A ZRÍNYI MIKLÓS NEMZETVÉDELMI EGYETEM KIADVÁNYA

Kommunikáció 2002

Nemzetközi szakmai tudományos konferencia anyaga

-2002-

Zrínyi Miklós Nemzetvédelmi Egyetem
Budapest, 2002. október 30.

Szerkesztették a szervező bizottság tagjai:
Dr. habil. Sándor Miklós ezredes
Hamar Sándor mk. ezredes
Fekete Károly mk. alezredes
Dr. Rajnai Zoltán mk. őrnagy

Lektorálta:
Fekete Károly mk. alezredes

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

ISBN 963 86229 2 X

TARTALOMJEGYZÉK

A nemzetközi tudományos konferencia kommunikációs partnere:

Magyar Távközlési Részvénytársaság

A tudományos konferencia szponzorai:

- ANTENNA HUNGÁRIA Rt
- Thales
- Fercom Kft
- Kapsch Telecom Kft
- Siemens Telefongyár KFT nemzeti védelmi és biztonsági üzletág

HÁTTÉR INFORMÁCIÓK

A konferencia fővédnöke:
- Fodor Lajos vezérezredes, a Honvéd Vezérkar főnöke

A konferencia védnökei:
- Prof. Dr. Szabó Miklós vezérőrnagy, akadémikus, rektor
- Mikita János mk. dandártábornok, HVK vezetési csoportfőnök

A konferencia kommunikációs partnere:
- Magyar Távközlési Részvénytársaság

A konferencia támogatói:

- ANTENNA HUNGÁRIA Rt
- Thales
- Fercom Kft
- Kapsch Telecom Kft
- Siemens Telefongyár KFT nemzeti védelmi és biztonsági üzletág

A konferencia rendezői:
- Zrínyi Miklós Nemzetvédelmi Egyetem Katonai kommunikációs rendszerszervező tanszék
- Honvéd Vezérkar Vezetési Csoportfőnökség
- Hírközlési és Informatikai Tudományos Egyesület helyi csoport

A szervező bizottság elnöke:
- Dr. habil. Sándor Miklós ezredes

A szervező bizottság titkára:
- Fekete Károly mk. alezredes

A szervező bizottság tagjai:
- Hamar Sándor mk. ezredes
- Dr. Rajnai Zoltán mk. őrnagy

BEVEZETŐ

A Tisztelt Olvasó a Zrínyi Miklós Nemzetvédelmi Egyetem Katonai kommunikációs rendszerszervező tanszék, a HVK Vezetési Csoportfőnökség és a Hírközlési és Informatikai Tudományos Egyesület helyi csoportja által rendezett nemzetközi szakmai tudományos konferencia szerkesztett anyagát tartja a kezében.

Az immár harmadik szakmai tudományos konferencia célja volt áttekinteni a kommunikációval kapcsolatos változásokat. Különös figyelemmel kezelte az állandó versenyt túlélő és a kísérleti fázisban levő távközlési és informatikai megoldásokat. A konvergencia megjelenési formáit a konferencián kiállított és a konferencia résztvevők intézményeinél konkrétan megvalósított kommunikációs hálózatokon keresztül mutatta be.

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

A szakmai konferencia egyben áttekintést adott a témakör elméleti tudományos kutatásának eddigi nemzetközi és hazai eredményeiről.

A szervező bizottság nem titkolt szándéka volt, hogy az előadásokon elhangzottak minél szélesebb körben ismertté váljanak, ezért a konferencia anyagát közreadjuk.

A szervező bizottság

Jean-Louis DEBEURET

RÉSEAU TACTIQUE WAN DE NOUVELLE GÉNÉRATION RITA 2000

(THALES Communications - unité Réseaux - FRANCE)

THALES Communications à l'honneur de vous présenter le système de Télécommunications Tactiques de nouvelle génération RITA 2000, un système parfaitement adapté aux nouvelles interventions des Forces Terrestres.

RITA 2000 rénove complètement la notion de réseau tactique terrestre en permet aujourd'hui de réaliser le "Champ de Bataille Numérisé".

• Il offre des services sécurisés, et compatibles des standards civils, pour la mise en œuvre des systèmes d'information opérationnels, de téléphonie et de visioconférence en service dans les Postes de Commandement en opération

• Une intégration technologique poussée a permis de réaliser des éléments très modulaires. Le système RITA 2000 a la capacité de projection rapide sur des Théâtres d'opérations extérieurs, tout en réduisant considérablement le personnel nécessaire à sa mise en œuvre.

• Son interopérabilité avec les réseaux civils ou militaires, et en particulier de l'OTAN, permet de répondre aux nouveaux scénarios de projection de forces multinationales.

C'est **l'élément indispensable de la chaîne de commandement**, qui s'inscrit dans le concept de « Tactical Internet ».Les cas tactiques les plus fréquemment considérés par les État-majors montrent que les Forces Terrestres n'occupent pas la totalité d'une région, mais se concentrent sur les zones les plus stratégiques.

• La capacité de transport aérien du couple station RITA 2000 et station SATCOM tactique est particulièrement adapté à desservir des zones non contiguës dispersées dans un Théâtre d'opérations.

À titre d'exemple pour supporter :

- une zone de déploiement initial
- une zone logistique
- une zone opérationnelle principale
- des zones d'extension : pour les missions de reconnaissance ou les opérations dans la profondeur

Le système RITA 2000 assure la continuité des services de télécommunications entre les bulles opérationnelles non connexes, constituées d'unités opérationnelles de taille et de missions diverses.

RITA 2000 est un réseau de type Wide Area Network (WAN). Basé largement sur des standards civils, il offre aux usagers en opération tout une gamme de **services multimédia**. Comme nous le verrons l'accent a été mis sur la mobilité avec le principe de station unique et autonome. Le nombre de véhicules et d'opérateurs a été limité au strict minimum pour offrir aux Forces de véritables capacités de projection stratégique et de déploiement rapide, tant pour le transport vers la zone opérationnelle que pour la mobilité sur zone.

Enfin RITA 2000 a été prévu pour un emploi dans un contexte multinational, et offre non seulement tous les types d'interfaces vers les réseaux alliés de l'OTAN et des "Partner for Peace", mais été réalisé selon une architecture conforme aux **standards TACOMs post 2000.**

RITA 2000 se plaque exactement sur l'architecture TACOMs post 2000.

• il offre une composante WAS de Transit,

• une composante LAS de Poste de Commandement,

• et une composante interface avec les Systèmes Mobiles.

• il s'interface avec les réseaux du théâtre ou de la métropole et peut accéder directement aux réseaux de satellites.

• Enfin il permet **l'interopérabilité avec les réseaux de l'OTAN** par la mise en œuvre des standards les plus actuels: d'une part le STANAG 4206, et dispose d'ores et déjà des fonctionnalités du futur STANAG 4578, dérivé de la norme T2 RNIS (ISDN / E1).

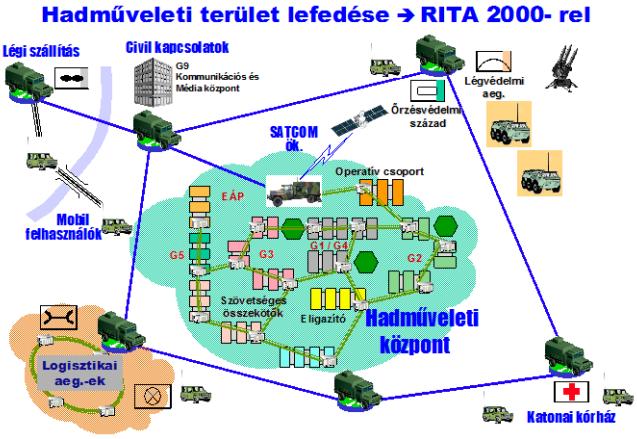
Parmi les besoins opérationnels prioritaires, exprimés par les Forces Armées, l'un des plus importants a été certainement de donner aux moyens de Transmissions une véritable capacité de transport par voie aérienne.

• Les systèmes de communications tactiques de la génération des années 80, et encore en service dans la grande majorité des armées, sont organisés en nœuds de Transmissions de la taille d'une section. Il faut une trentaine d'hommes et une dizaine de véhicules pour assurer la fonction de Centre de transmissions. Le volume et le poids de ces moyens, les personnels nécessaires à leur mise en œuvre, sont peu compatibles avec les impératifs de projection rapide.

• L'élément de base autonome de RITA 2000 a été réduit à un seul véhicule de transmissions et un véhicule cargo, servis par et une demi douzaine de personnels.

• **Sur le plan économique RITA 2000 réduit fortement le coût d'exploitation du réseau tactique**- en terme de nombre de stations

- et pour le nombre de personnels qualifiés.



Les services offerts aux usagers :

• Un objectif particulièrement important du système RITA 2000, est d'offrir aux personnels militaires en opération les mêmes technologies et les mêmes **services multimédia** que ceux qu'ils utilisent aujourd'hui au quotidien dans leurs garnisons et leurs État-majors.

• En particulier les services IP pour la bureautique opérationnelle, la téléphonie et les fax du commerce, la continuité vers les usagers des réseaux extérieurs, la visioconférence, l'accès partagé à des bases de données opérationnelles, la conférence téléphonique, et l'interconnexion avec des réseaux cellulaires type TETRA.

Ceci bien sûr dans un environnement tactique où les usagers sont mobiles, et où les nœuds du réseau le sont aussi, ce qui n'est pas la moindre des difficultés à résoudre.

A travers cet exemple nous allons voir successivement les briques qui constituent le système de télécommunication tactique RITA 2000.

• C'est un réseau maillé, dont la finalité est de couvrir très rapidement une zone opérationnelle d'artères de communication sécurisées.

Au service des usagers

• qui se situent dans les Postes de Commandement Importants, tels que les PC de Corps et de Division installés soit en shelters soit en bâtiments

• au service des usagers des Postes de Commandement Tactiques, au niveau des Brigades et des Bataillons installés typiquement dans des véhicules de commandement blindés

• Ces usagers doivent être en mesure de coordonner leurs actions avec leurs alliés. Chaque élément du réseau est donc en mesure de s'interconnecter avec les réseaux voisins de l'OTAN.

• Trois types de stations permettent de remplir l'ensemble des fonctions de Transit, de raccordement des usagers, et de gestion du réseau.

La fonction Transit du réseau est assurée par les stations "CART" :

Centres d'**A**ccès **R**adio et de **T**ransit

• les CART sont dotés de six Faisceaux Hertziens pour d'une part s'interconnecter et constituer le maillage du réseau, d'autre part pour raccorder les Postes de Commandement.

Les liaisons d'artère sont réalisées en Bande IV (OTAN) et offrent un débit de 8 Mb/s. Le raccordement des Postes de Commandement s'effectue en Bande V (OTAN) à des débits jusqu'à 34 Mb/s.

Les caractéristiques des équipements Faisceaux Hertziens seront données en fin de cette exposé.

• Les CART ont une deuxième fonction, qui est de constituer une infrastructure de Points d'Accès Radio pour le raccordement automatique des abonnées mobiles dotés de postes de combat PR4G. •Les usagers mobiles dotés de postes de combat PR4G disposent d'un service automatique et sécurisé de radio-téléphone avec des fonctions phonie et transmissions de données.

• Ils peuvent appeler et être appelés par les usagers du réseau RITA 2000. S'ils ont autorisés dans l'annuaire électronique, les usagers mobiles peuvent joindre les réseaux d'infrastructure ou les réseaux alliés raccordés à RITA 2000.

• Le système effectue le changement de raccordement des mobiles d'une balise à une autre d'une manière transparente au cours de leurs déplacements.La fonction d'accès des abonnés des Postes de Commandement est assurée par les stations "CMAI" **C**entres **M**ultiservices d'**A**ccès et d'**I**nterface.

• Ces stations se situe au sein des Postes de Commandement, et sont conditionnées suivant leur emploi en camionnettes tactiques, ou en **V**éhicules de l'**A**vant **B**lindés (VAB) pour assurer la même protection et la même mobilité que les unités qu'ils desservent.

• Pour les Postes de Commandement de taille réduite, la station CMAI permet un accès direct phonie, fax et Ethernet à une trentaine d'usagers (pour

la version en VAB) et de 60 à 80 usagers (pour la version en camionnette tactique).

• Dans les Postes de Commandement plus importants la station CMAI est l'interface entre le réseau de Transit et un **réseau local RITA LAS à haut débit** capable de desservir plusieurs centaines d'usagers.

Comme nous venons de la mentionner, la station CMAI peut étendre le service d'accès à de grands Postes de Commandements par la fonction **Local Area System de RITA 2000**.

• Un réseau local LAS est constitué de switch-routers à Haut Débit, reliés entre eux en Fibres Optiques. La station CMAI assure alors l'interface entre le **LAS** et le réseau de **Transit**.

• L'architecture d'un LAS est de type réseau d'entreprise et permet de mettre à la disposition d'un grand nombre d'utilisateurs tous les **services d'accès multimédia et IP**. La spécificité du LAS réside dans la taille évolutive d'un Poste de Commandement en opération, et dans la mobilité des usagers qui veulent pouvoir obtenir une connexion en différents points d'accès au réseau.

• Les contraintes opérationnelles de déploiement conduisent fréquemment les Postes de Commandement à être éclatés géographiquement en plusieurs entités. Les éléments d'un même PC vont cependant bénéficier des services d'un LAS unique, par des connexions hertziennes à des débits jusqu'à 32 Mb/s. Dans de telles opérations certains éléments des forces militaires ou de police utilisent des **systèmes mobiles PMR** (Professional Mobile radio).

• Les stations RITA 2000 peuvent accueillir un système de téléphonie cellulaire PMR au standard TETRA. L'inter fonctionnement entre les deux systèmes est réalisé par une passerelle IP sur artère RNIS.

• Ainsi les usagers dotés de téléphones mobiles TETRA peuvent entrer en communication, et coordonner leur action, avec les usagers du réseau RITA 2000.Voici le déploiement typique complet du système RITA 2000 pour desservir une zone opérationnelle :

• D'abord arrivée du binôme **station RITA 2000 / station SATCOM**, et service immédiat d'un Poste de Commandement Avancé

• Extension du **LAS** au fur et à mesure de la constitution du PC Principal avec ses cellules d'état-major

• Déploiements successifs d'une zone logistique, d'une zone aéroportuaire, déploiement d'unités de protection, d'un hôpital de campagne, etc..

• Mise en place du maillage RITA 2000 adapté à cette zone

• La zone opérationnelle est couverte et offre un réseau de communications pour les unités, et un service de radiotéléphone pour les mobiles

Voyons brièvement les équipements principaux du système.

Les jonctions du réseau sont assurées par des Faisceaux Hertziens de la gamme TRC 4000.

Le principe retenu est un un équipement extérieur (RFE) comprenant l'antenne et la partie Radio Fréquence (RF), et un équipement Bande de Base intérieur (BBE). BBE et RFE sont reliés par une fibre optique de 600 mètres. Cette solution permet de séparer l'installation de la station RITA 2000 de celle des antennes.

Un combiné permet d'assurer la fonction de téléchargement des paramètres radio et la Voie de service des opérateurs

• La station CMAI pourra être au plus près des abonnés du PC

• La station CART pourra être camouflée dans un endroit facilement accessible à proximité du point haut

La famille TRC 4000 existe en deux versions :

• l'une en bande IV OTAN pour les liaison d'artère entre les CART, offre un débit de 8 Mb/s. L'antenne électronique est constituée de multiples émetteurs type patch.

• l'autre en bande V OTAN pour les liaisons de raccordement des Postes de Commandement permet un débit de 34 Mb/s

Voici la mise en œuvre typique d'une station RITA 2000 avec un Faisceau Hertzien TRC 4000. Le commutateur tactique ATS 20 assure les fonctions de Transit, d'accès radio des mobiles, d'accès des usagers fixes, et d'interface aux autres réseaux

Dans les stations sur VAB, le commutateur tactique ATS 8, assure les mêmes fonctionnalités de Transit, d'accès des usagers, et d'interface mais dans un conditionnement de taille plus réduite

Les LAS de Poste de Commandement sont constitués de commutateurs à haut débit, installés dans les véhicules de l 'état-major et reliés entre eux à 155 Mb/s par un réseau de fibres optiques

RITA 2000 dispose d'un système de commandement et de gestion du réseau , le NMS 2000 (**N**etwork **M**anagement **S**ystem) :Les grandes fonctions de cet ensemble informatique réparti permettent d'assurer la planification du réseau avant un déploiement, la gestion et l'administration du RITA 2000 en zone opérationnelle,

en particulier :

• le calcul des liaisons hertziennes
• les zones de couverture radio des stations CART
• le déploiement et la manœuvre des stations du réseau
• la gestion des bases de données des commutateurs
• la gestion des éléments secrets du réseau
• et la transmission de ces données à l'ensemble des nœuds
• finalement la présentation de l'image du réseau en temps réel

Le NMS 2000, système de commandement et de gestion du réseau, est constitué de stations de management: les NMC, localisées dans les Postes de Commandement Principaux, et de terminaux FC à chaque station RITA 2000.

Les NMC et les FC échangent:

• des messages opérationnels pour la manœuvre du réseau, les déplacements de stations, les ordres logistiques et les compte-rendus d'exécution

• et des messages techniques pour le transfert des données de configuration du réseau, et la connaissance temps réel de l'état des liaisons et des équipements.

UNIVERSAL SOFTWARE RADIO PLATFORM FOR WIDEBAND, MULTICHANNEL AND PHASED ARRAY APPLICATIONS

Dr. Bertalan Eged*, Gábor Négyesi**
*Budapest University of Technology and Economics, Department of Broadband Telecommunications Systems
Goldmann ter 3. Budapest 1111 Hungary T: +36-1-463-3614 F: +36-1-463-3289
**Sagax, Ltd. József krt. 75. 1085 Budapest Hungary T: +36-1-317-6097 F: +36-1-317-6143
bertalan.eged@mht.bme.hu

Introduction

The term software defined radios (SDRs) is used to describe radios that provide software control of a variety of modulation techniques, wide-band or narrow-band operation, communications security functions (such as hopping), and waveform requirements of current and evolving standards over a broad frequency range. The frequency bands covered may still be constrained at the front-end requiring a switch in the antenna system.

Software Defined Radio (SDR) is an enabling technology applicable across a wide range of areas within the wireless industry that provides efficient and comparatively inexpensive solutions to several constraints posed in current systems. For example, SDR-enabled user devices and network equipment can be dynamically programmed in software to reconfigure their characteristics for better performance, richer feature sets, advanced new services that provide choices to the end-user and new revenue streams for the service provider. SDR is uniquely suited to address the common requirements for communications in the military, civil and commercial sectors. [1,2,3]

The evolving standards for wireless mobile communications trends to use the wide bandwidth spread spectrum and CDMA modulation schemes. The software radio platforms has to meet the requirements of the existing and new communications systems. The paper introduces a new universal platform which can be used for handle the modulation scheme of WCDMA or any other system with wide bandwidth requirements.

Digital radio as the hardware platform of SDR solutions

Traditionally, a radio has been considered to be the ‘box’ that connects to the antenna and everything behind that, however, many system designs are segmented into two separate subsystems. The radio and the digital processor. With this segmentation, the purpose of the radio is to down convert and filter

the desired signal and then digitize the information. Likewise, the purpose of the digital processor is to take the digitized data and extract out the desired information.

An important point to understand is that a digital receiver is not the same thing as digital radio(modulation). In fact, a digital receiver will do an excellent job at receiving any analog signal such as AM or FM. Digital receivers can be used to receive any type of modulation including any analog or digital modulation standards. Furthermore, since the core of the digital processor is a digital signal processor (DSP), this allows many aspects of the entire radio receiver itself be controlled through software. As such, these DSPs can be reprogrammed with upgrades or new features based on customer segmentation, all using the same hardware.

The reconfiguration feature is the base attribute of the digital radio which enable to use it as the hardware platform for software radio applications. Different level of implementation of software radio can be exist, but without a flexible hardware platform the basic functionality can not be fulfil.

The IF sampling architecture

Already, it is common practice to use an analog-to-digital converter to form the detector and a DSP (digital signal processor) to process the data. However, this does not reduce the cost or complexity of the design (to digitize the baseband), it simply adds flexibility. What is needed is an analog to digital converter that can digitize closer to the antenna. Sampling at the antenna is not realistic since some amount of band select and filtering must occur prior to the ADC to minimize adjacent channel issues. However, sampling at the first IF is practical.

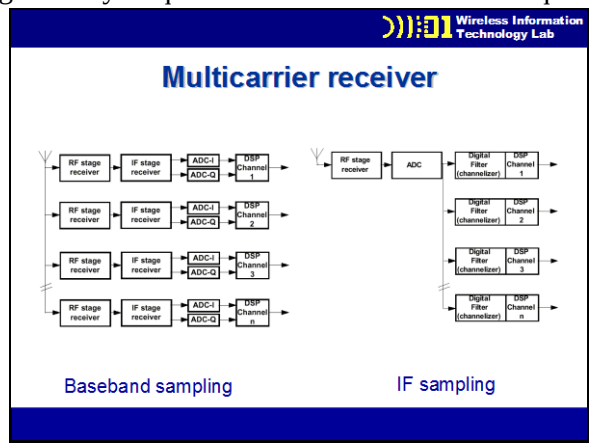
Recent advances in converter technology have allowed data converters to faithfully sample analog signals as high as several hundred MHz. Sample rates need only be as high as twice the signal bandwidth to keep the Nyquist principle. Since most air interface standards are less than a few MHz wide, sample rates in the tens of MHz are required, eliminating the need for extremely fast sample rates in radio design. Thus allowing for low cost digitizers.

Multi-carrier and wideband operation

There are two basic types of radios under discussion. The first is called a single-carrier and the second a multi-carrier receiver. Their name implies the obvious, however their function may not be fully clear. The single carrier receiver is a traditional radio receiver deriving selectivity in the analog filters of the IF stages.

The multi-carrier receiver processes all signals within the band with a single rf/if analog strip and derives selectivity within the digital filters that follow the analog to digital converter. The benefit of such a receiver is that in applications with multiple receivers tuned to different frequencies within the same band can achieve smaller system designs and reduced cost due to eliminated

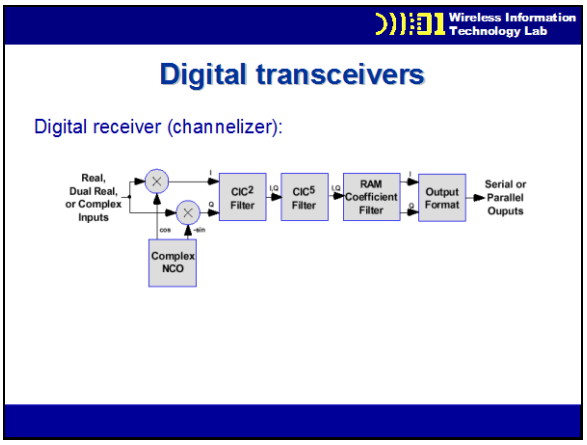
redundant circuits. A typical application is a cellular/wireless local loop base station. Another application might be surveillance receivers that typically use scanners to monitor multiple frequencies. This applications allows simultaneous monitoring of many frequencies without the need for sequential scanning.



The wideband radio can be seen as a single carrier with wide instantaneous bandwidth. These type of digital radio elements require high-speed processing elements not available yet. Today a lot of hardware infrastructure elements are available to build a digital multi carrier radio. However in some cases this elements can be used in wideband operation mode. In this mode the bandwidth available in the single channel of the multi carrier device are summed and the processing capacity of the single channels are used to reach the requirements of processing the wide bandwidth signal.

Programmable digital receiver for multi channel operation

The purpose of the receiver chip is to tune in the desired carrier and then perform the channel selection of that carrier. Since the chip is fully programmable, the decimation rate and filter characteristics can be changed for each air interface as necessary. Since a typical system will require many receiver chips, it is possible for different air interface standards to be in operation at once. This is possible since each tuner chip can be programmed independent of the others. In this way, one chip can process AMPS and another TDMA or even CDMA. The digital throughput of the chip should be matched to the converter chip. The transmit path could be implemented in same way, but opposite direction of signal path.



The numerically controlled oscillator (NCO) provides spurious performance to better than -105 dBc. This ultra clean digital local oscillator is mixed with the digitized input through 18 bit multipliers. The spurious performance of the NCO is hidden well in the 16-bit noise floor shown below.

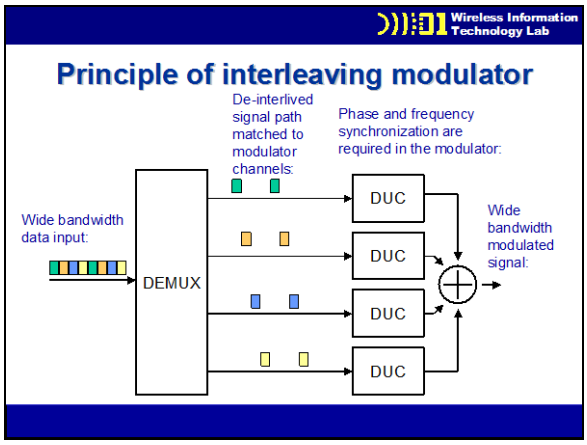
Other than programmable decimation rates, the response of the CIC filters are fixed. The FIR filters are fully programmable and the pass band and stop-band characteristics can be programmed to nearly any unique specification. Inter-stage precision is maintained at 18 bits while individual stages use much higher precision to prevent artifacts due to truncation.

The channel bandwidth is determined by the processing capability of the filters in the channelizer block. This processing capability limits the bandwidth of input data signal and the minimum of the interpolation factor which can be used.

In programmable radio receiver or transmitter chip up 4 such kind of channelizer is placed and the on-chip summer which is responsible to add the data from on-chip channels there is external input. This makes it possible to connect more channel together even up to 16 channels.

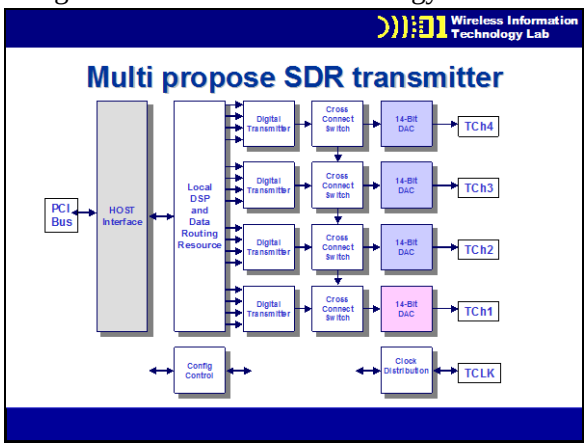
Programming the multi carrier receiver for wideband operation

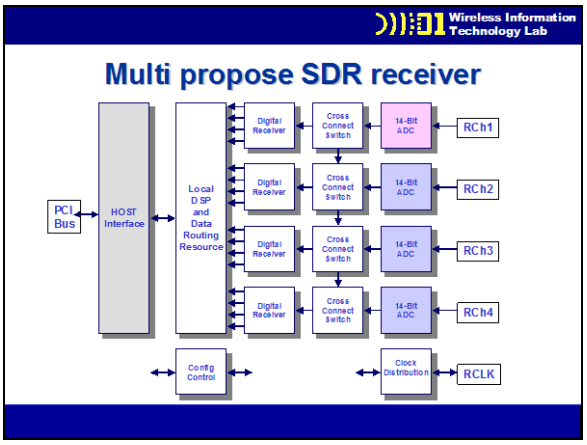
When we want to use the multi channel digital radio for wideband operation it can be done by using it in de-interlived mode. The basic principle is that the incoming high-speed, wideband signal should be demultiplexed into signal flows matched to processing capability of each channels. The interpolation filters of the channels should be programmed to the required wideband channel operation. The numeric controlled oscillator of the up-converters should be matched in frequency and phase at each channel. In this way after the summation the outgoing modulated signal will contain a modulation content equivalent to the wideband input data stream.



Design and implement a universal software radio platform

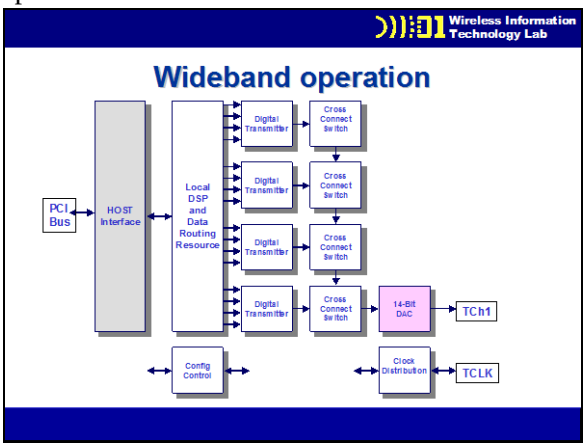
Based on the principle above we started to develop the required hardware and software elements for a digital radio platform which can be programmed for wideband, multichannel and phased array operation using the multi carrier channelizer chips. The interleaving modulator is realized in FPGA using standard VHDL language. The high-speed hardware design is ready and basic operation software modules are running. The filter designing has been done for some wideband operation modes. The platform is tested using the measurements of outgoing modulated signal. The platform is based on the DSP technology from Analog Devices and FPGA technology from Xilinx.

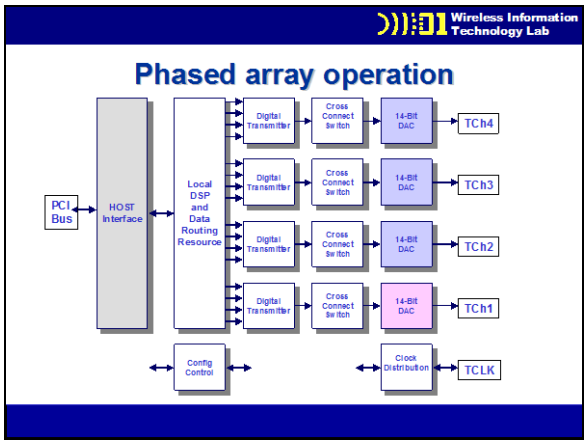




Programming the phased array operation

When we want to use the multi channel digital radio for phased array operation it can be done by using separated converters for each channel or channel block. The phase and amplitude distribution of the separated channel block should be programmed. It can be done by fine tuning of the frequency and phase of the output NCO.





Conclusions

We introduce the method to realize a universal digital radio which can be used as a hardware platform for software radio applications. The platform is able to handle narrowban multi carrier signals and wideband single carrier signals too, depending on the software configuration.

The configuration can be done trough a standard serial interface, which implemented using an on-board micro controller. This fulfil the requirements of software control object element in software defined radio reference model by SDR Forum. The platform is designed and realized and basic measurements results are available.

References

[1] J. Mitola III, Editor, Special Issue on Software Radio, IEEE Comm Magazine, May 1995.

[2] Lackey, Upmal, "SPEAKeasy: The Military Software Radio", Special Issue on Software Radio, IEEE Communications Magazine, May 95

[3] Software Defined Radio Forum, www.sdrforum.org

[4] P.Horváth, T.Marozsák, E.Udvary, A.Zólomy, T. Berceli, B. Eged ",A direct microwave down-conversion method for software radios" Proceidings of European Microwave Conference, October 2-6, 2000 Paris France, pp. 407-410.

[5] B. Eged, P. Horváth. I. Frigyes "Digital Compensation in IF modulated Upconversion Software Radio Architecture", Software Radio Technologies and Services, E. Del Re (editor) pp. 211-216., Spinger-Verlag London Limeted, 2001, ISBN 1-85233-364-4

Dr. Zoltan RAJNAI

LA GUERRE INFORMATIQUE

La Chine : une force potentielle dans la guerre informatique ?

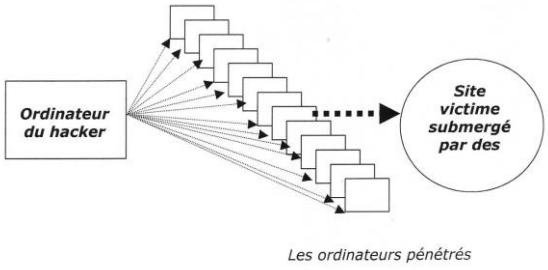
Bien que la Chine soit en retard en matiere informatique, le pays a commencé son rattrapage technologique. Le président Jiang Zemin, dans un discours début mars 2000, identifia la technologie internet comme étant le nouveau grand développement dans les domaines de la guerre et de la paix. Les auteurs du livre intitulé «La guerre illimité» ont popularisé l'idée d'une utilisation d'internet dans le cadre d'une stratégie de désinformation contre l'adversaire. Pour le moment, la Chine est loin derrière Taiwan en matière informatique. Une récente recherche officielle a exposé les failles du système informatique chinois: 80% des 635 sites gouvernementaux seraient vulnérables a des attaques menées par des hackers.

La Chine est néanmoins capable d'offensive informatique. Ce sont en général de jeunes nationalistes qui spontanément, c'est-a-dire sans l'appui direct du gouvernement chinois, mene des offensives informatiques. Depuis 1998, les chinois ont répondu à des critiques internationales perçues comme des insultes en attaquant les sites du Japon, de Taiwan, de l'Indonésie. L'été dernier, après que le président taiwanais déclara que la Chine et son pays devraient parler «d'Etat à Etat», des hackers chinois lancèrent 72 000 attaques contre 20 sites gouvernementaux taiwanais. Selon des experts militaires taiwanais, ces attaques furent co-dirigées par des spécialistes militaires et des civils chinois.

Taiwan : un expert reconnu

Pour le moment, il semble que Taiwan ait largement le dessus en matière de guerre informatique. Taiwan fabrique plus de 80% des «mother-boards» mondiaux et dispose de nombreux spécialistes en informatique. Le budget du pays alloué à la guerre informatique est de 300 million de dollars. Pour les élections de mars, 1 million de dollars a été alloué pour assurer l'impénétrabilité du système informatique de décompte des votes. Non seulement Taiwan dispose des moyens et de la technique nécessaires pour assurer sa protection mais elle a aussi un arsenal impressionnant de moyens pour lancer une offensive informatique. Le chef des départements de la communication et de l'informatique au ministere de la défense affirme que Taiwan a fabriqué plus de 2000 virus qui pourraient etre utilisés contre la Chine. Taiwan, en effet, a dans le passé mis au point un grand nombre de virus redoutables. Michelangelo, un virus notoire mondialement fut créé par une firme taiwanaise. La Chine a intégré des scénarios de guerre informatique dans ses exercices opérationnels, Taiwan est un producteur important de

composantes pour ordinateurs ; elle peut mener des attaques informatiques d'un niveau avancé.



Les ordinateurs pénétrés

La guerre technologique

La Chine a amélioré son système de défense contre les virus ; se prépare à développer sa capacité de fabrication de virus, Taiwan est considérée comme un hacker de statut mondial ; est un expert dans la création de «bugs» et virus.

L'infrastructure de télécommunication

Les réseaux de commande et de contrôle sont vulnérables ; ne dispose pas de satellites de communication. Des réseaux civils et militaires séparés; un accroissement rapide dans la mise en place de réseaux.

Les stratégies psychologiques

La Chine utilise des techniques traditionnelles d'espionnage ; les medias de Hong Kong servent d'instrument de propagande, Taiwan est habile en matière de propagande et offre des récompenses financières aux transfuges. Pour le moment, la menace d'une guerre informatique est de l'ordre du discours mais elle est une réelle possibilité pour l'avenir puisque les deux pays développent avec sérieux leurs capacités informatiques dans l'éventualité d'un conflit. On voit ici que la menace psychologique au moins autant d'impact que la menace réelle.

La vulnérabilité du réseau : le paradoxe du net

La connectivité d'internet, c'est-à-dire la possibilité de joindre deux individus situés a deux points opposés de la planète, en fait aussi sa faiblesse puisque qu'un saboteur peut garder son anonymat tout en pénétrant un site protégé. Il s'agit du phénomène décrit comme étant «la faiblesse du maillon de la chaîne». La source de certains des problèmes de sécurité provient de l'architecture de base du réseau internet. Développé aux Etats-Unis par le département de défense il y a trente ans, l'internet était destiné a des usagers connus, et non au grand public, pour partager des informations. De nombreuses mesures pour sécuriser le réseau sont simplement des ajouts a un système déja ancien. Selon Bruce Schneier, technicien en chef de Counterpane Internet Security Inc., «Le système se dégrade plus rapidement que nous sommes en mesures de le sécuriser».

