár elemeket.

A felderítő (ESM) munkahely tehát egy 20-3000 MHz frekvenciatartományban működő rádiófelderítő-iránymérő berendezés.

A 2. képen, az SRS-3000 képernyőképén az alsó mezőben ún. vízesésdiagramon (waterfall display) az áttekintett frekvenciasáv időben „története" látható, legfelül a jelen pillanat, alatta lefelé nő az eltelt idő. Ez az ábrázolási mód lehetővé teszi a **frekvenciamanőverek felfedését**, a frekvenciaugratásos rádiók jelenlétének észlelését, paramétereik meghatározását. A középső mezőben az áttekintett frekvenciasáv amplitúdó spektruma látható, ami a jelszintek összevetésére, az egyes adások modulációs fajtáinak megállapítására, az elfoglalt sávszélesség megállapítására szolgál. A legfelső mezőben az egyes vett jelekhez tartozó iránymérési értékek (bearing spectrum) olvashatók le.

Az n x 16 csatorna mindegyike egy-egy szabadon konfigurálható ablakban jeleníthető meg, egyszerre legfeljebb 4. Itt állítható be a frekvencia, az offset, a demoduláció típusa, a sávszélesség, a zajzár, a rögzítés módja és a megjelenítés fajtája, ami lehet KF, video, vagy audio amplitúdó spektrum, illetve az iránymérő kijelzője, mint a 3. képen.



3. kép. Az SRM-3000 monitoring vevő képernyő megjelenése

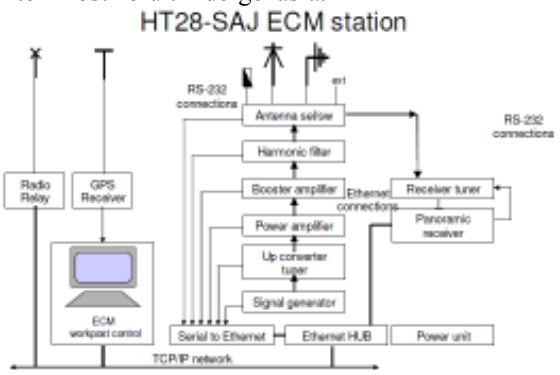
8. A zavaró (ECM) munkahely

A zavaró (ECM) munkahely egy lehetséges konfigurációja a 4. ábrán látható. A zavaró jelet egy zavarjel generátor állítja elő, ezen lehet kiválasztani a modulációs módot, valamint a moduláló jel fajtáját. A névleges vivőfrekvenciát egy konverter egység állítja elő, amelynek kimenő jele egy teljesítményerősítőre kerül, amely a végfokozatot (booster) vezérli. A moduláció hatására nemkívánatos harmonikus tartalom is megjelenne a kimenő jelben, ami zavarná a saját, védendő kommunikációnkat, ezért egy harmonikus szűrő került a booster fokozat után beiktatásra. Ennek a kimenete táplálja az antennakapcsolót. Az adóhoz telepíthető antennák egy antenna elosztó-kapcsolóra csatlakoznak és a feladattól függően kerülhetnek kiválasztásra. A rack szekrényben helyezkedik el a nagyteljesítményű tápegység is, amely a rádiófrekvenciás teljesítményerősítők megtáplálására szükséges.

Az adóberendezés erősítőit, a tápegységeket, a harmonikus szűrőket és antennakapcsolókat a Budapesti Műszaki és Gazdaságtudományi Egyetem, Szélessávú Hírközlés és Villamosságtan Tanszék laboratóriumában konstruálták és a kivitelezés is az ő munkájukat dicséri.

A zavaró (ECM) munkahely vezérlőprogramja egy számítógépen fut, amely valamennyi egységgel TCP/IP hálózaton tart kapcsolatot. A saját települési hely pontos meghatározása céljából egy GPS vevőmodul is tartozik a munkahelyhez. A TCP/IP kommunikáció rádiórelével biztosítható, amely az állványon kívül építhető be.

A munkahely szinte valamennyi fő egysége, így a moduláris tápegység család, a teljesítményerősítő fokozatok, a jelösszegző, a harmonikus szűrő és a nagyteljesítményű antennakapcsoló a projektben került kifejlesztésre. A működtető program szintén most került kidolgozásra.



4. ábra. A zavaró (ECM) munkahely elvi felépítése (változat)

2. kép. A kész munkahely

A 4. ábrán látható, hogy a **zavaró (ECM) munkahely is rendelkezik panorámavevő készülékkel,** amire akkor van szükség, amikor a válaszzavaró (responsive jamming) üzemmódban szükséges a zavarandó jel detektálására, gyakorlatilag az indítja a zavarást. Ez a zavarási elv teszi lehetővé pl. a frekvenciaugratásos adások követő zavarását (escort jamming) is.

A saját működtető program, a saját beépített vevőkészülék és a saját adatbázis – feladattár – struktúra lehetővé teszi az olyan alkalmazást is, amikor a zavaró (ECM) modul önálló energiaellátással, távvezérelve, vagy előre leprogramozott feladatrenddel felügyelet nélkül kerül telepítésre a terepen, rejtve, fedezékben. Beállítható szabad „vadászat" üzemmód is ezek alapján egy adott frekvenciatartományban, amikor is a zavaró berendezés minden megjelenő kommunikációs jelre zavaró jellel válaszol.

A fentiek alapján kivitelezhető az a gyakorlati feladat is, hogy egy adott frekvenciatartományban **csak a meghatározott frekvenciákon** üzemelhessenek kommunikációs berendezések és minden más, - szabálytalan forgalom – azonnal zavarásra kerüljön, függetlenül attól, hogy egy perce, vagy egy hete felügyeljük az adott forgalmat.

A saját adatbázisba beírhatók a saját csapatok védendő frekvenciasávjai is, amelyek zavarása nem következik be vett jelek esetén sem.

9. Az Interjam állomás főbb harcászati-technikai adatai [4]

Vételi frekvenciatartomány: 20-3000 MHz, a frekvencialéptetés felbontása: 1 Hz

Scannelési sebesség: 20 GHz/s (25 kHz raszter, 40 MHz sávszélességben)

Valós idejű sávszélesség: 40 MHz

Vízesés diagram időbeni felbontás: 1 ms

Frekvencia spektrum ábrázolt felbontás: 1 kHz

Frekvencia spektrum előállítása: gyors FFT

Audio rögzítés: szabványos .wav fájlba

Demodulációs módok: AM, FM, SSB, ISB

Zavarási frekvenciatartomány: 20-1000 MHz

Teljesítmény: 500W (1 kW opcionálisan)

Frekvenciaugratásos adás zavarása: <1000 hop/s

Reakcióidő: max. 200 ms

Védett frekvenciák tára: max. 1000 frekvencia, vagy sáv

Zavarási módok: spot, subband, TDM (16 fr.)

Zavarójel modulációs módok: CW, AM, FM, USB, LSB, Chirp, sweep

Moduláló jelforrások: single tone, dula tone, wobbulált jel, fehér zaj, Syllabic noise, .wav file, külső moduláló forrás jele

Antennák: körsugárzó, iránymérő, műantenna, más, külső antenna

Fizikai méretek: 19”/12 U

Tömeg: kb. 60 kg egységenként

Működési hőmérséklet tartomány: 0-50 C^o

Tárolási hőmérséklet tartomány: -20 C^o - + 50 C^o

Tápfeszültség: 230 V, 50 Hz, teljesítményfelvétel max. adási teljesítmény mellett: <5 kW

10. Következtetések

A projekt eredményei biztató alapot adnak arra, hogy demonstráljuk, hogy a hazai szakembergárda képes a kor valóban korszerű színvonalán komoly eredményeket felmutatni, amelyek túljutva a mintapéldány szakaszon, úgy harcászatilag, mint a katonai követelmények szempontjából képesek a hazai igényeket kielégíteni, illetve megállják a helyüket a nemzetközi környezetben is.

Irodalom

[1] Jedlik Ányos program - K+F projektek támogatása. http://www.nkth.gov.hu/palyazatok-eredmenyek/jedlik-anyos-program/jedlik-anyos-program-f (2008.12.15.)

[2] Pályázati konzorcium: „Integrált elektronikai felderítő és zavaró rendszer fejlesztése” - benyújtott projektdokumentum. Sagax Kft, 2007.

[3] Az ábrákat a projekt vezetője, Dr. Eged Bertalan bocsájtotta rendelkezésünkre, a képeket készítette: Dr. Ványa László.

[4] http://www.sagax.hu, illetve projektdokumentáció.

SEREGE Gábor

AZ IPV6 ELTERJEDÉSÉNEK KÉRDÉSEI

Az ipari társadalom örökösének tekinthető információs társadalom kialakulásának kezdete az 1970-es évek elejére tehető, amikor a TCP/IP szabvány ősének tartott többközpontú csomagkapcsolt kommunikációs rendszert szabályzó (NCP) protokoll átlépve a titkos katonai kutatások határait, világhódító útjára indult. A kezdetekben csupán négy csomópontot összekötő rendszer a XXI. század elejére behálózta a Földet, és ezzel a fejlett társadalmak mindennapi életének meghatározó elemévé lépett elő. Az információ-technológia kiemelt szerepe a termelésben rákényszerítette a társadalmat egy szövevényes „mindenkit" összekötő hálózat kiépítésére, annak folyamatos használatára, és egy öngerjesztő folyamat eredményekét mindezek robbanásszerű továbbfejlesztésére.

Az Internet a társadalom kritikus infrastruktúrájává nőtte ki magát, amelynek egyenes következménye, hogy a számos kulcsfontosságú előny mellett jelentkező működési zavarokból származó hátrányok, illetve biztonsági kockázatok, veszélyek szerepe is felértékelődött. Az Internet alapjának számító TCP/IP protokollkészletet megvizsgálva megállapítható, hogy az 1979-ben dokumentált negyedik generációs IP napjainkra olyan szembeötlő hiányosságokkal rendelkezik, amelyek felszámolása nem tűrhet további halasztást. [1]

A problémák közül kiemelkedik a kimeríthetetlennek gondolt 32 bites címtartomány kioszthatója elemeinek az elfogyása, amelynek várható időpontja –az olyan elemzők, mint például az iNetCore legoptimistább számításai alapján is - kevesebb, mint két éven belül be fog következni. Az IPv4 által biztosított egyedi azonosító 90%-a már felhasználásra került, ezért ha az internetszolgáltatók, kormányzati-, és vállalati hálózatok nem térnek át rövid időn belül az IPv6 használatára, akkor valószínűleg fennakadásokkal kell számolni.

A téma aktualitásából adódóan publikációm célja, hogy egyrészt bemutassam az IPv6 kialakításától napjainkig tartó életútját, illetve az elterjedését lassító körülményeket, másrészt röviden össze kívánom foglalni az IPv4-hez viszonyított legfontosabb tulajdonságait, amely alapján a jelenlegi protokoll méltó utódjává válhat.

Az IPv6 életútja

A fejlesztőmérnökök az 1990-es évek elején kezdték felismerni az Internet mérhetetlen sikerét és egyben hiányosságait is. A különböző alkalmazások, file cserélő szolgáltatások, a World Wide Web az email népszerűségének hatására exponenciálisan növekedni kezdett a világhálóra csatlakoztatott számítógépek száma. A kibontakozó sikertörténet egyik legkorábban felismerhető gátját a gépek hálózati azonosítását biztosító egyedi címek belátható időn belüli kimerülése jelentette, ezért megkezdődött az IP új verziójának a kidolgozása.[64] 1992-ben hét kü-

[64] Az Internet Engineering Task Force által összehívott 1994-es torontói értekezleten létrehozott Address Lifetime Expectation munkacsoport, a rendelkezésre álló statisztikai adatok alapján a 2005 és 2011 évek közötti időszakra prognosztizálta az IPv4 címtartomány

lönböző javaslat született, amelyek „összefésülése” hatására három évvel később megszületett az IPv6 végleges, az Internet Engineering Stearing Group által is elfogadott (RFC 1883,) verziója. [2] [3]

Az Internet Engineering Task Force, mint az Internet legfelsőbb felügyeletéért, illetve a vonatkozó szabványok használatáért felelős szervezet, 1996-ban határozott egy nemzetközi kísérleti, virtuális számítógép-hálózat létrehozásáról. A 6bone projekt, az IPv4 „felett” felállított kísérleti környezet célja az olyan feladatok megvalósítása volt, mint:

- egy tesztkörnyezet kialakítása az IPv6 fejlesztéséhez;
- IPv6 alkalmazások tesztelése;
- a gyakorlati tapasztalatok megszerzése;
- az IPv6 hálózatok működőképességének igazolása.

A projekt a világszerte önkéntes alapon csatlakozók által mintegy ötven ország részvételével, és 1000 különböző helyszín sikeres kapcsolódásával 2008-ban, az utolsó fázis befejezésével zárult le.

A tesztidőszak kezdetétől a lezárásáig számos olyan fontos előrelépés (RFC[65]) történt, amelyek közül a legfontosabbakat kronológiai sorrendben kívánok felsorolni.

- 1998 (RFC 2460) alap protokollkészlet,
- 2003 (RFC 3315) DHCPv6,
- 2004 (RFC 3775) mobil IPv6,
- 2006 (RFC 4291) stabil címzési architektúra,
- 2006 (RFC 4294) minimális követelmények a hálózati eszközök használatához.[4]

Az RFC kidolgozásával párhuzamosan az olyan szoftvergyártó óriások, mint például a Microsoft és az Apple is megkezdték saját kutatásaikat az új protokollkészlet implementálásához. A Microsoft már 1998-ban elindította fejlesztéseit, így a Windows2000 operációs rendszer már rendelkezett olyan tulajdonságokkal, amelyek lehetővé tették az IPv6 tesztelését. Az IPv6 teljes körű támogatásával a Vista kiadásától lehet számolni.

Az Apple céghez köthető OSx operációs rendszerek 2004-től támogatják az IPv6 használatát.

Az ezredfordulót követően az aktív hálózati eszközöket forgalmazó vállaltok termékeiben is egyre gyakrabban jelentek meg az IPv6 képes berendezések. Napjainkra az összes neves gyártó rendelkezik IPv6 képes termékkel.

Véleményem szerint az IPv6 tényleges elterjedésének kiemelkedő időpontját a 2008-as pekingi olimpiai játékok sikeres lebonyolításához kell kötni, ahol az új protokollkészlet gyakorlatban bizonyította kiforrottságát.

---

kimerülését. A hátralévő idő rövidségére való tekintettel szükséges volt azt is vizsgálni, hogy a címtartomány kiterjesztésén kívül megoldható-e a további újítások kidolgozása.

[65] Reyuest for Comments: Eredetileg: „kéretik megkritizálni”. Olyan dokumentum, amelyet egy új, az Internethez kapcsolódó szabvány bevezetésekor adnak közre, és egy adott intervallumon belül bárki hozzászólhat.

Miben több az IPv6

Az elmúlt 30 év alatt az ipv4 alapokra felépített „szolgáltatások” robbanásszerűen hódították meg a világot. A széleskörű elterjedés együtt járt a szolgáltatásokkal szemben fellépő igények gyors ütemű növekedésével, amely eredményeként az ezredfordulóra nyilvánvalóvá vált az alapok kibővítésének, illetve megújításának a szükségessége. A hálózati reformokat sürgették a konvergencia hatásaként kifejlesztett és milliárdos számban értékesített telekommunikációs (infokommunikációs) eszközök is, amelyek egyben hálózati erőforrást igénylő „hostokká” is váltak.

Az IPv6 képességeinek meghatározásánál nemcsak az IPv4 protokollkészlet hiányosságainak a foltozgatása volt a cél, hanem az olyan új típusú technológiák és alkalmazások által támasztott igények kielégítése is, mint a cellás telefonhálózatok működésének támogatása, vagy az IP alapú szolgáltatások kibővítése.

A következőkben röviden be kívánom mutatni az IPv6-ban rejlő legfontosabb lehetőségeket:

IP címtér kiterjesztése.

Az IPv4 által használt 32 bites címzés mintegy 4 milliárd egyedi IP cím kiosztását teszi lehetővé. A hálózati kapcsolatot igénylő eszközök számának gyors növekedésével számolva, előreláthatólag két éven belül felhasználásra kerülhet az utolsó 8 byte-os IP cím is. A IT társadalom „felébresztése” érdekében több weboldalon találhatunk már olyan vészharangként szolgáló számlálókat, mint, amilyen az 1. ábrán látható.

1. ábra: X-nap

Ezzel szemben az IPv6 128 bites architektúrája 3,4X1038 egyedi IP címet jelent. Az óriássá nőtt címtér alkalmas lenne a Föld összes lakójának fejenként több, mint egy milliárd egyedi cím kiosztására.

Peer-to-peer66 rendszerek támogatása.

A peer-to-peer alapgondolata már az ARPA NET kezdeti fejlesztésénél is jelen volt, hiszen alapvető célja egy autonóm, önkonfiguráló és hibatűrő hálózat létrehozása. [5] A 30 évi várakozás után, a működési mechanizmusának teljes támogatása az IPv6 által látszik megvalósulni. Az IPv6 hálózatokban nincs szükség NAT berendezésekre, ezáltal egyszerűsödik a rendszer és szabad utat biztosít a tényleges végpont-végpont közötti kapcsolatokhoz.

Beépített biztonsági elemek

Az IPv4 tervezésekor nem volt elvárás a biztonsági elemek beépítése, ezért az adatátvitel titkosításának kérdése áthárult a végponton futó alkalmazásokra. Példaként említhető az elektronikus levelezés, amely esetében az email kliens feladata a felhasználó által választott biztonsági szint megvalósítása . Általánosan kijelenthető, hogy ha az alkalmazás nem használ kriptográfiai eljárásokat, akkor az elküldött adat nyíltan „utazik”[67] a címzett irányába.

Az adatok nyílt átvitele figyelhető meg a 2. ábrán, ahol az elküldött email tartalma nyerhető ki egyszerűen.

2. ábra: egy email "mindenkinek"

Az IPv4 estében az IPSec opcionális lehetőség, meg az IPv6-nak ezt a szolgáltatást kötelezően magába kellett foglalnia.[B] A hét csoportba sorolható IPSec protokoll együttes három fő biztonsági szolgáltatást kínál:

- csak hitelesítés
- kombinált hitelesítés és titkosítás
- kulcskezelés

Ezek a biztonsági eljárások már a hálózati szinten találhatók, és fontos kiemelni, hogy használatuk nem zárja ki a már meglévő magasabb szintű biztonsági megoldások további alkalmazását sem.[6]

---

[66] A P2P rendszer első képviselője az 1999-ben feltűnt Napster volt, amely a szerzői jogokat sértő mp3 filecserélő szolgáltatása által vált híressé. A jogvédő szervezetek a rendszer működési sajátosságából adódóan a szolgáltatást hosszú időn keresztül képtelenek voltak felszámolni.

Napjainkban az egyszerű file-cserélő P2P alkalmazások mellett egyre népszerűbbé válnak az online játékok, a videokonferencia szolgáltatások vagy épp a VOIP típusú beszélgetések.

[67] A „man-in-the-middle”- típusú támadások esetén az elfogott csomagok minden nehézség nélkül olvashatók. (Pl.: freemail levelező kliens alapbeállítása esetén legelőször a felhasználónév és jelszó páros nyíltan csatornára)

Gyorsabb hálózati útvonalválasztás

Az IPv6 esetében a fejléc szerkezet egyszerűsödött. Az eddigi kötelező mezők opcionálissá tételével gyorsult az IP csomagok feldolgozása.

Kétféle opcionális rész

- végpontokra vonatkozó rész, melyeket csak a végpontokon található berendezéseknek kell feldolgoznia
- hop-by-hop rész, melyet minden egyes közbenső állomásnak ki kell értékelni.

Ezek a fejrészek kötött sorrendűek, így a routerek csak azt a részt dolgozzák fel, amelyikre ténylegesen szükségük van. Ezzel a rugalmasan kialakított fejlécek használatával lényegesen lecsökkentők a routerekre háruló feldolgozási folyamatok mennyisége.

Az IPv6 bevezetését lassító körülmények

Az előzőekben bemutatott új lehetőségek és szolgáltatások ellenére az új protokollkészlet a „születését" követő húsz éve alatt nem vált képessé az IPv4 teljes mértékű leváltására. A dominancia felé vezető egyenes út csak a jelenlegi címtartomány kimerülése után nyílhat meg.

A következőkben feltárom azokat a körülményeket, amelyek a kezdeti lépésektől kezdve a mai napig gátló tényezőként működnek.

USA ellenállása

Földünk egyetlen szuperhatalma nemcsak katonai szempontból mérvadó a világ többi országa számára, hanem az új technológiák kifejlesztésében és azok mindennapi életbe történő átültetésében is vezető szerepet tölt be. Az új termékek elterjedésének aránya szorosan összekapcsolható az amerikai gazdasági szereplők által sugallt elismertség mértékével.

Az IPv6 esetében is felismerhető ez az összefüggés. Az amerikai IT szereplők ezt a „merész" előrelépést, mint sok ezer más hasonló előremutató fejlesztéssel esetén már megannyiszor megtették, ebben az esetben nem voltak hajlandóak. Értékelve az új protokollkészletben rejlő potenciált, nem ismerték fel annak sürgető szükségességét, ugyanis a világ IT szektorát leginkább kétségbeejtő címtér kifogyásával nem kellett sem akkor, sem most foglalkozniuk. Az Internet alapjaként számon tartott ARPANET[68] az USA Védelmi Hivatala által indított kutatások eredménye, ezért az IPv4 címtér felosztásában igen nagy tartalékot tudtak lefoglalni saját használatra.

A kialakult aránytalanságot jól szemléltetik a következő százalékos viszonyok: az USA lakossága 22%-a Dél Korea és Kína lakosságának, amely országok csupán csak a névtér 2%-val rendelkeznek.

Gazdasági megfontolások

Véleményem szerint az új protokollkészlet széleskörű bevezetését jelentősen visszavetette a gazdasági válság. A kirobbanásából származó negatív hatások eredményeként számottevően csökkent a fejlesztésekre fordítható tőke mennyisége. A gazdasági szereplők túlélési stratégiájára a kiadások csökkentésére való tö-

[68] ARPANET: Advanced Research Projects Agency Network

rekvés, vagy a kisebb anyagi ráfordításokkal fenntartható infrastruktúrára való átállás vált jellemzővé.

Az IPv6 technológiát támogató aktív hálózati eszközök rendszerbe állítása mindenképp anyagi ráfordítást igényel. A beruházások egyik mozgatórugójaként számon tartott UMTS[69] (mobilIP) elterjedésének lassú üteme is a jelenlegi infrastruktúra változatlan üzemeltetését teszi lehetővé, hiszen ilyen szempontból tekintve a fejlesztés megtérülése nem realizálható.

A fejlett társadalmakban túl sok az IPv4-alapokra felépített aktív hálózati berendezések száma, ezért országos szinten a váltás jelentős anyagi beruházást igényelne.

A gazdasági tényezők mérlegelésénél élesen el kell választani a már régóta szövevényes hálózatokkal rendelkező fejlett nyugati társadalmakat, a most kiépülő távol keleti úttörő hálózatoktól. Azokon a területeken a fentebb említett aránytalan címkiosztás hatásaként alapvető érdek az IPv6 rendszerbe állítása, és mivel az IPv6 képes berendezések ára nem tér el lényegesen az IPv4-et támogató eszközöktől, ezért természetesen ott eleve az újabbat választják.

NAT[70] technológia

A több, mint 256 darab hálózati hozzáférést igénylő szervezetek, illetve vállalatok –az eredetileg kialakított három nagy (A, B, C) hálózati kategória alapján- „B" osztályú címet kellett, hogy igényeljenek, amelyből mindösszesen 16384 hálózat létezik. Könnyen belátható, hogy ez a kioszthatő mennyiség viszonylag korán kimerült volna. Ennek a problémának a megoldására született a hálózati címfordítók bevezetése, amelyek jelentősen redukálták a hálózati igényeket.

A NAT berendezések alkalmazása számos hátránnyal jár, azonban oly mértékben terjedt el és „szoktak hozzá" a felhasználók, hogy ezzel az IPv4 címek elfogyásának a réme tulajdonképpen szerte foszlott.

A NAT technológia mellett elkötelezettek álláspontja szerint teljesen felesleges az IPv6 használatára való átállás, helyette inkább a címfordítókat kellene tovább fejleszteni.

„Későn jött és túl kevés"

Egyes IPv4 mellett elkötelezett csoportok nézőpontja alapján az IPv6 bevezetésével túl sokat késlekedett a világ. A NAT eszközök „jelenleg" még fenntartható sikere kifogta a szelet az IPv6 zászlóshajójaként számon tartott elfogyó címtér hajójából. A gazdasági válság is pont a kritikus ponton robbant ki. Ezek hatására a számottevő beruházások ideje is minimum 3, de inkább 4 évvel későbbre tolódott ki. A távoli időpontot tekintve pedig már az IPv6-ban rejlő újítások is kevésnek bizonyulhatnak és lehet, hogy érdemesebb lenne egy merészebb, előbbre mutató generációs **protokollkészletet alkalmazó eszközökre váltani.**

[69] UMTS:

[70] NAT: Network Address Translation (hálózati címfordítás) a csomagszűrő tűzfalak, illetve a címfordításra képes hálózati eszközök (pl. router) kiegészítő szolgáltatása, mely lehetővé teszi a belső hálózatra kötött gépek közvetlen kommunikációját tetszőleges protokollokon keresztül külső gépekkel anélkül, hogy azoknak saját nyilvános IP-címmel kellene rendelkezniük. [7]

Magyarország és az IPv6

Meglátásom szerint Magyarországnak az új generációs protokollcsalád bevezetéséhez fűződő viszonya megegyezik az európai hozzáállással. Eltérően az USA-ban kialakult nézőponttól Európa nem zárkózott el élesen az IPv6 bevezetésétől, de a távol keleti országokra jellemző azonnali váltás sem következett be. A két szélsőséges állapotot véve a tényleges megvalósításban a kettő közötti utat választotta.

Az európai országokban számos olyan fejlesztő csoport jött létre, amelyek a kezdetektől hozzájárultak az IPv6 teszteléséhez.

Ebben a munkában hazánk is szervesen részt vett, ugyanis Magyarországon is voltak olyan vállalkozó kedvű hálózat specialisták, akik hozzájárultak az általánosan kitűzött célok eléréséhez.[71] Ezt bővítette ki 2001-ben az Oktatási Minisztérium Kutatás Fejlesztési Államtitkársága által támogatott TIPSTER6 konzorcium, amely az alapkutatási témákon kívül választ keresett az olyan kérdésekre, mint:

- az IPv6 áttérés mechanizmusa;
- az IPv6 multicast;
- az IPv6 protokoll stackek működése. [8]

A kutatott témákban elért eredmények fontos szerepet töltöttek be az IPv6 alkalmazásához köthető kérdések megválaszolásában.

Kormányzati szinten az IPv6 részletesebb megismerésével 2008-ban kezdtek el foglalkozni hazánkban. Ekkor készült el az „Elektronikus közigazgatási keretrendszer” tárgyú kiemelt projekt megvalósításának a részeként az „Új generációs hálózati protokollok” elemzését tartalmazó hivatalos tanulmány.

A tanulmány összegzése szerint hazánk közigazgatási informatikai hálózatát nem fenyegeti közvetlenül olyan hatás, amely az IPv6 gyors ütemű bevezetését indokolná. A jelenlegi IPv4 alapokon nyugvó hálózat képes kielégíteni a fellépő igényeket, azonban figyelembe véve az előremutató trendeket, a jövőbeni fejlesztési projektek tervezése során IPv6 kompatibilis beruházásokat célszerű előírni. [9]

Az internet több keresőmotorját használva Magyarországon jelenleg a Magyar Telekom által nyújtott, 2009 őszén indított IPv6 teszt lehetőség látszik országosan elérhetőnek. Természetesen más kisebb lefedettséggel bíró internet szolgáltatókat is találhatunk a piacon, akik szintén IPv6 tesztelési, illetve csatlakozási lehetőséget kínálnak. Sajnos általános tapasztalatom, hogy nincsenek elérhető adatok az IPv6-t választott felhasználók táboráról.

A hazai tisztán IPv6 alapon nyugvó weboldalak száma sem jelentős. A „6ixy” jelentés alapján a világon regisztrált 4190 új típusú webhely között 24 magyar található.[10]

Összefoglalás

Az ezredforduló küszöbén számos vállalat vélte úgy, hogy minél előbb át kell térniük az IPv6 alapokra, hiszen elsőként, az új hálózat használatában szerzett tapasztalatokkal, vezető szerephez fognak majd jutni a jövő protokolljára épülő IT világában. Ez a remény azonban még a mai napig nem valósult meg, hiszen az

[71] Az első magyar IPv6 host 1997 áprilisában, a Budapesti Műszaki Egyetem Folyamatszabályozási Tanszékén kialakított teszt számítógépekkel csatlakozott a 6bone hálózatához.

ázsiai térséget leszámítva a világ többi pontján nem történtek tényleges törekvések a tisztán IPv6 alapokon működő hálózatok üzemeltetésére. Ez a lassú tempó jól magyarázható a feltárt gátló tényezők jelenlétével.

Természetesen az átállási folyamat nem állt meg, az IPv6 színre lépéséhez napról napra közelebb kerül a világ. A témához kapcsolódó szakmai fórumok véleménye egységes: IPv6 lesz. Ezt támasztja alá az a tény is, hogy a nagyobb szoftverfejlesztők és az aktív hálózati eszközök gyártásával foglalkozó vállalatok is már egytől egyig készek az IPv6 támogatására.

Véleményem szerint napjainkban már nem az a kérdés, hogy el fog-e jönni az IPv6 korszaka, hanem az, hogy ez mikorra valósul meg, továbbá amikor ez megvalósul, akkor mennyire lesz kiforrott az alkalmazása. Jelenleg a számos új, előremutató lehetőség mellett, még mindig találhatunk nyitott kérdéseket, illetve nem teljesen letisztázott részeket.

Meglátásom szerint a védelmi szféra biztonságorientált tekintetéből értékelve a bevezetésére fel kell készülni. Ebben a felkészülésben nagy segítséget jelenthet ez a lassú átállás, hiszen nem alakul ki azonnal kényszerhelyzet és több idő marad a teszt-, illetve éles hálózatokban szerzett tapasztalatok beépítésére.

Irodalom

[1] Munk Sándor: A jövő internete kutatások, egy védelmi/katonai kutatási program keretei, 2009 december, IV évfolyam 4. szám, Hadmérnök, 2010-04-03

[2] http://www.ietf.org/rfc/rfc1883.txt, 2010-04-03

[3] http://www.laynetworks.com/IPv6.htm#CH3, 2010-09-02

[4] IPv6 - The History and Timeline, http://ipv6.com/articles/general/timeline-of-ipv6.htm, 2010-09-15

[5] Peer-to-peer alapú elosztott filerendszerek Vincze Gábor, Pap Zoltán, Horváth Róbert, http://www.hiradastechnika.hu/data/upload/file/2005/2005_5/HT_0505-5.pdf, 2010-09-09

[6] Máray Tamás – Mohácsi János – Szigeti Szabolcs: Az IPv6 hálózati protokoll, http://ipv6.niif.hu/tipster6/oldpapers/nw1997/ipv6abs_h.html , 2010-09-08

[7] http://wiki.hup.hu/index.php/NAT, 2010-09-04

[8] Testing Experimental IPv6 Technology and Services in Hungary, http://ipv6.niif.hu/tipster6; 2010-09-06

[9] Új generációs hálózati protokollok, www.nfu.hu, 2010-09-07

[10] http://sixy.ch/, 2010-09-25

HORVAYNÉ Fehér Judit

AZ INFORMATIKAI BIZTONSÁG SZABÁLYOZÁSÁNAK KÉRDÉSE A MAGYAR RENDŐRSÉGNÉL

Horvayné Fehér Judit r. szds.
Belügyminisztérium
Informatikai Főosztály
Információ-védelem és Rejtjel Osztály
BM:13-784
Városi:01/441-1843
Szolg.Mob.:06/30/941-1897

Manapság, amikor a számítógép egyre komolyabb szerepet játszik életünkben, az információ védelme új értelmet kap.

Mint minden közigazgatási szervezetnél, a Rendőrségnél is problémaként jelentkezett a védelem kialakítása és a biztonság megteremtése az informatika területén. Ennek érdekében a Rendőrség szabálykeretek közé próbálta szorítani az informatikai területek biztonságosság tételét, és megtenni a szükséges védelemi intézkedéseket a lehetséges fenyegetések ellen, a rendőrségi informatikai rendszerek megóvásáért. Jelen publikációm célja meghatározni a Rendőrség tekintetében a szabályozás kérdéskörét. Továbbá felfedni minden olyan segítő és akadályoztató körülményt, amely a szabályozási rendszer egyes elemeinek elkészítésekor, a Rendőrség Ideiglenes Informatikai Biztonsági Szabályzata megalkotásakor felmerült. Be fogom mutatni a szabályozás céljait, akadályait, megoldásait. Végkövetkeztetésként, rá kívánok világítani azon fontos célokra, melyeket a szabályozással minden más szervezetnek is el kellene tudnia érni. De először tisztázzuk a fogalmakat.

Jelen publikációmban az információn általános értelemben a valóság folyamatairól és dologi viszonyairól szóló felvilágosítást értem. Ebből következően véleményem szerint értelmezése kapcsolatfüggő. Informatikai vonatkozását tekintve állításom szerint az információ olyan jelentéssel bíró szimbólumok összessége, amelyek jelentést hordozó adatokat tartalmaznak és olyan új ismeretet szolgáltatnak a megismerő számára, hogy ez által annak valamilyen bizonytalanságát megszüntetik, és célirányos cselekvését kiváltják.

A fogalmak eltérő alkalmazása és értelmezése alatt jelen publikációmban Prof. Dr. Munk Sándor értelmezését kívánom alkalmazni a biztonság és a védelem tekintetében.

Ennek megfelelően „a ***biztonság*** egy olyan állapot, amelyben valaki/valami a lehetséges fenyegető hatások ellen a megkívánt mértékben védett.

A ***védelem*** pedig ebben az értelemben a fenyegetések elleni, a biztonság (mint megkívánt állapot) megteremtésére és fenntartására irányuló tevékenységek, rendszabályok összessége.”[1;3.o.]

Véleményem szerint, az informatikai biztonsági szabályzat egy eszköz az információk védelmére, és azok biztonságának fenntartására.

A szabályozás kérdésköre

A fogalmakat kivetítettem a Rendőrségre és megállapítottam, hogy igen nagy szerepet játszik a feladatai között az adatvédelem, továbbá azon informatikai rendszerek védelme, melyeken szinte a legfontosabb adatok nap, mint nap megjelennek.

Éppen ezért, a Rendőrség informatikai rendszereinek védelmével kapcsolatban – a hatályos adat- és titokvédelmi előírásokra is figyelemmel – az információtechnológiai eszközökkel és rendszerekkel kapcsolatos tevékenységek szabályozása érdekében, a Rendőrség Ideiglenes Informatikai Biztonsági Szabályzatot adott ki. Ideiglenes mivoltát a jogszabályok kellően nem megalapozott végrehajtásának bizonytalan végkimenetele indokolta. A Minősített Adat Védelméről szóló (továbbiakban: MAV) törvény igen szigorúan fogalmaz az adatok védelmével kapcsolatosan, melyek megvalósítása a magyar közigazgatás részére mind pénzügyi mind adatvédelmi területen igen komoly nehézséget okozott. A Rendőrségen ennek a kérdéskörnek a megoldására több munkacsoport is alakult az évek során egymás feladatait átvéve. A vizsgálataik során megoldhatatlan, alapvető hiányosságokat tartottak szem előtt, és problémákat görgettek maguk előtt.

Felmerülő tényezők

A szabályzat megalkotásánál a szervezet nagyságából és a kormányzati rendszerben elfoglalt szerepköréből adódó élő problémákat tapasztaltam. A készítésnél a munkacsoportnak négy tényezőt kellett figyelembe vennie:

- A rendőrség állandó változása;
- A szervezeti egységek önálló költségvetéssel rendelkeznek;
- Egyedi ügyrenddel rendelkeznek a szervezeti egységek;
- Nincs fellelhető dokumentáció.

A magyar rendőrség állandó változását- a közigazgatás állandó változását okozta a politikai rendszerváltozások. A szervezeti változások időközönként nagyszámú eszköz injekciót eredményeztek, melynek következménye az egyszerre bekövetkező amortizációs csere dömping lett. Megyénként, szervezetenként eltérő az eszközpark felépítése. Vannak olyan szervezetek, ahol, majdhogynem a korral lépést tartva a legmodernebb eszközök megtalálhatók, viszont vannak olyan apró Örsök, ahol még a Rendészeti hálózat elérése is problémát okoz.

A rendészeti hálózaton lévő rendszerek, alkalmazások a legtöbb szervezetnél elérhetőek. Ugyan e változások idézték elő az informatikai rendszerek váltását, változását, újak bevezetését. A bevezetést követően azok karbantartására, fejlesztésére viszont pénzhiány miatt a legtöbb esetben nem volt lehetőség.

Periodikusan visszatérő változások keletkeztek a humán állományban is az állandóan változó szervezeti felépítések miatt, emiatt a különböző szakterületek hol megjelentek ismét, hol beolvadtak vagy teljesen eltűntek más kisebb szervezetek alatt.

Minden rendőrségi szervezet önálló gazdálkodási egység, amely saját költségvetéssel rendelkezik. Ha túl szigorú szabályozási rendszert dolgozunk ki, bizonyos szervezetek a pénzügyi forrást el tudják különíteni az adott feladatok ellátására, bizonyos szervezeteknek a fenntartási költségek kifizetése is problémát okoz. Pél-

dául: Minősített adatkezeléshez szükséges biztonsági körletek kialakítása. Minősített adatok védelmére irányuló intézkedések, speciális adathordozók beszerzése.

Bizonyos szervezeti egységeknél problémát jelentett a biztonsági felelősök kijelölése. Egyes megyék nem rendelkeznek saját rendszergazdával, regionális átcsoportosítással oldhatóak meg a jelentkező hibák kijavítása.

Az eszköz park elavultsága miatt, egyes egységeknél adott alkalmazások nehezen kezelhetőek, egyedi esetben egyáltalán nem használhatóak.

Mondhatnám azt, ahány szakterület, annyi ügyrend. És ez igaz is. Sajnos még mai is elmondható, hogy a szakterületek egyedi ügyrenddel rendelkeznek. Rendkívül nehéz egy fajta értelmezést, egy fajta ügykezelést ráerőltetni azon emberekre, akik a szokásrendszernek megfelelően eddig is jól végezték a munkájukat. Minden ember tisztában van azzal, hogy a szabályokat az ő érdekükben hozzák, de azok alkalmazását már vitatják. A Rendőrség, mint szervezet szakmai szempontból oly heterogén, hogy nem lehet olyan szabályozást hozni, amelyet mindenkire egyformán lehetne alkalmazni.

Ha túl szigorú a szabályozás nem tartják be az emberek. Indokolatlannak tartják. Akkor, pedig nincs értelme szabályzatokat gyártani. Ez is indokolta a szabályozás puszta tényekre való alapozását, azt hogy részletekbe nem bocsátkoztunk a készítése során.

A fenti tapasztalatokból adódóan, megállapítottam, hogy állandó összeütközés áll fenn a jelenlegi törvényi szabályozás és a gyakorlat között, ezért javaslatomra a szabályzat ideiglenes mivoltot kapott. A cél az volt, hogy a problémákat számba véve, azokat sorba állítva oldjuk meg. Ennek folytán a lépcsőzetes bevezetést, szigorítást, és a szakterületenként egyedi szabályozást határoztuk meg.

Minden szabályozás megalkotása kutatással kezdődik. Elsődleges megkeressük azokat az írásos anyagokat, amelyek az irattárban vagy jogi szabályozók között fellelhetőek. A Rendőrség esetében ez a kutatás nem vezetett eredményre. Megvizsgáltam a jelenleg használt alkalmazások dokumentációit, és rendkívülien szűkszavú belső intézkedéseket és utasításokat találtam. A jelenleg is érvényben lévő stratégiai tervek és informatikai politikák pedig már a jelenkornak megfelelő célokat határoztak meg. Egyöntetűen kijelenthetem, hogy nem találtam az informatikai biztonsági szabályzatnak megfelelő korábbi dokumentációt a Rendőrségnél, amelyből kiindulhatott volna a szabályozás, vagy alapkőül szolgálhatott volna. A szervezeti egységenként kialakult belső egyedi szabályozások egymásnak sokszor ellentmondóak voltak, a legtöbb esetben szokásrendszerre épültek, és a Rendőrség egészét nézve nem voltak egységesek. Indokolttá vált egy egységet megteremtő szabályozó rendszer kidolgozása, egy olyan dokumentum együttes megteremtése, mely olyan biztonsági fogalmakat határoz meg, melyet minden szakterület egyformán értelmez.

A szabályozás céljai, akadályai, megoldásai

A szabályozás céljainak meghatározásánál több szintet határoltunk el egymástól a munkacsoport. Ezek az alábbiak voltak:

- a kört behatárolni, amelyre vonatkoztatjuk a szabályozást;
- az egységes rendőrségi informatikai rendszer megteremtése;

- olyan minimálisan érvényesíthető szabályi keretekbe terelje az informatika területén az információ védelmét, amely a jelenlegi körülmények között érvényesíthető;
- intézkedések az informatikai rendszer környezetével kapcsolatban;
- Dokumentációk és dokumentumok elkészítése;
- a szabályozás megismertetése: oktatás, vizsgáztatás.

Minden védelemmel kapcsolatos szabályozásnál az elsődleges feladat azt Az alap cél az volt, hogy a minden egyes kormányzati szintű szabályozásban megjelenő területet, ahol az információvédelmet tetten érhessük, a szabályzatunk érintse.

Az információvédelem területei

- „azonosítás, hitelesítés;
- jogosultság kiosztás, ellenőrzés;
- hozzáférés-szabályozás;
- elszámoltathatóság;
- hitelesség garantálása;
- sértetlenség garantálása;
- auditálhatóság logikai védelmi funkciói;
- bizonyítékok rendszerének és folyamatának kialakítása.”[2;1.o.]

Az első akadály már itt jelentkezett. Túl sok területet, talán túlzottan szerteágazóan szeretet volna magába foglalni a szabályzat készítő csoportja. Ezért az alap három informatikai biztonsági elvet szétdarabolták több területre.

Álláspontom szerint az informatikai védelem alap három elvét kell követni és abból leágaztatni a fennmaradó területeket így elkerülhetőek az átfedések:

- bizalmasság
- sértetlenség
- rendelkezésre állás.

Ezen elvek kifejtését és átfedését a későbbiekben a szabályzat által taglalt fejezetekben majd tetten fogjuk tudni érni. Továbbá be fogom bizonyítani ezen elvek összekeverése okozta a megteremtendő biztonság egyensúlyának elvesztését.

A egységes rendőrségi informatikai rendszer megteremtése érdekben 10 darab olyan alapelvet határoztunk meg, amelyet szakterülettől függetlenül minden egyes alkalmazottnak be kell tartania. Ilyen volt például: Az informatikai eszköz felhasználója csak az a személy lehet, aki a Rendőrség állományának tagja, alapfokú informatikai ismeretekkel rendelkezik, jelen Utasítás rendelkezéseiből vizsgát tett, és az elöljárója engedélyével hozzáférési jogosultságot kapott a Rendőrség informatikai rendszereihez.

Kijelölésre került az Informatikabiztonsági felelős személye, feladatköre, valamint egyes biztonsági jogkörök gyakorlásával kapcsolatos hatásköri és illetékességi szabályok.

A Rendőrség informatikai rendszereinek egymástól való elhatárolását, továbbá a Rendőrség informatikai biztonsági intézményrendszerének kialakításával új szemléletet vezettünk be. Az informatikai rendszerek biztonsági osztályokba sorolását alábbiakban összegzem:

- „információvédelmi alapbiztonsági (1.) osztály:
  nyílt, jogszabályok által nem védett adatok,

személyes adatok,

üzleti titkok,

pénzügyi adatok, illetve az intézmény belső szabályozásában hozzáférés-korlátozás alá eső (pl. egyes feladatok végrehajtása érdekében bizalmas) adatok;

- információvédelmi fokozott biztonsági (2.) osztály:

szolgálati titok, valamint a nem minősített adatok közül a különleges személyes adatok,

nagy tömegű személyes adatok,

- információvédelmi kiemelt biztonsági (3.) osztály:

államtitok,

nem minősített adatok közül a nagy tömegű különleges személyes adatok."[2;5.o.]

A biztonsági osztályok szintű elkülönítési módszert a szabályzat minden egyes fejezetében alkalmaztuk. Az adott témakörökkel kapcsolatosan külön szabályozó passzusokat határoztunk meg az egyes biztonsági osztályokra vonatkozólag. Miután rendszereztük a különböző alkalmazásokat és a rendszerkörnyezetet, a szabályzatban a legfontosabb volt az intézményesített rendszer résztvevőit megszemélyesíteni, és teljes körűen tisztázni a rendszergazda személyét, feladatkörét, illetékességét, és jogköreit.

A szabályozás bizonyos esetekben az alaptételekkel kapcsolatosan nem kellő részletességgel rendelkezik, ami értelmezési kérdéseket vet fel, és félreértésekre ad okot. Az informatikai rendszer meghatározása és körvonalainak tisztázása behatárolja azok körét, akikre a szabályozás tartozik. További problémát vet fel, hogy a MAV törvénynek köszönhetően a kárértékű minősítési rendszer az informatikai rendszerek biztonsági osztályba sorolásánál eltérő értelmezése, szubjektív megítélésre ad okot.

Véleményem szerint az egységes értelmezési rendszerek kidolgozása, a mérő számok bevezetése, a kockázati tényezők számbavétele egyforma értékrendszer kialakítását eredményezi. A rendelkezése állás mérő számai, a fenyegetések felmérése, és a kockázati elemzések eredményeit rendszerezve pontosabb besorolást eredményezhet az biztonsági szintek meghatározásánál.

A szabályozás során azt a minimális szintet határoztunk meg az informatikai rendszerkörnyezet szereplői részére, amelyet mindenkinek maradéktalanul be kell tartania, függetlenül attól, hogy mely szervezet tagja.

Olyan nyilvántartást vezettünk be, melyet személyi és anyagi oldalra osztottunk szét. Erre egységes nyilvántartó űrlapokat dolgozunk ki. Egyes nyilvántartások az adott felhasználóhoz köthetőek, mellyel nyomon követhető, hogy ki milyen hozzáférést kapott, mely rendszerhez, milyen jogosultsággal rendelkezik. Anyagi oldalról teljesen visszakövethetővé tettük az eszközpark összetételét egészen az eszközök gyári számának nyilvántartásáig és személyhez kötéséig. Ezzel teljesen zártkörűvé tettük az eszköz- és személy nyilvántartás rendszerét és nem utolsósorban a felelősségre vonás rendszerét. Az adatkataszter nyilvántartásához szervesen tartozik a felhasználó azonosítása. Különböző felhasználói szerepköröket választottunk el egymástól, azokhoz azonosítókat és hozzáféréseket rendeltünk. Ezek alapján egy személy hozzáférése, szerepköre és az informatikai rendszerekkel kapcsolatos adatai több nyilvántartásból visszakereshetőek. Szabályrendszert dolgoztunk ki a

felhasználói nevek és jelszavak megalkotására. A szerepkörök meghatározásánál figyelembe kellett vennünk, hogy az adminisztrátorok és a rendszergazdák is bizonyos szinten a rendszerek felhasználói. Ezért megalkottuk az adminisztrátori jelszavakra és egyben a rendszergazdai jelszavakra vonatkozó kiegészítő rendelkezések.

A jogosultságokat rendszerbe integráltuk, amely lehetővé tette az esetlegesen felmerülő Jogosulatlan hozzáférések monitorozását, ellenőrzését, auditálását. Az ilyen incidensek kezelésére egyedi szabályrendszert dolgoztunk ki, meghatároztuk a vonatkozó intézkedések körét, és eljárások lefolytatását.

A szakterületek sokrétűsége, az egyedi költségvetésű szervezetek körében megvalósítható biztonsági környezetek kialakításának pénzügyi és személyi akadályai „lenyomták" az elvárható biztonsági szintet egy minimális teljesíthető szintre. Amely sok esetben a veszélyhelyzetek megjelenésének valószínűségét emeli.

Magasabb biztonsági szint meghatározása mellett fokozatos bevezetése a biztonsági szabályozásnak. Az újonnan kialakítandó rendszerek és környezetek esetében a magasabb biztonsági szint megalkotása és alkalmazását indokoltan tartom feltétlenül. Viszont a már meglévő rendszerek és környezetek esetében

A korábbi fejezetekben, ahogy már említettem meghatározták az informatikai rendszert, a felhasználókat és jelen fejezet részben az informatikai elemeket és az informatikai környezetet is.

A szabályzat készítése során egyik feladatom volt azon rendszerelemeknek az összegyűjtése, amelyek aktívan, a rendszert befolyásoló tényezőként jelentkeznek a rendszer használata során. Az alábbiakat gyűjtöttem össze:

- Adathordozók
- Hardver eszközök
- Szoftver eszközök, alkalmazások

A szabályzatban a készítőkkel meghatároztuk a rendőrségi eszközparkban alkalmazható adathordozók fajtáját, és kezelési szabályait. Az adatvagyon kataszter nyilvántartó meghatározásait használva megalkottuk azon hardver eszközök körét, amelyeket a Rendőrség alkalmazásában állnak, és állhatnak, azok beszerzésének lehetőségét és a beszerzés szabályait. Behatároltuk a rendőrségi hálózaton használható alkalmazások és szoftverek fajtáit. Rendszerbe szettünk mindazon alkalmazásokat, amelyeket a Rendőrség fejlesztett és alkotott meg, további fejlesztés céljából. Megvizsgáltuk a rendelkezésre álló nyilvántartásokból a használatban lévő szoftverek sorát, és azok jogtisztaságát. A vizsgálat igazolta, hogy ezen a területen a korábbi évekhez képest a Rendőrség igen nagy fejlődést ért el, a szoftverek majdhogynem 99 %-a jogtisztának bizonyult. Ami azt is bizonyítja, hogy a korábbi rendszerelemekhez kapcsolódó intézkedések pozitív eredményre vezettek.

Az informatikai rendszer környezetét képezte maga az infrastruktúra és a benne lévő személyzet is.

Minden rendszer rendszertervezőnek a rendszer elkészítésénél az a célja, hogy a rá bízott rendszer a nap 24 órájában működjön. Egy rendszernek, ha valamilyen egységben ki szeretnénk fejezni az értékét, akkor nagyon sok szempontot kell figyelembe vennünk. Kutatásaim során az alábbi szempontokat vizsgáltam meg:

- „Rendelkezésre állás szempont rendszere, melyen azt a valószínűséget kell érteni, amellyel egy definiált időintervallumon belül az alkalmazás a tervezés-

kor meghatározott funkcionalitási szintnek megfelelően a felhasználó által használható.

- Más szemszögből vizsgálva, a megbízható működés szempontjából értelmezett biztonsági osztályokra jellemző paraméterként a rendelkezésre állást, a kiesési időt és az ezen belül egy alkalomra megengedett maximális kiesési időt
- Az információvédelem szempontjából történő osztályozás a különböző szervezetek esetén különbözhet a megbízható működés alapján történő besorolástól. Egy minősített adatállománnyal kapcsolatos megbízható működési követelmény a felhasználás módjától és körülményeitől függően lehet alacsony (akár több órás kiesés is megengedhető), ugyanakkor nem minősített, nyílt adatokkal kapcsolatos megbízható működésre magas (csak néhány másodperces kiesést megengedő) követelmények is előfordulhatnak."[2;18.o.]

A fenti szempontrendszert a szabályzat megalkotása során maradéktalanul figyelembe vették, és adott rendőrségi informatikai rendszerekre meghatározták a rendelkezésre állás valószínűségi mutatóit, biztonsági osztályba való sorolását, rendelkezési idejét, kiesési idejét, és az információ védelmének szempontjából történő osztályozását.

A szempont rendszer vizsgálata során megállapítottam, hogy szélesebb körű rendszer szemléletet kell követni, a rendszerek heterogén összetétel és egymástól eltérő felépítése miatt a rendelkezésre állás, megbízható működés külön kezelve azt az eredményt hozták, hogy az értelmezések sok helyen egymásnak ellentmondnak, a mutató számok nem egyértelműen fejezik a rendszer állapotát.

A három fő elvet taglalva, osztályozva és egyenként kibontva kellene a rendszereket elemezni, az elemzések végeredményét összevetni, és egy új értékelő eljárást kidolgozni. alapvetően a fogalmakat tisztázni kell, meg kell határozni, hogy mit értünk rendszeren, mik az elemei és pontosan a környezete. Meg kell tudni a határvonalat élesen jelölni, és a határon belüli információkat össze kell vetni egymással. Ez alapján kell az értékrendet, az osztályozását a különböző rendszereknek és rendszerelemeknek meghatározni.

Az alap biztonsági szabályok meghozatala után az egyik legfontosabb fordulópontnak tartottam a Kommunikáció, és az osztott rendszerek meghatározását és szabályozását. Minden féleképpen külön szabályozási dokumentumok megalkotását javasoltam. Véleményem szerint ezek a szakterületek olya annyira elkülönülnek más szabályozandó területtől, és nagyságukat tekintve is sokkal terjedelmesebbek társaiknál, hogy külön szabályozást igényelnek. Ezt bővebben az eredmények között fogom taglalni.

Az egyik legnagyobb támadási felületet képviselik egy informatikai rendszeren, ezért álláspontom szerint nagyobb odafigyelést is igényelnek az osztott rendszerek és hálózatok. Ezért javasoltam, hogy a szabályzatban alkossuk meg az Összekapcsolási szabályokat. A szabályok létrehozatalánál felmerült a veszélyhelyzeteknek a kezelése is. Kiegészítő rendelkezésként indokoltnak láttuk külön intézkedések meghozatalát a vészhelyzet-megelőzéssel kapcsolatban. Ilyen volt az elektronikus határvédelem, számítógépes topológia elkészítése és az elektronikus vírusvédelem.

Minden adatvagyon nyilvántartó rendszer alkalmazásánál elsődlegesen elvárható szolgáltatás a vészhelyzet, rosszabb esetben a katasztrófa helyzetet követő visszaállíthatóság, és visszakereshetőség. A legegyszerűbb megoldás ezen esetekre az

elektronikus dokumentálás, a mentés és archiválás, ezért az IBSZ egy legfontosabb fejezetének szánták a készítők e rendszerek szabályozását. Három részre tagolták:

- Általános rendelkezések (mely minden egyes rendszerre, alkalmazásra, felhasználóra, vagy bármely rendszerkörnyezeti szereplőre egyaránt alkalmazandó feladatokat tartalmaztak esemény bekövetkeztétől függetlenül)
- Szerverek, központi kiszolgálók mentése (olyan speciális intézkedések halmaza, melyek az informatikai szakembereknek írnak elő feladatokat a központi adattárakkal, és azok eszközrendszerével kapcsolatosan)
- Alkalmazás szintű mentések (kisebb biztonsági események jelentkezésekor végrehajtandó biztonsági intézkedéseket határoztak meg az informatikai szakemberek számára)

Ahogy a publikációm elején már jeleztem a problémák között a szabályzat megalkotásánál az egyik legfőbb akadály volt a dokumentációk és írásos anyagok hiánya. Nem készült korábbi szabályzat, vagy a szabályzat egyes elemeinek megfelelő normatíva, amire támaszkodni lehetett volna, vagy kiindulási pontul szolgált volna a szabályozásnak. A szabályozás körébe a Rendőrség korábban bevonta az Internet és az Intranet alkalmazásának normatíváit, melyek sajnos mára már felújításra szorulnak.

Elsődlegesen ezek megalkotására tettem javaslatot a szabályzók részére. Véleményem szerint a szabályozást a későbbiekben több részre kellene szét tagolni.

- biztonságtechnika,
- kommunikáció,
- rejtjel,
- hálózatvédelem,
- üzemeltetés- karbantartás,
- mentések-archiválások,
- vészhelyzet-katasztrófahelyzet elhárítás,
- informatikai védelem megalkotása,
- informatikai biztonság fenntarthatósága.