La menace la plus importante viendrait d'une attaque dirigée contre les organes vitaux du net, les «root name servers». Ces ordinateurs contiennent les listes maîtres des adresses internet et dirigent les flux d'information. Ces ordinateurs ne sont qu'au nombre de 13 mondialement et ils ont déjà fait signe

de faiblesses. En 1997, une erreur humaine eu pour résultat de bloquer le fonctionnement de ces serveurs: pendant plusieurs jours, tout le réseau fut désorganisé.

La fragilité intrinsèque des logiciels

Un nombre tout aussi important des vulnérabilités du net dérive de la faiblesse intrinseque des logiciels. Les logiciels sont souvent victimes de bugs. Les programmes contiennent des millions de lignes d'instructions, et il est impossible de les vérifier toutes effectivement avant la commercialisation du produit. Les bugs, d'ailleurs, sont souvent utilisés par les hackers comme moyen d'accès aux sites web et aux ordinateurs personnels. Selon Steve Bellovin, chercheur a AT&T Labs, il est impossible d'écrire des programmes qui ne comporteraient pas de bugs. Toutes les informations personnelles et sensibles qui sont utilisées par le net peuvent etre la proie facile d'intrus violant la confidentialité de ces données. Il s'agit du vol d'identité. Cette violation peut prendre la forme de la prise de contrôle non seulement d'informations confidentielles mais aussi de la gestion d'un compte en banque. Au mois de janvier 2000, un hacker appelé « Maxim » aurait exploité les bugs contenus dans un logiciel d'un vendeur de CD on-line et aurait ainsi pu prendre les numéros de 300 000 cartes de crédit. Une des conséquences paradoxales serait que les gouvernements développent des méthodes de plus en plus perfectionnées pour contrôler le net, justifiées par le fait qu'il est nécessaire de sécuriser d'avantage le réseau. Le problème des libertés individuelles et de la vie privée se pose alors sous un autre angle.

Roland GÉMESI, Balázs IVÁDY, László ZÖMBIK

SECURITY ANALYSIS OF MOBILE AD HOC NETWORKS

Roland Gémesi* Balázs Ivády* László Zömbik#
gemesi@alpha.ttt.bme.hu ivady@alpha.ttt.bme.hu laszlo.zombik@eth.ericsson.se
* Department of Telecommunications and Telematics (DTT), BUTE
# DTT-BUTE; Ericsson Hungary, ResearchLab

Abstract

Ad hoc networks resolve the emerging communication problems of the battlefield. However those networks have to solve several security issues. The security of routing and the protection of user data are the most important tasks. Those require authentication and key management also. However several solutions are published, most of them neither verified formally nor evaluated by simulation.

Introduction

The basic idea of Mobile Ad-hoc networks (MANET) was developed especially for military needs during the 2nd World War. There has been no previously built infrastructure on the battlefield, while communication was required. The solution has been a fully distributed system, where there are no central roles; there is no existing infrastructure. This can be achieved only if nodes cooperatively serve collective goals without the help of any specific entity. For example this system has no central routers or gateways, each node should act as a router to provide hop-by-hop packet forwarding. In these days the trend is to embed the wireless communication capability into consumer electronic instruments, which can form a network without any centralised entity.

Mobile ad-hoc networks have some special attributes. The architecture of the network is not static, so routes are valid only for a short time. Moving or disappearing nodes should not disturb the operation. Usually nodes are small handheld devices with a limited capacity of resources like battery power, CPU or memory. Our wireless links often have much lower bandwidth and these resources are often shared and limited. Moreover the links and devices are more vulnerable than in fixed, wired networks.

Mobile ad hoc networks has more threats, than fixed network. Security properties of ad hoc protocols are modelled with Casper. This simulator can analyse security protocols and even it is able to find possibilities for attacks.

In section 2 we introduce routing types of ad hoc networks and we show two protocols. Section 3 gives overview about the security mechanisms needed in ad hoc networks. Security issues of routing mechanisms are discussed is

section 4. In section 5 we introduce the Casper simulator and in section 6 we present some ad hoc protocols modelled with Casper.

Routing mechanisms in ad hoc networks

In a multi-hop environment one of the most important task is the routing. Packets have to be routed effectively to find their destinations, they should be transferred through a correct route. In a regular (non ad hoc) network dedicated points (gateways, servers) hold information about the architecture of the network, so they can determine in which direction the packet should be forwarded. Ad hoc networks have no fixed infrastructure, so there is no centralised knowledge or role. All nodes therefore should participate in the routing process; ad hoc networks should have distributed knowledge from routing and other signalling point of view.

Types of routing

Routing protocols can be divided to two main groups: to pro-active and to reactive.

In a pro-active protocol, routes are constantly being tracked and stored. The main advantage of these protocols is that the possible routes are continuously known. However these can cause a high quantity of data to be stored and a lot of packages have to be transmitted through the network. On the contrary reactive protocols only try to find a route, when it is needed. This can cause higher delay at the beginning of the communication, because routes have to be discovered at this time. These are also known as on-demand protocols. Hybrid protocols combine the above two methods.

In the next sections the DSR and the AODV reactive protocols will be introduced.

Dynamic Source Routing (DSR)

In the Dynamic Source Routing (DSR) Protocol the sender strictly determines the full path of packets. The headers of packets contain the complete sequence of hops, from which intermediate nodes will be able to figure out the address of the next hop.

Sender maintains a route cache, and it always checks first their database in order to find a path towards the destination. If a route does not exist, sender initiates a route request. This is a broadcast message that spreads through the network and locates the target host. If the destination is reachable, it will send back an answer message that will include the list of intermediate nodes of the path. If the path that the sender tries to use is broken, then an error message is being generated as the detection of failure. In this case the sender should try to request a route again.

In networks with low mobility this protocol can be quite effective, because the entries in the cache tables will stay usable. A disadvantage is that all packets have to carry all the intermediate node addresses in the route, which

can cause significant overhead in the signalling and in the sender's memory. [1]

Ad hoc On-Demand Distance Vector Routing (AODV)

AODV is also a reactive protocol, which uses a broadcast route discovery mechanism similar to DSR, but instead of source routing, AODV relies on the dynamically established route table entries at intermediate nodes. Endpoints not require to know the whole path, since the intermediate nodes know only the correct direction and as a result they form the actual route. Loop freedom is reached with the application of sequence numbers.

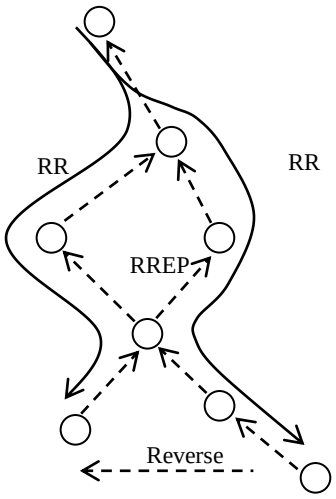


Figure 2.1. Established reverse routes

When a node starts to communicate, it initiates a Path Discovery process, which is a broadcasted route request (RREQ) message containing the address of destination and originator. Each node receiving a RREQ message sets up a reverse route back to the source, increments the hop-count and rebroadcasts the request. The destination replies to the first incoming RREQ with a route reply (RREP) message on that way to the originator. This reply message runs back through the selected reverse route and sets the forward route in the nodes. (Figure 2.1.) Each route entries have a specific lifetime, consequently unused reverse route entries will be deleted. When there is no traffic in a link, nodes can perform local connectivity management. This means broadcasting Hello messages only to the neighbours to check connectivity.

When a link error is detected a route error (RERR) message is generated with the list of unreachable destinations and sent back to the sources. In AODV it is possible to repair a link locally, which is called local repair. If the local repair process succeeds, the endpoints will not be informed about the action.

AODV is a scalable protocol, it offers low processing and memory overhead, low network utilisation and it can determine and maintain routes effectively. This protocol can handle networks with higher mobility. [1]

Security mechanisms

In order to ad hoc networks remain reliable and information never discloses to unauthorised members, security services as authentication, data encryption,

key management is also needed. This section focuses on authentication and key management, because those services solve several essential ad hoc related issues.

Authentication

Authentication of communicating entities can be reached by using certificate authorities (CA). The goal of certificate authorities is to sign certificates so to bind public keys to nodes. A CA should stay on-line to reflect the current bindings. It should track changes and it can revoke certificates if the node is no longer trusted. However in ad hoc environment, where centralised services are not preferred, distributed CA with the help of threshold cryptography should be used.

Another solutions for authentication are the self-organised trust chains or the ID based cryptography.

Threshold cryptography

A solution for certificate authority in ad hoc environment is the distribution of trust using threshold cryptography. A (n, t+1) threshold cryptography scheme allows n parties to share the ability to perform a cryptographic operation, so that any t+1 parties can perform this operation jointly, whereas it is infeasible for at most t parties to do so, even by collusion.

In this case n servers of the key management service share the ability to sign certificates. This scheme can tolerate t compromised servers by dividing the private key k of the service into n shares (s_1, s_2,…,s_n) assigning one share to each server. We call this composition an (n, t+1) sharing of k. After this each server can generate a part of the signature, which are merged. Strength of this solution is in contrast with the centralised CA is that this certificate still adequate even if t parties are compromised.

Besides the advantage of threshold signature, this kind of key management service is easily able to refresh the participants' shares. This is very effective against mobile adversaries that compromise a server and then moves on the next victim. An attacker can take several servers, but by the end of periodical share refresh the obtained node loses the ability of service. During a share refresh a new threshold configuration can be created, which is a good occasion to adapt to network changes. Moreover share refresh is not a complicated operation, so once created share configurations can be adapted for a long time. When too many participants are compromised, an entirely new share should be created. [2]

Self organising Public key infrastructure

Trusted third parties are a very troublesome part of certificate-based authentication. Therefore it would be beneficial to avoid them and build a self-organised structure. There are some certificate-based systems (e.g. Pretty Good Privacy (PGP)), in which certificates are issued by the users themselves and distribution of certificates is managed by a self-organised structure.

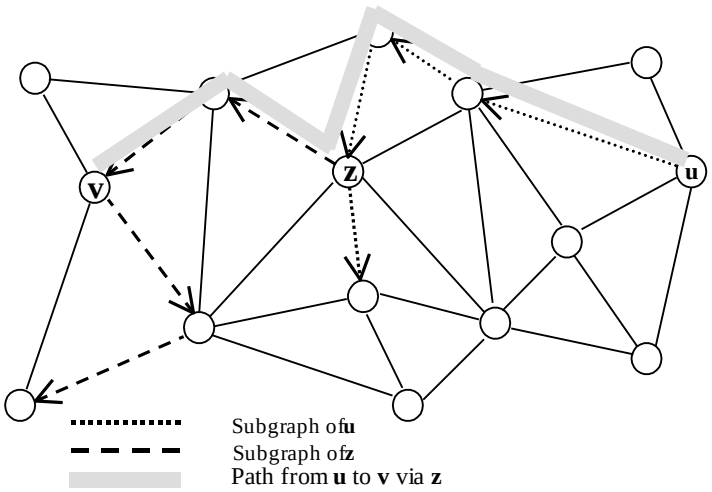


Figure 3.1. Certificate chain in the merged trust repository

Each user maintains a local certificate repository that contains a limited number of certificates. When user *u* wants to obtain the public key of user *v*, nodes in the network merge their local certificate repositories and *u* tries to find an appropriate certificate chain from *u* to *v* in the merged repository (Figure 3.1). For the construction of the local repositories several algorithms exists to provide that almost any pair of users can find certificate chains, even if the size of the local repositories is small compared to the total number of users of the network. [3]

ID-Based cryptography

The basic idea of identity-based cryptoschemes is that information used for identification (node address, user name, etc.) could act as a public key, so that CA is no longer needed to bind keys and identities. In this case, only a central entity is able to derive the secret pair of a public key (identity). This operation is needed only once, at the registration of users. After this, participants are able to authenticate each other in a non-interactive manner, without communicating with a third party. [3]

Common key architecture

A group of nodes that previously identified each other wants to form a secure network, therefore they should establish an encrypted session. Symmetric key architectures are usually used for this purpose, because of the relatively low processing overhead of the encoding and decoding mechanisms. This requires the participants to have common (shared) secret key, which they use for both encrypting and decrypting. By the application of symmetric keys, secure broadcast and multicast communication is also possible. Several key

establishment protocols exist, here the GDH.2, the Hypercube and the Octopus is introduced.

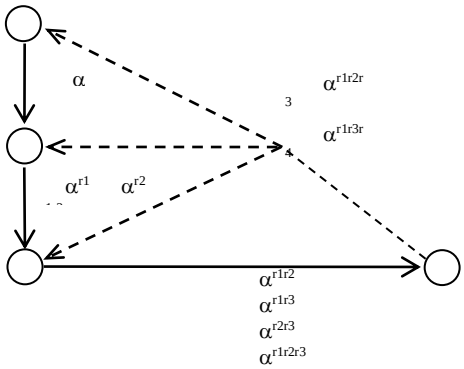


Figure 3.2. GDH.2 common key generation

GDH.2

GDH is the acronym of generalised Diffie-Hellman. Nodes form a chain and the first sends a message containing DH public value to the next one, who extends it with his DH public value and forwards. This process goes till the last node. This node is now able to generate the common key, and also key pieces that needed by each participant. These pieces are all broadcasted. So the actual session key is successfully established. (Figure 3.2)

An eavesdropper cannot generate the common secret from these public values. The last (broadcaster) node should play a central role, which is not advantageous in an ad hoc environment. [4]

Hypercube and Octopus

The main concept for a common secure key between more than two participants in Hypercube is to form pairs of nodes and establish the common secret using DH protocol. Then form pairs of pairs and perform key exchange by all participants. The problem with the Hypercube is that the number of members must be 2^n which cannot be supposed.

An extension to this problem is the Octopus protocol. This forms a hypercube kernel of the network and extends it with tentacles. First these tentacles do a DH key exchange with their respective central nodes. After that the central nodes perform the Hypercube key exchange and inform the tentacle nodes about the new key. Disadvantage of this key exchange is that Hypercube kernel plays a central role and the involvement of a new participant is difficult. [4]

Security issues in routing mechanisms

Security properties of ad hoc networks depends on the used routing mechanism, although in present routing protocols security is not included. An attacker may become involved in packet forwarding, moreover it is sufficient to run an intermediate node close and force a DoS attack using the shared radio channel. The scramble of the attacker is mostly indistinguishable from the natural loss caused by the noise of the channel. The goal is to establish a reliable channel, where trustiness can be a QoS parameter of the route.

Consequently a routing protocol should be able to guarantee some level of security of a path and to force packets to travel through this route. Using distributed mechanisms or having a node with additional routing information (e.g. at the source) the path can be determined.

Security-aware routing

Traditionally, routing protocols try to find an optimal route. The metric for optimality is distance usually measured in hops. To improve the quality of security of an ad hoc route "Security Aware ad-hoc Routing" (SAR) is used presented, which incorporates security levels of nodes.

Different techniques exist to measure or specify the quality of security of a route.

One solution is when each host has the attributes such as "trust level" and "security level". The routing algorithm uses these attributes, and only nodes that provide the required level can participate in the routing protocol. However, these levels should be immutable, so nodes with a lower level can neither change it's own nor the requested level.

In SAR the sender who initiates a route discovery, embeds the needed security attributes into the request. Intermediate nodes forward it only if it has the proper security attributes, otherwise it should be dropped. If the destination receives a request with proper security attributes, consequently an end-to-end path with the required security properties can be found, and a security-aware route could be established. SAR can be implemented based on any on-demand ad hoc routing protocol with suitable modification. [5]

These protocol modifications result in changes the nature of discovered routes. The route discovered by SAR may not be the shortest one in the terms of hop count, although SAR is able to find a route with a quantifiable guarantee of security. If one or more routes that satisfy the required properties exist, SAR will find the shortest (optimal) such route. However SAR may fail even if a network is connected, but the required security attributes cannot be provided.

A problem with SAR is that the specific levels should be authenticated; nodes should not be able to increase their level arbitrarily. We could see that authentication in ad hoc networks is not a simple process. On top of that

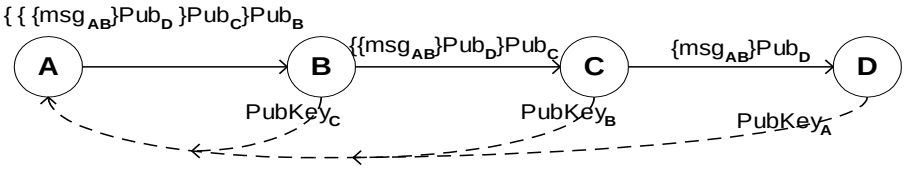
comprehensible levels reach new threats, because those levels are often related with the importance of nodes.

Onion routing

In onion routing, between peers the messages traversed securely. The sender collects the public keys of the intermediate nodes and encrypts the sent message with all of them. Each intermediate node decrypts it with its secret key, removes the outermost lock. At the destination the encryption disappears only if each intermediate node has used its secret key for decoding (Figure 4.1). [6]

This kind of routing security is applicable mostly when the sender knows the path. (e.g. DSR).

Routing security needs to be evaluated in order to eliminate undiscovered



4.1. Onion routing

vulnerabilities. This can be achieved by formal methods or by simulation. In the next section a tool for this purpose is introduced.

Casper

The language of the Casper simulator is based on the Common Authentication Protocol Specification Language (CAPSL [8]). However Casper not only defines the protocol, which is under investigation, but even a system to be checked should be specified. Therefore a player in the system is able to take different protocol roles (e.g. a player behave as an initiator or a responder also). In addition Casper can handle situations, where incoming messages are needed to forward seamlessly (*% notation*).

The basis of formal authentication and confidentiality analysis of Casper relies on the process algebra. The Communicating Sequential Processes (CSP) is a language to describe systems of parallel agents that communicates by messages in between them. This language is primarily designed to ease finding and solving the problems of concurrency (issues originated from the interaction of parallel agents) like deadlock, livelock or nondeterminism.

Process behaviour can be analysed in CSP with the Traces, Failure and Divergence model. In the Traces model the analysis is based on sequences of possible visible events (traces). The Failure model tries to identify failures caused by internal decisions of processes, while the Divergence model tries to determine cases when infinite sequence of internal events occurs.

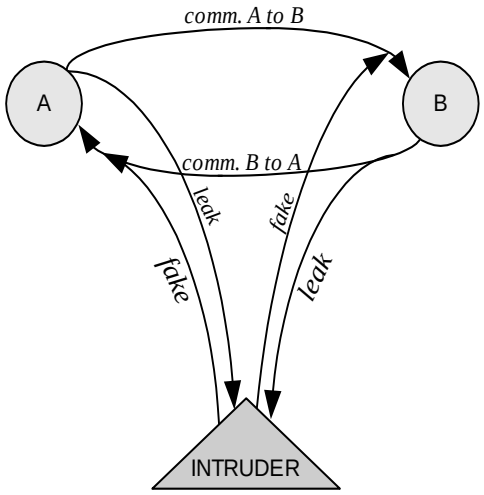


Figure 5.1. Intruder model

The Traces model is used for security analysis, because it makes an attacker easy to model, since a malicious node can deduce facts based on traces of other processes.

The method of the analysis of security protocols with Casper is the following. Between two communicating processes a communication channel exists. This channel is eavesdropped by the intruder via the *leak*, message can be forged via the *fake* channels (Figure 5.1.).

In case of analysis of complex security protocols the number of messages can be sent on the fake channel by the intruder unfortunately explodes. However in some cases with the Failure or Failure-Divergence model the behaviour of security protocols can be modelled. [7]

The input script of Casper

The input script of the Casper compiler is written in a simple descriptive language. Since this language is similar to the CAPSL notation, creation of such scripts is much easier than the creation of CSP scripts. Casper reads its input file (.spl) and creates the output (.csp).

A Casper input file is divided into eight sections. Each of these are started with a # symbol followed by the section name. Otherwise the input file can be divided into two distinct parts. The first four sections define the way the protocol operates, while the last sections describe the actual system to be checked. [8]

In the following, we will briefly examine each section in order to introduce their function. (Figure 5.2.)

```
#Free variables
A, B: Agent
S : Server
na, nb : Nonce
kab : SessionKey
f : HashFunction
SKey : Agent -> ServerKey
InverseKeys = (SKey, Skey)

#Processes
INITIATOR(A,S,kab) knows SKey(A)
RESPONDER(B) knows SKey(B)
SERVER(S) knows SKey

#Protocol description
0.    -> A : B
        [ A!=B]
1.  A -> S : {B, kab}{SKey(A)}
2.  S -> B : {A, kab}{SKey(B)}

#Specification
    Secret(A, kab, [B,S])
    Agreement(A, B, [kab])

#Actual variables
Anna, Bea, Pongo : Agent
Cili : Server
Na, Nb, Np : Nonce
Kab : SessionKey

#Functions
symbolic Skey

#System
INITIATOR(Anna, Cili, Kab)
RESPONDER(Bea)
SERVER(Cili)

#Intruder Information
Intruder = Pongo
IntruderKnowledge  =  {Anna,  Bea,
Cili, Pongo, Np, SKey(Pongo)}
```

Figure 5.2. Casper input syntax

The first section deals with the free variables, defines the variables and functions used by the protocol. Any names can be used for type names, although we mostly use standard names (*Agent*, *Nonce*, etc.). *HashFunction* and *Timestamp* types are exceptions, because they are treated differently. Functions can be defined using the −> sign, which gives the assignment. The *InverseKeys* line defines the keys that are inverses of each other, symmetric keys can be modelled as self-inverse keys.

The second section gives information about the agents running the protocol. It defines the role they play and the initial knowledge they have. Variables in brackets after the role name gives initial knowledge to the protocol run, while after the *knows* keyword the agents' functions are defined.

The protocol description is presented in the third section, which follows the commonly used notations. It describes how the sequence of messages build up a protocol run. *{m}{k}* means that the *m* message is encrypted with the *k* key. Sent messages should be evaluated by the receiver, otherwise the % notation can be used. The *{m}{k}%var* notation puts the left expression into the receiver's variable instead of evaluating it, while the *var%{m}{k}* reads the variable and sends it as *{m}{k}*. Line 0 means a message to *A* from the system. The *[A!=B]* notation forces an additional check.

The Specification section is used to specify the requirements of the protocol. There is two main type of specification: secrecy an authentication, however there exists some additional specification (e.g. *StrongSecret*, *TimedAgreement*). The first secret specifies that after a protocol run *A* thinks that *kab* is a secret that can be known by himself, by *B* and by *S*; and none of them is an intruder. The agreement specification in Figure 5.2. means that if *B* completes a run of the protocol apparently with *A*, than *A* has been running the protocol apparently with *B* and they agree in data values *kab*

Till this point, the general protocol was described. However testing the protocol always requires an actual system with specified participants, roles and variables. The actual system to be checked will be described in the following sections.

First, the variables used in the observed system are presented. The types of the actual variables must be identical to the corresponding types defined in the free variables section. Our conception is to mark actual variables with a capital first letter.

In the next section any functions used by the agents and declared in the free variables section here also have to be defined. The keyword *symbolic* means that Casper produces its own values to represent the result of function applications.

Under the system section the actual roles have to be specified. It is possible for an agent to run a protocol as an initiator and a responder too, or to run it sequentially more than once.

The last section deals with the intruder and defines the knowledge it has.

Modelling in Casper

In the following section the DSR protocol will be introduced. We show that this protocol has some security flaws and we will give some solutions for the vulnerabilities. Onion routing is also verified.

Simple DSR protocol

The first example (Figure 6.1.) models the operation of an ad hoc system using the DSR routing algorithm. In such systems sender determines the path of the packages (e.g. SAR route). This means that the destination and all the forwarder nodes are in its initial knowledge.

```
#Free variables
A, B, C : Agent
na : Nonce
skey : SecretKey
InverseKeys = (skey, skey)

#Processes
INITIATOR(A, B, C, na, skey)
FWDER(B)
RESPONDER(C, skey)

#Protocol description
1.  A -> B : C, {na}{skey}%enc
2.  B -> C : A, enc%{na}{skey}
3.  C -> B : {na}{skey}%enc2
4.  B -> A : enc2%{na}{skey}


#Specification
Secret(A, na, [C])
Agreement(A, C, [B])
Agreement(A, B, [C])

#Actual variables
Anna, Bea, Cili, Pongo : Agent
SKey : SecretKey
Na : Nonce
InverseKeys=(SKey, SKey)

#Functions

#System
INITIATOR(Anna,  Bea,  Cili,  Na,
SKey)
FWDER(Bea)
RESPONDER(Cili, SKey)

#Intruder Information
Intruder = Pongo
IntruderKnowledge  =  {Anna,  Bea,
Cili, Pongo}
```

Figure 6.1. DSR protocol

We suppose the sender and receiver have previously established symmetric keys that allow of using peer-to-peer encrypted messages. Intermediate nodes are used only to forward those encrypted messages. We model all forwarder nodes as one (*FWDER*), because introduction of several forwarders does not make additional benefit.

We use a nonce (*na*) as data that is encrypted with a secret key (*skey*) known only by the initiator and the responder. The encrypted message is sent to *B*, who forwards the given encrypted message to the next given node without evaluating it. This is why the *%enc* notation is used. The responder answers with the same encrypted message that arrives back.

The actual system is the simplest one, where each role is played only once by given agents.

The following result has been given for this system.

The secret specification passes, which means no one can get *na* except the *A* and *C* agents.

The *Agreement(A, C, [B])* specification fails, and Casper gives an attack that can be seen in Figure 6.2.

```
System level:
1.  Anna    ->  I_Bea   : Cili, {Na}{SKey}
2. I_Pongo ->  Cili    : Anna, {Na}{SKey}
3.  Cili    -> I Pongo : {Na}{SKey}
```

Figure 6.2. DSR attack 1.

The intruder (*I_Bea*) eavesdrops and removes the first message sent from *Anna* to *Bea*. This intruder participated the protocol as *Bea*, however it uses the identity of *Pongo* (*I_Pongo*) to send the second message to *Cili*. So *Cili* completes a turn of the protocol apparently with *Anna*, and *Anna* has been running the protocol apparently with *Cili*. On the contrary to the specification they did not agree in the data value *B*, because *Anna* uses *Bea* and *Cili* uses *Pongo* as *B*. This is a wormhole attack, where the attacker forwards the messages in a way different from the source-route specification.

```
System level:
1.  I_Bea  ->   Bea    : Pongo, Garbage
2.   Bea   -> I_Pongo : Bea, Garbage
3. I_Pongo ->   Bea    : Garbage
4.   Bea   ->  I Bea   : Garbage
```

Figure 6.3. DSR attack 2.

The *Agreement(A, B, [C])* specification fails too that can be seen in Figure 6.3. An intruder can give the forwarder node garbage data, therefore it will not be able to distinguish this garbage from encrypted data. Keep in mind that *Bea* is the model of a sequence of forwarder nodes, so this DoS attack can consume resources of many nodes.

DSR protocol with hash chain

```
#Free variables
A, B, C : Agent
na : Nonce
f : HashFunction
Skey : Agent -> SecretKey
InverseKeys = (Skey, Skey)

#Processes
INITIATOR(A, B, C, na) knows Skey(A)
FWDER(B) knows Skey(B)
RESPONDER(C) knows Skey

#Protocol description
1.     A   ->   B   :   C,   {na}{Skey(A)}%enc,
f(Skey(A))%henc
2.     B   ->   C   :   A,   enc%{na}{Skey(A)},
f(henc%f(Skey(A)), Skey(B))
3.  C -> B : {na}{Skey(A)}%enc2
4.  B -> A : enc2%{na}{Skey(A)}

#Specification
Agreement(A, C, [B])
…
```

Figure 6.4. DSR protocol with hash chain

In the following example, we have modified messages, in that way each participant puts some hashed secret into the outgoing message. This provides that the forwarder nodes can be verified by the peers. The first part of the modified file can be seen in Figure 6.4. We can see in message 1 and 2 that each forwarder appends its own hashed secret.

The agreement specification fails now again (Figure 6.5.), because the first message is intercepted by the intruder (*I_Bea*) and the second message says *Cili* that *Pongo* is the forwarder node, who gave his correct hashed secret.

So this hash chain still did not solve the problem.

Modified DSR protocol

An appropriate solution should contain the source route information signed by the sender, which can be checked by the receiver. The first part of this third example can be seen in Figure 6.6.

```
#Free variables
A, B, C : Agent
na : Nonce
f : HashFunction
Skey : Agent -> SecretKey
InverseKeys = (Skey, Skey)

#Processes
INITIATOR(A, B, C, na) knows Skey(A)
FWDER(B) knows Skey(B)
RESPONDER(C) knows Skey

#Protocol description
1.  A -> B : C, {na}{Skey(A)}%enc, f(A, B, C,
Skey(A))%henc
2.     B   ->   C   :   A,   enc%{na}{Skey(A)},
f(henc%f(A, B, C, Skey(A)), Skey(B))
3.  C -> B : {na}{Skey(A)}%enc2
4.  B -> A : enc2%{na}{Skey(A)}

#Specification
Agreement(A, C, [B])
…
```

Figure 6.6. Modified DSR protocol

In this example, message 1 contains the keyed hash of the path. Therefore this cannot be manipulated by agents. A forwarder node attaches a keyed hash to the incoming message and sends to the receiver *C*. *C* is able to verify all the hashed values, since it knows all the secret components.

Casper found no attacks, so this protocol can be an appropriate solution for the given specification. This means that the source route cannot be manipulated, the forwarder nodes cannot be replaced by an intruder.

Onion routing

In section 4 we have described the Onion routing mechanism. Its behaviour will be examined in the following example. The input file can be seen in Figure 6.7.

The initiator knows all public keys and each agent knows only his secret key. The route information included in the encrypted message. Therefore the receiver is able to verify the forwarder's identity, so man in the middle attacks are eliminated.

```
   #Free variables
   A, B, C : Agent
   na : Nonce
   PKey : Agent -> PublicKey
   SKey : Agent -> SecretKey
   InverseKeys = (SKey, PKey)

   #Processes
   INITIATOR(A, B, C, na) knows SKey(A),
PKey
   FWDER(B) knows SKey(B)
   RESPONDER(C) knows SKey(C), PKey

   #Protocol description
   1.  A -> B : {({na, A, B,
C}{PKey(C)}%enc), C}{PKey(B)}
   2.  B -> C : enc%{na, A, B, C}{PKey(C)}
   3.  C -> A : {na}{PKey(A)}

   #Specification
   Agreement(A, C, [B])
   Agreement(C, A, [B])

   #Actual variables
   Anna, Bea, Cili, Pongo : Agent
   Na : Nonce

   #Functions
   symbolic PKey
   symbolic SKey

   #System
   INITIATOR(Anna, Bea, Cili, Na)
   FWDER(Bea)
   RESPONDER(Cili)


   #Intruder Information
   Intruder = Pongo
   IntruderKnowledge = {Anna, Bea, Cili,
Pongo, SKey(Pongo)}
```

Figure 6.7. Onion routing

Conclusion

Security analysis of ad hoc networks is a recent research topic. Investigations in ad hoc networks are focused on mostly performance and scalability properties, however security is essential. Several solutions have evolved for security in ad hoc networks, however most of them are not evaluated by simulation or by formal methods.

References:

[1] Charles E. Perkins: Ad-hoc Networking, Addison-Wesley 2001

[2] Lidong Zhou and Zygmunt J. Haas. Securing Ad Hoc Networks (IEEE Network Magazine, vol. 13, no.6, November/December 1999)

[3] Jean-Pierre Hubaux, Levente Buttyán and Srdan Capkun. The Quest for Security in Mobile Ad Hoc Networks (ACM Symposium on Mobile Ad Hoc Networking and Computing, MobiHOC 2001)

[4] Maarit Hietalahti. Key Establishment in Ad-hoc Networks (Proceedings of the Helsinki University of Technology, Seminar on Network Security fall 2000)

[5] Seung Yi, Prasad Naldurg and Robin Kravets. Security-Aware Ad-Hoc Routing for Wireless Networks (Technical Report UIUCDCS-R-2001-2241(ps/pdf), August 2001)

[6] M.Reeds, P.Syversion and D.Goldschlag. Anonymous Connections and Onion Routing. IEEE Journal on Selected Areas in Communications, vol.16 no 4., May 1998

[7] Steve Schneider. Concurrent and Real-time Systems. The CSP Approach. 2000

[8] Peter Ryan, Steve Schneider, Michael Goldsmith, Gavin Lowe and Bill Roscoe. Modelling and analysis of security protocols. 2001

Beatrix FREGAN

POURQUOI LA GUERRE INFORMATIQUE ?

Contre qui les systèmes d'information doivent-ils servir ?

Les techniques qui suffisent contre un adolescent équipé d'un modem ne seront d'aucune utilité face a une importante agence de renseignements. Contre le premier, on utilisera une sécurité renforcée des mots de passe, tandis que le second peut recourir et recourra aux écoutes, à la cryptanalyse, à l'interception des signaux électroniques provenant des ordinateurs et des câbles et même à la fouille des poubelles en salle informatique. La sécurité informatique n'est pas un but, c'est un moyen d'atteindre le but : la sécurité de l'information. Toutes sortes de moyens peuvent être utilisés lorsque cela s'avère nécessaire et approprié. La force des moyens de protection informatique doit être adaptée à la menace. Le rôle de l'Etat est central pour aussi bien protéger l'économie nationale, que des données militaires ou diplomatiques qui lui sont vitales. Dans cet exposé, ne seront analysées que les menaces à la souveraineté nationale d'un Etat. Les auteurs de ces menaces étant des professionnels de l'informatique soit a la solde d'autres Etats ou obéissant à des motivations personnelles et difficilement prévisibles.

L'élargissement du concept de sécurité

Les menaces, via internet, pour la sécurité nationale deviennent de plus en plus d'actualité avec l'élargissement du concept de sécurité nationale. Définissant d'abord les menaces de nature militaire, c'est-à-dire les guerres essentiellement, le concept a été modifié pour prendre en compte différents types de menace non-militaires tels que les menaces environnementales, démographiques etc…

Buzan[1] définit le principe de sécurité par rapport à une menace pesant sur des valeurs essentielles pour une société. Le stratégiste américain Ullman affine cette thèse en explicitant la double nature d'une menace. D'une part, une menace contribue a la dégradation du niveau de qualité de vie d'une population d'un Etat, et d'autre part, l'ampleur des choix politiques est considérablement réduite pour le gouvernement et ses administrations ainsi que pour les acteurs du privé.

Les cybers-attaques, les nouvelles menaces du XXI siecle ?

Bien que les formes traditionnelles de menaces sécuritaires demeurent, il semble néanmoins que les pays industrialisés, en particulier, soient nouvellement menacés par des formes d'agression via les réseaux de communication informatiques. « Les Armes sont les ordinateurs et le front est

[1] People, States, and Fear. The National Security Problem in International relations

partout », tel est le sous-titre du livre de James Adams, La prochaine guerre. Bill Clinton prononça le discours suivant en s'adressant à l'Académie Navale américaine: « Notre sécurité est de plus en plus mise au défi par des menaces non-traditionnelles de la part d'adversaires, anciens et nouveaux, non seulement des régimes hostiles, mais aussi des criminels et terroristes qui ne peuvent pas nous vaincre sur le terrain de bataille, mais qui néanmoins recherchent des nouvelles façons de nous attaquer en exploitant les nouvelles technologies et la mondialisation». Ces menaces sont plus que réelles. Deux jeunes, par exemple, dirigés par un hacker israélien en février 1998, organisèrent des attaques contre les systèmes informatiques du Pentagone, de la NSA et d'un laboratoire de recherche nucléaire. Les perturbations informatiques qui suivirent cette attaque furent décrites par John Hamre, le vice-secrétaire à la défense comme étant «l'attaque la plus systématique et la mieux organisée» qu'il y ait jamais eu contre les systèmes de défense américains. Plus récemment, début mars 2000, la police japonaise dévoila l'origine du « group M », une entreprise de software dont les propriétaires seraient liés à la secte Aum qui provoqua en 1996, une attaque au gaz dans le métro japonais. Depuis le début de cette année, les sites gouvernementaux japonais ont été victimes de 11 attaques. Il semblerait ainsi que la secte Aum s'oriente vers une stratégie de cyber-attaque.

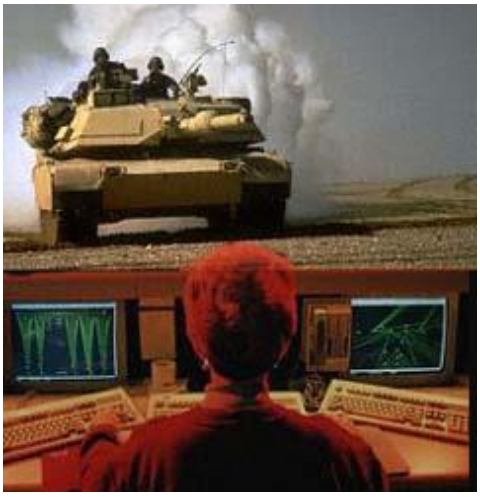
Penser la cyberguerre

Après la guerre menée au Kosovo, les certitudes héritées de la guerre froide s'effacent, laissant la place à des nouvelles doctrines militaires. Le réseau, système nerveux par lequel circule l'information, se fait paradigme organisationnel. Dans leur analyse de cette mutation, des stratèges sont impatients de voir les Etats-Unis se préparer à la «cyberguerre», ou, pour subjuguer l'adversaire, il suffirait de perturber ses structures de commandement, de communication et de pensée, plutôt que d'entreprendre sa destruction physique[2].

La vulnérabilité du net (exemples récents)

Lundi 21 février 2000, vers 10H20, les internautes surfant sur Yahoo, habitués a attendre 1,7 secondes pour le téléchargement du serveur, durent patienter 6 secondes. A 10H30, tous ceux qui essayèrent d'accéder au site de Yahoo virent s'afficher sur leurs écrans des messages d'erreur. Au même moment, Global Center, le serveur californien de Yahoo, était envahi par d'immenses vagues d'informations. Soit 1 milliards de bites par seconde, l'équivalent de la masse d'information qui est perçue en période normale pendant une semaine.

[2] voir F.Pisani, Penser la cyberguerre et F.Pisani : Les doux penseurs de la cyberguerre



Yahoo fut victime d'un « refus d'accès » : une tentative délibérée de fermer le réseau en l'encombrant de données inutiles. L'attaque fut déclenchée de 50 lieux différents, un signe évident que le manipulateur utilisait des ordinateurs dispersés pour mener son attaque. Du lundi au mercredi de la meme semaine, les grands sites américains furent victimes d'attaques. Entre autres, Buy.com dont l'acces ne fut possible que pour 9% des demandes d'entrée, eBay qui fut paralysé plusieurs heures mardi 22 février, Amazon.com ou il fallait 380 secondes pour accéder au site de 5H a 5H45 etc…

Les "hackers" procèdent en 5 étapes :

a) Le hacker cherchent sur internet des serveurs et ordinateurs réseau vulnérables parmi les entreprises et les universités.

b) Le hacker peut ensuite pénétrer ces ordinateurs en y installant un logiciel « esclave » (« slave » software program) qui attend ses instructions.

c) Il émet un signal nécessitant des ordinateurs pénétrés une réponse.

d) Leur réponse n'est pas redirigée vers le hacker mais au contraire, il crée « une adresse de retour » qui oriente les réponses vers les sites victimes.

e) Le site attaqué est submergé de fausses réponses de centaines d'ordinateurs qui encombrent le système.

Un exemple de guerre inter-étatique: une nouvelle forme d'expression du conflit sino-taiwanais (Les élections présidentielles de mars 2000 à Taiwan)

Durant les élections présidentielles, en mars 2000, les spécialistes de l'informatique au ministère de la défense nationale à Taiwan scrutèrent le réseau informatique à la quète de «hackers rouges», les saboteurs informatiques de la République Populaire de Chine. En effet, Le ministère de la défense craignait un sabotage électronique de la part de la Chine dans le but d'interrompre les élections. Les spécialistes étaient à la recherche de bombes e-mail, de virus et de tentatives clandestines de pénétrer les sites

gouvernementaux protégés. Un haut membre du ministère de la défense taiwanaise a d'ailleurs signifié le degré d'inquiétude du ministère en disant: «nous voulons que le Comité en charge du déroulement de l'élection traite ce problème comme un exercice militaire». En effet, des l'origine du conflit sino-taiwanais, la Chine a toujours essayé d'intimider son adversaire. En 1996, La Chine, lors d'un exercice militaire, lança des missiles à proximité de Taiwan. Cette année, la Chine a encore menacé d'envahir Taiwan si les discussions portant sur la réunification continuaient à être reportés.

La Chine semble s'être orientée en particulier vers la recherche de moyens pour faire pression sur Taiwan par le biais des nouvelles technologies de l'information. Pour le moment, les armes dont disposent les saboteurs informatiques sont simples : des logiciels qui peuvent détruire, subtiliser ou désorganiser les sources d'informations utilisées par l'armée ainsi que les réseaux nationaux de communication.

Pour le futur, il est envisageable que les «hackers» des deux camps adverses puissent paralyser les systèmes bancaires, les réseaux de transport et de communication.

Károly FEKETE

PERSONAL MILITARY COMMUNICATIONS SYSTEM

Károly FEKETE
fekete@zmne.hu
Department of Military Communications
System Management, ZMNE

Keywords: Personal area network, Body LAN, Wireless LAN

Abstract

Anytime, anywhere – they are information on demand in todays battlespace, when the Land Force Warriors with the most information have the advantage. Nowadays military professionals talk about the coming of the information age and globalization. Globalization is a result of the information age and the world has shrunk with special regard to telecommunications.

Aldous Huxley in his book „Brave New World" mentioned that dictators do need to control information to maintain control – since knowledge is power. Over the last decade great changes have occured in telecommunications and information science, but contrary Huxleys predictions, information technology in today's world *has curbed* the power of dictators. With contact this social standing, as warfare moves away from bipolar large and vulnerable formations to small, qualified units, speediness and comrehensive command and control becomes a priority.

If we want increase the responsibility, effectiveness and autonomy given to individual Land Force Warriors, then warfighters support with personal communications system is indispensable. The personal location and communication system must function on platoon, squad and individual level under a variety of conditions while receiving information from multiple sources, soldiers, sensors deployed on battlefield (Fig. 1.).

Higher command and control has been a major contributing factor to successful military operations because of advanced information gathering now offer commanders a dinamic, real-time picture of the battlefield. For example if a soldier sees an armoured enemy troops he will update descriptive data into his mobile network database. After these if another soldier requests a situational update, the software in the first soldiers personal communication system (PCS) will pass on the data about the enemy troops.

In these conditions the PCS must be able to transmit from 10 bit/s up to 1 Mbit/s. Consequently we must allow the creation of an autonomous adaptive network.

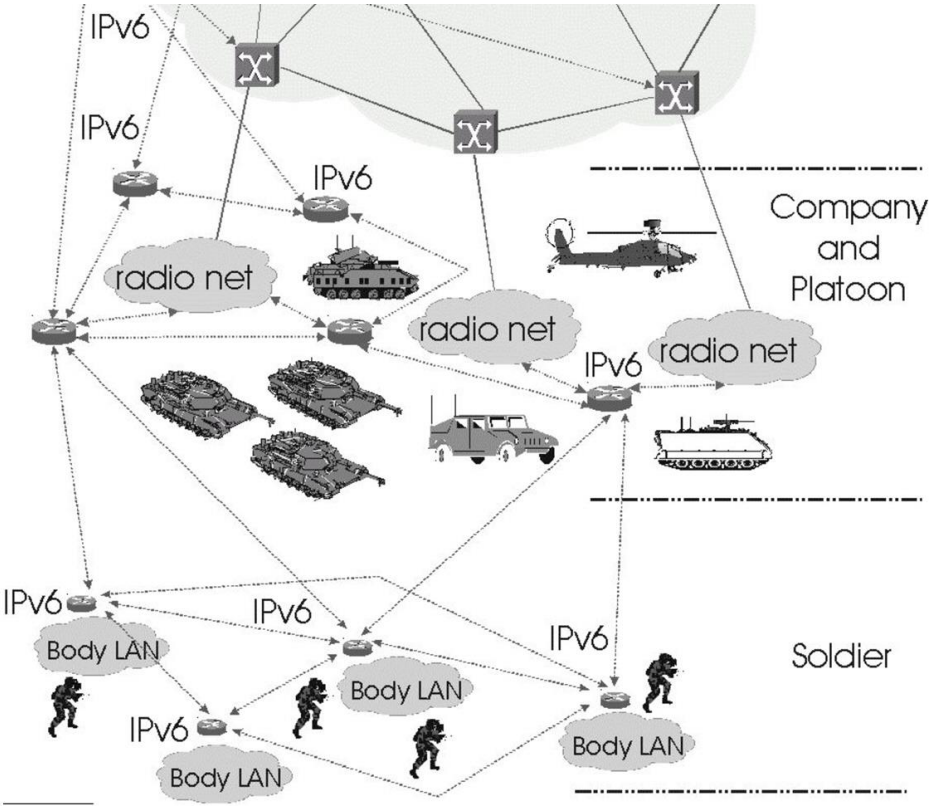


Fig. 1.The personal location and PCS

As illustrated by the network specifications provided in Fig. 2, for the PCS or Body LAN the best selection is IEEE 802.11b Wireless LAN. 802.11b defines an from 1 to 11 Mbit/s data rate in the 2,4 GHz band. Using this technology a land warrior with a Nootebok or a Personal Digital Assistan (PDA) can get broadban speeds within 300 m (1000 m in boosted method) of an access point, and these access points are being installed in tank, armored and unarmored military vehicles (Fig. 3, 4).

The functionality supported by the IEEE 802.11b includes:

- Intercom voice conversations and digital datacommunications;
- Voice intercom communications;
- Multiple virtual channels;
- Broadcast datacommunications;
- Automatic switching between distributed network control.

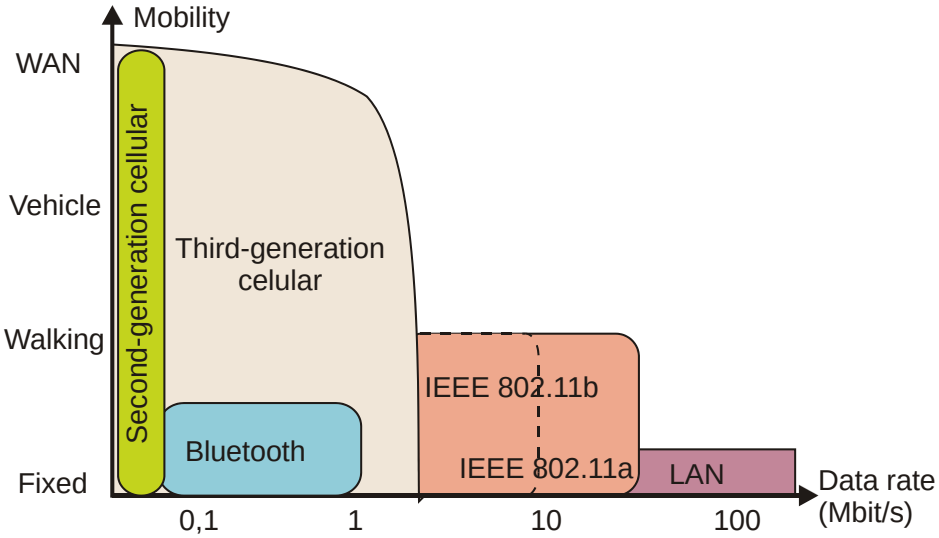


Fig. 2. Mobility versus peak data rate *(Source: HiperLAN2, IEEE Communications Magazine, June 2002, pp. 131.)*

Fig. 3 Internal connection of Body LAN in armored military vehicle

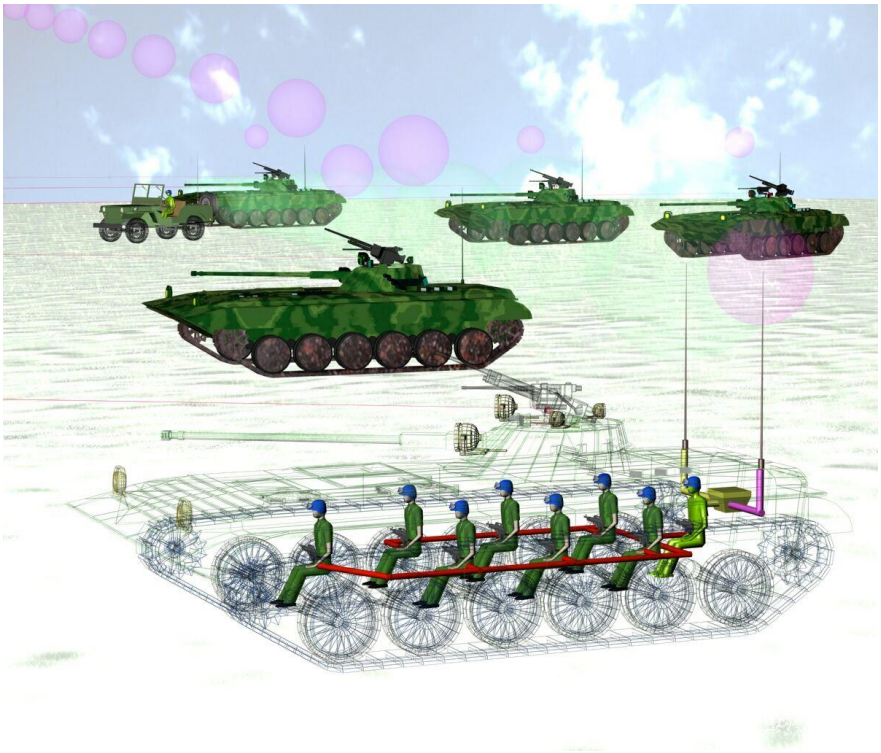


Fig. 4 Squad level communications

A typical network system architecture for the PCS is depicted in Fig. 5. The architecture contains two main components:

- Universal adapter interface (UAI);
- Personal communication units (PCU).

The PCU grants for an individual soldier access to the Wireless WAN (WWAN). The UAI is a device provides centralized control of the wireless network. Messages transmitting and receiving by the PCU are routed through the UAI. PCU capable of forming a small wireless network in the absence of UAI.

If the PCU is out-of-range of an UAI, then wireless configuration we can call an „autonomous PCU”. Autonomous PCUs may initiate communications with PCUs already in ad-hoc, repeater-based network.

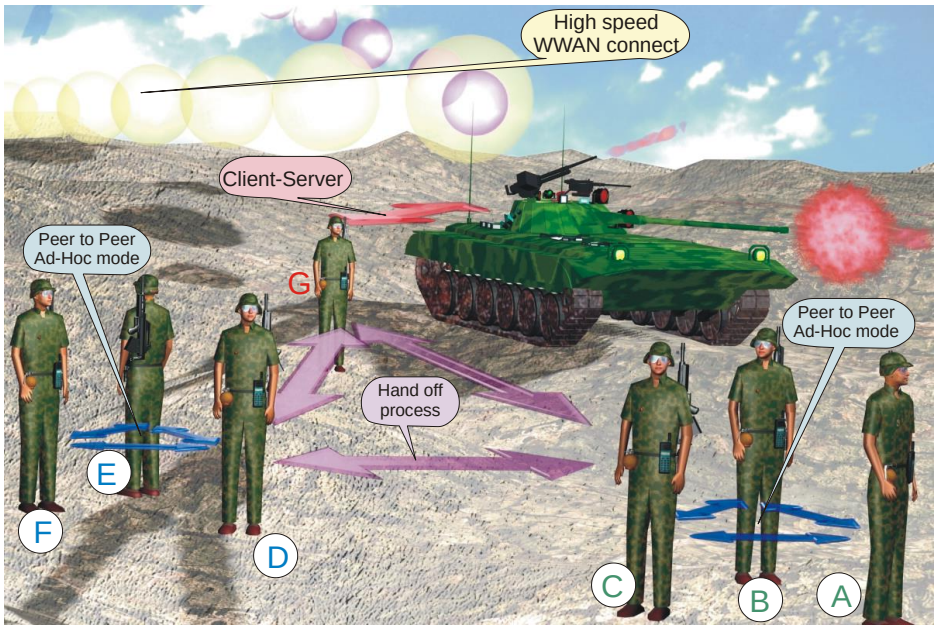


Fig. 5. A typical network system architecture for the PCS

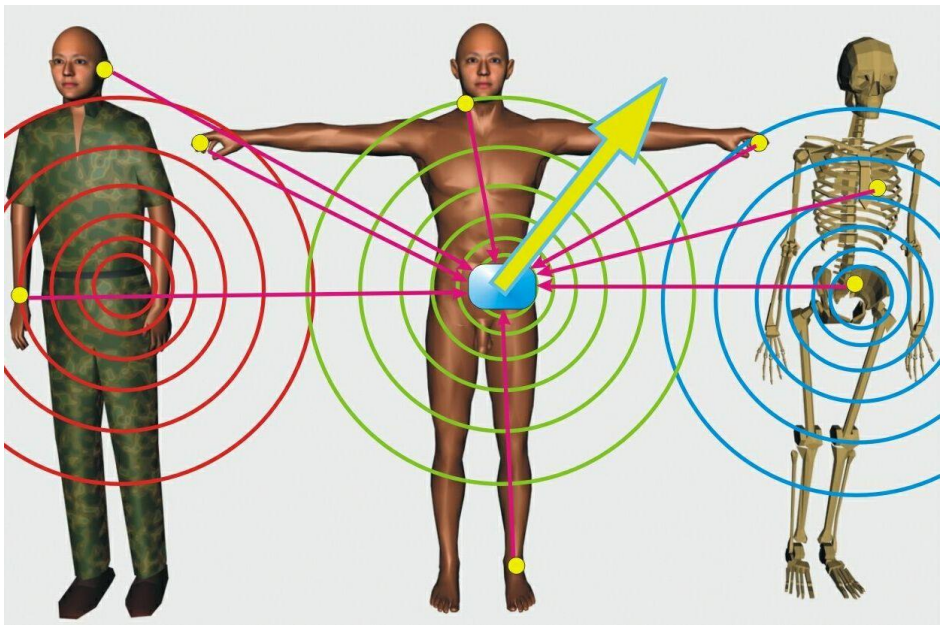


Fig. 6. Possible placing of biomedical sensors

About physiological readiness of soldiers the commander can receive basic information via portable biomedical sensors. The sensors we may integrate into a wireless Body LAN (Fig. 6.).

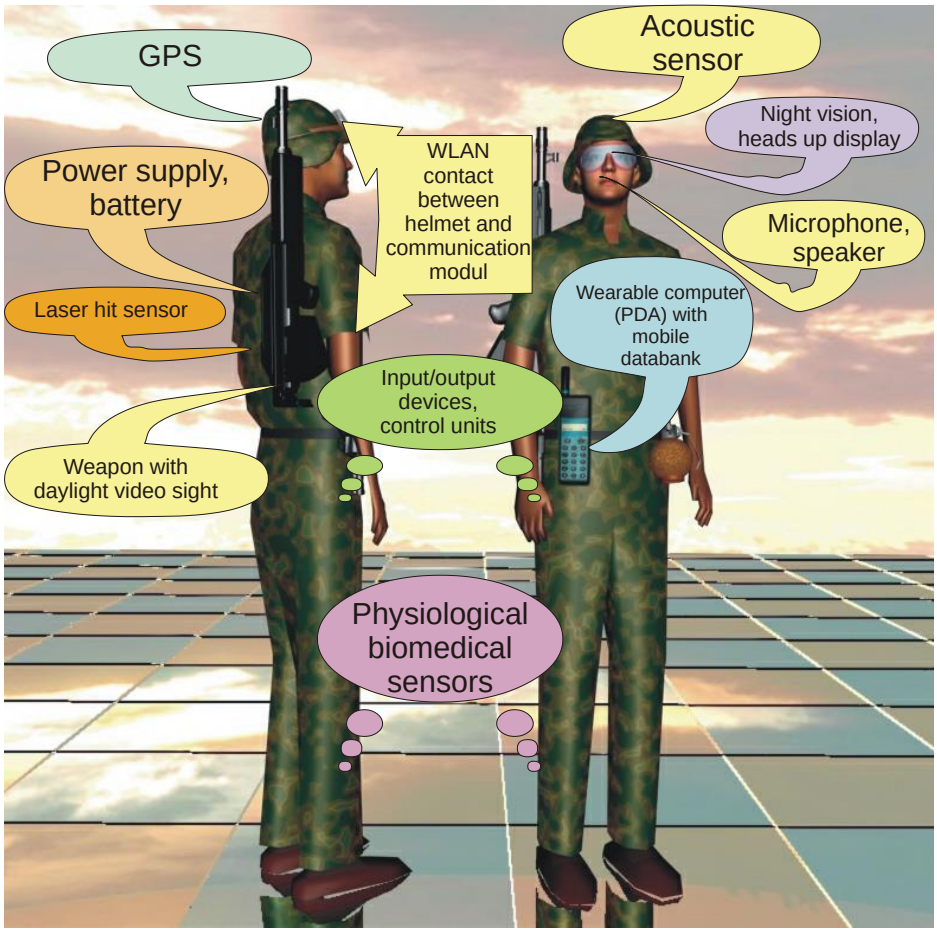


Fig. 7. Parts of Body LAN

The portable biomedical sensors capable detect:

- Injury;
- Dehydration;
- Sleep deprivation;
- Stress- (by measuring eye movements, hormonal tests, voice);
- Movement;
- Soldier system weight;
- Blood pressure;
- Fatique;

- Arterial oxygen saturation;
- Core and skin temperature;
- Respiratory rate.

The Land Forces Warriors Body LAN may involves:

- Navigations system (Global Positioning System);
- Power supply (accumulators, batteries);
- Laser hit sensors;
- Acoustic sensors with high sensitivity;
- WLAN for contact between helmet and communication modul;
- Night vision, heads up display;
- Adjustable michrophone and head speaker;
- Physiological and biomedical sensors;
- Wearable computers with IEEE 802.11b (e) WiFi modul;
- Input/Output devices (mouse, keyboard, tension sense devices).

The PCS of Land Force Warriors is not cheap, but nowadays opened a technological window before realization of PCS. There is a question only: What do we want?

References

[1] Derek Kerton: Wireless and Telco Glossary v.1.2, www.kerton.com

[2] GPRS – General Packet Radio Service, Usha Communications Technology, 26 June 2000.

[3] Mats Nilsson: Third-generation radio access standards, Ericsson Review No. 3, 1999., pp. 110-121.

[4] Commercial Portables Product Marketing: Bluetooth Technology Overview, Compaq Computer Corporation, Fourth Edition, November 2000, pp. 1-21.

[5] Kaveh Pahlavan: Introduction to Local Area Networks, Telecommunications Laboratory and CWC, University of Oulu, Finland.

[6] Kaveh Pahlavan: Trends in Wireless LANs, Second IEEE Workshop on Wireless LAN, Worchester Politechnic Institute, Worchester, MA 01609.

[7] Pekka Sahi: Standards Related to Wireless LANs (survey and comparison), Department of Computer Sciences, Helsinki University of Technology, October 1999.

[8] Jim Zyren, Al Petrick: IEEE 802.11 Tutorial, pp. 1-7.

[9] Jim Zyren: 802.11g spec: Covering the basics, Strategic Marketing for Wireless Networking, Intersil Corp., Irvine, USA., February 2002., www.commsdesign.com/story/OEG20020201S0035

[10] Gregory Parks: 802.11e makes wireless universal, Network World, 3 December 2001., pp. 1-2.

[11] Sean Convery, Darrin Miller: SAFE: Wireless LAN Security in Depth, Cisco Systems, Inc., San Jose, USA, 2001. pp. 1-48.

[12] Remote VPN Implementation Issues: Network Security Newsletter, Volume 1, Issue 3, 4/4/00.

[13] Stephen Brewster, Robin Murray: Presenting Dynamic Information on Mobile Computers, Glasgow Interactive Systems Group, Department of Computing Science, Universiti of Glasgow, www.dcs.gla.ac.uk/~stephen

[14] Optimized interactive images and graphics for the Wireless Web, Simlylook, Inc, November 30, 2000.

[15] W. Jacklin, S. Collar, S. Stratmoen: A personal and inter-vehicle cordless communications system, Northrop Grumman Corporation, Electronics Systems Integration Division, Rolling Meadows, Illinois, USA.

[16] Mathew Cox: Like a Chameleon, DefenseNews, July 15-21, 2002., pp. 40.

[17] Mariann Lawlor: Personal Physiological Monitors Find Warfighter-effectiveness edge, SIGNAL, Agust, 2000., pp. 47-50.

[18] George I. Seffers: New Kind of Soldier, DefenseNews, February 14, 2000., pp. 20.

[19] Fekete Károly: Toward the within of military CIS convergence (IPv4 and IPv6), A katonai kommunikációs rendszerek fejlődési irányai –kihívások és trendek a XXI. században, Nemzetközi szakmai tudományos konferencia, 2001. november 28., Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, pp. 53-62., ISBN 963 00 8819 3

Ferenc EGEDI, Bertalan EGED

ROUND-TRIP TIME MEASUREMENTS IN MOBILE ENVIRONMENT

Budapest University of Technology and Economics
Department of Broadband Infocommunication Systems
Wireless Information Technology Laboratory
3 Goldmann Square, Budapest, H-1111 Hungary
Phone: +36-1-463-4319 Fax: +36-1-463-3289
E-mail: egedif@wit.mht.bme.hu URL: http://wit.mht.bme.hu

Abstract

Using of wireless equipment for Internet access is one of the highest increasing service segments in the telecommunication area. This kind of service offers the freedom of mobility and mass information backbone to the user. Providing general quality of service assurance framework around the system is necessary for a lot reason. Continues measurements and monitoring of the network performance and parameters are the key elements of such framework.

Because of the different properties of the mobile terminal clients, used protocol stack and the server content, the methods developed for performance measurements in normal Internet environment can not be applied directly. However, the methodology is usable and with the appropriate modifications the required procedures can be defined.

The paper deals with the definition, the implementation and the results of the proposed measurements and monitoring method of the round-trip time delay in a mobile phone, using WAP based wireless Internet access, environment.

Keywords: network performance, performance monitoring, QoS, round-trip time delay

Introduction

There are approximately 400 million mobile phone users all around in the world. There are more also millions of Internet users in the world. These two market segments are rapidly converging on the same spot: the small, lightweight and inexpensive mobile computing devices that are equally suitable for high-quality voice communication, moderate bandwidth data communication, wireless Internet connectivity, access to the Internet services such as e-mail and other Web server contents.

Few years ago several industry leader companies in the telecommunication area predicted this convergence and started the collaboration to standardize an architecture for providing advanced data services to mobile phones.

This architecture, which draws heavily from the existing Internet technologies, is based on a protocol stack called the Wireless Application Protocol (WAP) [1].

WAP sits on top of a variety of wireless bearers. Today the most widespread is the GSM infrastructure and its data carriers like SMS, USSD, CSD, HSCSD, GPRS. It provides the integration of telephony and data services with using of the Wireless Application Environment (WAE) for building applications.

As in all of the modern telecommunication and networking services performing the quality assurance framework around the services is important for service providers. Measuring and continues monitoring of the network performance (NP) and parameters are the main elements of the general quality of service (QoS) framework.

The paper after the brief introduction of the WAP based wireless Internet access introduces the place of a network performance measurement and monitoring in a QoS system. It introduces a new method for measurements of the round-trip time delay between the mobile terminal client and content provider server in the WAP environment and shows the results of the measurements obtained using the network of the three Hungarian GSM service providers.

WAP Based Wireless Internet Access

The Characteristic of the Wireless Environments

Mass-market, hand-held wireless devices present a more constrained computing environment compared to desktop computers. Because of fundamental limitations of power and form-factor, mass-market handheld devices tend to have:

- less powerful CPUs,
- less memory (ROM and RAM),
- restricted power consumption,
- smaller displays, and
- different input devices (eg, a phone keypad).

Similarly, wireless data networks present a more constrained communication environment compared to wired networks. Because of fundamental limitations of power, available spectrum, and mobility, wireless data networks tend to have:

- less bandwidth,
- more latency,
- less connection stability, and
- less predictable availability.

The WAP programming model

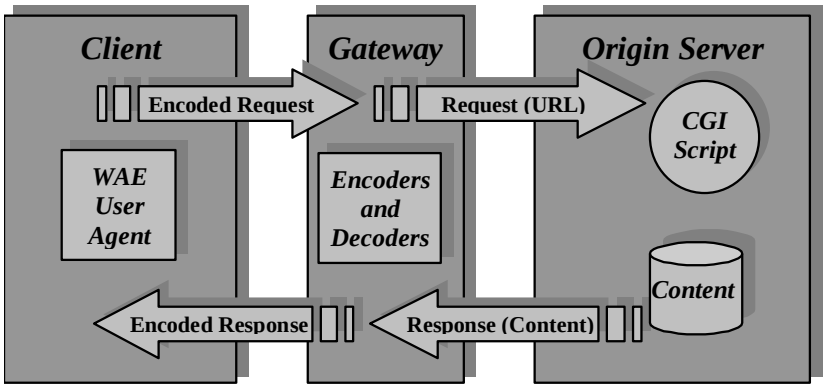


Figure 1: The programming model of the WAP contains a WAP gateway between the server and client

The WAP content types and protocols have been optimized for mass market, hand-held wireless devices. WAP utilizes proxy/gateway technology to connect between the wireless domain and the WWW. The WAP proxy/gateway typically is comprised of the following functionality:

- Protocol Gateway – The protocol gateway translates requests from the WAP protocol stack (WSP, WTP, WTLS, and WDP) to the WWW protocol stack (HTTP and TCP/IP).
- Content Encoders and Decoders – The content encoders translate WAP content into compact encoded formats to reduce the size of data over the network.

This infrastructure ensures that mobile terminal users can browse a wide variety of WAP contents and applications, and that the application author is able to build content services and applications that run on a large base of mobile terminals. The WAP proxy/gateway allows content and applications to be hosted on standard WWW servers and to be developed using proven WWW technologies such as CGI scripting.

The WAP Stack Architecture

Let us take a more detailed look at the overall WAP stack architecture. WAP has a layered protocol architecture according to recommendation of the International Standard Organization (ISO) network model.

The WAP Application Environment (WAE) is the topmost layer of the architecture that provides a markup (WML) and a script language (WMLScript) similar to HTML and JavaScript accordingly for application development. The next layer of the WAP architecture is the Wireless Session Protocol (WSP). The simples description of WSP is that it is a binary,

tokenized version of HTTP 1.1 designed specially for browser-like transactions an low-bandwidth wireless networks with relatively long latency. The third layer of the WAP architecture is the Wireless Transaction Protocol (WTP), a lightweight transaction protocol. The next on is the Wireless Transport Layer Security (WTLS) that is a security protocol based on the industry-standard Transport Layer Security (TLS). The final layer of the WAP architecture is the Wireless Datagram Protocol (WDP). This is the layer provides a consistent interface for different wireless carriers and the higher layers of the architecture.

Consideration of the Network Performance Monitoring

Network Performance

A general definition of network performance (NP) can be found in the Recommendation E.800 of ITU [2] and is reproduced hereby: "The ability of a network or a network portion to provide the functions related to communications between users".

Network performance is a statement of the performance of connection element or concatenation of connection elements employed to provide a service. It is defined and measured in terms of parameters that are meaningful to the network and service provider and are used for the purposes of system design, configuration, operation and maintenance. NP is defined independently of terminal performance and user/customer actions. It is also service independent in that it must be able to support all the services the particular network level is required to transport.

The performance of the network is generally aimed to provide the Quality of Service (QoS) offered to the user/customer.

Relationship Between of QoS and NP

Methodology for handling aspects of NP related to QoS can be the following [3]. The user's QoS requirements is the starting point. This is mapped into QoS offered parameters by the service provider. These are mapped to network and non-network related performance parameters. The network related parameters are mapped into NP parameters and target values are assigned.

Planning documentation are derived from these parameters. Several set of monitoring systems keeps track of the desired performance. The achieved end-to-end QoS performance is derived from the measurements and combined with the non-network related QoS. This is compared with the users/customers' QoS perceived obtained, usually customer surveys. Corrective action is taken where necessary.

Definition of Characteristics

As it is declared in [4] a QoS characteristic is a quantifiable aspect of QoS, which defined independently of the means by which it is represented or controlled. Efforts are made to achieve maximum consistency of definition

across different characteristic by defining ‘generic’ characteristics, and then specializing them to particular environments and deriving others from them.

So, for example time delay is a generic characteristic parameter. Some specialized characteristic can be defined from time delay, one of them is transit delay. Various further specialization can be done they may or must be applied to make the characteristic concrete, these include specifying the type of data transferred, the points between which transit is defined, and so on.

Specialization makes an abstract characteristic more concrete. When developing a widely applicable QoS mechanism, it may be valuable to work with characteristic at appropriate levels of abstractions. In any practical application of QoS management a characteristic must be completely specialized, so that it is clear what its value mean.

Some characteristic can be defined as (mathematical) function of others. These are termed ‘derived’ characteristics. One of the most important type of derivation is statistical. Technically the statistical derivations are regarded as a function of random variable that represents the ‘base’ characteristic from which they are derived. The specialization that apply to statistical derivation are exactly those that apply to the base characteristic from which is derived. From time delay, for examples, one can derive the characteristics mean transit delay, variance of transit delay between mobile terminal and switching center, and so on.

Round-Trip Time Measurements in WAP Environment

Specialized delay times

As we can see in [4] time delay is one of the defined QoS characteristics with general importance. Using the introduced methodology we can divide the general time delay to some different parts and we have to specialize these delays to fill them with concrete meaning. Because the time delay in wireless networking environment is a random variable we derive the statistical characteristic of the time delay.

The general framework model of the QoS management requires the measurements of the specialized parameters and the calculation of the derived characteristic. The connection between the measured and derived values for the time delay parameters and for example the percentage of users/customers experiencing payment transaction delay should be made available. For keeping the QoS characteristic at a constant level continues monitoring of the time delay is necessary as it is defined in a general QoS framework model.

Our goal was the development of a measurement procedure and measurement setup with the necessary hardware and software elements to satisfy the measurement and monitoring requirements of a QoS framework.

In the model of an on-line payment service with WAP enabled device there we can specialize some different delays. The concrete content of these time delays can be defined and translated into performance parameters of different

components of the transaction. At the first assumption the transaction delay can be a sum of the delay from WAP enabled client terminal to WAP gateway, the processing time of the gateway, the delay from the WAP gateway to the telebanking server, the processing time of the server, the delay from server to gateway, the processing time of the gateway and finally the delay from the gateway to the terminal. All of these delays depending on some factors like network load, count of concurrent on-line requests, and so on.

The connection between the WAP gateway and telebanking terminal implemented as a standard Internet connection. The measurement and monitoring methods are developed for that kind of delay [5]. The processing time of the servers and WAP gateways also can be characterized by some way [6]. We are focusing on the delay between the WAP gateway and the WAP enabled client terminal device.

Server side round-trip time delay

Measurements of the time delay can be easily realized in the environment where the server and client has some computing capacity and the real-time synchronized reference clock is available. The simplest way is generating the request and the sending time of the request can be stored in the message. On the server side the receiving time is recorded and after processing the given request the starting time of the response has to be included into the content. On the client side the receiving time of the response available, so the delay of the request, processing time of the server and the delay of response can be evaluated.

In the kind of environment where the server side programming is not available or the exact synchronizing of the clocks can not be sure only the staring time of the request and receiving time of the response is available. The difference of these two delays is called round-trip time delay. So it contains the two way propagation time in the network and a processing time of the server. In a lot of practical cases we can assume that the processing time is negligible compare to the propagation time, and we can assume that the transmitting medium is reciprocal, so the propagation time does not depend on the direction of the transmission. Using the introduced approximation the one way propagation delay is the half of the measured round-trip delay time.

Let us see the case of WAP environment where a client is a WAP enabled mobile phone and a server is the WAP gateway of the service provider. In that kind of environment we can find some limitation for establishing a delay measurements procedure.

First, the client terminal equipment has limited computing capacity. It means that we are not able to program the cell in phone as can be done with a PC class client.