Rendőrségi munkáim során azt tapasztaltam, hogy a szabályok maradéktalan betartásnak más emberi oldala is jelentkezett a fentiekben említetteken túl. Az alábbi akadályoztató tényezőket gyűjtöttem össze:

- nem ismerik kellően a szabályokat az alkalmazók,
- nem tudják alkalmazni a szabályokat, átvetíteni a gyakorlatba az elvi szabályok meghatározásait;
- nincsen oktatása a szabályoknak, csak ismertetik, hogy léteznek a szabályok;
- ha vannak oktatások, akkor azok tantervszerűek, elméleti síkon mozognak, nem gyakorlat orientáltak;
- a felhasználók nagy százaléka nem rendelkezik kellő szintű alapképzéssel az számítástechnikai eszközök kezelésének tekintetében;
- a számonkérési rendszer nem tükrözi a felhasználó tényleges tudásának szintjét.

A fenti problémák miatt az alábbiakat javasoltam megoldásként az oktatás és számonkérés területén:

- minden egyes felhasználó, aki rendőrségi alkalmazásba került, alap számítástechnikai képzésen vegyen részt;
- továbbá ne kaphasson jogosultságot rendőrségi informatikai alkalmazásokhoz, amíg az informatikai biztonsági szabályrendszerekből sikeres vizsgát nem tesz;
- szituációs vizsgafeladatokkal mérjék a számonkérés során a vészhelyzetekre, és kompromittálódásra okot adó helyzetekre való felkészültségét a vizsgázónak.

Összegzés - Következtetések

A szabályozás a célját elérte, felölelt minden egyes olyan szakterületet, amely az informatikai alá tartozik, és egy szervezet szempontjából szabályozható. De az Informatikai Biztonsági Szabályzat még csak az első lépés volt egy teljes értékű szabályozó rendszerben. A Rendőrségnek az a célja, hogy létrehozzon egy Informatikai Biztonsági Könyvet, mely részletekbe menően működését szabályozza a Rendőrség Informatikai szakterületének minden egyes kérdéskörét. Ennek érdekében a Rendőrségnek az alábbi feladatokat kell még ellátnia:

- „az informatikai biztonságpolitika és stratégia meghatározása;
- az informatikai rendszerek biztonsági osztályba sorolása;
- az információvédelmi követelmények meghatározása;
- az információbiztonsági követelmények meghatározása;
- az informatikai működés-folytonossági terv (katasztrófa-elhárítási terv);
- az informatikai működési szabályzat;”[2;32.o.]

Publikációm célja volt, hogy a Rendőrség tekintetében a szabályozás kérdéskörét, a segítő és akadályoztató körülményt felfedni, amely a szabályozási rendszer egyes elemeinek elkészítésekor, a Rendőrség Ideiglenes Informatikai Biztonsági Szabályzata megalkotásakor felmerült. Bemutattam a szabályozás céljait, akadályait, megoldásait, az informatikai szakterületek szabályozási lehetőségeit a Rendőrség Informatikai Biztonsági Szabályzatán keresztül. Rá világítottam azokra a sarkalatos pontokra, amelyek egy informatikai rendszer összeomlásához vezethet kellő figyelem ráfordítás nélkül. Rámutattam azokra a vészhelyzetet okozó eseményekre, amelyeket, hogy ha nem kezelünk időben komoly anyagi és erkölcsi kárt tudnak a szervezet számára okozni. Továbbá meghatároztam azon feladatokat, melyeket a Rendőrségnek a Biztonsági Könyv elkészítéséhez még végre kell hajtania.

Következtetésként megállapítom, hogy bármilyen szerteágazó, és gondoskodó, minden problémára kiterjedő szabályozási rendszert dolgozunk is ki egy informatikai közeg védelmére, ha azokat az alkalmazók és felhasználók nem tartják be, pusztán csak papír marad. Nincs olyan technikai és szabályozási megoldás, amely az emberi figyelmetlenségtől megóv minket.

Felhasznált Irodalom

[1] Munk Sándor: Információbiztonság VS. Informatikai biztonság - A "Robothadviselés 7" konferencián 2007. november 27.-én elhangzott előadás kibővített, szerkesztett változata. Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem, Hadmérnök, Különszám, Robothadviselés 7 konferencia kiadvány (1-21.o.)

[2] 60/2008. (OT 32.) ORFK utasítás a Rendőrség Ideiglenes Informatikai Biztonsági Szabályzatának kiadásáról,(1-63.o.)

[3] 2009. évi CLV. törvény a minősített adat védelméről

KURIS Zoltán - SÁNDOR Miklós

A KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRA VÉDELEM ÉS A VÉDELMI CÉLÚ KATASZTRÓFAVÉDELMI HÍRADÁS KAPCSOLATRENDSZERE

Sandor.miklos@zmne.hu zoltan.kuris@bm.gov.hu

Absztrakt

Az információs társadalom működésének zavarai, katasztrófavédelmi és különböző minősített helyzet kialakulásához vezethetnek. A szerzők a társadalmi szintű megközelítést követően, részleteiben fejtik ki a Kritikus Információs Infrastruktúra működési zavarainak hatásait a létfontosságú infrastruktúrákra. Bizonyítani szeretnék, hogy a kialakuló katasztrófavédelmi és egyéb minősített helyzetekben, különösen fontos és nélkülözhetetlen az infokommunikációs rendszerek megbízható működésére alapozott katasztrófavédelmi híradás zavarmentes üzemelése. Az információs stabilitás fogalmának bevezetésén keresztül mutatják be a rendszerközpontú működtetés alapvető irányelveit.

A catastrophy might emerge from the disorders of the informational society. The social effects are analysed. Then the disorders of the critical infrastructure of information is described in detail, How they affect the infrastructures of vital importance the authors describe it in detail. The significance and functioning of sending news are proved as well as the significance of notifying news.

Kulcsszavak:

Kritikus Információs Infrastruktúra Védelem, minősített adat, fizikai biztonság, elektronikai biztonság, dokumentum biztonság, személyi biztonság, Az európai unió létfontosságú infrastruktúrák figyelmeztető és információs hálózata

Marathon Terra; K-600/KTIR, Trans European Services for Telematics between Administrations,CIWIN, TESTA, sTESTA

Bevezetés

Ma már alapvető axiómának tekinthető az, hogy a biztonság újkori értelmezésének megfelelően, a biztonság dimenzióinak rendszere – az elemek közötti kapcsolatrendszer – alapvetően átalakult. Bizonyos biztonsági dimenziók felértékelődtek, más dimenziók pedig veszítettek súlyukból. Különösen igaz ez, amikor az utóbbi évtized változásait, az információs társadalom működésének tükrében vizsgáljuk. Ma a modern társadalmak nagy része felismerte annak jelentőségét, hogy a társadalom zavartalan működését biztosító „létfontosságú infrastruktúrák" működtetése alapvető biztonságpolitikai cél. Ennek megfelelően a modern társadalmak, a biztonsági stratégiájuk megfogalmazásakor különös figyelmet tanúsítanak az újkori

kihívások, kockázatok és fenyegetések részletes feltárására. Az információs társadalmi formációban működő államoknak különös figyelemmel kell lenniük tehát a létfontosságú infrastruktúráik és információs infrastruktúráik védelmére, mert a védelmi rendszer egyenszilárdságának csökkenése alapvetően képes befolyásolni az adott ország geopolitikai és geostratégiai helyzetét egyaránt. A biztonsági stratégia a társadalom működésének biztosítására irányuló alapvető dokumentum. A hazai biztonsági stratégiát elemezve megállapítható, hogy hazánk a fent említett új kori követelményrendszerre építkező, megfelelő biztonsági stratégiával rendelkezik. Ha tovább vizsgáljuk az ágazati stratégiák rendszerét, megállapítható hogy igen ritka a pragmatikus, rendszerszemlélettel rendelkező ágazati stratégia.

Az általános biztonságpolitikai szemléletű megközelítést követően célszerű megvizsgálni azt, hogy a létfontosságú infrastruktúrák zavartalan működtetését célzó Kritikus Infrastruktúra védelem (a továbbiakban: KIV) milyen kapcsolatban van a Katasztrófavédelmi területtel, illetve milyen szerepe van ezen a területen a Kritikus Információs Infrastruktúrák (a továbbiakban KIIV) zavarmentes üzemeltetésének. Érdemes azt is vizsgálni, hogy ezen a területen hogyan valósul meg, - vagy milyen igény mutatkozik - a vezetési irányítási, távközlési és informatikai, rendszerek komplex rendszerének alkalmazásának. Elfogadható állítás az, hogy a társadalom információs és infokommunikációs rendszereinek rendelkezésre állása ugrásszerűen felértékelődik, katasztrófavédelmi és a minősített időszak helyzetében. Célszerű tehát azt vizsgálni, hogy milyen jogalkotási, szabályozási és technológiai feladatok körvonalazódnak ezen a területen. A fentiekből következik, hogy azt is célszerű megvizsgálni, hogy a fentiekben kifejtett vezetés-irányítási, távközlési és informatikai rendszerek, milyen előfeltételekkel és környezetben tudják biztosítani azt az információs stabilitást, bonyolult katasztrófavédelmi és minősített helyzetben.

A biztonság újkori dimenziói

A biztonság fogalmának néhány definícióját az alábbiakban szükséges összefoglalni annak érdekében, hogy az újkori dimenziókat értelmezni tudjuk.

A szó eredetét illetően, a latin securus, securitas: sine-nélkül + cura-aggodalom, félelem összetételéből ered. Tovább fűzve a gondolatat, egy változatban az alábbiak szerint lehet értelmezni a biztonságot.

Egyrészt. fenyegetettség hiánya (abszolút).

Másrészt, olyan állapot, ahol kizárhatók, vagy megbízhatóan kezelhetőek a fenyegetések.

Ezzel összefüggésben a biztonságérzet: veszély, kockázat érzékelése (szubjektív).

A Külföldi szakirodalomban a biztonság fogalmának általános megfogalmazása így hangzik.

„A biztonság fizikai a fizikai veszély hiányát, vagy az e veszéllyel szembeni védelmet jelenti.” [1]

Az Amerikai Egyesült Államok szakirodalmából idézve, pedig így hangzik.

„ A nemzetbiztonság nemcsak lakosságunk és területünk védelme a közvetlen támadástól, hanem létfontosságú gazdasági és politikai érdekeink védelme is különféle eszközökkel.” [2]

A Hadtudomány 2007/1 számában megfogalmazottak szerint a biztonságelmélet új fogalmára közölt meghatározást. Ennek analógiájára: a biztonságelmélet a legtágabb értelemben a nemzeti, a nemzetközi biztonságot befolyásoló kihívások, veszélyek és kockázatok megszüntetésére, a lehető legkisebb szintre mérséklésére hivatott nemzeti, szövetségi, regionális, nemzetközi szervezetek tevékenységének sikerét meghatározó, elméleti tételeket és gyakorlati tapasztalatokat összefoglaló ismeretrendszere. [4]

A Hadtudomány 2006/3 számában [5] biztonság kérdéseivel foglalkozó cikk szerzője egy kutatónak ebben a kérdésben kifejtett véleményét összegezve írja, hogy „azon túlmenően, miszerint a statikus állapotnak tartott biztonságot komplex rendszerként értelmezi, a biztonság meglétét az esetleges veszélyek leküzdésére való képességgel, az erre való felkészültséggel köti össze. Ezzel a biztonság nem egyszerűen állapot, hanem egy olyan cél, amelynek eléréséhez aktivitásra, cselekvésre van szükség."

Az 1985-ben kiadott német Biztonságpolitikai Szótár az alábbiakat tartalmazza.

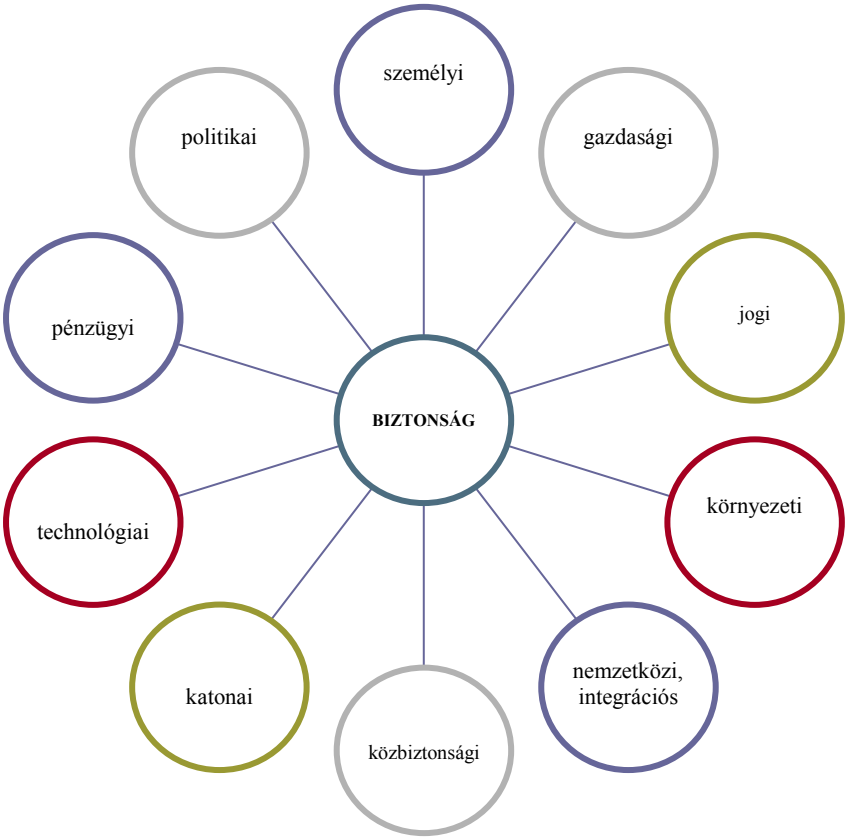
- A biztonság nem más, mint a veszély hiánya;
- a biztonság az egyes emberek vagy azok csoportjainak, az államoknak és az államcsoportoknak a bizonyossága arról, hogy a lehetséges veszélyektől védve vannak;
- a biztonság olyan állapot, amelyben az egyéneket, csoportokat és az államokat komoly veszélyek nem fenyegetik, illetve azoktól védettnek érzik magukat, vagy – pozitívan kifejezve – amelyben biztosak abban, hogy jövőjüket saját elképzelésük szerint alakítják. A biztonság és a fenyegetettség foka jelentős mértékben függ tehát a szubjektív érzettől, a történelmi tapasztalattól, az önmegértéstől és a környezethez való viszonytól. [6]

Végül a Magyar Hadtudományi Lexikon szerint „a biztonság az egyének, csoportoknak, országoknak, régiónak (szövetségi rendszereknek) a maguk reális képességein és más hatalmak nemzetközi szervezetek hatékony garanciáin nyugvó olyan állapota, helyzete (és annak tudati tükröződése), amelyben kizárható vagy megbízhatóan kezelhető az esetlegesen bekövetkezhető veszély, illetve adottak az ellene való eredményes védekezés feltételei." [6]

A fentiekből látható, hogy a biztonságot az államok manapság komplex módon értelmezik. Az elemek fontossági sorrendben: a politikai, gazdasági szociális ökológiai és katonai területek. Természetesen ez béke állapotra jellemző fontossági sorrend és az adott körülményeknek megfelelően a súlypontok áthelyeződhetnek. A fenti elemeket megvizsgálva következtetés eredménye ként egyértelműen megállapítható, hogy a fenti elemek megjelenésének színterei a különböző létfontosságú infrastruktúrák és ezen belül a kiemelt fontosságú szektorok.

Ahhoz, hogy a biztonság hatókörét értelmezni tudjuk meg kell határozni a tartalmát. Ezzel összefüggésben a biztonság szintjei, az egyének, csoportok, kisebbségek, nemzetek, államok, régiók és a nemzetközi rendszer.

Ugyanakkor a 90'-es évektől elterjedt a biztonság fogalmának parttalan használata, kiterjedt azon jelenségek köre, amelyek kiváltói lehetnek a már elemzett biztonsági hiányérzetnek. Ezért szükséges és elégséges értelmezés szerint az alábbi biztonsági dimenziók körvonalazódnak.



3. ábra jellemző biztonsági változatok (szerző)

A társadalom biztonsági érzete összességében mérhető jelenség. E mérés és a biztonsági érzetek meghatározására hívták segítségül a biztonságpolitikával foglalkozó szakemberek a szociológia eszköztárát. A TIT HABE72 (a honvédelmi tárca megbízásából) a Szonda Ipsos-sal közösen két ízben is végzett közvéleménykutatást e terület vonatkozásában. 1999-ben ezer, míg 2008-ban háromezer főt kérdeztek meg „az utca emberei közül”! A következő táblázat ennek rövid összefoglalását szemlélteti.

[72] A TIT Hadtudományi és Biztonságpolitikai Közhasznú Egyesületet életünk legfontosabb kérdéseivel, a biztonsággal és biztonságpolitikával foglalkozik az ország egész területén. A TIT HABE 1996-os megalakulása óta aktívan részt vesz az ország kül-és biztonságpolitikájával, NATO- és EU-tagságával és a nemzetközi biztonság erősítése érdekében végzett egyéb tevékenységével összefüggő kérdések elemzésében és publikálásában, hazai és nemzetközi rendezvények szervezésében, a lakosság különböző célcsoportjainak a tájékoztatásában és felkészítésében.

4. ábra (Forrás: Gondolatok és vélemények a biztonságunkról – a biztonságkultúra kérdései, TIT HABE, 2008)[73]

A biztonság a fejlődés előfeltétele.

A konfliktusok nemcsak az infrastruktúrákat – így a szociális infrastruktúrákat – teszik tönkre, hanem ösztönzik a bűnözést, eltántorítják a befektetőket és lehetetlenné teszik valamennyi szokásos gazdasági tevékenység gyakorlását is. Számos ország és régió a konfliktus–bizonytalanság–szegénység ördögi körének a foglya.

A fenti rövid áttekintés jól példázza, hogy a társadalom működését biztosító infrastruktúrák működésében előforduló zavarok visszahatnak a társadalom biztonsági érzetére és alapvető hatással vannak a társalmi fejlődésre is!

Az infokommunikációs rendszerek információbiztonsági stabilitását biztosító összetevők elemzése

Az információs társadalom nagyon fejlett és hatékony társadalom, ugyanakkor meglehetősen sebezhető is. Sebezhetőségének alapját az adja, hogy működése szorosan kapcsolódik a globális, nemzeti, regionális és lokális információs környezethez [h 67.old.] Irányadó szakemberek szerint, napjainkban várhatóan felértékelődik az információs környezet átfogó védelme. A Magyar Köztársaság nemzeti biztonsági stratégiájáról szóló 2073/2004. (IV.15.) Korm. határozat [3] a fenyege-

[73] Dr. Radványi Lajos szociológus, biztonságpolitikai szakértő, a TIT Hadtudományi és Biztonságpolitikai Közhasznú Egyesület alelnöke *„A magyar lakosság biztonságfelfogásának változásai 1999 – 2008”* című előadásából. Veszélyhelyzetek kezelésének kormányzati koordinációja – munkaműhely, Göd, 2009. március 10.

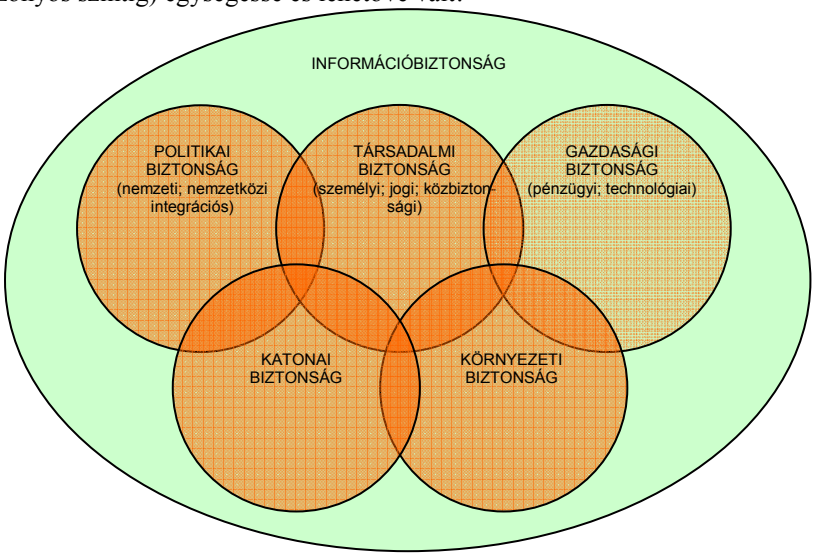
tések, kockázatok, kihívások szakaszában (II.) nevesíti az információs társadalom kihívásait, ezen belül a telekommunikációs hálózatok sebezhetőségét és kockázatait emeli ki. A terrorizmus elleni védekezés szakaszban (III.3.1) külön kiemeli a kritikus infrastruktúrák védelmének feladatait is. Az információs rendszerek védelme szakaszban (III.3.7) pedig hangsúlyozza a kormányzati információs rendszerek védelmének szükségességét és felhívja a figyelmet a sikeres védelem érdekében szükséges együttműködésre, az érintett informatikai és távközlési szolgáltatókkal. Sajnos a Magyar Köztársság Nemzeti Biztonsági Stratégiájával összefüggő ágazati (távközlés, informatika) területét fellelő gyűjtő néven infokommunikációs doktrínának [8] nevezhető dokumentum a mai napig nem került kidolgozásra.

A Magyar Köztársaság kritikus információs infrastruktúrái az alábbiak:

- Informatikai rendszerek és hálózatok,
- automatizálási, vezérlési és ellenőrzési (SCADA, távmérő, távérzékelő és telemetriai)rendszerek,
- internet szolgáltatás és infrastruktúrája,
- vezetékes távközlési szolgáltatások és infrastruktúrái,
- mobil távközlési szolgáltatások és infrastruktúrái,
- műholdas távközlési szolgáltatás és infrastruktúrái,
- földfelszíni műsorszórás és infrastruktúrája,
- közigazgatási informatika és kommunikáció és infrastruktúrái,
- a kritikus infrastruktúrák létfontosságú infokommunikációs rendszerei.

A biztonság dimenzióiban értelmezett információbiztonsággal összefüggésben megállapítható, hogy a KIV szektoraiban gyűjtött, feldolgozott tárolt és továbbított információkat a különféle infokommunikációs eszközök alkalmazásával kezeljük. Infokommunikációs eszközök gyűjtőfogalom kőré csoportosíthatóak, az informatikai és a távközlés, illetve az egyéb információtechnológiai eszközök konvergenciájának következményeként alkalmazott „informatizálódott" eszközök. A fenti infokommunikációs rendszerek információbiztonsági stabilitásának biztosítása alapfeltétel, a katasztrófavédelmi és egyéb minősített időszaki helyzetekben is. Az előző gondolatot tovább fűzve megállapítható, hogy a kritikus információs infrastruktúra azokat az infokommunikációs rendszereket jelenti, amelyek önmagukban is kritikus infrastruktúra elemek, vagy lényegesek az infrastruktúra elemei működésének szempontjából (távközlés, számítógépek és szoftverek, internet,GPS,stb.) [8] A kritikus információs infrastruktúrák védelme tehát a tulajdonosok, gyártók, és használók, valamint a hatóságok programjai és tevékenységei, melyek célja fenntartani a kritikus információs infrastruktúra teljesítményét meghibásodás, támadás vagy baleset esetén a meghatározott minimális szolgáltatási szint felett, illetve, illetve minimálisra csökkenteni a helyreállításhoz szükséges időt, valamint a károkat. [8] Az információs stabilitás elérésének érdekében komplex információbiztonsági elveket kell alkalmazni. Ezeket a komplex és integrált védelmi intézkedéseket tudati, információs és fizikai dimenziókban is érvényesíteni kell a kritikus információk védelmének érdekében. Ezzel összefüggésben elmondható, hogy ezen a területen a minősített adat védelméről szóló 2009. évi CLV. Törvény (a továbbiakban: MAV törvény) már egységes irányelveket szab. A MAV törvény nyomán, a Nemzeti Biztonsági felügyelet működésének, valamint a minősítet adat kezelésé-

nek rendjéről szóló 90/2010.(III.26.) Kormányrendelet, és a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010.(V.6.) Kormányrendelet, viszont már egységes alapokra helyezi a minősített adatok védelme érdekében érvényesítendő, személyi, fizikai, dokumentum és elektronikai védelem komplex rendszerét.[10] Az elektronikai védelmi intézkedések keretei között megjelenik az átvitel út védelme, számítógép (szoftver, hardver és hálózat) védelme. [11] Egységesítésre kerültek a rejtjelzéssel összefüggő követelmények és megjelennek a kompromittáló kisugárzással kapcsolatos alapvető irányelvek. Sajnos a kompromittáló kisugárzás védelmének részletes szabályozását illetően megállapítható, hogy a magas színvonalú védelmi intézkedésekkel összefüggő követelményrendszert nem sikerült érvényesíteni. Ennek az is lehet az oka, hogy – ez a viszonylag új és bonyolult terület – a leg költségigényesebb védelmi intézkedések megvalósítását feltételezi és ezen a területen hazai tapasztalatok hiányában a nemzetközi irányelvekre figyelemmel kell kialakítani a hazai szabályozást! Ezen a területen, az irányadó hazai információvédelmi szakemberek bevonásával, további lépések szükségesek ahhoz, hogy az elektronikai védelem területén a maradvány kockázatot optimalizáljuk és növeljük az elektronikai rendszerek egyenszilárdságát. Az viszont egyértelmű eredménye a fenti törvényben és kormányrendeletekben megfogalmazott szabályrendszernek, hogy a minősített adat védelmével összefüggő komplex védelmi intézkedések többé kevésbé koherensek lettek a nemzetközi szabályokkal, ennek okán az Európai Uniós és a NATO rendszereken belüli információáramlás (bizonyos szintig) egységessé és lehetővé vált!



***5*. ábra A biztonsági dimenziók és az információbiztonság kapcsolata.**

Az országos távközlő hálózat (OTH) felhasználása a védelmi feladatokkal öszefüggésben

Annak érdekében, hogy a rendszerben keletkezett kritikus információk kellően támogassák a döntési helyzetben lévő felelős vezetőket, az információ továbbítására alkalmas és képes nemzeti Országos kommunikációs távközlési hálózat magas szintű rendelkezésre állását kell biztosítani. Meg kell határozni a szükséges és elégséges szolgáltatás mértékét. Ennek előfeltétele a megfelelő szintű és tartalmú törvényi szabályozás, amely lehetővé teszi ezt a rendelkezésre állást a bonyolult nemzetközi tulajdonosi rendszer esetén is. Különösen fontos abban az esetben jól szabályozni ezt a területet, amikor például a védelmi szektor zártcélú vezeték nélküli kommunikációját biztosító rendszer szolgáltatója egy olyan egyetemes szolgáltató, amely külföldi tulajdonosi rendszerben üzleti alapokon szolgáltat. Ezt a részterületet hivatott szabályozni a Miniszterelnöki Hivatalt vezető miniszter 4/2010. (III. 26.) MeHVM rendelete a védelmi feladatokban részt vevő elektronikus hírközlési szolgáltatók kijelöléséről és felkészülési feladataik meghatározásáról.

Az elektronikus hírközlésről szóló 2003. évi C. törvény 182. § (4) bekezdés l) pontjában kapott felhatalmazás alapján a Miniszterelnöki Hivatalt vezető miniszter feladat- és hatásköréről szóló 29/2008. (II. 19.) Korm. rendelet 1. § j) pontjában meghatározott feladatkörében eljárva, a miniszterelnöki hivatalt vezető miniszter az alábbiakat rendelte el [12]:

Az elektronikus hírközlés szolgáltatási tevékenységének a minősített időszakban történő ellátásához szükséges védelmi felkészülési feladatok előkészítésében és végrehajtásában való részvételre kijelölt, valamint az informatikai és elektronikus hírközlési, továbbá postai ágazat (a továbbiakban: ágazat) ügyeleti rendszerébe bevont elektronikus hírközlési tevékenységet végző szervezetek (a továbbiak ban: szolgáltatók) felsorolását a rendelet 1. melléklete tartalmazza.

A riasztási és tájékoztatási feladat ellátásában részt vevő nem közszolgálati műsort sugárzó országos, körzeti, helyi rádió és televízióadók, az adókat üzemeltetők (engedélyesek) jegyzékét a rendelet 2. melléklete tartalmazza.

A kijelölés alapján a szolgáltatók a tevékenységi körüket érintően ellátják a minősített időszakban bekövetkező rendkívüli események megelőzésére, elhárítására, a következményeik csökkentésére, illetve megszüntetésére, valamint a helyreállításra irányuló védelmi felkészülési és végrehajtási feladatokat.

A rendelet alkalmazásában minősített időszak a Magyar Köztársaság Alkotmányáról szóló 1949. évi XX. törvény 19. §-a (3) bekezdésének h) pontjában meghatározott rendkívüli állapot és i) pontjában meghatározott szükségállapot, az Alkotmány 35. § (1) bekezdésének i) pontja és a polgári védelemről szóló 1996. évi XXXVII. törvény 2. § (2) bekezdése szerinti veszélyhelyzet, valamint az Alkotmány 19. § (3) bekezdés n) pontjában meghatározott megelőző védelmi helyzet, továbbá a 19/E. § (1) bekezdésében foglalt, a szükségállapot vagy a rendkívüli állapot kihirdetésére vonatkozó döntésig terjedő időszak.

Az elektronikus hírközlésért felelős miniszter (a továbbiakban: Miniszter), illetve a Nemzeti Hírközlési Hatóság (a továbbiakban: NHH) a védelmi felkészülés és a végrehajtás időszakában felmerülő egyedi védelmi feladatokat az érintett szolgáltatók számára külön jogszabály szerint határozza meg.

A védelmi felkészülési feladatok végrehajtásáért minden esetben a szolgáltató vezető tisztségviselője felelős.

A szolgáltatók – a minősített időszakra történő felkészülés keretében – az alábbiakban meghatározott tevékenységi körökből a saját szervezetük szakmai feladat- és hatáskörébe tartozó védelmi feladatokat látják el:

A szervezeti készenlét előkészítésének és fenntartásának körében:

- a védelmi felkészülési feladatok ellátásához szükséges személyi, szervezeti és anyagi-technikai feltételek megteremtése, folyamatos biztosítása,

A védelmi felkészüléssel, műszaki, forgalmi, katasztrófa vagy egyéb veszély miatt keletkező üzemzavar elhárításával kapcsolatos intézkedések kidolgozása, tervek készítése és azok folyamatos aktualizálása,

- a védelmi felkészüléssel összefüggő rendszeres képzési, továbbképzési és gyakoroltatási feladatok meghatározása és végrehajtása,
- az ügyeleti szolgálatnak a külön jogszabályban foglaltak szerinti működtetése,
- a külön jogszabály alapján a meghagyással kapcsolatos feladatok végrehajtása;

A hálózatok felkészítésének és irányításának terén:

- a gerinchálózati struktúra és az elektronikus hírközlési létesítmények védelmi, biztonsági feltételeinek biztosítása,
- a zártcélú hálózatokhoz szükséges összeköttetések és kapcsolódó szolgáltatások előkészítésének és alkalmazásának biztosítása,
- a meghatározó szerepű elektronikus hírközlési csomópontok, illetve felhasználók több útvonalon történő elérhetőségét segítő megoldások kialakítása,
- a riasztási és tájékoztatási feladat ellátására létrehozott rendszerben szükséges elektronikus hírközlési összeköttetések biztosításában való közreműködés,
- be) a honvédségi, kormányzati, rendvédelmi elektronikus hírközlési eszközöknek a szolgáltató hálózatához történő csatlakoztatásához szükséges hozzáférési pontok és jogosultságok biztosítása;

Az üzemviteli és tartalékolási rendszer kialakítása terén:

- a nemzeti és a nemzetközi gerinchálózati irányító és üzemviteli funkciók működésének összehangolása,
- az illetékes hazai, valamint nemzetközi szervek és szervezetek közötti védelmi jellegű kapcsolattartás feltételeinek kialakításában és végrehajtásában való közreműködés,
- az elektronikus hírközlési szolgáltatások területén elrendelhető korlátozó vagy szüneteltető rendelkezések végrehajtására és következményeik kezelésére történő felkészülés,
- a védelmi feladatok ellátásához szükséges mértékű és összetételű tartalékkészletek biztosítása,
- a hálózati létesítmények és eszközök meghibásodása, rongálódása, sérülése, megsemmisülése esetére az elsődleges helyreállításhoz és az üzemszerű állapot visszaállításához szükséges feladatok megtervezése és végrehajtási feltételeinek folyamatos biztosítása;

A szolgáltatási igények kielégítése terén:

- a védelmi felkészülésben részt vevő, külön jogszabályban meghatározott követelménytámasztó szervek minősített időszakra vonatkozó szolgáltatási igényei-

nek kielégítéséhez szükséges feltételek biztosítása, az összefüggő tervezési, szervezési tevékenység ellátása, szolgáltatási feladatok végrehajtása,

- a lakosság minősített időszaki elektronikus hírközlési igényeinek az egyetemes szolgáltatási, illetve koncessziós szerződésben meghatározott szinten és tartalommal történő kielégítéséhez szükséges feltételek biztosítása,
- a védelmi felkészüléssel kapcsolatos jogszabályok által meghatározott gazdasági és anyagi szolgáltatási kötelezettségek teljesítésére, illetve kezelésére való felkészülés,
- da kormányzat minősített időszaki szolgáltatási igényeinek kielégítéséhez és kommunikációs tevékenységéhez szükséges feltételek megteremtésében, fenntartásában való közreműködés,
- a Befogadó Nemzeti Támogatás tervezési és végrehajtási feladataiban történő részvétel;

A nyilvántartások vezetése és az adatkezelés terén:

- a védelmi felkészülési feladatokkal kapcsolatos jogszabályokban meghatározott adatszolgáltatási kötelezettség teljesítéséhez szükséges nyilvántartási rendszer kialakítása és adatainak a követelményekhez igazodó pontosságú karbantartása;

A műsorszórási tevékenység körében:

- a műsorszórási tevékenység folyamatosságához szükséges technikai és biztonsági feltételek megteremtése, a meghatározó szerepű létesítmények őrzésvédelmének biztosítása,
- a műsorszóró hálózaton a lakosság légi-, illetve katasztrófariasztásra és tájékoztatására létrehozott rendszer működésében való közreműködés,
- a lakosság légi-, illetve katasztrófariasztásának és tájékoztatásának elrendelésére illetékes szervek intézkedésére a riasztási és tájékoztatási közlemények leadásának – az elrendelő szervekkel kötött megállapodás szerinti, saját eszközökkel történő – biztosítása.

A riasztási és tájékoztatási feladat ellátásában külön jogszabály alapján – az illetékes honvédelmi és rendvédelmi szervek, valamint a közszolgálati rádió és televízió műsorszolgáltatók, műsorszóró adók és az adókat üzemeltető szolgáltatók mellett – részt vesznek:

- a Miniszter és az NHH;
- a rendelet 2. mellékletében meghatározott nem közszolgálati országos, körzeti és helyi rádió és televízió műsorokat sugárzó adók, az adókat üzemeltetők (engedélyesek);
- azok az elektronikus hírközlési szolgáltatók, amelyek összeköttetést, illetőleg modulációs vonalat biztosítanak
  - a riasztási és tájékoztatási közlemény leadását kezdeményező szerv és az érintett rádió, televízió stúdiója között,
  - a riasztási és tájékoztatási feladatban részt vevő stúdió és a részére sugárzást végző rádió, televízió adóállomás között, valamint
  - a műsorszolgáltatók és a műsorszóró adók között;

- a riasztási rendszer technikai elemeit, a riasztási és tájékoztatási közlemények átvételére és továbbítására szolgáló átkapcsoló berendezések fenntartását ellátó gazdálkodó szervezet;

Az európai unió létfontosságú infrastruktúrák figyelmeztető és információs hálózata (CIWIN)

Vezetés irányítási rendszerek alapvető megközelítése:

Az információbiztonsági stabilitást alapvetően befolyásoló OTH, magas szintű rendelkezésre állása és a minősített adatok védelmével összefüggő részterületeken túl, az alábbiakban célszerű megvizsgálni a globális, nemzetközi, nemzeti és regionális infokommunikációs rendszerekre épülő vezetés-irányítási rendszerekkel összefüggő alapvető ismereteket és követelményeket. Ennek nyomán célszerű áttekinteni - egy a kritikus infrastruktúra védelmével összefüggő- adattovábbítási értesítési és riasztási rendszerrel szembeni alapvető igényeket is. Különösen indokolt ez, annak fényében, hogy az összekapcsolódó (adott esetben globális) infrastruktúrákon keresztül – az incidens bekövetkezését követően- a működési zavarok felhalmozódnak, hatványozódnak az interdependencia jelenség miatt. Ebben a helyzetben indokolt egy nemzetközi (európai) adatok cseréjére alkalmas megosztott figyelmeztető és tájékoztató rendszer alkalmazása, amelynek segítségével a döntéshozók, az egységes és valós idejű adatok alapján rövid idő alatt a helyzettel összefüggő széleskörű adatszolgáltatás alapján képesek meghozni az optimális döntéseket. Az információs társadalomban alapvető igény fogalmazódik meg az infokommunikációs eszközökre épülő valós idejű globális döntés támogató rendszerek üzemeltetésére. Ezzel összefüggően megállapítható, hogy a kritikus infrastruktúra védelem területén is alapvető igény az információs fölény birtoklása, annak érdekében, hogy a fenyegetések előrejelzése, majd annak realizálódását követően a kár elhárítás és a működőképesség helyreállításának időszakában is optimális szinten tartható legyen a szükséges és elégséges szintű védelmi intézkedések alkalmazása.

A CIVIN kezdeményezés bemutatása:

A CIWIN létrehozására irányuló kezdeményezések már 2006 decemberére nyúlnak vissza. A létfontosságú infrastruktúra védelem Európai Programja (EPCIP) javaslatok célkitűzések értelmében fogalmazódott meg egy az infrastruktúra védelemmel összefüggő, biztonságos információcserére alkalmas eljárás kidolgozása. Ez a kezdeti lépés alapozta meg egy tagállamok közötti kölcsönös tájékoztató rendszer létrejöttét, illetve fogalmazta meg annak igényét. Erről az Európai Bizottság határozatban is gondoskodott ugyan, de a tagállamok CIWIN- hez történő csatlakozása nem kötelező. Ugyanakkor az EPCIP-vel kapcsolatos irányelveknek megfelelően a tagállamoknak az Európai Bizottság részéről rendelkezésre bocsátott információkat hozzáférhetővé kell tenniük a kijelölt ágazatok részére. A tagállamoknak viszont a saját területéről gyűjtenie kell az adatokat az európai létfontosságú infrastruktúrákról, a sebezhetőségi és függőségi pontjairól, a védelmi fejlesztésekről és ezt elérhetővé kell tenni az EU részére.

A CIWIN (szerver / kliens) rendszer funkcionalitását illetően, a Bizottság és a tagállamok közötti viszonylatban alkalmasnak kell lennie a két vagy többoldalú

információ megosztásra, illetve gyors riasztási funkció megvalósítására. A bizottsági felületen az ágazati területek jelennek meg. A rendszer kötött és dinamikus területi adatkezelésre egyaránt alkalmas.

A kötött területen jelennek meg a tagállami, szektor, vezetői, külső együttműködési területek és egy gyors információcserét biztosító RAS alrendszer.

Egy speciális esemény, vagy tagállami projektek, szakértői munkacsoport terület részésze, igény szerint dinamikus területek hozhatók létre.

Az elrendelt figyelmeztetés esetén lehetőség van egy ideiglenes RAS terület létrehozására, amely az együttműködés színtere az adott projektre vonatkozóan.

A kritikus infrastruktúra védelmével összefüggő és rejtelzéssel védeni rendelt, minősített információk megosztására speciális terület áll rendelkezésre azok számára, akik a „muszáj tudni" elv alapján azokhoz jogosultak hozzáférni.

A CIWIN rendszer (MS SharePoint 2007), piaci alkalmazásra épül és beépített, minden nyelvre automatikus fordítóprogramot, illetve „off the shelf" tartalomkezelőt használ. Funkcióit illetően megtalálhatóak benne a vitafórum, kalendárium, és a személyes belső levelező funkciók is.

A TESTA rendszeren történő elérést megelőzően, minősített információk továbbítására nem alkalmas. Az elérést követően korlátozott terjesztésű minősített adatok továbbítására alkalmas, de közép távon -sTESTA hálózaton- Bizalmas minősítésű információk megosztására lesz alkalmas.

A TESTA (Trans European Services for Telematics between Administrations) egy független zártcélú (publikus hálózatoktól független) gerinchálózat, amely az Európai Unió adminisztrációja és a tagállamok közötti kommunikációs hálózat. A TESTA rendszer, információvédelmi szempontból továbbfejlesztett változata az sTESTA, amely már megfelelő egyenszilárdságú rejtjelző eszközöket és algoritmusokat használ. A tagállamok részére a CIWIN rendszerre történő csatlakozás opcionális, azonban a rendszerhez csatlakozó tagállamoknak a minősített adatkezeléssel összefüggő kötelezettség alapján az elektronikai, dokumentum, személyi és fizikai védelmi követelményeknek meg kell felelni. Az előzőekben már kifejtett EU minősített adatvédelmi követelményekkel koherens szabályozási rendszer, különösen ezen a területen nyit új távlatokat, melyeket az Európai Bizottság, a tagállamokkal kötött többoldalú szerződésekkel is megalapozott.

Az elérést követően korlátozott terjesztésű minősített adatok továbbítására alkalmas, de közép távon Bizalmas minősítésű információk megosztására lesz alkalmas.

Információvédelmi kérdések:

Az Európai Bizottság által kiadott irányelv 9. cikkelyében megfogalmazottaknak megfelelően., a minősített információt kezelő személyeknek, személyi biztonsági tanúsítvánnyal kell rendelkezniük. Ennek előfeltétele a megfelelő szintű nemzetbiztonsági átvizsgálást követő kockázatmentesség megállapítása. A tagállamoknak, a Bizottságnak és az illetékes felügyeleti szerveknek (ez hazánkban a Nemzeti Biztonsági Felügyelet) biztosítaniuk kell, hogy a minősítet információkhoz a létfontosságú infrastruktúrák védelme céljából jussanak hozzá, az arra jogosult személyek. Ezzel összefüggésben elengedhetetlen a nemzeti és nemzetközi jog harmonizációja (ez meg is történt) valamint az egységes jogértelmezésen alapuló

jogkövető magatartás érvényesítése. Az egyes tagállamoknak és a bizottságnak egyaránt tiszteletben kell tartania a minősített adat minősítője által megállapított minősítési szintet.

A CIWIN rendszer információs funkciója biztosítja, hogy az adathoz való hozzáférés alapja a már említett"tudnia kell" elv alkalmazása. A rendszeren belül az információ birtokosa dönti el azt, hogy ki és milyen biztonsági szinten férhet hozzá az adathoz. A tagállamok jogosultsága és felelőssége az, hogy tagállamon belül hogyan szabályozzák a hozzáférést az adathoz. Természetesen itt vissza kell utalni a koherens EU és nemzeti szabályokra, melynek rendelkezéseit maradéktalanul be kell tartani. A tagállamnak minden alkalommal ki kell jelölnie egy arra jogosult vezetőt, aki a jogosultságokat illetően dönteni tud. Ez az egyszemélyi vezető jogosult ezeket a jogokat – korlátozott mértékben- a tagállam más tisztségviselőjére delegálni. A szabályoknak megfelelő szintű személyi biztonsági tanúsítványokkal a kezelőknek és felhasználóknak egyaránt rendelkezniük kell.

Hazai rendszerek együttműködése a CIWIN rendszerrel:

A nemzeti KIV hatókörében, az irányadó szakemberek szerint nem szükséges külön riasztási és értesítési rendszereket létrehozni. Azt azonban célszerű elemezni, hogy a jelenleg működő riasztási és értesítési rendszerek, hogyan tudják támogatni a nemzeti KIV-ben érintett szektorok és az állami szektor döntésképes vezetőit. Ha a vizsgálat eredménye ként erre a jelenlegi rendszerek nem alkalmasak, akkor (és csak is akkor) szükséges új, különálló rendszerek fejlesztésében gondolkodni. Ugyanakkor védelmi vezetéstechnikai rendszerszervezési szempontokat figyelembe véve, nem indokolt sok sziget rendszerű riasztási rendszert üzemeltetni. Célszerű a jövőben megvizsgálni annak a lehetőségét is, hogy a meglévő nemzeti rendszereket (Marathon Terra; K-600/KTIR) illetve azok bizonyos adatbázisait (amelyek nem sértenek nemzeti érdekeket) egy funkcionális interfészen keresztül, hogyan lehet elérhetővé tenni a CIWIN számára, egységes és redundáns platformra helyezve ezzel a nemzeti és európai KIV figyelmeztető és információs rendszereit.

Összefoglalás

A biztonság újkori értelmezéséből kiindulva - elfogadva azt, hogy a dimenziók átalakultak és némely dimenziók felértékelődtek – megállapítható, hogy az információs társadalom kritikus infrastruktúrának és ezen belül a kritikus információs infrastruktúra védelmével összefüggő kérdések a biztonsági stratégiába épülő és annak szerves részét képező elemei. Megállapítható, hogy a társadalom zavartalan működésén túl, a katasztrófa helyzetben és a különböző minősített időszaki helyzetekben súlyponti kérdés a kritikus információs infrastruktúrák rendelkezésre állása. Az mára bizonyított tény, hogy az információk gyors, hiteles és változatlan formában történő áramlása alapvetően befolyásolja a védelmi intézkedések hatékonyságát. A fentiekből azt a végkövetkeztetést lehet levonni, hogy ezen a területen is fontos az információs fölény elérése.

A külföldi és hazai jogi és technológiai környezetet elemezve az a végkövetkeztetés vonható le, hogy a hazai szabályozás – a hazai doktrínák rendszerét vizsgálva – ugyan igyekszik követni az európai folyamatokat, de különösen technológiai területen az útkeresés fázisában lévő folyamat érzékelhető. A felhasználók igénye az információs rendszerek használatával kapcsolatban nagyon határozott és

jól érzékelhető, de különösen az érzékeny, vagy minősített adatok gyors, hiteles és változatlan továbbítására alkalmas hazai rendszerek kialakítása még várat magára. Ezen a területen több párhuzamos fejlesztési folyamat érzékelhető. Ezért is különösen fontos annak a problémának a feloldása, hogy a hazai és nemzetközi értesítési rendszerek egységes platformon és egységes elvek alapján képesek legyenek a hatékony együttműködésre. A fentieket összefoglalva, irányadó szakemberek szerint az információs társadalom zavartalan működését veszélyeztető fenyegetésekkel szembeni védelmi intézkedések foganatosítása az információs dimenzióban, meghatározó szerepet töltenek be.

Irodalom

[1] Egyesült Nemzetek Nevelésügyi és Kulturális Szervezete (UNESCO) társadalomtudományi szótár

[2] Amerikai nemzetbiztonság c. könyv (1981)

[3] A Magyar Köztársaság nemzeti Biztonsági Stratégiájáról szóló 2073/2004.(IV.15) korm. határozat.

[4] Kőszegvári Tibor: A hadtudomány mai problémái, területei és új fogalma (Hadtudomány, Magyar Hadtudományi Társaság, Budapest XVII. évfolyam 2007/1. szám) 13. oldal

[5] Farkasné dr. Zádeczky Ibolya: A biztonságot veszélyeztető globális kihívások (Hadtudomány, MHTT. Budapest XVI. évfolyam 3. szám, 2006. szeptember) 41. oldal.

[6] Wörterbch zur sicherheitspolitik, Mitter Kiadó, 1985. 113. o.

[7] Szabó József::Hadtudományi Lexikon, Magyar Hadtudományi Társaság, 1995. 144. o.

[8] Muha Lajos A Magyar Köztársaság Kritikus Információs Infrastruktúráinak védelme doktori (Phd) értekezés 2007.

[9] A minősített adat védelméről szóló 2009. évi CLV. Törvény

[10] A Nemzeti Biztonsági felügyelet működésének, valamint a minősítet adat kezelésének rendjéről szóló 90/2010.(III.26.) Kormányrendelet

[11] A minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010.(V.6.) Kormányrendelet

[12] Az elektronikus hírközlésről szóló 2003. évi C. törvény

KORONCZAI Tibor - SÁNDOR Miklós

NATO COMMUNICATIONS AND INFORMATION SYSTEMS

Abstract

This work gives an overview of the Communications and Information Systems (CIS) of the North Atlantic Treaty Organization. It focuses on the structure, history and the main missions of the different elements of the system, however, due to several limiting factors, I intend to concentrate on the most important NATO organisations and agencies that are responsible for the provison of the communications and information systems. The CIS support that is being provided for the present NATO missions and the way ahead for the Alliance are out of the scope of this work.

Introduction

With the dissolution of the Warsaw Pact and the fall of the Soviet Union, the international security environment had changed. Former enemies turned into allies and new security challenges appeared. NATO needed to adjust its policy in order to meet the new requirements posed by the then security challenges. The Alliance had to transform its mission, both its military and political structure and its procedures as well. The new security challenges necessitated to rethink and reorganise the communications and informations system of NATO. No sooner had the Berlin Wall fallen, when the Alliance started to reorganise its CIS structure and assets.

1. NATO C3 Organisation and the NATO Consultation, Command and Control Board

Consultation, Command and Control matters are known within NATO under the collective name of "C3". The NATO Consultation, Command and Control Organisation (NC3O) is responsible for the provision of a NATO-wide, cost-effective, interoperable and secure capability to ensure high level political consultation and command and control of military forces. This is accomplished by a number of Communications and Information Systems (CIS) which also interface with national fixed and mobile networks to cover the whole NATO area, linking the NATO Headquarters in Brussels, all Headquarters of the Integrated Military Command Structure, national capitals and the highest levels of national military command.

The NC3O was created in 1996 to ensure the provision of a NATO-wide cost-effective, interoperable and secure C3 capability, meeting the NATO users' requirements by making use of common funded, multinational and national assets. The NC3O also ensures the provision of services and support in the field of C3 to NATO users. The NATO Consultation, Command and Control Board (NATO C3 Board or NC3B) oversees the NC3O.

The Board is the senior multinational policy body, advising the Council and the Defence Planning Committee on collective interests of all the member states acting as the Board of Directors of the NC3O. It is composed of senior national

representatives from each member states; representatives of the Military Committee and Strategic Commanders and NATO committees with an interest in C3, the General Manager of the NATO C3 Agency (NC3A), and the Controller of the NATO CIS Operating and Support Agency (NACOSA). The Board is chaired by the Deputy Secretary General and has a Permanent Chairman (the Assistant Secretary General for Defence Support) and two Co-Vice Chairmen (Director NHQC3S and a Co-Vice Chairman elected from national nominees). It is assisted by the Group of National C3 Representatives (NC3REPS), which acts as the NC3B in permanent session. These National C3 Representatives are normally attached to their national delegations or to their military representatives at NATO.

The NC3B is supported by a NATO C3 Subordinate Structure of multinational bodies composed of eight sub-Committees (Joint C3 Requirements and Concepts, Interoperability, Frequency Management, Information Systems, Information Security Systems, Communications Network, Identification and Navigation). Each of these has its own substructure. The NC3B, NC3REPS and the NC3B Substructure is supported by the NATO Headquarters C3 Staff (NHQC3S), a single integrated civilian and military staff directed by the Assistant Secretary General for Defence Support, IS and the Director of the IMS. The NHQC3S provides support to the Council, Military Committee, CNAD, SRB and other NATO committees on C3 matters.

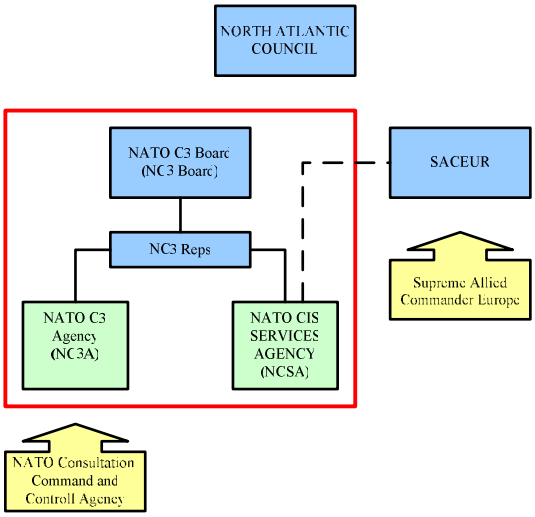


Figure 1

The Board also oversees the work of the two NC3O agencies, the NC3A and NACOSA. The NC3A performs central planning, system integration design, system engineering, technical support and configuration control. It also provides scientific and technical advice and support in the field of C3 sensor systems and operational research, and procures and implements projects assigned to it. The NC3A is located in Brussels, Belgium and in The Hague, the Netherlands. NACOSA exercises operating control and supports the in-service NATO CIS and installations assigned to it. The NACOSA central staff is located in Mons, Belgi-

um. Figure 1. shows the layout of the NATO C3 Organisation and the elements it contains and their subordination.

2. NATO Communication and Information Systems Services Agency

The NATO Communication and Information Systems Services Agency, (NCSA), is a service provider to its NATO and national customers. Wherever NATO deploys on operations or exercises, NCSA is there, providing communication and information systems (CIS) services in support of the mission. Equally important, NCSA supports NATO's ten major headquarters in Europe, North America, and Asia.

2.1. History

The NATO Communication and Information Systems Services Agency (NCSA) has had a long gestation which began in the 1970's and metamorphosed into various NATO organisations along the way.

The first identifiable communications and information distribution organisation was called the NATO Integrated Communications Systems Central Operating Authority (NICS-COA) and was established to control, operate and maintain the NATO Communication systems of that time. The main elements of these systems were the Initial Voice Switched Network (IVSN), Telegraph Automated Relay Equipment (TARE), Status Control Alerting and Reporting System (SCARS), SATCOM systems and equipments and the ACE High Tropospheric Scatter trunk communication network. By the early 1990's due mainly to the arrival of new systems and new technology it became necessary to reorganize the Communication and Information systems support for NATO. This coincided with a major restructuring of the NATO Command to take advantage of the "peace dividend" after the fall of the Berlin Wall. In 1993 the NATO Communication and Information Systems Operating and Support Agency (NACOSA) was formed by the integration of functions previously undertaken by NICS-COA and some elements of the Communications and Information Systems Division of the Supreme Headquarters Allied Powers Europe (SHAPE CISD). Over time it became apparent that there was still a need for establishments to streamline their operations to improve management and control and also to make a manpower saving of some 25% so NACOSA also took command of 4 subordinate elements. These were the Integrated System Support Centre (ISSC), Allied Command Europe Communications Security (ACE Comsec) (which later became INFOSEC Command NACOSA), The NATO Communication and Information Systems School (NCISS) at Latina, Italy and the Regional Signal Group SHAPE. In the following years, NACOSA developed into an organization with responsibilities for the operation and support of communication and information systems on both sides of the Atlantic and for all NATO Operational deployments.

In 1997 due mainly to the arrival of new systems and technology, but also as a result of lessons learned in areas like the Balkan Operations, the expansion of NATO, the introduction of Partners for Peace, and the NATO Long Term Study, NACOSA was reorganized once more. An additional result of this reorganization was to bring the previously named Regional Operating Centre Northwood (UK) under direct control as a subordinate element to be known as The NACOSA

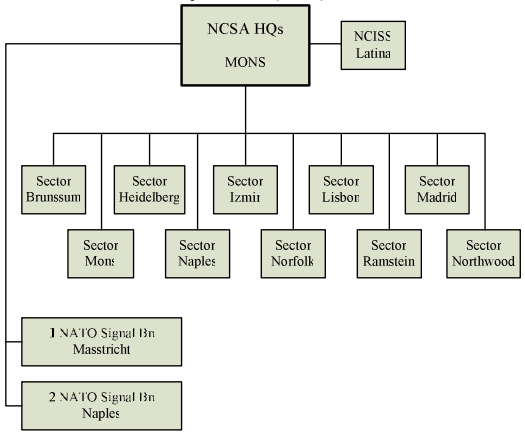
Support Element (NSE) Northwood. The Charter for NACOSA at that time was redefined and signed by the NATO Consultation Command and Control Board (NC3 Board) in December 1997. This Charter persisted until October 2003, when, after a comprehensive study, the North Atlantic Council was moved to endorse the following recommendations: - All of NATO‘s fragmented CIS service provision elements will be integrated into one centralised organisation, separating ‘customers‘ from ‘suppliers‘. - All deployable CIS capabilities will be combined in two NATO Signal battalions and become part of NCSA. - The new organisation will be an agency and remain under non-operational direction of the NC3 Board. The Director NCSA should be accountable to the NC3 Board for executing the Agency's general policy decisions, directives and strategy, and for the provision of CIS services to all its "customers".