Second, the local real-time clock is present in the mobile device, but not available due to the limited programming possibilities provided the WAE. The

structure of the WAE layer of the WAP stack contains the Wireless Telephone Application Interface (WTAI) which can provide access to the built in real-time clock, but this features is not implemented in the currently available devices, or the implementation limited very much.

Third, the resolution of the real-time clock is not enough precise to make such kind of delay time measurements, and the clock of the client terminal is not synchronized to the clock running in the server environment.

To overcome the mentioned problems we introduce the server side round-trip time delay measurement method. This procedure based on a CGI based program, which send a special dynamically generated content to the client. The content sending to the client contains a command to generate a new request to the server using the WAE timer function. The response to this request again sends the content with a new request, and so on. The content generator CGI program at the server-side logs the start time of the content sending response and the arrival time of a new request. In this way the difference of the two logged time stamp is the server side round-trip time delay which contains the two way propagation delay and a processing time of a client terminal. Using the assumptions that the processing time is significantly smaller than a propagation delay in the network the result is the delay time of the whole network on the path of the request and the response.

Our measurement procedure can be started by sending a request from the client terminal to the server for a special measurement content. The procedure does not use the server initialized push method of the WSP protocol to initiate a response from the client. Using this method the measurement can be automatically generated by service providers at the server-side independently from client, and that way the continues monitoring of the delay parameter can be achieved which is necessary for a QoS management framework.

The developed measurement procedure has another assumption. We are not able to place the dynamic content generator CGI program directly onto the WAP gateway/server of the service providers. Instead of this the content is placed on the server of our laboratory. So the measured delay contains the two-way delay between the WAP gateway of the service provider and our content server. This delay is significantly less than a delay of a GSM network from the client terminal to gateway due to a high-speed Internet connection. On the other hand the error factor can be calibrated using the delay, measurements between the server of the service providers and our content server.

Equation (1) show the measured time delay using the introduced procedure and assumptions.

$$TD_{Measured} = 2 \cdot TD_{Gateway\text{-}Server} + 2 \cdot TD_{Client\text{-}Gateway} + TD_{Client\ processing}. \quad (1)$$

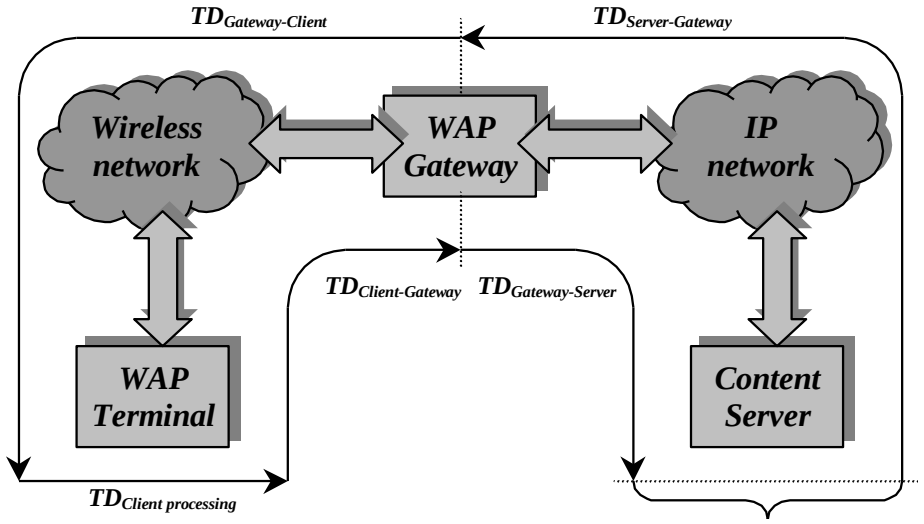


Figure 2: Round-Trip Time and its components

Measurements Results

The above introduced measurement procedure was implemented using a C language program called trough CGI to generate the dynamic WML content again and logging the start and arrival time. The source code (A Appendix) and the generated WML page (B Appendix) can be found in the appendix.

Measurements were done in the GSM network of three different Hungarian service providers with different types of WAP enabled mobile phones as a client terminal. The measured server-side round-trip time delays are the followings. Each figure contains the possibility density function of the measured time delay as a random variable. The derived characteristics like minimum, maximum, expected value and variance are also determined.

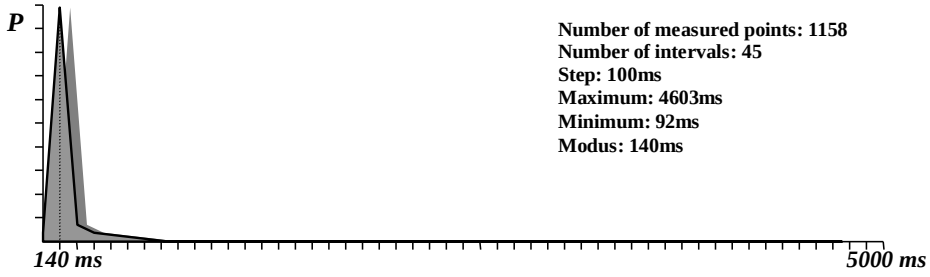


Figure 3: A simple HTTP connection

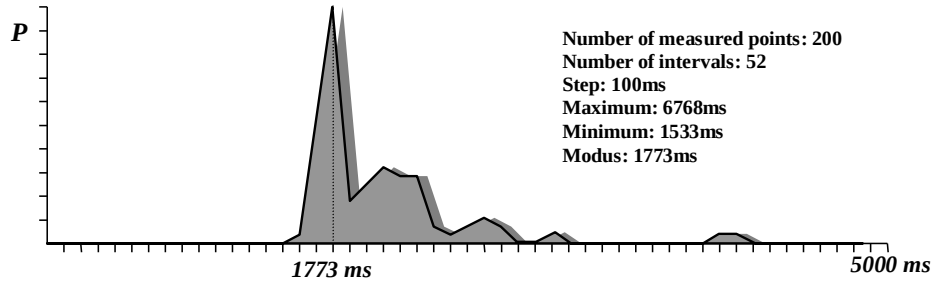


Figure 4: WAP connection with Motorola-Timeport mobile phone in Westel network

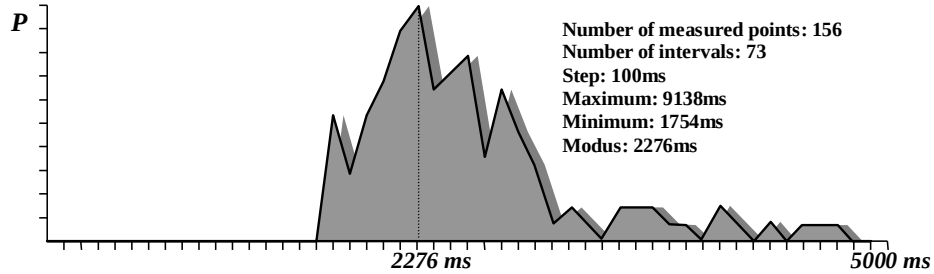


Figure 5: WAP connection with Siemens C35i mobile phone in Pannon GSM network

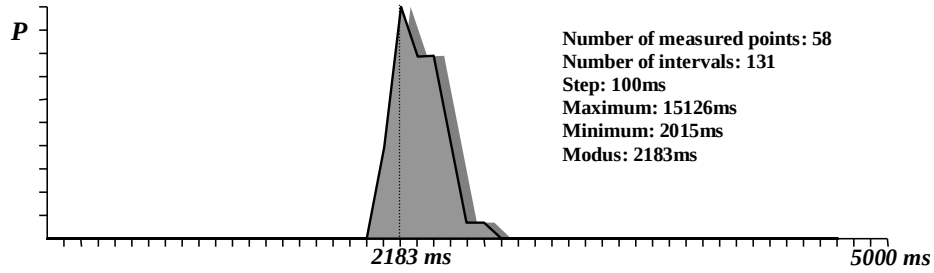


Figure 6: WAP connection with Siemens C35i mobile phone in Vodafone network

Conclusions

The introduced measurements procedure can be used for measurement of the round-trip time delay between the WAP content server and WAP enabled

wireless client terminal. The method solves the problem of the low computing capacity of the terminal and introduces a new way for the measurements and monitoring in a real wireless networking environment.

The proposed method was implemented and measurement results of the Hungarian GSM service providers' network are presented. This clearly shows the usability of the described new measurement procedure.

References

[1] "The Wireless Application Protocol Specification, Version 1.2", WAP Forum, November 1998

[2] "The International Telecommunication Union (ITU) Recommendation E.800, Terms and Definition Related to Quality of Service and Network Performance", ITU, August 1994

[3] "ETSI Technical Report ETR 003, Network Aspects (NA); General aspects of Quality of Service (QoS) and Network Performance (NP), Second edition", ETSI, October 1994

[4] "The International Telecommunication Union (ITU) Recommendation X.641, Information technology – Quality of Service Framework", ITU, December 1997

[5] John Heidemann, Katia Obraczka, Joe Touch, "Modeling the Performance of HTTP Over Several Transport Protocols", IEEE/ACM Transactions on Networking, Vol. 5. No. 5, October 1997, p.616–630

[6] "The SPECWeb99 Benchmark", Standard Performance Evaluation Corporation, November 1999

A Appendix

The source code (`rtt.c`) of the server-side CGI program used for the measurements is the following.

```
#include <sys/timeb.h>
#include <stdio.h>
#include <stdlib.h>

int main(int argc, char *argv[])
{
    struct timeb actTS;
    char *lastTS;
    FILE *out;

    ftime(&actTS);
```

```
    printf("Content-type: text/vnd.wap.wml\n\n");
    printf("<?xml version=\"1.0\"?>\n");
    printf("<!DOCTYPE wml PUBLIC \"-//WAPFORUM/DTD
WML 1.1//EN\" "

"\"http://www.wapforum.org/DTD/wml_1.1.xml\">\n");
    printf("<wml>\n");
    printf("<card id=\"rtt\" ontimer="
           "\"http://wit.mht.bme.hu/~egedif/cgi-
cin/rtt.cgi?%ld%03.3ld\">\n",
           actTS.time, actTS.millitm);
    printf("<timer value=\"1\"/>\n");
    printf("<p>%ld</p>\n", actTS.time);
    printf("</card>\n");
    printf("</wml>\n");

    lastTS = getenv("QUERY_STRING");
    out = fopen("rtt.txt", "at");
    fprintf(out, "%s %ld%03.3ld\n", lasTS,
actTS.time, actTS.millitm);
    fclose(out);

    return(0);
}
```

B Appendix

The WML page (`rtt.wml`) resulted the running of the above introduced CGI program is the following.

```
<?xml version="1.0"?>

<!DOCTYPE wml PUBLIC "-//WAPFORUM/DTD WML 1.1//EN"

"http://www.wapforum.org/DTD/wml_1.1.xml">
<wml>
  <card id="rtt"
        ontimer="http://wit.mht.bme.hu/~fegedi/cgi-
bin/rtt.cgi?957965409503">
    <timer value="1"/>
    <p>957965409503</p>
  </card>
</wml>
```

Károly KASSAI

AREAS AND ACTIVITIES FOR THE INFORMATION (AND INFORMATION SYSTEM) SECURITY

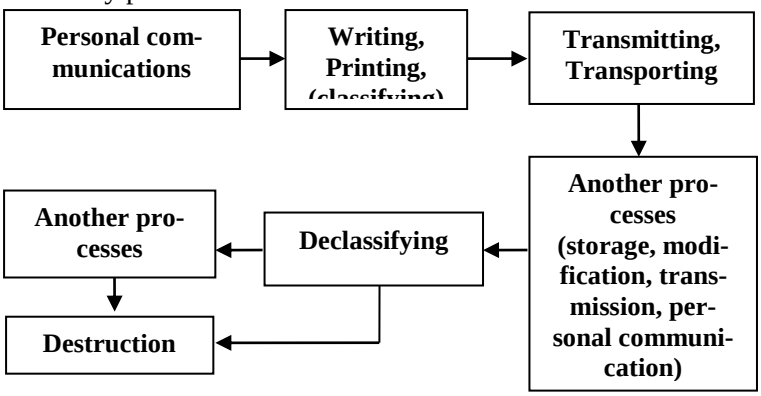
Nowadays several information sources say about the importance of information. However the coin has two sides so sometimes one data has value for the owner and their adversary too.

There are some sensitive areas in the states' defense (e.g. critical infrastructures, military communication and information system; CIS) where is very important the information assurance (IA) and the protection of information.

The specialists and the organizations have different approaches about the information security. The sources of this various view are the condition of the economic, the level of the technology, the condition of the research and develop and the commercial connections and so on. Each state, organization or person builds own information security model that depend on the environment and the possibilities so very difficult to give a general solution for the protection of sensitive or classified information.

First of all we have to understand the complexity of the 'information'. The NATO AAP-31 describes the meaning of this word as 'the intelligence or knowledge capable of being represented in forms suitable for communication, storage or processing' and the third note of this definition: 'Information may exist in the human mind, in document form and in electronic form'.

The organizations have to operate comprehensive systems for the transmission and process the information include networks, equipments, special organizations, support and operational capabilities and certainly policy, procedures, rules. When the knowledge transforms into data and after maybe the data is transforms into another form data there are some processes around this information and every process has own vulnerabilities.



The information lifecycle (one possibility)

We can see (without special knowledge) several possibilities to threat the information/data or information system (physical attack, eyes dropping, sabotage, espionage, steal, hacker or cracker attack, traffic analysis, crypto analysis, deception, unauthorized modification, denial of an authorized use access, destruction of system or data, flood, earthquake, lighting, power cut etc.) thought this model. These threats appear in different local and time, alone or in-group so the protection is a difficult task.

There are some security areas against these threats where different technologies and methods help to support the IA and protect the information and the information system (IS).

1) The physical-, personal-, procedural- and documental security elements are responsible for the basic protection of information (every form information). Each security area includes a lot of protection measures, methods and means and the security management has to organize these elements precisely.
2) Because of the specialty of electronic form information there are six special security fields: Cryptographic Security (CRYPTOSEC), Emission Security (EMSEC), Transmission Security (TRANSEC), and hardware-, software-, firmware security. The NATO and another sources share this six fields between the Communications Security (COMSEC) and Computer Security (COMPUSEC) areas but I think this separation maybe not necessary in the future because of the convergence of the telecommunication, media, computer technology and another fields.
3) In some cases (e.g. military CIS) the security not only the system owner's responsibility so the law enforcement and some governmental authorizations and organizations work for this tasks (e. g. Counterintelligence, Intelligence, Security Authorization, Communication Security Authorization).

If the MoD wants achieve the complex security in the information field it has to use all of sources of this areas as 'three protection rings' around the information and IS. When one of these security areas absences *the effectiveness of the protection will injure* and grow the potential risk of the loss of security level.

However not only this is the main problem in the real life. The protection isn't a statically state but the *result of more coordinated activities.* The successful information security requires different offensive and defensive steps and the result of the protection is a fragile period without *harmony*. Here are some interesting activities what can show the complexity of the protection.

Analysis

The aim of the analysis are the environment, the characteristics of the applied IS, the protection methods, and the occurred security accidents.

The environment and the potential threats

Each system has one or more point of contact where it can communicate with another systems or touches them or changes material, gets energy e. t. c. During these processes the adversaries have some possibilities to attack the IS and modify, destroy the information or denial the authorized access.

If appropriate capabilities scan the environment and they can indicate the changes or threats the protection is easier, faster and more effective.

The characteristics and vulnerabilities of the applied IS and the control

The communication protocols, the transformation between the protocols, the different interfaces, the operation systems, the maintenance and upgrade processes, the responsibility of users and supervisors, the security rules, and several parts of the IS include some holes and problems where not too difficult to attack the IS or catch some information that can help to another attack (maybe in another place or time).

The control of the IS may occurs *outside* or *inside* of the IS. The first method has simply logic: if the adversaries can try the vulnerability and can exploit it we also can do it for the protection! Therefore the security management has to identify all machines in the network, which can be targeted for potential compromise or intrusion.

> There was a simulation exercise (it was called Eligible Receiver) at the Pentagon, to control the protection ability of the nation's military and civilian infrastructure in 1997. The tester group had to use only COTS material and information available on the Web and *the result of this exercise was Top Secret information.*[3]

The most important inside control the *accreditation process*. Before the operations the appropriate authority has to control every equipments and rules and authorizes the application. If an important element of the IS changes (or after determined time) the commander (or leader) has to ask a new accreditation process and the responsible organization will repeat it.

The commander and the security management always have to *control* the IS security during the IS lifetime. Thus if an operation rule is not correct or there is a problem about a user's knowledge or habit or the ordered control finds another problem, the security management immediately can start the correction.

The potential protection methods

New equipments or methods appear day to day in the information age and they usually change something in the information technology so isn't smart

[3] Assessing the threat, point 24. [2.]

opinion to build only one protection method in the IS field or to use a system without upgrade and permanently control.

The occurred secity accidents

The adversaries sometimes can access the sensitive or classified information or data through the vulnerabilities (e.g. system or means fault, objective or subjective personal cause, not effective protection method). This problem signs that something wasn't correct about the security system or a new effective information attack method appeared or the organization had an unreliable person inside the IS.

The analysis of security accident the most important responsibility for the owner of the IS because maybe this accident *will repeat in the future*. The owners of the IS sometimes have to repeat these analysis activities automatically or when something changes in the environment (or when a dangers security event is occurred).

Reduction of the risk (the protection)

When the organizations build or purchase our IS during the planning phases and later have to fight against a lot of dangers but there are some limits what border the protection (e.g. time, resources, circumstances). So the planners have to choose the threats that real dangers and have to build a *cost-effective protection system* against these problems regard of the result of the analysis.

Built-in security

The security measures and tools have to build into the system or processes both in traditional case (e. g. courier or documentation service) and computer network (built in security method). Therefore when a user works he/she automatically does the necessary protection process and doesn't spend more time because of the security.

Monitoring

There are several type communication systems with different protection levels. The users have to understand exactly what is the different among the protection levels and what is the appropriate security method in their job. The security management has to control the users' *official communication activities* and if the monitoring activity signs problem the management have to start the needed protection steps and call the negligent user to account immediately.

Education

The modern communication system and the protection are comprehensive and every system has some specialty so before the job everybody has to learn the application rule (together the security rules). The appropriate separated education system protects the system and the other users from the dangers personal fail and security problem so needn't leave out that.

Training

The IS's are sometimes updated so we mustn't think about our condition of the IS as an Egyptian pyramid from the beginning the civilization. The system management has to sign the new conditions and rules for the users in appropriate form *before all of the change*. Maybe this is a short notes or an accurate, short and clear briefing but the management has to organize a 2-3 days training course in difficult case. The good solution depends on the users' knowledge, the difficulties of the system, the measurement of the change and the applied security level.

Detection, reaction and response

When somebody attacks a communication network this activity sometimes leaves behind some trails so with appropriate detection tools the system administrator and the security management can take some additional offensive or defensive protection steps.

Certainly the offensive protection is a very difficult, fast activity and only special teams can achieve this assignment. The detection, reaction and response movements require logical security structure with well-organized tasks and excellent cooperation among the services, users and special computer teams in the networks.

Control the residual risk

Each environment might include some residual risk that can threat the IS because of the cost-effective protect method. Therefore the planners of the IS have to think to the low probability but danger events and they can make effective plans for this case (this is the emergency plan). There are a lot of good solutions but the main emergency plan the *emergency destruction* and the *emergency transport* plan. The commander has to activate this planes when something threats the sensitive or classified information and isn't another way to protect them in that place.

Certainly the users, the crypto custodian and the responsible persons have to understand these plans and sometimes have to training them with the desired cooperation partners (e.g. transport services, security guards) for the effective execution.

Restore, rebuild

The natural and intentional threats can destroy the capabilities of the IS or hinder the required communication so the management has to correct the problem immediately. In case a modern communication system this is an automatic process because the network have some another transmission ways and switches so the network control can change the applied topology.

Sometimes too many parts of the system are destroyed and the system resources not enough to support the communication services so the operation organization has to apply outside sources for the system rebuild. There are

some kinds of the fast rebuild capability as reserve elements and crew, or centralized organizations for the IA. The management sometimes needed install another form communication method (e.g. courier or transport service, another electronic form) among the most important elements of the military mission.

Conclusion

The organizations' tasks, the environment, the actual security policy and measures surround the new IS but this is a permanently updated process not a stabile state.

The security organization structure depends on the needed security activities. First we have to build a *local security structure* in every place and unit with required security positions.

Beside the local security system there is a responsible *system security management* and this organization has to achieve the security policy *inside the traditional or electronic system*.

Although we can't arrange every work in local or system level so finally the HDF has to build a *centralized security management*. This main management responsible for the up-dated security policy, the outside contacts and the cooperation, and the control of the information security system include the appropriate centralized response, rebuilding and control capabilities.

References

1. Information Systems Security Monitoring, AR 380-53, Washington DC 1998
2. Information Systems Security, AR 380-19, Washington, DC1998
3. Information Warfare and International Security, NATO Science and Technology Committee, 1999
4. Know your enemy, www.infowar.org
5. NATO glossary of communication and information systems terms and definitions, AAP-31, 1998

Attila BOZSIK, Márton PROSZ, László ZÖMBIK

ANALYSIS OF SSL/TLS TRAFFIC BEHAVIOUR

Attila Bozsik* <bozsik@ttt-atm.ttt.bme.hu>
Márton Pósz* <posz@ttt-atm.ttt.bme.hu>
László Zömbik# <laszlo.zombik@eth.ericsson.se

* Department of Telecommunications and Telematics, BUTE
\# Ericsson Hungary, ResearchLab

Abstract

SSL/TLS are employed for securing web servers, mail services and other security sensitive application protocols. Most system administrators know the benefits of these protocols, although only some of them are aware of the additional load and delay caused by the use of such a protocol. The SSL/TLS overhead highly depends on services, configuration and applications used during the communication. In this paper, we analysed a specific web-mail system concentrating on the overhead of network traffic, and the delay between the SSL/TLS handshake messages.

1 Introduction

As the number of security incidents in computer networks has been increasing, the demand for protocols providing secure communication has been increasing as well. It is necessary to know what is the cost of secure communication, therefore thorough analysis of security protocols must be performed. This analysis of the SSL and TLS protocols mainly focuses on the overhead of network traffic, and the delay caused by using such security protocols.

This paper is organised as follows. Section 2 gives a brief description of application layer protocols, their possible security improvements, and the place of security protocols in the TCP/IP protocol stack. Section 3 details the structure of the TLS protocol and explains the communication of a client and a server. Specification of security methods used during communication will also be discussed in this section. Section 4 covers the method of our analysis, while in Section 5 results are introduced, focusing on the overhead in network traffic both in size and in time. Finally, Section 6 summarises the analysis of the SSL/TLS protocols.

2 Background

The Hypertext Transfer Protocol (HTTP), used for sending diverse data across the Internet, is the most popular protocol of the World Wide Web since 1990. The HTTP sends every data in unencrypted form, such communication can be easily compromised.

Two different possibilities appeared for securing insecure protocols:

1. Redesign the whole protocol so that it includes new encryption algorithms - thus making a totally new protocol,
2. Create a standard interface - called wrapper - that handles all the security for the protocol.

There are examples for both: the Telnet protocol was redesigned to include security functions and it is called SSH (Secure Shell); on the other hand POP3, IMAP and HTTP [17] use the SSL (Secure Socket Layer)[15] or the TLS (Transport Layer Security)[16] protocols to secure communication.

The HTTP protocol combined with SSL or TLS is called the HTTPS protocol, where the "S" obviously stands for "Secure". The HTTPS protocol tries to guarantee the following requirements of secure communication.Authentication is achieved by digital certificates and asymmetric encryption algorithms, while confidentiality is achieved by the use of symmetric encryption algorithms. Integrity is ensured by using various hash algorithms.

Both the SSL and the TLS are between the transport-layer (TCP) and the application-layer (HTTP) as it is shown on figure 1. There are other security protocols that reside in the application layer, like SSH, or in the network layer, like IPSec.

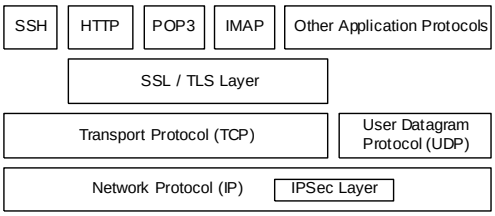


Figure 1 - Protocol stack diagram

Practically use of SSL/TLS is transparent to the user, except in those cases when the user is asked to either accept or decline the certificate offered by the server.

The SSL protocol is only a "de facto" standard, so the IETF released the TLS standard to replace SSL. The initial version of TLS is 3.1, indicating it is the continuation of the SSL 3.0 protocol. The two protocols are almost identical, so we mean both, when referring only to TLS in the rest of this paper.

3 TLS

3.1 Structure

The goal of the TLS protocol is to provide a transparent secure channel between two communicating applications. The protocol consists of two layers: the Handshake Layer and the Record Layer (figure 2).

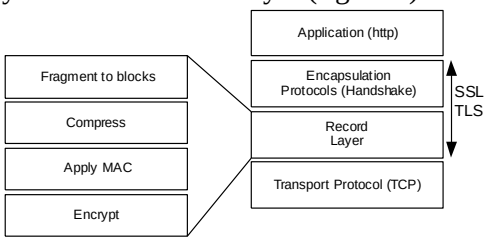


Figure 2 - TLS protocol stucture

The Record Layer provides privacy by the use of symmetric encryption algorithms, and integrity by secure hash methods. It receives messages from the upper layer, fragments the data into smaller blocks, compresses the data (optionally), applies a Message Authentication Code (MAC), encrypts the data and sends the result down to the Transport Layer. When data is received from the Transport Layer, the Record Protocol decrypts it, verifies the MAC, decompresses if it was compressed, reassembles the fragments, then delivers it to the upper layer.

3.2 Handshake

The Handshake Layer ensures three important properties. The first is to authenticate the identity of the server and/or the client by public key algorithms. The next goal is to prevent eavesdroppers from obtaining the shared secret, finally to ensure communicating parties to detect any malicious modification of negotiation.

The Handshake Protocol consists of the following steps. First, the client sends a ClientHello message including protocol version, session ID, ciphersuite list, compression method and a random value.

The server replies with a ServerHello message including the chosen ciphersuite, compression method and another random value. Following the hello messages, the server should authenticate itself by sending a Certificate message. This message usually includes an X.509 digital certificate [10]. In case the server intends to authenticate the client, it transmits a CertificateRequest message. If the server has too few information in its Certificate to generate the shared secret, it also attaches a ServerKeyExchange message. The server indicates the end of its hello-message phase with a ServerHelloDone message.

In the next step, the client answers with its Certificate if a CertificateRequest was received. All the key materials, needed for the generation of a shared secret, are available by then at the client side. It sends a ClientKeyExchange with parameters according to the cryptographic methods selected by the current ciphersuite. If the client sent its Certificate with signing ability, a digitally-signed CertificateVerify message can be attached to explicitly verify the certificate. Next, the client sends a ChangeCipherSpec message, and starts to use the cryptographic parameters. An encrypted Finish message is also forwarded immediately to the server. The client finished its part of the handshake phase and waiting for server response.

The server replies with a ChangeCipherSpec, and starts to apply its cryptographic parameters. It also sends a Finished message encrypted with the new parameters.

After this point, the client and the server can exchange encrypted application data over the secure channel.

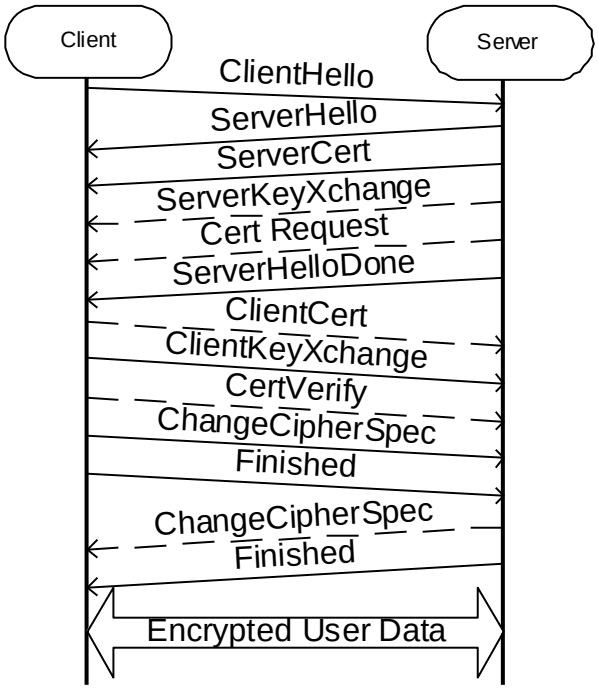


Figure 3. - Message flow of a full handshake

3.3 Ciphersuite

A Cipher Suite is a combination of cryptographic algorithms used to ensure secure communication. The advantage of such combination is that key exchange, hash and cipher algorithms can be replaced independently and simultaneously. The following algorithms are:

- an authentication and key exchange algorithm, such as RSA [7], DSS [3], DH, DHE, etc.
- a bulk encryption algorithm (including secret key length), like RC4 [6], RC2 [5], DES [2], 3DES [1], DES40
- a MAC algorithm, e.g., SHA-1 [8] and MD5 [4]

The most common ciphersuite in our research was TLS_RSA_WITH_RC4_128_SHA. This ciphersuite includes RSA key exchange algorithm, the RC4 conventional stream cipher with key length of 128 bits, and MD5 secure hash algorithm.

During handshake phase, client sends its list of supported ciphersuites to the server. This list is sorted in in the order of preference of the client. Next, the server answers with the chosen ciphersuite back to the client. Later, keys are exchanged according to the key exchange algorithm in the ciphersuite, and the selected ciphersuite is used after the ChangeCipherSpec message.

4 Analysis

We were looking for answers to show the characteristics of network communication using security features. In order to find answers, live network traffic was needed. After introducing the environment of our analysis, the empirical average behaviour and the dispersion is presented.

4.1 Environment

Network traffic for our analysis was collected from the local network of a secondary grammar school and stored on the central server for further inspection. This server provides a web based mail service that can be accessed via a 10Mbit/s local UTP network. Half the number of connections is originated from the local network, so delay was smaller than in the case of clients connecting through the Internet. The server was running Apache v1.3.23 compiled with OpenSSL 0.9.6c library. The local client computers were Celeron-400Mhz boxes. The topology of the network is shown on figure 4.

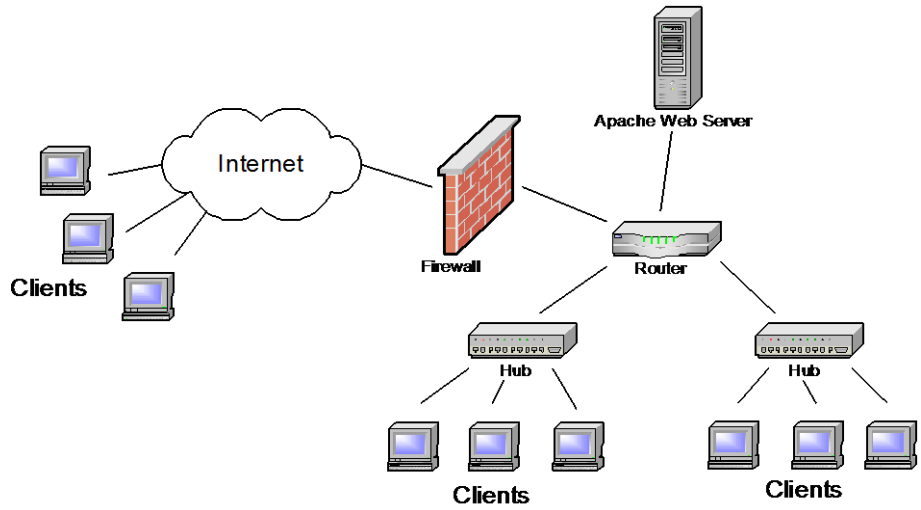


Figure 4 - Network topology

The certificate of the Apache webserver is automatically accepted as authentic by local clients. Therefore no dialog box appears requesting the confirmation of the user when accessing the server. Of course, users browsing from outside this local network have to decide whether to accept the offered certificate.

4.2 Measurements

We collected HTTPS traffic using tcpdump [11] on the server for two weeks. This data was further processed in two different ways:

- it was processed by *SSLDump* [13], that extracts messages of the TLS layer from tcpdump traces,
- on the other hand, the RTT (Round Trip Time) characterising each connection, was estimated by the help of *tcptrace* [12].

Determination of the RTT was necessary, due to make our measurements independent of delays caused by the transport layer. It is achieved by subtracting each RTT value from the time of the corresponding packet's timestamp. Data from the SSLDump was processed, converted, and arranged to charts by serveral Perl, Awk [14] and shell-scripts. From these charts we created graphs using Gnuplot [15]. All data processing - except for the estimation of RTT - were exclusively performed in the TLS layer.

5 Results and Explanations

In this section, results of our research are presented. First, the histogram of connection length is introduced. Later, the average size of messages is shown in time. Both subsections explain the observed behaviour and characteristics of connections.

5.1 Histogram of connection length

In this subsection, we examine the histogram of the total number of messages occuring in a connection. First, all defective connections - which did not contain any payload - were filtered out, because it is meaningless to determine the overhead of such connections. Approximately 60 percent of the connections contain 11 messages, as shown on Figure 5. That means short connections are dominating in this environment. The first nine messages are the part of the handshake phase. The following two encrypted messages carry the client requests for a web page and the server response. This behaviour has heavy impact on the overall performance of the HTTPS protocol, which is detailed in subsection 5.2.

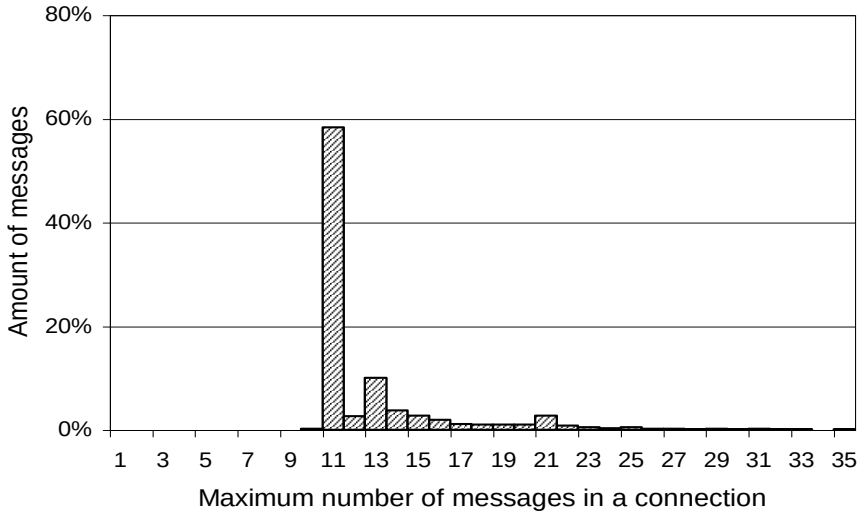


Figure 5. - Histogram of total number of messages in a connection

5.2 Average size of messages

The average behaviour of a connection can be seen on Figure 6. The horizontal axis shows the message sequence number in the connection, the vertical axis shows the average size of the message. It can be clearly seen that the first application data is sent in the tenth message of the connection. This average behaviour was determined from 13,000 samples.

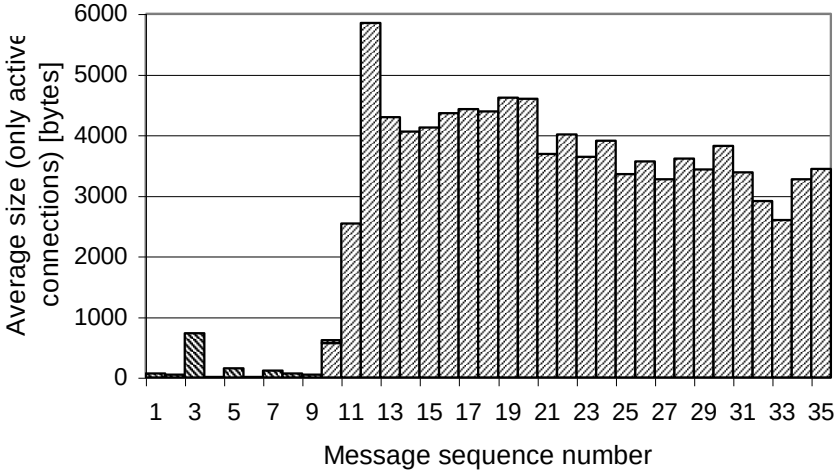


Figure 6. - Average behaviour of a connection decomposed to messages

Usually the third message is the server's Certificate, which is significantly larger than any of the handshake messages. The X.509 digital certificate itself is 714 bytes, which is included in the Certificate message with some additional header.