Under these guidelines the NCSA was designed and it formally took over responsibility from the decommissioned NACOSA on 1 August 2004. At the same time NATO's new Command Structure was implemented, cutting approximately 12% of NATO's overall manpower. The transition period is assumed to last about 18 months, i.e. until mid-2006.

A formal NCSA Activation Ceremony took place at SHAPE on 7 September 2004. Acting on behalf of the Secretary General, the Presiding Officer was the then Deputy Supreme Allied Commander Europe, Admiral Rainer Feist.

2.2. The Organisation

NCSA comprises a central headquarters staff co-located with Allied Command Operations at the Supreme Headquarters Allied Powers Europe (SHAPE) in Mons, Belgium; two deployable NATO Signal Battalions, each with four deployable communication modules, comparable in size and mandate to signals companies; ten Sectors that support the 10 major headquarters in NATO; and the NATO Communication and Information Systems (CIS) School in Latina, Italy.



NCSA Structure

NCSA Headquarters

The staff at the headquarters coordinates the work of the Agency by working closely with the political authorities of NATO in Brussels and with various bodies within NATO's military command structure. The staff also provides strategic advice whenever needed to ensure the efficient and effective use of NATO's CIS resources. The Agency's centralised budget and human resources functions are also located in the headquarters.

NCSA Sectors

The Sectors' principal task is to install, operate, maintain and support the communication and information systems of their affiliated headquarters during peacetime and crisis.

NATO Signal Battalions

NCSA operates two NATO Signal Battalions. Each is responsible for providing communication and information systems facilities for deployed headquarters. The battalions connect the supported headquarters to available communication systems, and also connect to suitable transmission media such as very-high frequency (VHF) microwave links or satellite communication links. Each battalion also provides supply services and maintenance services to the field wherever that field may be.

NATO Communication and Information Systems School

NCSA also operates the NATO Communication and Information Systems School. It provides from basic to advanced level training for its military and civilian students so they can operate and maintain NATO's CIS systems. The school conducts over 50 courses ranging from one to 10 weeks' duration.

2.3. The main mission

The Agency's tasks fall into four major areas in order of priority:

1. Support to NATO operations:

- Providing secure computer network, telephone, and videoconference services to the NATO Response Force, the International Security Assistance Force in Afghanistan (ISAF), the NATO Training Mission in Iraq, and NATO operations in the Balkans.
- Providing NATO's first line of defence against cyber threats such as detecting and preventing computer viruses and unauthorized intrusion into NATO's networks.
- Operating, maintaining, controlling and administering the central components of NATO's networks, providing coverage of mission essential systems 24 hours a day, 7 days a week.
- Providing logistics support for the deployed CIS assigned to NCSA, working closely with the NATO Maintenance and Supply Agency (NAMSA) and the NATO C3 Agency.

2. Support to NATO exercises:

Providing deployable communication systems and CIS support to NATO exercises that are used to develop, maintain or accredit the effectiveness of operational elements within NATO, the NATO Response Force (NRF) being one example.

3. Support to NATO's major headquarters:

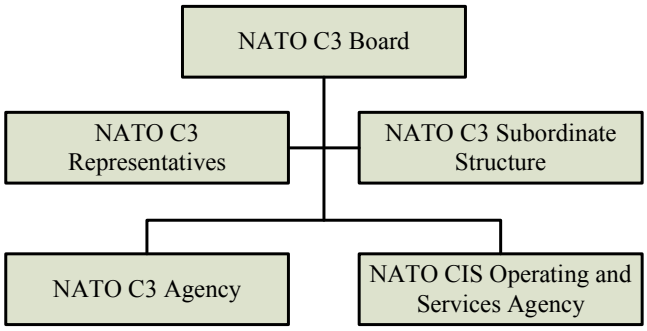
- Providing strategic and policy advice to headquarters' leadership to ensure the efficient and effective use of CIS resources.

Providing secure and non-secure computer, telephone and video conference services to NATO's static headquarters in Europe, North America, and Asia.

4. Support for new CIS systems and projects:

- Ensuring the compatibility of new CIS hardware and software on NATO's networks.
- Providing technical advice; installing computers, telephone and video conference equipment; conducting hardware and software maintenance; configuring and controlling networks; and training for personnel on NATO communication and information systems.

3. NATO Consultation, Command and Control Agency (NC3A)



The NC3A operates across the spectrum of the C4ISR life cycle, acting as a catalyst, a facilitator, a coherence agent and a delivery agent for many NATO systems and capabilities. For the Agency, the capability process begins with helping Allied Command Transformation (ACT), in conjunction with Allied Command Operations (ACO), identify and articulate coherent and long-term capability requirements.

Through the vehicles of NATO's capability packages and national force requirements and proposals, NC3A helps the Alliance focus its common-funded programmes, together with nationally-funded initiatives, into a common coalition-based force. As NATO's designated C3 Architect, we work closely with national agencies and industry to ensure that the Alliance gains maximum synergy from this process. The end goal is to deliver those viable forces that ACO needs to execute the missions and tasks given to it by the North Atlantic Council.

Our areas of expertise, or core competencies, are organized into nine capability area teams:

- Capability Planning and Architectures
- Interoperability
- Exercises and Training
- Operations Planning and Execution (J3/J5)
- Intelligence, Surveillance and Reconnaissance
- Integration Support and VAS
- Core Services
- Information Assurance and Service Control
- Infrastructure Services

3.1. Organisation

The NATO C3 Agency was established on 1 July 1996 by the amalgamation of the former SHAPE Technical Centre (STC) and the former NATO Communications and Information Systems Agency (NACISA). Both of these organizations take their roots from the origin of NATO and from the requirement to provide Consultation, Command and Control capabilities to NATO authorities. The Agency has therefore been at the centre of C3 matters in NATO for 50 years.

The NC3A is officially founded under the Charter for the NATO C3 Organization, an entity comprised of a governing body, the NATO C3 Board; a supporting substructure including the NATO C3 Representatives, and two agencies — the NATO C3 Agency and the NATO Communication and Information Systems Services Agency (NCSA).

The roles given to the NC3A under the charter are diverse and include:

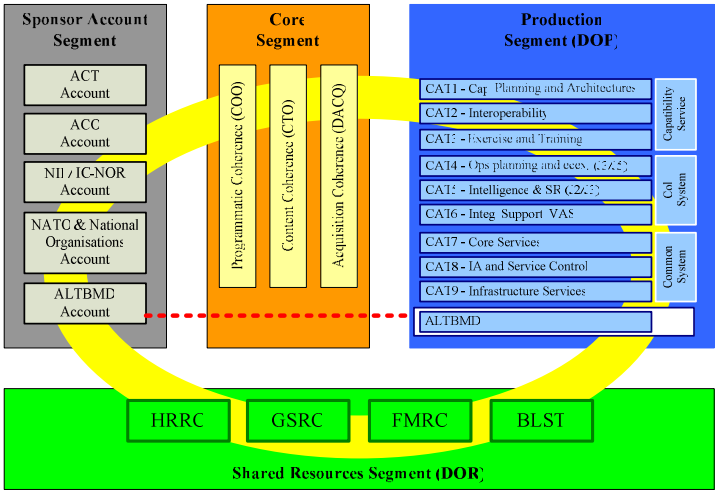
- Central planning, systems integration, design, systems engineering, technical support and configuration control for NATO C3 systems and installations
- Scientific and technical support to the Strategic Commands
- Technical support and advice in the areas of operations research, surveillance, air command and control including theatre missile defence, electronic warfare, airborne early warning and control, and communications and information systems
- Immediate support to NATO military authorities during military operations
- Technical policy and standardization work for the NATO C3 Board and its substructure

The Agency's structure is based on four segments:

- **The Sponsor Account Segment** – the interface to our sponsors, where we develop new business and manage the customer accounts, and where our sponsors find their single and dedicated interface point. The customer accounts are:
  - Allied Command Transformation (ACT)
  - Allied Command Operations (ACO)
  - NATO Network-Enabled Capability Implementation Programmes
  - NATO and Partner Nations and NATO structures
  - NATO Consultation Command and Control Board

- Active Layered Theatre Ballistic Missile Defence Programme Office

- **The Production Segment** – where the projects are executed; The segment consists of nine Capability Area Teams (CATs) under a Director of Production:
  - CAT1 – Capability planning and architectures
  - CAT2 – Interoperability
  - CAT3 – Exercises and training
  - CAT4 – Operations planning and execution
  - CAT5 – Intelligence, surveillance and reconnaissance
  - CAT6 – Integration support and value added services
  - CAT7 – Core enterprise services
  - CAT8 – Information assurance and service control
  - CAT9 – Network Information Infrastructure (NII) communications infrastructure services
- **The Core Segment** – which is responsible for ensuring that the Agency's work is coherent in terms of its internal business processes, technical and architectural solutions, and acquisition processes. This consists of a Chief Operating Officer, Chief Technology officer, supported by Chief Architects and Scientists, and the Director of Acquisition.
- **The Shared Resources Segment** – where Agency-wide shared support services, such as human resources, building maintenance, stores, finance and IT services are delivered;



Agency Structure

Summary

NATO's C3 structure has been developed and improved in order to be able to provide more flexible and reliable support for the Alliance. In the last two decades a lot of efforts have been put into the transformation and reorganisation of the C3 system which needs thorough monitoring and if needed, it has to be taylored to the new requirements.

Krisztina KÖRMENDI - Miklós SÁNDOR

THE POSSIBILITY OF COMMUNICATION DURING ELECTRICITY OUTAGES

Introduction

The electricity supply is one of the basic needs of the modern society. The sufficient electricity supply is indispensable for the proper functioning of several areas of the society and the economy. Many previous cases prove that the disturbances of the electricity supply system could have serious impacts to the operation of other critical infrastructures and the availability of basic supplies (like communication, drinking water supply, sewage treatment, transportation etc.).

In this paper we search for the answer to the following questions: how an electricity outage affects the communication infrastructure, do the communication system remains operable and what possibilities remain available

- to provide information to the public
- for the communication among people
- for the communication among the electricity-industry organization
- for the communication among the emergency management bodies

The concept of electricity-crisis and the basic principles of its management

The impact made by an electricity outage to the communication infrastructure depends on the size of the affected area and the duration of the outage. The cause of the outage can be an operational break-down or the enforced restriction on consumers made by the system operator in order to maintain the balance of the electricity power system and to prevent that the problem become worse.

The concept of the electricity-crisis is determined by the No. 285/2007 Order of the Government [1] about the heavy disturbance of the electricity power system and the actions required in case of electricity emergency (henceforward: Electricity Crisis Order). The Electricity Crisis Order determines the following concepts:

- heavy disturbance of the electricity power system (henceforward: heavy disturbance),
- impending electricity emergency,
- (state of) electricity emergency

together called as “electricity crisis” (henceforward: crisis).

According to the 138. § (1) and 139. § (1) of the Electricity Act (Act No. LXXXVI. in 2007) [2] together with the 16. § (1), 17. § (1) and 18. § (1) of the Electricity Crisis Order the „heavy disturbance” is a serious failure in the electricity system, because of which the generation, transmission, distribution, service or consumption of electricity become limited or cease or rather the operation safety, controllability, interoperability of the electricity system become endangered. If the disturbance directly threatens the persons, the assets, the nature, the environment or the electricity supply of the significant proportion of consumers it is rated as electricity emergency. The state of electricity emergency according to the Electricity

Act does not reach the level of other state of emergencies defined by other laws[74]. [3]

A state of electricity emergency can evolve because of the prolonged outage of electricity generation or import or the prolonged outage of primary fuels. In order to prepare for these cases, the Electricity Crisis Order brings in the concept of „impending electricity emergency". The impending electricity emergency has two phases, which are determined by the volume of the reserve power of the electricity system and the volume of the primary fuel stocks available nationwide[75]. [3]

Besides the above, a state of electricity emergency can be evolve because of an environmental pollution or the shutdown of power-lines, which causes outages lasting several days in the electricity supply of the country or the parts of the country, or because of the supply disruptions of the consumers or if heavy disturbances occur in the electricity system more than 3 times in 30 days.

According to the Electricity Crises Order in the management of an electricity crisis participate:

- all electricity-industry licensees (organizations doing permission required activities according to the Electricity Act),
- the following administrative bodies: Ministry of Economy and Transportation, Ministry of Environmental Protection and Water, Hungarian Energy Office, Directorate General of National Disaster Management and Governmental Coordination Committee,
- the Government. [3]

The prevention of heavy disturbances and the management of response are the responsibility of the Transmission System Operator such as the management of response during impending electricity emergencies. During state of electricity emergency the management of response is the responsibility of the Government. [3]

The Electricity Crisis Order brings in the concept of the „essential consumers" and „vital consumers". The Order prescribes that in case of an electricity crisis the electricity supply of these consumers should be maintained as long as possible and the restoration of the supply of these consumers has priority. According to the 1st annex of the Order the operators of equipments needed to the main communication services – except that have power generation possibilities independent of the grid – are vital consumers.

The protection of the vital consumers appears in the so called „rotational restriction order" (henceforward: RKR[76]). The Electricity Crisis Order prescribes that during an electricity crisis the system operator can apply enforced restrictions on

[74] Different types of „state of emergency" are defined by the 19.§ (3) i) section of the Constitution of the Hungarian Republic (Act No. XX. in 1949) and the 2.§ (2) section of the Civilian Defence Act (Act. No. XXXVII. in 1996.)

[75] The phase I. is when the reserve power decreases to 10% and/or the fuel stock available nationwide decreases so that the electricity supply of the country may became endangered in 3 days. The phase II. is when the reserve power decreases to 7% and/or the fuel stock available nationwide decreases so that the electricity supply of the country may became endangered in 2 days.

[76] The abbreviation comes from the Hungarian name: Rotációs Kikapcsolási Rend

consumers in order to maintain the balance of the power system and to avoid the collapse of the system, if the crisis could not be avoided by other measures. If the foreseeable duration of the restrictions exceed 6 hours, the system operator should apply the RKR.

In the RKR the national consumption load are geographically divided into 18 approximately equal sized groups. The restriction is executed in rotation among the groups in such way that the duration of the restriction of a group does not exceed 3 hours. There are two version of the RKR, the „blue RKR" does not contains the consumption of the vital consumers, so these consumers will not be switched off during the execution of the restriction. The other version, the „red RKR" contains the vital consumers eke. But the „red RKR" only executed in such cases, when the necessary consumption could not be restricted by the half of the consumption contained by the „blue RKR". [4]

It should be noted that large scale break-downs are rare, in regard that generally the failures in the power system occur locally and are eliminated automatically. The escalation of the local problems leads to system break-downs, but there are several protection measures to interfere that. They use Defence Plans to prevent the collapse of the power system and the Restoration Plan to recover the system after a blackout. [5] [6]

Based on the above we can assume, that during a potential electricity crisis the power supply of the equipments of the communication infrastructure do not be restricted, if it is not necessary. Even if it is, the restriction do not exceed 3 hours expectedly. Of course the power supply of the equipments can break because of the disturbance of the power system and in serious cases – like blackouts - the restoration of the supply may take hours or days, such as occurs in August 2003 in North America.

The experiences of the blackout in North America occurred in August 2003 related to the communication systems

In August 2003 due to the collapse of the power system a serious power outage occurs in the north-eastern and midwestern states of the United States and Ontario, Canada. Several cities were affected such as New York, Detroit, Cleveland, Connecticut, New Jersey, Michigan (USA), Ottawa, Toronto, Montreal, Quebec (Canada). Approximately 50 million residents remained without power. While the cascading blackout passed off during minutes, the restoration of the power systems took more than a week. [7]

During the blackout the essential services remain more or less operable due to backup generation. The phone system and the television and radio stations remain operable in most of the affected areas, but there were significant service disruptions in the cellular phone systems. The increased volume of traffic was also a challenge to the telephone and cellular phone systems.[8]

As the battery-powered transistor radios had been replaced by portable CD players and other devices, which did not work during the blackout the possibilities to provide information to the public was difficult. The cable television system did not worked, such as the personnel computers and internet connections were not

available either. The internet news sites were available only with the dialup connections from laptops, until the batteries ran out of charge. [8]

Due to the impact of the long lasting and wide spread black out in some states, for example in Michigan, „state of emergency" was declared. In the following, based on the report [9] made by the Michigan Public Service Commission, the impacts of the blackout to the communication system in Michigan will be introduced.

In the State of Michigan 6 million residents remained without power for 2 days. The local telephone system, which has 3 million customers, remained operational, even though the volume of calls increased to 149%. Only 50.000 consumers remained without telephone service for slightly more than an hour. The operator company of the phone system provided the power supply of their equipments and offices with stand-by generators and batteries for an average of 28 hours. [9]

The operator company had two large trailer-mounted generators and many smaller portable generators and borrowed two additional larger generators from a local manufacturer. The batteries at the remote terminals had to be periodically recharged, so the technicians of the operator company moved portable generator to each of the terminals one after other and recharged the batteries. [9]

Beside the fuel resupplies of the generators they had to provide the fuel needed for the company vehicles. The fuel demand increased very strong because many government offices and private entities were operating their generators and competing for limited fuel supply. Some fuel suppliers and distributors – who did not have backup generators - could not provide supply without power. The so called State Emergency Operation Center (SEOC) helped the phone system operation company locating supplemental fuel supplies. The company bought at about 320.000 gallons of fuels for almost 650.000 dollar. [9]

There were no problems reported by the long distance phone companies, because their services depended on the operation of the local phone system. Many companies had business continuity plans and were able to continue operation. [9]

At the cellular phone system there were service interruptions for a time. The cell phone companies also had to operate stand-by generators but the power was restored before the fuel resupply for the generators became a problem. [9]

The communication between State and local agencies worked very well due to the Michigan Public Safety Communication System which is a state wide 800 MHz digital trunked radio system established by the State of Michigan. The control centre and the antennae of the system had independent generators, so they remained fully operational during the blackout. The system was used by 374 public agencies for their primary radio communication and 90 agencies for emergency management purposes only. There were more than 11.000 radios on the system. [9]

The needs for communication during electricity crisis and the tools of communication

The management of a potential electricity crisis requires the aligned work of several organizations.

1. The transmission system operator keeps contact and directs electricity-industry organizations.
2. The transmission system operator has to provide information on the evolving of the situation and on the enforced restrictions on consumers to the responsible minister, the Hungarian Energy Office and the Directorate General of National Disaster Management.
3. The transmission system operator – or in state of electricity emergency the Government – have to provide information to the public on the evolving situation, the actions and measures taken and may call the public to voluntary electricity conservation.

If the situation worsens, because of the interdependencies of critical infrastructures or the occurrence of another events may made necessary the response of the disaster management and civilian defence bodies. In this case the communication between these organizations should be provided also.

Providing information to the public and the communication between the people

The people communicate each other by phone, cell phone or the internet on public communication systems. These systems can be the tool for providing information to the public too. If an electricity crisis occurs – beside the service disruption caused by the power outages – the communication system operators have to face with that the systems may become overloaded due to the increasing demand.

In a state of emergency or state of disaster providing warnings, information and alerts to the public is the task of civilian defence. In Hungary alerts can be provided with sirens, megaphones or via the media. There are problems with the efficiency of both three ways of alerting. For example the electric sirens do not work during electricity outages, the people do not know the siren signs, the audibility of sirens and megaphones are affected by the ambient noise, weather conditions (e.g. the direction and intensity of wind) or it may depends on where are the people staying (e.g. sound-proof rooms etc.). Information via television and radio broadcasting are not get to the people if they do not switch on their equipments or the equipments do not work because of power outage. The modern telecommunications provides more effective ways for inform, warn and alert the public by automatic calls or text messages to the residents of the affected areas. [10]

The electricity-industrial special communication system

For the communication between the electricity-industry organizations the electricity-industrial special communication system is used. According to the 42. § of the Electricity Act the power transmission, distribution and generation companies may create and maintain closed communication systems in order to do their activities, to maintain the undisturbed and safe operation of transmission and distribution grids, to supply electricity demands continuously, to obviate malfunctions in a fast and safe way and to convey measurement data.

The system consists of the following:

- lines hired from communication companies
- microwave connections

- carrier-wave connections deployed to high voltage transmission-lines and cables
- owned cable network
- ultra short wave radio grid (URH) [11]

The requirements of the system are determined in the Operating Rules [12] of the Hungarian electricity system. According to the Operating Rules the creation and the operation of the system is the responsibility of the transmission system operator. The system has the following functions and parts:

- telemechanics and process management
- the system of operation management
- the system of energy-payoff
- information infrastructure
- relay protection and automatization systems
- other applications [12]

The communication system provides data and voice transmission services. The most important facilities of operation management – besides the other reserves prescribed by the Operating Rules – have to has public telephone systems connections and have to be accessible by cellular phone too. The voice transmission system has to assure the communication among the participants at least for 3 hours even in case of a blackout. [12]

The unified digital radio-communication system

In Hungary the analogue radio systems was changed to the unified digital radio-communication system (henceforward: EDR[77]) in 2007. It is based on the Terrestrial Trunked Radio (TETRA) standard and provides effective communication possibilities to the emergency bodies, such as police, fire-service, ambulance. In Hungary the system consist of 4 centres and 227 base stations and can manage 42.000 radios. 11 bodies have already joined to the system. [13]

The EDR is a closed system, joining to that is possible only for the organization named in the first annex of the No.109 of 2007 Order of the Government about the EDR. The annex lists 29 groups of potential users of the system, such as the departments of the Prime Minister's Office, the Ministry of Defence, the Ministry of Justice and Law Enforcement, Ministry of Local Governments, Ministry of Environmental Protection and Water participating in the management of states of emergency and disaster, furthermore the Hungarian National Police, the fire-services, the Directorate General of National Disaster Management. Organizations that have emergency response roles or contribute to such roles of administrative bodies and organizations providing public services or operating critical infrastructures can also join to the system.

The operability of communication systems in cases of electricity supply disturbances

In the following we outline how the disruptions of electricity supply affect the operability of communication systems, how long can the communication systems

[77] The abbreviation comes from the Hungarian name: Egységes Digitális Rádió-távközlő rendszer

remain operable without power from the power grid, what are the possibilities to applying standby or alternative electricity sources.

It should be noticed, that in case of an electricity emergency the communication system have to face not only the power outage but the overloading caused by the increasing demand. In this paper we do not discuss the latter phenomena.

The standby electricity supply of the telecommunications equipments is usually provided by diesel generators and batteries. The batteries run out of charge after a few hour, the operational time of the diesel generators depends on the volume of the available fuel. [10] In case of a long lasting power outage the fuel resupplying can be difficult because of the fuel outage due to the increasing fuel demand, the transportation difficulties, the shutdown of refineries and fuel distribution stations etc.

Therefore in case of a power outage in a few hour– after the batteries ran out of charge – problems occurs in the communication system. After the batteries ran out of charge diesel generators can provide the power supply if there any and if the fuel resupply can be provided. According to a study [10] a power outage longer than half of a day causes serious problems to the communication systems, and in case of an outage last 2-3 days the majority of the communication systems may lose its operability. [10]

The solution of this problem could be to provide the standby electricity supply with regional electricity generation systems using alternative or renewable energy resources. In several countries local power plants using alternative energy sources (e.g. biogas, wind-, water-, and solar energy) are applied regionally to provide the electricity supply for smaller townships. In case of a failure of the power grid these power plants could provide the electricity supply to the equipments of the communication systems. To switch these power sources takes a few hours, during which the diesel generators and batteries can provide the electricity supply. [10]

Summary

The sufficient electricity supply is one of the vital needs of the modern society; the failure of the supply affects other critical infrastructures too and can raise many serious problems in several areas of the modern life. In this paper we examined the effects of power outages to the communications systems. The effect depends on the size of the affected area and the duration of the outage. The cause of the outage can be an operational break-down or the enforced restriction on consumers made by the system operator in order to prevent that the problem become worse.

In the Hungarian legal regulation the Electricity Crises Order brings in the concept of heavy disturbance of the electricity power system, the impending electricity emergency and state of electricity emergency (together called as electricity crisis) and determines the role and responsibilities regarding to prevent and manage crisis. The order rates the operators of the main communication system equipments as vital consumers, the supply of which should be maintained as long as possible during an electricity crisis. Vital consumers are protected from the rotational restriction order too, applying the restriction order contains the vital consumers is allowed only when serious outages occur.

In serious cases the outage can lasts for days, for example in August 2003 in Michigan it lasts for 2 days. Maintaining the operability of the telecommunications system was possibly with standby generators and batteries, but it required significant efforts and resources. The communication between administrative bodies worked very well due to the Michigan Public Safety Communication System, a 800 MHz digital trunked radio system created by the State of Michigan.

The management of a potential electricity crisis requires the aligned work of several organizations and needs proper communication. The electricity-industry organizations communicate on the electricity-industrial special communication system. The civilian defence and disaster management organization in Hungary communicate on the unified digital radio-communication system, a closed system based on the TETRA standard. To provide information to the public is accomplished through radio and television broadcasting and on the internet. If a state of emergency occurs it is supplemented with the warning system of civilian defence bodies. The methods used for to provide information, warnings and alerts to the public do not use the possibilities of the modern telecommunications, automatic voice calls and text messages would be applicable.

According to a study [10] in case of a long lasting outage the telecommunication systems may have problems after a few hours as the batteries run out of charge. After 2-3 days - due to the difficulties regarding to the fuel resupply of the standby generators - the main part of the system may loses its operability. The solution could be to switch local electricity generator systems with power plants using renewable energy in case of a long lasting outage.

References

[1] No. 285/2007. (X. 29.) Order of the Government About the Heavy Disturbance of the Electric Power System and the Actions Required in Case of Electricity Emergency

[2] Act No. LXXXVI. of 2007 About the Electricity (Electricity Act)

[3] Körmendi, K., Solymosi, J.: The Legislation for Electricity Crisis Management in Hungary. Hadmérnök Vol. III. No. 2. – June 2008 http://www.hadmernok.hu/archivum/2008/2/2008_2_kormendi.html (downloaded on 1 June 2010)

[4] Rotational Restriction Order. Annex of the No. 432/2007 Order of the Hungarian Energy Office 22 June 2007. http://portal.mavir.hu/portal/page/portal/Mavir/Hivatalos/Fogy_korl_rsz/RKR20070903.pdf (downloaded 6 June 2010)

[5] Gerendás, D.: Black Start in the Hungarian Power System. BME Energetikai szakkollégium. March 2010. http://www.eszk.org/content/archivum/2010/beszamolo/Black_Start_beszamolo.pdf (downloaded on 24 May 2010.)

[6] Almási, K., Zerényi, J.: Large System Disturbances in the Power Systems, System Restoration and „Black-start". Presentation on the event of the BME Szakkollégium „Black Start in the Power System" on 18 March 2010. http://www.eszk.szakkoli.hu/content/archivum/2010/eloadas/Nagy_rendszeruzemzavarok_restauralas_2010-03-18.pdf (downloaded on 24 May 2010.)

[7] Körmendi, K. – Solymosi, J.: Method and Causes of an Electricity Supplies Outage as It Occurred in the Case Of "The Great North American Blackout of 2003". Hadmérnök Vol. III. No. 1. – March 2008.

http://www.hadmernok.hu/archivum/2008/1/2008_1_kormendi.html (downloaded on 21 May 2010.)
[8] Knowledgerush: 2003 North America Blackout http://www.knowledgerush.com/kr/encyclopedia/2003_North_America_blackout/ (downloaded on 21 May 2010.)
[9] Michigan Public Service Commission: Report on August 14th Blackout. November 2003 http://www2.tech.purdue.edu/eet/courses/eet331/blackout/Michigan_blackout_report.pdf (downloaded on 22 May 2010.)
[10] Maros, D.: Questions of national and international regulation of the operation of the telecommunication networks in emergency and disaster cases. PhD dissertation. ZMNE. 2006. http://phd.okm.gov.hu/disszertaciok/ertekezesek/2007/de_3625.pdf (downloaded on 4 June 2010.)
[11] Dr. Fekete, K.: The Communication Infrastructure of the Hungarian Republic. ZMNE EKK No. 952/525. Budapest. 2004.
[12] Operational Rules. Hungarian Energy Office 167/2010. M1/2010.03.29. http://portal.mavir.hu/portal/page/portal/Mavir/Hivatalos/Szabalyzatok/Uzemi_szab/Uzemi_szabalyzat_167_2010.pdf (downloaded on 9 June 2010.)
[13] Hanák, T.: Communication Systems in Case of Disasters. Hadmérnök Vol. III. No. 2. – June 2008. http://www.zmne.hu/hadmernok/2008_2_hanak.php (downloaded on 1 June 2010.)
[14] No. 109/2007. (V. 15.) Order of the Government about the Unified Digital Radio-Telecommunication System

Szabolcs MÁRKUS

OPERATING ASSURANCE ISSUES OF IP BASED VOICE COMMUNICATION

Szabolcs.markus@hm.gov.hu

Introduction

The demand of telephone services on IP networks continuously increases with the spread of IP based Internet. This interest can be explained by the need for cost effectiveness, the widely known and adopted protocols and the demand for rationalization of bandwidth.

Nowadays acronym IP identifies a digital network technology too, in which information is transported in an electrical form with Internet Protocol.

The voice as an information source can be transmitted duly in the quality which can be accepted by the developed *compression methods* and coding procedure on IP networks. The technology, which provides the delivery of voice over packet switched network, is called Voice over IP (VoIP).

Note that Internet telephoning in addition to full IP telephony (IPT) systems to appear. In IP telephony system all telecommunication functions, such as routing, transmission of the signal system, electrical phonebook, call accounting system are built on services of data transport systems. Due to the technology change (from ISDN to IP) planners, operators and maintainers have got to face the new challenges. Here is an example: Because of the structure of the technology the execution of the passive attack, such as eavesdropping or wiretapping, is very simple exercise without defensive mechanisms.

In a packet switched system stealing of information is an easy put into affect for the reason that in a given subnetwork all sent information gets to all network cards of hosts. In a normal function every cards takes exclusively those frameworks, at which the aim address is the same on its MAC address. If the aggressor switches the card into a special mode of action like that, the card can explain all broadcasted frameworks, he can get the desired information.

In military systems the telephone service is of overriding importance among the centrally provided services. This is confirmed by its role in military command and control system, its fast information delivery capability, and the requested high availability rate[78].

Subsequently the communication systems have to be protected by adopted method of information assurance with some changed details. This protection is based on well known three pillars: confidentiality[79], integrity[80] and availability[81]

[78] In the communication system of the HDF the availability rate is better then „four nines" (99,99%), which means only 53 minute period of breakdown annually. Traditionally the users demand this ability.

[79] Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems.

(CIA) according to the basic NATO security objectives [1], international standards [1], and the actual national military information security policy [4]. At communication systems *operating assurance* should be the most suitable expression, which basically originates from integrity and mostly availability. This publication delineates the parts of operating assurance, and the problems on these parts. It will also be explained that which solutions need to be considered with the development or the deployment of information and -communication systems.

Areas of Operating assurance and their details

The security is not enough only to be developed, it is necessary to maintain it continuously, which is through the full life cycle of the telecommunication system. The longest term of a system's or equipment's life cycle is the operation. We can section the operation onto more areas, in which there are different safety expectations. Therefore concerted and balanced activities in this areas are unequivocal important. Let think about the protection of a military base. Despite of the fact that we set up a checkpoint, a barbed wire, portable barricades, marksmen at the gate of the base, it is not adequate the protection if we do not builds a fence around the base. To sum up, the security is a complex activity.

A telecommunication system has to fulfil several requirements to achieve the expected safety. First of all, this system should be operational under any circumstances, due to the fact that voice communication is the basic tool for command and control. It is follow from this, the forwarded voice, and the handled data in operation of the system may not be cognized by an unauthorized person or an application. The access to system services and management devices may happen in such a manner that authenticated only. Naturally the system has to make it possible that authorized people are entitled to access data and information in suitable time, form and content.

According to the above, for achievement of assurance goal it is necessary to create safety procedures in proportion to risk. Therefore risk analysis[82] is important to execute before installing a telecommunication system, and it has to be reviewed continuously (annually). The result of this risk analysis and the concerning safety requirements must be attached to the system conception plan. After the establishment of communication system, documentation and registers have to be created, managed and updated continuously.

The telephone systems do not operate as an island generally, but other PSTN, or system of organisations are attached to their networks. The system has to defend its exterior accession points with mechanisms that prevent and alarm an unauthor-

[80] In information security, integrity means that data cannot be modified without authorization.

[81] For any information system to serve its purpose, the information must be available when it is needed.

[82] Risk analysis is a procedure to identify and assess factors that may jeopardize the success of operated telecommunication system. This also helps to define preventive measures to reduce the probability of these factors from occurring and identify countermeasures to successfully deal with these constraints when they develop to avert possible negative effects on the unserviceable of the system.

ized penetration or its experiment, and support the efficient answer reactions. The exterior contacts of a telephony system have to be created with protected access, and entry points, which is adequate to complete the regulation of assurance. It is obvious from the above that the safety is a complex task, where we proceeded from integrity and availability at the operating assurance of IP based telecommunication system.

Since the very early days of packet switched and open networks' invention and forming the demand of information integrity has appeared, which was called for by defending against unauthorized or spiteful users. The attacks against the integrity come from the circle of the so-called active attacks, in the course of this not only does an aggressor trace the network, but he/she modifies it (tampering), exchanges it.

In the followings I deal with availability, which is mostly close to operating assurance. The requirements of availability can be declared exactly (life time, redundancy, capacity, etc.) At the injuring requirement of availability, the point at issue is not the getting information to unauthorized users or the tempering but the operating of system is changing, where it can not purpose normal function or it works incorrectly.

The availability is influenced by direct and indirect attacks, practical factors and operating circumstance (breakdown, human omission, damage, etc.).

PreDeCo

After the planning of fundamental safety requirements for telecommunication system it is advisable to declare the defensive mechanisms. It is expedient to establish as PreDeCo precept show that [6] It is based on prevention, detection, correction. At the operation of telecommunication systems all three of the mechanisms should be adopted against any threats during the lifecycle of these systems.

The *prevention* is a preparation which means protection ability, continuing operation procession and reservation developing.

The main point of the *detection or the recognition* is that as soon as possible the system can find any redundant event, this capability gives an opportunity to prevent the spreading of incident. It can improve efficiently the rebuilding activity to the system can get the normal operation situation.

The correction consists of the series of interventions in the course of the restoration which can stop the dysfunction operation quickly, and prevent furthermore additional destruction or damage of the telecommunication system. The response time and responsible time may be an important index-number. The efficiency of the reconstructive activity can be improved by preparation in the period of the prevention. (Backup file, maintenance teams, reserve equipment, etc.).

Operating assurance

There is a national standard (as a best practice) to supply a suitable basis to the examination of an operating assurance issues of IP based voice communication system, and its *protective mechanisms* 158. This publication consists of the next assignments:

- - awareness and training;
- - configuration management;

- - contingency planning;
- - incident response;
- - maintenance;
- - media protection;
- - physical and environmental protection;
- - personnel security;
- - system and information integrity.

Awareness and Training

To the safe function the users and operators of the communication system have to know their role and responsibility in this system. It has to be recognised and to understand the operation and safety regulation of the communicational system, and these the order of a procedure.

There are threats with regard to a system if operators are not able to operate the system on a suitable level, and if operators and users do not know the dangers, and the responsible leaders can not be demand the safe operation and usage. The education subjects have to be divided and organized as level of role: leadership or command level; vocational designer and management level, operator level (operator, system engineer); application (user) level. The execution of training must be planned, and the body of knowledge must be refreshed, updated continuously.

Configuration Management

The configuration management is a process, which in the requirements and characteristic of a system, system components, and the environment of the procedures is changed, which provide this system's suitability. The configuration management is consistent with standards, applicable laws, policies, regulations continuously, and it have to react on the different changes.

On a vocational high level leadership the configuration management's task is to define the requirements of the system, which are understandable for everybody, clear ones, and at all times valid. The documentation of the configuration, which appears on an operator level, describes handling, functionality and architecture of the system, a product under development or use, access rights, and the catalogue of services, resources and reserves. Inside operator tasks are to put changes down to the documentation. Strict rules are necessary to getting an access to the execution of changes. By outlining at communication systems the documentation is not equal to configuration.

Contingency planning

Contingency plan is a plan devised for a specific situation when things could go incorrect so sometimes contingency plan is called worst-case scenario plans. Contingency plans are necessary to the communication system have to be prepared for anything that could happen. A communication system can experience a serious incident that can prevent it from continuing normal operations. This can range from a flood or fire to a serious computer malfunction or information assurance incident.

The management of the organization has a responsibility to recover from such incidents in the minimum amount of time, with minimum disruption and at minimum cost. This requires careful preparation and planning.

The stage of reaction ability is depended on the development of the plan and the successful testing and audit of the plans activities. It is necessary that all personnel have to be made aware of the plan and be aware of its contents and their own related duties and responsibilities. It can be accomplished users and administrators training. Obviously the plan must always be kept up to date and applicable to current political, military and IT circumstances.

At the communication systems we should emphasize the next areas:

- reactivating of auxiliary systems, networks and cables;
- utilization of reserve equipment;
- establishment of temporary links;
- process of personnel and tools redeployment;
- restriction of services;
- the process of rebuilding and recharging.

Incident response

The operating assurance incidents not desired or waited unique or serial assurance events, which jeopardizes the operation and threats operating assurance in all probability.

The incidents may be accidentally events, or results the results of deliberate damage. The incident response policy may be included as part of the general information security policy for the organization. Incident response procedures can be developed for the security program in general and for a particular telecommunication system. Automated mechanisms can provide the ability to more thoroughly and effectively test or exercise the incident response capability by providing more complete coverage of incident response issues, selecting more realistic test/exercise scenarios and environments, and more effectively stressing the response capability.

It is necessary, that official event reporting procedures are established, which can be based automatic and manual system. Following a happened incident it is obligatory to learn a lesson and the experiences must be implemented into incident response documents.

Maintenance

Operated telecommunication devices by maintenance staff procedures belong to this part such as maintenance, patching stopping, starting, etc. The most important is that management of the system prepares the system operation order. Also it is necessary to define the requirements for the exterior operator's activity, and its change. The *Information Security* publication lists the areas with which it is essential to deal under the operator activity in detail.

- schedules, performs, documents, and reviews records of maintenance and repairs on system components in accordance with organizational requirements;
- controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;

- requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;
- sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;
- checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

Naturally we can count the above list, here are some additional requirements.

It is unequivocal role, that centralised supervisor function has to be deployed, which can manage and hold together maintenance and service activity. The operation staff has to keep the maintenance diaries continuously. Maintenance activity has to be executive by designated and appointed persons on designated operator workplaces. The remote access must be only inside an own network with separated maintenance (management) systems. The dealing with problem announcements (on phone, from system error messages) belongs to operator activity too. So the maintenance is a multilevel action: local operator, and regional, national, system engineer.

Media

Data store like that devices, which take a part in the information processing, belong to this part. Fundamentally in telecommunication concern media may store system files, backup files, log files, tariff data, or other management information (engagement, capacities, congestions, etc.). Media can be paper, or magnetic, electronic and optical storage. To ensure protection of media is necessary to prevent the unauthorized access, modification and wrong storage. Access, making, storage, transport, and abolishing method must be declared.

Physical security

Physical security is the protection of telecommunication system and its equipment, networks, and data from physical circumstances and events that could cause serious losses or damage to an institution, enterprise or facility, resource, information stored. This includes protection from flood, fire, natural disasters, vandalism, and terrorism. Here can be the regulation of entrance to CIS centre.

Power-supply belongs to this security too, due to the fact that indisputably the telecommunication system has need of energy.

Systems have to be supplied more directions electricity, and completed with uninterruptible power supply (UPS). The sizing of the uninterruptible systems with 4 hours of bridging time is proposed to plan. Signalling of UPS must be connected to supervising system.

According to opportunities the central supervisory and controller function is necessary to be duplicated, as they are distant physically from each other (other settlement).

Personnel Security

By this time the telephone systems have got to automation adequately already, conversely the human collaboration is indispensable.

The personal work involves a vital responsibility so that a personal intervention can change the control mechanisms, the entitlements, defensive functions, parameters, diary files, and they can get the sensitive information, furthermore systems, furthermore they may stop system components.

Here are some instructions:

- It is necessary to check the person before giving him authority to the system for somebody.
- Let there be procedures onto that case, if somebody leaves the organization.
- Let all employees sign a declaration about the usage and operation of the system.
- Let roles be distinguished and rotated.

System and Information Integrity

In telecommunications, the explanation system and information means that telecommunication system completes its intended function in an intact operating, free from inadvertent or deliberate unauthorized manipulation of the system. Furthermore there is complete operating assurance that under all conditions the system is based on the logical correctness and reliability of the hardware and software that implement the protection mechanisms, and voice (data) integrity. Those hardware, software, networks and their elements belong here, which take a part in the processing and forwarding of the information such call-managers, switchboards, gateways, cables, computers, peripheries, applications, etc.

In the following some important protective measures and issues are detailed concerning telecommunication system establishment without the claim of the completeness.

The new hardware and software have to be examined and tested prior to systematizing.

The different classification systems are necessary to be separated from each other (physically, logically). Different networks are needed (switch) to be useful for them. VPN architecture must be developed on MPLS network.

There is redundant forming of centre elements.

- The support servers are organised in cluster structural design. (High-availability, load-balancing, High-performance computing, Grid computing)

The support elements are deployed in security areas.

The cables of system are protected against unauthorised access.

- There is password protection and password renewing method.
- There is an amortisation treatment, support system.
- Cryptograph procedures are used in connection (IPSec).
- There is activating method.
- There are strict and controlled authentication and access mechanisms (multilevel password system, token, PKI).

- Firewall and antivirus, intrusion detection system, intrusion prevention system are deployed.

Summary

The basic service of IP based telecommunication system is voice. Although the voice transportation and its network usage are accomplished easily, the operating of the full system is a complex task. To the continuous availability we have to reveal problems and to solve them at operating assurance. This is an interaction process, which are spread from users to operators and from administrators to commanders.

Referencies

[1] C-M (2002) 49 Security Within the North AtlanticTreaty Organisation
[2] Information technology. Security techniques. Information security management systems. Requirements ISO/IEC 27001:2006
[3] Information technology. Security techniques. Code of practice for information security management ISO/IEC 17799:2006 (27002)
[4] 94/2009. (XI. 27.) HM utasítás a honvédelmi tárca információbiztonság politikájáról
[5] Quality management systems. Requirements (ISO 9001:2008)
[6] Technology Special Publication 800-53 Revision 3, Information Security

Norbert NÉMETH – László ZÖMBIK

IMPROVING THE EFFECTIVENESS OF TRAFFIC ANALYSIS ATTACKS ON IEEE 802.11 PROTOCOL BY CORRECTING THE DISTORTION OF RADIO INTERFACE

Abstract

The purpose of traffic analysis is to obtain subsidiary information based on the network traffic. Radio channels, however, distorts the traffic shape and thus makes it harder to extract the needed information. In this paper we analyse IEEE 802.11 protocol to identify those meta-data which could be used for improving the effectiveness of the traffic analysis. We show through measurements the effectiveness of our solution.

1 Traffic Analysis Overview

The methods aimed to extract information from network meta-data are called traffic analysis. Network meta-data includes the volume and timing of network packets, network addresses, protocol properties and headers.

In IEEE 802.11 [13] networks, a possible use of the traffic analysis is the *Identification* of a certain endpoint. Another use of the traffic analysis is the *Proof of Presence*. In these attacks, the attacker has some previously known traffic pattern that is specific to the victim. This traffic pattern could then be recognised on the wireless interface. If the traffic pattern is found then it is a proof that the victim is in range. From the wireless traffic the layer two information of the victim is also determined.

Unfortunately IEEE 802.11 wireless channel as a physical medium is highly unreliable, thus it introduces distortions. Our goal was to decrease the effect of such distortions to easily identify the traffic pattern of the victim.

In the following we present some examples of traffic analysis. After giving some historical examples from the military intelligence we give some peculiar examples of active and passive traffic analysis. Chapter 2 describes the impact of traffic analysis on IEEE 802.11 interface. In chapter 3, the IEEE 802.11 protocol family is analysed from the angle of how the protocol meta-data can be used for traffic shaping. Finally we conclude our paper by presenting our results.

1.1 Historical background

The first real traffic analysis examples [1] have roots in military intelligence of the early last century, where traffic analysis methods were used to gather important information way before computer networks came to existence.

It was first used in world war one actively, to pick up telegraph signals and extract information out of it. When the German forces entered France, they started to use radio communication to send telegraph messages. The French gathered information and tried to localize stations using trilateration. They analyzed traffic inten-

sity as before military operations much greater volume of traffic was expected from the stations located near the combat groups.

Later in world war two, its importance has risen especially in naval and air warfare. Before major operations radio communications were terminated in fear of the enemy analyzing the direction and other statistical properties. By that time the cryptographic algorithms were unbreakable, traffic analysis was still useful.

There are even records of radio operators identifying enemy operators, by the statistical properties of how they have typed Morse code. This could be used to identify military units. The method is very similar to the one presented in the following section which identifies users by their keystroke dynamics.

1.2 Passive Traffic Analysis

During Passive traffic analysis attacks, attackers only observe the communication passively they do not interfere with the communication flow. With this method various information could be deduced such as the identity or position of the user or of the device. Even some unique or specific relations could be identified, which could lead to reveal some more important facts or secret information.

1.2.1 Traffic Analysis of SSH

Secure Shell is a network protocol for logging into a remote machine and executing commands on it using a secure channel between the two devices [2]. After authentication, SSH encrypts all data flowing between the communicating parties providing confidentiality and integrity. An interesting property from traffic analysis point of view is that in interactive mode every keystroke typed by a user is sent in separate package after the key is pressed.

It was shown [3] that simple statistical techniques are able to reveal sensitive information, such as password length. More advanced techniques can be used to derive information of what users are typing based on their typing patterns. Because of their uniqueness, typing patterns were proposed to be used for hardening password schemes [4]. In the research it is shown, that typing patterns can be considered as biometrics, strong enough to identify users. From this it can be concluded, that the information can also be used to identify users by their typing habits over an encrypted channel.

1.2.2 Traffic Analysis of SSL/TLS

Transport Layer Security and its predecessor Secure Socket Layer are cryptographic protocols securing communications over computer networks, encrypting end-to-end traffic at the transport layer [5]. It was shown [6] that it is possible to build profiles of web sites and due to insufficient padding employed by TLS, it is possible to link users to resources accessed on the site.

Another research [7] shown that HTTP traffic can be analyzed not only over TLS, but other encrypted links such as WEP/WPA, IPSec and SSH tunnels.

1.2.3 Location Data Exploitation in Wireless Networks

During the Hackers at Large Conference in 2001 meta-data based traffic analysis attack were carried out on wireless networks [8].

Wireless MAC addresses were collected from the multiple access points deployed at the conference, and profiled users.

Based on the wireless traffic, it was determined which presentations the users attended and conclusions were made about their social connections. If a user pair had above average correlation of location data, they were suspected to be related.

1.2.4 Attacks Against Anonymizer Solutions

Most of the attacks employing traffic shaping or traffic analysis were presented in research to defeat anonymizer networks such as Tor. Tor's importance is being the most widely adopted anonymizer, which promises protection against traffic analysis [9]. An anonymizer network is trying to hide the user's real origin to improve their privacy and security on the Internet. It usually employs cryptographic solutions to achieve this goal, thus hiding the traffic, IP address and routing information.

Existing active traffic analysis attacks against Tor were overviewed and a new active attack was presented using traffic shaping method in [10] [11].

1.3 Active Traffic Analysis

In active traffic analysis, the attacker not only observes communication, but modifies it. An example of such an attack is traffic shaping.

1.3.1 Traffic Shaping

Traffic shaping [11] [12] or packet shaping is controlling of computer network traffic to increase performance, latency or bandwidth. Traffic shaping is applied as bandwidth throttling or rate limiting. Bandwidth throttling is controlling the volume of traffic sent into the network in a period of time, while rate limiting is setting a maximum rate at which traffic can be sent. Nodes buffering traffic in an IP network can cause traffic shaping effects, too.

The essence of the traffic shaping attack is when a user accesses a service, a malicious server or a man-in-the-middle attacker can change the shape of the traffic. On the client's side of the link this unusual shape can be detected, by collecting network meta-data. The efficiency of this attack against anonymizer networks were demonstrated in [10] [11].

2 Traffic Analysis on 802.11 Radio Interface

When communication is properly encrypted at the wireless MAC level (by using WEP, WPA, WPA2) or at a higher layer, like using IPSec encryption, it is impossible to obtain the protected information. At some times, however, not only the encrypted information matters, but also the side-information related to the protected traffic. For example, in a battlefield, if the attacker can realize that the enemy’s general is present then they may make decisions accordingly.

The purpose of IEEE 802.11 protocol fields is to establish layer two communication between the parties on the shared radio channel. Therefore those protocol fields are transferred in clear text.

In addition, several of those layer two encryption mechanisms were proven to be weak. Network layer encryption (IPSec) only protects its own payload. Regardless of those facts, let us suppose that where encryption is used, the encrypted data cannot be restored for the attacker and the integrity of the data is also protected.

Active attacks on encrypted channels are quite limited as if the encrypted data is tampered, the peers can detect the attacks. The shared radio channel makes it

possible to the attacker to easily eavesdrop or actively interfere with the communication.

In the above situation the most typical goal of the attacker is to identify that a specific user/endpoint is present in its range. For that purpose, the attacker either actively mark the traffic pattern of the traffic which is destined to the target. Or, the attacker has some information beforehand of the traffic pattern of the encrypted traffic, which is destined to the target.

In both cases, if an encrypted traffic, which has a pattern previously known to the attacker, destines to the neighbour of the attacker, the attacker will know that his target is in range.

The radio channel may distort the marked or previously known traffic pattern, because of other users of the radio frequency or the reflection or shielding of the environment. The distortion could render the shape of the traffic hard or impossible to identify. For this reason, we analyse the protocol fields of IEEE 802.11 MAC frames in the next section.

3 IEEE802.11 Meta-data from Traffic Shaping Point of View

There are plenty of fields in the 802.11 protocol available without protection. Most of the fields are not used, only in special cases and circumstances. Here we try to show which fields can be used to improve the success of traffic shaping attacks and are available in every environment. Our investigation was focused on the most common environments, like accessing a wireless network from a laptop.

Let us inspect the medium access control frame format as the common structure shared by all the types and subtypes and is always available no matter if WEP or WPA is used.

The most obvious thing to do is to separate traffic streams based on the sender and receiver MAC address. The MAC address of the Access Point (AP) can be easily fetched from management frames which are meant to exchange information serving the IEEE 802.11 architecture. All the other clients (STAs) using the same BSSID (Basic Service Set Identifier) are the clients. The downstream traffic can be filtered by selecting data frames which are destined to a STA address and originated by the AP.

The frame control field, which is the first two octets of IEEE 802.11 frames is a collection of fields signalling various options. Among those, three fields can be considered: more frag, retry and more data fields.

More frag field is used to indicate there is more data to be sent, when fragmentation is employed. The circumstance in which this field is used is not general.

There are two major uses considered. The first is when a fragmentation limit is set in a station in a hope that by sending smaller pieces of data, collisions are less likely to occur.

The second is when a sending time period is dedicated to a station in case of a contention free channel access method is employed. Fragmentation occurs, when this period is expired before the sending of the whole data unit can be finished.

The more data field could be very useful, as it indicates that there is data buffered waiting to be sent. It is only used by non-AP STAs in power saver mode, or it is used in upstream or STA-STA communication, which is not our interest during

traffic shaping. We do not consider power saver mode STAs to be in the attacked environment, as this mode is not used in regular cases.

The field we can actually investigate and use from the frame control field is the retry field. It is to indicate that the frame is being retransmitted. We can try to process our communication stream trying to remove distorting resent frames. This is useful to exclude the distortions of the physical channel from the stream.

The next attribute to consider from the media access control frame is the QoS Control field. It contains one interesting subfield from a traffic analysis perspective, the AP PS buffer state. In power saver mode, it would indicate to a STA, how much data is buffered for it of the highest traffic class.

The last field that might be used for our cause is the TXOP limit subfield. TXOP indicates to a STA that a dedicated channel use period was granted to it by the coordinator function. Multiple traffic classes and TXOP requests are not common in general environments.

After this short overview it can be concluded, that there are three straightforward filtering methods that can be generally used, based on 802.11 meta-data in everyday environments. The downstream and upstream traffic of each client can be separated, and the retransmitted frames can be detected.

4 Results

We have first separated traffic based on their destined endpoint, so that traffic of each client can be processed separately by the pattern matching algorithm.

Our focus was on unidirectional traffic, as it can be easily distorted to actively mark patterns into it, or it can easily be observed passively. In our investigation, the unidirectional downstream traffic had more interest for two reasons. First, the order of magnitude of the downstream traffic is expected to be higher than the upstream. The second reason is that the attacker could mark specific traffic somewhere in the network. That traffic arrives via an AP to the victim on the downstream link.

On the other hand, upstream traffic could also be used. In this case, either some knowledge specific to the traffic pattern of the victim equipment needs to be possessed in advance for the attacker. Or the equipment of the victim needs to be tampered with, to put mark actively into the upstream traffic.

Our patterned signal was the bandwidth distorted by a periodically sampled sinusoid function. In our measurement, we generated this marked signal at a specific point of the network and we sent the traffic through the Internet towards a remote Access Point. The AP then forwarded the patterned traffic to the victim equipment via the downstream link.

In Figure 1 we show how Internet and an undisturbed wireless link (with no background traffic and good SNR) could distort this bandwidth, which was used as a reference measurement. We have made measurements at two points of the network. The first measurement point was right next to the origin of the shaped traffic, the other measurement was made on the wireless medium, near the victim. The relationship of these signals is shown on the figure, the bandwidth of the wireless traffic in proportion with the original patterned sinusoid function. It can be seen that the Internet and the noiseless, congestion free wireless link gives only infini-

tesimal disturbances into the traffic shape. This is given by the fact, that the points of the function are strictly following, the ideal, 45 degree line.

In Figure 2, the same network configuration is used, except the wireless medium was disturbed. During this investigation we tried to achieve constant 20% loss on the wireless link. Instead of adding background traffic, we rather decreased the SNR by a noise generator. Our noise generator was a microwave owen as it operates in the same ISM (Industrial, Scientific, Medical) frequency band, as IEEE 802.11b/g wireless networks.

The loss, which was generated by the increased noise, enforced the AP to buffer and re-send the damaged packets. We have applied the same measurement approach as above and illustrated the results. On the figure, with pale the bandwidth of the wireless traffic is shown in proportion with the original patterned sinusoid function, similarly to the previous figure. It can be seen that this traffic, compared to its input is increased drastically. Our correction, which was based on that the packets with retry fields were removed, is represented in dark. It can be seen that with that correction, the original input bandwidth was restored.

Based on our investigation we could conclude that in case of bandwidth based traffic analysis is used, the distortion of wireless link could be mitigated. If packets with retry field are removed, then the effectiveness of the traffic analysis attack is improved. This method can be applied effectively even on a noisy channel.