In the first two or three messages after the handshake phase, the average size of messages carrying encrypted payload gradually increases to a maximal value, then falls back to approximately 4000 bytes. This value is affected by the applied ciphersuite and the direction of transmitted messages. In our analysis, the most common upper limit was 4117 bytes in case the server sends more data to the client using the TLS_RSA_WITH_RC4_128_MD5 ciphersuite. Such connections, representing 40% of the number of total connections, are further inspected on Figure 7. It is seen that the average size of application data hardly depends on time. The first application data is always smaller than the following messages, until it reaches a certain value, e.g. 4117 bytes. In this case, the TLS Record Layer fragments user data to 4096 bytes (Figure 2.), then applies a MAC of 16 bytes (MD5), and encrypts the payload. With the TLS generic header of 5 bytes added, data of 4117 bytes results.

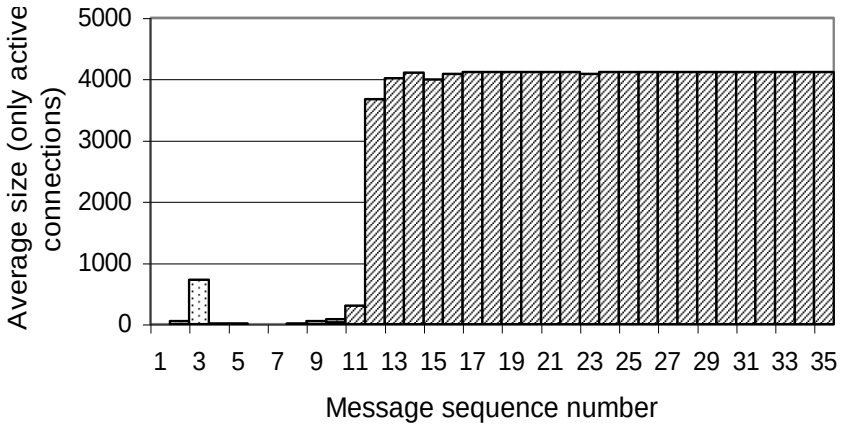


Figure 7. - Average behaviour of common connections decomposed to messages [from server]

Figure 8. shows the characteristic of the average size of incoming messages. When the client intends to send information that cannot fit in one application data message, it sends several application data messages. The first and the last message is usually small, while the inner ones are maximum sized. On Figure 8., the graph reaches its peak of 1874 bytes at the eleventh message, which is the second application data message. The average size of the later messages is significantly reduced by the last (smaller) message of other connections.

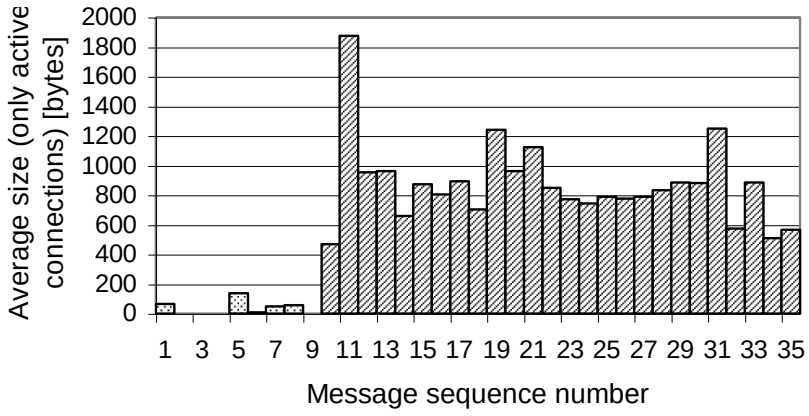


Figure 8. - Average behaviour of a connection decomposed to messages [from clients]

The same characteristic can be observed on Figure 9., showing the average size of outgoing messages. However, the graph reaches its maximum value of 4898 bytes at the twelfth message, because that is the second outgoing application data message. The average size of later messages is smaller for the same reason as in the case of incoming messages.

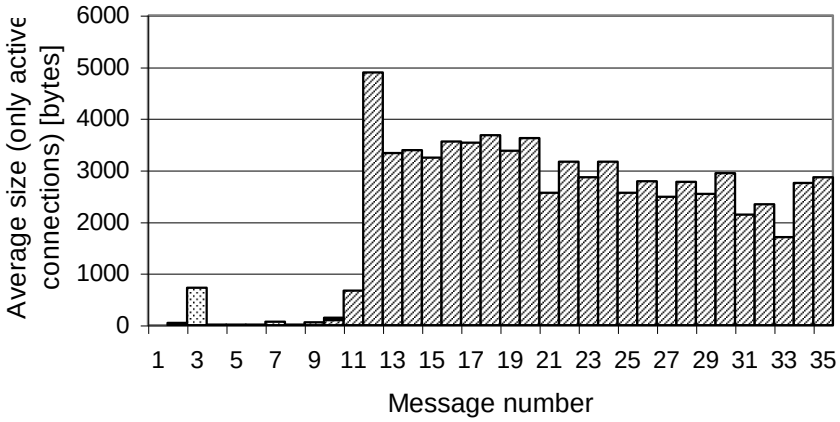


Figure 9. - Average behaviour of a connection decomposed to messages [from server]

The overhead of the security protocol was calculated in the following way. The sum of the size of handshake messages was divided by the sum of the size of all messages. The calculated overall overhead was 13%, it means that such communication needs additional 13% data to ensure security. (Note that this can be dramatically decreased by the use of session key caching [9].)

5.3 Delay of messages

In this subsection we focus on the temporal behaviour of the TLS security protocol. We examined the delay between each message-block. A message-block indicates messages transmitted together in a single packet. Four message-blocks were inspected: the first contains the ServerHello, Certificate, ServerKeyExchange and ServerHelloDone messages; the second includes the ClientKeyExchange, ChangeCipherSpec and Finished messages; the third one consists of the ChangeCipherSpec and Finished messages sent from the server; and the fourth one includes the first incoming Application Data message. In order to make our analysis independent of the network delay, half of the Round Trip Time (RTT) value was subtracted from the original timestamp of each message. Each of the following diagrams shows the average message-block size in milliseconds. Each delay's expected value, maximum place, median and standard deviation are shown in Table 1.

Table 1. - Statistic parameters

Time Delay of	Expected Value [ms]	Maximum Place [ms]	Median [ms]	Standard Deviation D(x)
ServerHello	181.2	1.2	27.9	380.6
ClientKeyExchange	559.1	8.8	51.7	2,257.1
ChangeCipherSpec	189.0	21.6	24.3	385.2
Application Data	6,747.3	2.6	49.8	76,256.1

On figure 10., the time of all messages are represented relative to the time of the ClientHello message. Thus, the time of ClientHello messages in each connection indicate 0 millisecond. The expected value of the average delay of the next message-block (ServerHello, Certificate, ServerKeyExchange and ServerHelloDone) is 181.2 milliseconds.

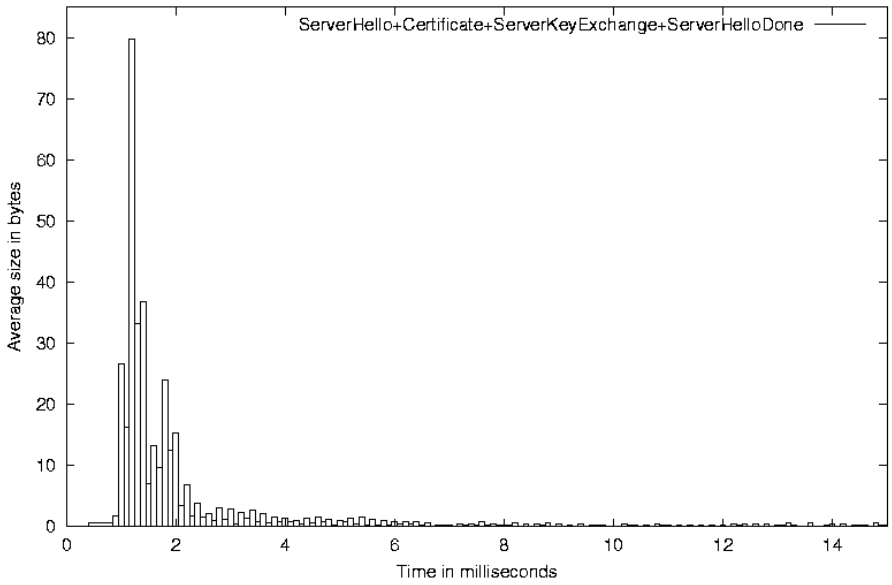


Figure 10. – Average size of the ServerHello message-block in time relative to the ClientHello message

Figure 11. shows the time of the third message-block relative to the ServerHello message-block. The peak of the average size of the ClientKeyExchange message-block is approximately 80 bytes. The expected value of the delay is 559.1 milliseconds, while its median is 51.7 milliseconds.

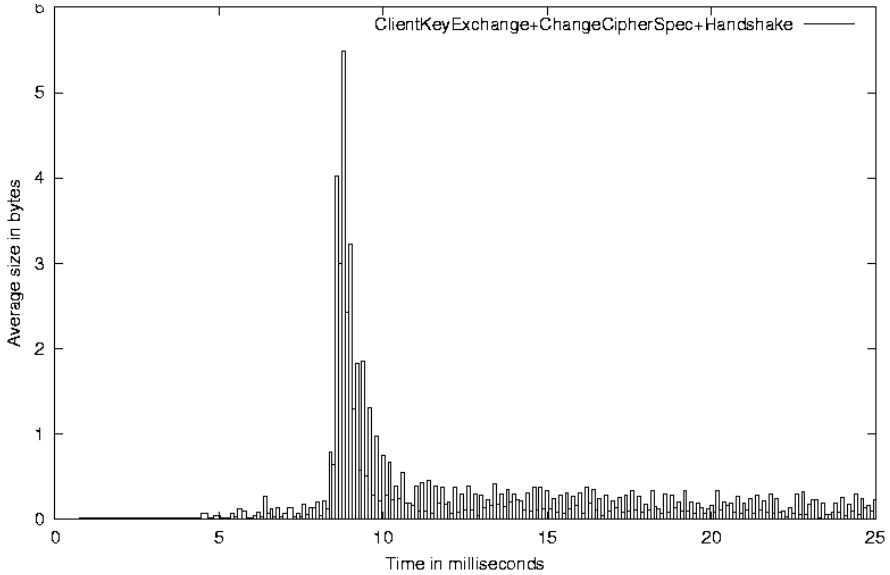


Figure 11. - Average size of the ClientKeyExchange message-block in time relative to the ServerHello message-block

On Figure 12., the delay between the ClientKeyExchange message-block and the ChangeCipherSpec outgoing message-block is represented. The ChangeCipherSpec message-block reached a maximum average size of abour 3.5 bytes. The expected value of its delay is 189 milliseconds, its median is 24.3 milliseconds.

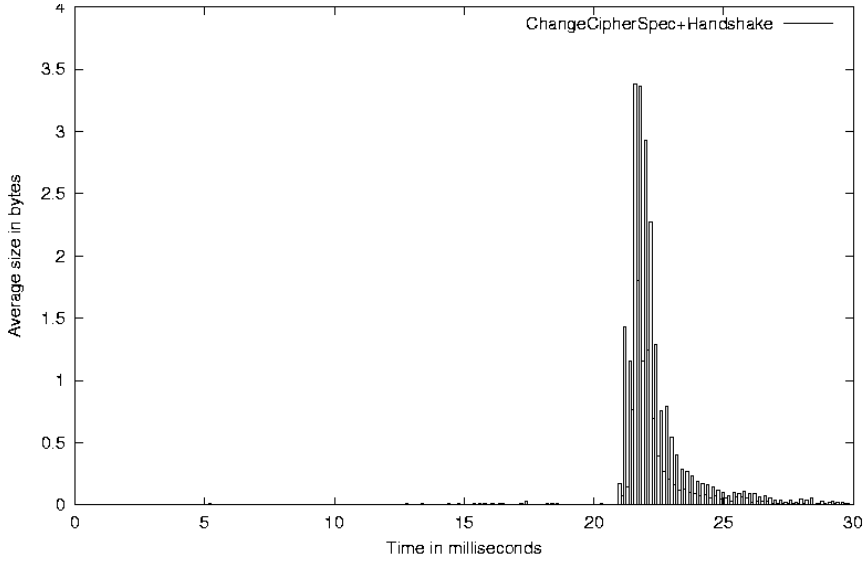


Figure 12. - Average size of the ChangeCipherSpec message-block in time relative to the ClientKeyExchange message-block

The delay between the outgoing ChangeCipherSpec message-block and the first incoming Application Data message can be seen on Figure 13. The maximum value of the graph is at 2.6 milliseconds. The expected value of the delay is 6,747.3 milliseconds, and its median is 49.8 milliseconds.

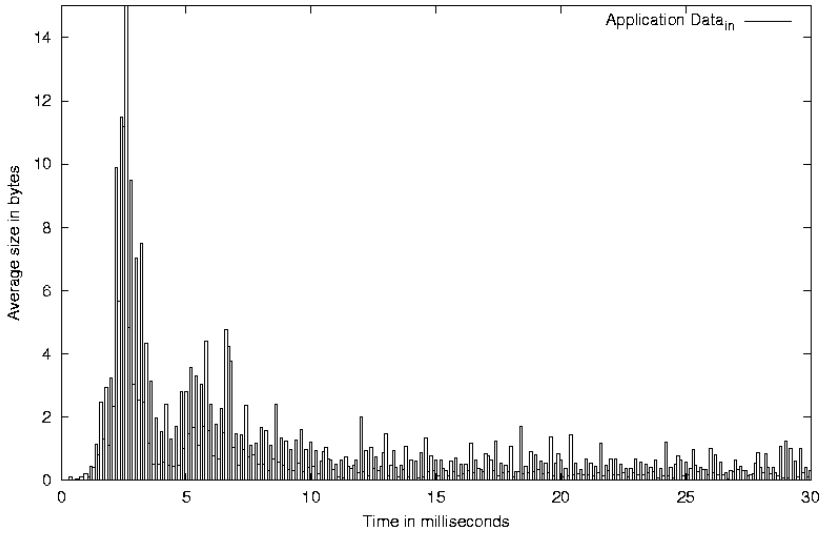


Figure 13. . - Average size of the first incoming Application Data message in time relative to the ChangeCipherSpec message-block

6 Conclusion

We have presented an experimental analysis of the SSL/TLS behaviour focusing on the network traffic overhead and the delay caused by the these protocols. It could be seen that secure communication has approximately 13% more network traffic in case of an ordinary web-mail server environment. On the other hand, the delay of TLS handshake messages was examined. The expected value, the maximum place, the median and the standard deviation of delays were also presented. These observations are useful for network designing, where both security and network resources are important.

References

[1] W. Tuchman, "Hellman Presents No Shortcut Solutions To DES," IEEE Spectrum, v. 16, n. 7, July 1979, pp40-41.

[2] ANSI X3.106, "American National Standard for Information Systems-Data Link Encryption," American National Standards Institute, 1983.

[3] NIST FIPS PUB 186, "Digital Signature Standard," National Institute of Standards and Technology, U.S. Department of Commerce, May 18, 1994.

[4] Rivest, R., "The MD5 Message Digest Algorithm", RFC 1321, April 1992.

[5] Rivest, R., "A Description of the RC2(r) Encryption Algorithm", RFC 2268, January 1998.
[6] Thayer, R. and K. Kaukonen, A Stream Cipher Encryption Algorithm, Work in Progress.
[7] R. Rivest, A. Shamir, and L. M. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, v. 21, n. 2, Feb 1978, pp. 120- 126.
[8] NIST FIPS PUB 180-1, "Secure Hash Standard," National Institute of Standards and Technology, U.S. Department of Commerce, Work in Progress, May 31, 1994.
[9] A. Goldberg, R. Buff, and A. Schmitt. Secure web server performance dramatically improved by caching SSL session keys. In Proceedings of the Workshop on Internet Server Performance, Madison, Wisconsin, June 1998.
[10]CCITT. Recommendation X.509: "The Directory – Authentication Framework". 1988.
[11] Tcpdump software: http://www.tcpdump.org.
[12] TcpTrace software: http://www.tcptrace.com
[13] SSLDump software: http://www.rtfm.com/ssldump
[14] GNU Awk software: http://www.gnu.org/software/gawk/gawk.html
[15] Frier, Karlton, Kocher, “The SSL 3.0 Protocol”, Netscape Corp., 1996. Internet Draft
[16] Dierks, T. and C. Allen, “The TLS Protocol”, RFC 2246, 1999. Proposed Standard
[17] Fielding et Al, “Hypertext Transfer Protocol – HTTP/1.1”, RFC 2616, 1999.

Erik PÁNDI

QUESTIONS ON THE REGULATION OF INFORMATION SYSTEMS USED BY THE HUNGARIAN POLICE

Preamble: In the past couple of years the Ministry of Interior of the Hungarian Republic (MoI) has prioritised the development of its communicational network. The available funds were used to modernise and extend conventional telephony systems, then later information systems. The extension of modern technical solutions and services has made it unavoidable to rethink the directives regarding the use of the system. This short summary of lecture discusses the rethinking of the group of problems arising, and introduces the finer points of the directives created as a result.

I. Developments in systems technology

After a short transitional period, Act LXXII of 1992 – Act on telecommunication – was issued to re-regulate the conditions under which the telecommunications sector could operate. Under this act the previous closed-purpose networks built for reasons peculiar to Central-Eastern-Europe, could longer operate. The conditions of use of these networks were regulated by the later issued governmental decree No. 50/1998.

During the first stage of technical developments due to the issuing of the previously mentioned acts, primarily telephony systems were digitalized. Due to the availability of advanced technologies in telephony and informatics, and the changing international trends in the application of communicational systems (e.g. the convergence of telephony and IT, the wider use of the Internet, rapid changes in data handling and processing methods) the management of the MoI and the police, has decided to continue the further development of informational systems after the reconstruction of the telephony network.

Domestic political notions regarding Hungary's role in the European Union, since it has become more and more inevitable to improve cooperation abilities in order to become up to date with Western-European systems naturally also supported these efforts. It can be said that the all-time government has generally supported the plans of the management of the MoI regarding this topic, for conforming to the international ideas regarding the Information Society, and an electronic government, has been a goal of every government. Examples for this, among others could be the National Information Technology Strategy (1995.), governmental regulation No. 1071/1998., Hungarian reply to the challenges of the Information Society (1999.), governmental regulation No. 1066/1999., governmental regulation No. 1122/2001., etc.

In 1999 the MoI announced its three year programme, which set it's target to increase transmission capabilities and capacity, extend informational sys-

tems through the further development of the Uniform Digital Network of the MoI.

With the completion of the project, it can be said that the capacity of the networks connecting the central police bodies with the regional, and local bodies has increased, the number of police internet and Intranet user terminals has increased, special software were developed and introduced (e.g. Robocop).

In summary, it seems that the developments have been a positive effect on the effectiveness of police work, although the current level of quality and quantity of IT infrastructure is far from optimal. Off course there must be continued development in the future, however during further coordination governmental goals regarding the construction of the Electronic Governmental Main Line Network have to be taken into view.

II. Solutions of control

With the development of information systems group of users in the sector has also expanded. With regard to the level of development of the intranet network the Minister of Interior in 2001 issued the BM** directive No. 36/2001.) controls the safe operation of IP based networks, and the use of the Internet.

II/1. BM directive No. 36/2001.

The directive contains tasks in relation to the application of the Internet by the home affairs sector, it is valid first of all for the Ministry of the Interior, the official units, the organs of the Ministry, the individual agencies of the Ministry of the Interior, furthermore the administrative offices. Basically four chapters and seven chart-annexes were elaborated. It is expressed in the preamble, that the directive itself intends to arrange for the safe operation of the IP-based networks of the Ministry of the Interior; and for the control of the sectoral application of the Internet as a user and supplier of contents.

As the Internet and IP-based networks are considered quite a new technology, application in civil governance, chapter I explains several definitions to be cleared (e.g.: IP, DNS, DHCP, Home page, web, etc.). Points 3-17 of chapter II sum up the commitments and possibilities of the application of the Internet as a user. The next chapter, that is chapter III governs the application of the Internet as an informational medium. The last part details the tasks related to the ensuring of operational, development conditions, which is followed by 7 annexes.

The contents of the directive

As it was already mentioned above, the first part contains details of the explanation of definitions, that are included in the text of the directive as elements of unknown definition.

The remaining three parts divide well the personal and technical rules of the gathering of information and communication of information, furthermore the method of the application and improvement of the required infrastructure.

Part II expresses clearly the theory, which intends to make possible the application of the Internet by all home affairs employees, for the more ambitious execution of their official tasks. The measure of course prefers Internet access ensured by the government, that can be only used exclusively through the network operated by the Ministry of the Interior. Since the prevalence of the communication infrastructure of the Ministry of the Interior is limited in Hungary, so called modem-connections are not impeded, however the permission for this solution is quite strict.

The points stipulated in this chapter basically show the efforts to achieve safety, as those mainly support the application of own infrastructure. The introduction of the record system is an innovation, however it is unfortunate, that the registration of ports (intranet and modem) and the control of overall traffic are the tasks of the competent department of the Ministry.

The third part includes all those conceptions, which tend to ensure the establishment of communication and consulting with the population. It can be considered a modern approach, that home affairs organizations have to appear on the Internet along with the assurance of quality of the contents and appearance. It is also objectionable in this chapter, that the Information-technology Department did not always consider the proper division of tasks; for example it can be hardly presumed, that a ministry organ mainly dealing with "theoretical" questions will be able to undertake the operation of web-systems and servers outside the firewall.

Chapter four clearly covers the tasks related to the provision of conditions for operation and development, however it considers evident that each organ belonging to the named category has the proper information-technology service.

The annexes mainly cover the form of reporting and recording the Internet terminals, exits, division of IP-address ranges; the introduction of which will integrate the existing, various data-bases.

The importance of the directive

All things considered, the rule tends to organize the control of the services that can be provided by a technology, much earlier enforced by the ambience of administration. The substance of the directive is advanced, however there are not many practical indications for the method of co-operation between the communication and information-technology organs, although it is known that some organs of the Ministry of the Interior do not have any proper information-technology subunit.

The directive slightly combines the parts of the strategic decider and the practical executive. In the Hungarian administrative practice it is not common to modify the alteration of the power of a theoretical ministry department towards the executive direction.

Apart from the above exceptions the BM directive No. 36/2001 can be considered a milestone and supplies a deficiency in the improvement of the civil service work of home affairs services, and in the shifting along governmental conceptions.

II/2. ORFK* measure No. 9/2002**

The ORFK measure No. 9/2002 was issued according to the permission given by point 37 of the BM directive No. 36/2001. The order relates to the operation of the homepage of the Police, the provision of access to the Internet, and questions on providing and security issues regarding its use.

Access to the Internet is becoming an everyday part of governmental work, since it enables mutual exchange of information between the public and the police. Data appearing on police homepages, and electronic messages sent by members of the public form the main channels of communication. Beside this it's important to make it possible for the police staff to gain information placed on a number of homepages, and perhaps use electronic mail through the use of the Internet, in order to fulfil their duties more effectively.

Starting out from the aspects mentioned above the creators of the order concentrated on, or in other word regulated these two fields:

the group of people maintaining the homepage, the method of uploading the data onto the homepage, the data- and encryption- standards, and the tasks regarding the operation of the electronic mailbox.

the use of the Internet as a user, the methodology of permitting, recording, and controlling access, and the financial, technical, and security standards.

Off course it is the object of the police management that similarly to the widely used telephony network, in the future, access to the Internet can be provided to a wider range of police staff, however for this it is necessary to reconstruct the currently available PC stock, and to continue further development on LAN and WAN networks.

Looking at one of the points of the directive, it becomes clear that in case of computers connected in a network, data exchange on the Internet is only allowed through gateways protected by firewalls maintained by government. In every other case the ordering party can only get connected to the network through a PC outside the LAN, and also has to bear the service fee of the ISP, and any further costs involved establishing the connection (e.g. cost of software, hardware, and telecommunications).

In summary the directive is harmonious with what is described in directive in BM directive No. 36/2001 However the directive does not limit the number of the size of the group of users able to access the system, neither does it set any conditions on how the police staff may use the electronic mail (rights, types of data allowed to be sent, etc.).

II/3. ORFK measure No. 20/2002

The temporary measure on the regulation of access to different information services provided by the intranet network of the police, has been long awaited both by telecommunications and IT experts. The technical debates concerning the further operation, and maintenance of the system, which keeps expanding as a result of the developments home affairs sector, were settled according to the following points:

- the development of the main line network (WAN), was assigned as the task of the central telecommunications service unit of the police;
- it is the duty of the central informatics (computing) service unit of the police to develop, operate, and maintain the main databases, and applications;
- the central telecommunications coordination unit of the police coordinates the development of the MAN, and LAN networks of the regional bodies, and monitors any connections to the MAN network;
- the central informatics coordination unit of the police develops, maintains, and operates the network software, network applications, and the system handling user rights.
- the integrated telecommunications and informatics provision units of the regional bodies develop and operate their MAN, and the LAN networks.

The directive clarifies and identifies the roles, responsibilities, and rights of the police network administrator, system administrator, system manager, webmaster, and postmaster. It also declares the services available such as: e-mail (internal and external electronic mail) service, www based service, FTP information service.

Furthermore the directive also goes into the details of other restrictions in data transfer (because of the limited set of resources); operation and authorisation to the public information services; the detailed regulations of the web based services; responsibilities involved in uploading the data; the method of dealing with further occurring problems.

In summary the directive corrects some of the previous shortfalls, however it is only a temporary solution, so the finalised regulations on the operation and use of the intranet police network, and the informatics security regulations have to be worked out as soon as possible.

III. Summary

In order to improve the ability to cooperate the standards set by the European Union and NATO, and impacts of the convergence of telecommunica-

tions and informatics require the police to constantly renew and modernise its systems. However currently due to the limited set of resources, unlike with conventional telephony services (e.g. telephone, cell phone, fax, etc.), it is not yet possible to provide access to services provided by these information systems to a wider range of police staff.

However it can be said that the police has reached a level in modernising its systems, when there has become a need for issuing new regulations on application, since the information systems have grown beyond the level of "home use". Off course the finished regulations still contain a number of errors, however it should be clear that their issuing was quite pressing.

If developments keep on going until Hungary's joining the European Union, once again it becomes timely to reconsider the views on the integration of the telecommunications and informatics organisations of the sector, because the ORFK measure No. 20/2002 only partially settles the debates on competence.

*Pándi, Erik: major of Hungarian Police;
Telecommunications Service of Financial General Directorate of the Hungarian Police Headquarters;
Technical and Regulation Department; head of sub-department
**BM: Ministry of Interior
***ORFK: Hungarian Police Headquarters

Ferenc KUBINSZKY[4], Zoltán LÁZÁR[5], Bertalan EGED[6]

IP BASED VOICE AND DATACOMMUNICATIONS ON MOBILE AD HOC NETWORKS

Technical University of Budapest
Depatment of Microwave Telecommunications
Wireless Information Technology Lab[7]

Absrtact

The rapid development of Internet and telecommunication technologies has driven the natural demand to use the IP based networks to carry the human voice and thus replace the traditional telephony. This service is realised by VoIP (Voice over Internet Protocol) technology, which has been developed for real-time voice, video and data communications. Although it is a young technology its rapid development makes it able to be used to satisfy the needs of IP telephony and video communications.

For military communications MANET (Mobile Ad Hoc Network) is a practical solution due to its special features. In battlefield environment troopers can not rely on access to a fixed, pre-deployed infrastructure. Due to this technology if the participating nodes which communicate other nodes are not in radio range or not in the line of sight they use a multi-hop (store-and-forward) packet routing to exchange messages between the users.

Our goal is to demonstrate the behaviour of IP based voice and data-communication systems on mobile ad hoc networks. The main parameters of data and voice communications are investigated like delay and jitter.

VoIP

VoIP technology was developed for telephone and fax calls over an IP based network. The first VoIP application was the Internet Phone what initiated the IP based telephone technology. The ITU-T accepted H.323 [1] recommendation in 1996 October, which deal with the method of internal communications of multimedia systems. However the call-setup process contain high message overhead it takes many time. Considering the modified requirements the ITU accept the second version of H.323. Furthermore the third version of this recommendation try to develop faster method of connection setup, and the packet based delivery of fax data.

[4] ferenc.kubinszky@wit.mht.bme.hu
[5] zoltan.lazar@wit.mht.bme.hu
[6] bertalan.eged@wit.mht.bme.hu
[7] http://wit.mht.bme.hu

Paralel to this H.323 recommendation the IETF MMUSIC (Internet Engineering Task Force – Multiparty Multimedia Session Control) develop the SIP [2] (Session Initiation Protocol) protocol. This protocol is suitable to set up an IP based phone call and supervise it. SIP is text based, very easy to apply this is why it may be a rival of H.323.

VoIP protocols

In the VoIP applications the most important thing is to convert the voice into data and deliver the data to the remote host as fast as possible. For this purpose the analog voice is transformed to digital signal and encoded. In the remote host the opposite operations must be used to decode the voice. The most important technology challenge that the encoding and decoding process and the transfer of the packages must be fast enough to avoid disturbing time delay during the conversation. The well-known call processing protocols like H.323 (ITU), SIP (IETF) take apart in the call-setup and call supervision process. The voice packages are delivered by a standard multimedia transport protocol like Real Time Transport Protocol (RTP) [3].

Quality of Service

Because the human voice is very sensitive for time delay and time delay jitter Quality of Service is very important goal. There are many methods against the disadvantages of IP network like time-delay, jitter, package congestion, package loss and the reorder of the packages.

- Queing delay jitter: during package transfer a package can wait in the routers' queue various time depending on network load and speed of network components. The queuing delay time can change on a big scale.
- End-to-end delay: due to the network load rapid changing the transmission can suffer a delay jitter too. This is why the time between two packages can change on a relatively wide scale. Because of a package which delay is large enough the decoding procedure can be interrupted. To avoid this effect we usually use a dejitter buffer. Whit this method the respectable delay can increased significantly. The function of this kind of buffer is to eliminate the rapid changing of the end-to-end delay by transmit the packages within equal time interval.
- Package loss: when a package is loss, the receiver side can't decode this time interval. This gap can be eliminated by using redundant encoding and extrapolation decoding algorithm. The speech quality can dramatically decreased as the packet loss increase.

Mobile ad hoc networks

A mobile ad hoc network (MANET) [4] is a network of mobile computers, hand-held devices like mobile phones, and PDAs typically using their wireless interface, and forming the network without any pre-built infrastructure such as routers or base stations. This type of networks can be used for example on conferences, meetings where participants form their small networks or at some

areas where no pre-built infrastructure exists or has been damaged. A MANET can be a reasonable form of voice and data communication network for military use, for example for a small group of troopers. They can talk to each other, download data files from the headquarters or send back pictures or video frames.

As there are more and more powerful mobile computers and there are big performance improvements in wireless communications technologies, advanced wireless mobile computing is expected to be used increasingly widespread, and will involve the use of the Internet Protocol (IP). The vision of mobile ad hoc networking is to support robust and efficient operation in mobile wireless networks by incorporating routing functionality into mobile nodes. These networks can have dynamic, sometimes rapidly-changing topologies and they support multi-hop routes and have to use relatively narrow-bandwidth wireless links.

Attributes of mobile ad hoc networks

Mobile ad hoc networks have certain differences from wire-line networks. Some of these differences are listed below:

- Dynamic topology
- Limited capacity of the mobile nodes
- Limited bandwidth of the links
- Vulnerability by disturbances
- Security issues

Dynamic topology means that the nodes of the network can move, so the routes are not static at all in mobile ad hoc networks. Since the nodes can move quite rapidly the calculated routes are valid only for a short time period. The average movement speed of the nodes or mobility might be an important parameter of the network. The limited capacity of the nodes is caused by the nodes usually being mobile computers like mobile phones and PDAs with less powerful CPU, limited memory size and limited battery power. Hence the administrative (routing, path maintenance, etc.) usage of their resources should be kept low. The bandwidth of the links is limited because the cost of RF bandwidth is relatively high, and there are a lot of restrictions using them. So the usage of the links should be as low as possible. Vulnerability by disturbances is caused by the wireless links. A wireless link is of course more vulnerable by static noises than a wired one, and there are different types of errors (bursts, etc.).Some security issues on wireless links are different compared to security issues on wired links. Digital security and privacy keys are needed for these applications.

IP telephony over ad hoc networks

Due to the attributes of ad hoc networks and the requirements of voice over IP technology a lot of important issues has to be solved. In an ad hoc network satisfying QoS requirements is much more complicated than in wired

networks. In a mobile ad hoc network guaranteeing bandwidth and delay bound for the whole length of a session is almost impossible, because the network topology can change rapidly. Routes can be easily overloaded by earlier admitted flows just because the network topology has changed. When a path breaks it should be repaired locally or a new route has to be established between the two endpoints. Finding a new path always takes some time for ad hoc routing protocols. The more serious problem is that these protocols use broadcast floods to discover the requested destination, and this packet flood can overload temporarily the whole network. The network can be partitioned by the failure of a node or a link, so the communication between two nodes may fail permanently.

In spite of the difficulties mentioned above mobile ad hoc networks can serve as a bearer of VoIP applications with some restrictions like low mobility of the nodes, limitation of best effort traffic etc.

Routing in MANETs

There are two main groups of routing protocols in the mobile area, the pro-active and reactive. Pro-active means that the routing protocol constantly tries to keep track the route changes in the variable network topology. The traditional distance vector and link state algorithms are known as pro-active. Reactive protocol only tries to find a route when it is needed. These protocols (eg. AODV [5], DSR [6]) also known as on-demand protocols.

Simulating mobile ad hoc networks

Simulation results have been carried out in Berkeley Network Simulator 2 (ns2) [7] environment.

Ns2 is a powerful tool for examining a wide variety of network protocols including TCP, UDP and routing protocols. Ns2 has got the capability to examine both wired and wireless networks such satellite links and ad-hoc mobile networks.

802.11 MAC characteristics

In this section IEEE 802.11 [8] MAC layer characteristics have been investigated. The most important attributes for VoIP and datacommunication systems are delay and the throughput capacity of the whole network.

The simulated scenario is shown in figure 1. In this case the MAC characteristics has been simulated so a single hop network has been used, all nodes reside in radio range, sharing a common channel. One VoIP flow has been started between node 1 and node 0, increasing number (1,2,5,20) of nodes generate background traffic to the common channel. The VoIP flow is modelled by a constant bitrate (CBR) flow (40bytes/30ms), so its bandwidth is negligible compared to the background load. The background traffic is also modelled by increasing CBR flows. The results of MAC characteristics simulation are shown in figure 2.