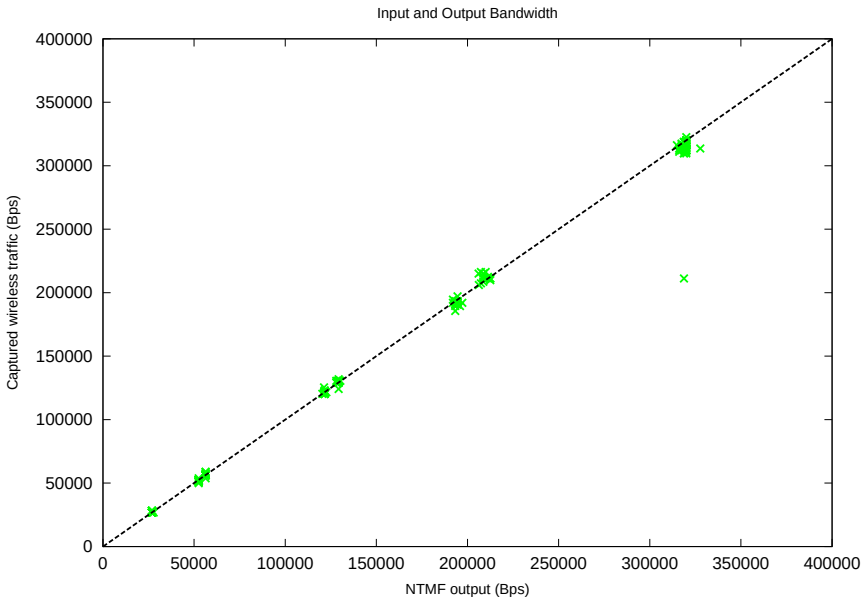


Figure 1. Wireless link with no background traffic, good SNR

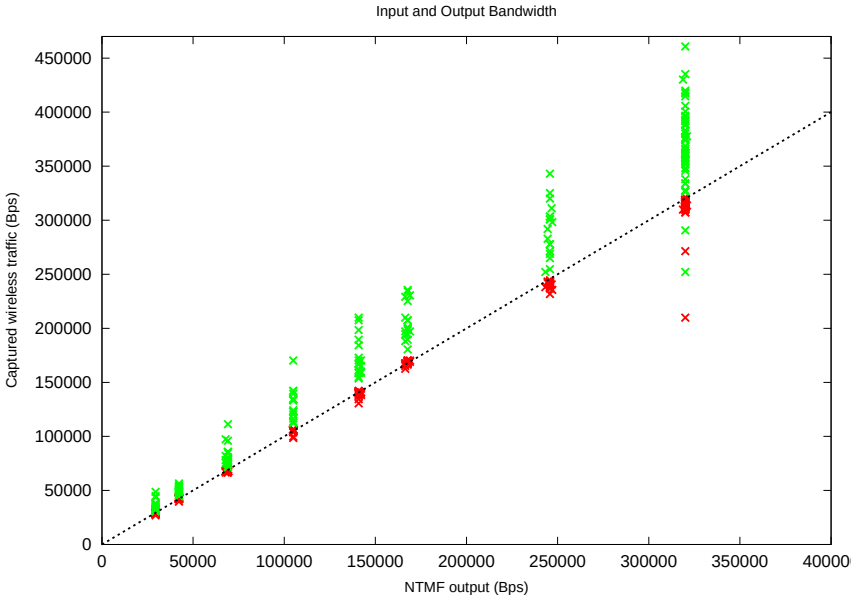


Figure 2. Wireless link with 20% loss. Resent frames distorted the traffic shape

References

[1] Simon Singh. The Code Book: The Evolution of Secrecy from Mary, Queen of Scots, to Quantum Cryptography. Doubleday, New York, NY, USA, 1999.

[2] C. Lonvick T. Ylonen. The secure shell (SSH) protocol architecture. RFC 4251 (Standards Track), January 2006.

[3] Dawn Xiaodong Song, DavidWagner, Song David, and Xuqing Tian. Timing analysis of keystrokes and timing attacks on SSH. In SSYM'01: Proceedings of the 10th conference on USENIX Security Symposium, pages 25-25. USENIX Association, 2001.

[4] Fabian Monrose, Michael K. Reiter, and Susanne Wetzel. Password hardening based on keystroke dynamics. In International Journal of Information Security, pages 73-82. ACM Press, 1999.

[5] E. Rescorla T. Dierks. The transport layer security (TLS) protocol version 1.2. RFC 3775 (Standards Track), August 2008.

[6] George Danezis. Traffic Analysis of the HTTP Protocol over TLS, (accessed on Apr 29, 2010). http://research.microsoft.com/en-us/um/people/gdane/papers/TLSanon.pdf.

[7] George Dean Bissias, Marc Liberatore, David Jensen, and Brian Neil Levine. Privacy vulnerabilities in encrypted HTTP streams. In In Proceedings of Privacy Enhancing Technologies Workshop (PET 2005), pages 1-11, 2005.

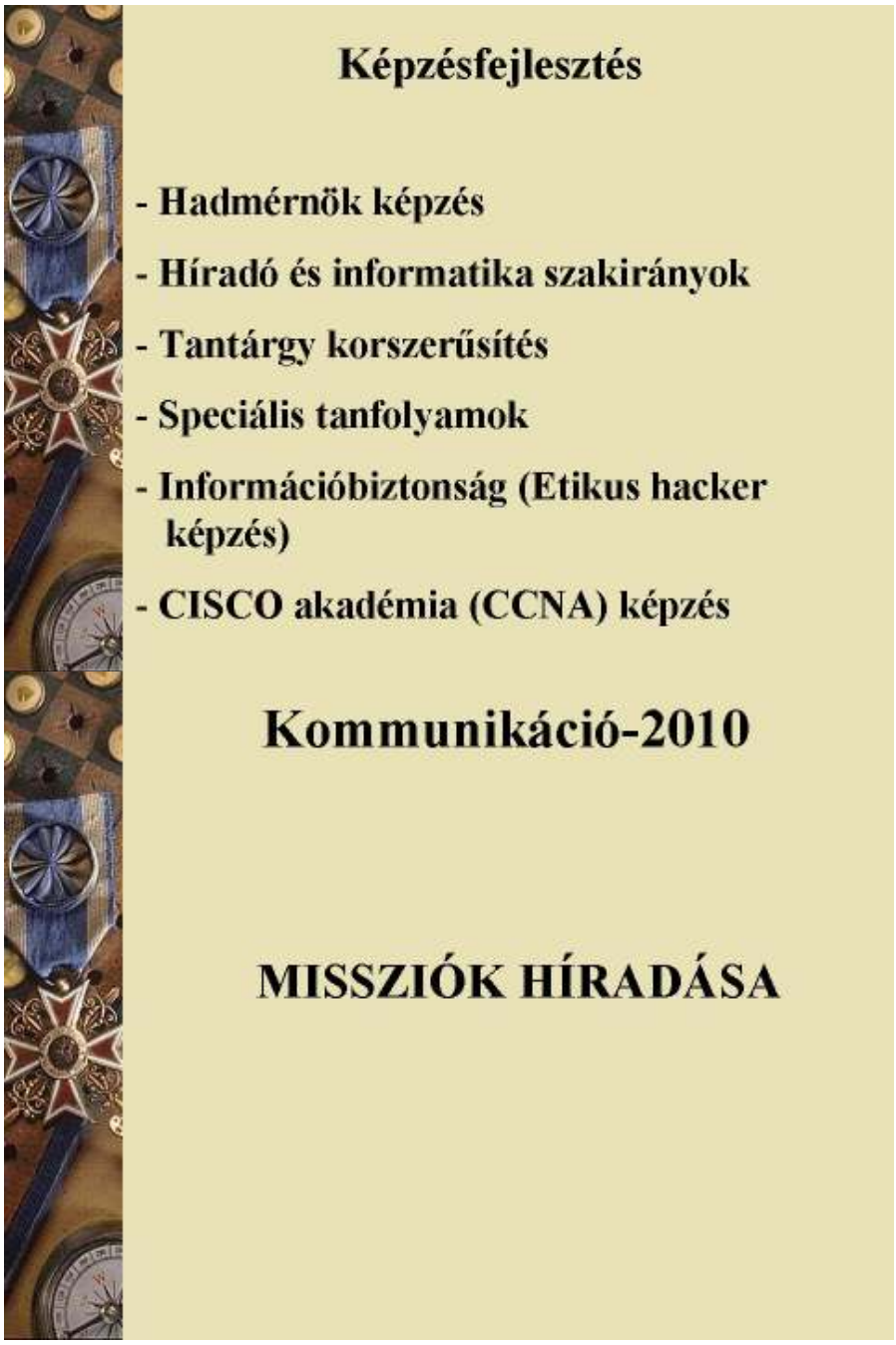
[8] George Danezis. Introducing traffic analysis: Attacks, defences and public policy issues... In Invited Talk. Santa's Crypto Get-together., Prague, December 2005.

[9] TOR anonymizer, 2010 (Accessed on Sept 2, 2010). http://www.torproject.org.

[10] Laszlo Czap. Security analysis of anonymiser networks. MSc Thesis at BUTE, 2008.
[11] Zoltan Szentpal. Real-time network traffic modification. MSc Thesis at BUTE, 2006.
[12] M. Carlson E. Davies Z. Wang W. Weiss S. Blake, D. Black. An architecture for differentiated services. RFC 2475 (Standards Track), December 1998.
[13] Part 11: Wireless lan medium access control (MAC) and physical layer (PHY) speci_cations. IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Local and Metropolitan area networks - Specific

RAJNAI Zoltán

KOMMUNIKÁCIÓ 2010


Képzésfejlesztés
- Hadmérnök képzés
- Híradó és informatika szakirányok
- Tantárgy korszerűsítés
- Speciális tanfolyamok
- Információbiztonság (Etikus hacker képzés)
- CISCO akadémia (CCNA) képzés
Kommunikáció-2010
MISSZIÓK HÍRADÁSA


Jó programot, kellemes napot kívánok minden résztvevőnek
Dr. Rajnai Zoltán mk. ezredes

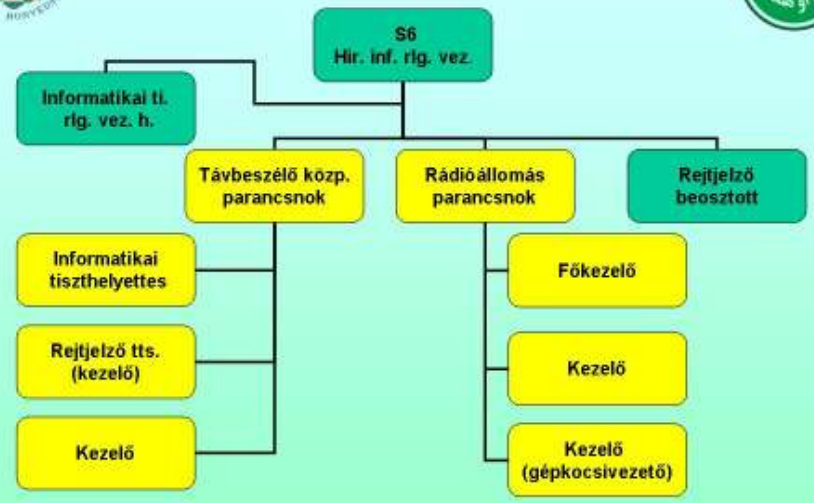
LABODA János

ISAF CIS

MH PRT felelősség:

- Tábor belső híradása;
- Kommunikáció biztosítása a lehetségesen legtöbb csatornán az OPS és a kivonuló csoportok, valamint az elöljáró RC N között;
- MH Intranet (Exchange, file-server és backup szolgáltatások), MH Internet hálózatának helyi kezelése, számítógépek konfigurálása (MH/CIVIL), VTC biztosítása, vetítések előkészítése;
- ISAF HQ IVSN és Secure Computer Network NCN / FOC+ biztosítása, kapcsolattartás a ISAF HelpDesk-eivel, a THALES helyi képviselőjével;
- Műholdas kommunikáció biztosítása (HUN V-SAT);
- Telekommunikációs eszközök üzemeltetése, konfigurálása, programozása (HICOM és PANASONIC központ, NORTEL switch, CISCO router, TACSAT, GP-340…);
- Rejtjelfelügyeleti és rejtjelzési feladatok (Honi és NATO, SSO).

MH PRT S6 Felépítése



S6 – CIS

…alapvető információk a telekommunikációs rendszerről…

PRT Belső Telefon Kommunikáció

- 60 vonalas Magyar Nemzeti Kommunikációs Központ (HICOM) 95%-ig kihasznált;
- Programozása elsősorban távfelügyelet útján történik, de lehetőség van helyszíni programozásra is;

- 32 vonalas Panasonic központtal kapcsolódik (S6-on, jelenleg az őrség és Bunkerek kiszolgálására).

THALES FOC+ rendszer

ISAF

•THALES FOC+ rendszer (Mikrohullámú és műholdas

•IS/NS/NU rendszere;
•Telefon szolgáltatás
•NCN
•VoIP (OPS, COM, S2)
•STU-II (OPS, COM)
•IFTS
•PRC-117F
•SECTERA mobil

NCN (IVSN) rendszer

- Mikrohullámú és műholdas ISAF telefon hálózat ;
- NATO által fenntartott;
- Elérhető minden NATO/ISAF haderő rendszere;
- Szükséges prefix híváshoz:
  60-684- (FOC+ RC-N)

FOC+ rendszer

- Szolgáltatások:
  - IS/NS/NU levelező rendszer;
  - Telefon szolgáltatás ;
  - Szükséges prefixek híváshoz:
    - 60-686- (HQ KABUL)
    - 60-684- (RC-N)
    - 60-682- (RC-W)
    - 60-688- (RC-C)
    - 60-683- (RC-E)
    - 60-685- (RC-S)

RCN HQ MES	1XXX
KDZ PRT	62XX
FEYZABAD PRT	63XX
PEK PRT	64XX

Titkosított telefonok

THIS TELEPHONE IS SECURE

STUIIB phone
- Titkosított végberendezés;
- Minősítése: NATO SECRET;
- PRT rendelkezik 2 készlettel,
  - OPS
  - COM

SVoIP phone
- Titkosított telefon
- ISAF Secret LAN-t használja (VoIP);
- PRT 3 darabbal rendelkezik
  - COM
  - OPS
  - S2

MH PRT **RÁDIÓ** kommunikáció

Rádió eszközök:
- GP-340 MOTOROLA, MH-300
- MTS-2000 TRUNK MOTOROLA
- RF-5800
- PRC-138, PRC-117/D, PRC-117F
- R-173, MV-300,
- RF-5200 (Stacioner-HIK)

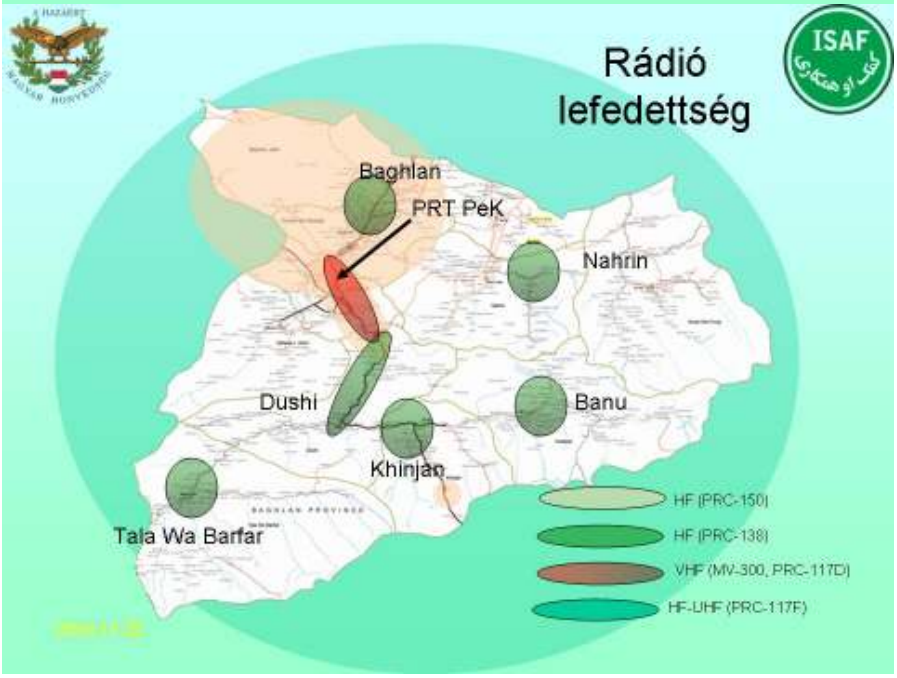
ISAF által biztosított:
- TACSAT RADIO (Műholdas alkalmazású PRC-117F)

A müveletek alatt csak TACSAT rádióval van titkosított kommunikáció és a földrajzi adottságokból eredően szegényes a rádió lefedettség, alkalmazhatóság!


PRT rádiókommunikáció
✓Konvojkíséret és hadművelet
✓MEDEVAC
✓Járőr
✓Törzs, FP
HF
VHF
UHF


PRT rádiókommunikáció
ISAF
Konvojkíséret, hadműveleti rádióhíradás:
RF 5200/20, 150W
RF 5800HH
PRC-138/20, 150
PRC-117D/F/20W
R-142/5W (tartalék)
MRR/MHH
MOTOROLA MTS 2000
HF
VHF/
UHF
RF 5200 HARRIS
AN/PRC 138 HARRIS
R-143


PRT rádiókommunikáció
ISAF
MEDEVAC
PRC 117D
R- 173
Járőrök, outside teams
Motorola GP 340
R-173
RF 5200/ 20/150W
PRC 138/20/150W
PRC- 117
Törzs, FP, QRF, mission team, MP
Motorola GP 340, MRR/MHH


Rádió
lefedettség
ISAF
Baghlan
PRT PeK
Nahrin
Dushi
Banu
Khinjan
Tala Wa Barfar
HF (PRC-150)
HF (PRC-138)
VHF (MV-300, PRC-117D)
HF-UHF (PRC-117F)

CIVIL RÁDIÓTELEFONOK

ROSHAN (network prefix: 79)

AWCC (network prefix: 70)

- Civil Orosz érdekeltségű Afgán mobil szolgáltató;
- Elérhető: összes civil vonal minden államban;
- Költsége (10 US cent percenként más Roshan felhasználók irányában)
- Country code +93 / 0093
- Minden szolgáltatás feltöltő kártyás (pre-paid)
- 2 db HIK GSM adapteren, személyi állománynál 56+1; (1 T-Mobile, 13 AWCC, 41 ROSHAN)

MH PRT Mobiltelefonok

ROSHAN

AWCC

Minden szolgáltatás feltöltő kártyás (pre-paid)

Probléma:

A szolgáltatás 1700-0600 között szünetel

Afghan Telecom

GSM Lefedettség RC N

MŰHOLDAS
Kommunikáció

IRIDIUM

•Adatátviteli lehetőség (SMS / e-mail 8816XXXX@msg.iridium.com)

•NATO/ISAF UNCLASSIFIED minősitésig alkalmazható

INMARSAT

Titkosított vonalak

- Titkos Fax: 1 db;
- STU-IIB: 2 db;
- VoIP: 3 db;
- Nato Secret: 2 db;
- ISAF Secret munkaállomások: 8 db.

MH PRT Informatika

- **MH Intranet ≈ 60 munkaállomás**
  Hazai feltételek és biztosítási feladatok érvényesek
- **Internet**
  - **MH**
  - **Civil**
- **IP alapú kamerás megfigyelő**

HÁLÓZATOK

INTRANET, INTERNET elérhetőség, hozzáférés

- 62 db gép (STN TARTOMÁNYBAN)
- HM NYÍLT INTERNET (max. 256 Kb/sec),

Internet alkalmazása:

- Minden részleg a saját helyén;
- FP a Szolnok konténer (8 db végpont);
- Internet szobában (2-2 db civil végpont; 3 db HM Internet);
- Dohányzó (1 db civil végpont)
- Log. sz. a műhelyben 2 db HM végpont.

INTRANET HÁLÓZAT

MH Intranet

- Hazai feltételek és biztosítási feladatok érvényesek
- Exchange kiszolgáló
- Nem minősített adatok továbbítására alkalmas!
- Szolgáltatások:
  - OUTLOOK (levelezés, naptár, feladatok)
  - Hálózati meghajtók (K, R,)

INTERNET HÁLÓZATOK

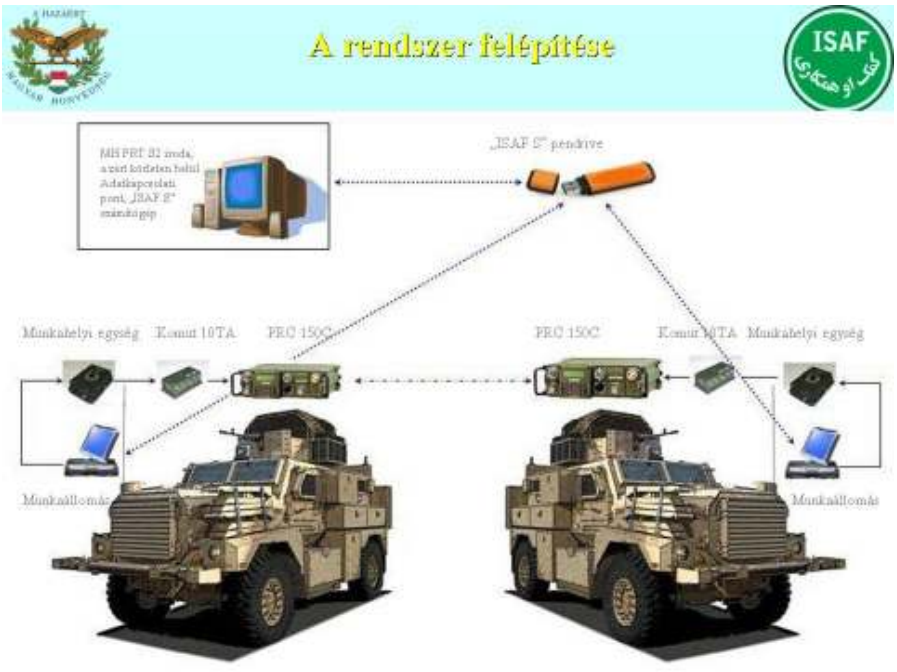
Civil internet 512/512

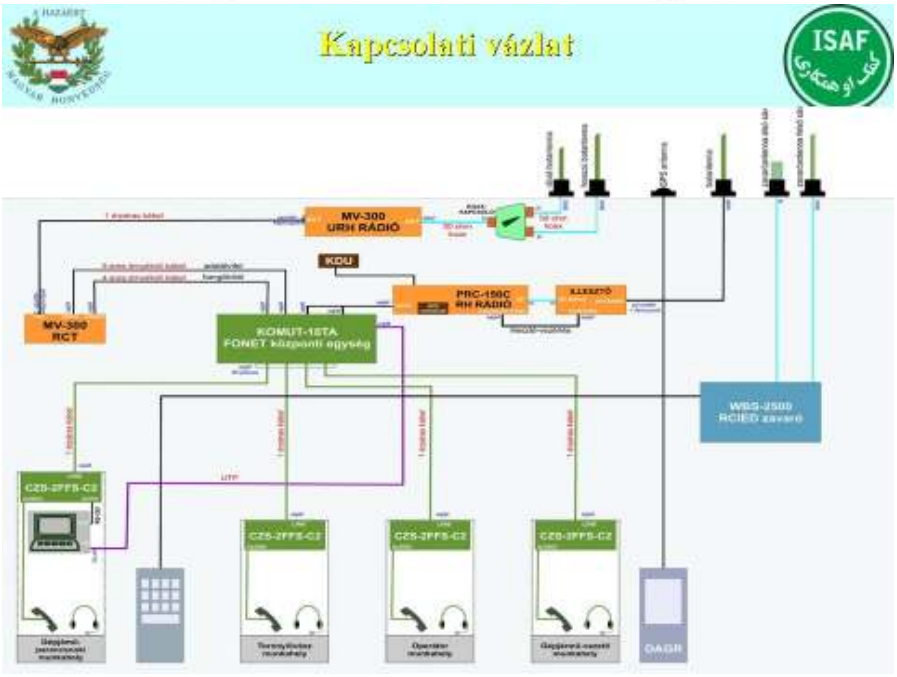
- Helyi beszerzésű szolgáltatás
- Kábeles kapcsolódás a Szolnok barakkban, Internet szobában, dohányzóban.
- A hálózat továbbosztása (wifi) TILOS! **ELLENŐRZÉS!**

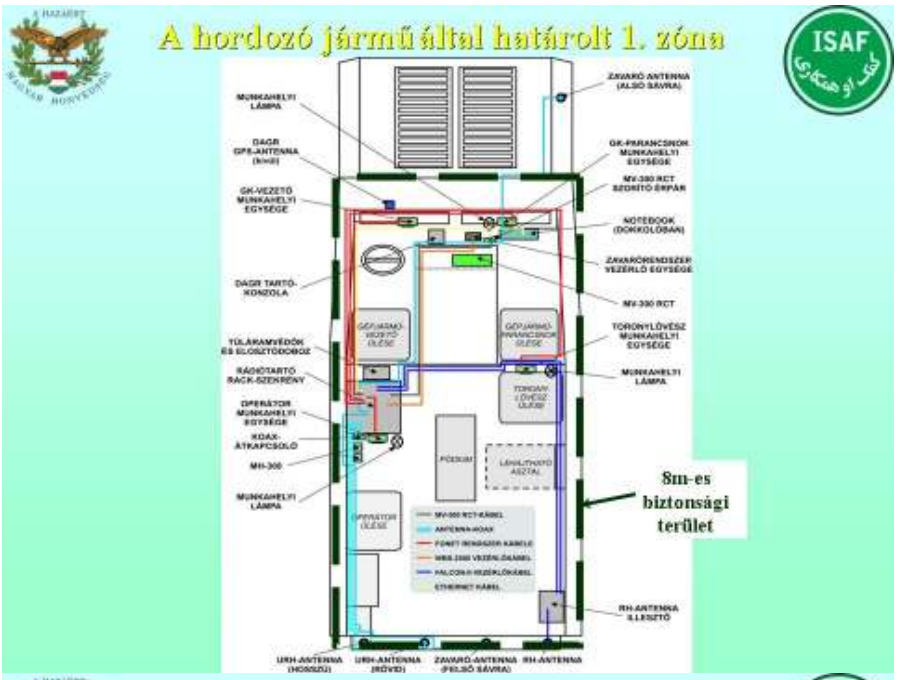
MH Internet 256/256

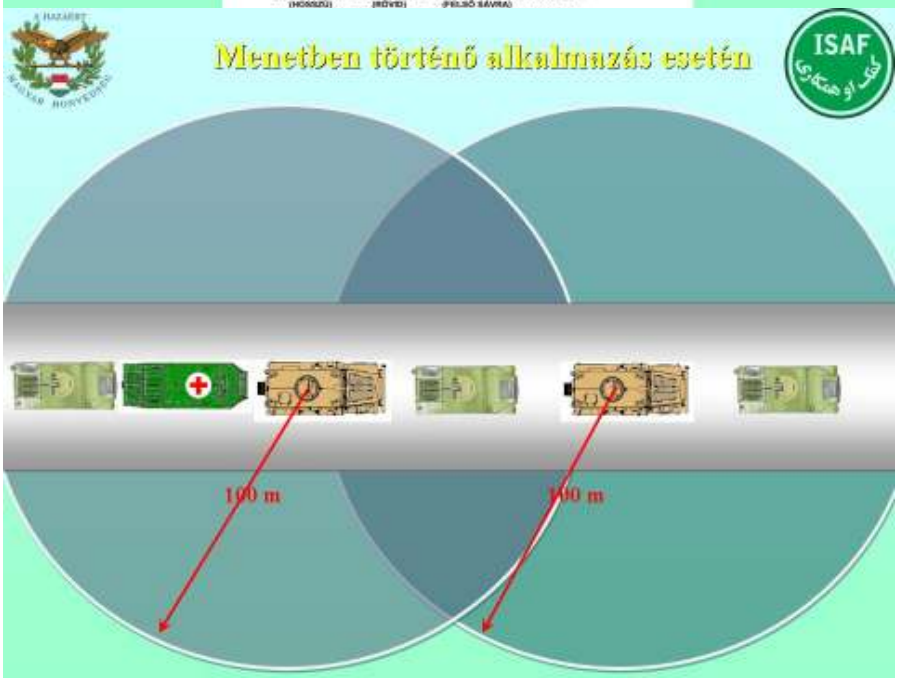
- Otthoni szolgáltatás (→ szabályok);
- Böngészésre, csevegésre;
- Munkahelyeken elérhető;
- Hazai házirend (szabályok) érvényesek.
- Távmenedzselt hálózat, csak a legszükségesebb jogokkal rendelkezünk.

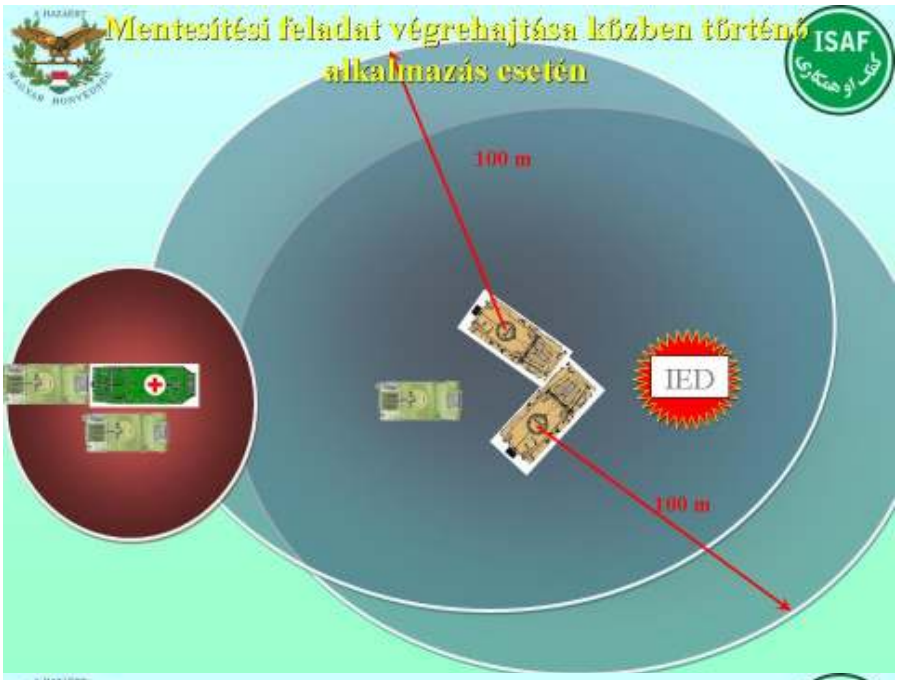
A MH 1. HTHE Afganisztáni Védelmi Ajánlások Tűzszerész Alrendszer (AVATAR) a PRT-ban


A rendszer felépítése
ISAF
„ISAF 5" pendrive
Munkahelyi egység
Komut 10TA
PRC 150C
PRC 150C
Komut 10TA
Munkahelyi egység
Munkaállomás
Munkaállomás


Kapcsolati vázlat
ISAF
MV-300
URH RÁDIÓ
KDU
PRC-150C
RH RÁDIÓ
MV-300
RCT
KOMUT-10TA
FONET központi egység
WBS-2500
RCIED zavaró
CZS-2FFS-C2
CZS-2FFS-C2
CZS-2FFS-C2
CZS-2FFS-C2
UTP


A hordozó jármű által határolt 1. zóna
ISAF
8m-es biztonsági terület


Menetben történő alkalmazás esetén
ISAF
100 m
100 m



„BLACK HOLE”

A kommunikáció korlátozása a műveletek érdekében.

Célja:

Megakadályozni az információk ki- és beáramlását illetéktelen személyek és szervezetek (pl.: sajtó) részére. Ezáltal biztosítani a vezetés, irányítás és munkavégzés „nyugodt” feltételeit.

Időt nyerni a műveletek tervezésére, információ gyűjtésre és jelentések összeállítására.

Műveletek tervezéséhez, szervezéséhez, irányításához szüksége információáramlás biztosítása, foglalt csatornák felszabadítása.

NEM AZ INFORMÁCIÓ ELHALLGATÁSA, TITKOLÓZÁS A CÉL, HANEM A PONTOS KORREKT TÁJÉKOZTATÁSHOZ, INTÉZKEDÉSEKHEZ, JELENTÉSEKHEZ SZÜKSÉGES INFORMÁCIÓGYŰJTÉS ÉS ÁRAMLÁS FELTÉTELEINEK BIZTOSÍTÁSA!

KAPCSOLATTARTÁS

A hozzátartozókkal való kapcsolattartásra 3 nyilvános távbeszélő készülékkel folyamatosan biztosított.

A telefonkészülékek a rendelkezésre álló fülkékben vannak telepítve.

A készülékeken a kapcsolattartás 24 órában biztosított Magyarországgal, személyenként max. 10 perces beszélgetési idővel!

(Kézi beszélő felemelése → KP. Jelentkezik (Bp.) → Megadni a kívánt számot→ Várni a kapcsolást → Hozzátartozót kiértesítik, „hívja a …. számot" → hívás → kapcsolás) „Türelem!"

KMCS Kapcsolattartás a magasabb szint felé

- Amerikai csoport által biztosított rendszeren keresztül
  - NIPR/SIPR
  - ISAF SECRET
  - Red phone
- Személyes kapcsolatfelvétel
  -hetente
- Nem minősített információk átadása telefonon vagy faxon

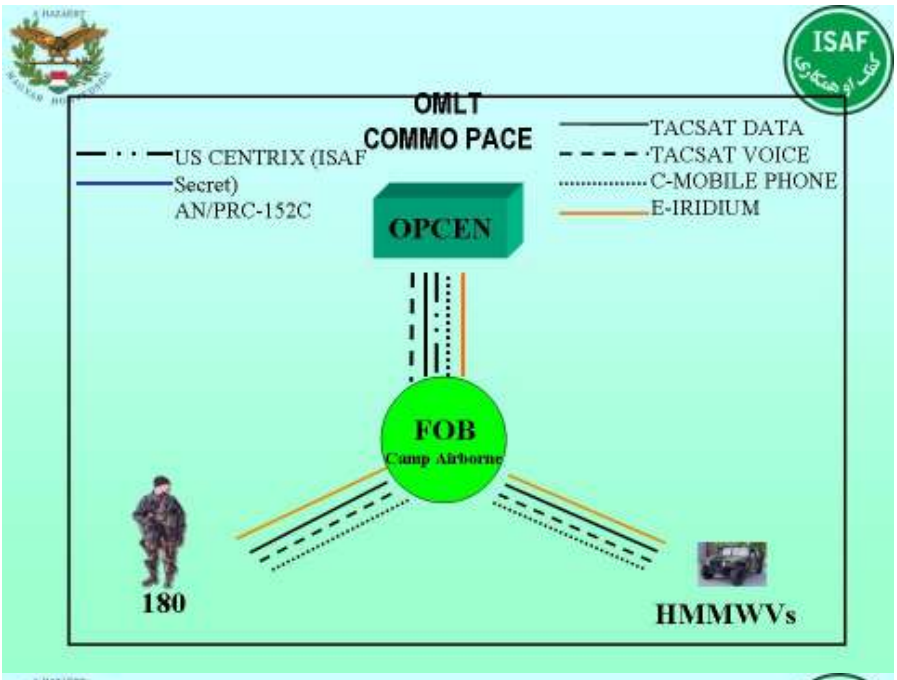
KMCS híradó eljárások

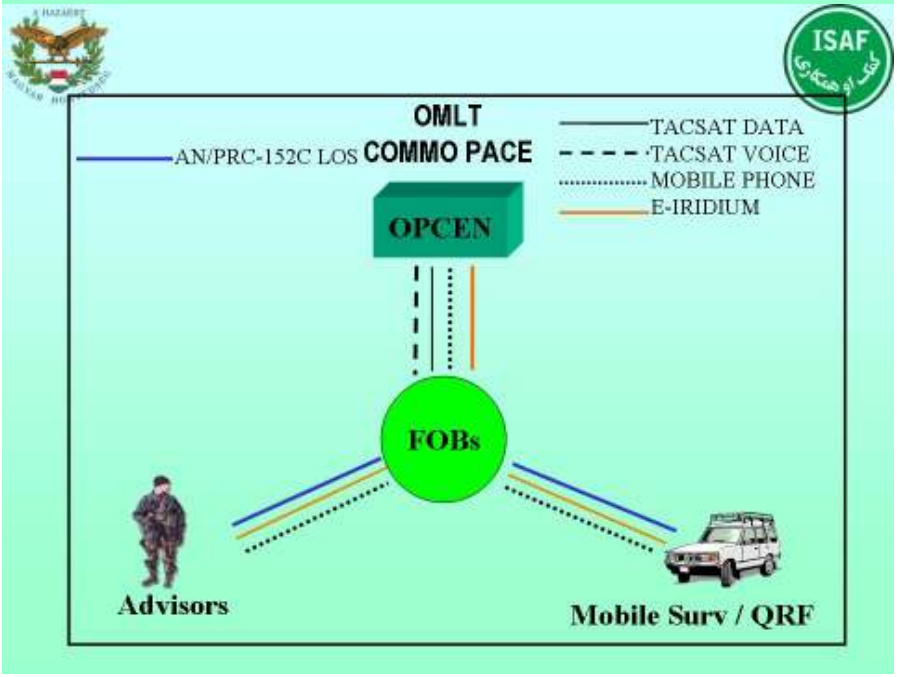
- Elsődlegesen hang kommunikáció
  - Dedikált műholdas a magasabb szint felé (AN/PRC-117F, AN/PRC-152)
  - URH a gépjárművek közt és személyenként (AN/PRC-152)
- Főleg saját szavakkal, nincs protokoll (angol)
- Előre meghatározott és beprogramozott állandó frekvenciák és csatornák
- Kapcsolat minősége helyszín és antenna függő

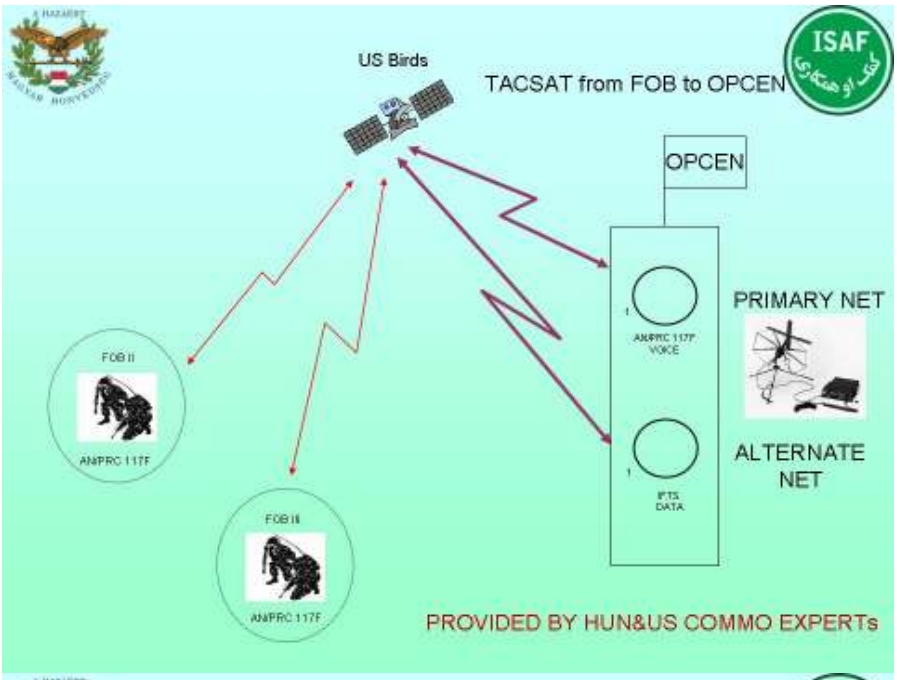
KMCS Egyéb híradó eszközök

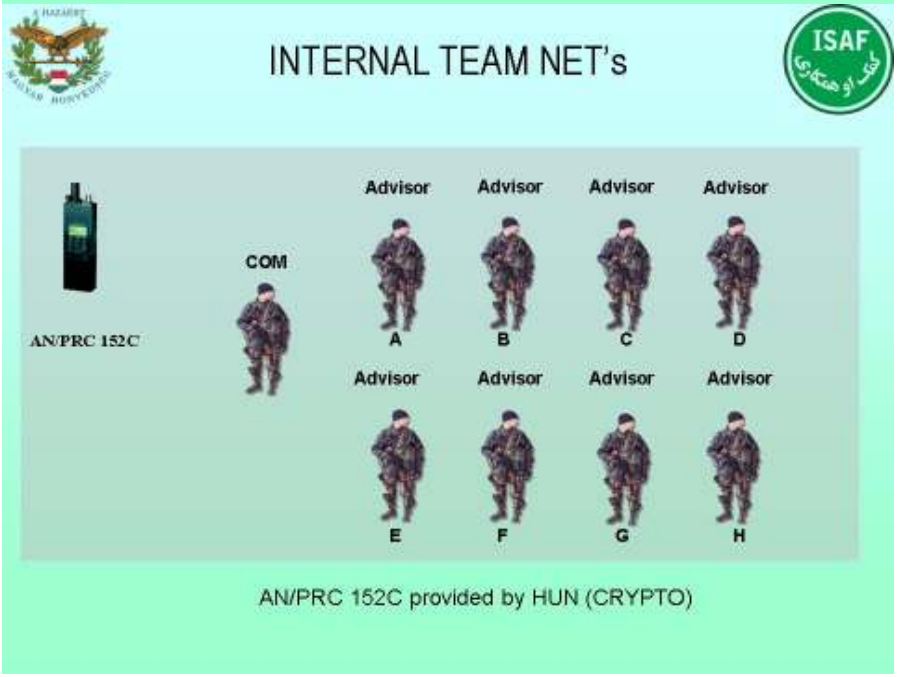
- FBCB2

- MMBJ2


ISAF
OMLT
COMMO PACE
US CENTRIX (ISAF Secret)
AN/PRC-152C
TACSAT DATA
TACSAT VOICE
C-MOBILE PHONE
E-IRIDIUM
OPCEN
FOB
Camp Airborne
180
HMMWVs


ISAF
OMLT
COMMO PACE
AN/PRC-152C LOS
TACSAT DATA
TACSAT VOICE
MOBILE PHONE
E-IRIDIUM
OPCEN
FOBs
Advisors
Mobile Surv / QRF


US Birds
TACSAT from FOB to OPCEN
ISAF
OPCEN
PRIMARY NET
ALTERNATE NET
FOB II
AN/PRC 117F
FOB III
AN/PRC 117F
AN/PRC 117F VOICE
IFTS DATA
PROVIDED BY HUN&US COMMO EXPERTs


INTERNAL TEAM NET's
ISAF
AN/PRC 152C
COM
Advisor
A
B
C
D
E
F
G
H
AN/PRC 152C provided by HUN (CRYPTO)

EMERGENCY

- IRIDIUM (INMARSAT) terminals gonna be provided to each FOBs for MEDEVAC CASEVAC;
- V-SAT terminal gonna be provided for NIPRNET only (3 Mb/s – 9 users, Ku-C band, full capacity for telephony, intranet and Internet).

Radio terminals and equipments provided by HUNGARY

terminals	*frequency*	*sets*
AN/PRC-117F	30-512 MHz	5
RF-3577-23EN LAPTOP (Panasonic CF-29/19)	-	1/6
RF-5800H-MP	1.6-59.999 kHz	5
RF-3578-CP002 PDA	-	5
Nokia	-	26
MOTOROLA 9505 SATCOM telephone	-	5
Inmarsat MINI-M	-	2
AN/PRC 152C	30-512 MHz	36
MH-300 KONGSBERG	30-88 MHz	60

OMLT
ANA Capabilities

- **PRC-1077:**
- • 30 to 88 MHz, 25 kHz Steps
- • 10 Programmable Memory
- Channels
- • Rugged, Completely Immersible
- • Manpack/Mobile/Base
- Configurations
- • 2/5/50 Watts

OMLT

- **PRC-1099:**
- The radio operates from 1.6 to 30 MHz with a maximum power output of 20 W. The internal automatic antenna tuner is fairly wide range, but a series connected outboard doorknob capacitor is recommended for long random wires. The rig operates from "ham friendly" 12 V dc.

OMLT

- PRC-1070:

Datron's PRC1070 is 2W portable squad radios that offer handheld tactical communications capability in the 30 to 88 MHz band in 25 kHz steps. The radios have 2,320 available channels and up to nine preset-able memory channels.

OMLT tapasztalatok

- - nagy fokú „ szakmai" leterheltség (híradó, rejtjelző, informatika, elektronikai harc, internet)
- - ANA híradó eszközeinek ismerete, „ ismeretlensége",
- - kettős feladat rendszer (toronylövész esetleg sofőr),
- - ISAF secret szg. hiany.

Az MH NTE és az elöljáró közötti kapcsolattartás híradó/ informatikai eszközeinek lehetősége:

- **VSAT műholdas rendszeren keresztüli MH távhívó rendszer,**
- **Intranet és Internet kapcsolatok,**
- **A NATO ISAF által biztosított NCN kapcsolat,**
- **INMARSAT, IRIDIUM egyedi műholdas eszközök,**
- **Hazai (magyarországi), vagy helyi GSM rádiótelefonok,**
- **ISAF SECRET minősített munkaállomás.**

MH KAIA TTCS

Az összeköttetések biztosítását a felelőssége alá tartozó épületkomplexumokban a műveleti elöljáró által kiépített vezetékes vonalakon (NATO NCN), GSM mobiltelefonokon és IRIDIUM műholdas telefonon valósítja meg.


ISAF
KÉRDÉS?
Köszönöm a figyelmet!

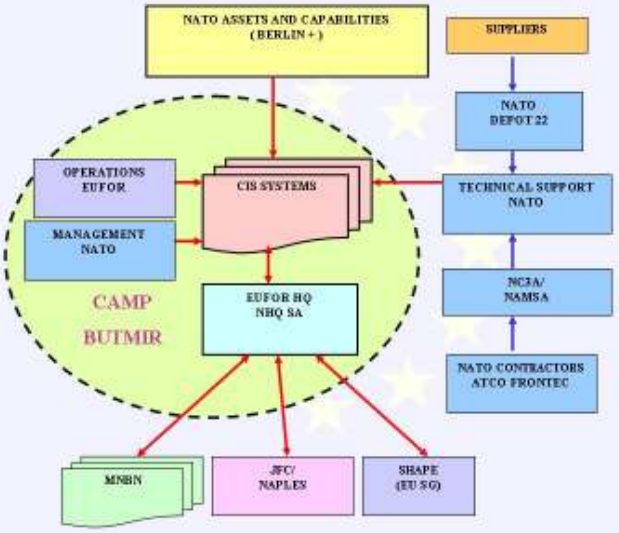
MÉSZÁROS Sándor

EUFOR OPS ALTHEA CIS SUPPORT

CIS MISSION

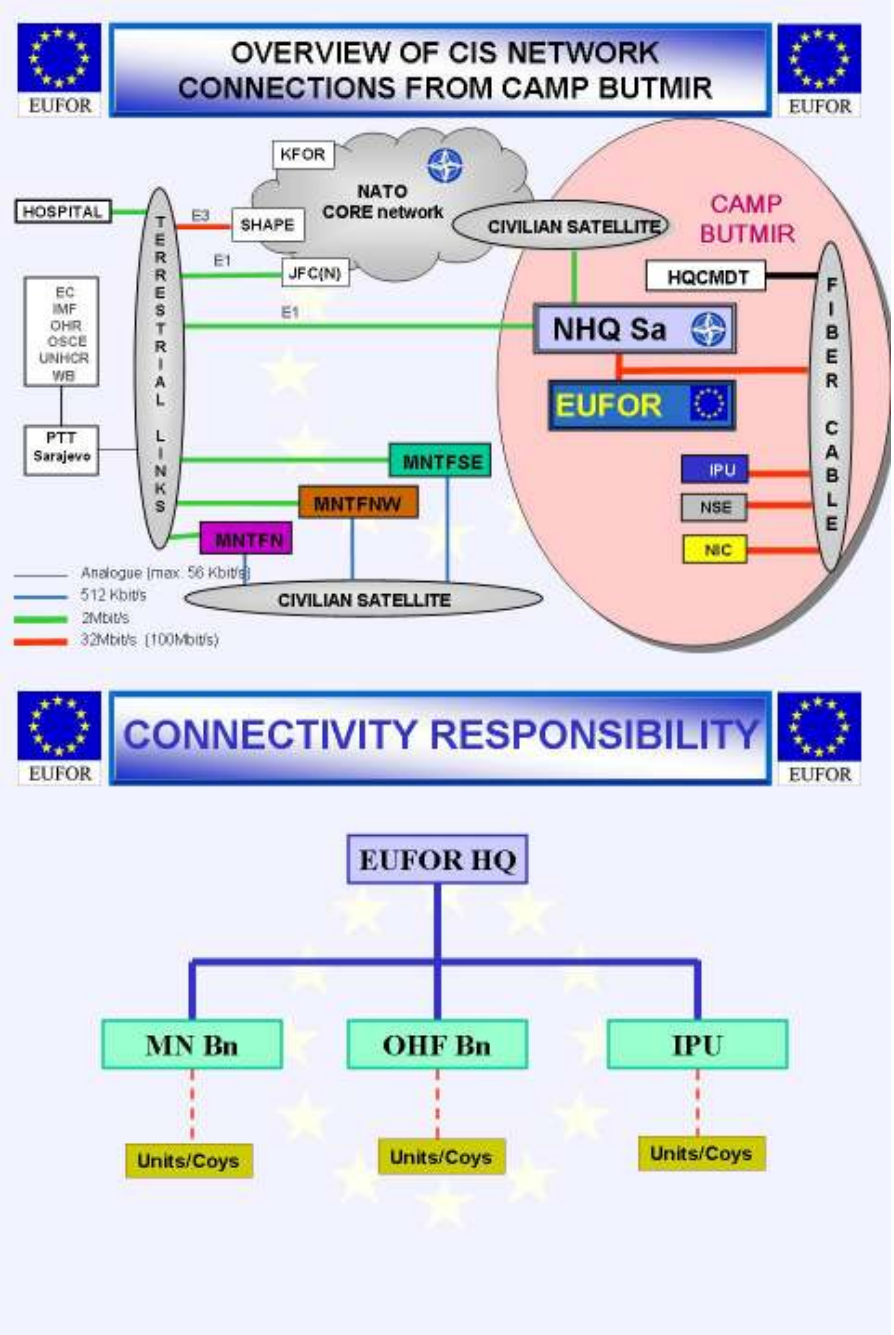
- Provide a reliable and robust CIS connectivity, both secure and non-secure, conforming to OP ALTHEA OPORD and STANAG 5048.
- Support C2 system for COMEUFOR and deployable units TCP on area of operation.
- Maintain secure, robust and reliable connectivity from HQ EUFOR to the RCC, LOT and HUMINT Houses in accordance with the Operational Commanders OPLAN

GENERAL CIS STRUCTURE




EUFOR
SERVICES AT EUFOR HQ
EUFOR
Telecom services:
– Non-secure voice and fax (including DECT & pagers)
– Secure voice and fax
– Non-secure GSM
– Secure GSM
EUFOR CIS services
NATO CI6 services
Information systems:
– EUFOR secret LAN
– NATO secret LAN (access to NATO databases)
– Non-secure: GALAXY, connected to Internet
VTC: secure connection to higher NATO HQs
TLK: classified and unclass. voice and data transmission capability up to MS level
TACSAT comms: secure/non-secure voice/data transmission up to NS level


EUFOR
EUFOR HQ – CIS ACTIVITIES
EUFOR
Co-ordinate with RCC/LOT/HUMINT, MN Bn and OHF Reserve Bn for all CIS issues:
– Frequency Management
– COMSEC / Crypto
– TACSAT (Channel allocation and equipment)
– TLK (Theatre Liaison Kit) establishment
– GSM Unsecure Phones allocation
– GSM Satellite phones (TURAYA three -band "GSM/SAT Phones") procurement
– Secure comms. assets with Sectra Tiger XS – up to NATO Confidential level
– EUFOR SECRET WAN / EUFOR Non-Secure Galaxy LAN
– SharePoint portal services
– CIS assets and PC support for EUFOR HQ and RCC/LOT/HUMINT houses


EUFOR
OVERVIEW OF CIS NETWORK CONNECTIONS FROM CAMP BUTMIR
EUFOR
KFOR
NATO CORE network
HOSPITAL
E3
SHAPE
CIVILIAN SATELLITE
CAMP BUTMIR
E1
JFC(N)
HQCMDT
EC
IMF
OHR
OSCE
UNHCR
WB
E1
NHQ Sa
TERRESTRIAL LINKS
FIBER CABLE
EUFOR
PTT Sarajevo
MNTFSE
IPU
MNTFNW
NSE
MNTFN
NIC
Analogue (max. 56 Kbit/s)
512 Kbit/s
2Mbit/s
32Mbit/s (100Mbit/s)
CIVILIAN SATELLITE
EUFOR
CONNECTIVITY RESPONSIBILITY
EUFOR
EUFOR HQ
MN Bn
OHF Bn
IPU
Units/Coys
Units/Coys
Units/Coys

RCC AND LOT HOUSES

EUFOR
'Strategic CIS Reserve'

1x IPN
1x STU IIB (secret level)
1x ACID W/S (restricted level)
1x INTERNET W/S

EUFOR CIS ASSETS

TACSAT Network

TACSAT NETWORK

Tactical Satellite radio.

PRC 117 F

AN/PRC 117F
- DLOS VHF can be plain or secure voice.
- can only be used in secure modes over Satellite.
- robust and portable.
- can be used both man packs and vehicle mounting.

The TACSAT network covers the whole of BiH area and by using satellites removes the problem of the mountainous terrain.

MN Bn CONNECTIVITY

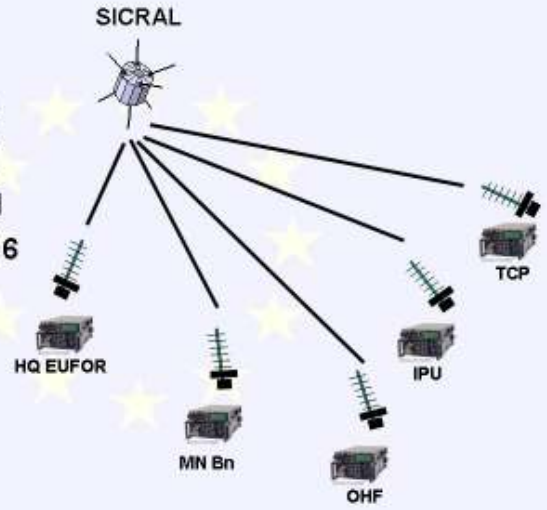
HQ EUFOR to MN Bn HQ

ES WAN	(3 Workstations)
IPN	(23 phones)
STU IIB	(1 phone)
TACSAT	(As required)
TLK	(1 set)

SATCOM CONNECTIVITY

HICOM Network

- Provided by NATO
- 1 x 25kHz Channel
- Wideband Channel
- EUFOR = Priority 16

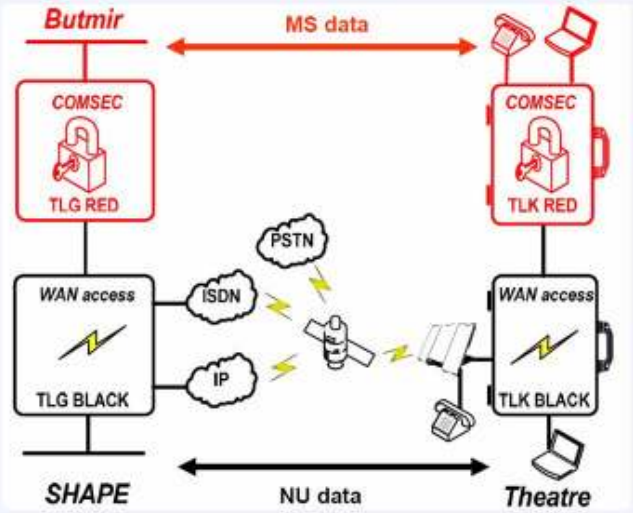


EUFOR CIS ASSETS

Theatre Liaison Kit (TLK)

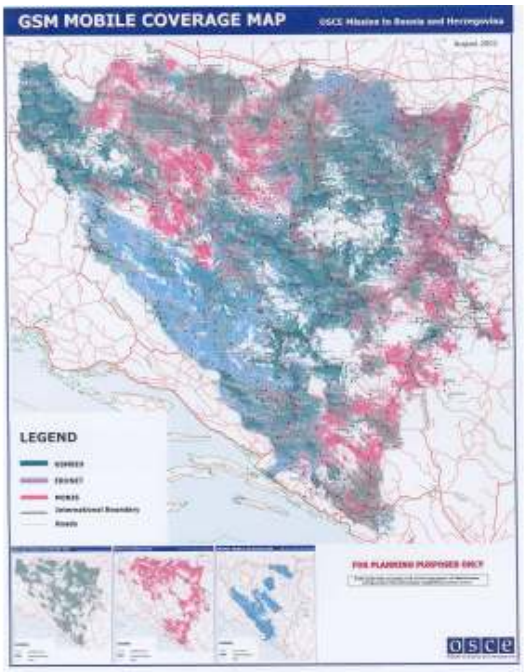
Theatre Liaison Kit (TLK)

TLKs SERVICES




EUFOR CIS ASSETS
EUFOR
EUFOR
GSM Mobile
non secure
GSM NETWORK
EUFOR
EUFOR
3x GSM operators in BiH
GSM BiH (Bosnian)
ERONET (B-Croat)
MOBIS (B-Serb)
non secure

GSM coverage



EUFOR

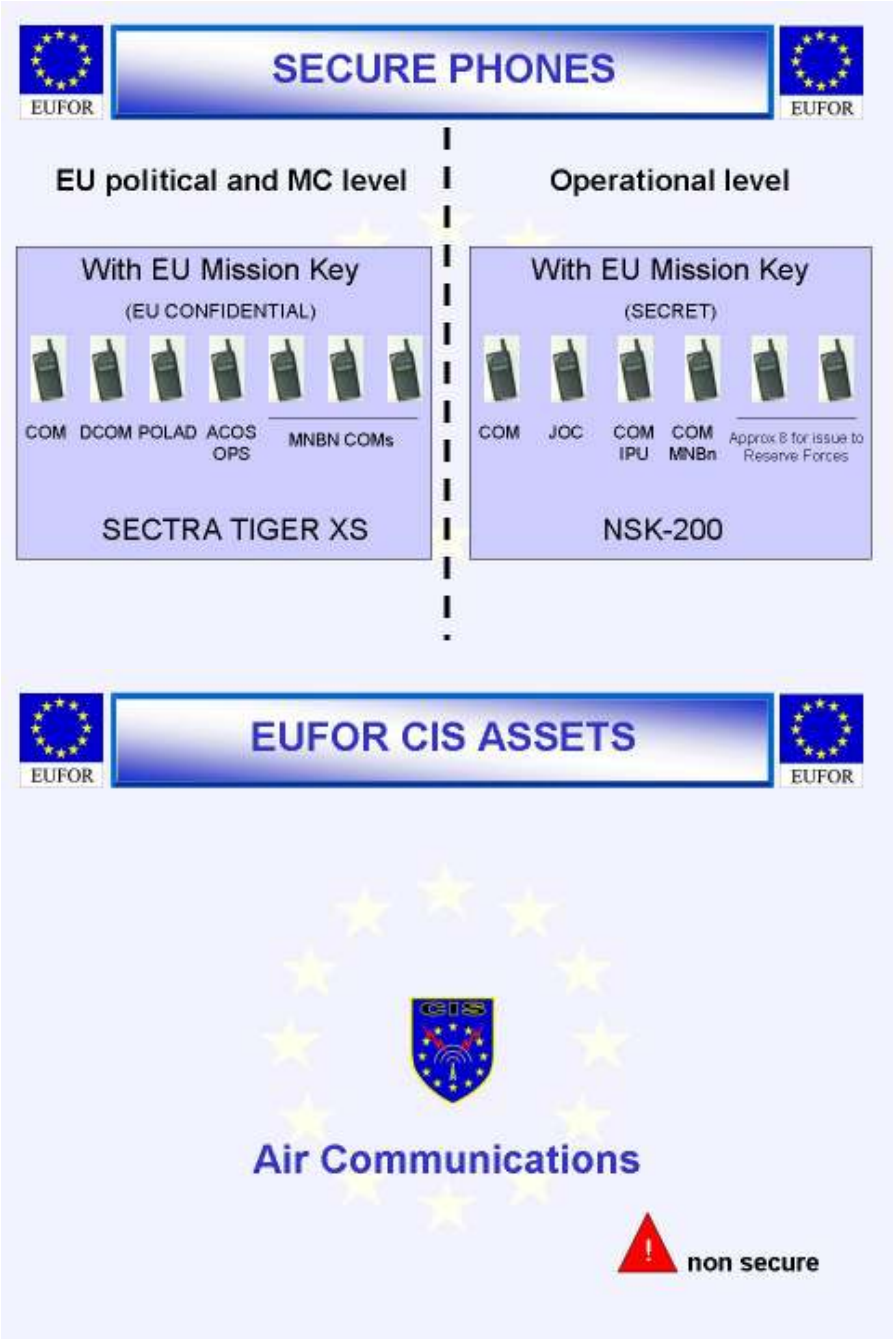
GSM NETWORK

EUFOR

9x TURAYA GSM Satellite phones

- Issued as required.
- Over The Horizon Reserve Force (OTHF) would be high priority.

non secure


EUFOR
SECURE PHONES
EUFOR
EU political and MC level
Operational level
With EU Mission Key
(EU CONFIDENTIAL)
COM
DCOM
POLAD
ACOS OPS
MNBN COMs
SECTRA TIGER XS
With EU Mission Key
(SECRET)
COM
JOC
COM IPU
COM MNBn
Approx 8 for issue to Reserve Forces
NSK-200
EUFOR
EUFOR CIS ASSETS
EUFOR
CIS
Air Communications
non secure


AVIATION ASSETS
EUFOR
EUFOR
2 x CHE Cougar
3 x IT AB - 205
2 X DEU UH - 1D
BELL
MEDEVAC
2 x SVK MI-17
AIR TO AIR
EUFOR
EUFOR
130.8 MHz
Vlasic
130.8 MHz
Plocno
5 GHz
5 GHz
130.8 MHz
Bukovic
5 GHz
H
Archer Base
130.8 MHz
Helo to Helo transmissions are line of sight only although the transmission will also go through the net.
Helo to Ground transmissions are carried through Bukovic to Archer Base Helipad.

EUFOR

HELICOMS COVERAGE

EUFOR

80% of Bosnia covered

EUFOR

THEATRE FREQUENCY MANAGEMENT CELL (TFMC)

EUFOR

CIS

Frequency Management

FREQUENCY REQUIREMENTS

Frequency requirements !

- Intra unit (Tactical radios)
- Intra theatre comms (HQ EUFOR, MN Bn, etc)
- National comms (HF, SATCOM)

FREQUENCIES

Military and Civilian Bands:

- **TFMC** (Theatre Frequency Management Cell)
  -- 7 days notice required.
- **CRA** (Civilian Regulatory Agency)
  -- 90 days notice required.

THEATRE FREQUENCY MANAGEMENT CELL (TFMC)

Applying for frequencies:

- Complete 14 Point Request Form
- Send it to EUFOR TFMC via national NARFA (National Allied Radio Frequency Agency)

HUN NATIONAL CIS CAPABILITY

MN Bn A-Coy

CIS STAFF AND ASSETS

CIS section – 5 personnel

CIS Assets – 3x NCN (2x phone, 1x fax)
- Panasonic KXT-7436
- RF-5200/150W HF radio
- 1x T-Mobile GSM
- 13x BiH GSM (6 pre-paid)
- 1x INMARSAT Mini-"M" SATCOM
- 7x IRIDIUM SATCOM
- non-secure LAN (with Internet access)
- 23x MV-300 Kongsberg MRR

QUESTIONS?


Thank You for Your Attention!

Bertrand GIFFAULT

FRENCH CIS OPERATIONAL DEPLOYMENTS

- The state of terrestrial forces CIS

- Which networks
  - A main one used primarily under optimal conditions.
  - A secondary network used when the principal one does not function.
  - An emergency network exploited when the nominal networks are not available

- Which Information Systems
  - NATO Secret.
  - NATO "Unsecured".
  - Mission Secret
  - French unsecured
  - Special France support
  - Special France in theatre

Deployment constraints

- Context of engagement
- Nature of the operation
- Level of committed forces


Deployment constraints: Haiti
HAITI

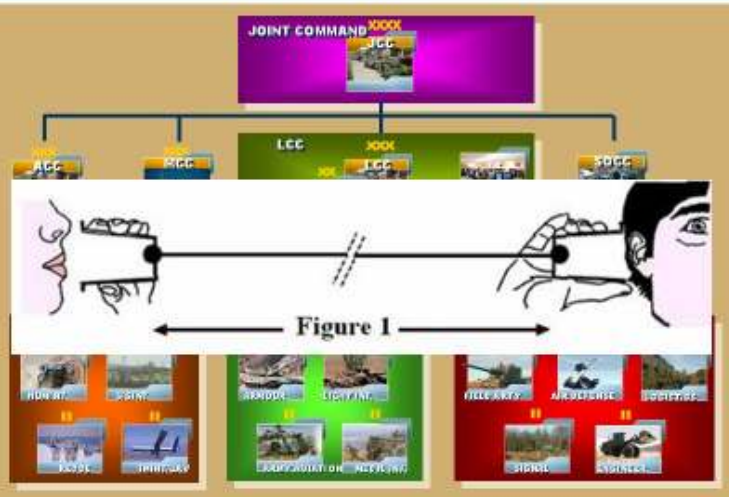

IMPLANTATIONS DES STATIONS INMARSAT
LICORNE
ONUCI
6 M4
3 SAT B
1 M4 à venir
1 SAT B à venir
GFS
7 M4
2 SAT B
12 MINI M
GUINEE
KORHOGO
1 M4 (PC)
1 MINI M
(INF)
NIAKARAMANDOUGOU
1 SAT B (PC)
BOUAKE
M4 (PC TAC)
LYNX (PC)
PAKOUABO
1MINI M
GTIA 1
GUEZON
1 MINI M
(EVS)
BANGOLO
1 M4
GUIGLO
1 M4
DETGE
KOKUMBO
1 LYNX
(ACA)
COTE D'IVOIRE
GHANA
ABIDJAN
1 MINI M
(PC BIMa)
1 MINI M
(GEND)
SAN PEDRO
1 LYNX
ABIDJAN
1 M4 PC TAC
1 M4 en rép
1 MINI M INF
1 M4 DETGE
1 SAT B CENTRS

Deployment constraints: Ivory Coast

Deployment constraints

- Evolution of communication system in operations

Conclusion

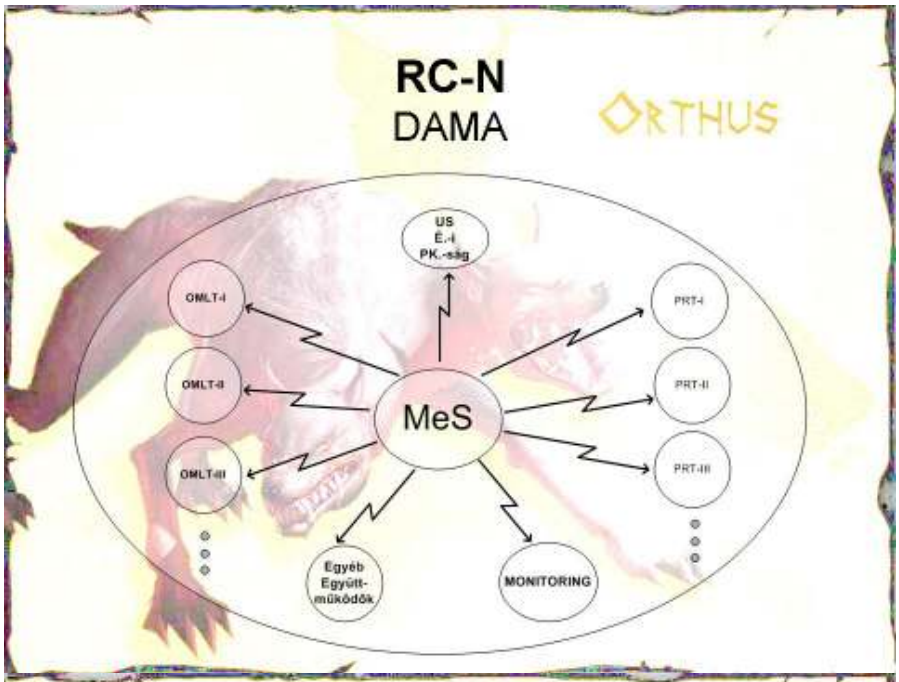


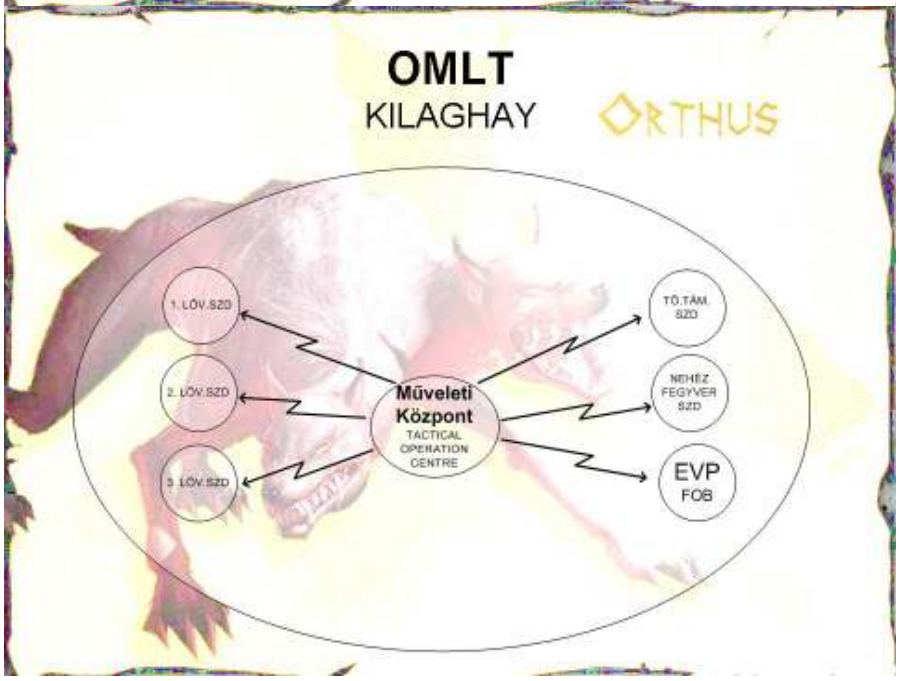
CSAVAJDA József

OPERATION MENTOR AND LIASON TEAM


OMLT
Híradása
ORTHUS
OMLT híradásának tagozódása
US
Csak a rádió és híradó eszközök felsorolása, fényképeiknek bemutatása
ISAF
- Rádióhíradás & műholdas & RH & URH
- Távbeszélő Ök. & mobil & műholdas
- Követő berendezések
- Zavaró berendezések
MH
- rádióhíradás
- műholdas, vezetékes
-mobiltelefon


ISAF
Műholdas rádióhíradás rendszere
ORTHUS
DAMA
Afganisztán
RC-N
RC-C
RC-E
RC-W
RC-S


RC-N
DAMA
ORTHUS
US
É.-i
PK.-ság
OMLT-I
OMLT-II
OMLT-III
MeS
PRT-I
PRT-II
PRT-III
Egyéb
Együtt-
működők
MONITORING


OMLT
KILAGHAY
ORTHUS
1. LÖV.SZD
2. LÖV.SZD
3. LÖV.SZD
Műveleti
Központ
TACTICAL
OPERATION
CENTRE
TŰ.TÁM.
SZD
NEHÉZ
FEGYVER
SZD
EVP
FOB


US Felszerelés
ORTHUS
ISAF felszerelés
Magyar felszerelés, amerikai segélyből


URH
Rádióforgalmi Rendszer
ORTHUS
URH
C2
TOC
FONTOS!
Együttműködő frekik
Elöljáró frekik
CAS
MEDEVAC

A magyarok által használt URH eszközök

ORTHUS

A nemzeti gárdától, de örökbe

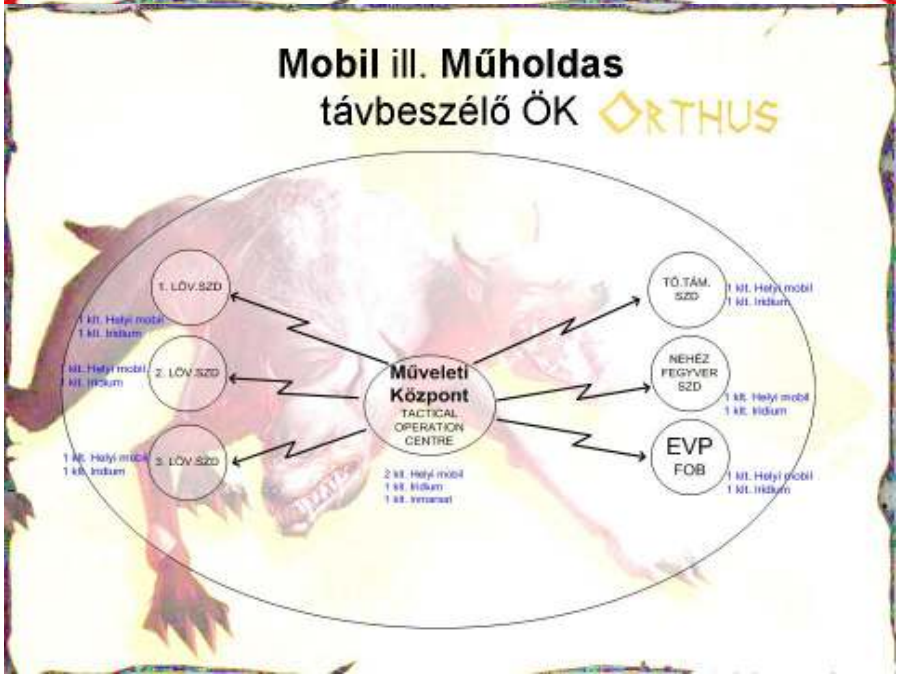
Amerikai féltől

„**kölcsön**" kapott

Az amerikaiak által használt URH eszközök

ORTHUS


ORTHUS
RH
Rádióforgalmi Rendszer


Mobil ill. Műholdas
távbeszélő ÖK
ORTHUS
1. LÖV.SZD
1 klt. Helyi mobil
1 klt. Iridium
2. LÖV.SZD
1 klt. Helyi mobil
1 klt. Iridium
3. LÖV.SZD
1 klt. Helyi mobil
1 klt. Iridium
Műveleti Központ
TACTICAL OPERATION CENTRE
2 klt. Helyi mobil
1 klt. Iridium
1 klt. Inmarsat
TÜ.TÁM. SZD
1 klt. Helyi mobil
1 klt. Iridium
NEHÉZ FEGYVER SZD
1 klt. Helyi mobil
1 klt. Iridium
EVP FOB
1 klt. Helyi mobil
1 klt. Iridium

- Előny: egyszerű kezelhető, nem igényel szaktudást
- Hátrány: CSAK NYÍLT adatok továbbítására alkalmazható
  a kint használt mobilok átlag életkora 8 ÉV!
  a megváltozott, és a felhasználási körülmények miatt gyors elhasználódás
- Javaslat: Sectera típ. titkosítóval ellátott mobiltelefonok beszerzése (min. 2 db)

ORTHUS

por, csepp és ütésálló mobilok beszerzése és alkalmazása,
tartalék eszközök és felszerelések biztosítása,
900/1800/1900 Mhz-es jelerősítő a mobiltelefonokhoz

IFTS & BFTS

ORTHUS

- Nyomkövető
- Segélyhívó
- Üzenet és adadtküldő berendezések
- alkalmazásuk zárt üzemmódot tesz lehetővé
- A két típusú eszköz egymással csak a láthatóságot biztosítja

Javaslat: ezen eszközökhöz is beépítőkeret biztosítása

JAMMER

ORTHUS

Zavaró berendezések, amelyek egy adott frekvencia tartományt lefognak, így megakadályozva a nem kívánt összeköttetés létrejöttét, vagy egy mobiltelefonnal, civil frekvenciát használó rádióval szerelt IED aktiválását.

Az OMLT sajnálatos módon csak gjmű-be szerelt zavaró eszközökkel rendelkezik, abból sem elegendő mennyiséggel, és minőséggel.

Előnye: Adott esetben megóvja az emberi életet (még a katonáét is!)
Hátrány: Nagy helyigény, viszonylag érzékeny a sivatagi körülményekre

Javaslat: egy korszerűbb Jammer típus alkalmazása
takarítás
a „gyalogjárőr"-t alkalmazó alegységek felszerelése háti zavaróval (PRT...)

Titkosítás

Zárt üzemmód biztosítása

ORTHUS

- A rádiók esetében a használt eszköz a **KYK-13**
  6 db kulcs egyidejű tárolására és töltésére alkalmas

Előnye: egyszerű használat
Hátránya: belső elem, inkább csak töltőként használandó, nem tárolóként

- Jammerek kulccsal való feltöltése (**US SECRET**)

- IFTS/BFTS ált.-ban műholdon keresztül, vagy személyesen


MAGYAR HONVÉDSÉG
ORTHUS
• Rádió híradás: 0
• Mobiltelefon: 2 kit. honvédségi díjcsomag
• Műholdas, vezetékes híradás: VSAT
amit biztosít: - HM vonalak (jogosultságtól függően mobil, vagy IVSN is hívható)
- INTRANET
- INTERNET (honvédségi)
- HOT-LINE
- titkos vezetékes összeköttetés
Satellite
VSAT Remote Sites
HUB Station
Host Computer
HUB Equipment
Outdoor Unit
Indoor Unit
User's Terminal
• Send • Receive
• Send • Receive


Készítette:
Csavajda J. Rajmund szds.


KÉRDÉS?
ORTHUS
NINCS
KÖSZÖNÖM
IGN.COM

MIHÁLYI Gábor

EDR A SZÁMOK TÜKRÉBEN

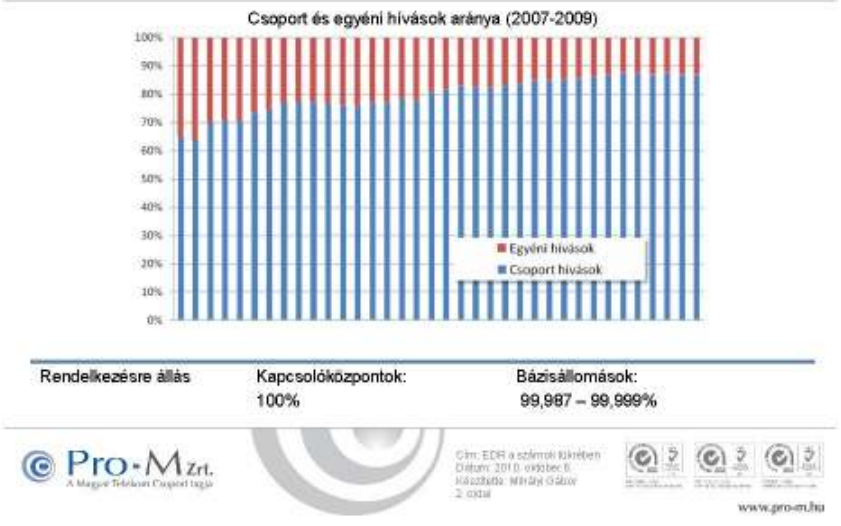
Pro-M Zrt.
A Magyar Telekom Csoport tagja

EDR a számok tükrében

Ügyfél-elégedettség mérés: eredmények és tapasztalatok

Mihályi Gábor
Műszaki- és Üzletfejlesztési Igazgató
Pro-M Zrt.

Tények



Rendelkezésre állás	Kapcsolóközpontok:	Bázisállomások:
	100%	99,987 – 99,999%

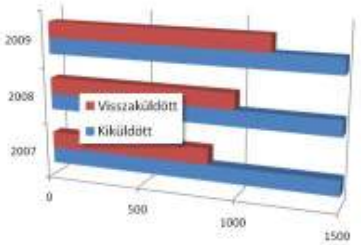
A felmérés körülményei

„A Szolgáltató évente legalább egyszer köteles felmérést készíttetni arról, hogy a Felhasználók mennyire elégedettek a Szolgáltató által nyújtott szolgáltatásokkal"

Évente végrehajtott felmérés

Fontos visszajelzési csatorna

Szerződéses előírás



Mi befolyásolja az elégedettséget? - 2007

Mi befolyásolja az elégedettséget? - 2008

Pro-M zrt.
A Magyar Telekom Csoport tagja

Cím: EDR a számok tükrében
Dátum: 2010. október 6.
Készítette: Mihályi Gábor
3. oldal

www.pro-m.hu

Mi befolyásolja az elégedettséget? - 2009

Pro-M zrt.
A Magyar Telekom Csoport tagja

Cím: EDR a számok tükrében
Dátum: 2010. október 6.
Készítette: Mihályi Gábor
4. oldal

www.pro-m.hu

I. Alap és rendszerszolgáltatások

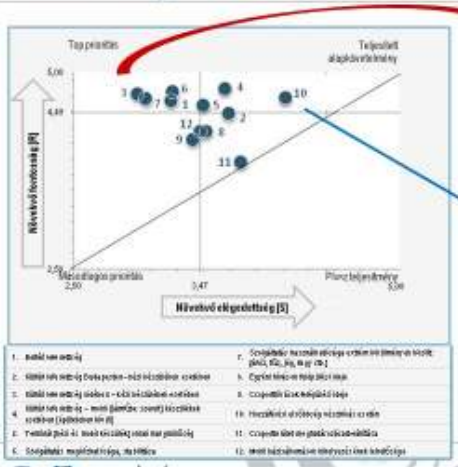
Kültéri lefedettség (mobil, vidék kézi, Budapest kézi)
Szolgáltatás megbízhatósága, stabilitása
Hozzáférési elsőbbség vészhívás esetén
Szolgáltatás használhatósága extrém körülmények között
Beltéri lefedettség
Terminál oldali hangminőség
Egyéni hívások felépülési ideje
Mobil bázisállomások kihelyezésének lehetősége
Csoporthívások felépülési ideje
Csoportterület meghatározása/beállítása

Pro-M Zrt.
A Magyar Telekom Csoport tagja

Cím: EDR a számok tükrében
Dátum: 2010. október 6.
Készítette: Mihályi Gábor
7. oldal

www.pro-m.hu

Szolgáltatáselemek fontossága és az ezekkel való elégedettség



- **Továbbra is a legkomolyabb probléma a vidéki kültéri lefedettség kapcsán merül fel [kézi készülékkel] [a mélyinterjúk szerint Bp-en jobb a helyzet]**
- **Problémás a szolgáltatás extrém körülmények közötti használhatósága is.**
- **Hozzáférési elsőbbség relevanciája és a vele való elégedettség is magas.**
- **A tényező többsége mind a fontosság, mind az elégedettség tekintetében az átlag körül helyezkedik el, a válaszadók kevéssé differenciálnak.**

Pro-M Zrt.
A Magyar Telekom Csoport tagja

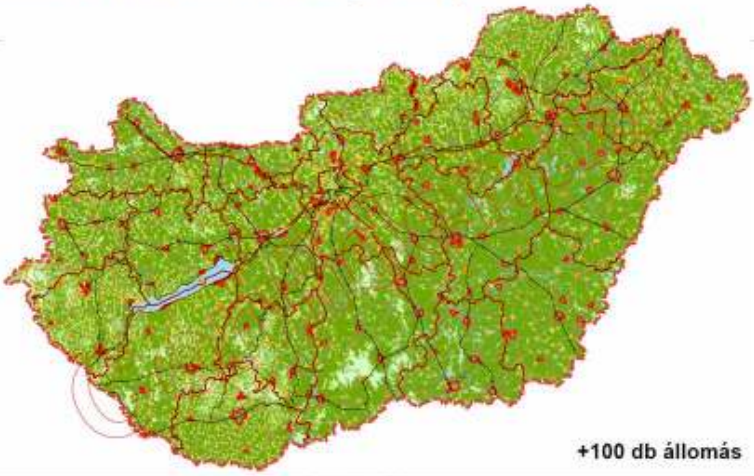
Cím: EDR a számok tükrében
Dátum: 2010. október 6.
Készítette: Mihályi Gábor
8. oldal

www.pro-m.hu

Kültéri lefedettség – lehetőségek

Lehetőségek	Kézi kültéri %	Mobil kültéri %
+0 db TBS	86,5	99,1
+15 db TBS	88,0	99,2
+35 db TBS	89,9	99,4
+60 db TBS	91,4	99,5
+100 db TBS	92,6	99,6

Modellezett lefedettség térképek



Lefedettség intézkedések

Gateway és repeater telepítések

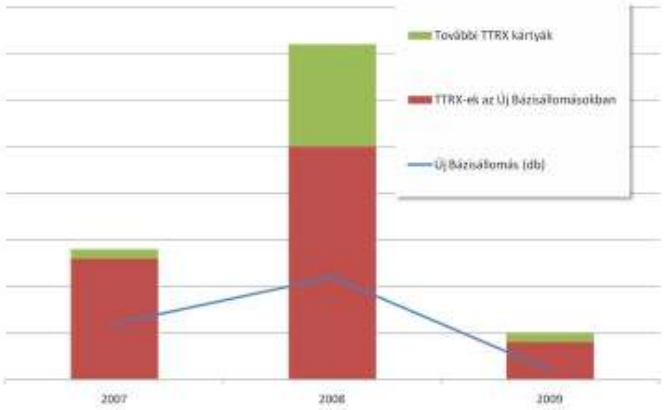
Újdonság: piko-repeater

Pro-M zrt.
A Magyar Telekom Csoport tagja

Cím: EDR a számok tükrében
Dátum: 2010. október 6.
Készítette: Mihályi Gábor
11. oldal

www.pro-m.hu

Lefedettség fejlesztések (kivonat) – 1

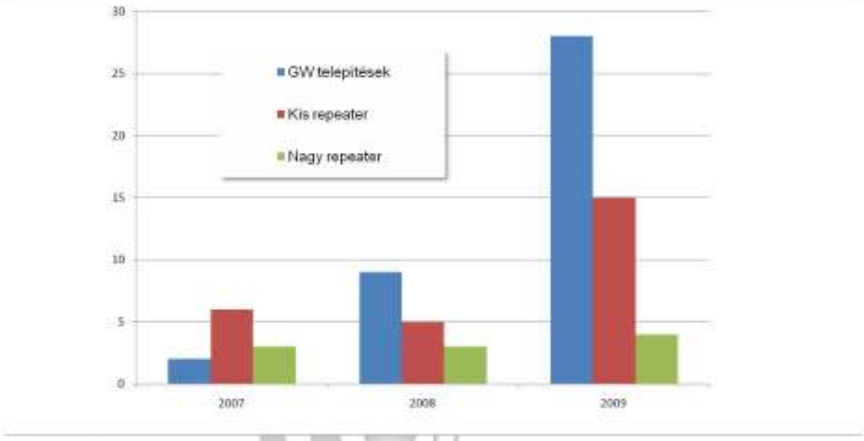


Pro-M zrt.
A Magyar Telekom Csoport tagja

Cím: EDR a számok tükrében
Dátum: 2010. október 6.
Készítette: Mihályi Gábor
12. oldal

www.pro-m.hu

Lefedettség fejlesztések (kivonat) – 2

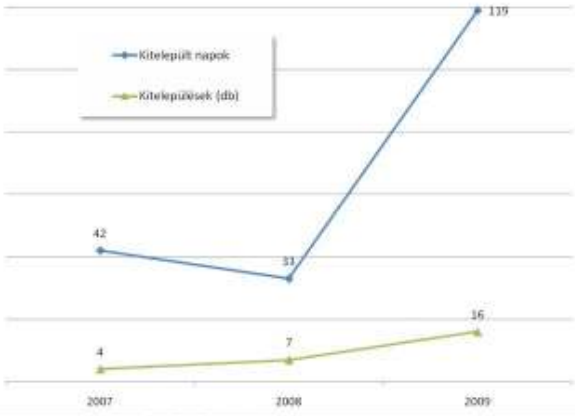


Pro-M zrt.
A Magyar Telekom Csoport tagja

Cím: EDR a számok tükrében
Dátum: 2010. október 6.
Készítette: Mihályi Gábor
13. oldal

www.pro-m.hu

Mobil bázisállomás kitelepülések



Pro-M zrt.
A Magyar Telekom Csoport tagja

Cím: EDR a számok tükrében
Dátum: 2010. október 6.
Készítette: Mihályi Gábor
14. oldal

www.pro-m.hu

Újdonságok az Ügyfélkapcsolatban

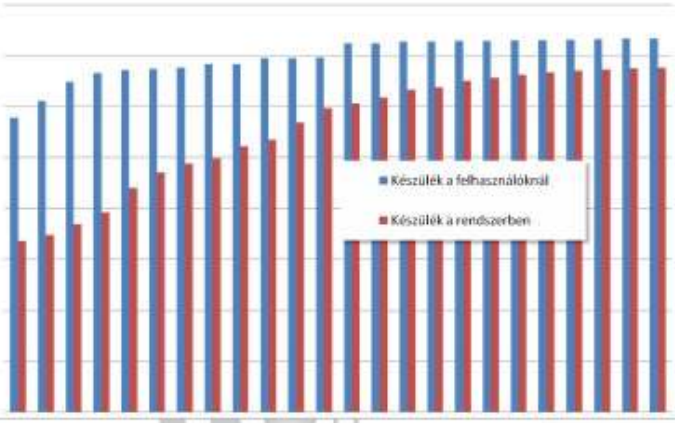
- Hírlevél
- E-learning: szervezet-specifikus tananyagok
- Pro-M szakemberei személyes részvétellel és előadással segítik a helyi oktatásokat
- Készülékjavítás: budapesti szállítások közvetlenül (min 1 nap átfutási idő csökkentés)

Pro-M Zrt.
A Magyar Telekom Csoport tagja

Cím: EDR a számok tükrében
Dátum: 2010. október 6.
Készítette: Mihályi Gábor
15. oldal

www.pro-m.hu

Rádiókészülékek a felhasználóknál

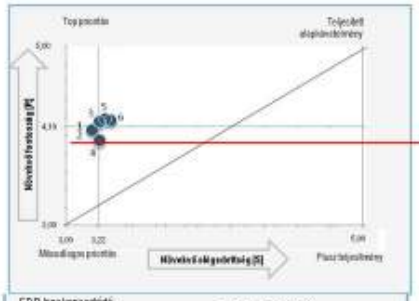


Pro-M Zrt.
A Magyar Telekom Csoport tagja

Cím: EDR a számok tükrében
Dátum: 2010. október 6.
Készítette: Mihályi Gábor
16. oldal

www.pro-m.hu

Információnyújtás, képzés



- Az információnyújtás és képzés minden vizsgált dimenziójával elégedetlenebbek a válaszadók, mint amilyen fontosnak tartják őket.
- Leginkább kritikus pontnak az oktatás mennyisége és gyakorisága, valamint az információszolgáltatás minősége bizonyult.
  [de nem jellemző, hogy nagyon szóródnának a vélemények]
- Alapvető jellemző: az oktatás általában rövid, és a szervezet saját munkatársai tartják.
- Sokan szívesen vennének részt továbbképzésben.
- Hiányzik a más VPN-ekkel való együttműködésre történő felkészítés.

Pro-M Zrt.
A Magyar Telekom Csoport tagja

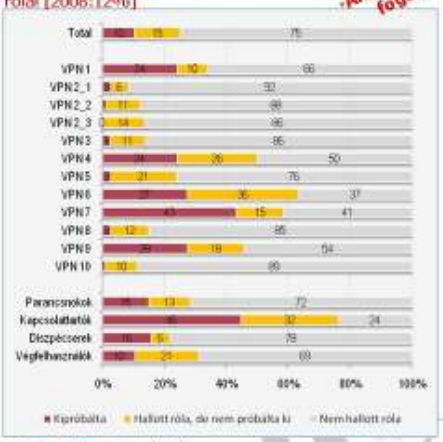
Cím: EDR a számok tükrében
Dátum: 2010. október 6.
Készítette: Mihályi Gábor
17. oldal

www.pro-m.hu

Információnyújtás, képzés

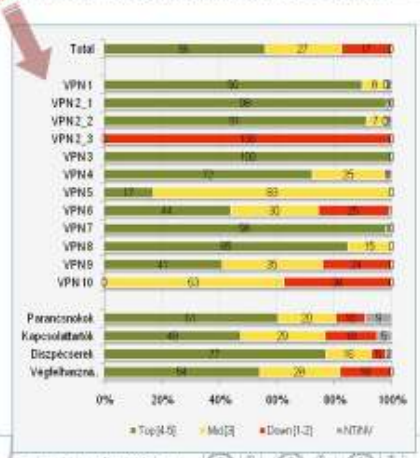
•Az EDR e-learning lehetőséggel kapcsolatos tapasztalatok

•Már 25% hallott róla! [2008:12%]



•Alapvetően pozitív fogadtatás!

•Az EDR e-learning lehetőség fogadtatása [akik kipróbálták]

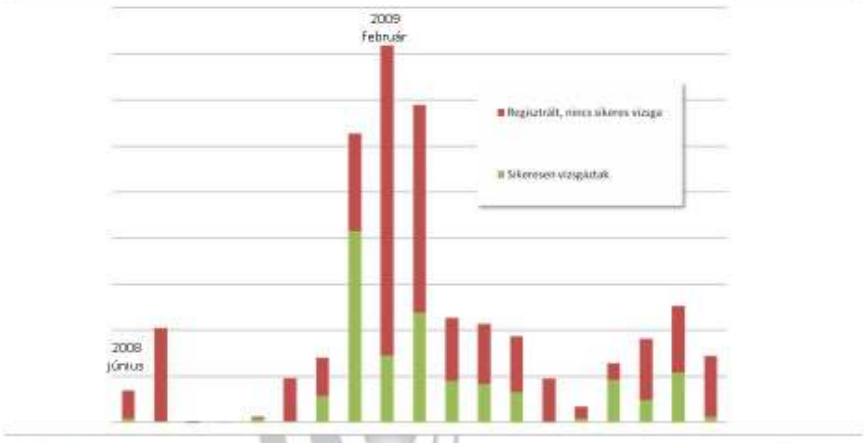


Pro-M Zrt.
A Magyar Telekom Csoport tagja

Cím: EDR a számok tükrében
Dátum: 2010. október 6.
Készítette: Mihályi Gábor
18. oldal

www.pro-m.hu

E-learning felhasználók



Pro-M Zrt.
A Magyar Telekom Csoport tagja

Cím: EDR a számok tükrében
Dátum: 2010. október 6.
Készítette: Mihályi Gábor
19. oldal

www.pro-m.hu

AVL – Járműkövető rendszer

Minden DWS-en elérhető

Sávszélesség növelés

Új mobil eszközök: LINX, TETRAtab

Pro-M Zrt.
A Magyar Telekom Csoport tagja

Cím: EDR a számok tükrében
Dátum: 2010. október 6.
Készítette: Mihályi Gábor
20. oldal

www.pro-m.hu

Az ügyfél hangja 2010-ből…

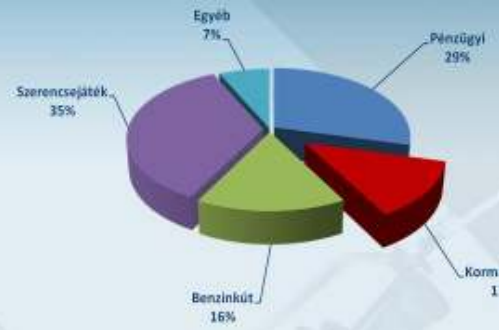
Összefoglalás

- A szerződés az akkori állapotokat kezelte az igények változnak
- Pro-M a szerződésen túlmutató fejlesztései
- EDR rendszer fejlesztés szükséges
- Az igényekkel Pro-M is egyetért és kész a megegyezésre

LÁZÁR János – ZAUTASVILI Péter

MŰHOLDAS TELEFONOK ÉS MOBIL MŰHOLDAS MEGOLDÁSOK

Főbb referenciáink



- KözHáló
- Magyar Honvédség
- Külügyminisztérium
- OKF
- egyéb

Főbb kormányzati projektek

Állandóhelyű nemzetközi és mobil műholdas szolgáltatások a védelmi szféra számára:

- 10 év tapasztalat a katonai alkalmazásokban
- Modern és rugalmas műholdas platform (több műholdas kiszolgálás)
- Szélessávú (8 Mbps-ig), dedikált vagy dinamikus (statisztikus multiplex) megoldások
- Globális lefedettség (több műhold használatával)
- IP adat, videó és hang szolgáltatások műholdon keresztül
- 24 órás támogatás és hálózatfelügyelet
- Telepítési és karbantartási oktatás a távoli végpontok egységeinek
- Költséghatékony üzem

Műholdas telefónia

Műholdas telefónia

Két műhold pálya használata:

Alacsony röppályás szolgáltatások (LEO):

- **Iridium (globális lefedettség)**
- Globalstar (lefedettségből hiányzik Afrika jelentős része és Ázsia nagy része – így Kína is)

Geostacionárius pályás szolgáltatások (GEO):

- ACeS (Kelet-Ázsia lefedése)
- **Inmarsat (globális lefedettég)**
- Thuraya (Amerika és Dél-Afrika nem lefedett)
- MSAT/SkyTerra (Észak-Amerika)
- Terrestar (Észak-Amerika lefedése)

Inmarsat

A műholdas telefónia nagyapja.

A szolgáltatás 1979-ben kezdődött egy non-profit nemzetközi szervezetként, mely fő feladata a tengeri élet biztonságosabbá tétele volt.

Eredeti nevét International Maritime Satellite Organization (Inmarsat) megváltoztatták, amikor elkezdte szolgáltatásai árulni a légi és mobil ügyfelek számára. Az új neve International Mobile Satellite Organization lett, de megtartotta az Inmarsat rövidítést. A szervezetet később két részre osztották az Inmarsat Plc. és IMSO között.

Jelenleg 11 geostacionárius műholdon keresztül szolgálja ki az ügyfeleit.

Műholdas telefon – Inmarsat BGAN

Alkalmazások:

Távoli hozzáférés: nagysebességű hozzáférés a vállalati hálózatokhoz,

Internet: akár 384 kbps sávszélességű hozzáférés,

E-mail: levelezőrendszereken vagy interneten keresztüli fogadás és küldés,

Telefon: az adathozzáféréssel egyidejű telefonbeszélgetés (4 kbps),

Streaming: akár 64 kbps sávszélességű kapcsolat audió és video alkalmazásokhoz,

Fájl transzfer: nagyméretű adatmennyiségek fogadása és küldése.

Műholdas telefon – Inmarsat BGAN

Legfőbb előnyök:

Könnyű hordozhatóság – 1,4 kg-os súlyával a ma kapható egyik legkönnyebb és legkisebb Immarsat terminál,
Rendkívül rugalmas használat –a terminál a laptophoz csatlakoztatható Bluetooth vagy Ethernet adapterrel,
Globális lefedettség – a BGAN szolgáltatások lefedettségi területén belül bárhol használható,
Egyszerű használat – 1 percen belül forgalmazásra kész állapotba hozható
Üzembiztos felépítés – a tervezés során a különböző környezeti körülmények között történő megbízható működésre helyezték a hangsúlyt,
Nagyfokú adatbiztonság – az ügyfél által preferált VPN hálózathoz csatlakoztatható.

Inmarsat BGAN készülékek

Iridium

LEO (alacsony röppályás – 160-2000km) műholdakon keresztül kommunikál

Nevét az Iridium elemről kapta:

- 77 elektron kering a mag körül (77 műholdat terveztek, melyet később felülvizsgáltak és 66 műholdat (Diszprózium) elegendőnek találtak a lefedettség biztosításához)
- A keringési pályájuk ~780 km magasan van és 7600 m/s sebességgel keringenek a föld körül
- 1997-ben lőtték fel a műholdakat és a cég 1999-ben tönkrement (ekkor 25 millió dollárért vette meg egy befektető az 5 milliárd dollárnyi eszközt)
- 2001-ben indult újra a szolgáltatás

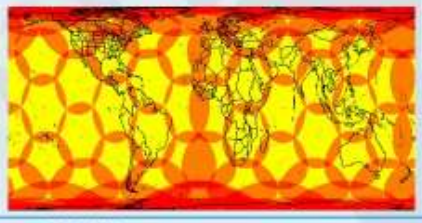
Iridium

Iridium 9555 készülék

Az Iridium 9555 műholdas telefon egy kompakt, könnyű és könnyen kezelhető készülék, mely ipari szintű strapabíróságú.

Alkalmazások:

- Telefon: telefonbeszélgetés (2,2-3,8 kbps),
- Hang szolgáltatások: hangposta, hívásvárakoztatás, hívástiltás, hívástartás, hívásátirányítás,
- Beépített kihangosító
- SMS: 160 karakter
- E-mail



Iridium

Fontosabb műszaki adatok:

Méretek: 143 mm (H) x 55 mm (SZ) x 30 mm (M)
Súly: 266 g (9.4 oz)
Készenléti idő: akár 30 óra Beszélgetési idő: akár 3.1 óra
Kijelző tulajdonságai:

- 200 karakteres megvilágított grafikus kijelző
- Hangerő, jel és akkumulátor erősség mérő
- Megvilágított időjárásálló billentyűzet

Hívás tulajdonságok:

- Beépített kihangosító
- Gyors Iridium hangposta csatlakozás
- Kétirányú SMS és rövid email lehetőség
- Előprogramozható Nemzetközi Hívókód (00 vagy +)
- Levelesláda a hang, szám és szöveges üzeneteknek
- Választható csengő és figyelmeztető hangok (8 lehetőség)

Memória: 100 bejegyzés a belső memóriában, 155 bejegyzés a SIM kártyán
Fogadott, nem fogadott és tárcsázott számok visszakeresése

Műholdas telefon – Iridium, Thuraya, IsatPhone Pro

Általános műszaki adatok:

- Telefon: telefonbeszélgetés (2,2-3,8 kbps),
- Hang szolgáltatások:
  hangposta,
  hívásvárakoztatás,hívástiltás,
  hívástartás, hívásátirá
- Beépített kihangosító
- SMS: 160 karakter
- E-mail

Műholdas telefon – Titkosító megoldások

- Nagysebességű IP/Ethernet hálózati titkosító megoldások
- Beépített TCP/IP gyorsítás
- Soros kialakítású berendezések védelmi, stratégiai és egyéb kormányzati alkalmazások számára
- Biztonságos Iridium és Inmarsat BGAN műholdas hálózati szolgáltatások egyéb perifériák bevonása nélkül
- Helyi és távoli menedzsment

Professzionális mobil műholdas megoldások

Mobil műholdas megoldások – Felhasználási lehetőségek

- Mobil ellenőrzési pont felállítása (mélységi határ ellenőrzés)
- 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

Mobil műholdas megoldások

- 1 gombnyomásra üzemképes
- Automatikus műholdra állás
- Gyors műholdra állás (kb. 5-10 perc)
- Könnyen szállítható
- Nem kell minden helyszínen
  - összeszerelni
  - szétszerelni
- Nem igényel szakértelmet
- Nem igényel fizikai munkát
- Tömege kompletten: <100kg

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


Köszönjük megtisztelő figyelmüket!
Továbbiakban is szívesen áll rendelkezésükre:
Lázár János
kereskedelmi igazgató
e-mail: lazar@hdt.hu
Zautasvili Péter
fejlesztési igazgató
e-mail: zautasvili@hdt.hu
2310 Szigetszentmiklós-Lakihegy, Komp u.2.
Tel: +36 1 4888 500
Fax: +36 1 4888 501
www.hdt.hu
Kommunikáció 2010 - Hungaro DigiTel Kft.
23

TRENCSÁNSZKY Imre

NATO SÁVBAN MŰKÖDŐ WIMAX RENDSZER


Alvarion Advantage
Largest number of WiMAX deployments
•250+ commercial networks
•10k+ sectors, 100k+ CPEs
•100+ countries
Strong network of partners to fulfill customer requirements for solution almost anywhere
Largest WiMAX pure-player committed to customer long term success
Leader of innovation in broadband wireless IP technologies
Financial strength and stability
Over 7 years of WiMAX experience
Over 15 years of broadband wireless IP experience
Introducing BreezeMAX Extreme 5000
First WiMAX 16e in 5 GHz
alvarion
alvarion

Alvarion's Point-to-Multipoint 5 GHz Solutions

BreezeMAX Extreme

First WiMAX™ 16e solution for 5 GHz market

BreezeMAX Extreme is designed to complement existing 5 GHz product offering

Complementary Solution: BreezeMAX Wi²

Wi²

BreezeACCESS® VL

AU-BST

AU-SA

SU-3 / SU-6 / SU-54 / SU-V

SU-3L / SU-6L / SU-12L

BreezeACCESS EZ

EZ-AU

EZ-SU

alvarion

BreezeMAX Extreme 5000 Specification Highlights

	Base Station	CPE
Standard	WiMAX 802.16e Wave 2 compliant	
Model	Single or dual* sector	Outdoor, MIMO
Channel Bandwidth	5, 10, 20 (2x10)* MHz	5,10 MHz
Max Tx Power	21dBm	20dBm
Power Consumption	Up to 57W	Up to 16.5W
Diversity	2x2, MIMO A/B*, MRC	2 Rx, 1 Tx
Bands	4.9 - 5.35 GHz, 5.47 - 5.95 GHz	4.9 - 5.95 GHz
Dimensions	51 x 28 x 15 cm, 11 kg (mounting: + 5 kg)	23 x 23 x 6.3 cm, 2 kg
Installer Aid	Advanced Spectrum Analyzer and DCS (Dynamic Channel Selection)*	Freq. Scan, Best AU, Preferred AU, SAU
DFS	EN 301 893 v1.5.1, FCC	
ASN-GW	Integrated or external	
Networking	IPCS, ETHCS	
Security	AES WiMAX 16e	
Authentication	AAA centralized over RADIUS Local provisioning (SU MAC-based, fixed network)	

* In future release

alvarion


alvarion
Your Open WiMAX Choice
Market and Deployment Scenarios
Wide Range of Applications
Access
Public Safety
Business Applications
Remote Office
Utilities
Mining
Fleet Management
Meter Reading
Emergency Services
Municipality Applications
alvarion

BreezeMAX Extreme 5000: A Network That Works for You (1)

CURRENT APPLICATIONS

Access

- Quality of Service enabling additional services
- Capacity: designed for high occupancy
  - Scheduled, multiple access protocol
- Ease-of-use: centralized provisioning and management

Business

- Diverse services and deployment scenarios:
  - Combined Eth.CS and IP.CS services
  - QoS with diverse classifiers
- Security: AES encryption, keys generated per session by AAA
- Enhanced ROI: carrier of carrier

Remote Office

- Centralized provisioning: nomadicity
- Access anywhere (potential ROI - roaming)
- Improved efficiency, reach, and service

alvarion

BreezeMAX Extreme 5000: A Network That Works for You (2)

PLANNED APPLICATIONS

Video / Public Safety

- Leveraging 16e QoS for video reliability
- Enhanced performance
  - Video centric service profile
  - Optimized video delivery
- Multicast, broadcast and unicast

Municipality

Fleet Mgmt.

- 16e separates between access and service
  - Ability to lease part of access network to local vendors
- QoS for diverse municipality services
  - Inter-building connectivity, remote office, video surveillance, first responders, fleet management

Mobility

- True vehicular mobility powered by 16e
- 5 GHz suits vehicular mobility
  - First responders, trains, buses, watercraft
- Special subscriber under development

alvarion

Adam Internet, Australia

Customer Type	Internet Service Provider
Country / Region	Australia
URL	http://www.adam.com.au
Application	Broadband services for residential and business customers

The Result

- Rated within top-ten ISPs in Australia, serving over 80,000 DSL subscribers
- Deploying WiMAX 16e in 5 GHz spectrum
- Part of the Australian Government's Broadband Guarantee Program (BGP)
- Targeting 55,000 underserved customers metropolitan Adelaide (across 5000 square km)

AdamMax

Adam
High Performance Internet

Greg Hick's, Chairman of Adam Internet

"...WiMAX offers a high-capacity network that is quick to deploy and very economical to operate. The excellent performance results of BreezeMAX Extreme 5000 coupled with its compact flexible outdoor design configuration enables us to significantly reduce our upfront network investment and accelerate our return on investment.."