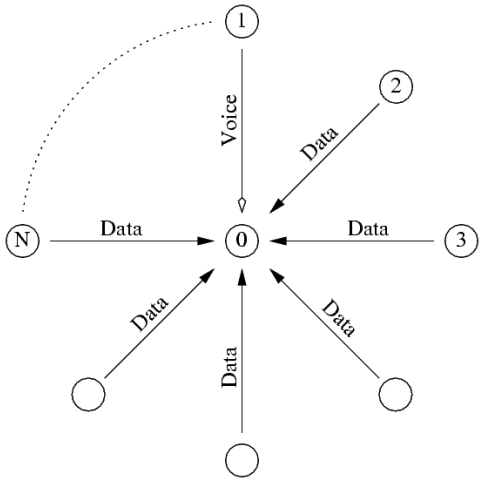


Figure 1.: Simulation scenario

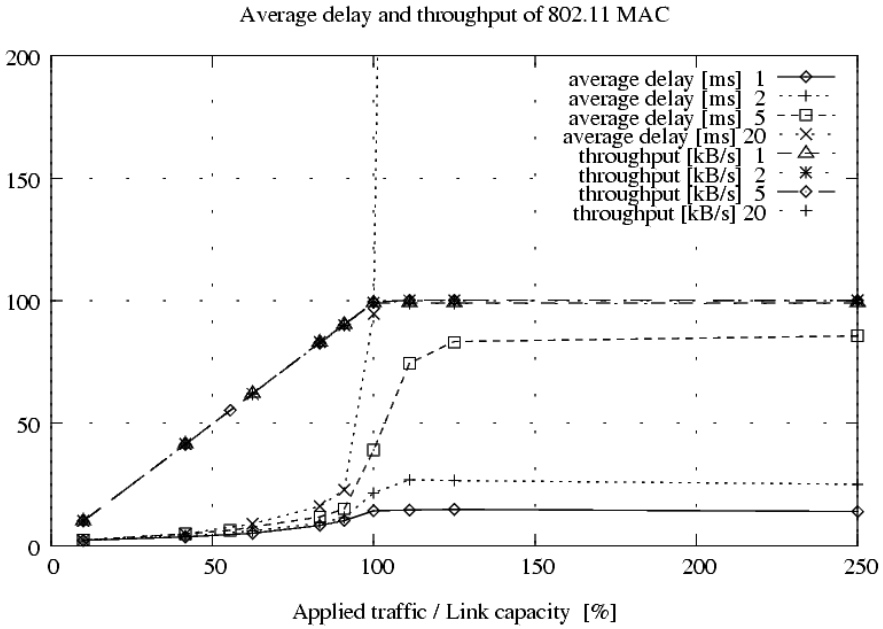


Figure 2.

Network throughput is almost independent from the number of data sources, at least on moderate load. Applying traffic less than the maximum capacity of the network the throughput increases linearly, equal to the applied traffic. The throughput saturates at maximum network capacity and remains at the same level in spite of overloading the channel.

The delay measured on the VoIP flow increases exponentially by increasing load. The delay remains at acceptable level until offered load reaches approximately 90% of the link capacity. Above this point delay increases significantly so the flow suffers unacceptable high time delay. It is also observable that the number of nodes has significant impact on delay variation. Delay saturates also on different level depending on number of nodes trying to send data to the channel at the same time. There are two possibilities to keep delay at an acceptable level. First control the traffic load and keep it down approximately at 90%. The delay increases exponentially, so it is very sensitive against temporal load changes. If load increases only one percent, delay can change on a large scale at this working point. The other possible solution is to limit the number of contenting nodes. Let us suppose that the aggregated VoIP bandwidth is not significant compared to the total bandwidth. The average delay can be limited to an acceptable level by only restricting the number of nodes transmitting traffic best-effort packets such as FTP or HTTP flows.

Voice over IP on a multihop network

We will demonstrate operation of VoIP on a multihop ad hoc network. In this simulation 25 nodes were moving in an 800x800 metres area at maximum speed of 4 m/s. All the nodes have 250 metres radio range. These parameters provided moderate length (max. 4 hops) of routes between the two communicating nodes. AODV (Ad Hoc On-Demand Distance Vector) routing has been used to provide connection over radio range in a multihop manner.

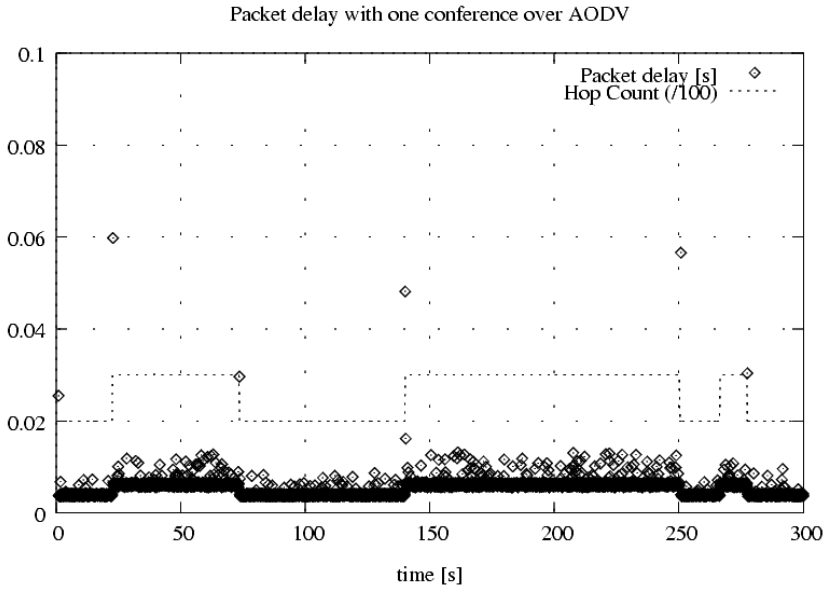


Figure 3.

Figure 3 shows the results of delay analysis in the network where only one duplex VoIP flow has been applied. Dotted line shows the number of hops in the path of the packets. Points represented by diamonds show the packet transmission delay between the two endpoints. It is clear that there is a strict relation between the number of hops and the time delay of the majority of the packets. The changing of the hop count shows that there was a link failure in the path between the communicating peers, a new route requested to continue communication. The route establishment procedure take some time for the routing protocol, during this procedure delay time increases, so the data packets suffer additional delay. In a relatively small network this delay still remains at an acceptable level.

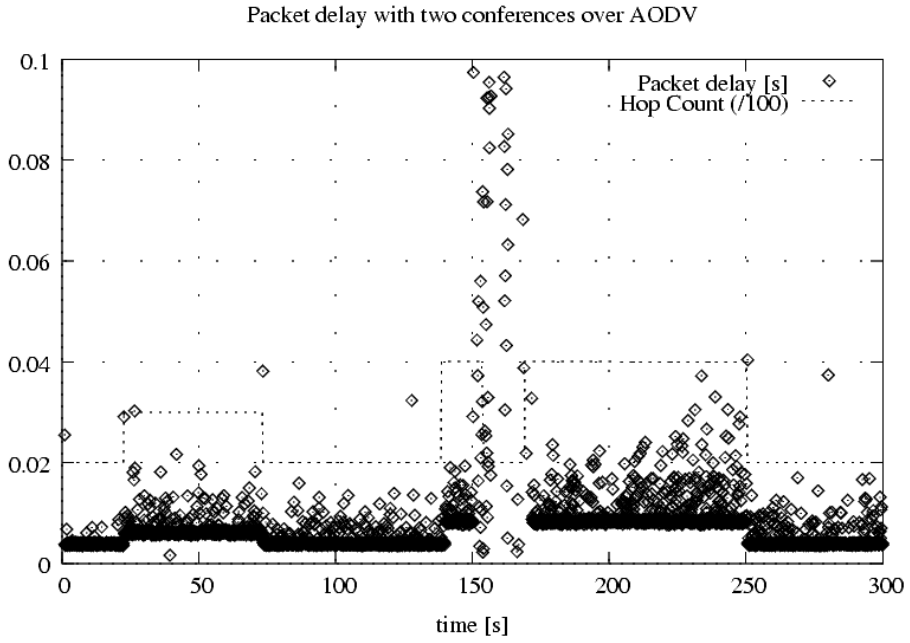


Figure 4.

In the last simulation the effect of a short data burst has been shown. All the parameters were the same as in the previous simulation, except there were two nodes loading the channel with a short packet burst at 150 sec. It is observable, as shown in figure 4, that VoIP packets suffer serious delay in the time period of the burst. Note that this simulation shows a multi-hop network so the end-to-end delay increases more than in the first simulation where only one hop has been examined. It is well shown by the results that there should be some restrictions on the best-effort traffic bandwidth to avoid unacceptable delay variation and voice quality degradation.

Conclusions

In this article we have demonstrated the behaviour of IP based voice and datacommunication systems on mobile ad hoc networks. The main parameters of data and voice communications were investigated like delay and jitter. As it is shown by the simulation results, mobile ad hoc networks have the capability of carrying voice data. It is also possible to load the network with short and moderated best-effort data burst.

References

[1] H.323 ITU Standard

[2]. M. Handley, H.Schulzrinne, E. Schooler, J. Rosenberg, "SIP: Session Initiation Protocol", RFC 2543, IETF, March 1999

[3] H.Schulzrinne, S. Casner, R. Frederick, V. Jacobson, "RTP: a transport protocol for real-time applications", RFC 1889, IETF, January 1996

[4] Internet Engineering Task Force, MANET working group, http://www.ietf.org

[5] Charles E. Perkins, "Ad Hoc On/Demand Distance Vector (AODV) Routing", Internet draft (work in progress), IETF Mobile Ad Hoc Networks Working Group, November 1997.

[6] David B. Johnson, David A. Maltz, Mobile Computing, chapter 5, pages 153-181. Kluwer Academic Publishers, 1996

[7] Berkeley Network Simulator 2, http://www.isi.edu/nsnam

[8] IEEE Std 802.11-1997

Dr. LINDNER Miklós[8]

PUSKÁS TIVADAR AZ EGYETEMES MAGYAR HÍRADÓ SZOLGÁLAT ÚTTÖRŐJE

Most amikor a ZMNE Katonai Kommunikációs és rendszerszervező tanszéke nagyszerű kezdeményezése nyomán immár harmadszor lehetünk aktív résztvevői annak a technikai konferenciának amelynek fókuszában az a nemes cél áll miszerint a híradó szolgálat tervezett fejlesztése feleljen meg annak a stratégiai célnak amely a haderőt az információs társadalom jelentékeny részévé tegye.

E konferenciákon jelentékeny vita folyt és folyik a haderő híradó erőinek és eszközeinek az elkövetkező évtizedben történő fejlesztésének irányairól, nagyságrendjéről.

E kérdésben kifejtett vélemények és javaslatok, a kidolgozott magas színvonalú értekezések arról tanúskodnak, hogy a híradó szolgálat állományában az innovatív gondolkodásmód uralkodik, amelyben a meglévő gondok megoldására irányuló elgondolások sokszínűsége, racionalitása biztosíthatja a szolgálat reményekkelvárt reneszánszának bekövetkezését.

Ez a gondolkodásmód arra a hagyományos alapra támaszkodik amelyek a nagy magyar kutatók nevéhez és tevékenységéhez kötődnek.

Kérem engedjék meg, hogy mint a Puskás Tivadar Híradó Bajtársi Egyesület elnöke e konferencián méltassam a hosszú időn át méltatlanul mellőzött nagy magyar feltaláló és hazafi Puskás Tivadar munkáját és emlékét.

Régi adósságot törlesztett 1999-ben - a VK.. Híradó Csoportfőnöksége, együttműködve a Puskás Tivadar Távközlési Technikum vezetésével - amikor a megszervezett "Puskás Tudományos Hét" keretében először állította reflektorfénybe a nagy magyar feltalálót.

Puskás Tivadar azok közé a magyar hazafiak közé tartozik, akik a reformkor szellemét követő Deáki kiegyezéssel járó elodázhatatlan gazdasági fejlődés igénye állított a közérdeklődés fókuszába.

A kor, melyben élt és dolgozott a nemzet függetlenségéért, a polgári átalakulásért, az önálló gazdasági felemelkedésért vívott állandó harc időszaka volt.

Széchenyi István álmainak fokozatos megvalósulását jelentették azok az események, melyek a XIX. század II. felének Magyarországát jellemezték, melyek nagy hatást gyakoroltak a fiatal Puskásra, aki nem csak a műszaki fejlesztés elkötelezett híve, hanem jó érzékkel megáldott üzletember is.

[8] Dr. Lindner Miklós nyá.vezérőrnagy, A Puskás Tivadar Híradó Bajtársi Egyesület elnöke

A nemzeti ipar létesítményeinek gyors kialakulásával párhuzamosan tekintetét Angliára veti, mivel ez időben Anglia Európa legélenjáróbb ipari országa, köszönhetően annak az ipari forradalomnak, melynek kezdete a gőzgép feltalálásának idejére datálható.

Puskás Tivadar az osztrák Teresianumban szerez diplomát, ezt követően Angliában tanul, majd Erdélyben egy angol vasútépítő társaság alkalmazottjaként vasútépítéssel foglalkozik.

Magyarországon az 1867. évi kiegyezést követően felgyorsult a külföldi tőke beáramlása, bankok, hitelintézetek, szövetkezetek alakulnak, gyárak, gyártelepek, malmok épülnek, fejlődik a kereskedelem. Ez parancsolólag követeli a közlekedési infrastruktúra mielőbbi gyors kiépítését.

A nemzetközi munkamegosztás megvalósulásának reménye új távlatokat ígér Ennek szép példája az 1873. évi bécsi világkiállítás, ahol a kor másik nagy magyar műszaki zsenije Jedlik Ányos mutatta be az általa szerkesztett dinamót, melynek elvét 6 évvel a német Siemens előtt álmodta meg.

Puskás nagy érdeklődést mutatott az új világ, az Amerikai Egyesült Államok és annak ipara iránt. Ez időben Amerika ténylegesen a korlátlan lehetőségek hazája, a különféle bevándorolt népek nagy olvasztótégelye. Puskás 30 éves korában Amerikába utazik. Első időkben aranyásással is foglalkozik, majd a világ nagy műszaki zsenije Edison közeli munkatársa lesz, akitől sokat tanul. Egymás iránti kölcsönös érdeklődésük tartós barátsággá fejlődik. A tőke koncentrálódása már zömében létrehozta az infrastruktúrát Amerikában, amit csak nagyon rossz hatásfokkal tudnak irányítani.

Már van ugyan távírógép, de összefüggő, továbbkapcsolható, szelektív hálózat hiányában hatásfoka gyenge, áteresztőképessége minimális, esetenként katasztrofális, szinte gátja a gazdaság további fejlődésének.

E közben Bell 1876-ban feltalálja a telefont, ami világszenzáció, azonban csak pont-pont között használható. Ez viszont nem felel meg az egyre jobban prosperáló gazdaság sokrétű igényeinek.

Puskás érzi, valamit tennie kell. Ötlete, hogy olyan berendezést kell létrehozni, mely segítségével a telefonok tetszés szerint célirányosan egymással összekapcsolhatók. Az ötletet valóra váltja, ami fényesen igazolja a hozzáfűzött reményeket. Amerikában 1877-78-ban létrejönnek az első Puskás elvén működő telefonközpontok. Mint Edison barátja és európai képviselője 1879-ben elkészül első európai telefonközpontjával Párizsban. A központ építését nem kíséri a jogosan elvárható társadalmi támogatás.

Már 1878-ban felmerül benne egy hazai telefonközpont megépítésének gondolata. A gondolatnak megnyeri öccsét Ferencet, aki magyarországi teljhatalmú megbízottjává válik.

A Magyar arisztokrácia feudális beidegződése, a kivárásra játszó óvatossága az égető gyakorlati igény ellenére meggátolja a szükséges hitelek felvételében.

Puskás így saját finanszírozásában hozta létre 1881-ben az első 200 vonalas telefonközpontot Budapesten, mely a XIX. századi Magyarország egyik kiemelkedő műszaki létesítménye, ami a közelmúltban két városrészből egyesített fővárost Európa egyik legjelentősebb fővárosává emelte.

1884-85-ben jelentős volt a hálózat építése és a nyilvános állomások telepítése. Puskás a hálózatot saját pénzén fejlesztette. Miután hitelfelvételi forrásai nem voltak, saját anyagi lehetőségei kimerültek, a fejlesztés megtorpant.

1888-ban Baross Gábor hazánk kiemelkedő közmunka és közlekedési minisztere felismerte, hogy a beindult gazdasági növekedés érdekében a távközlési infrastruktúra gyorsabb fejlesztése szükséges ezért a hálózatot állami kezelésbe vette. Így a fejlesztést az állam finanszírozta, de szakértelmével Puskás mint bérlő részt vett a munkában.

Baross 1888-ban törvényjavaslatot nyújtott be, mely elfogadását a követően 1888. évi távbeszélő törvényként látott napvilágot.

E törvény kimondja: " A berendezések létesítésére és üzletére vonatkozó műszaki és eljárási szabályokat a közmunka és közlekedési miniszter állapítja meg" , továbbá

" a ház és földtulajdonosok kártérítés nélkül eltűrni tartoznak, hogy a közhasználatú távbeszélők és villamos jelzők huzalai épületeik és földjeik felett elvezettessenek (illetve azok) az épületekre vagy azok tetőzetére való felerősítését és bekapcsolását eltűrni kötelesek" . Talán van valami hasonlóság a hatályos távközlési törvényünk (1992. évi LXXII. törvény) és 1999. évi júniusi módosításában (1999. évi LXVI. törvény).

E törvény lényeges előrelépést jelentett:

- a fejlesztési tervek megvalósítása
- a kettős vezetékre való áttérés
- a helyközi kapcsolatok fokozott kiépítése terén

1893-ban - röviddel halála előtt - megalkotta a telefonhírmondót mellyel a telefónia és az újság ötvözetéből egy világraszóló kommunikációs lehetőséget varázsol a századvég közvéleménye elé. Ezt tartjuk a közszolgálati rádióhír szórás ősének.

Mit köszönhet az egyetemes magyar hírközlés - benne a Magyar Honvédség híradó szolgálata - Puskás Tivadarnak.

Elsősorban azt, hogy találmányaival erősítette Magyarország nemzetközi tekintélyét.

Tevékenységével bebizonyította, hogy egy európai kis nép fiai a világ élenjáró tudósai között - a népesség számából származtatható többszörösen meghaladó .számban- foglalhatnak helyet. Gondoljunk csak a műszakiak közül Jedlik Ányosra, Bláthy Ottóra, Zippernovszky Károlyra, Ganz Ábrahámra, Bánki Donátra és a többiekre, továbbá legújabb kori történelmünk Nobel díjasaira. Köszönhetjük Puskásnak az is azt, hogy a XX. század elején Magyarországon jelentős híradástechnikai ipar jött létre (Standard, Siemens, Orion) és ezek

több generáción át kitűnő szakember gárdát neveltek, amelynek hatását még ma is érzékeljük.

Ha Puskás Tivadar találmányainak katonai vonatkozásait vizsgáljuk, úgy a fejlődés a haderő híradó szervezeteinél is megindult.

A XIX. század végén szórványosan, az első világháborúban már nagyobb számban jelentek meg a katonai híradás esetenként kezdetleges eszközei melyek a katonai vezetés nélkülözhetetlen elemeit képezték.

Az 1930-as évek Magyar Királyi Honvédségének voltak Puskás elven épített 10-es, 30-as, központkapcsolói, 2-4 Néper erősítési tényezővel rendelkező tábori vonalerősítői, tábori könnyű és nehézvezetékes alegységei. Távírógépek, közepes és nagyteljesítményű rádiói melyek az 1950-es évekig a Néphadsereget is kiszolgálták.(R-3, R-7 stb.)

Az 1940-es években kerültek rendszerbe a Hell aritmikus és a Siemens ritmikus távírógépek.

Az I. és II. világháború valamint az ötvenes évek katonai híradóeszközei megtalálhatók a Bólyai János Katonai Műszaki Főiskola igényesen és szakszerűen rendezett Híradó Múzeumában amelyet a híradó tanszék gondoz, őszinte köszönet érte Dr. Koczka Ferenc ezredes úrnak..

A Néphadseregben rendszeresített híradóeszközök részben szovjet importból kerültek beszerzésre, részben a kiemelkedő eredményességgel működő magyar híradástechnikai ipar produktumai.

Kiemelkedően magas színvonalon állt a katonai vevőberendezések tervezése és gyártása. Némely típusért a tervezők Állami díjban részesültek. Panorámavevők a központkapcsolókat 10, 20, 40, 80, 160 kapacitással a hazai ipar gyártotta.

A vezetékes eszközök között találjuk a tábori könnyű és az egységes nehézvezetéket melyen géppel építve hazai gyártású vivőfrekvenciás berendezésekkel - az adott vezetési szinttől függően -12-24-36-48 csatornás összeköttetések létesíthetők.

Már a 80-as években rendelkeztünk egyes digitális jelek átvitelére alkalmas híradóeszközökkel. R-414 rádió relé, R-412 troposzféra állomás.

Talán nem tűnik szerénytelenségnek a hadsereg híradó szolgálata rendelkezett az országban először GHz-es sávban működő digitális mikrohullámú rendszerrel melynek létrehozásában a magyar ipar az Orion, míg üzemeltetésében az akkori

Magyar Posta nyújtott, jelenleg az Antenna Hungária nyújt hathatós segítséget. Hazánknak a NATO-ba történő felvétele kapcsán természetesen új eszközök, új szervezési elvek, és új módszerek kerülnek a híradó szolgálat birtokába. Ezek az új eszközök és módszerek egy tekintetben változatlanok, magukon viselik Puskás Tivadar zseniális felfedezését amelyek az állomások tetszésszerinti összekapcsolásának elvében, valamint a rádió hírszórásnak, ha úgy

tetszik a rádióhíradásnak a telefonhírmondóból történő szárrmaztatásában jut kifejezésre.

A HVK. Vezetési Csoportfőnökségnek távlati fejlesztési tervében a stacioner és tábori hírrendszer teljes digitalizálása szerepel ami előreláthatólag 2010-ig valósul meg.

Puskás Tivadar viszonylag rövid élete bizonyítja, hogy a célok világos megfogalmazása, az emberi akarat és leleményesség produktuma évszázadokon és kontinenseken átnyúló megbecsülést vált ki a hálás utókorból.

Ma a hálás utókor meghajtja az elismerés és az emlékezés zászlaját a nagy hazafi előtt. A Puskás Tivadar HíradóBajtársi Egyesület elnöksége és tagsága, melynek célja az alapszabály szerint - az aktuálpoltikától fényévnyi távolságot tartva- a híradással foglalkozó szakemberek összefogása, az együvé tartozás érzésének kialakítása, az egyetemes magyar híradó szolgálat becses értékeinek és hagyományainak megőrzése. Egyesületünk várja a hivatásos és nyugállományú katonákat, polgári szakembereket, a szolgálattal kapcsolatban álló szervezetek dolgozóit, munkatársait.

Mindannyiuk közös és megtisztelő kötelessége a jövő híradó szolgálatának kialakítása Puskás Tivadar alkotó szellemének megőrzése és ápolása.

E nemes feladathoz kívánok valamennyi jelenlévőnek jó erőt-egészséget.

Köszönöm megtisztelő figyelmüket.

JAMRIK Péter[9]

URH RÁDIÓTÁVKÖZLÉSI TRENDEK – CIVILEK A HONVÉDELEMBEN

NOVOFER Innovációs Rt
Rádiótávközlési Mérnökiroda

Az URH rádiótávközlés nemzetközi fejlődési trendje nyomán létrejövő megoldások katonai felhasználást is lehetővé tesznek. E – főként „civil" – műszaki megoldások ma már olyan műszaki színvonalat jelentenek, amelyek a katonai alkalmazásban elfogadottak. A magyarországi haderőreform révén több feladat is hárulhat a civil szférára. Ennek néhány lehetőségét szeretném ismertetni előadásomban.

Az URH frekvenciatartomány (tipikusan 40 MHz és 900 MHz között) készülékfejlesztései úgy az áramköri megoldásokat, mint a mechanikai kiviteleket illetően figyelembe veszik a katonai célú minőségi szabványok előírásait. A legtöbb készülék megfelel a MIL 810 C/D/E szabványoknak. Az áramköri felépítés révén a frekvenciatartományon belül szinte bármely sávrészre rendelhetők készülékek. Ennek előnyeit már ma is kihasználják nemcsak a katonai célú alkalmazásoknál, hanem a civil célközösség körében is. A nagyfokú kompatibilitás, a sorozatnagyságból fakadó alacsony gyártási költségek és a kiterjedt szervizhálózat mindkét felhasználói réteg számára előnyöket jelent. Az analóg berendezéseknél alkalmazási hátrányt jelent, hogy könnyen lehallgathatóak, illetve zavarhatóak az összeköttetések.

A legújabb digitális fejlesztési trendek e hátrányt nagyrészt képesek kiküszöbölni. A TDMA, CDMA stb. technológiákon alapuló rendszerek – GSM, UMTS, TETRA, TETRAPOL stb. – nemcsak széleskörű infrastrukturális elemeket biztosítanak magas fokú titkosítás lehetőségével, hanem az u.n. közvetlen vagy DM üzemmódban is jó képességekkel rendelkeznek.

Ma a távközlési, informatikai költségek egyre növekvő arányt képviselnek. Főleg a békevezetési feladatoknál, a hátországi kapcsolatoknál

[9] Jamrik Péter NOVOFER Innovációs Rt, Rádiótávközlési Mérnökiroda vezérigazgató, vezető tervező

jelentős költségcsökkentési lehetőséget jelent a közös infrastruktúra. Ennek előnyei az üzemeltetés mellett a javítási és karbantartási feladatoknál is jelentkeznek. A haderőreform csökkenő tiszti és sorkatonai állománnyal számol. E területen nemcsak egzisztenciális lehetőséget kaphatnak a leszerelő szakemberek, hanem a katonai alkalmazások lehetőségei az egyébként polgári (üzleti) hálózatok jobb kihasználását is lehetővé teszi. A közös használatú rendszerek a katonai rendelkezésre állási követelmények miatt általában minőségi előnyöket jelentenek a civil alkalmazásban is. A civil szolgáltatók – szakmai szervezetek – számos olyan lehetőséggel rendelkeznek, amelyek a haderők számára is alkalmazhatóak.

A NOVOFER Rt Rádiótávközlési Mérnökirodája is ezek közé tartozik. A tervezés során korszerű, PC alapú digitális adatbázisokat használunk. A legkorszerűbb készülékeket alkalmazzuk. Szerviz-hátterünk és műszerparkunk lehetővé teszi a gyors javítást. Telepítőink bármilyen körülmények között telepítik a berendezéseket, antenna rendszereket.

Az együttműködés e téren is kölcsönös előnyökkel járhat.

HAMAR Sándor[10]

A KATONAI HÍRADÁS FEJLŐDÉSÉNEK ÉS FEJLESZTÉSÉNEK LEHETSÉGES ÚTJAI

1. Történeti áttekintés

A Magyar Honvédség állandó jellegű távbeszélő és távgépíró rendszerének első elemeit - többnyire polgári eredetű híradó eszközökre alapozva - lényegében a második világháború után kezdték kiépíteni, kizárólag a postai hálózat igénybevételével, az építéskor hozzáférhető technikai színvonalon.

A **70-es évek elején** a Honvédelmi Minisztériumban, a katonai felső vezetés fontosabb objektumaiban, a hadsereg és a hadosztályok laktanyáiban az objektumokon belüli híradás biztosítására az automata (általában Rotary rendszerű, a postai hálózatból leszerelt központok átvételével) központok már megjelentek. Az ezredeknél és ennél alacsonyabb szervezeti egységeknél az objektumon belüli híradásra kizárólag kézi kapcsolású telefonközpontok működtek. Az egyes objektumok között egy, a hadosztály-hadsereg viszonylatban egy-két, míg a hadsereg és a vezérkar között három-négy távbeszélő vonal biztosította az összeköttetést.

Nyilvánvalóvá vált, hogy a Magyar Posta által üzemeltetett általában kézikapcsolású országos hálózat alkalmatlan – az un. „K" telefonhálózat kivételével – a katonai vezetés országos és nemzetközi, békeidejű és háborús vezetési igényeinek kielégítésére. A politikai és katonai vezetés az 1970-es évek közepén döntött a Magyar Néphadsereg önálló állandó jellegű hírhálózatának kiépítéséről.

Az MN Híradófőnökség **1976** elejére elkészítette „Az MN távhívó rendszere létrehozásának koncepciója" c. okmányt, amely 1976. novemberében került jóváhagyásra.

Ennek eredményeképpen 1976-ban elkezdődött a HM-II objektum hírközpontjában az első 3000 vonalas ARF-102/A crossbar rendszerű alközpont telepítése. 1979 végére elkészült Budapest és környékén egy ARM-503 tranzit központtal, egy ARF-102/A típusú alközponttal és 18 darab ARK-511/A típusú távhívó végközponttal az első szigetszerű távhívó hálózat, még egyedi tervek alapján.

Ugyanebben az évben elkészültek az országos távgépíró hálózat tervei is. A hálózat kiépítése 1981-re lényegében befejeződött. A hálózatban 20 központkapcsoló, több mint 500 géptávíró állomás működött és évente kb. 100 ezer közleményt továbbítottak;

[10] Hamar Sándor mk. ezredes, HM-HVK VCSF-ség híradó osztályvezető

1980-ban a POTI (Posta Tervező Iroda) elkészítette és jóváhagyásra került az ”MN Távhívó Hálózat Rendszertechnikai Terve”. Ez évben kezdődött meg a hazai digitális PCM alapú átvitel-technikai eszközök kifejlesztése az Orion és a TERTA (Telefongyár) együttműködésével.

1983-ban elkészült a kor színvonalán álló „Területi Hírközpont” Kaposvárott, egy háromszintes épületben 144 m² alapterületen. Az ARM és az ARF távbeszélő-távhívó központoknak 20 000 vonalas rendezővel, BK-300 vezetékes átviteltechnikával, mikró és URH, valamint rádió-távvezérlővel, valamint az akkori előírásoknak megfelelő távbeszélő titkosító és rejtjeltő zártésszel együtt.

1990-ben lényegében befejeződött a TEHK rendszer telepítése az analóg távhívó hálózat kialakítása, amelyben csúcsponton 9 darab végközponttal egybeépített tranzit központ, 8 darab távoli ARF-102/A, 3 darab EPF-512, 35 darab ARK-511 és ARK-522, 26 darab EPK-128/Z és EPF-128 távhívóközpont működött 28 000 mellékállomással, valamint 65 000 alközpontokon lévő mellékállomással.

Ez időszakban kiépült az MH mikrohullámú hálózatának alapja (45 állomás, 1000 km nyomvonalhossz, 1200 távbeszélő és 600 távíró csatorna kapacitással, 5 PCM-es lecsatlakozó kábelirány 90 km. hosszban).

A tábori hírrendszert analóg átviteli utakat biztosító 2-6-12-21 csatornás rádiórelé, 6-12 csatornás kábelvivős rendszerek, kézikapcsolású távbeszélő, automata kapcsolású távgépíró központok, valamint fixfrekvenciás, alapvetően beszédre alkalmas rádió berendezések képezték és képezik a mai napon is.

A Magyar Honvédség távhívó hálózatában - 1998-99-ben a légtérszuverenitási program keretében elkezdett fejlesztéssel - már minőségi változás is érezhető volt. A digitális ISDN típusú kapcsolóelemek telepítésével elsősorban a légierő és csapatai, valamint a Honvédelmi Minisztérium és a Honvéd Vezérkar híradása javult. Az új rendszeren ugyan még a beszédátvitel és a telefax a meghatározó, azonban egyes viszonylatokon (pl. HM KGIR adatátviteli rendszerének legfontosabb állomásai között) már sikerült a nagy sebességű adatátvitelt is biztosítani. Kialakult egy egységes digitális hálózatmenedzsment rendszer.

A működő digitális hálózat lehetővé tette, hogy az MH távközlő hálózata összekapcsolható legyen a NATO katonai távközlő rendszerével (IVSN rendszer) kiegészítő beruházás, vagy fejlesztés nélkül beszéd, telefax, adatátviteli és videokonferencia üzemben egyaránt képes együttműködni.

A HVK Híradó Csoportfőnökségen a különféle távközlési rendszerek vizsgálatai, gyakorlati alkalmazásuk lehetőségei és tanulmányutak tapasztalatai alapján, 1994-95 években különböző tanulmányok készültek a digitális technika MH távközlő hálózatában történő alkalmazásának lehetőségéről.

A jelenleg érvényes fejlesztési célkitűzések kialakításával már 1992-ben foglalkoztunk, 1997-re elkészült a fejlesztési koncepció és 2000. április 26-án elfogadásra került a részletes hosszú távú fejlesztési terv.

Az elfogadott fejlesztési terv alapján lehetővé vált az MH híradó és informatikai korszerűsítési programjának tervszerű végrehajtása, valamint a programok végrehajtásához szükséges közbeszerzési eljárások megindítása.

2. Az MH híradása fejlesztési stratégiáját meghatározó tényezők

Az MH híradása fejlesztési stratégiájának kidolgozása 1992-97 közötti időszakra tehető, melynek során célul tűztük ki egy olyan egységes digitális hírközlő hálózat kialakítását, amelyben az állandó jellegű és tábori (mobil) hírrendszerek felépítése azonos rendszertechnikájú átviteli és kapcsolástechnikai, korszerű digitális ISDN alapú központokból áll.

Az MH egységes digitális híradó rendszere fejlesztési koncepciójának kidolgozását hosszú elemző tevékenység és kutatómunka és különböző tanulmányok kidolgozása előzte meg.

Egyrészt figyelembe kellett venni a polgári távközlésben tapasztalható technikai fejlesztéseket és fejlődési trendeket, melyek az 1990-es évektől kezdődően az ISDN típusú kapcsolástechnika elterjedését prognosztizálták. Másrészt figyelembe kellett venni azon nemzeti és NATO követelményeket és elvárásokat, amelyek a meglévő mobil és stacioner híradó rendszerekkel a kor színvonalán nem voltak biztosíthatóak. Harmadrészt a figyelembe kellett venni a légtérszuverenitási program keretében letelepített ISDN típusú kapcsolóközpontok üzemeltetési tapasztalatait, valamint azt a tényt, hogy e rendszerek a polgári távközlésben általánosan, széleskörben elterjedt technológiát alkalmaznak és ezek, hogyan „katonásíthatók”.

Az MH híradó rendszere fejlesztési terve megfelel a jelenleg érvényben lévő NATO elvárásoknak, valamint az NC3 Testület albizottságaiban meghatározott irányelveknek és a NATO Katonai Tanácsának MC 337 számú dokumentumában (A szárazföldi csapatok harcászati híradó és informatikai rendszereivel szemben támasztott harcászati-műszaki követelményei 2000 után) foglaltaknak.

Ez utóbbi dokumentum meghatározza azokat a főbb szempontokat, amelyeket a híradó rendszer fejlesztése során figyelembe kell venni.

Főbb megállapításai a következők:

a) Commercial of the shelf: ahol csak lehetséges a polgári életben használatos technikai eszközöket célszerű (elsősorban gazdaságossági okok miatt) a katonai infokommunikációs rendszerekben alkalmazni.

b) Interoperabilitás a lehető legmagasabb technikai szinten (Tábori-Stacioner rendszerek, Fegyvernemek, harcászati-hadműveleti vezetési szintek, NATO-Nemzeti rendszerek között stb.)

c) A rendszer feleljen meg az általános katonai követelményeknek, mint:

- Biztonság;
- Megbízhatóság;
- Túlélőképesség, alkalmazkodóképesség (automatikus útvonalválasztás, autentikáció);
- Többszintű hozzáférési jogosultság és bontási jog beszéd és adat típusú összeköttetésekre egyaránt (MLPP-Multi-Level Precedence and Preemption);
- Mobilitás;
- Rejtettség;
- Szállíthatóság;

d) Nemzeti, Nemzetközi szabványok és ajánlások használata;

A hálózati architectúra meghatározása vonatkozásában a fenti dokumentum megkülönböztet általános célú híradó rendszert (GPS-General Porpose Segment), és különleges célú híradó rendszereket (SPS-Special Porpose Segment). A kettő rendszer között az alkalmazás körülményeiben van különbség.

A kommunikációs architectúra három szintből tevődik össze:

Első szinten a stratégiai rendszerek állnak, mely magába foglalja mind az általános mind a különleges célú híradó rendszereket, kapcsolási funkciót biztosít az alsóbb szintű kommunikációs alrendszereknek.

A második szintű alrendszer magába foglalja a harcászati szintű rendszereket, beleértve a hadszíntér nagykiterjedésű alrendszereit (WAS-WIDE AREA SUBSYSTEM), valamint a hozzá kapcsolódó helyi alrendszereket (LAS-LOCAL AREA SUBSYSTEM).

A harmadik szintű alrendszert mint helyi alrendszert definiálja (LAS), mely nagy sávszélességű kommunikációs kapcsolatot biztosít a parancsnokságokon, béke elhelyezési körleteken belül.

Ez a hármas tagozódás megkülönbözteti az állandó telepítésű hálózatokat első szinten, mint például az MH állandó jellegű távközlő hálózatát, a nemzeti védelmi célú hálózathoz kapcsolódó közcélú hálózatokat, a NATO

CORE NETWORK stb., valamint a kettes, hármas szinteken a harcászati szintű alrendszereket.