Proprietary Information

MIMO Single Sector Model

MIMO Single Sector 2x2

- Superior performance utilizing 2nd order diversity
- Maximal sector capacity (MIMO B)*
- Maximal sector coverage (MIMO A)
- Supports 5, 10, 20(10+10)* MHz per sector
- Max UDP Capacity:
  - MIMO A: 27 Mbps (10 MHz), 54 Mbps (20 MHz)
  - MIMO B: 32 Mbps (10 MHz), 65 Mbps (20 MHz)
- Integrated or external antenna

Best Fit for

- High-capacity driven deployments
  - Urban
  - Video
- NLOS conditions

* In future release

alvarion

SISO Single Sector Model

SISO Single Sector 1x1

- Single sector
- Supports 5, 10, 20(10+10)* MHz per sector
- Integrated or external antenna
- Max UDP sector capacity
  - 5 MHz: 13 Mbps
  - 10 MHz: 27 Mbps
  - 20 MHz: 54 Mbps

Best Fit for

- Capacity-driven deployments
  - Suburban
  - Rural

* In future release

SISO Dual Sector Model*

SISO Dual Sector 1x1*

- Dual sector served by a single unit
  - Full functional sectors, enabling reduced CAPEX and OPEX
- Up to 10 MHz per sector
- Max UDP sector capacity
  - 5 MHz: 13 Mbps
  - 10 MHz: 27 Mbps
- External antenna only

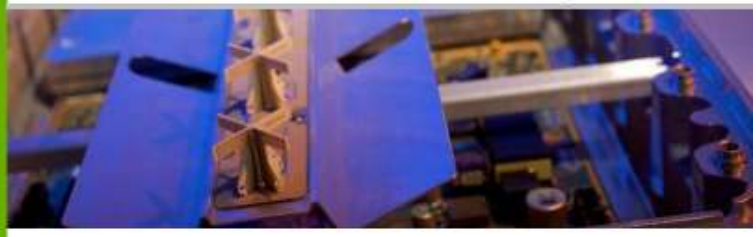
Best Fit for

- Coverage-driven deployments with lower capacity requirements
  - Rural

* In future release

alvarion
Your Open WiMAX Choice

BreezeMAX Extreme 5000
The Power of Enhanced Radio System



Extreme Radio System

Built for best fit and ease-of-use

alvarion
Your Open WiMAX Choice

Above standard capabilities

WiMAX 16e

Advanced radio technology

alvarion

MIMO A

MIMO A (Diversity)

- Base station transmits same data over two transmission paths
- Transmissions are coded in time and space
- 2nd order diversity is featured in downlink

Benefits:

- Increased coverage due to redundant and parallel paths
- Less re-transmission on cell edge with multiple path

alvarion

MIMO B*

MIMO B (Capacity)

- Base station transmits two different data streams over same channel
- Same number of sub-carriers, twice as many QAM symbols to MAP interleaving

Benefits:

- Increased capacity due to reuse of bandwidth channel

* In future release

alvarion

MIMO A/B*

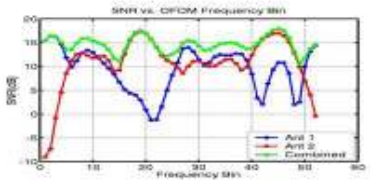
Extreme Performance with MIMO A/B Switching

- **MIMO A or MIMO B* utilization**
- Maximizing coverage or capacity per deployment type
- **Adaptive MIMO switching**
- Changes rapidly between Matrix B and Matrix A
- Maximizing capacity while maintaining connection

* In future release

Maximum Receive Ratio Combining (MRRC)

- **Combining signals from antennas at each frequency**
- **Improve overall gain, especially in multipath environments**
- **Increase uplink gain**
- **Reduce imbalance between uplink and downlink power budgets**

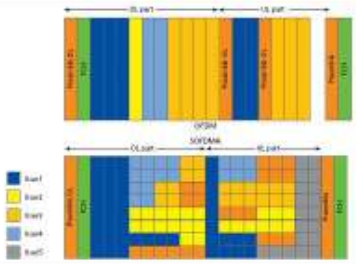


Benefits:

- **Enhanced system gain**
- **increased sector coverage and capacity**
- **Improved business case**

OFDMA

- Two dimensional (time and frequency) based scheduling
- Dynamic allocation of sub-channels to best fit link budget and capacity demand
- Increase SNR and improved modulation rate
- Increased flexibility for enhanced throughput and robustness



Benefits:

Connect subscriber units (SUs) with relatively poor link conditions

- Increase maximum transmit power of SU by 3, 6, 9 or 12 dBm
- Better bandwidth utilization enabling several SUs to simultaneously share bandwidth

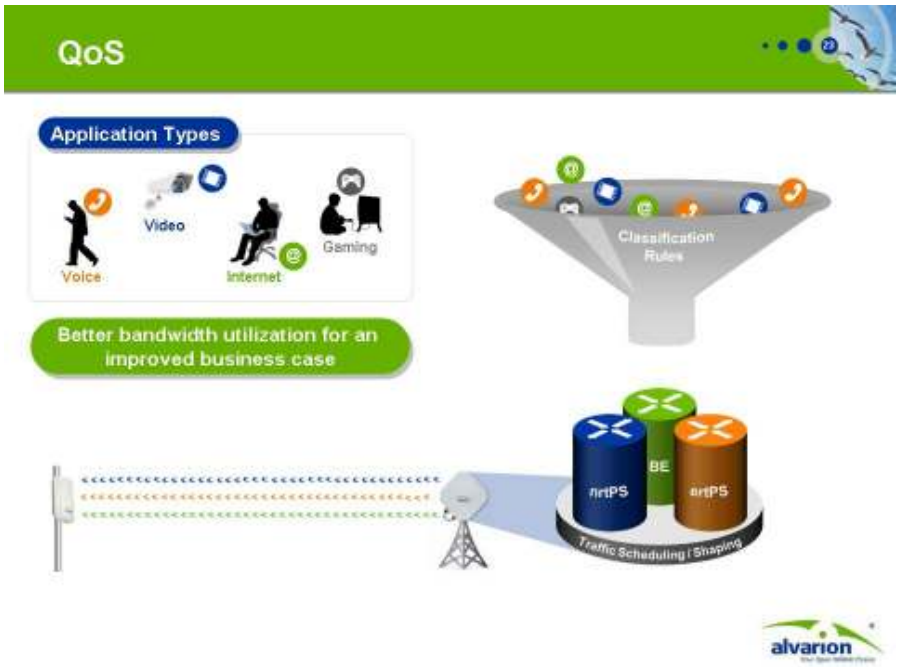
alvarion

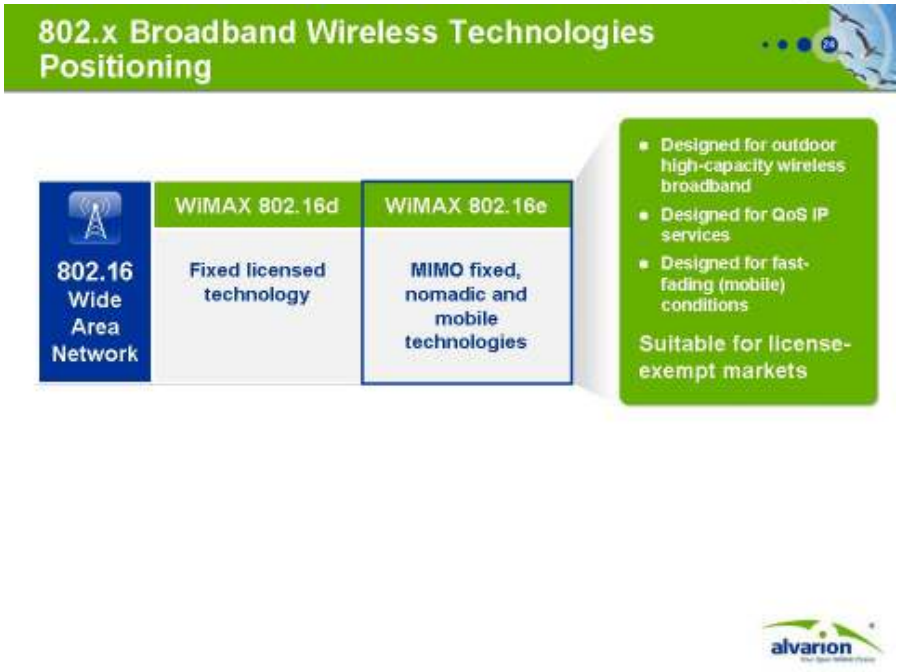
QoS

Classification Rules

- Packets received by base station or CPE are sorted
- Cross classification of application to QoS service flow
- Classification performed according to fields in packet header:
  - IP-CS: e.g. DSCP
  - Eth-CS: DSCP, PPPoE (EtherType), VLAN ID (.1q), VLAN Priority (.1p), Any

alvarion

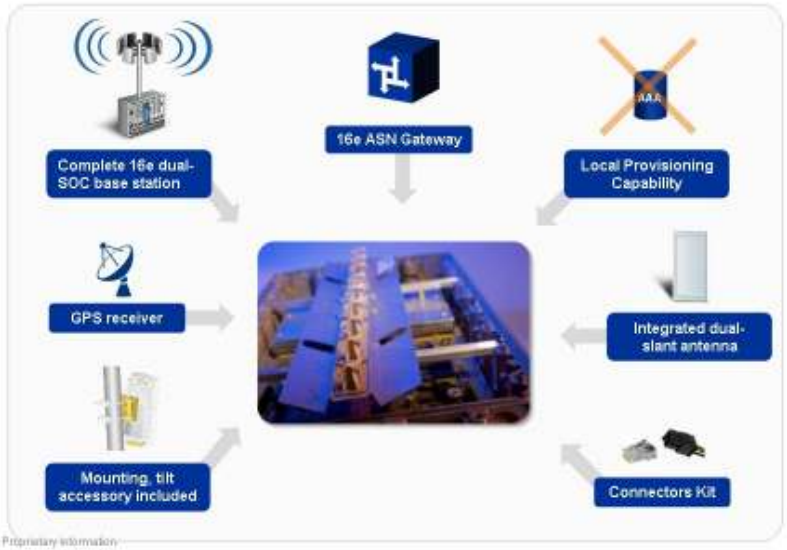

QoS
Application Types
Voice
Video
Internet
Gaming
Classification Rules
Better bandwidth utilization for an improved business case
BE
nrtPS
ertPS
Traffic Scheduling / Shaping
alvarion

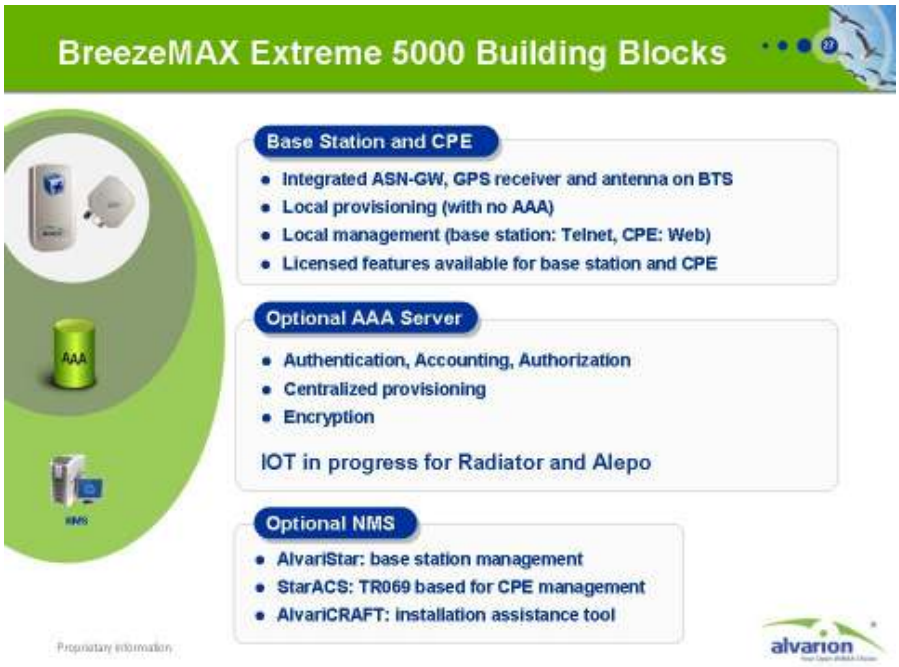

802.x Broadband Wireless Technologies Positioning
802.16 Wide Area Network
WiMAX 802.16d
Fixed licensed technology
WiMAX 802.16e
MIMO fixed, nomadic and mobile technologies
Designed for outdoor high-capacity wireless broadband
Designed for QoS IP services
Designed for fast-fading (mobile) conditions
Suitable for license-exempt markets
alvarion

alvarion
Your Open WiMAX Choice

BreezeMAX Extreme 5000 Solution Building Blocks

Distribution in Mind: Making it All-in-One




BreezeMAX Extreme 5000 Building Blocks
Base Station and CPE
Integrated ASN-GW, GPS receiver and antenna on BTS
Local provisioning (with no AAA)
Local management (base station: Telnet, CPE: Web)
Licensed features available for base station and CPE
Optional AAA Server
Authentication, Accounting, Authorization
Centralized provisioning
Encryption
IOT in progress for Radiator and Alepo
Optional NMS
AlvariStar: base station management
StarACS: TR069 based for CPE management
AlvariCRAFT: installation assistance tool
AAA
NMS
alvarion


BreezeMAX Extreme 5000: High Level Roadmap
Q3/09
Q4/09
H1/10
Q1/11
Release 1.0
Release 1.2
Release 1.5
Release 2.0
Application
Access
Access
Business
Video p.1
Voice
Video p.2
Mobility
Platform
SISO (Int/Ext Ant)
MIMO (Int/Ext Ant)
2 SISO (Ext Ant)
Radio
MIMO A, 5-10 MHz, IP,CS, BE, nRT
Eth.CS
MIMO B, 20 MHz, DL/UL, eRT, GPS chaining
Mobility, Enh. RRM, RT, optimized video
CPE
MIMO, outdoor (Int Ant.)
MIMO, outdoor (Ext. Ant.)
ETSI 5.8
Video-PoE
SU-M
Subject to the presentation disclaimer

Regulation / Certification Map

Low Band (4.9-5.3 GHz)

- Universal (4.9)
- 4.9 FCC
- 5.1 FAA (no certification profile)
- 5.2-5.3 ETSI

High Band (5.4-5.9 GHz)

- Universal (5.4, 5.9)
- 5.4 ETSI
- 5.4, 5.8 Australia
- 5.8 FCC

Plans

- 5.4 FCC (DFS): pending FCC (not before Q1 2010)
- 5.3 FCC (DFS): pending FCC (not before Q1 2010)
- 5.8 ETSI (DFS, CPE): release 1.5 (H1/10)
- 4.9 Japan: finalizing certification plan (during Q1/10)

alvarion

SCI-NetWork

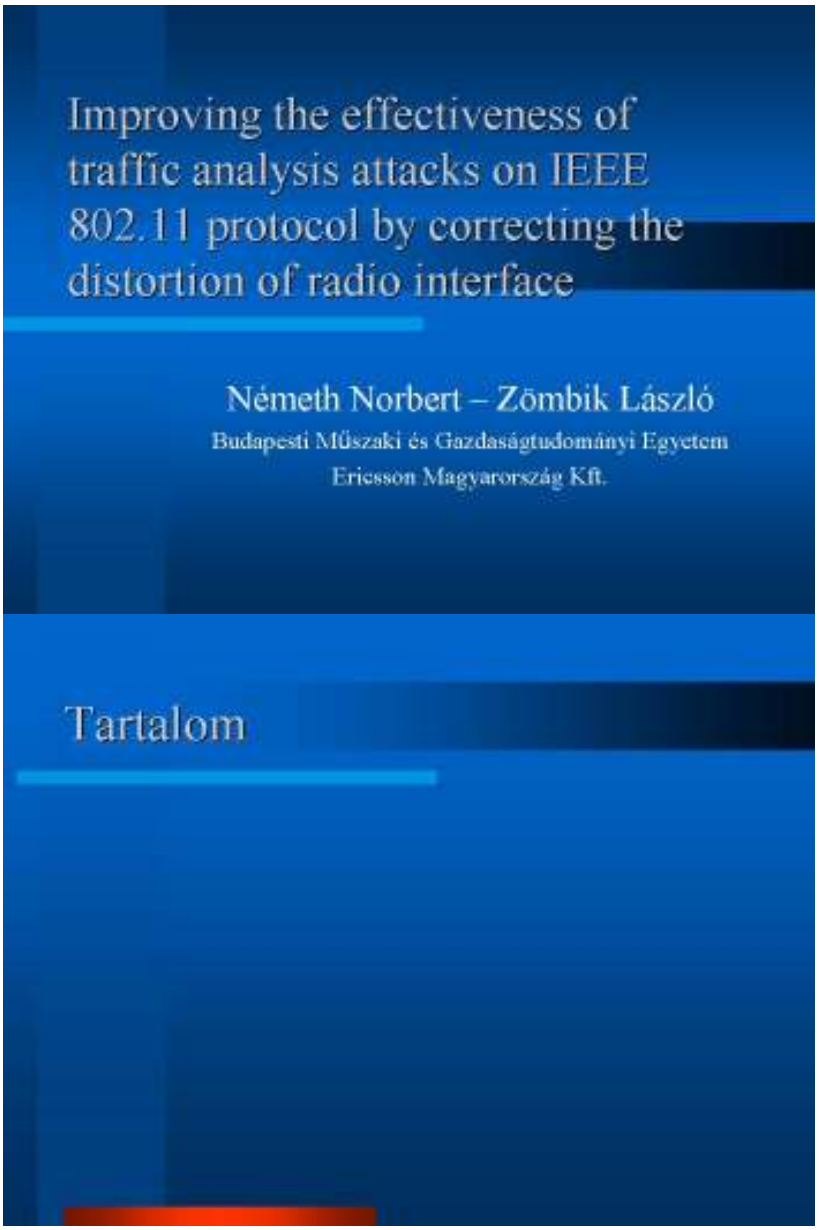
alvarion

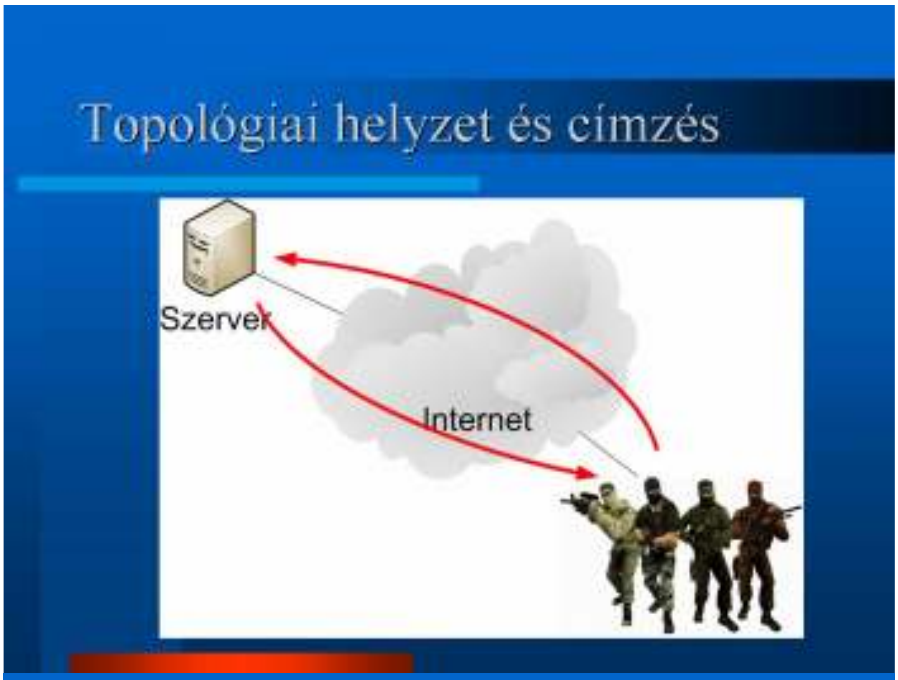
Köszönöm
figyelmüket!

timre@scinetwork.hu

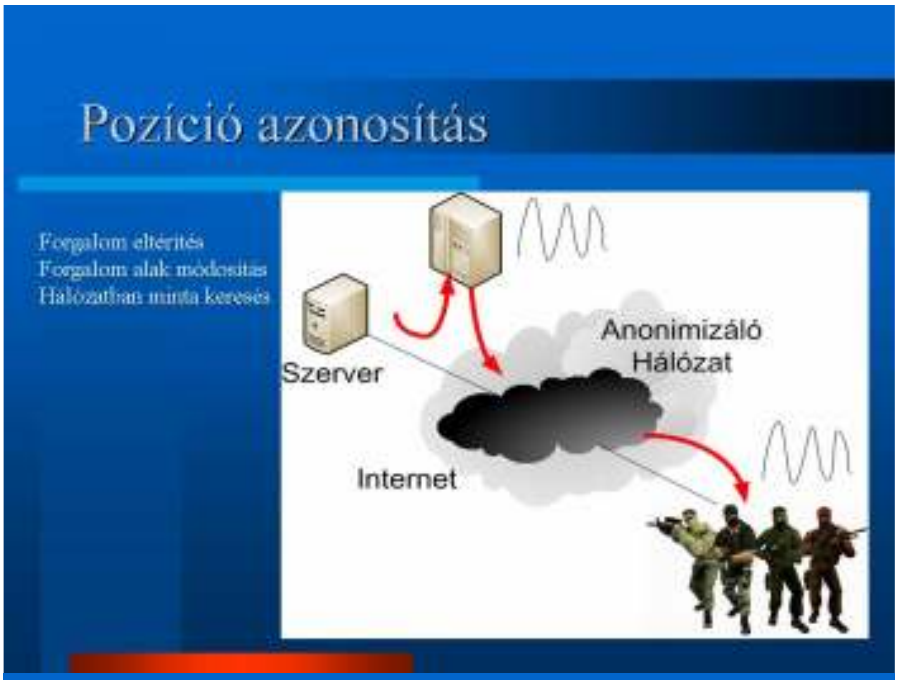
NÉMETH Norbert – ZÖMBIK László

IMPROVING THE EFFECTIVENESS OF TRAFFIC ANALYSIS ATTACKS ON IEEE 802.11 PROTOCOL BY CORRECTING THE DISTORTION OF RADIO INTERFACE




Topológiai helyzet és címzés
Szerver
Internet

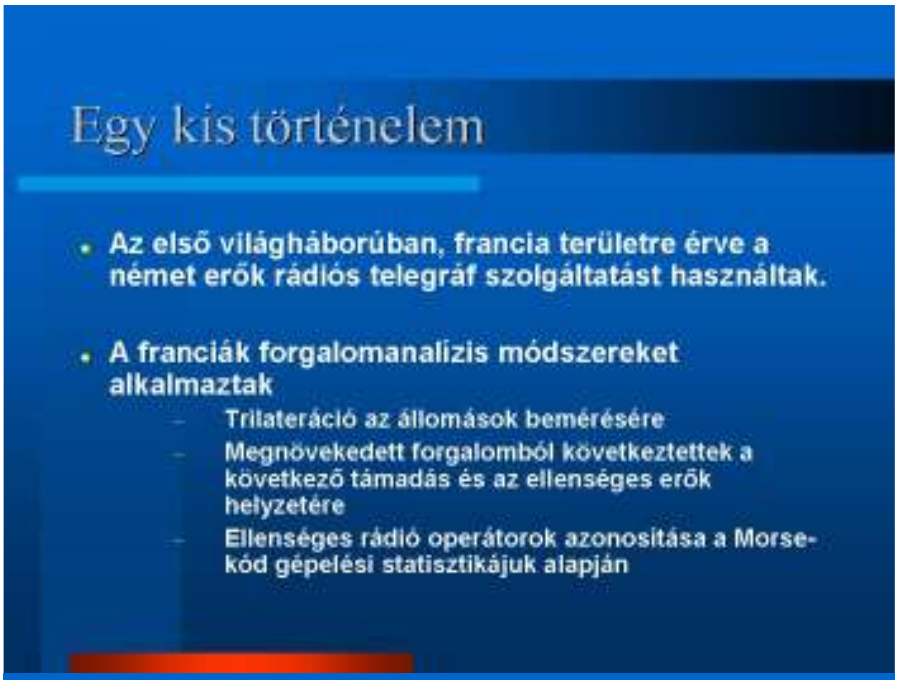

Anonimizáló hálózat
Szerver
Anonimizáló
Hálózat
Internet
Naval
Research
Laboratory
Project

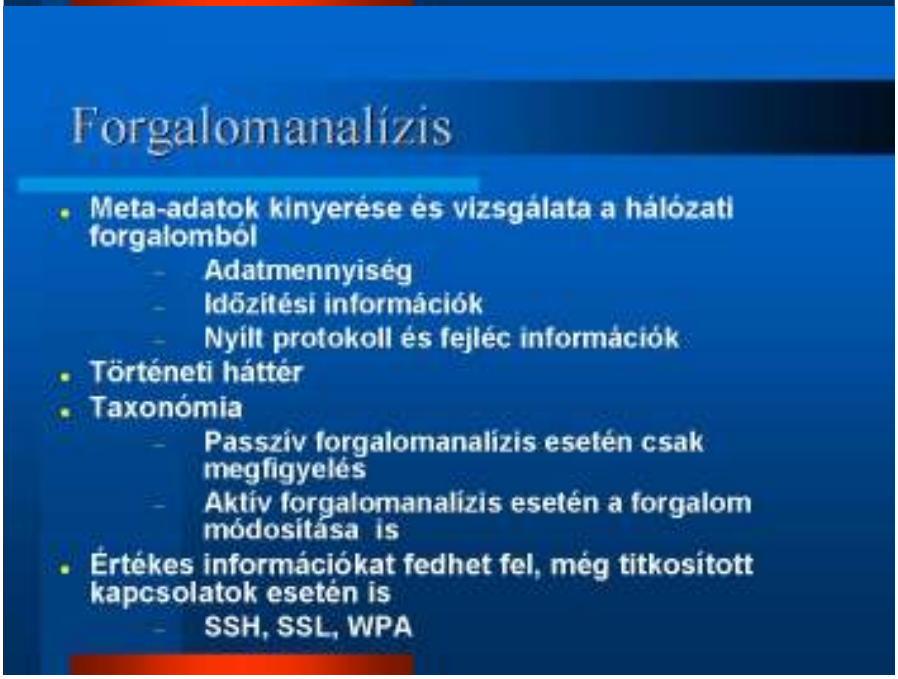

Pozíció azonosítás
Forgalom eltérítés
Forgalom alak módosítás
Hálózatban minta keresés
Szerver
Anonimizáló
Hálózat
Internet

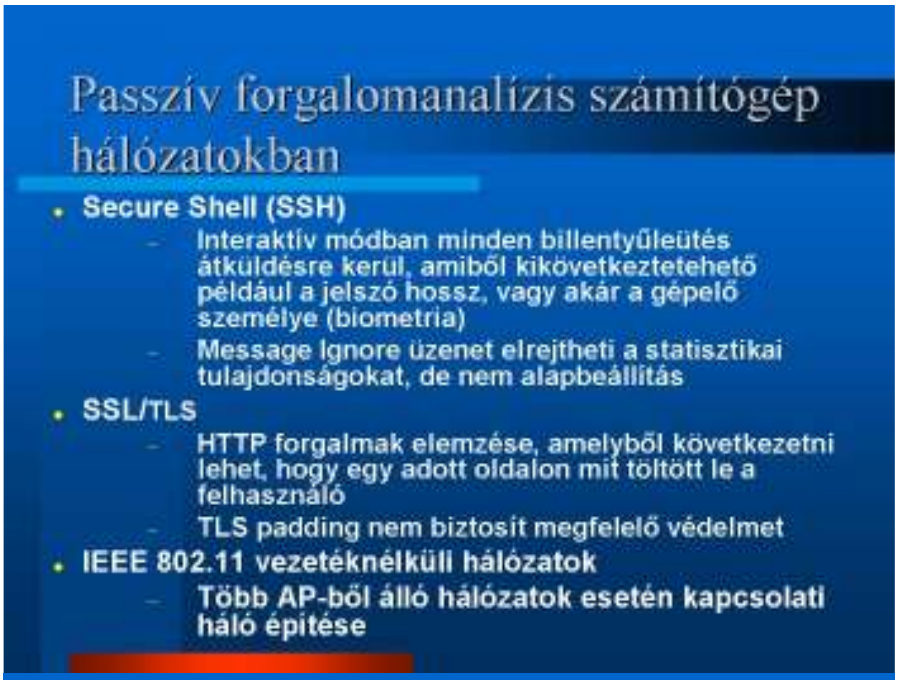

Mobil IPv6
Otthoni ügynök
Otthoni Hálózat
(Home Network)
Szerver
IPv6, mobilitás

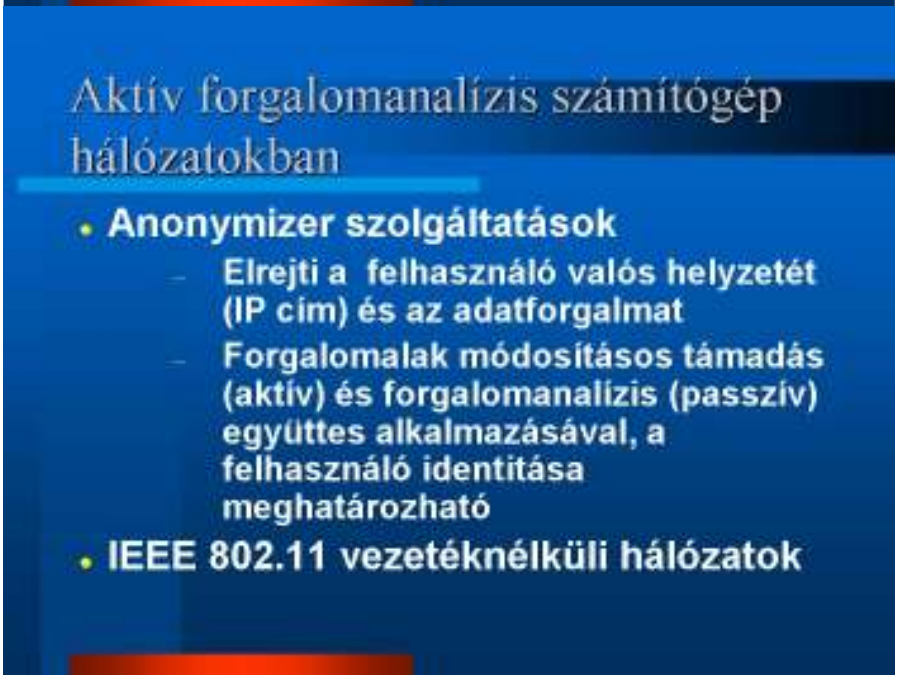

Mobil IPv6 és vezetéknélküli hozzáférés
•IP mobilitás hasonló, mint az ancestrális Hálózat
•Vezetéknélküli Csatorna terzitás
IPv6 Otthoni ügynök
Otthoni Hálózat
(Home Network)
Szerver
vezetéknélküli
hálózat


Vezetéknélküli hozzáférés
Szerver
vezetéknélküli
hálózat
Internet


Egy kis történelem
Az első világháborúban, francia területre érve a német erők rádiós telegráf szolgáltatást használtak.
A franciák forgalomanalízis módszereket alkalmaztak
Trilateráció az állomások bemérésére
Megnövekedett forgalomból következtettek a következő támadás és az ellenséges erők helyzetére
Ellenséges rádió operátorok azonosítása a Morse-kód gépelési statisztikájuk alapján


Forgalomanalízis
Meta-adatok kinyerése és vizsgálata a hálózati forgalomból
Adatmennyiség
Időzítési információk
Nyílt protokoll és fejléc információk
Történeti háttér
Taxonómia
Passzív forgalomanalízis esetén csak megfigyelés
Aktív forgalomanalízis esetén a forgalom módosítása is
Értékes információkat fedhet fel, még titkosított kapcsolatok esetén is
SSH, SSL, WPA


Passzív forgalomanalízis számítógép hálózatokban
Secure Shell (SSH)
Interaktív módban minden billentyűleütés átküldésre kerül, amiből kikövetkeztetehető például a jelszó hossz, vagy akár a gépelő személye (biometria)
Message Ignore üzenet elrejtheti a statisztikai tulajdonságokat, de nem alapbeállítás
SSL/TLS
HTTP forgalmak elemzése, amelyből következetni lehet, hogy egy adott oldalon mit töltött le a felhasználó
TLS padding nem biztosit megfelelő védelmet
IEEE 802.11 vezetéknélküli hálózatok
Több AP-ből álló hálózatok esetén kapcsolati háló épitése

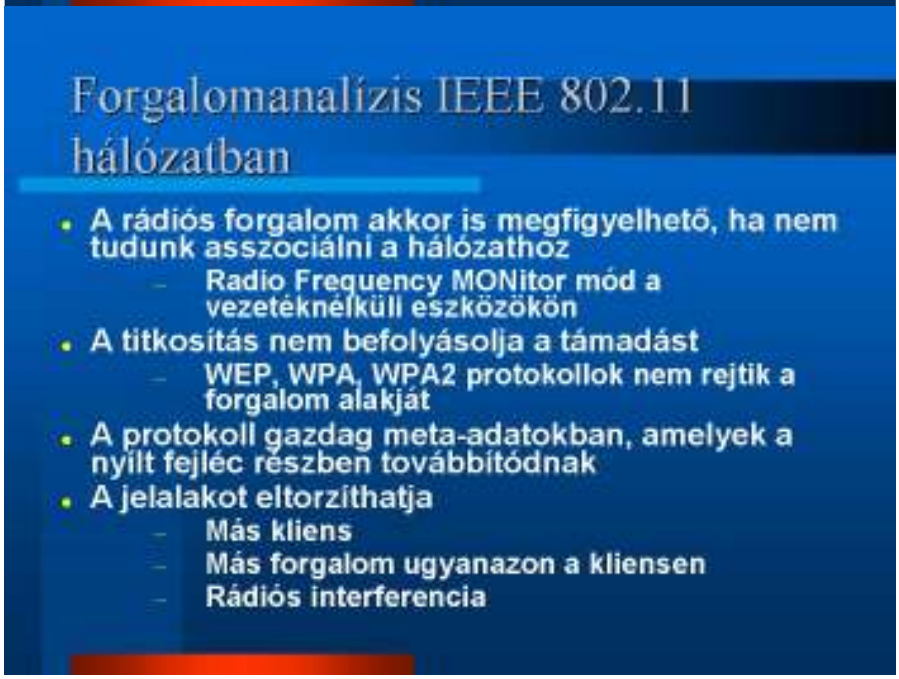

Aktív forgalomanalízis számítógép hálózatokban
Anonymizer szolgáltatások
Elrejti a felhasználó valós helyzetét (IP cím) és az adatforgalmat
Forgalomalak módosításos támadás (aktív) és forgalomanalízis (passzív) együttes alkalmazásával, a felhasználó identitása meghatározható
IEEE 802.11 vezetéknélküli hálózatok

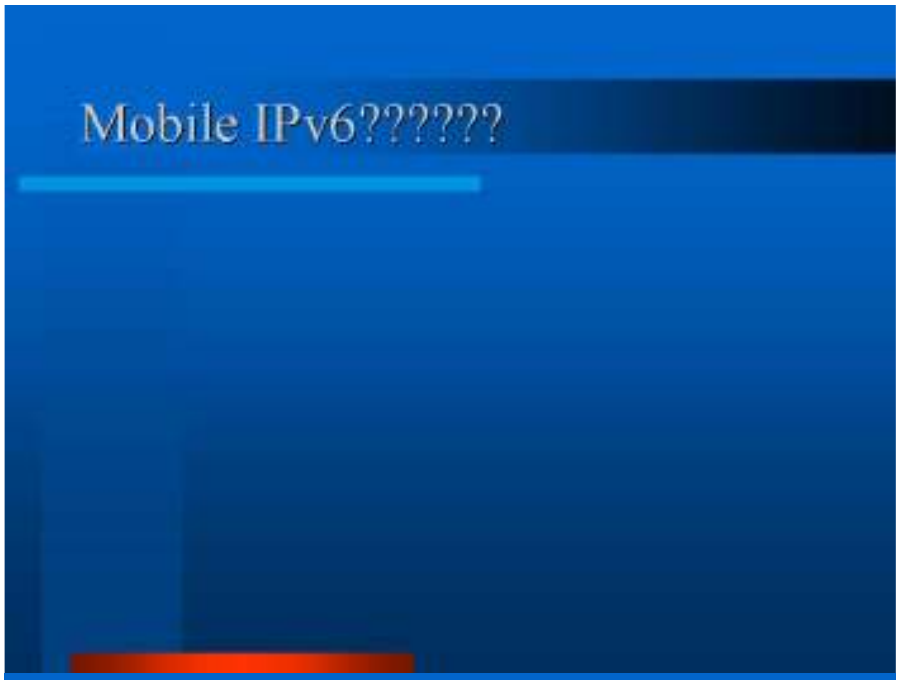
Forgalomalak módosításos forgalomanalízis

- Felismerhető minta alapján módosítjuk a forgalom valamely paraméterét, mielőtt a célponthoz ér
  - Paraméterek például: sávszélesség, időzítés
  - Minta: például szinuszjel, de lehet szinte bármi
- Kliens oldalon keressük a forgalomra ültetett mintát, passzív forgalomanalízissel
  - Azonosítás sikeres, ha nagy bizonyossággal megtaláljuk a mérőjelet
- IEEE 802.11 hálózatokban használható a kliens jelenlétének detektálására az adott környezetben

Architektúra


HTTP Session Riding ?????
Támadás idejének megnyújtása
Content-Length mező törlése
– A kliens addig fenntartja a kapcsolatot és fogadja az adatokat, amig <\html> taget nem kap
Teljes tartalom átküldése, majd a TCP sequence number módosítása
– A kliens továbbra is fogadja a forgalmat
– Nem jeleníti meg azt


Forgalomanalízis IEEE 802.11 hálózatban
A rádiós forgalom akkor is megfigyelhető, ha nem tudunk asszociálni a hálózathoz
– Radio Frequency MONitor mód a vezetéknélküli eszközökön
A titkosítás nem befolyásolja a támadást
– WEP, WPA, WPA2 protokollok nem rejtik a forgalom alakját
A protokoll gazdag meta-adatokban, amelyek a nyílt fejléc részben továbbítódnak
A jelalakot eltorzíthatja
– Más kliens
– Más forgalom ugyanazon a kliensen
– Rádiós interferencia

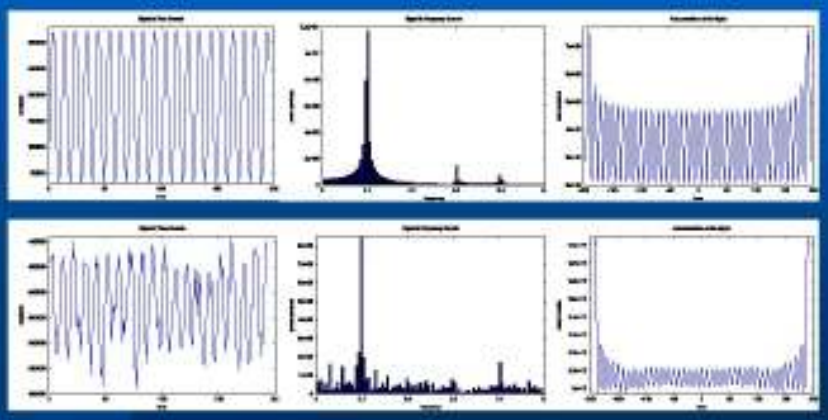

Mobile IPv6??????


Másik kliens hatása
TODO kép

A keresett minta felismerése

- Periódikus jel esetén
  - Könnyen felismerhető, de
    - nem csak a támadó számára
  - Detektálás: autokorreláció
- Nem periódikus jel esetén
  - Nehezebben felismerhető,
    - jobban rejti a támadást, de
    - érzékenyebb a zajra
  - Szórt spektrum
    - Keresztkorreláció, mint a radarok esetében

Adatforgalom hatása a támadásra



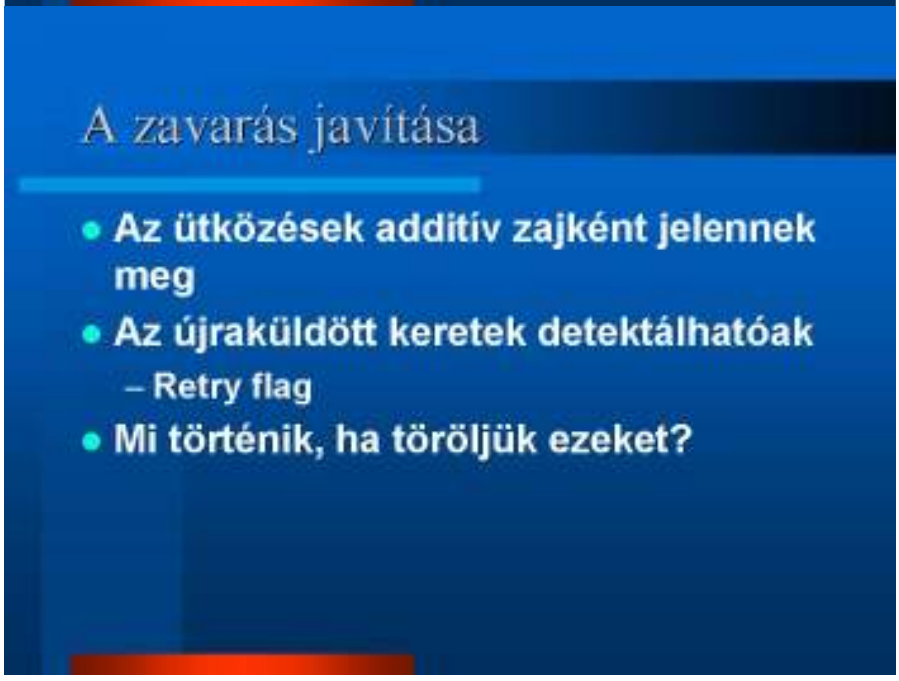
Kliens forgalom hatásai

- Forgalom másik kliensen
  - Kevésbé zavarja a jelalakot, amíg nem folytják le egymást
  - Szűrhető MAC cím alapján
- Forgalom ugyanazon a kliensen
  - Súlyosabb probléma lehet, a módosított jel és az egyéb forgalmak arányától függ
    - Időben és sávszélességben
  - Folyamatos letöltés additív zajként jelenik meg, ami könnyen kezelhető
- Tesztelt forgalmak
  - HTTP forgalom
  - Torrent forgalom

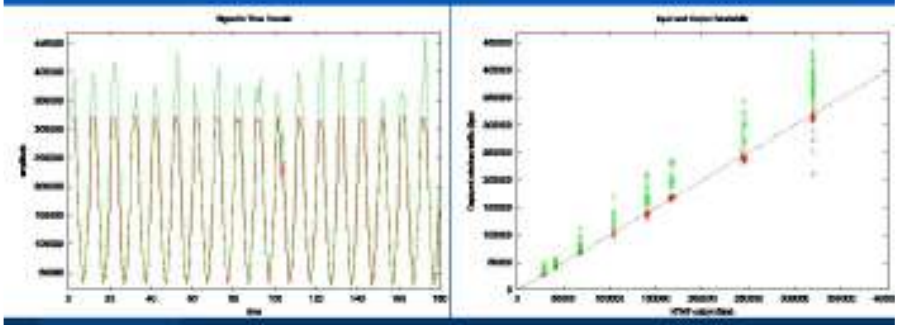
IEEE 802.11 meta-adatok forgalomanalízis szempontból

- A kliens forgalmak szétválaszthatók MAC cím alapján
- A fel- és letöltés különválasztható
  - FROM_DS és TO_DS mezők alapján
- Újraküldés detektálható
  - Retry flag alapján
- Ezenkívül is vannak hasznos flagek, de
  - QoS kliensek esetén
  - Több forgalmi osztály, ritkán használt koordináló függvények esetén

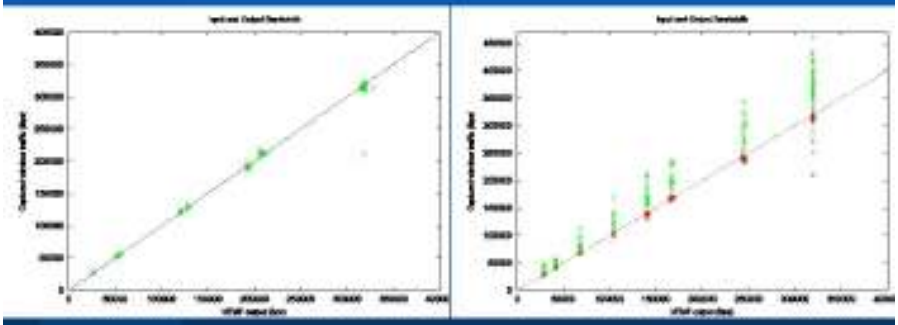

Radiós interferencia generálás
Mikrohullámú sütő
– Könnyen elérhető és tesztelhető
– Industrial, Scientific and Medical band
• Mint az IEEE 802.11b/g hálózatok
– „Nem illedelmes”
• Nem ismeri a protokollt (nyilvánvaló), ezért folyamatos zavarás
– „Ütközésgenerátor”


A zavarás javítása
Az ütközések additív zajként jelennek meg
Az újraküldött keretek detektálhatóak
– Retry flag
Mi történik, ha töröljük ezeket?

A zavarás javítása



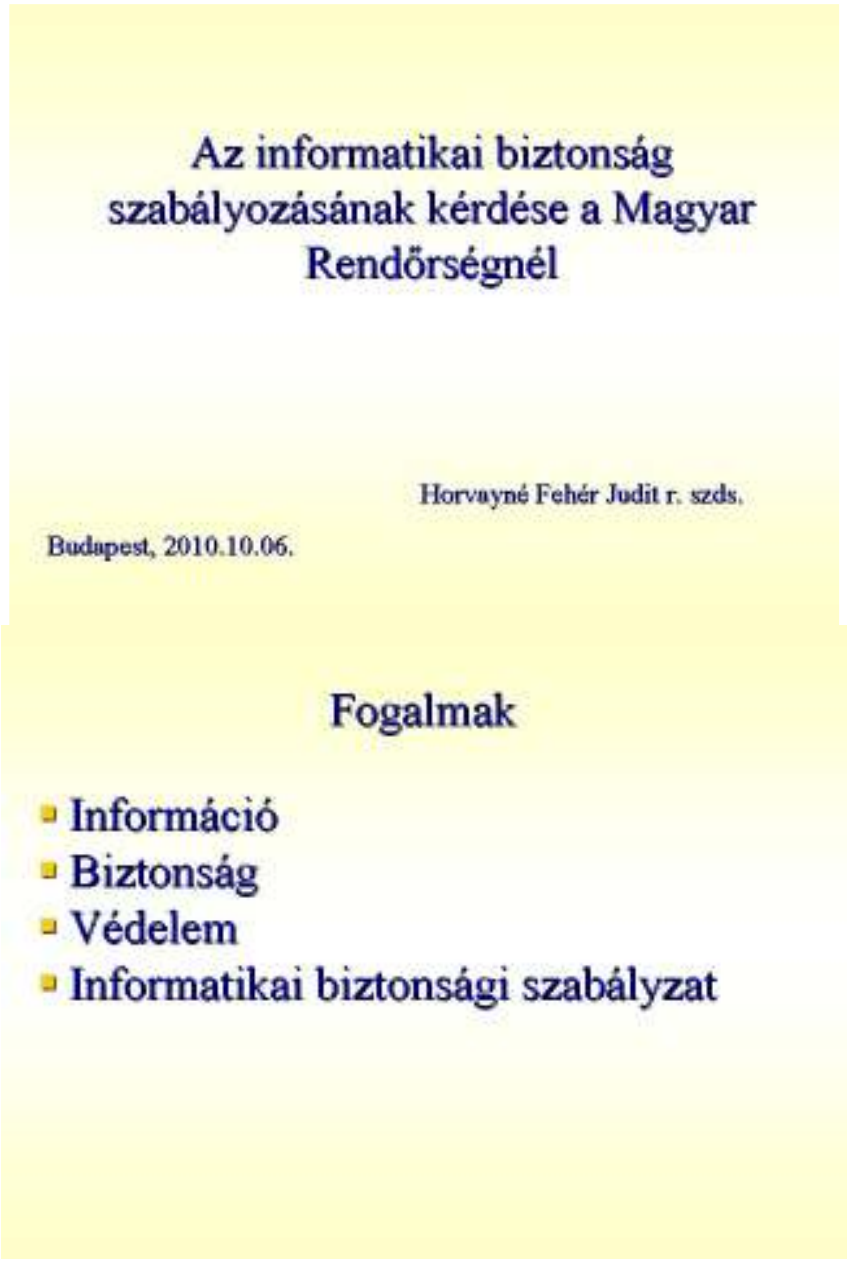
A bemeneti jel kapcsolata az eredeti és feldolgozott kimenettel




Összefoglalás
Az IEEE 802.11 csatornán fellépő ütközéseket, csomagvesztéseket a protokoll újraküldésekkel javítja
Az újraküldések torzítják a forgalom alakját
Ezt a torzítást meta-adatok alapján korrigáltuk
Megoldásunkkal képesek vagyunk azonosítani egy olyan titkosítottan kommunikáló végpont pozícióját, mely anonimizáló hálózatot, mobile IPv6-ot illetve IEEE 802.11 vezeték nélküli hozzáférést használ

HORVAYNÉ Fehér Judit

AZ INFORMATIKAI BIZTONSÁG SZABÁLYOZÁSÁNAK KÉRDÉSEI A MAGYAR RENDŐRSÉGNÉL



A szabályozás kérdésköre

- Adatvédelem
- Informatikai rendszerek védelme
- A Rendőrség Ideiglenes Informatikai Biztonsági Szabályzata
- Minősített Adat Védelméről szóló törvény

Felmerülő tényezők

- A rendőrség állandó változása;
- A szervezeti egységek önálló költségvetéssel rendelkeznek;
- Egyedi ügyrenddel rendelkeznek a szervezeti egységek;
- Nincs fellelhető dokumentáció.

A szabályozás céljai

- a kört behatárolni, amelyre vonatkoztatjuk a szabályozást;
- az egységes rendőrségi informatikai rendszer megteremtése;
- olyan minimálisan érvényesíthető szabályi keretekbe terelje az informatika területén az információ védelmét, amely a jelenlegi körülmények között érvényesíthető;
- intézkedések az informatikai rendszer környezetével kapcsolatban;
- Dokumentációk és dokumentumok elkészítése;
- a szabályozás megismertetése: oktatás, vizsgáztatás.

Alapelvek

Az információvédelem területei:

a) azonosítás, hitelesség;
b) jogosultság kiosztás, ellenőrzés;
c) hozzáférés-szabályozás;
d) elszámoltathatóság;
e) hitelesség garantálása;
f) sértetlenség garantálása;
g) auditálhatóság logikai védelmi funkciói;
h) bizonyítékok rendszerének és folyamatának kialakítása.

A Rendőrség informatikai rendszerei

Az információvédelmi biztonsági osztályok

a) információvédelmi alapbiztonsági (1.) osztály:

aa)nyílt, jogszabályok által nem védett adatok,

ab) személyes adatok,

ac)üzleti titkok,

ad) pénzügyi adatok, illetve az intézmény belső szabályozásában hozzáférés-korlátozás alá eső (pl. egyes feladatok végrehajtása érdekében bizalmas) adatok;

b) információvédelmi fokozott biztonsági (2.) osztály:

ba) szolgálati titok, valamint a nem minősített adatok közül a különleges személyes adatok,

bb) nagy tömegű személyes adatok,

c) információvédelmi kiemelt biztonsági (3.) osztály:

ca)államtitok,

cb) nem minősített adatok közül a nagy tömegű különleges személyes adatok.

Az informatikai rendszer környezete

- Alkalmazások rendszerezése
- Rendszerkörnyezet meghatározása
- Intézményesített rendszer résztvevők
- Értelmezést segítő szabályok (rendelkezésre állás mérőszámai, fenyegetések felmérése, kockázati elemzések)

A minimális szint

- Adatkataszter, nyilvántartások
- Szerepkörök meghatározása
- Jogosultsági rendszerek kidolgozása
- Biztonsági szint elérése
- Informatikai eszközök, rendszerelemek

Kiegészítő szabályzatok megalkotása

- Kommunikációs rendszerek szabályozása
- Összekapcsolási szabályok
- Elektronikus határvédelem
- Számítógépes topológia elkészítése
- Elektronikus vírusvédelem

Szolgáltatások vészhelyzet esetén

- Általános rendelkezések (mely minden egyes rendszerre, alkalmazásra, felhasználóra, vagy bármely rendszerkörnyezeti szereplőre egyaránt alkalmazandó feladatokat tartalmaztak esemény bekövetkeztétől függetlenül)
- Szerverek, központi kiszolgálók mentése (olyan speciális intézkedések halmaza, melyek az informatikai szakembereknek írnak elő feladatokat a központi adattárakkal, és azok eszközrendszerével kapcsolatosan)
- Alkalmazás szintű mentések (kisebb biztonsági események jelentkezésekor végrehajtandó biztonsági intézkedéseket határoztak meg az informatikai szakemberek számára)

Akadályok az oktatás és számonkérés területén

- nem ismerik kellően a szabályokat az alkalmazók,
- nem tudják alkalmazni a szabályokat, átvetíteni a gyakorlatba az elvi szabályok meghatározásait;
- nincsen oktatása a szabályoknak, csak ismertetik, hogy léteznek a szabályok;
- ha vannak oktatások, akkor azok tantervszerűek, elméleti síkon mozognak, nem gyakorlat orientáltak;
- a felhasználók nagy százaléka nem rendelkezik kellő szintű alapképzéssel az számítástechnikai eszközök kezelésének tekintetében;
- a számonkérési rendszer nem tükrözi a felhasználó tényleges tudásának szintjét.

Megoldás az oktatás és számonkérés területén

- minden egyes felhasználó, aki rendőrségi alkalmazásba került, alap számítástechnikai képzésen vegyen részt;
- továbbá ne kaphasson jogosultságot rendőrségi informatikai alkalmazásokhoz, amíg az informatikai biztonsági szabályrendszerekből sikeres vizsgát nem tesz;
- szituációs vizsgafeladatokkal mérjék a számonkérés során a vészhelyzetekre, és kompromittálódásra okot adó helyzetekre való felkészültségét a vizsgázónak.

Akadályok: a dokumentációk hiánya

- biztonságtechnika,
- kommunikáció,
- rejtjel,
- hálózatvédelem,
- üzemeltetés- karbantartás,
- mentések-archiválások,
- vészhelyzet-katasztrófahelyzet elhárítás,
- informatikai védelem megalkotása,
- informatikai biztonság fenntarthatósága.

A rendőrségnek az alábbi feladatokat kell ellátnia

- az informatikai biztonságpolitika és stratégia meghatározása;
- az informatikai rendszerek biztonsági osztályba sorolása;
- az információvédelmi követelmények meghatározása;
- az információbiztonsági követelmények meghatározása;
- az informatikai működés-folytonossági terv (katasztrófa-elhárítási terv);
- az informatikai működési szabályzat;
- az informatikai biztonsági kézikönyv.

Köszönöm a figyelmet

Horvayné Fehér Judit r. szds.
Belügyminisztérium
Informatikai Főosztály
Információ-védelmi és Rejtjel Osztály
Tel.: 13-784
01/4411843
judit.feher.horvayne@bm.gov.hu

HÜBLER Viktória

RÁDIÓKOMMUNIKÁCIÓ ÉS ADATÁTVITEL BÉKE ÉS MINŐSÍTETT HELYZETBEN

Digitális rendszerek (szabványok)

Digitális rádiós rendszerek közötti alapvető különbség a csatorna fogalmában és a csatorna használatában (hozzáférésében) mutatkozik meg.

- TDMA – Time Division Multiple Access
- FDMA – Frequency Division Multiple Access
- FHMA – Frequency Hopping Multiple Access
- CDMA – Code Division Multiple Access

Általános jellemzők:

- ✓ Spektrumhatékonyság
- ✓ ITU-R és/vagy ETSI szabványnak megfelel

KENWOOD 3

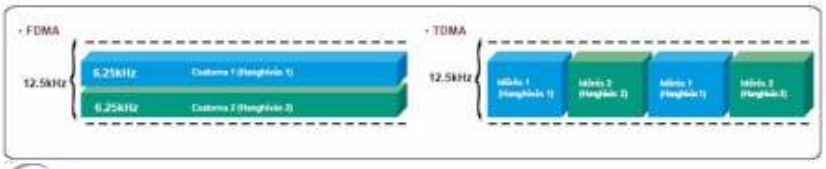
FDMA / TDMA

FDMA technológia

A csatornát az adott sávszélesség és az adott frekvencia határozza meg, hasonlóan az analóg rendszerekhez.

TDMA technológia

Adott sávszélességű és frekvenciájú rádiós jelet időrésekre osztja és így alakul ki a csatorna.



KENWOOD 4

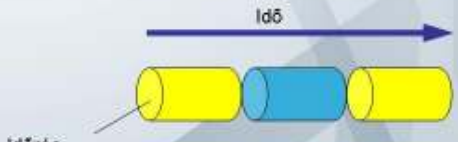
2. FDMA vagy TDMA?

KENWOOD

FDMA vagy TDMA?

KENWOOD
Listen to the Future

- TDMA (Time Division Multiple Access)
  - Előny
    - Alacsonyabb fogyasztás az analóg FM technológiával szemben
    - Teljes duplex üzemmód
  - Hátrány
    - Hatótávolság korlátozott a digitális protokoll miatt (kb. 35 km)
    - Infrastruktúra szükséges az összes funkció használatához
    - „Fizikailag" nem osztja meg a 12.5 kHz-et két csatornára

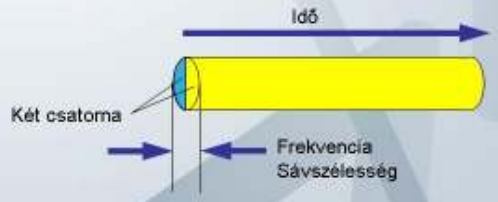


NEXEDGE™

FDMA vagy TDMA?

KENWOOD
Listen to the Future

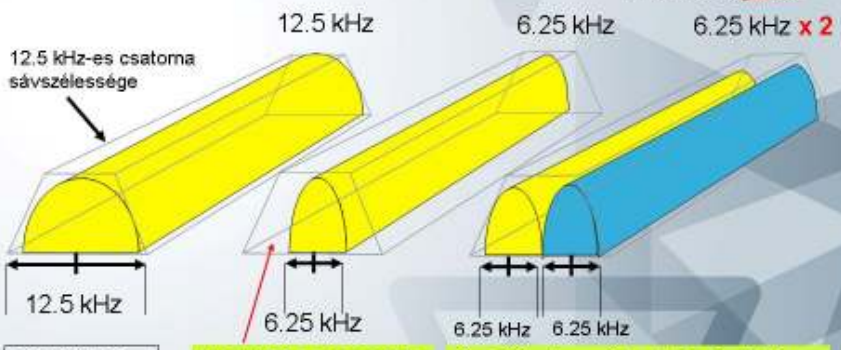
- FDMA (Frequency Division Multiple Access)
  - Előny
    - Nem limitált a hatótávolság (a protokoll által)
    - Ténylegesen 6.25 kHz-es csatorna
    - Könnyű átállási lehetőség analóg felhasználóknak
  - Hátrány
    - Frekvencia hatékonysága 1 az 1-hez ☹



NEXEDGE™

FDMA spektrum hatékonyság

KENWOOD
Listen to the Future



FDMA 1 hívás csatornánként

Nagyobb interferencia védelem

FDMA 1 hívás csatornánként

A vivő frekvenciák eltolásával két csatorna alakítható ki a 12.5 kHz-es sávszélességen belül

NEXEDGE™

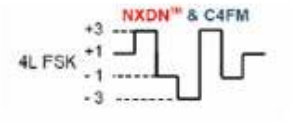
3. NEXEDGE ™

KENWOOD

NEXEDGE™ - NXDN™

- **NXDN™**
  - A neve és védjegye a Kenwood és Icom cégek által közösen fejlesztett digitális vezetéknélküli interfész protokollnak.
    - 4 LFSK moduláció
    - 12,5 és 6.25 kHz-es sávszélesség
  - Az NXDN™ hozzáférési módszer FDMA technológián alapszik.
  - NXDN ™ fejlesztők és gyártók létrehozták 2008 júliusában az NXDN Fórum-ot, melynek tagjai:

- Kenwood Corporation;
- ICOM Incorporated,;
- Kenwood USA Corporation;
- ICOM America Incorporated,
- Aeroflex Wichita Inc.;
- Daniels Electronics Ltd.;
- Ritron Inc.;
- Trident Micro Systems.



NEXEDGE™ KENWOOD 10

NEXEDGE™- készülékek

NEXEDGE™ KENWOOD 11

NEXEDGE – Mi az, hogy DIGITÁLIS?

A hang digitalizálása és digitális jelformában történő kisugárzása.

Fontosabb jellemzők:

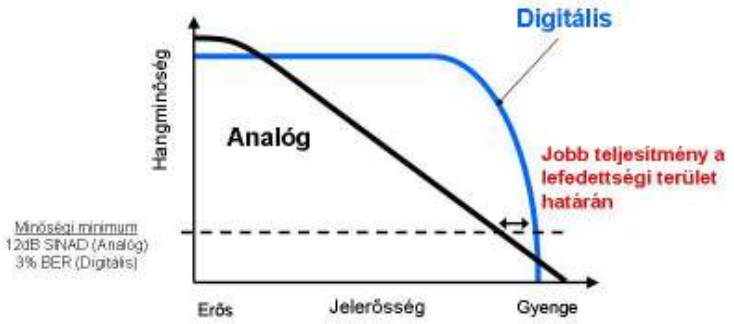
- Digitális jelzésrendszer és hangátvitel
- AMBE+2 analóg / digitális jelátalakító
- FDMA – Frequency Division Multiple Access
- 12.5 kHz vagy 6.25 kHz sávszélesség
- IP alapú kapcsolat a site-ok között

NEXEDGE™ KENWOOD 12

NEXEDGE – Lefedettség

A digitális hibajavító eljárásnak köszönhetően a lefedettségi terület határán is tisztán érthető hang és biztos adatátvitel érhető el.

→ Analóg FM rendszereknél kb. 20%-kal nagyobb lefedettségi terület



NEXEDGE™ KENWOOD 13

4. NEXEDGE készülékek

KENWOOD

NX-200/300 kézi hordozható adóvevő

- 5W / 512 csatorna / 128 zóna
- 12 gombos billentyűzettel is rendelhető
- 14 karakteres, alfanumerikus hívólista
- Háttérvilágítású LCD kijelző
- Térerő kijelzés (RSSI)
- 6 programozható funkció gomb az előlapon
- 2 funkció gomb a készülék oldalán
- Vészhívó gomb a készülék tetején
- 500 mW-os hangszóró
- VOX funkció
- Opciós panel csatlakozási lehetőség
- Programozható adás / vétel jelzés
- Akku töltöttségi szint kijelzés
- Időjárás védett tartozék csatlakozó
- Firmware frissítési lehetőség

KENWOOD 15

NX-700/800 mobil adóvevő

- Adóteljesítmény 1-25 W
- 512 csatorna / 128 zóna
- Levehető előlap (opció)
- 14 karakteres hívólista
- Háttérvilágítású LCD kijelző
- Térerő kijelzés (RSSI)
- Adás / Vétel / Hívás / Foglaltság jelző LED
- 4 fel/le funkció gomb
- 6 funkció gomb az előlapon
- 4W-os hangszóró
- DB-25-ös tartozék csatlakozó
- 9 programozható I/O port
- 2 programozható kimenet (relé)
- 12 gombos DTMF mikrofon (opció)

NEXEDGE™

KENWOOD 16

NXR-700/800 átjátszó és bázis állomás

- Átjátszó, bázis állomás és digitális vezérlő egyben
- 25 W adóteljesítmény
- Átjátszó, duplex vagy szimplex üzemmód
  - 30 csatorna programozható
- Analóg FM funkciók:
  - 16 QT/DQT átjátszó vezérlő (TOT, tartásidő, CW azonosító, stb…)
  - Külső vezérlők számára csatlakozási lehetőség (pl.: MPT1327)
- Digitális üzemmód:
  - 16 RAN átjátszó vezérlő (TOT, tartásidő, CW azonosító, stb…)
- Digital Trönkölt üzemmód (Software opció)
- Multi-Site trönkölt üzemmód, IP kapcsolattal (Software opció)

NXR-700	146-174 MHz
NXR-800	440-470 MHz

NEXEDGE™ KENWOOD 17

NXR-710E / 810E

Új NEXEDGE átjátszó

- 136-174 MHz VHF és 400-470 MHz UHF
- 30 csatorna programozható
- Analóg, vegyes és digitális üzemmód
- Kedvező ár
- Adóteljesítmény 5 – 50W
  - Folyamatos adás 25W-on
- 6 programozható funkció gomb
- 16 RAN vagy QT kódos átjátszó vezérlő

 KENWOOD 18

5. NEXEDGE üzemmódok

KENWOOD

NEXEDGE üzemmódok

Vegyes üzemmód

Analóg készülék adásindítása

KENWOOD 20

NEXEDGE üzemmódok

Vegyes üzemmód

Digitális készülék adásindítása

NEXEDGE™ KENWOOD 21

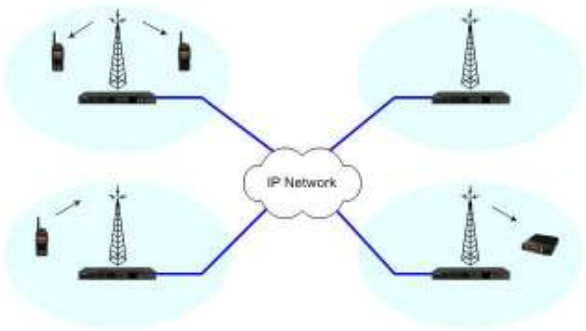
NEXEDGE üzemmódok

Vegyes átjátszó üzemmód

Analóg készülék adásindítása

KENWOOD 22

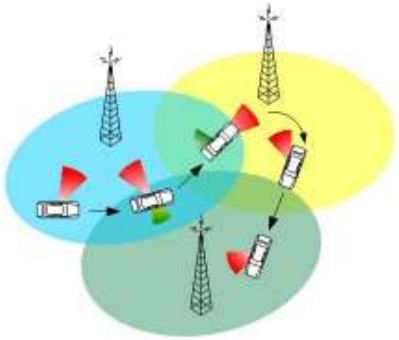
Konvencionális IP hálózat



A NEXEDGE rendszer konvencionális IP hálózati funkciójával átjátszó állomások köthetőek össze IP hálózaton keresztül.

KENWOOD 23

Site roaming funkció



A kézi és mobil rádiók automatikusan kiválasztják a legjobb térerőt biztosító átjátszó állomást.

KENWOOD 24

NEXEDGE üzemmódok

Digitális trönkölt – Single Site – 2-től 30 csatornáig

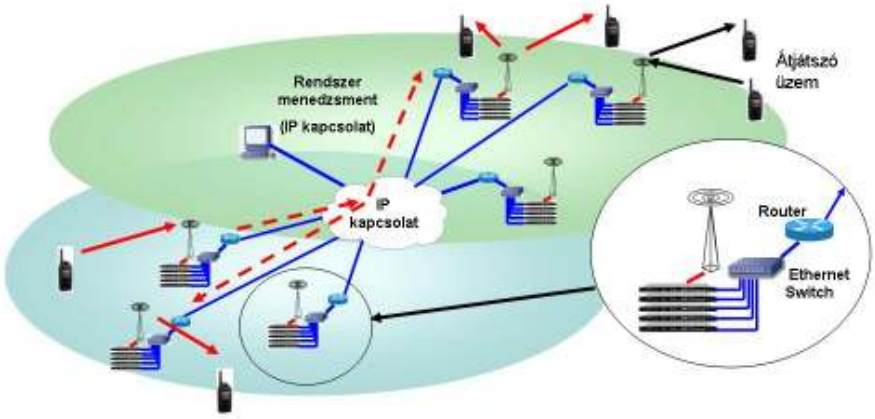
Funkciók:
- Egyéni hívás
- Csoport hívás
- Státusz hívás
- Adat hívások
- Titkosítás

NEXEDGE™

KENWOOD 25

NEXEDGE üzemmódok

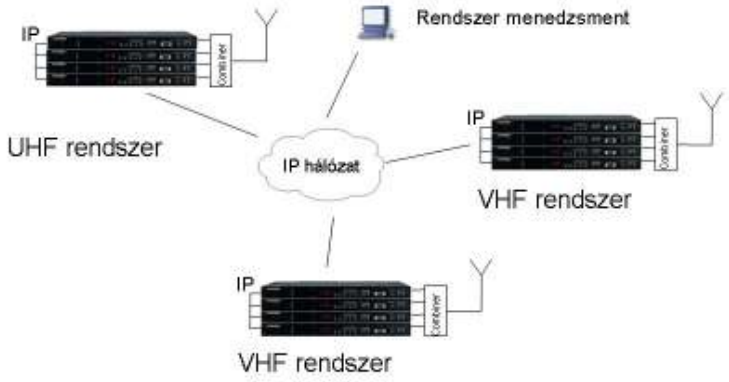
Digitális trönkölt – Multi Site – 16 site / 30 csatorna site-onként



KENWOOD 26

NEXEDGE üzemmódok

Digitális trönkölt – Multi Site – UHF / VHF rendszer összekapcsolása



NEXEDGE™ KENWOOD 27

6. NEXEDGE biztonsági funkciók

KENWOOD

Az üzenet biztonsága

A NEXEDGE® rendszer által kínált emelt szintű beszédtitkosítás növeli a felhasználók személyes biztonságát, csökkenti az érzékeny és bizalmas információk kiszivárgásának veszélyét.

● –Alapfunkció ○ –Opció	FM mód	NXDN mód	Biztonsági szint
Inverziós beszédtitkosító (beépített)	●		Alacsony
Opciós analóg titkosító panel Jelenleg nem rendelhető	●		Változó
NXDN™ titkosító (beépített)		●	Közepes
AES titkosító modul opció (2010-ben várható)		○	Magas

32,767 kód

KENWOOD 29

7. Kiegészítő eszközök

KENWOOD

KVT-11 M / KAS-11 M

KENWOOD
Listen to the Future

Képátviteli megoldás

- KVT-11 M
  - Kép tömöritő és küldő egység
- KAS-11 M
  - Kép fogadó és kezelő program
- Kompatibilis rádiók
  - NX-700E/800E
- Szállítás
  - 2010 október/november

KAS-11 M

KVT-11 M

KAS-10 – AVL és diszpécser program

- 250 jármű / személy kezelhető a programmal
- Hívástípusok: csoport, egyéni, körözvény, flotta, felügyelői
- Vészhívás funkció és üzemmód
- Státusz üzenet lekérdezés és fogadás
- Automatikus pozíció lekérdezés
- Geofencing – Terület figyelés
- Üzenetküldés:
  - NEXEDGE:
    - 100 karakter – rövid szöveges üzenet;
    - 4090 karakter – hosszú szöveges üzenet;
  - FLEETSYNC / 5-Tone:
    - 48 karakter – rövid szöveges üzenet;
    - 1024 karakter – hosszú szöveges üzenet;

NEXEDGE™

KENWOOD 33

KAS-10 – AVL és diszpécser program

NEXEDGE™ KENWOOD 34

KMC-47GPS/48GPS

- **KMC-47GPS / 48GPS**
- A következő rádió típusokhoz
  - KMC-47GPS : NX-200/300/200S/300S, TK-2180/3180
  - KMC-48GPS : TK-2170/3170

- Minden tekintetben jobb, mint a KMC-38GPS
  - Jobb érzékenység (SiRF Star III)
  - 30%-al kevesebb fogyasztás
  - Gyorsabb pozíció hidegindításnál

- Első szállítások
  - 2010 október

KENWOOD

9. Összefoglalás

KENWOOD

NEXEDGE – összefoglalás

- Digitális jelzésrendszer és hangátvitel
- AMBE+2 analóg / digitális jelátalakító
- FDMA – Frequency Division Multiple Access
- 12.5 kHz és 6.25 kHz csatornatávolság
- Nagyobb lefedettségi terület
- IP kapcsolat site-ok között

NEXEDGE™

 KENWOOD 37

NEXEDGE – összefoglalás

- VHF és UHF sávban rendelhető
- Ideális analóg rendszerről digitálisra áttérő ügyfeleknek
- Szimplex üzemmód
- Átjátszó üzemmód
- Konvencionális IP hálózat
- Single Site trönkölt üzemmód
- Multi Site trönkölt üzemmód
- Alkalmazások – Diszpécseri kezelők, programok

KENWOOD

Listen to the Future

NÉMETH József

A HÍRADÁS ÉS INFORMATIKA BIZTONSÁGPOLITIKAI ÖSSZEFÜGGÉSEI


NÉHÁNY LÉNYEGES MOMENTUM


MOTTÓ I.
A jel elvesztése egy telefonbeszélgetés során bosszantó lehet, de a harctéren akár halálos is.
MOTTÓ II.
Hosszú úton, ködben eltévedni kellemetlen, míg a háború ködében ugyanez a teljes megsemmisüléshez vezethet.


A megközelítés problematikája
• Indukció vagy dedukció?
• Elmélet vs. gyakorlat
• Teljes spektrumú képességek vs. erősen korlátozott képességek
• Hadműveleti és/vagy harcászati probléma?
• Stratégiai kommunikáció stratégiája?


Mi a biztonság?
• Fenyegetettség nélküli állapot (van ilyen?)
• Készség és képesség a védettség fenntartására és/vagy a fenyegetések/veszélyek elhárítására
Fontos összetevői
• Társadalmi biztonság
• Politikai dimenzió
• Gazdasági dimenzió
• Környezeti dimenzió
• Katonai dimenzió
valamint
• Információs, belbiztonsági dimenzió
• helyi szint
• regionális szint
• országos szint
• kontinentális szint
• globális szint


A biztonságpolitika kulcskérdése
A politikai, a döntéshozatali és az adminisztratív/végrehajtói szintek KOORDINÁLT működése/működtetése.
A híradás és informatika kulcskérdése
A különböző vezetési szintek tevékenységéhez szükséges híradó és informatikai eszközök KOORDINÁLT működése/működtetése.


KÖZÖS JELLEMZŐK
• A gyors/azonnali (helyzet)érzékelés és értékelés szükségessége
• Összetett rendszerek
• Elegendő és minőségi szellemi, anyagi (technikai) és személyi javak/források
• Hatékony eljárási (igazgatási, szervezési, végrehajtási) rend
• A veszélyek elhárításának követelménye, bekövetkezésük esetén azok mérséklése
• Rugalmasság
• Egységesség
• Hely (tér) és idő általi meghatározottság
• Folyamatos változás és fejlődés


ELVÁRÁSOK
A biztonságpolitika oldaláról:
Az információk (jelek) biztonságos, gyors, valósidejű és pontos továbbítása és tárolása.
A híradás és informatika oldaláról:
Megfelelő, minőségi és egyértelmű (világos) politikai, szakmai, megrendelői és alkalmazói környezet.


ZÁRÁSKÉNT I.
A jel megbízhatósága a sikeres harctéri tevékenységet jelenti.
ZÁRÁSKÉNT II.
A híradás és az informatika segít a háború ködének megkerülésében/eloszlatásában, így járulnak hozzá stratégiai célkitűzéseink megvalósításához.


Köszönöm a figyelmet!
NO SIGNAL
00:00
00-00-00
Dr. Németh József
okl. biztonság- és védelempolitikai szakértő
Zrínyi Miklós Nemzetvédelmi Egyetem
„Kommunikáció 2010" konferencia
2010. október 06.

KONCZ Bence

SPECIÁLIS CÉLÚ HADITECHNIKAI ESZKÖZÖK NEM POLGÁRI CÉLÚ FREKVENCIAMENEDZSMENTJÉNEK TÁMOGATÁSA

1. Probléma felvetése, előfeltételezés

PF: A Magyar Honvédségben jelentős számú analóg üzemű rádió berendezést használunk. Ebből fakadó problémák:

- Együttműködés a digitális rádiókkal - csak részleges kompatibilitás;
- Okmányrendszer hiányossága;
- A központilag kiosztott frekvencia kontingensen belül adott, hogy milyen frekvenciák használhatók (szűkülő együttműködési tartomány);
- A készülékek fizikai tulajdonságai sokszor nem teszik lehetővé a kapott frekvenciára való behangolást;

EF: Megoldásképpen segíteni kell a hiba kiszűrését a rendszerbe illesztés előtt;

(R-809 M2, rádió készülék nem tárgya a vizsgálatnak)

Page • 3

2. Jogi alapok

- A frekvencia igénylés folyamata is keretek között folyik, melyeknek alapját jogi meghatározások alkotják.
  - 346/2004. (XII. 22.) Korm. rendelet
    - Elosztási eljárás felépítése
    - MH feladatai
  - 29/2005. (VII. 27.) HM rendelet
    - Frekvencia kijelölés
    - Rádió engedélyezés

Page • 4

3. Kutatás irányai

- A témában való kutatásom két fő ágra osztható:
  - Okmányok témaköre
  - Műszaki, szervezési kérdések

Page • 5

3.1. Okmányok

A forgalmi rendszerben üzemelő állomás jelenleg egy Tartalék hívónévvel rendelkezik, ezáltal jobban ki van téve a rádióelektronikai zavarás lehetőségének.

Forgalmi okmányok

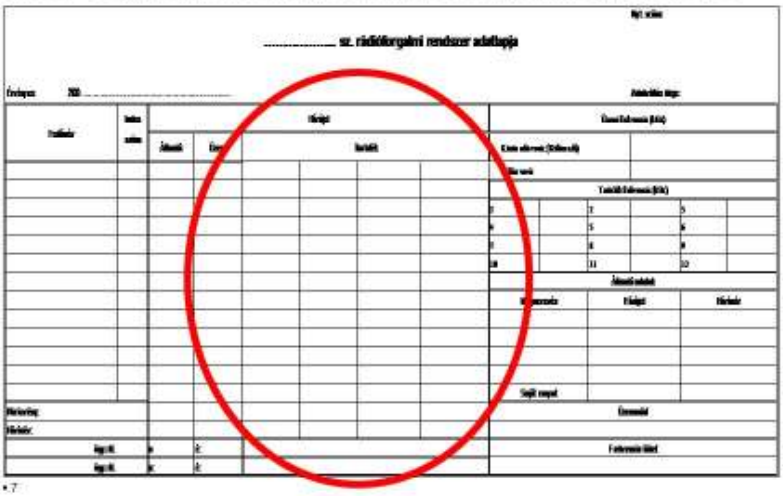
Rádió forgalmi adatlap

Hívónevek bővítése!

Page • 6

3.1. Okmányok

- Rádió forgalmi adatlap hiányossága/kiegészítése



Page • 7

3.2. Műszaki problémák R-123 MT

Page • 8

3.2. Műszaki problémák R-130

Page • 9

4. Mintaprogram

Page • 10

4. Mintaprogram

- Önütő frekvencia
- Forgalmazási sáv
- Hangolási tartomány
- Raszter távolság

A program fő feladata a megadott frekvenciák vizsgálata a rádió készülékek tulajdonságainak szempontjából!

Page • 11

4. Mintaprogram

- A program az egyes készülékek önzavarással fedet frekvenciáit tartalmazó táblázatokból álló adatbázis segítségével dolgozik, valamint képes fölajánlani együttnűködési frekvenciákat egyezés esetén.

R-130 rádió berendezés önzavarással fedett frekvenciá			
1	2	3	4
1520	3500	6300	8650
1600	3800	6390	9600
1800	3900	6400	9800
2000	4000	7600	10000
2100	4300	7800	10160
2280	4400	8000	10170
2400	4650	8160	10180
2800	4900	8170	10190
2840	4960	8180	10400
2900	5400	8190	10650
3040	5800	8390	10800
3100	6000	8420	talált

R-123 MT rádió berendezés önzavarással fedett frekvenciá			
1	2	3	4
21300	28725	37050	44475
22225	29625	37975	45375
22250	29650	38000	45400
23600	31325	39350	45450
23625	31475	39375	47225
23650	31500	39400	47250
23825	31525	39575	47275
27525	32975	43200	47475
28700	35475	44450	51200

Page • 12

4. Mintaprogram

Tekintsük át a program működését!

Page • 13

5. Konklúzió

- RFR adatlap változásai
- A program válaszlépés a problémákra
- Továbbfejleszthetőség
- Mindez egy átlagos platformon

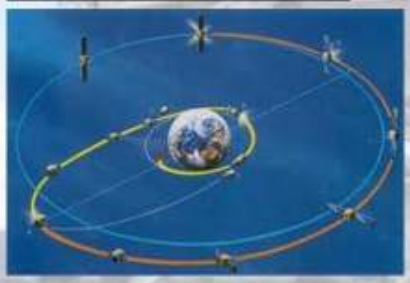
Page • 14

Köszönöm a figyelmet!

PARÁDA István

MŰHOLDAS ANTENNARENDSZEREK GYAKORLATI ALKALMAZHATÓSÁGA A MAGYAR HONVÉDSÉGBEN

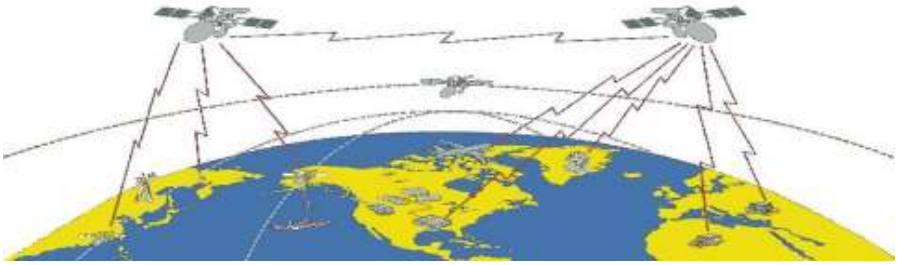
I. Fejezet: Áttekintés



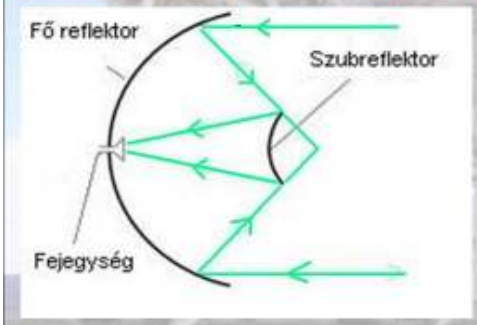
- Történelem
- Műholdas pályák
  - LEO (Magasság: 500-2000km. Gyakori felhasználás: meteorológiai, tudományos, telefon kapcsolatok, katonai. Élettartam: 5 év).
  - MEO (Magasság: 2000-35,800 km. Felhasználási területek: GPS és katonai. Élettartam:10-15 év).
  - GEO (Magasság:35,786 km, GSO. Élettartam: 10-15 év).
  - HEO (Magasság akár 40,000km is).

I. Fejezet: Áttekintés

- A műholdtávközlés lényege, hogy a műhold veszi az irányába sugárzott jelet, majd megváltoztatja a vivőfrekvenciát (keverés), és felerősítve visszasugározza a kívánt területre.
- A földi vevőállomások és a műhold nagy távolságra vannak egymástól ezért, mialatt a műhold jele a vétel helyére ér erősen lecsökken (szétszóródik) igy a jelteljesítmény összegyűjtésére- egy antennát helyeznek el.
- Frekvenciák



I. Fejezet: Áttekintés



- Antennák csoportjai (egy vagy több műhold jelét veszi az utóbbinál fix és motorizált)
- Antennák fajtái:
  - Prímfókuszos (ezen belül a szubreflektoros is)
  - Ofszet
- Antennák főbb jellemzői
- Összeállítás
- Katonai alkalmazás (navigáció,távközlés, felderítés,tűztámogatás)

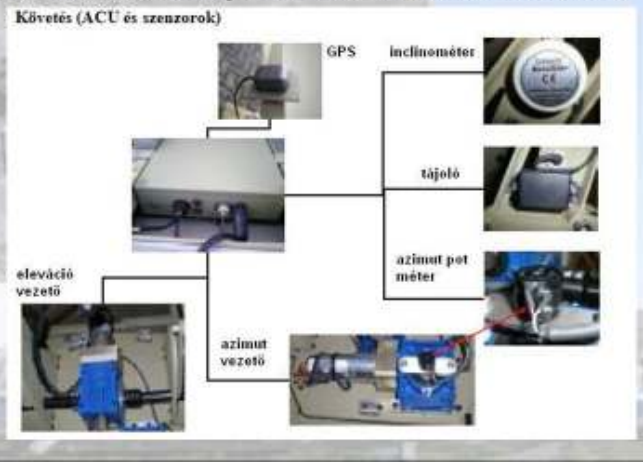
II. Fejezet: Kétsávú műholdterminál

- Kétsávú műholdas terminál katonai szempontból fontos követelményei.
- Kültéri egységei (maga az antenna; felkeverő erősítő; lekeverő erősítő; antennavezérlő; GPS jelforrás; meteorológiai állomás.)
  - QDMA antenna ami összetett reflektorpanelekből áll.

- A felkeverő erősítő átkonvertálja az L sávú frekvenciát a műhold frekvenciájává, X sávba.
- Alacsony zajszintű konverter, feladata az antennáról érkező jelek erősítése és lekonvertálása a műholdvevő frekvenciájára. A vételi frekvencia lehet Ku vagy X sáv ezt L sávba lekeveri a helyi oszcillátor frekvencia által.

II. Fejezet: Kétsávú műholdterminál

- Az antennavezérlő egység gondoskodik a manuális és automatikus műhold antennakövetésről. A követést a következő eszközök befolyásolják: maga az ACU, GPS, billentés érzékelő, tájolót, koordináta kalkulátort.



- Beltéri berendezés
  (switchek; GPS forrás; FO modem; műholdas modem)
  - A hálózati switch biztosítja a hálózati összeköttetést a telepített berendezések és a főhálózat között.
  - A referenciaforrást azaz 10MHz frekvenciát a GPS-ből vett jelből állítja elő.
  - FO modem a laptop és beltéri egység összekötése illetve adatforgalom.

II. Fejezet: Kétsávú műholdterminál

- A műholdas modem támogatja a különböző modulációkat. Legfontosabb funkciója hogy a digitális jeleket modulokra bontja és egy fokozaterősítő segítségével és a konténerbe továbbítja az adatokat.

II. Fejezet: Kétsávú műholdterminál

Elemek közti kapcsolatoknál fontos a csőtápvonal és a koax kábel.

Csomagolás és összeszerelés: a BBSST rendszer összesen 4 dobozból áll. Manuális szögbeállítás is kivitelezhető. Összeszerelésnél fontos a sorrend.

III. Fejezet: Telepíthető műholdas terminál

- Telepíthető műholdas földi terminálok
- Kültéri egységei (maga az antenna, adó alrendszer, vevő alrendszer, antennavezérlő alrendszer, ellenőrző és irányító egység, GPS referenciaforrás, kiegészítő rendszer)

– 2, 4 méteres hatszögű karbon szálas tányér.

– Adó alrendszer koax kábelbe kombinálja a modem közép frekvencia jeleit. Ez a koax kábel átmegy az IFL elosztó tápon keresztül a felkeverő erősítő átalakító rádió frekvencia bemenetébe. A felkeverő erősítő átalakítja a jelet L sávból X sávba.

III. Fejezet: Telepíthető műholdas terminál

– Vevő alrendszer.

Az LNB lekonvertálja és erősíti, az rádió frekvencia jelet mielőtt ezt megkapja a modemen, L sávon koax kábelen keresztül

– Antennavezérlő alrendszer.

Az antennavezérlő egység jellemzője az automatikus irányzás és helymeghatározás.

- Ellenőrző és irányító egység(maga a laptop).
- A frekvencia jel alrendszer biztosítja a 10 MHz frekvenciajelet és az időjelet a DSGT felszerelés számára. Ezt egy 20 méteres koax kábel segítségével oldja meg.
- Kiegészítő rendszer: meteorológiai állomás, villámhárító rendszer, jégtelenítés.

III. Fejezet: Telepíthető műholdas terminál

- Beltéri berendezés Megengedi az egyidejű átvitelt és fogadást a 6 duplex (kétirányú) hordozón, valamint csatlakoztatja és szinkronizálja az időzítő jelet 10 MHz külső frekvencia által, amit a DSGT biztosít.
- Teljesítmény: A nem megszakítható tápellátás. Ezeket az UPS-eket a missziók alatt a NATO nyújtja.

III. Fejezet: Telepíthető műholdas terminál

- A DSGT összeszerelésénél a egyértelműen címkézett rádió frekvenciás és tápkábeleket csatlakoztatjuk. A rendszer csőtápvonal része, ami az SSPA-t csatlakoztatja a fejegységhez,kétfajta: merev és rugalmas beleértve a szűrőt is.

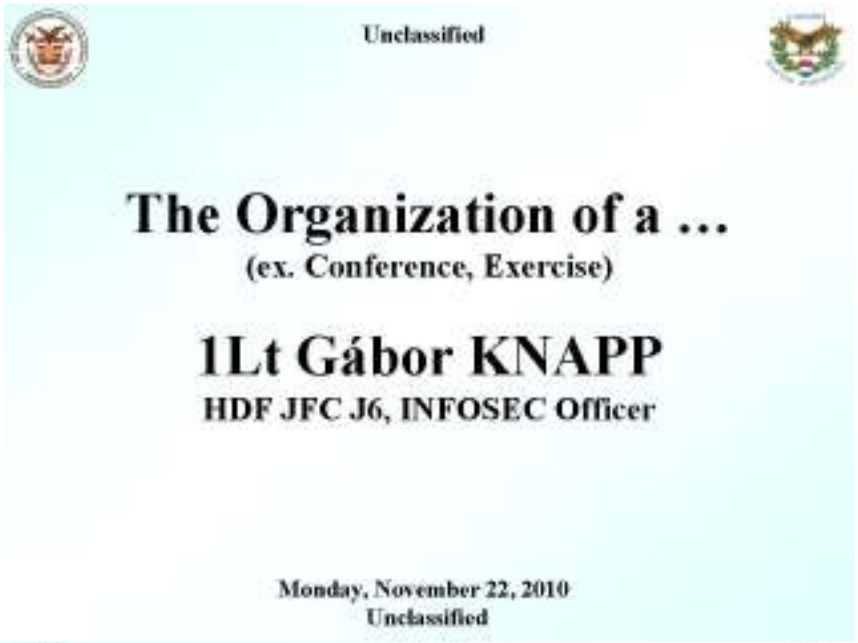
Következtetés

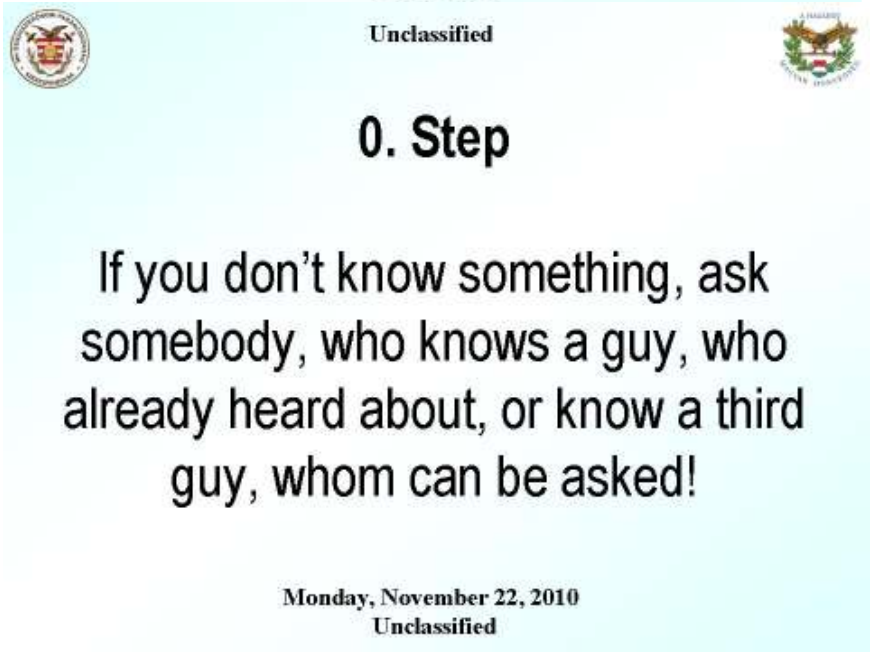
- Következtetés: Az antennarendszereknek a katonai szempontból legfontosabb előnye a könnyű össze és szétszerelés, valamint a nagyfokú mobilitás. A civil cég által biztosított rendszer talán hátrány, viszont alkalmazását figyelembe véve megéri, hisz korábban lényegesebben nagyobb rendszereket használtak az információáramlás biztosításához.

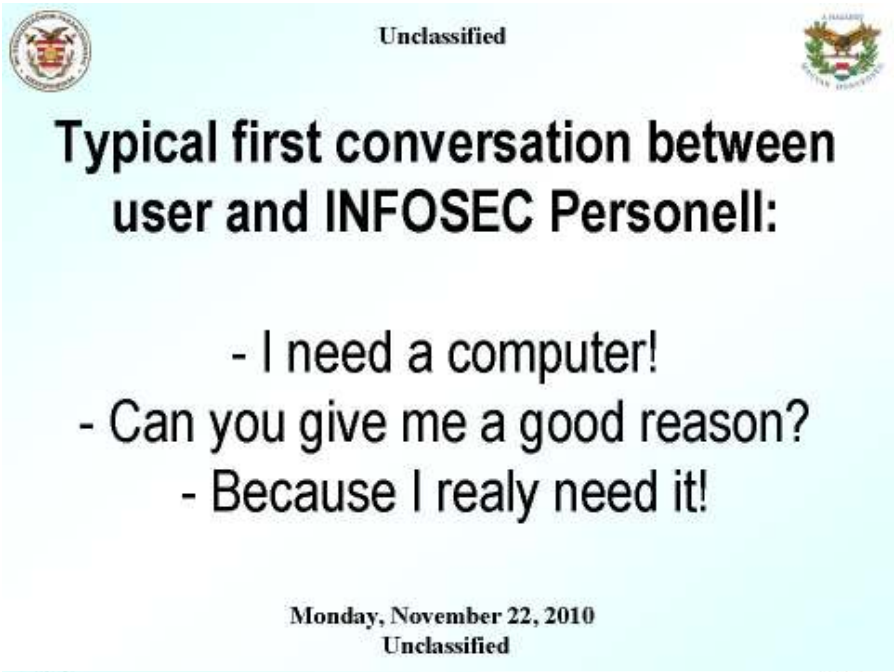

Köszönöm a figyelmet!
Kérdések?

Gábor KNAPP

THE ORGANISATION OF A …



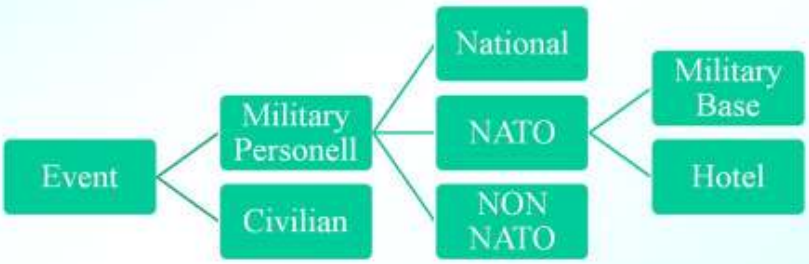



Unclassified
Typical first conversation between user and INFOSEC Personell:
- I need a computer!
- Can you give me a good reason?
- Because I realy need it!
Monday, November 22, 2010
Unclassified


Unclassified
1. Step
You have to know everything BEFORE start a planning!
There shouldn't be any unknown or variable!
Monday, November 22, 2010
Unclassified

Who (personnel, nationality)
What (highest classification of the information)
When (date)
Where (location)
What (equipment)
How (maintenace)

Variant solutions:



Unclassified

2. Step

Collecting of Information
Lucky if on Location,
Strong co-operated by maintenance personnel

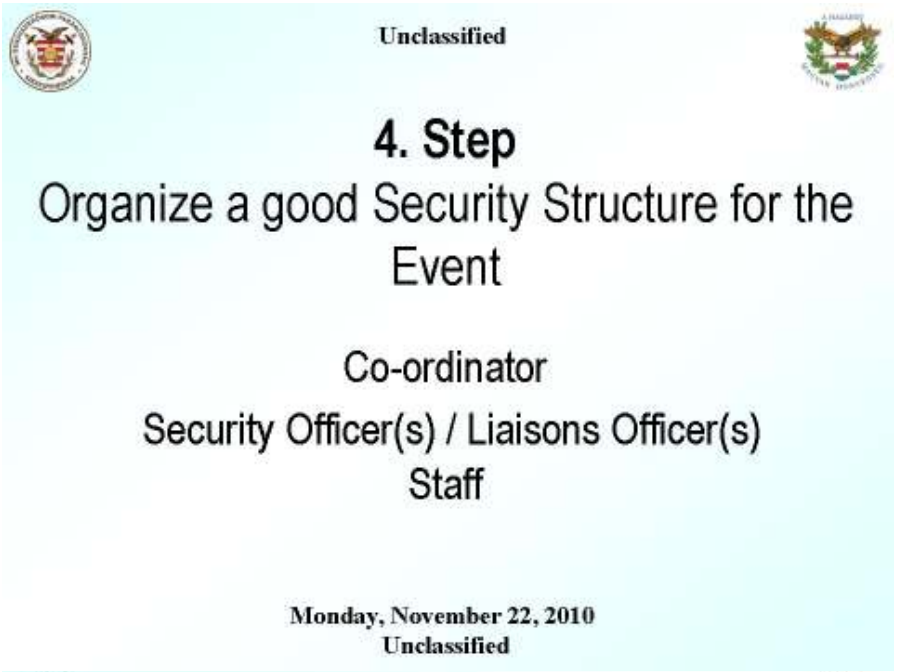
Monday, November 22, 2010
Unclassified

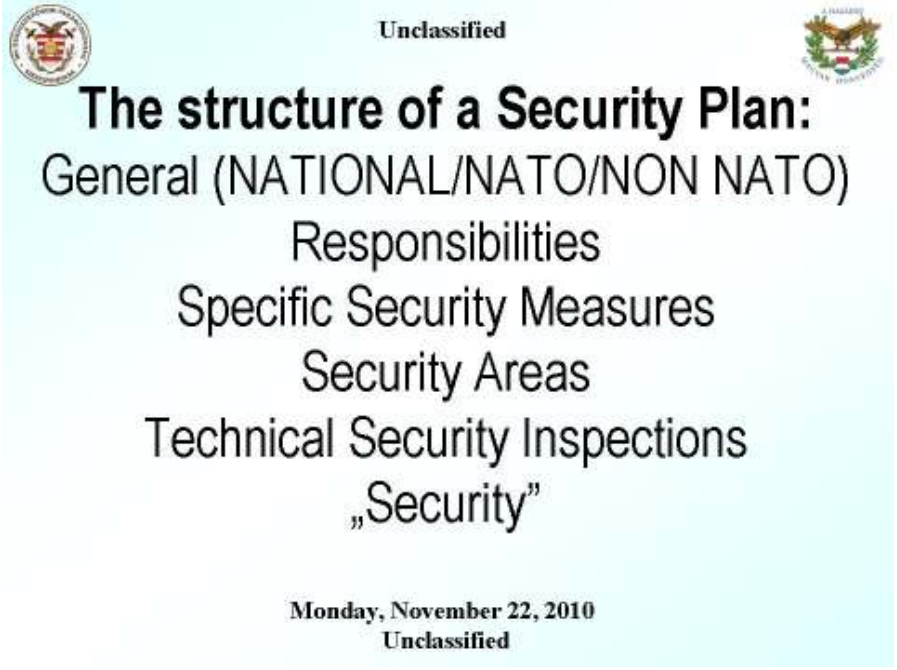
Unclassified

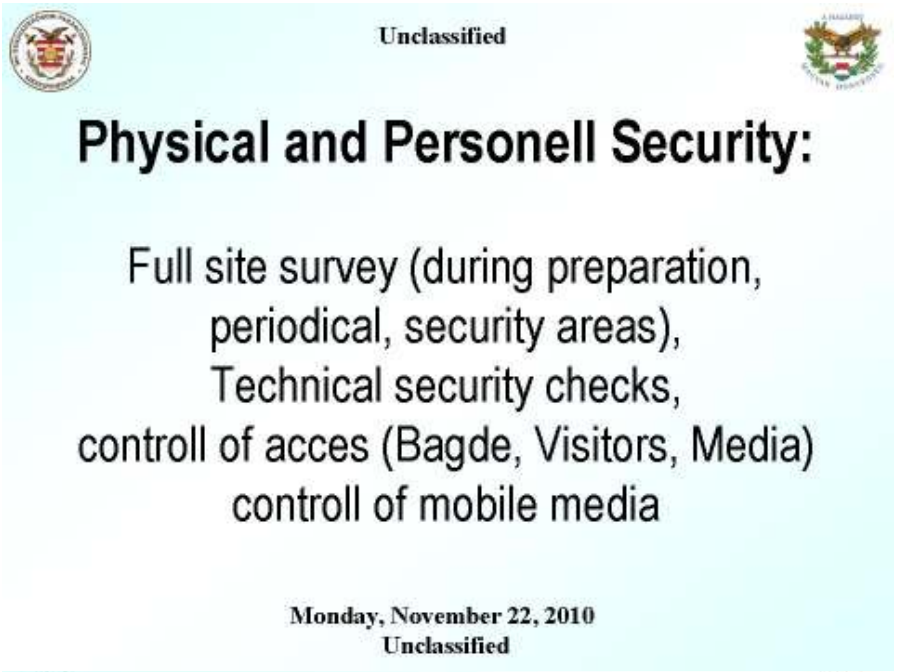
3. Step

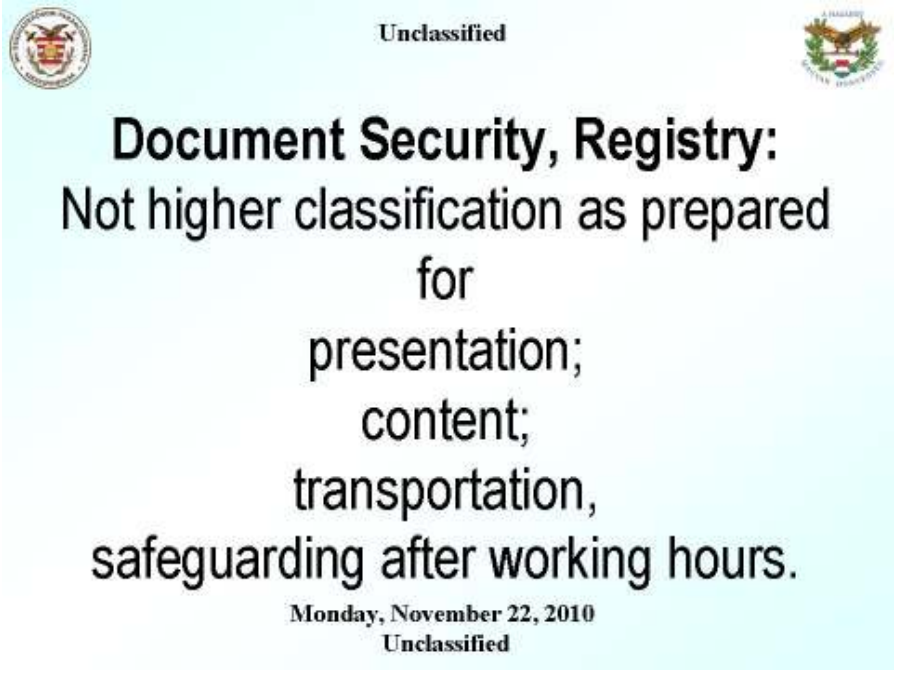
Brainstorming???? NO!!!

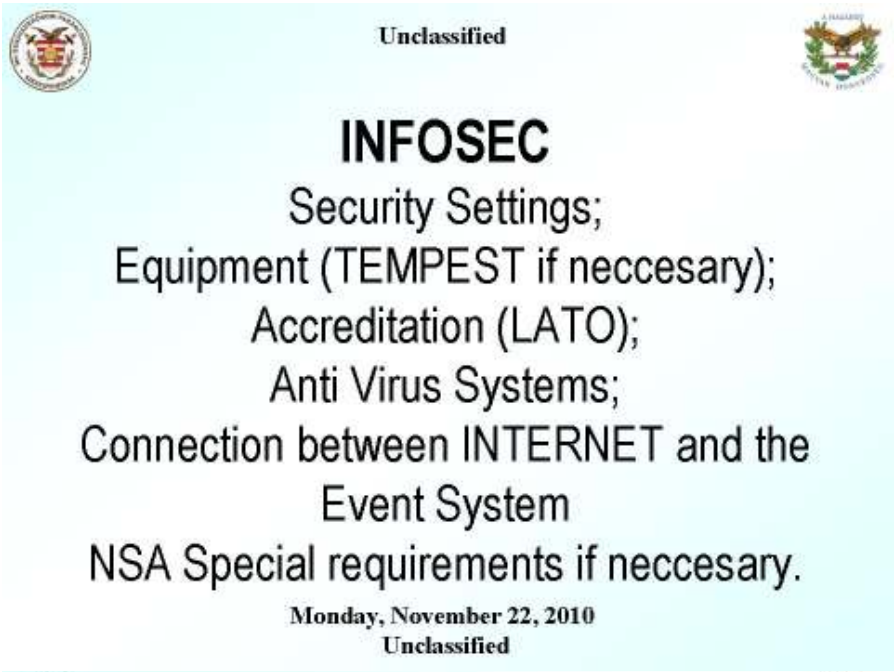
Monday, November 22, 2010
Unclassified

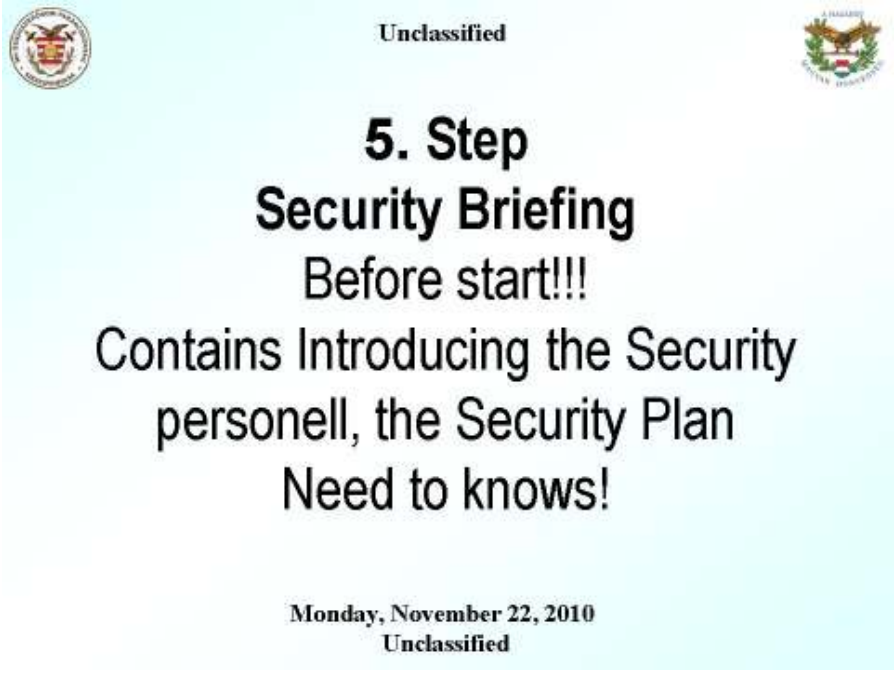

Unclassified
4. Step
Organize a good Security Structure for the Event
Co-ordinator
Security Officer(s) / Liaisons Officer(s)
Staff
Monday, November 22, 2010
Unclassified


Unclassified
The structure of a Security Plan:
General (NATIONAL/NATO/NON NATO)
Responsibilities
Specific Security Measures
Security Areas
Technical Security Inspections
„Security"
Monday, November 22, 2010
Unclassified


Unclassified
Physical and Personell Security:
Full site survey (during preparation,
periodical, security areas),
Technical security checks,
controll of acces (Bagde, Visitors, Media)
controll of mobile media
Monday, November 22, 2010
Unclassified

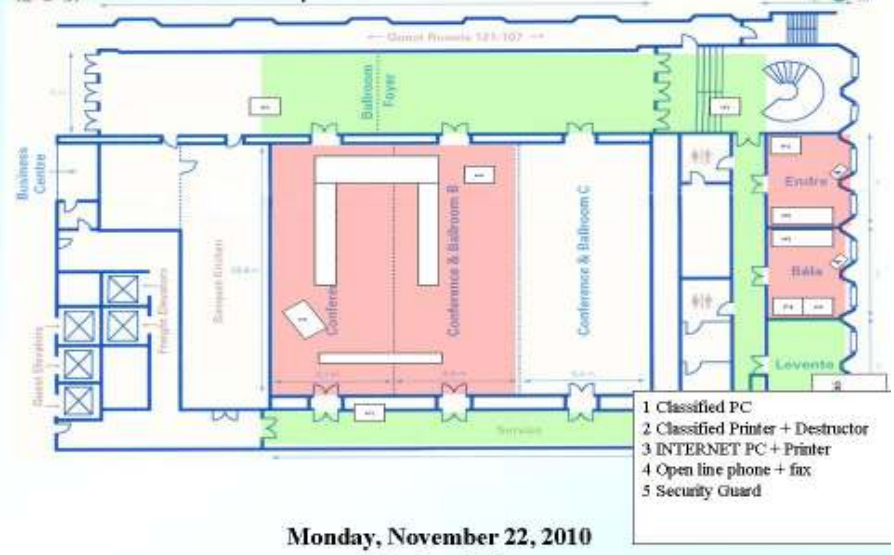

Unclassified
Document Security, Registry:
Not higher classification as prepared
for
presentation;
content;
transportation,
safeguarding after working hours.
Monday, November 22, 2010
Unclassified


Unclassified
INFOSEC
Security Settings;
Equipment (TEMPEST if neccesary);
Accreditation (LATO);
Anti Virus Systems;
Connection between INTERNET and the Event System
NSA Special requirements if neccesary.
Monday, November 22, 2010
Unclassified


Unclassified
5. Step
Security Briefing
Before start!!!
Contains Introducing the Security personell, the Security Plan
Need to knows!
Monday, November 22, 2010
Unclassified

Unclassified

Example for an Event in a Hotel



Monday, November 22, 2010
Unclassified

Unclassified

During the event:

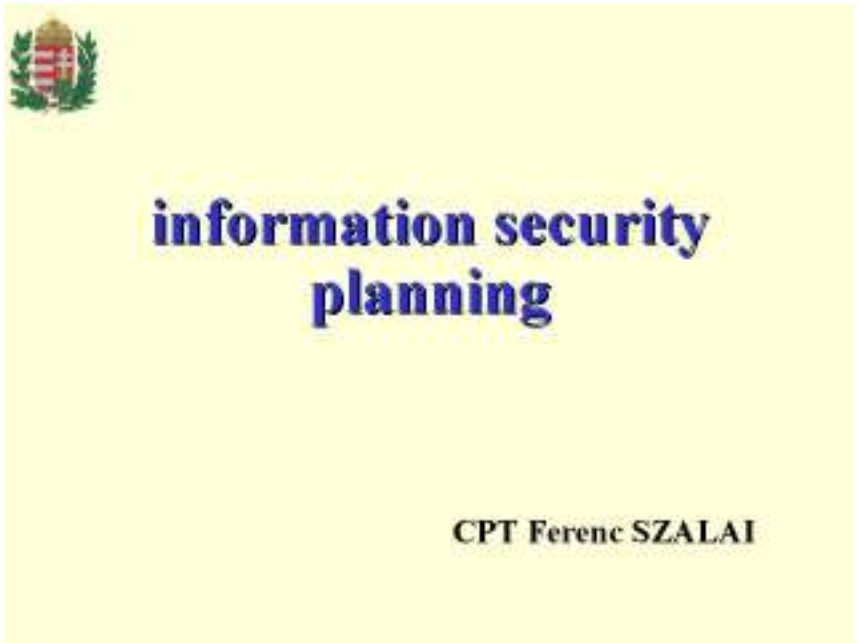
- Preparation
- Organization
  - Furnishing;
  - Operation and Use;
  - Solving any problems on place
- „Closing remarks”
  - Transportation
  - Downgrading of classification;
  - Destruction

Monday, November 22, 2010
Unclassified


Thank You for Your Attention!
Gabor KNAPP
+36306856643
Unclass Email: knapp.gabor@mil.hu
NS mail:

Ferenc SZALAI

INFORMATION SECURITY PLANNING



IS-IA

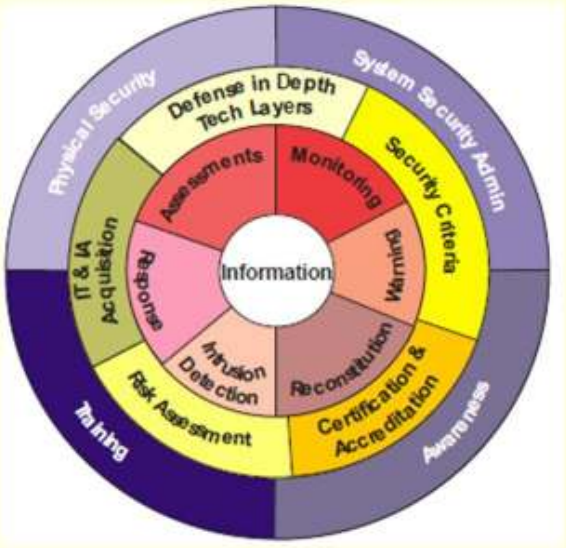
- **Information Security**
- **Information Assurance** – measures to protect and defend information and supporting systems, services and resources by ensuring their availability, integrity, **authentication**, confidentiality, and **nonrepudiation**. This includes providing for restoration of information systems by incorporating **protection**, **detection**, and **reaction** capabilities

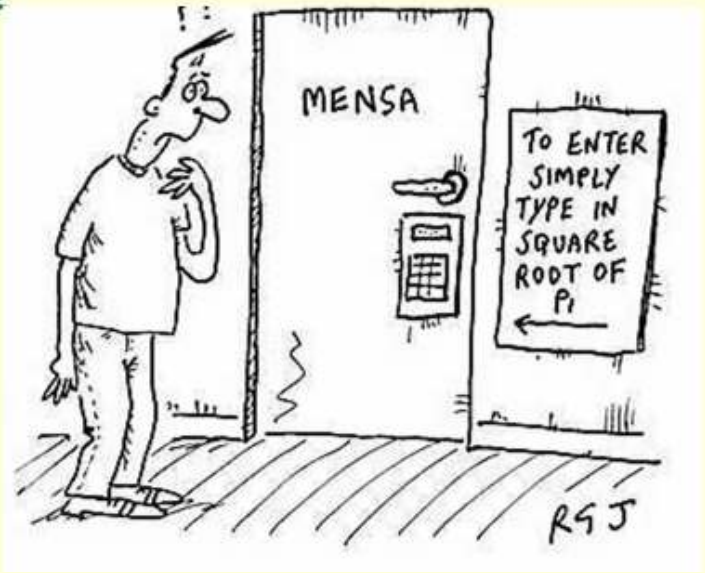
Foundations for IA

- Hardware and Firmware Security
- Secure Operating Systems
- Security-Centric Programming Languages
- Security Technology and Policy Management Methods and Policy Specification Languages
- Information Integrity
- Cryptography
- Multi-Level Security
- Secure Software Engineering
- Fault-Tolerant and Resilient Systems
- Integrated, Enterprise-Wide Security Monitoring and Management
- Analytical Techniques for Security Across the IT Systems Engineering Life Cycle

- Classified network
- Open communication network

Defense in depth





Risk assessment

- What assets are at risk (threats and vulnerabilities of CIS)
- What is the impact or consequence if the identified vulnerabilities are exploited successfully

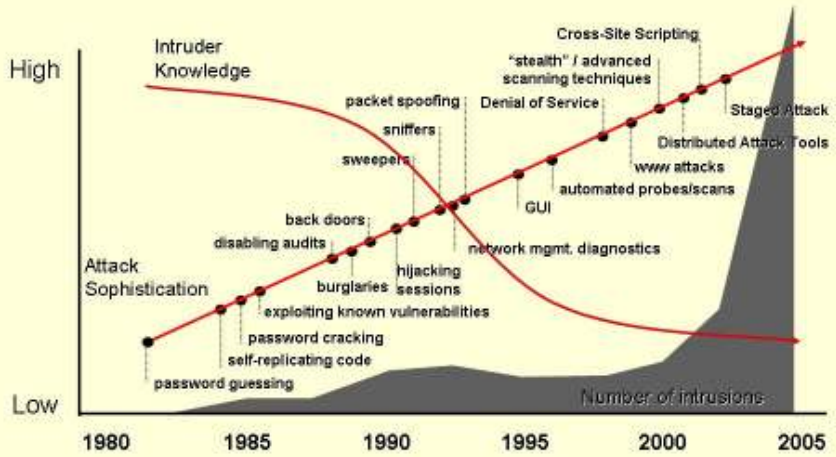
Threat

- In general, Cyber Threat stands for any kind of threat that exists against our CIS equipment.
- The threat can come from outside, or inside the organization, and affects the organization Intranet and/or the external interfaces
  - Insiders – deliberate or accidental
  - Outsiders – terrorists, hackers etc
  - Accidental – fire, flood, equipment malfunction

Today

- Vunerable web apps
- Sophisticated phishing
- Spam
- Social media attacks
- Identity theft
- Exploiting the latest technology
- Rise in portable data
- Complacency

Developing ease of initiating attacks

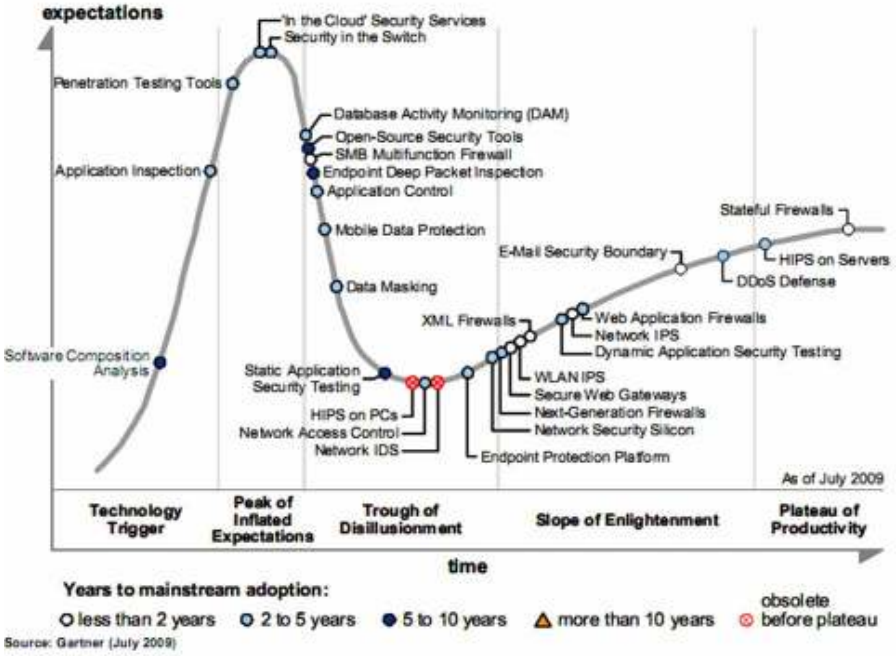


Future

- International Forecast (researches)
- NATO Architecture Framework v3 NSV-9 Technology Forecast
- EU Forecast
- National Forecast
- Organization Forecast (IT Strategy)

Research

- Hype Cycle for Infrastructure Protection



Future

- Securing virtualized environments
- Appliances
- Software-as-a-Service (SaaS) (one-to-many)
- Cloud computing
- IS in Web 2.0
- Securing mobile devices

Efforts

- Responding to unusual threats via standard security approaches (with minor modifications)
- Remaining - Prioritize

Plan

- Plan – implement
- allocate resources
  - HR
  - Organization
  - Services
  - Devices

Plan

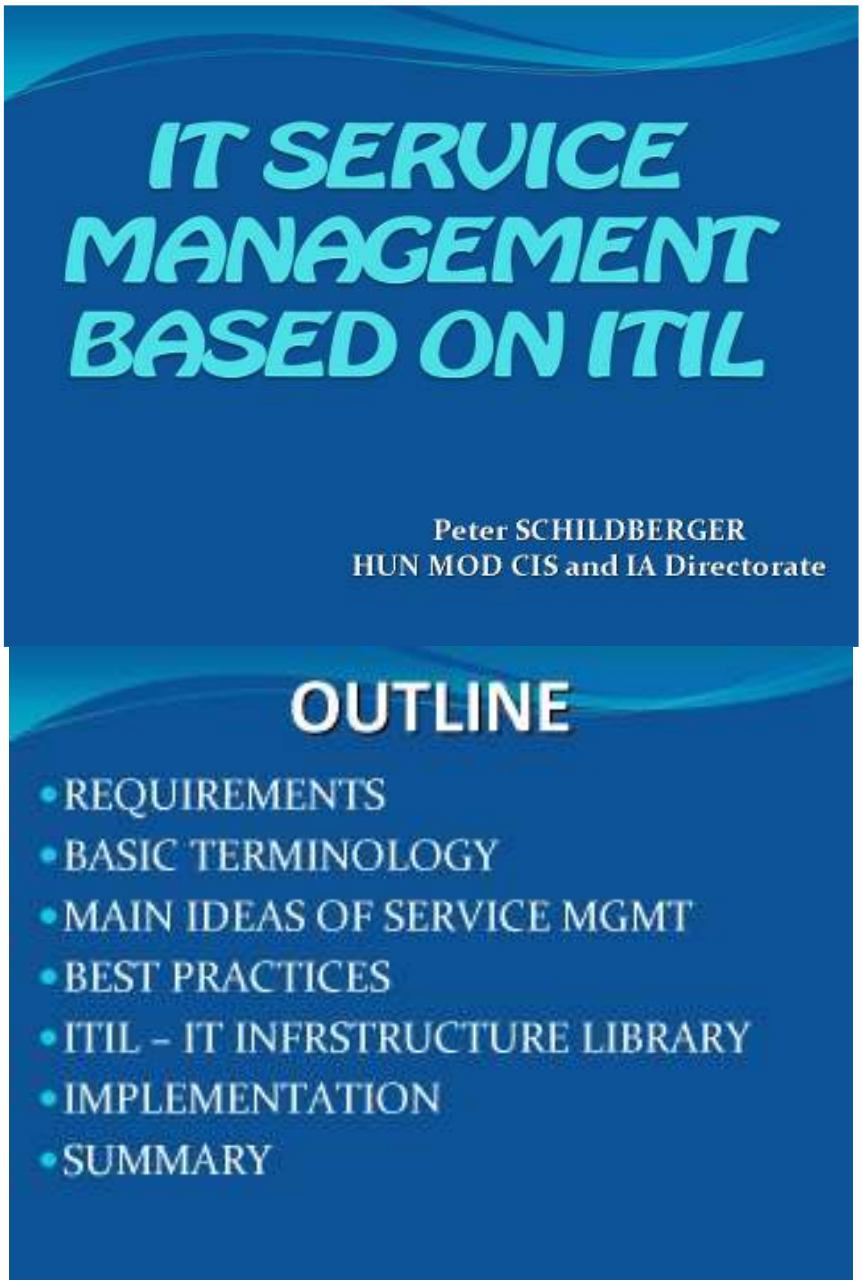
- Authority
- Roles and Responsibilities
- Security Program
- Security Components
- Risk Management
- Vulnerability Assessments
- Security Policy
- Organization of Information Security
- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Acquisition, Development and Maintenance of Information Systems
- Management of Information Security Incidents
- Management of Business Continuity
- Compliance
- Implementation

Questions?