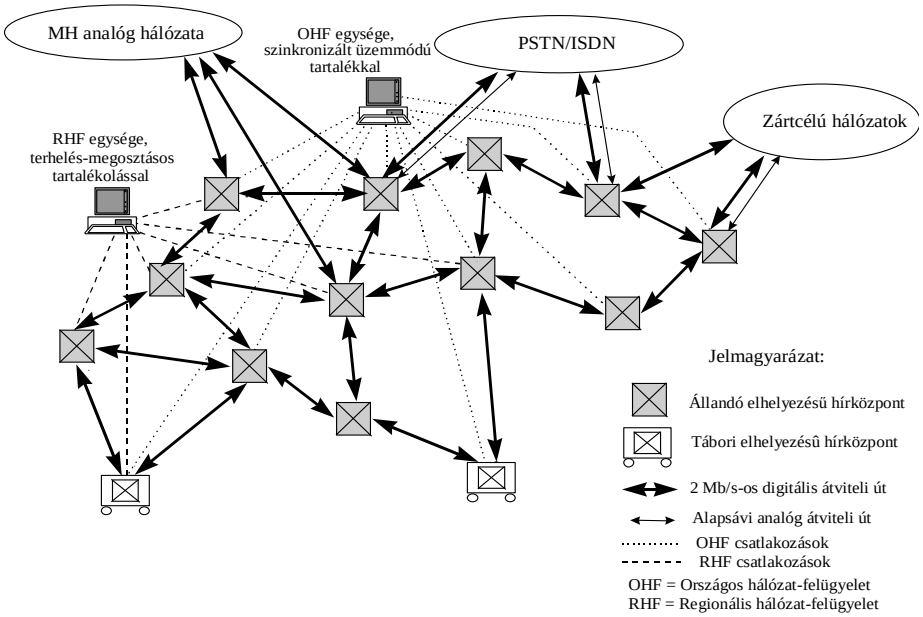
A dokumentum technikai paramétereket és szükséges szolgáltatásokat is definiál, többek között meghatározza a pont-pont közötti kommunikáció átviteli sebességét mint a 64 kbps-os alapcsatorna és 2 Mbps-os trunk csatorna, a vonalkapcsolt összeköttetéseket nx64 Kbps-os sebességen. Ez megfelel a ITU ajánlás szerinti PCM rendszerű átvitel-technikai eszközök, illetve az ISDN rendszerek technikai jellemzőinek.

Az NC3 Testület Kommunikációs Hálózatok Albizottsága (NATO Communications Network Subcommitee) megállapítása szerint, jelenleg három különböző típusú digitális interfész létezik és várhatóan a közeljövőben sem jelenik meg újabb.

Ilyenek az egyszerű katonai (pl. STANAG 4206, EUROCOM sorozat), katonai követelményekkel kibővített polgári (pl. STANAG 4578/ISDN), és a hagyományos polgári (pl. ITU, ETSI, IEE 802.3, stb.) interfészek. Ez meghatározza azon interfész készletet, amellyel a Magyar Honvédségnek az interoperabilitás biztosítása érdekében rendelkeznie kell.

Fejlesztési koncepcióban megfogalmazott egységes digitális hálózat rendelkezik mindazon szolgáltatásokkal és szabványos interfészekkel, amely mind a nemzeti mind a NATO követelményeknek eleget tesz. A rendszer kialakítása során arra törekedtünk, hogy az új távközlő és informatikai hálózatban csökkenjen az eszközök típusválasztéka, az üzemeltetés és fenntartás rendszere pedig egységes, biztonságos és gazdaságos legyen.

Egységes rendszer alkalmazásával kell és lehet megteremteni azt a lehetőséget, hogy a katonai felső vezetéstől a dandár, ezred, zászlóalj, osztály, önálló alegység szintig bezárólag a tábori és állandó jellegű vezetési pontokon a vezetők és törzsek mind békeidőben az állandó elhelyezéskor, mind pedig minősített időszakban a hadműveleti területen azonos távközlési és informatikai környezetben hajthassák végre feladataikat. A rendszer struktúráját a katonai követelményeknek megfelelő, területi lefedettséget biztosító, nagy életképességű, az ideális rácsrendszert közelítő szövevényes hálózatként lehessen kialakítani. Az így felépített hálózat megfelel az MC 337 dokumentumban meghatározott követelményeknek és struktúrának.



A rendszer felépítésének elvi vázlata

Az MH jelenlegi állandó jellegű digitális kapcsolástechnikai rendszere a SIEMENS 300E típusú központ családdal és készülékeivel egységes rendszerben van megvalósítva. A mintegy 40 digitális központból (tizenhatezer port nagyságrendű) és a hozzájuk kapcsolódó analóg (AR, EP típusú) központokból álló rendszer MH tulajdonú, jogilag zártcélú hálózatot alkot.

A digitális központok főleg 2 Mbps E1, illetve néhány helyen nx64 kbps (frakcionált E1) interfészekkel összekapcsolódva részleges szövevényes hálózatot alkotnak. A központok trönk oldalon csak egymáshoz, az állandó híradást biztosító központokhoz, a NATO Core hálózatához (NATO Core Network), esetlegesen a STANAG 4578-ban meghatározott digitális gateway segítségével a NATO tagországok harcászati (tábori) híradó rendszereihez, a közcélú hálózathoz (PTSN) csatlakoz(hat)nak. Az állandó jellegű hálózat ezen felül más zártcélú, különcélú hálózatokhoz történő csatlakozása is biztosított.

3. Fejlődési trendek a távközlésben

A távközlés területén az elmúlt évtizedben végbemenő változások gyökeresen átalakították és alakítják napjainkban is a magyar társadalom infokommunikációs rendszerekhez és szolgáltatásokhoz fűződő viszonyát. Általánosan elmondható, hogy a társadalom minden területén a működés számára nélkülözhetetlen a kommunikációs lehetőségek és az integrált információs infrastruktúra jelenléte. A szolgáltatók és felhasználók között közös érdekek mentén működő kapcsolatrendszerek alakulnak ki, ahol az egyensúlyi feltételeket egyrészt a hírközlési ágazat liberalizálódása és az egyre bővülő szolgáltatás-

készlet megjelenése, másrészt az árszabályozó mechanizmusok erőteljesebb jelenléte biztosítja.

A nyílt szabványokon alapuló digitális távközlő hálózatok megjelenésével lehetővé vált a távközlési szolgáltatások kiterjesztése, minőségi termékként történő forgalmazása.

Napjainkban a piaci igényekhez igazodó fejlesztési elképzelések olyan távközlő hálózatok kialakítását tűzték ki célul, amelyek közös platformon biztosítanak hozzáférést a különböző típusú kommunikációs igények, szolgáltatások eléréséhez. Az integrált szolgáltatású digitális hálózatok fejlődésével egyre inkább elkülönülnek a hálózat szereplői az üzemeltetői és szolgáltatói szerepkörök. Kirajzolódik az un. „Intelligens Hálózatok" koncepcionális modellje, melyben a szolgáltatási és fizikai síkok egymással a „nyílt rendszer elve" szerinti kölcsönhatásban biztosítják a komplex kommunikációs igények kiszolgálását, ahol a szolgáltatás menedzsment a hordozó szolgálatoktól függetlenül, autonóm módon szerveződhet a piaci játékszabályoknak megfelelően.

Napjainkban az informatikai szektor jelentősége nagymértékben felértékelődött. Világosan látszik, hogy az informatika elterjedése, fejlődési üteme a gazdasági és társadalmi folyamatokra is kihatással bír. Az informatikai hálózatok elterjedését nagymértékben meggyorsíthatják azok a folyamatok, amelyek arra utalnak, hogy az informatikai és távközlési technológiák fejlődési irányvonala egy közös megoldás felé mutat, konvergálódik.

A technológiai konvergencia mentén történő fejlesztések eredményeképpen ma már egyre szélesebb körben válik lehetővé a közös platformon biztosított multimédiás szolgáltatásokhoz való hozzáférés. Ez a törekvés összhangban van az un. intelligens hálózatok gondolatiságával, melyek műszaki-technikai vetülete az ISDN, ATM, TCP/IP, GSM alapú rendszerekben jelentek meg először, és vélhetőleg az elkövetkező időszakban is erőteljes fejlődésük várható.

Az intelligens hálózatok főbb jellemzői:

- személyre szabott távközlés (személyi kommunikáció);
- hálózati intelligencia (autorouting, öngyógyító mechanizmusok, automatikus (azonosítás) autentikáció, dinamikus erőforráselosztás, rugalmasság, az igényekhez igazodó rugalmas hírközlés politika)
- szolgáltatásfejlesztés (a központ alapfunkcióitól függetlenül történhet alkalmazásfejlesztés);
- elkülönülnek a hálózat szereplői: szolgáltatók, fejlesztők és üzemeltetők;
- hálózati erőforrások hatékony felhasználása;

- hálózati funkciók hordozhatósága;
- mobilitás és mindenütt elérhetőség;
- rendelkezésre állás és biztonság;
- nagy sávszélességű kommunikáció;

4. A fejlődés várható iránya(i)

A polgári hírközlés területén tapasztalható fejlődési trendek, a technológiai konvergencia és az intelligens hálózatok megjelenése természetszerűleg kihatással bír a katonai és benne a Magyar Honvédség jövőbeni híradó és informatikai fejlesztéseire is, valamint az azt meghatározó fejlesztési koncepciók és stratégiák meghatározására, kidolgozására.

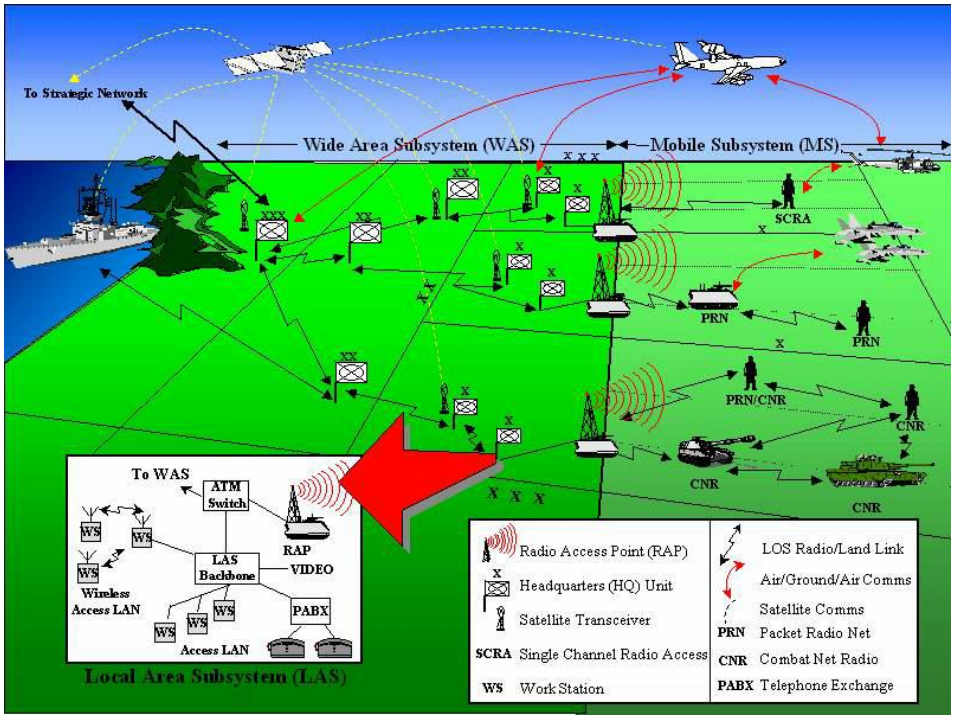
Azon doktrínális alapelvek, melyekből a híradó rendszerekkel szemben történő elvárások, és követelmények levezethetőek (mint például a mobilitás, túlélőképesség, alkalmazkodóképesség, rugalmasság, biztonság, védettség, stb.), valamint a polgári távközlésben megjelenő új technológiák és szolgáltatások lehetővé teszik magasabb szintű követelmények támasztását a híradó rendszerekkel szemben.

Ez előrevetíti egy olyan nagy sávszélességű, intelligens transzporthálózat kialakításának szükségességét, amely platform független hozzáférést biztosít a különböző típusú beszéd és nem beszédcélú összeköttetések létesítésére.

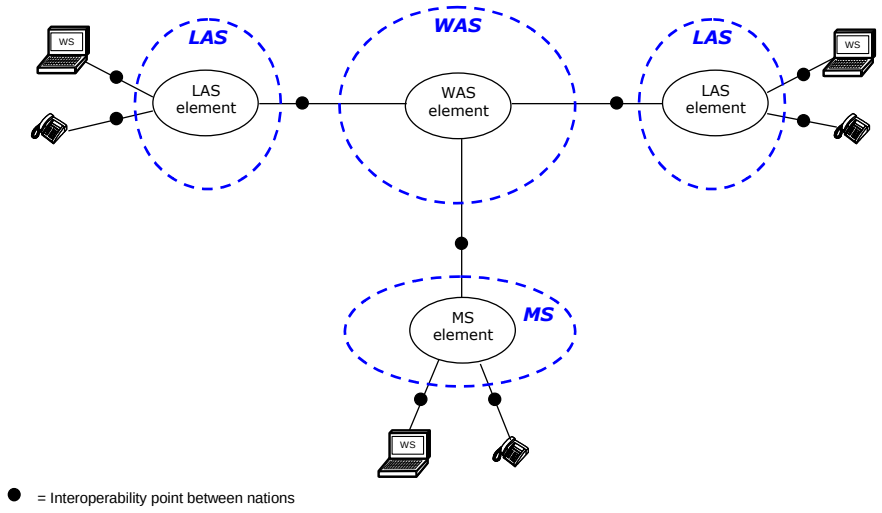
Az így kialakított hálózat biztosíthatja az intelligens kapcsolási funkciókat, szabványos interfészeket a hozzáférési pontokon, automatikus autentikáció (azonosítás) képességét a felcsatlakozó mobil és más helyi hálózatok részére, autorouting funkciót, magas szintű biztonsági és titkosítási funkciókat, MLPP képességet, megfelelő QOS (Quality of Services) képességet, dinamikus sávszélesség allokáció képességét, magas szintű túlélőképességet.

A hálózati architektúra kettős tagozódása várható. Megkülönböztethetünk transzport és hozzáférési (helyi) hálózatokat, mind az állandó mind a harcászati híradásban. Lehetővé válik a hálózati architektúra minden szintjét magába foglaló integrált hálózatmenedzsment szolgálat biztosítása.

Egyes NATO tagállamok részvételével megkezdődött – mondhatjuk úgy, hogy – egy fejlesztési koncepció kidolgozása, melyek az eredményes befejezés után várhatóan 2010 utáni NATO és tagországok híradó és informatikai rendszerei kialakítására fognak vonatkozni, az interoperabilitási követelmények figyelembevételével. A TACOMS POST 2000-nek nevezett project 12 NATO tagállam katonai és polgári vállalatainak, valamint a NATO szervezeteinek részvételével végzi a munkát.



A jövő NATO híradó és informatikai rendszere a jelenlegi publikációk, dokumentációk alapján az alábbiak szerint alakulhat:



A TACOMS POST 2000 alapvetően a TINA (Technology Independent Network Architecture - Technológiailag Független Hálózati Architektúra) koncepciót veszi alapul. A hírközlési rendszer (az MC 337 megállapításaival összhangban) nagy kiterjedésű hálózati szegmensekből (WAS), valamint a hozzá csatlakozó helyi (LAS) és mobil (MS-Mobile System) hálózati szegmensekből tevődik össze.

Az egyes hálózati elemek, un. hozzáférési pontokon, szabványos interfészekkel csatlakoznak egymáshoz, illetve a stratégiai hálózathoz. A hozzáférési pontokon különböző katonai követelményekkel bővített, polgári ajánlásoknak megfelelő szabványos interfészeket definiál:

- A WAS-hoz csatlakozó LAS vagy MS szabványos interfész felülete ATM alapúra tervezett.
- A felhasználói hang és videokonferencia terminálok ISDN míg az adatterminálok IP alapú hozzáférési ponton kapcsolódnak a LAS (MS) alrendszerekhez.

Ezen interfészeken keresztül biztosítani kell valamennyi felhasználói szolgáltatáshoz törtnő hozzáférést, valamint a hálózati és rendszerfunkciókat.

A LAS, WAS, MS szegmensek közötti hálózati szintű együttműködés a fenti hozzáférési pontokon valósul meg. Az egyes szegmensek belépési és kilépési pontjai közötti részt technológiailag független fekete dobozként kell kezelni, amely minden arra alkalmas technológiával megvalósítható. Az interfészkövetelmények meghatározásánál az OSI modellt veszi alapul.

Ez a koncepció megfelel a fentiekben felvázolt transzporthálózati, hozzáférési hálózati modellnek.

A dokumentum jelenlegi állapotában - figyelembe véve a WAS-ra meghatározott interfészeket - feltételezi, hogy a gerinchálózat ATM alapú, azonban a későbbiekben éppen a technológia független koncepció miatt ennek meghatározásától eltekint.

A projekt keretén belül kidolgozásra került a szükséges STANAG-k hierarchiája, melyből az első interfész STANAG-k megjelenése 2003-2008-re tehetők.

A teljes rendszer megjelenése, széles körű használata, tesztelést követően 2020 után várható.

Más NATO tanulmányokban (pl. NC3A Next Generation Convergence Technical Note 821) hasonló képen megfogalmazásra került egy olyan egységes intelligens transzport hálózat megvalósításának szükségessége, amely szabványos interfészeken keresztül hozzáférési pontot biztosít az egyes nemzetek távközlési hálózatai számára, biztosítva ezáltal a tagországok közötti információ átvitel lehetőségét, azaz a különböző rendszerek közötti teljes interoperabilitást.

A fenti követelményeknek eleget tevő transzporthálózatok megvalósítására a polgári távközlési trend figyelembevételével jelenleg az ATM és IP alapú hálózatok alkalmasak.

Az intelligens hálózatok koncepciója alapvetően két ágazat egyidejű fejlődésének a távközlési és informatikai szektorban végbemenő változásoknak az eredményeképpen született meg. Ez egyrészt köszönhető az Internet által közkedvelt és jelentős marketing stratégiával alátámasztott IP protokollnak, másrészt a távközlési szektorban kifejlesztésre került ATM protokollnak. Mindkét esetben a cél olyan technológiai megoldás kidolgozása volt, amely nagysávszélességű hálózati szintű szolgáltatást és közös platformot biztosít mind a beszéd, mind a nem beszéd célú kommunikációs igények kiszolgálására.

Az IP alapú hálózatok robosztussága (összetettsége) lehetővé teszi a rendszer szélsőséges körülmények közötti életképességét. Csomagkapcsolt rendszerként támogatja a hálózati erőforrások (pl. rendelkezésre álló sávszélesség) hatékony kihasználását. Dinamikus forgalomirányító képességgel rendelkezik, ezáltal lehetővé válik a forrás és cél állomás közötti lehetséges útvonalak automatikus meghatározása, az erőforrások elosztásának optimalizálása. A helyi hálózatokban az ethernet az elterjedt technológia, ezáltal bármely TCP/IP hálózathoz a csatlakozás megoldott. Az IP hálózatok sikerességét ezen felül a hálózati eszközök alacsony bekerülési költsége, az alkalmazott technológia elterjedtsége, az integrált szolgáltatások (pl file transzfer, telnet stb.) eredményezi. Az Internet protokoll nem kötődik fizikai hordozóközeghez, azaz bármilyen szabványos interfésszel és fizikai szintű hordozószolgálati protokollal képes együttműködni.

Az IP hálózatok hátrányaként említhetjük meg, hogy nem támogatja a valós idejű forgalom (multimédiaszolgáltatások hang, videó stb) garantált minőségben történő továbbítását (QoS), továbbra sincs egységes koncepciókon alapuló szabványosított hálózatmenedzsment képessége. A címzési rendszerének bővítése is szükségessé vált. Jelenleg az IPv4 mellett megjelent az Ipv6 protokoll, amelynek fejlesztése során nem csak a kioszthatő címtartományok bővítését, hanem a fenti problémák kiküszöbölését is célul tűzték ki.

Az ATM nemcsak mint protokoll, hanem mint átvitel-technikai eszköz is létezik. ATM megvalósítható saját ATM megoldással, SDH (szinkron digitális hiearchia) mikrohullámú/optikai, xDSL, CATV (kábeltévés hálózatok) felett. Biztosítja a nagysávszélességű, intelligens hálózati szintű szolgáltatásokat és szabványos interfészeket valamennyi ma létező alkalmazás számára. Hatékony belső jelzésrendszer, és hatékony előfizetői jelzésrendszer jellemzi. Önmagában egyesíti a vonal és csomagkapcsolt hálózatok előnyeit. Garantált minőségű szolgáltatást biztosít, támogatja QoS képességet. Terjed a LAN-okban és a „last mile" rádiós rendszerekben. A jelenlegi ATM alapú katonai rendszerek (mint pl. a RITA 2000), nem csak szabványos ATM interfészekkel rendelkez-

nek, hanem egyéb keskenysávú eszközök kiszolgálására közvetlenül alkalmas kapcsolódási felülettel is.

Az ATM hálózatok hátrányaként említhetjük az eszközök bonyolultságát, viszonylag nagy bekerülési költségét, lassú fejlesztési folyamatot. Érzékenyebb az IP hálózatokra jellemző forgalmi változásokra, a burst-ös adatfolyamokra.

Az jól érzékelhető, hogy az új adatátviteli technikák, mint pl. az ATM és IP költséghatékonyabb megoldást nyújtanak, mint a hagyományos PSTN hálózatok, azonban a jelenlegi fejlesztési, szabványosítási és az egyre növekvő piaci versenyben, hogy a jövő híradó rendszerei melyik technológián fognak alapulni, ma még nem lehet egyértelműen eldönteni.

A közeljövőben a polgári távközlés fejlődésének, és a TACOMS POST 2000 eredményeinek felhasználásával át kell gondolni a hosszú távú fejlesztési koncepcióinkat, terveinket. Annak ellenére, hogy a jelenlegi NATO rendszerekkel való együttműködés megoldott, fel kell készülnünk annak változására, a meglévő híradó rendszer együttműködési képességeinek folyamatos biztosítására.

Azonban feltétlenül hangsúlyozni szükséges azt a tényt, hogy a katonai követelményeknek és a lehetőségeknek az összhangjában dönthető el a fejlesztés útjai és módjai.

Felhasznált irodalom

1. MC/337 The NATO military operational requierment and communications archutecture for interoperable tactical communications system in support of land combat forces (post MC 277/2) (1994)
2. NC3A Next Generation Networks „Convergence” (Technical note 821) (2001)
3. TACOMS POST 2000 WP13202 Techonolgy Independent Network Architecture Concept study (Draft study report 2002)
4. The NATO General Purpose Segment Communications System (NGCS) Programme Volume-II Technical System Plan (Edition 3 1999)
5. DCI-CC2 porgress review within a NC3B SC/6-WG/1 context (2001)
6. TACOMS POST 2000 Draft STANAG Concept List

ENDRŐDI István

A BM ORSZÁGOS KATASZTRÓFAVÉDELMI FŐIGAZGATÓSÁG TISZA TÉRINFORMATIKAI RENDSZERE TOVÁBBFEJLESZTÉSÉNEK TERVE AZ EU ÉS NATO KÖVETELMÉNYEK TÜKRÉBEN

Bevezetés

Napjainkban, amikor az egész világ a környezetszennyezés, a természeti és civilizációs katasztrófák, a biológiai és vegyi terror lehetőségének árnyékában él kiemelt igényként jelentkezett a veszély- és katasztrófahelyzetek kezelését irányítani képes országos szintű szerv létrehozása, amely koordinátori és egyúttal a végrehajtói szerepkör betöltésével a rendelkezésre álló valós információk biztosításával jelentős mértékben elősegíti a mindenkori kormányzat döntéshozatali tevékenységét a katasztrófahelyzetek kezelése során.

A Magyar Köztársaság lakosságának biztonsága, a nemzetgazdaság és a nemzeti örökség javainak védelme minden állampolgárnak és szervezetnek kiemelt feladata. A „humanitárius segítségnyújtások" korában felértékelődött a katasztrófák megelőzésének és gyors felszámolásának szerepe. Az elmúlt években bekövetkezett jelentős számú katasztrófa- és veszélyhelyzetek „eredményeként" fokozott figyelem kíséri a katasztrófavédelem mindennapi tevékenységét.

Az 1996. évi XXXVII. törvény a Polgári Védelemről, valamint a 1999. évi LXXIV. Törvény (továbbiakban: Kat. Tv.) IV. fejezete, továbbá az érvényben lévő kormányhatározatok és rendeletek (pl. a 2/2001 korm. rendelet a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről) pontosan meghatározzák a katasztrófavédelem feladatrendszerét és tevékenységi körét. Mindezen feladatok és a katasztrófavédelemre felruházott hatósági és szakhatósági elvárások jelentős kihívás elé állították a BM Országos Katasztrófavédelmi Főigazgatóságot és területi szerveit.

A Kat. Tv. 14. paragrafusa határozza meg a katasztrófavédelmi célú távközlési és informatikai rendszerek egységes irányítási rendszerbe történő kialakítását és működtetését). Az Kat. Tv. 5.§ e. pontja kimondja, hogy a Kormány feladata a katasztrófavédelmi információs rendszer létrehozása.

A 179/1999. sz. korm. rendelet (XII. 10.) Kormányrendelet intézkedik a Kat. Tv. végrehajtásáról és egyben meghatározza a Kormányzati Koordinációs Bizottság (a továbbiakban: KKB) összetételét, illetve feladatait. A 2266/2000. (XI. 7.) Kormányhatározat intézkedik a Kormányzati Koordinációs Bizottság szervezeti és működési rendjéről, valamint eljárási szabályainak elfogadásáról.

A 179/1999. sz. korm. rendelet 8. § f. pontja a KKB feladataként határozza meg a katasztrófavédelmi kommunikációs és információs rendszerének kialakítására, működtetésére és fejlesztésére vonatkozó terv elkészítését.

Ennek részeként lett megtervezve, illetve kialakítva -a későbbiekben részletesen bemutatásra kerülő- A Katasztrófavédelmi Országos Információs Rendszer (a továbbiakban: KOIR) alapját képező Tisza térinformatikai rendszer 1. üteme.

A BM OKF hatósági tevékenységének várhatóan az egyik legjelentősebb feladata lesz a veszélyes anyagokkal kapcsolatos tevékenység keretén belül a veszélyes áruk fuvarozásának felügyelete. Az ipari üzemi technológiák esetében a veszélyforrás helyhez kötött ellenőrzése, valamint a megelőzés és beavatkozás jobban tervezhető, a felkészülés feltételei megteremthetőek.

A veszélyes anyag fuvarozás a veszélyforrás mobilitása miatt a fuvarozókat, a hatóságokat, valamint a mentőerőket lényegesen nehezebb feladat elé állítja. Az európai tendenciák is arra utalnak, hogy az elkövetkező időszak egyik legnagyobb kihívása az egyes - közúti, légi, vízi, vasúti - szállítási módok által okozott veszélyhelyzetek megelőzése, kezelése.

A veszélyes áruk közúti szállításával kapcsolatos tevékenység jogi alapja az egyes veszélyes árukat szállító közúti járművek útvonalának kijelöléséről szóló 122/1989 (XII.5.) MT rendelet, a módosítására kiadott 90/2001 (VI.15.) kormányrendelet, a veszélyes áruk közúti szállításának ellenőrzésére vonatkozó egységes eljárásról szóló 1/2002 (I.11.) kormányrendelet, a veszélyes áru szállítási biztonsági tanácsadó kinevezéséről és képesítéséről szóló 2/2002 (I. 11.) kormányrendelet.

Kormány 2/2001. (I. 17.) Korm.rendelet „a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről" 25.§ értelmében a hatóság (BM OKF) a veszélyes létesítményekről, a végrehajtott feladatairól, nyilvántartást köteles vezetni, és annak tartalmáról a Kormányzati Koordinációs Bizottság vezetőjének éves jelentést kell készítenie.

A Kormányzati Koordinációs Bizottság vezetője a jelentést évente egy alkalommal továbbítja az Európai Unió illetékes szervének.

A 3.pont értelmében „A hatóság (BM OKF) az üzemeltetők által benyújtott kérelmekről, biztonsági elemzésekről és biztonsági jelentésekről, külső védelmi tervekről és más, a nyilvánosságra tartozó információkról tájékoztatási rendszert hoz létre."

A 96/82 EK SEVESO II Tanácsi Irányelv az EU jogharmonizáció környezetvédelmi fejezetének illesztéseként került implementálásra.

A Nemzeti Katasztrófavédelmi Stratégia értelmében a veszélyes árú fuvarozásból fakadó veszélyeztetés a legnagyobb kihívás az elkövetkező időszakban a hazai katasztrófavédelmi szervezetrendszer számára. Bár a veszélyeztetés lokális, a beavatkozó erők, valamint a környező települések és a lakosság

megfelelő szintű védelme érdekében az uniós elveket és gyakorlatot figyelembe vevő rendszer létrehozása szükséges.

A veszélyforrás mobilitása a beavatkozáshoz szükséges erők/eszközök tervszerű díszlokációját nem teszi lehetővé, a beavatkozás várható helyszíne - az általánosan alkalmazott útvonalak ismertsége ellenére - nem prognosztizálható, az egyes veszélyes árú fuvarok valósidejű nyomon követése (GPS, vagy egyéb jeladós rendszer) jelenleg nem megoldott. A veszélyes áru fuvarozási balesetek elleni védekezés döntő területe tehát a megelőző védekezés.

A veszélyes áruk fuvarozásának európai szabályait - a szállítás módja (közúti, vasúti, vízi, légi) differenciáltan szabályozza. Ezen nemzetközi előírások részei a magyar jogrendszernek, megújításuk a nemzetközi szabályok változásait, módosításait figyelemmel kísérve, követő rendszerű.

A veszélyes áruk fuvarozásával kapcsolatos feladatrendszer megoszlik a különböző ágazati minisztériumok és azok által irányított szervek (közlekedési, határőrizeti, VÁM, katasztrófavédelmi szervek, hatóságok között.

A veszélyes áruk egy részének fuvarozása - sajátos, az uniós államokban nem szokott módon - útvonal kijelölési eljárás alapján előzetes engedélyhez kötött {122/1989. (XII. 5.) MT rendelet}. A rendelet hatálya alá tartozó veszélyes árúk (mindössze közel 100 anyag, ill. anyagcsoport) köre töredéke az ADR hatálya alá tartozó veszélyes anyagokénak. Az útvonal engedélyezési eljárás rendszerének fenntartása az uniós csatlakozás várható időpontjára is tekintettel középtávon sem tartható fenn.

E közúti veszélyes anyagfuvarozásban érintett hazai és nemzetközi vállalkozások már jelenleg is „támadják" a magyar szabályozás létjogosultságát, indokoltságát. Az útvonal engedélyezés alá tartozó anyagok és anyagcsoportok azonban az informatikai támogatási rendszerben kiemelt helyet kaphatnak azt követően is, ha az eljárás esetlegesen megszüntetésre kerül.

Az ADR, RID, DIR, valamint a vonatkozó ICAO annex hatálya alá tartozó veszélyes anyagok köre rendkívül széleskörű, egy részük katasztrófavédelmi szempontból érdektelen, illetőleg nem igényel megkülönböztetett kezelést. Biztosítani kell a kiemelt veszélyeztetést jelentő anyagok és anyagcsoportok prioritását.

Az útvonal engedélyhez kötött határokat átlépő közúti szállítások esetében a ki és beléptetés csak meghatározott közúti határátkelőhelyeken történhet. (122/1989. (XII. 5.) MT rendelet 2. sz. melléklete szerint: Hegyeshalom, Rábafüzes, Bánréve, Parassapuszta, Rajka, Salgótarján, Tornyosnémedi, Röszke, Letenye, Ártánd, Nagylak, Rédics, Záhony)

A veszélyes áruk fuvarozásának ellenőrzésében a katasztrófavédelmi szervek is közreműködnek. Ennek jogszabályi feltételei alapvetően rendezettek. Az ellenőrzés súlyponti helyszíneiben az uniós csatlakozással (2004) változás történik. Hazánk keleti és déli határszakaszain a „schengeni védvonal" felada-

tokat kell teljesíteni, s ezzel párhuzamosan a mobil ellenőrző rendszert kell működtetni az akkor már uniós határokon belül.

A fent felsorolt jogi szabályzókból egyértelműen látható, hogy a katasztrófavédelem információs rendszerének létrehozása kormányzati feladat és nem közvetlenül a Belügyminisztérium költségvetéséből megvalósítandó feladat.

A Magyar Köztársaság Európai Uniós csatlakozásához elengedhetetlen az EU követelményrendszerhez is illeszkedő katasztrófavédelmi információs rendszer továbbfejlesztése. A társadalom és szakma által támasztott elvárások is olyan komplex feladatrendszerek kidolgozását és végzését követelik meg, melyek kizárólag akkor valósíthatók meg eredményesen, ha a kellő időben a megfelelő mennyiségű és minőségű információ áll rendelkezésre a szükséges döntések meghozatala érdekében.

A fent említett elvárások következtében indokolt egy integrált Katasztrófavédelmi Információs rendszer megvalósítása. Maga a rendszer több alkotóelem egymásra építésével alakítható ki.

Az alkotóelemek az alábbiak:

1. A Katasztrófavédelem országos szintű informatikai- és távközlési hálózatának kialakítása és üzemeltetése (első és legfontosabb)
2. A Katasztrófavédelem meglévő és folyamatosan bővülő adatbázisai, és azok integrálása egy egységes adatbázis- és keretrendszerbe,
3. Az üzemeltetett és a telepítendő monitoring rendszerek által szolgáltatott adatok gyűjtése és folyamatos kiértékelése,
4. Hozzáférés a minisztériumok, társszervek és intézmények adatbázisainak azon részeihez, amelyek a Katasztrófavédelem alaprendeltetéséből adódó feladatok ellátásához szükséges,
5. A Kormányrendeletekben meghatározott lakossági tájékoztatási kötelezettség támogatása és megvalósítása az informatika és távközlés eszközeivel,
6. A nemzetközi kapcsolatok és együttműködések alapján a kölcsönös adatszolgáltatások adatbázisai kialakítása és továbbfejlesztése,
7. Az EU és NATO Programokban való részvétel, külső szabványok folyamatos implementációja, a fejlesztésekben ezek folyamatos figyelembevétele.

A Projekt helyzete

A KOIR megvalósítása érdekében 2001. második felében elindított TISZA Projekt a tervezési stádiumból 2002. augusztus 30-án az alábbi feladatok elvégzésével került kiépítésre:

- Elkészült a tervezett IP címkiosztás, amely jóváhagyásra felterjesztésre került a BM Informatikai Főosztály vezetőjéhez.
- Elfogadásra került a KOIR adathálózatának kiviteli terve és megkezdődött a telepítés. A telepített lokális hálózati eszközökkel megoldható az Internet

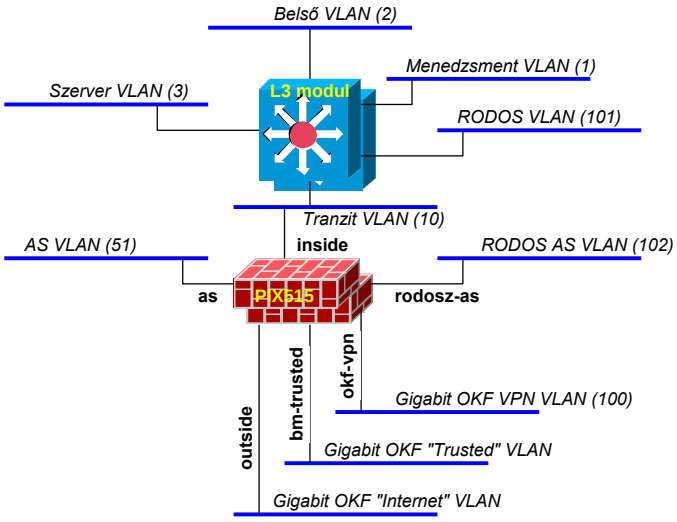
forgalom *tartalomszűrése*, a *forgalom-priorizálása* és a *lokális hálózat teljeskörű, biztonságos üzemeltetése*. Megfelelő *menedzsment szoftverrel* biztosítható a lokális hálózatok felügyelete, a trendek és a nem tipikus jelenségek folyamatos figyelése.