No – Lunch
Yes – Start from begining

Peter SCHILDERBERG

IT SERVICE MANAGEMENT BASED ON ITIL

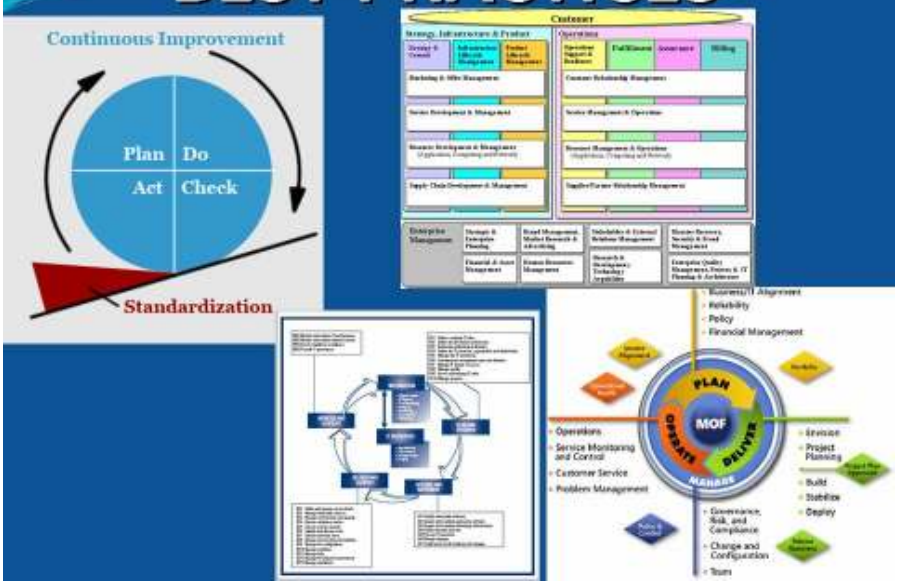


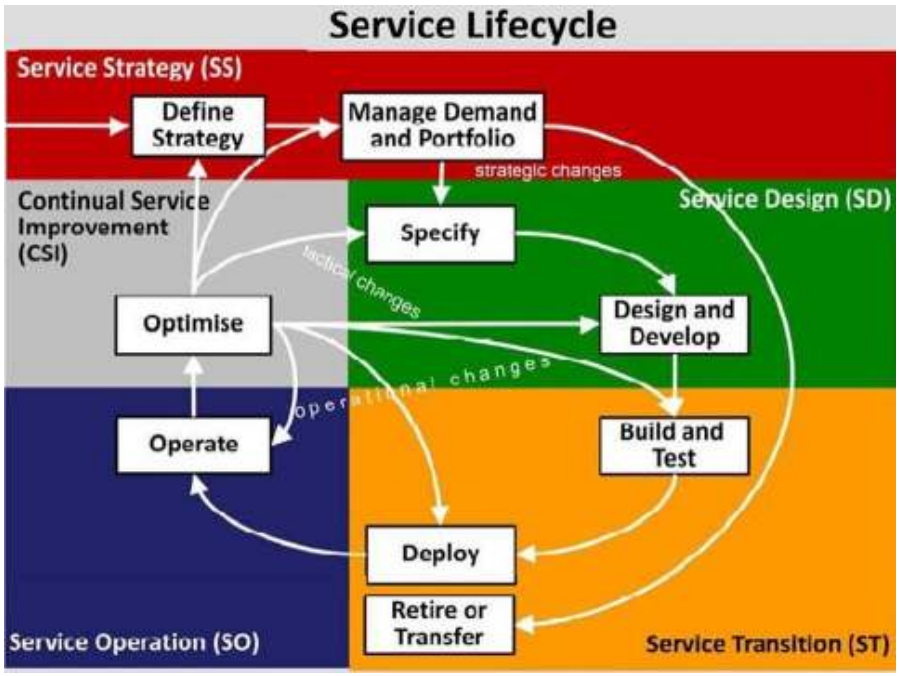

REQUIREMENTS
CIS COP
SLM
Configuration Management
Real time monitoring / measurement reports
End to end visibility
...
Cost effective
Quality
Value creating
BASIC TERMINOLOGY
Service – A means of delivering value to Customers by facilitating Outcomes Customers want to achieve without the ownership of specific Costs and Risks.
Service Management – a set of specialized organizational capabilities for providing value to customers in the form of services.

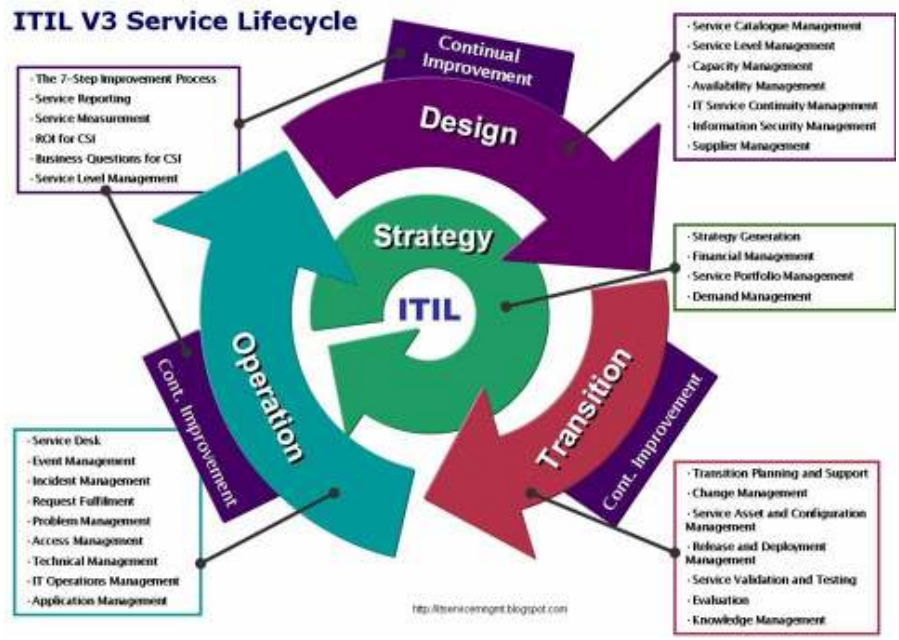
MAIN IDEAS OF SM

- Vision and strategy– overarching guideline that defines the role and place of IT from the point of view of business;
- Control – the goals and targets IT is facing and their tracking from the strategy implementation point of view;
- Processes – a structured set of activities designed to accomplish a specific objective;
- People – competence and capability for the implementation of processes;
- Technology – supporting infrastructure required for the implementation of processes;
- Organisational culture – the behaviour and attitude of business towards IT.

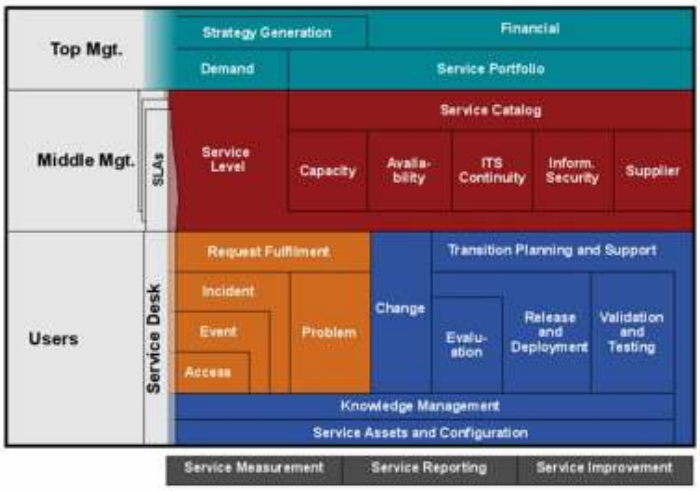
BEST PRACTICES




Service Lifecycle
Service Strategy (SS)
Define Strategy
Manage Demand and Portfolio
strategic changes
Continual Service Improvement (CSI)
Service Design (SD)
Specify
tactical changes
Optimise
Design and Develop
operational changes
Operate
Build and Test
Deploy
Retire or Transfer
Service Operation (SO)
Service Transition (ST)

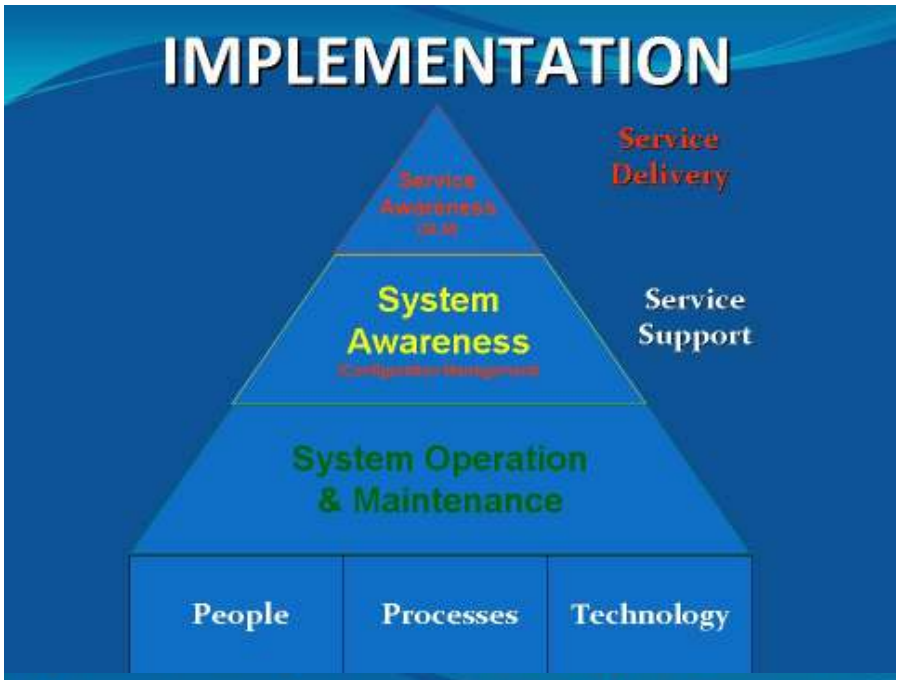

ITIL V3 Service Lifecycle
Continual Improvement
Design
Strategy
ITIL
Operation
Transition
Cont. Improvement
Cont. Improvement
· The 7-Step Improvement Process
· Service Reporting
· Service Measurement
· ROI for CSI
· Business Questions for CSI
· Service Level Management
· Service Catalogue Management
· Service Level Management
· Capacity Management
· Availability Management
· IT Service Continuity Management
· Information Security Management
· Supplier Management
· Strategy Generation
· Financial Management
· Service Portfolio Management
· Demand Management
· Service Desk
· Event Management
· Incident Management
· Request Fulfilment
· Problem Management
· Access Management
· Technical Management
· IT Operations Management
· Application Management
· Transition Planning and Support
· Change Management
· Service Asset and Configuration Management
· Release and Deployment Management
· Service Validation and Testing
· Evaluation
· Knowledge Management

ITIL v3: The Map



IMPLEMENTATION

- Top managements commitment for change and strategic direction;
- Clear formulation of targets, tracking and measuring their realisation;
- Accepting innovation and new methods of work;
- Clear understanding of business activities including all stakeholders;
- IT should understand business needs,
- Business should understand the capabilities of IT;
- Information available to all requiring it;
- Keeping pace with technology in order to exploit capabilities feasible supporting business needs



There is confusion about ITIL, stemming from misunderstandings about its nature. ITIL is, as the OGC states, a set of best practices. The OGC doesn't claim that ITIL's best practices describe pure processes. The OGC also doesn't claim that ITIL is a framework, designed as one coherent model. That is what most of its users make of it, probably because they have such a great need for such a model...

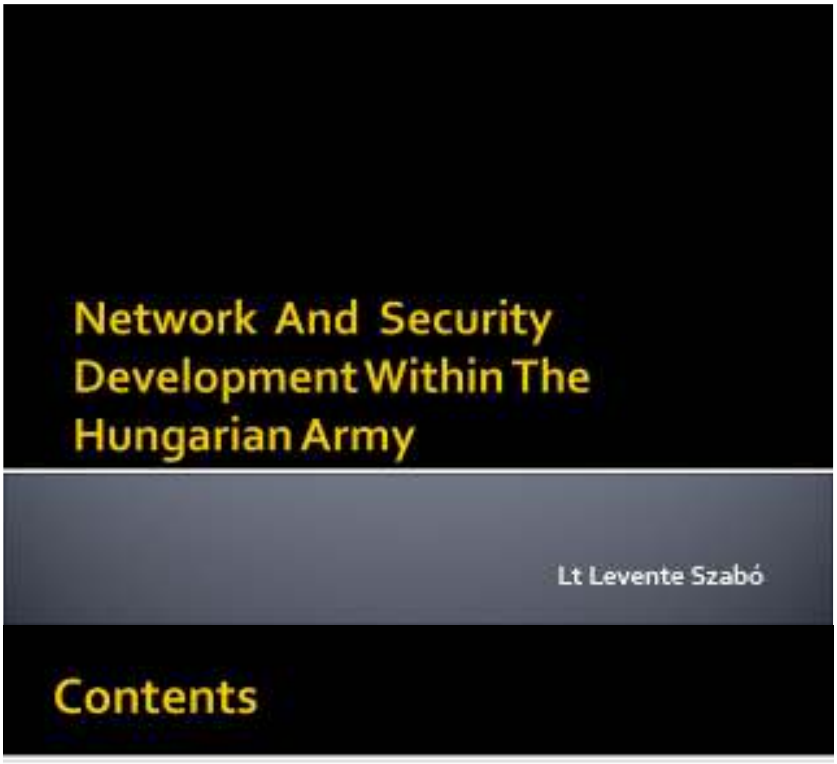
SUMMARY

- Long term commitment
- Best (good) practices to be applied with customisation
- Significant non-technical preparation
- People – processes - technology
- Phased approach

QUESTIONS

Levente SZABÓ

NETWORK AND SECURITY DEVELOPMENT WITHIN THE HUNGARIAN ARMY

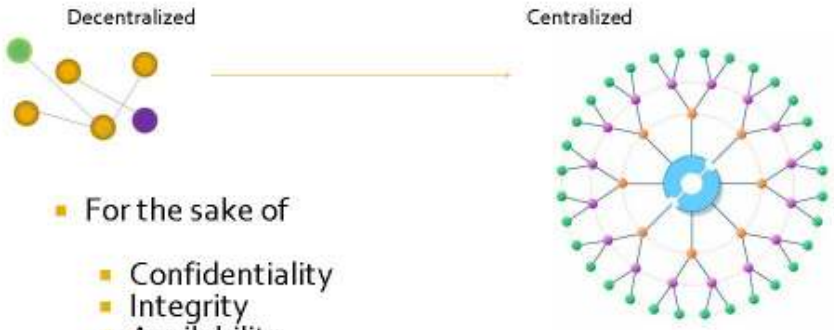


Historical overview

- Army IT networks
  - Small Local Area Networks, or stand-alone workstations
  - A few networks connected in the Budapest area
  - Connections built between Budapest and other main HQ's
  - Smaller units connected and the existing network upgraded
  - Ongoing development..

Historical overview

- In general:



- For the sake of
  - Confidentiality
  - Integrity
  - Availability

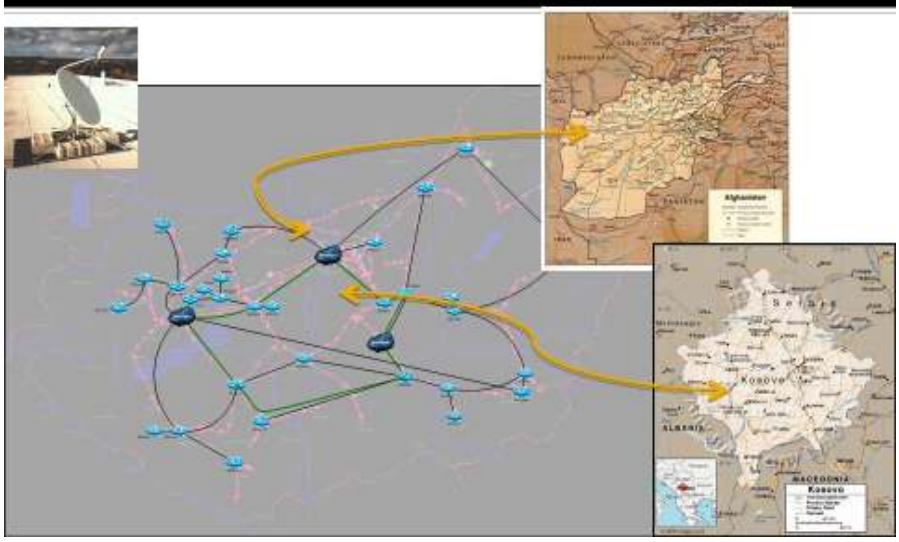
The Army's Transport Network

- A network interconnecting several LAN's
- Built in order to have the capability to
  - Assure communications
  - Centrally manage
  - Supervise
  - Troubleshoot

  All network activity passing through

- This network is also interconnected to our troops serving abroad

The Army's Transport Network



Services provided through the network

- Internet access
- Intranet access
- E-mail
- VoIP
- VTC
- Application virtualization
- Etc.

Security perspective

- The goal is to keep all information safe and accessible
- „CIA", as mentioned before
- Technical aspects
  - Firewalls
  - IDS systems
  - Anti-virus products
  - Etc.
- Human aspects
  - Security focused trainings
  - Proper clearences
  - Etc.

Frequently experienced issues

- Pendrives
- Lack of information both on the user's and the administrator's side
  - „Where could this cable go?" type of activities
- Laptops
- WiFi
- General discomfort of users towards security
  - It makes things slower and more complicated
  - I do this at home, why can't I do it here?

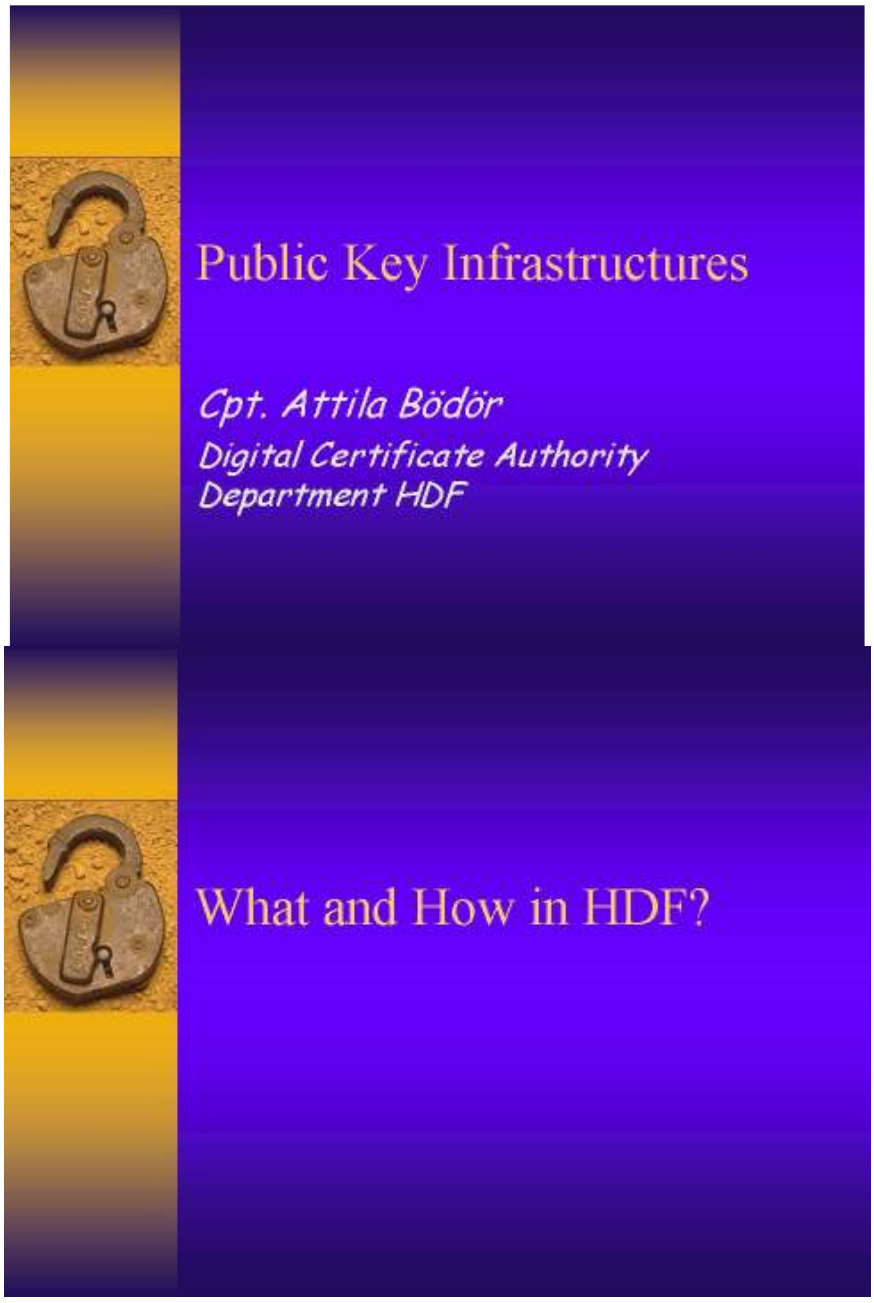
Difficulties in maintaining security

- Geographical dispersion
  - It's a long way from Budapest to Afghanistan..
- Emerging threats
- Malicious employees
- Partially segregated networks
- Money, money and money

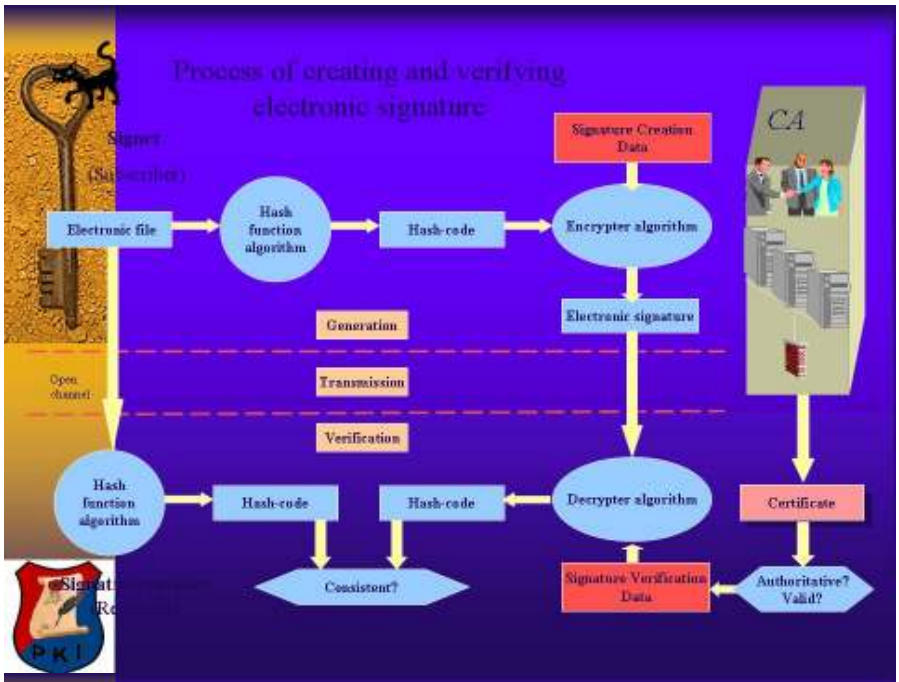
Any questions?

Attila BÖDÖR

PUBLIC KEY INFRASTRUCTURES




Solutions in security…
Authentication
Identity of originator confirmed
Non-Repudiation
Originator cannot disavow transaction
Integrity
Information has not been altered
Confidentiality
Content hidden during transport
PKI Provides – PKI Services
Privacy and Confidentiality
Secure Transport
File Encryption
Secure e-mail
Authentication
Network components & end users
Non-repudiation and Data Integrity
Digital signature
Trusted time stamp
Public Key Infrastructure is based on Public Key Cryptography



What is PKI? - Mechanism

A Public Key Infrastructure is an Infrastructure to support and manage Public Key-based Digital Certificates

- Crypto
  - Signatures, hash, ciphers, assymmetric technics
- Infrastructure
  - Certificates validate public keys…
  - PKI Components

    Authorities *(Trusted Third Parties - DCAD)*
    - Key Distribution (repository)
    - **Certificate**, Policy, Authorization,Time, Notary, etc.
    - Archives (long story… ☺)

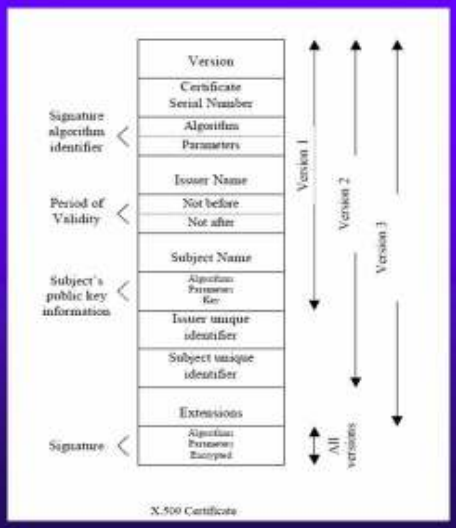
    Registration (CRA)

    Entities


PKI and the Services
♦ CLAIM: PKI *can* help in all
♦ Question (*subjective*)
– Where is the source of **trust** in all these?
– Suggestion (*subjective*)
• Try to do the same without PKI, using only symmetric techniques (usually possible!);
find the problem;
see how this problem is manifested and addressed in the PKI solution.
• Easier to "cheat" (including yourself!) with PKI. Symmetric techniques are more explicit.
♦ Make all the security & trust assumptions explicit!
„Culture of security"……
PKI
Pitfalls in general…
♦ Security breaches
– Key compromises
♦ Inherent difficulties
– Revocation
♦ Negligence
– Certificates are routinely not checked or some of the attributes ignored
– Alarms and warnings ignored
("certificate not valid. Press OK to proceed.")
♦ Inconsistencies & human factors
("*that's not what I* meant *by this policy!*")
PKI


Certificates
Certificates
♦ Certificates ≠ Signature
– Certificates are *implemented using* Signatures
♦ Certificates ≠ Authentication
– Authentication *can* be *implemented using* Certificates
– Same for Authorization, etc.
♦ Certificates are *static*
– Change => Re-Issue
• *This could be challenged, but not in standard x509
PKI

X.509 Certificate Format



Certificate Validation - states

- *Integrity*: signature is valid
- Signed by a *trusted* CA
  - *or certification path is rooted in a trusted CA*
- Certificate is valid *now*:
  - We are between *Not Valid Before* and *Not Valid After* time points in the certificate
- *Not Revoked*
- *Use* is *consistent* with the *policy*


CA – Certification Authority
Issuer/Signer of the certificate
Binds public key w/ identity+attributes
Enterprise CA
Individual as CA
Web of trust
"Global" or "Universal" CAs
VeriSign, NetLock, …
Trust is the key word
PKI
PKI management


Key & Certificate Management in general
Key/Certificate Life Cycle Management
Stages
♦ Initialization
♦ Issued (active)
♦ Revocation
♦ Cancellation
Generation
• Issuance
• [Usage] - Revoked
• Cancellation
PKI


Initialization - Issuing
♦ Registration
– Via RA (Central Registration Office)
– Identity verification
• According to CP/CPS docs
– If on-line, *should be* protected+*authenticated* (?)
♦ Key pair generation
♦ Certificate creation & delivery
♦ [Key backup]
PKI


Certificate Creation+Distribution
Creation – CA only
Distribution (to the owner)
Certificate only
Certificate + private key
Deliver key securely!
Direct to owner
To repository
Both (we are…)
PKI


Certificate dissemination
- storing and retrieving
Out-of-band
Public repositories
LDAP-like directories
Used mostly for confidentiality
In-band
E.g. signed e-mail usually carries certificate
Issues:
Privacy, scalability, etc.
PKI


Issued Phase
Certificate retrieval
– To encrypt msg or verify signature
Certificate validation
– Verify certificate integrity+validity
Key recovery
– Key backup – automate as much as possible
Key update
– When keys expire: new certificate [+new keys]
PKI


Certificate Revocation
Requested by
– Owner, employer, arbiter, ???, … entity
Request sent to
– RA/CA
Mechanisms for Revocation checks
– Certificate Revocation Lists (CRLs)
– On-line Certificate Status Protocol (OCSP)
• Will it live?
PKI


Complete CRLs
Advantage:
Self-contained, simple, complete
Problems:
Scalability
CRL may grow too big
Timeliness
Also results from CRL size
Conclusion: appropriate for some prepared domains
PKI


Key backup
Backup ≠ Escrow
Backup= only owner can retrieve the (lost) key
Escrow= organization/government can retrieve the key even against owner's wish
SOPIN for E.S. Devive
Updating keys
Archiving keys
PKI

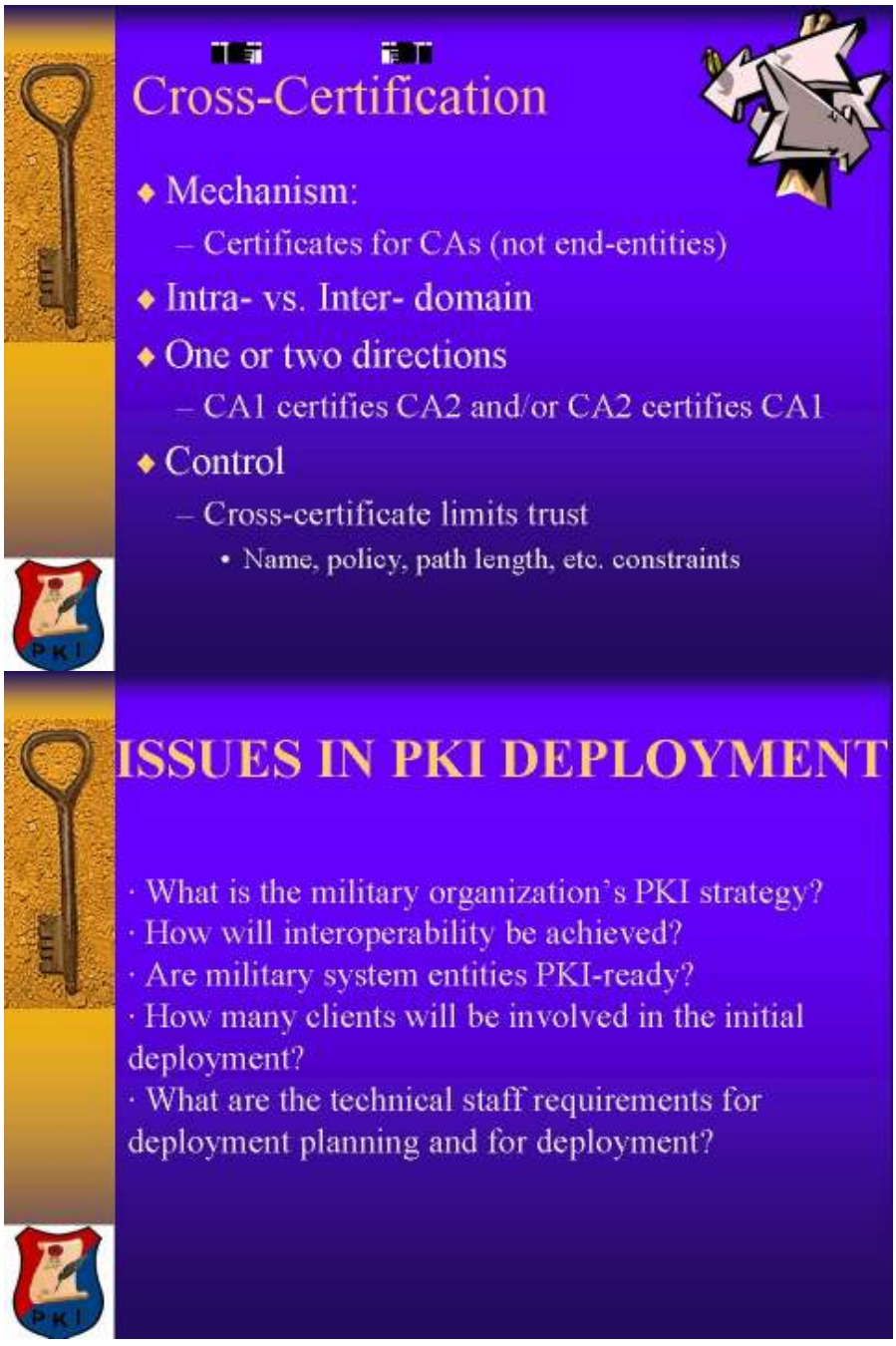

Trust models to NATO
„This is the beginning of the beatiful C.I.A. friendship…"
Trust model issues – Providing trust
Who to trust?
– Which certificates can be trusted
Source of Trust
– How it is established?
Limiting/controlling trust in a given environment
Certification Path Processing….
PKI


Certificate Path Processing
Path construction
– Aggregation of necessary certificates
Path validation
– Checking the certificates and the keys
• Includes all steps of certificate validation
Common Trust Models
CA Hierarchy
Distributed
Web
User-centric
Tool
Cross-certification (NATO ☺)


CA Hierarchy
Tree architecture
Single Root CA
Number of subordinate CA's
Etc…
Parent certifies children
Leaves are non-CA (end-) entities
Typically CA either certifies other CA's or end-entities, but not both (sub and prod)
Everyone has Root CA - regulatory
Distributed Trust Architecture
A set of independent hierarchies
May evolve as independent historically
Cross-certification or PKI networking
Connect the hierarchies
Fully-meshed – all CAs are cross-certified
Hub & spokes or bridge CA
Not Hierarchy
No root CA: every end-entity holds its CA PK


Web Model
A bunch of root CAs pre-installed in browsers
The set of root CAs can be modified
– But will it be?
Root CAs are unrelated (no cross-certification)
– Except by "CA powers" of browser manufacturer
– Browser manufacturer = (implicit) Root CA
PKI

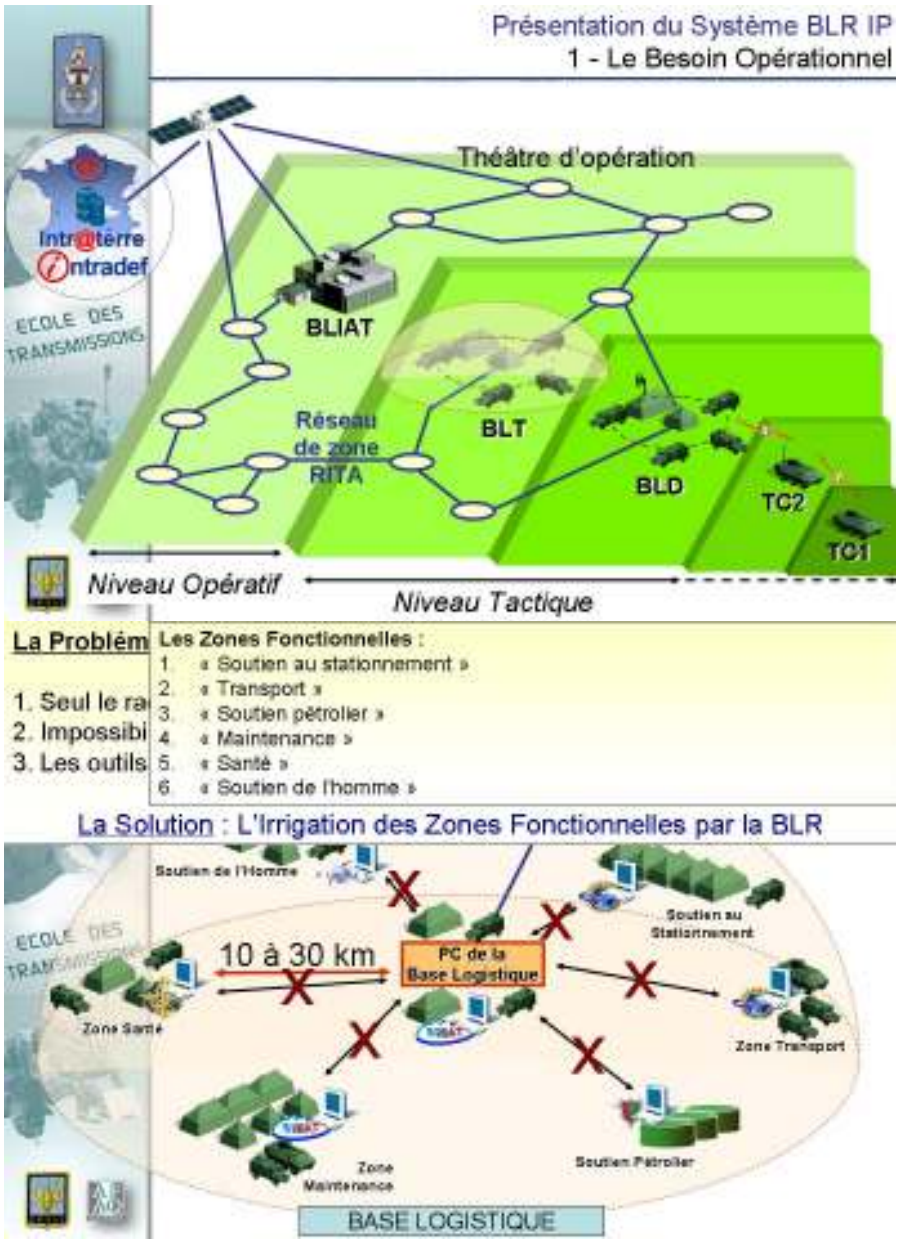

User-Centric
PGP
User = her own Root CA
– Webs of trust
Good
– User fully responsible for trust
Bad
– User fully responsible for trust
– Corporate/gov/etc. like to have central control
• User-centric not friendly to centralized trust policies
PKI


Cross-Certification
♦ Mechanism:
– Certificates for CAs (not end-entities)
♦ Intra- vs. Inter- domain
♦ One or two directions
– CA1 certifies CA2 and/or CA2 certifies CA1
♦ Control
– Cross-certificate limits trust
• Name, policy, path length, etc. constraints
ISSUES IN PKI DEPLOYMENT
· What is the military organization's PKI strategy?
· How will interoperability be achieved?
· Are military system entities PKI-ready?
· How many clients will be involved in the initial deployment?
· What are the technical staff requirements for deployment planning and for deployment?

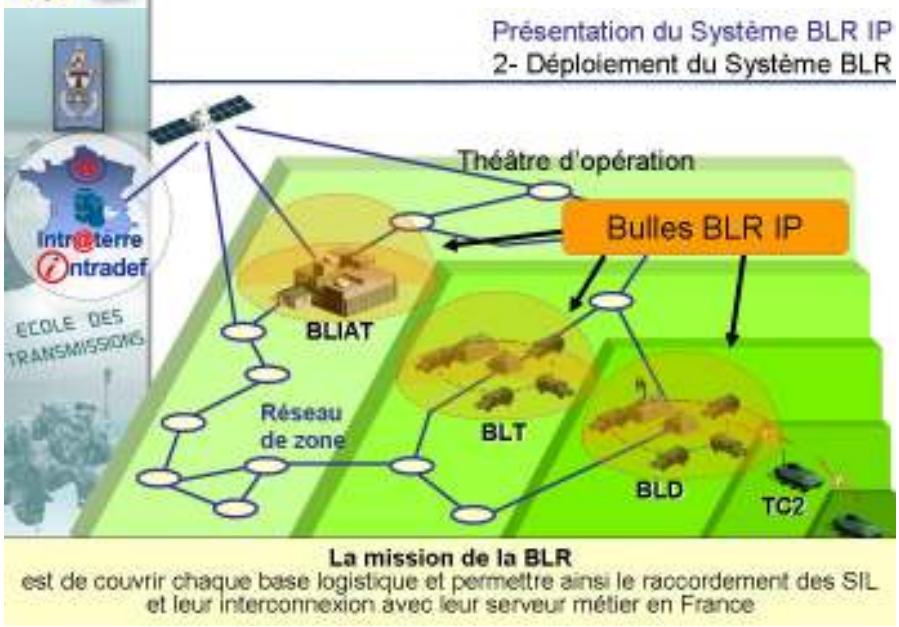

Thank you for your intention!
?
PKI

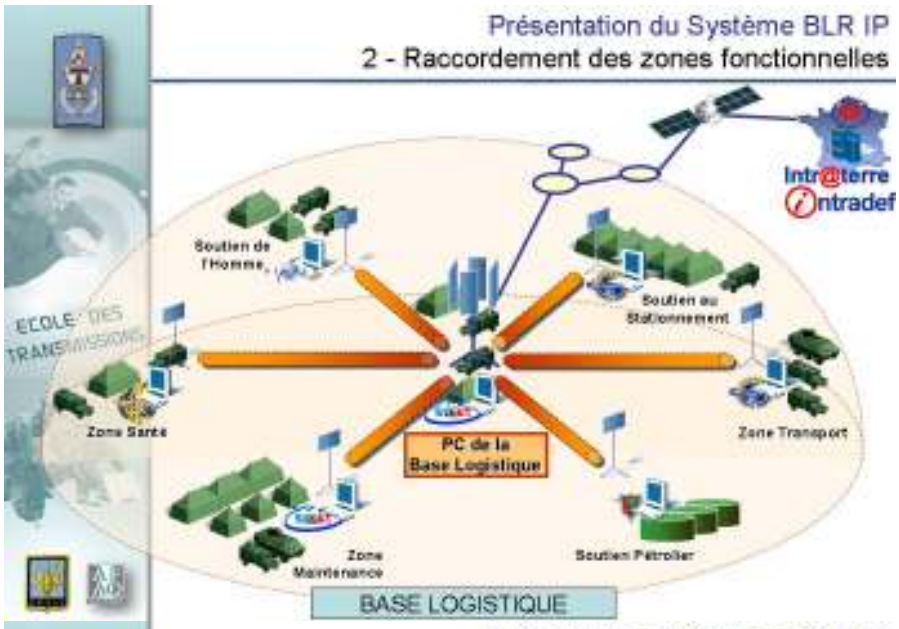
Philippe VAILLANT

BOUCLE LOCALE RADIO IP


Présentation du Système BLR IP
1 - Le Besoin Opérationnel
Théâtre d'opération
BLIAT
Réseau de zone RITA
BLT
BLD
TC2
TC1
Niveau Opératif
Niveau Tactique
La Problém
1. Seul le ra
2. Impossibi
3. Les outils
Les Zones Fonctionnelles :
1 « Soutien au stationnement »
2 « Transport »
3 « Soutien pétrolier »
4 « Maintenance »
5 « Santé »
6 « Soutien de l'homme »
La Solution : L'Irrigation des Zones Fonctionnelles par la BLR
Soutien de l'Homme
Soutien au Stationnement
10 à 30 km
PC de la Base Logistique
Zone Santé
Zone Transport
Zone Maintenance
Soutien Pétrolier
BASE LOGISTIQUE


Présentation du Système BLR IP
Sommaire
1. Le Besoin Opérationnel
(La Problématique du raccordement des SIL)
2. Le Déploiement Logistique
(La Mission de la BLR)
3. Technologie et Matériel utilisés
ECOLE DES TRANSMISSIONS

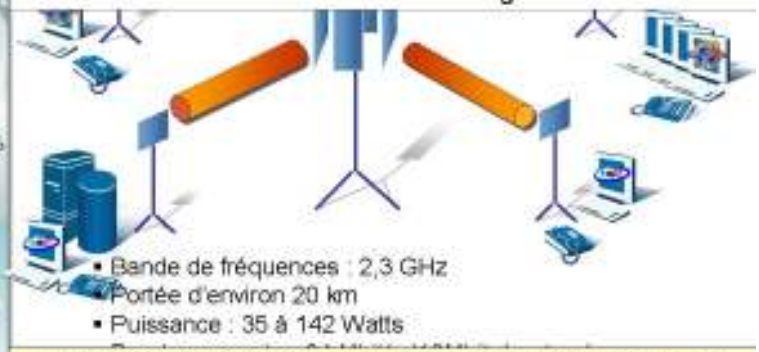

Présentation du Système BLR IP
2- Déploiement du Système BLR
Intra@terre
Intradef
ECOLE DES TRANSMISSIONS
Théâtre d'opération
Bulles BLR IP
BLIAT
Réseau de zone
BLT
BLD
TC2
La mission de la BLR
est de couvrir chaque base logistique et permettre ainsi le raccordement des SIL et leur interconnexion avec leur serveur métier en France


Présentation du Système BLR IP
2 - Raccordement des zones fonctionnelles
Intr@terre
Intradef
Soutien de l'Homme
Soutien au Stationnement
Zone Santé
Zone Transport
PC de la Base Logistique
Zone Maintenance
Soutien Pétrolier
BASE LOGISTIQUE


Présentation du Système BLR IP
Sommaire
1. Le Besoin Opérationnel
(La Problématique du raccordement des SIL)
2. Le Déploiement Logistique
(La Mission de la BLR)
3. Technologie et Matériel utilisés

Présentation du Système BLR IP
3 - La Technologie

La Boucle Locale Radio est un système de communication radio haut débit IP basé sur la technologie WiMAX 802.16d



- Bande de fréquences : 2,3 GHz
- Portée d'environ 20 km
- Puissance : 35 à 142 Watts

WiMAX (Worldwide Interoperability for Microwave Access)

Standard de réseau sans fil métropolitain

Présentation du Système BLR IP
3 - Le Matériel : La Station Point d'Accès

La STATION POINT d'ACCES

Permet le raccordement au réseau de tous les **S**ystèmes d'**I**nformation **L**ogistique

Elle assure la gestion des Stations « Client » ;
gère le plan d'adressage IP et l'interconnexion avec le réseau de zone.
Elle sécurise et supervise l'ensemble du réseau.

La Station « Client » (**SC**) permet :

- le raccordement de postes de travail ou de petits réseaux tactiques des SIL disposés sur les zones fonctionnelles à un débit minimal de 128 Kbit/s.

- un accès en téléphonie analogique et un accès en téléphonie IP.



- Le système de communication BLR IP a pour vocation principale de répondre au besoin en communication **téléphonique** et en **transmission de données** des Systèmes d'Information de la Logistique.

- L'objectif est de permettre le dialogue sur le **théâtre d'opération** des différents Systèmes d'Information de la Logistique jusqu'à leur service fonctionnel en **France**.

- La BLR répond ainsi à des contraintes **Opérationnelles**, d'**Emploi** et de **Sécurité**.

Boucle© Locale Radio IP

Köszönöm
Merci de votre attention

VÉGJEGYZETEK: FREGAN Beatrix-FÁBIÁN Éva

The special relationship for European integration

[i] TAMÁS SZEMLÉR: A francia-német kapcsolatok az Európa-politika kulcskérdései tükrében a XXI. század küszöbén: Folyamatosság vagy változás? Doktori (PhD) értekezés, Budapesti Corvinus Egyetem, Nemzetközi Kapcsolatok Doktori Iskola, 2000. http://phd.lib.uni-corvinus.hu/140/01/szemler_tamas.pdf (downloaded: 03.01.2009)

[ii] FERENC GAZDAG: A francia-német együttműködés évtizedei: negyvenéves az Elysée szerződés. *Európai utas*, 2003/1, p. 21-24.

[iii] SZEMLÉR, ibid.

[iv] This made clear for the west Europeans that since this time economically, politically and in the military field their areas would depend on the United States of America.

[v] The French political elite's activity in this domain was due to their thought that the USA did not give them enough guarantees to control the Germans more exactly West Germany.

[vi] Since the foundation of the United Nations (UN) France is one of the perpetual members in the Security Council. With its membership and as a nuclear power the Gallic state had a strategic advantage over the defeated Germany. The latter was waiting for its reunification and for the renovation of their national sovereignity till 1990.

[vii] GAZDAG, ibid.

[viii] FERENC GAZDAG Franciaország és az iraki konfliktus. *Külügyi Szemle*, 2007/2-3, p. 116-133.

[ix] Concerning the fragile balance between the French political power and the German economically force, it is made of the practical cooperations and of the fact that they were inevitable for each other.

[x] SZEMLÉR, ibid.

[xi] CSABA LOPPERT: A Sarkozy-koktél (Az új francia köztársasági elnök receptje az előtte álló kihívásokra). *Valóság*, 2007/6, p. 105-114.

[xii] MOIS, DOMINIQUE: Franciaország jó forradalma. *HVG*, 2007/19. p. 126-127.

[xiii] The French economy is increasing more slowly among Europeans country.

[xiv] It is French where the unemployment is the highest in Europe.

[xv] MOIS, ibid.

[xvi] CHARILLON, FRÉDÉRIC: Politique étrangère de la France: l'heure des choix. *Politique étrangère*, 2007/1, IFRI, Paris, p. 139-150.

[xvii] Entretien avec Nicolas Sarkozy President de la République Française conduit par la redaction de Politique Internationale: La France, puissance d'avenir. http://www.politiqueinternationale.com/revue/print_article.php?id=613&id_revue=115&content=texte (downloaded: 19.02.2008)

[xviii] In researcher's opinion at present the citizens of the European Union are in a deep identity crisis.

[xix] GAZDAG, ibid.

[xx] It is a good example that Sarkozy visited our region just after his official inauguration.

[xxi] PÉTER BALÁZS: Új német-francia tengely az Európai Unióban. *Egyenlítő,* 2007/9, p. 29-34.

[xxii] When the French president of the republic and the German chancellor lady met almost weekly.

[xxiii] See the European bank-saving package, the start of the European defense policy, launch of the negotiations between the European Union and Russia. The latter was interrupted because of the Russian intervention in Georgia.

[xxiv] FERENC GAZDAG: A francia-német együttműködés évtizedei: negyvenéves az Elysée szerződés. *Európai utas*, 2003/1, p. 21-24.

[xxv] Medvegyev elmegy a NATO-csúcsra. http://nol.hu/lap/vilag/20101020-medvegyev_elmegy_a_nato-csucsra (downloaded: 29.10.2010)

[xxvi] Le projet de durcir la discipline budgétaire provoque des remous dans l'UE. http://www.lemonde.fr/europe/article/2010/10/25/le-projet-de-durcir-la-discipline-budgetaire-provoque-des-remous-dans-l-ue_1430776_3214.html (downloaded: 29.10.2010)