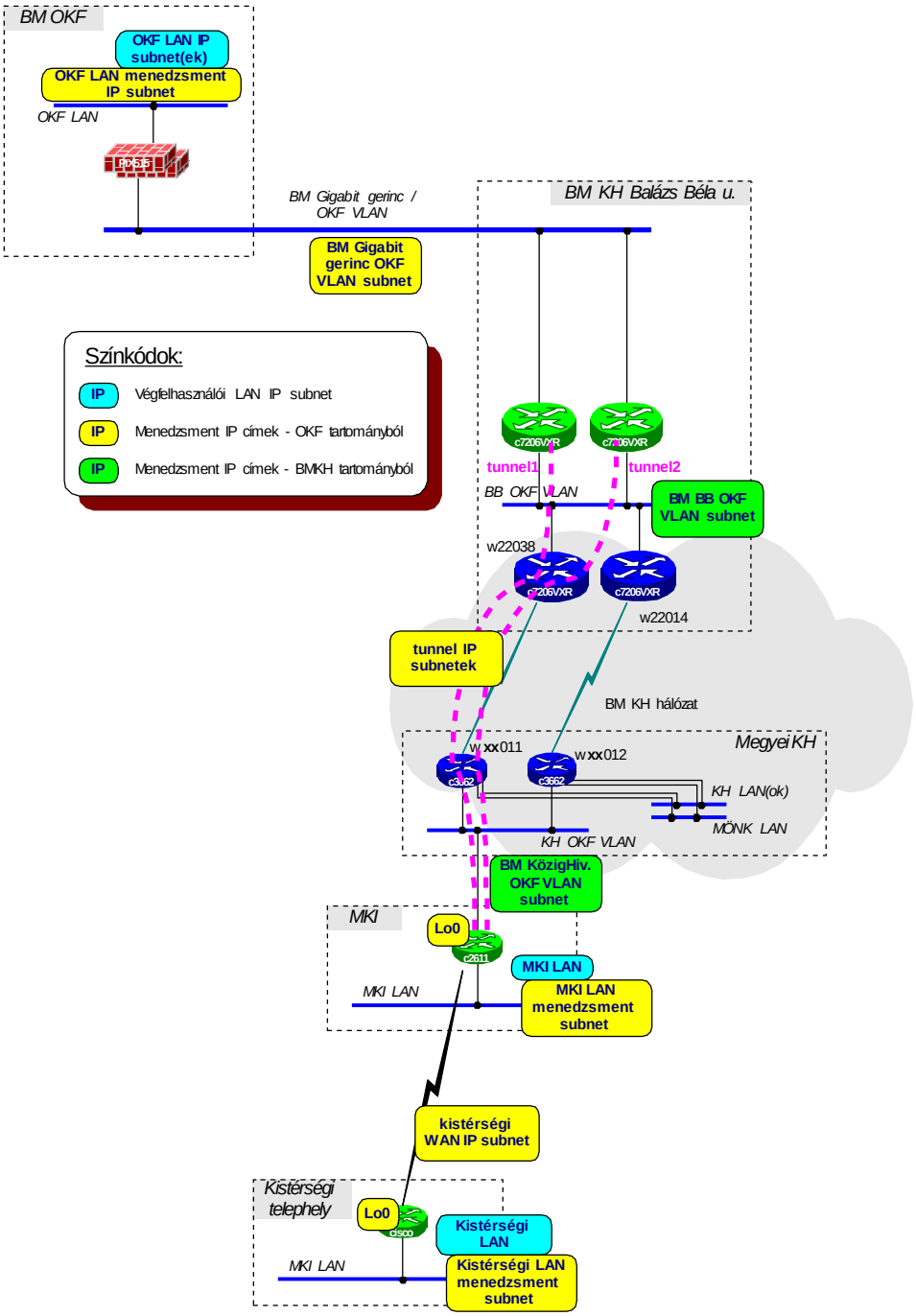
- Végrehajtottuk a MKI helyi hálózatának kiépítését, illetve bővítését minimálisan 48 végponttal működő strukturált hálózat kialakításához.

A Tisza Projekt az alábbi főbb hardveres és szoftveres beruházásokat tartalmazta:

- 100 db DTKszámítógép
- 22 db UNIX Host
- 23 db szünetmenetes tápellátórendszer
- 20db 48 portos SWITCH és C2611 router
- 1 db redundáns PIX 515 tűzfal
- 3 db C4006 SWITCH központi kapcsoló
- 1 db RSA és ACS authentikációsrendszer
- igazgatóságok és közigazgatási hivatalok közötti 128 kbps-os bérelt vonal
- 7 igazgatóság esetén redundáns összeköttetésként mikrohullámú ÖK kialakítása
- 22 db SCO UNIX és 10 felhasználós ORACLE szoftver

A jelenlegi rendszer VLAN topológiája:





A megvalósított országos rendszer

A rendszer továbbfejlesztésének terve:

Központi és megyei adatbázis-kezelő és döntéstámogató program létrehozása:

A jogszabályi kötelezettségekből, alaprendeltetésből adódó feladatok végrehajtása igényli egy komplex, ugyanakkor jól hozzáférhető folyamatosan bővíthető adatbázis létrehozását.

A döntés előkészítése és azok támogatása igényli, hogy különösebb informatikai képzettség nélkül a felhasználók egyszerű metódus alapján hozzáférjenek a fontos adatokhoz.

Ennek alapja lehet az Oracle adatbázis-kezelő szoftver, amelyet olyan döntéstámogató programmá kell konvertálni, hogy biztosítsa a minden szintű, felhasználóbarát munkavégzést.

Az adatbázis létrehozásához adatfeltöltési és adatszinkronizációs segédprogramokat kell létrehozni és a fizikai feltöltést végre kell hajtani. A feltöltés mind a központi, mind a területi szervek szintjén történik. A megyei szinten gyűjtött adatok automatikusan kerülnek át az országos szintre.

A szakállomány oktatását emelt szintű képzés keretében, a végrehajtó állomány képzését regionális szinten kell tervezni.

A sávszélesség menedzsment követelményei igénylik, hogy a jelenlegi 128kbps-os sávszélességet a meglévő gócközpontok felé növeljük.

Polgárivédelmi kirendeltségek és irodák bekapcsolása és kiszolgálása

A Megyei Katasztrófavédelmi Igazgatóságokhoz és a Fővárosi Polgárivédelmi Igazgatósághoz tartozó 200 kirendeltség és iroda számára a központi adatbázisok on-line elérését lehetővé kell tenni, akárcsak a vonatkozó helyi adatok feltöltését a MKI-k felé. A kirendeltségek és irodák esetén 1-5 fővel kell számolni. Az MKI-hoz való csatlakozás a helyi adottságok figyelembevételével kétféleképpen valósulhat meg: a polgármesteri hivatalokban elhelyezkedő felhasználók a BM Közigazgatási Hivatal hálózatán, az egyéb helyszíneken lévő felhasználók önálló bérelt vonali kapcsolaton, vagy mikrohullámon keresztül érhetik el az MKI rendszerét.

A kirendeltségek és irodák csatlakozását a vonatkozó BM belső szabályozás figyelembevételével, biztonságos módon kell megoldani úgy, hogy egy MKI és a hozzá csatlakozó intézmények a hálózati gerincről leválasztva önállóan is képesek legyenek együttműködni.

Önkormányzatok bekapcsolása és kiszolgálása

Az előzetes felmérések alapján a felhasználók 70%-a a Polgármesteri Hivatalokban helyezkedik el. Terveink alapján a titkosított kapcsolat ezekben az esetekben az egyes gépekről egy-egy központi Virtual Private Network (virtuális magánhálózat, a továbbiakban: VPN) fogadó egységbe fut be.

Az itteni felhasználók a BM OKF hálózatát -az MKI-n keresztül- csak a megfelelő authentikációval érhetik el, a BM OKF hálózatának védelmét a megfelelő biztonsági megoldások támogatásával kell megvalósítani. A javasolt

megoldás szerint a BM OKF hálózatát -az MKI-n keresztül- elérő felhasználók csak erős, kéttényezős authentikációt használva kapcsolódhatnak a BM OKF hálózatához. A kapcsolat során titkosított adatátvitelre van szükség.

További igény az, hogy a BM OKF hálózatába már bekapcsolódott távoli felhasználókon keresztül ne lehessen hálózati támadást intézni a BM OKF hálózata ellen. Ennek elérésére olyan VPN megoldás kialakítására van szükség, amely biztosítja, hogy a BM OKF hálózatához való kapcsolódás közben más kapcsolatot az adott számítógép ne tudjon se fogadni, se indítani. Így a BM OKF hálózatához kapcsolódó számítógép a kapcsolat idejére kizárólag a BM OKF rendszerével kommunikálhat.

Az önkormányzati Hivatalokban levő felhasználók támogatását az OKF már meglevő, erős authentikációt (személyi azonosítást) biztosító RSA Ace Server bővítésével lehet megoldani. A nagyszámú felhasználó megbízható kiszolgálását a szerver redundáns kialakításával javasolt megvalósítani. Az egyes felhasználók részére az erős azonosításhoz szükségesek az ún. SecurID hardver tokenek, amelyek segítésével (8 időben változó numerikus karakter) az illetéktelen behatolás gyakorlatilag kizárható.

A felhasználók fogadását központi, speciális VPN koncentrátor végzi. Ez teszi lehetővé, hogy az egyes felhasználókra távolról Firewall beállításokat érvényesíthessünk. Ez a megoldás biztosítja azt, hogy a BM OKF hálózatára bejelentkezett távoli gépek más hálózati kapcsolatot ezen időszak alatt ne tudjanak létesíteni.

A BM OKF alárendeltségébe tartozó telephelyek bekapcsolása és kiszolgálása

A felmérések alapján 20 %-nyi, mintegy 28 telephely bérelt vonali, vagy mikrohullámú bekötésére van szükség. A bérelt vonalas megoldás (akárcsak a mikrohullámú) alapul szolgálhat a későbbiekben az IP alapú hangátviteli bővítésnek. Így jelentős megtakarítások érhetők el a telephelyek telefonforgalmának költségeiben. (Az IP alapú hangátviteli bővítés lehetőséget a jelenlegi hálózat is támogatja.)

A felhasznált eszközök esetében fontos szempontok a menedzselhetőség és az egyszerű üzemeltethetőség, valamint, a BM hálózati koncepciójába illeszkedés. A bővítések során a meglévő bérelt vonali sávszélességek bővítése szükséges.

Hálózat rendelkezésre állásának növelése

A hálózat éves rendelkezésre állásának meg kell haladnia 99,5%-ot, a minősített időszakokban a hálózat működésének folyamatossága kiemelt fontosságú, ezért a KOIR rendszer alapvető egységeinek és adatátviteli útvonalainak redundanciájára kell törekedni.

Figyelembe kell venni azt, hogy az éves 99.5 %-os rendelkezésre állás maximálisan 43 óra kiesést eredményezhet. Amennyiben ez a kiesés minősített

időszakban történik, úgy, súlyos problémák keletkezhetnek, hiszen ez gyakorlatilag 2 napnyi folyamatos kiesést jelent.

A redundancia vonatkozik az adatátviteli útvonalakra és a hálózati útválasztókra is. A redundáns adatátviteli útvonal az elsődlegestől független backup útvonalon (második on-line kapcsolat – belügyi mikrogerinc hálózat, vagy ISDN hívás) keresztül valósul meg.

Az ISDN backup megvalósításához az egyes BM OKF routereket ISDN kártyával kell bővíteni. A központban a rendszerhez integrálható, IPsec titkosításra képes fogadó routert kell telepíteni, ISDN PRI szolgáltatói kapcsolatokkal.

A másodlagos útvonal terhelésmegosztással lehetőséget biztosít a minősített, megnövekedett adatforgalom kezelésére is (minősített időszakon belül automatikusan kiépül a kapcsolat a BM OKF felé a sávszélesség-igény növekedésével párhuzamosan).

Az alkalmazások válaszidejének hálózati garantálása

A WAN (Wide Area Network, nagy kiterjedésű hálózat) hálózatok esetében fontos, hogy a kritikus alkalmazások preferenciát élvezzenek az átviteli útvonalakon. A nem kritikus applikációk sokszor a WAN kapcsolatok sávszélességét indokolatlanul foglalják el.

A sávszélesség-menedzsment kérdése ezért minden hálózatban fontos kérdés, ennek segítéségével ugyanis esetenként jelentős költség takarítható meg.

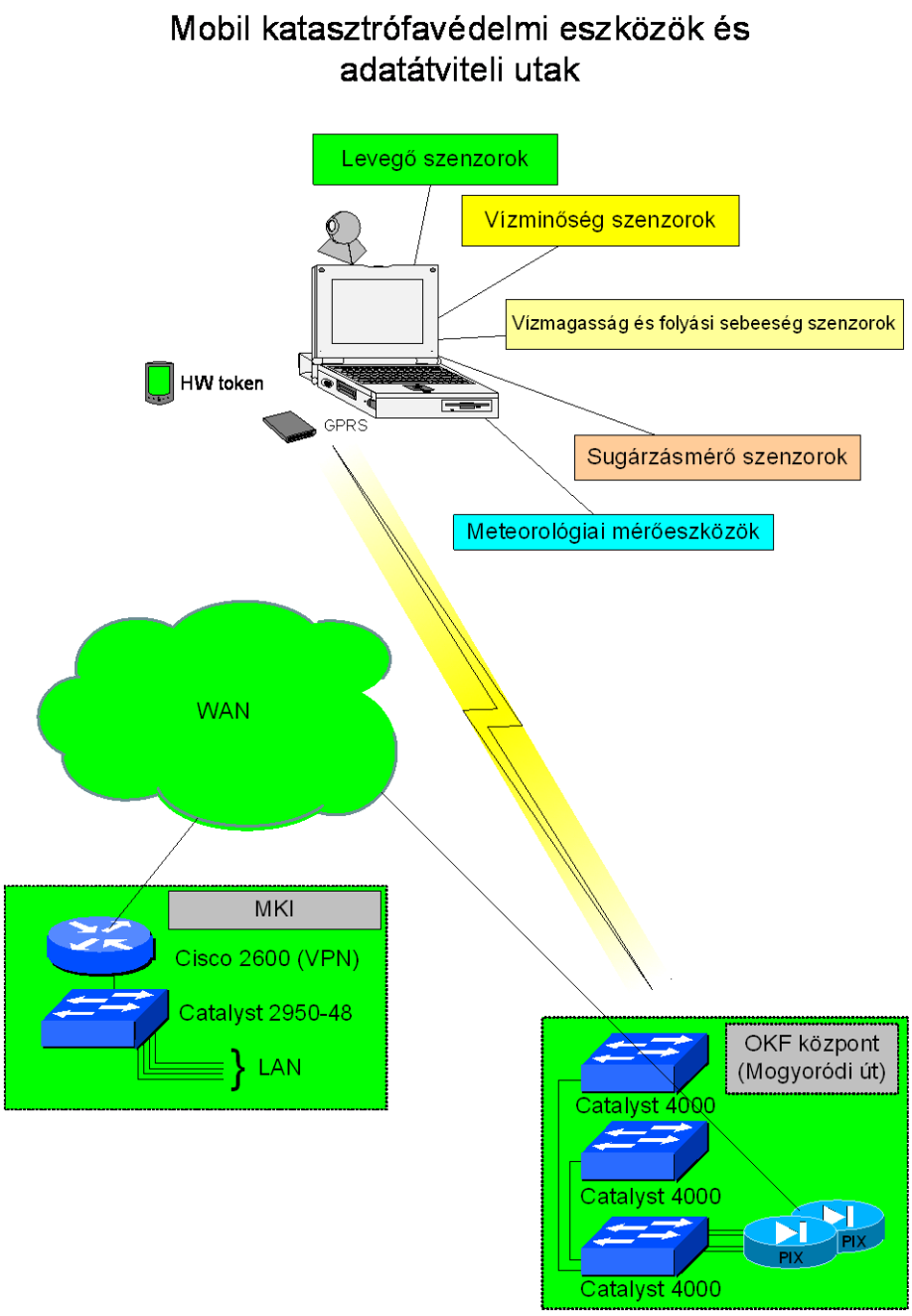
A sávszélesség-menedzsment központi megvalósítása lehetővé teszi, hogy segítségével minden távoli telephely forgalma optimalizálható legyen. A működés szempontjából kritikus alkalmazások előnyben részesülnek. A sávszélesség menedzsment lehetővé teszti a WAN kapcsolatok kihasználtságának figyelését is, így akár az egyes alkalmazások, szerverek, vagy felhasználók forgalmának ellenőrzését is megvalósíthatjuk.

Külső kapcsolatok fogadása

A hatékony katasztrófavédelem és katasztrófa-elhárítás független szervezetek szoros együttműködésével valósulhat csak meg.

Az adatcseréhez szükséges külső kapcsolatok fogadására mind központi mind MKI szinten fel kell készülni. A KOIR rendszer elérését szabályozottan, a belső hálózaton lévő adatok védelmének figyelembevételével kell megvalósítani.

A külső kapcsolatok esetén fel kell készülni a bérelt vonali, és behívásos rendszerek támogatására is.

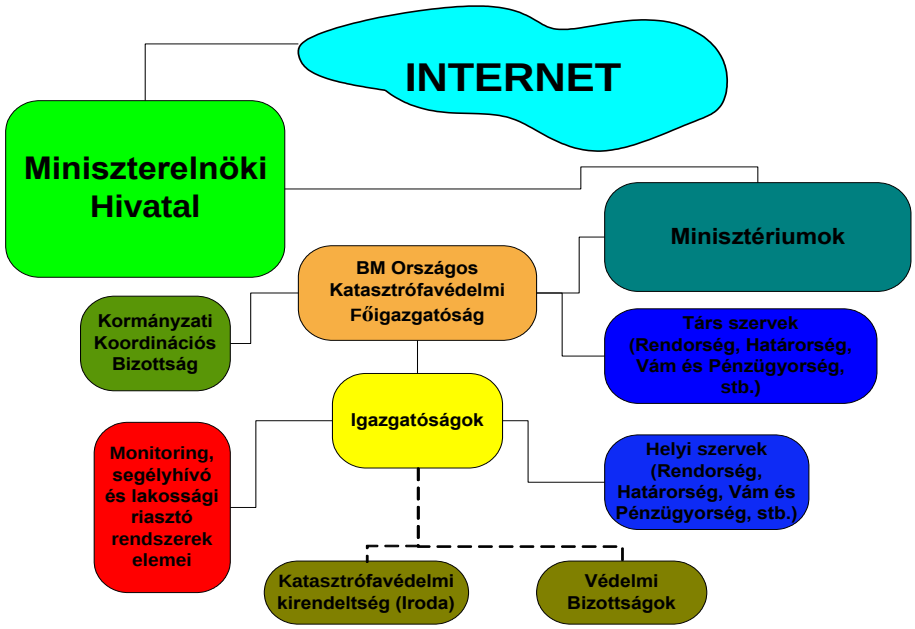

Mobil katasztrófavédelmi eszközök és adatátviteli utak
Levegő szenzorok
Vízminőség szenzorok
Vízmagasság és folyási sebeség szenzorok
HW token
GPRS
Sugárzásmérő szenzorok
Meteorológiai mérőeszközök
WAN
MKI
Cisco 2600 (VPN)
Catalyst 2950-48
LAN
OKF központ
(Mogyoródi út)
Catalyst 4000
Catalyst 4000
Catalyst 4000
PIX
PIX

A külső kapcsolatok szempontjából fontos az Internet, mint kommunikációs közeg. Hálózatbiztonsági megfontolások alapján a csatlakozás csak központon keresztül, a BM által biztosított felületen, jól védett kijáraton lehetséges.

A külső kapcsolatok esetében fontos szempont, hogy az ezeket egy, a DMZ-ben (Demilitarised Zone) levő, független router fogadja. Az adatszolgáltatásnak is a BM OKF belső rendszerétől független, DMZ-ben elhelyezett szervereken kell megvalósulnia.

Tárcaközi (kormány szintű) informatikai kapcsolódások terve

Információ csere lehetőségét kell biztosítani az Országos Katasztrófavédelmi Főigazgatóság és az együttműködési megállapodásokban és más a katasztrófavédelem működését szabályzó utasítások, intézkedések által meghatározott szervekkel.



Az adatbázis-kezelő rendszerekkel szemben támasztott követelmények:

Biztosítsa a

- különféle igények hatékony kielégítését,
- az adatbázis következetességét, vagyis, hogy csak valós adatokat tárolhat,

- az adatbázisbeli valamennyi adat elérését, (ezt egy filekezelő rendszer nem teszi meg)
- adatfüggetlenséget, (fizikai és logikai függetlenséget)
- adatok közti komplex kapcsolatok kezelését és ábrázolását,
- redundancia mentességet és annak ellenőrzését (ne szerepeljen az adatbázisban többször is ugyanaz az adat),
- az adatok védelmét, [mind fizikai, mind emberi (véletlen vagy szándékos rongálás) értelemben]
- helyreállíthatóságot,
- több felhasználós rendszerekben az egyidejű hozzáférést (tranzakciókezelés),
- osztott adatbázisokban az adatok szétosztását, kereshetőségét,
- az adatforgalom optimalizálását.

Hardver és szoftver feltételek, szükséges rendszer integrációk

Kifejlesztésre kell, hogy kerüljön a katasztrófahelyzetek megelőzése, felszámolása érdekében alkalmazható integrált adatbázisra épülő döntés előkészítő és támogató rendszer, amelynek alapját képezheti a már fejlesztés és adatfeltöltés alatt álló térinformatikai program.

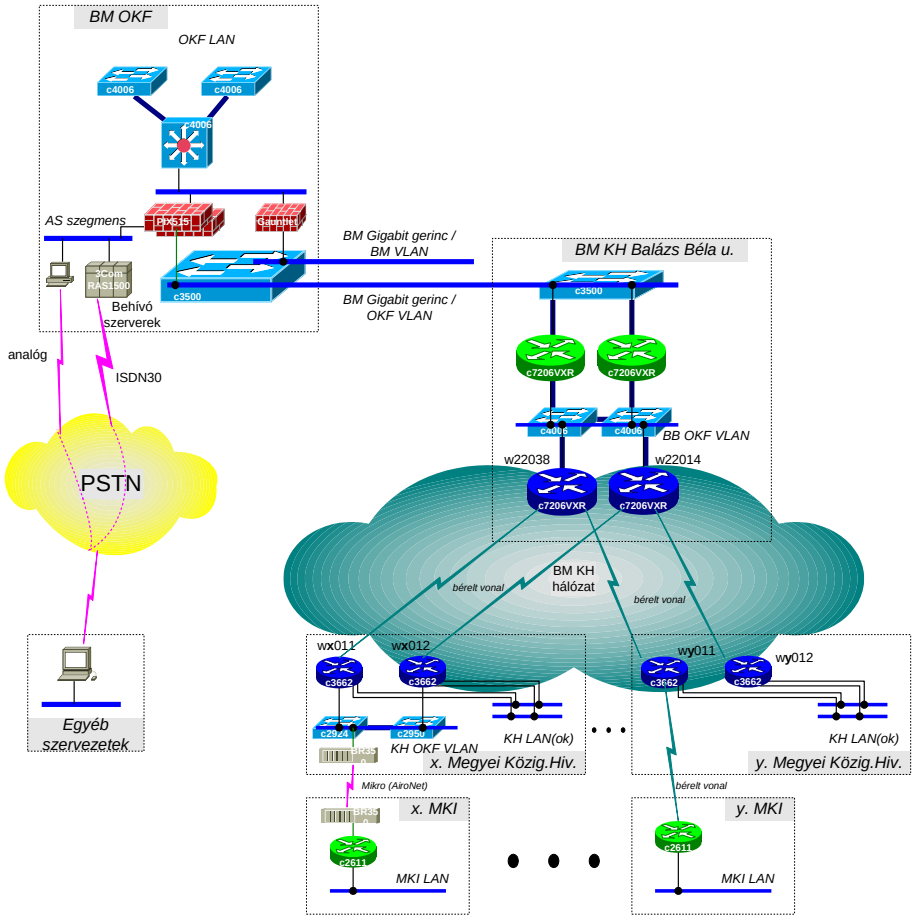
A Megyei Katasztrófavédelmi Igazgatóságokon, illetve az Országos Katasztrófavédelmi Főigazgatóságon alkalmazott ArcView 3.2 GIS szoftver megfelelő hátteret és felületet biztosít. Használatával megoldható a térképi ábrázolás és lekérdezés mellett az adatok gyors, célorientált, szelektív lekérdezése, értékelése.

A társszerveknél meglévő térinformatikai adatbázisok konverziója miatt szükség van rendszerillesztési feladatok megvalósítására is.

A rendszer képes arra is hogy „maga alá" integráljon azonosító, nyilvántartó, terjedésmodellező és kommunikációs programokat is.

Megfelelő térképi alapot biztosíthat a Transcarphatian Information Management System keretén belül feldolgozott hazai, nemzetközi térkép és adatbázis.

A veszélyes áruk fuvarozásának ellenőrzése, mint jogszabályi kötelezettség jelenik meg az informatika oldaláról is. A katasztrófavédelmi szempontú informatikai támogatás hardver feltételeit a nyomkövető rendszerekkel kell megoldani. Tervezzük mintegy ezer darab GPS alapú nyomkövető berendezés beszerzését és a hálózathoz történő csatlakoztatását.



A KOIR adatkapcsolati felépítése

A lakosság biztonsága égetően követeli meg olyan mobil, vegyi, sugárbiológiai állomás működtetését (pld: ANTHRAX), amelyet szintén be kell kapcsolni az informatikai hálózatba, ezek nagy pontosságú laboratóriumi műszereket (szondákat) és minden terepi viszonyok között jól működő eszközöket jelentenek a mobil kapcsolataikkal együtt.

Katasztrófaveszélyes helyzetek felderítése, a bekövetkezett események felmérése és helyre állítás megszervezése érdekében szükség van bárhol bevethető légi eszközökre, rájuk szerelt kamerákkal, hőérzékelőkkel, szondákkal, távközlési és informatikai eszközökkel.

Valamennyi a rendszerbe bekapcsolt szervezetet megfelelő erőforrás kezelő modullal (license-szel) kell ellátni.

A nukleáris balesetek időbeni megfigyelése és a következmények elhárítása igényli a jelenlegi mérőszondák hálózatának jelentős növelését.

Technikai eszközökkel történő ellátás

Főigazgatóság:

- Szerver termek kialakítása (beléptető rendszer, riasztó rendszer, klimatizálás, stb.)
- Nagybiztonságú központi adattárolók
- Személyi számítógépek és kiegészítők

Igazgatóságok:

- Szerver termek kialakítása (beléptető rendszer, riasztó rendszer, klimatizálás, stb.)
- Behívó rendszer (CACS, RSA)
- Tűzfal (PIX)
- Személyi számítógépek és kiegészítők

Kirendeltségek (Irodák):

- Személyi számítógépek és kiegészítők

Összegzés

A Katasztrófavédelmi Országos Információs Rendszer kialakításának és fejlesztésének fő célja az, hogy megteremtse a lehetőséget a jogszabályi előírások hatékony, gördülékeny teljesítésére, elősegítse a hatósági és veszélyhelyzet-kezelési tevékenységet, valamint az önkormányzati felkészülést, a lakossági tájékoztatást és a környezet magasfokú védelmét a veszély- és katasztrófahelyzetek kezelése során.

Dr. habil SÁNDOR Miklós

MI LESZ VELED … EMBERKE? AVAGY A TISZTKÉPZÉS JÖVŐJE?

I.

Ez évben jelent meg a HM 20/2002 (IV. 10) rendelete, mely szabályozta az egyes beosztások betöltéséhez szükséges, az azokhoz kapcsolódó szakmai, végzettségi, idegennyelv-ismereti, egészségi, pszichikai és fizikai alkalmassági követelményeket.

A rendelet tartalmazza, illetve meg határozza, hogy mely beosztás betöltéséhez milyen követelmények kapcsolódnak. A beiskolázások szempontjából ez egyfajta korlátot jelent. Ráadásul két azonos rendfokozatnál sem azonosak a követelmények. Pld. alezredes – egyetemi végzettség az egyik helyen, a másiknál főiskolai végzettség szükséges. Nem furcsa?

Tisztjeink egy jó része nem rendelkezik megfelelő nyelvvizsgával és ez is csökkenti a beiskolázhatóságot. És akkor nem beszéltünk a családi háttérről.

Nagyon jó képességű fiatal tisztek nem jelentkeznek nappali képzésre, mert **1.)** féltik a meglévő beosztásukat, az előrelépés lehetőségét; **2.)** bizonytalan, hogy végzés után az új helyőrségben feleségnek lesz-e munkahelye, a gyermeknek megfelelő iskolája stb., (ha nem keres annyit egy tiszt, hogy egy keresőként el tudja tartani a családját, hogy minden idegszálával a „sereg" érdekeit szolgálná és ne kenyérgondjai legyenek, ha a felesége nem dolgozik.) Arról még nem is beszéltünk, hogy a feleség is féltheti szakmai előmenetelét, karrierjét, ami a versenyszférában gyorsabb és jövedelmezőbb, mint a férjéé.

És ez csak az érem egyik oldala. Vizsgáljuk meg egy kicsit a másikat is!

Hiába szeretne bárki tanulmányokat folytatni, hiába ér el a felvételi vizsgán kimagasló eredményt, tanulni csak akkor tanulhat, ha a parancsnoka — a döntési helyzetben lévő parancsnok — engedélyezte a tanulmányok megkezdését.

II.

Lehet, hogy felületesen olvastam a törvényt, vagy nem tudtam felfogni az abban foglaltakat, de a 2001. évi XCV törvényben, amely a Magyar Honvédség hivatásos és szerződéses katonáinak jogállásáról szól, nem találtam olyan kitételt, hogy az egyetemet végzetteket egyetemi végzettséghez kötött beosztásba KELL! helyezni.

Sőt azt sem találtam a törvényben, hogy a parancsnoka csak! azt javasolhatja továbbtanulásra, akinek végzés után egyetemi végzettséghez kötött beosztási helyet tud adni.

A törvény 1. számú melléklete szerint a főtisztek: őrnagy, alezredes, ezredes. Akkor nem értem, hogy az őrnagy miért nem végezhet egyetemet, ha már főtiszt.

Két paragrafusát szeretném idézni a törvénynek, amelyek rávilágítanak a helytelen gyakorlatra.

80§ „A magasabb beosztás betöltéséhez szükséges iskolai végzettség megszerzését hazai, vagy külföldi … iskolarendszerű, vagy iskolarendszeren kívüli oktatási (képzés) keretében kell biztosítani. A beiskolázásra pályázat, vagy kijelölés útján kerül sor. Emellett lehetőséget kell adni a szolgálat tagjának a szolgálati érdek sérelmével nem járó, saját elhatározáson alapuló egyéni továbbtanulásra is."

81§ "Ha a továbbtanulás nem kapcsolódik közvetlenül a beosztáshoz, vagy a tervezett előmenetelhez, a képzéssel összefüggő támogatás csak tanulmányi szerződés alapján biztosítható …".

Nincs benne szó sehol tiltásról, semmilyen diszkriminációról. Pláne, ha a tiszt saját felkészültségét, szakmai ismereteit gyarapítandó akar az egyetemen továbbtanulni.

Lépést (szemléletet) válts!

Kinek képzünk?

Kinek képzünk? — tesszük fel sokan a kérdést baráti vagy félhivatalos beszélgetéseken. A megrendelőnek, saját magunknak, a polgári életnek, vagy kinek? Milyen őrült, kétségbeesett gondolat két diplomát adni a fiatal tiszt kezébe? Egy diploma nem elég? Egy tiszti diploma, amely arról szól, hogy a fiatal fel van vértezve mindazon tudással, amely egyfelől a haza fegyveres védelmére predesztinálja, másfelől tanúsítja, hogy szakmailag jól felkészült, szakmájának ugyanolyan értője és művelője, mint az a fiatal, amelyik polgári egyetemen, vagy főiskolán kapta meg az oklevelét.

Sokan felkapják, felkapnák erre a fejüket. Hüledeznének, felháborodnának, hogy „Milyen eretnek ötlet, gondolat!" — ki fog jönni ezek után — ha megvalósul — tiszti pályára!

Kettős a válaszom!

1. Meg kell teremtenie a politikának a pálya presztízsének feltételeit, a pályán lévőknek pedig ki kell harcolniuk a társadalom elismerését.
2. Olyan teljesítőképes tudást kell adni a diploma mellé, hogy az ekvivalencia ne lehessen kérdés a polgári életben.

Nem csak az intézményt, hanem a karokat, szakokat és szakirányokat is el kell tudni fogadtatni a polgári felsőoktatás szereplőivel. Ki kell követelnünk helyünket a tudományos közéletben és meg is kell védenünk azt.

Jól illik e képbe a Katonai kommunikációs rendszerszervező tanszék évi rendes nemzetközi szakmai tudományos konferenciája, melyen a polgári távközlés és a távközlési piac ismert és elismert szereplői szívesen vesznek részt évről-évre.

Tehát magas szintű elméleti és gyakorlati tudás a MEGRENDELŐ, a HM igényei alapján.

Meg kell alapozni egy életpályát, amely a permanencián, az állandó, folyamatos tanuláson, önképzésen, képzésen alapul. Mint köztudott, a megszerzett tudás egy része 5-10, de egy más része 2-3 év alatt elavulttá válik. Ezért is kell az alapképzésre felépíteni egy továbbképzési rendszert.

Ennek az alapnak nagyon szilárdnak, erősnek kell lennie, hogy elbírja a felépítmény súlyát. Hogy milyen legyen az alapozás? Hány évig tartson? Egyetemi vagy főiskolai kimenettel induljon? Ez mind-mind érdekes, átgondolandó, megvitatandó kérdés. De nem lehet elodázni, sokáig várni!

Miért? Mert a szakterület jelentős változáson, mondhatni robbanásszerű változáson megy keresztül, ennek alapvető indoka, oka a konvergencia. Mi is ez a konvergencia, amitől egyesek — szakmai féltékenységből — lekicsinylőleg beszélnek, mások viszont fennen hangoztatják, zászlóvivői a változtatás szükségességének. Csak zárójelben jegyezném meg, hogy tanszékünkön intenzíven 7-8 éve foglalkozunk a kérdésekkel, melyek eredménye többek között a 4 éve elindított egyetemi alapképzésünk is. Más kérdés, hogy parancsra két évfolyam elindítása után a képzés folytatását le kellett állítanunk — ez a képzésünk jelenleg kifutó képzés.

Visszatérve a konvergenciára. Ki, illetve mi konvergál kivel, illetve mivel?

Az informatika a távközléssel. Így, ennek hatására jöttek elő olyan fogalmak, mint az infókommunikáció, a telematika stb. Ha nagyon vulgárisan akarom a telematikát megfogalmazni, akkor azt mondom, hogy a telematika nem más, mint a távközlés és az informatika viszonyrendszerének közös része. Legfontosabb feladatán — az információk feldolgozásán, kezelésén és transzportálásán — túl az információ szükségletek kielégítése, esetlegesen az ilyen szükségletek teremtése. Igazi jelentőségük abban áll, hogy alapját, nélkülözhetetlen részét képezik számos gazdasági és társadalmi változást eredményező folyamatnak, csúcstechnológiák létrejöttének. Négy hierarchia szintre épülve egy összekapcsolódó egységet képeznek a hálózatok, a szolgáltatások, a végkészülékek és az alkalmazások szintjén.

Ezek megvalósulásában meghatározó szerepe van az ország gazdasági helyzetének, a nemzetgazdaság fejlettségének, illetve az ország szellemi potenciáljának, az ország szellemi tőkéjének.

És így kanyarodtunk vissza az eredeti kérdéshez, a képzéshez.

Egy olyan kis nemzetnek, mint a miénk, csak egy azaz egy jelentős kitörési pontja lehet — ha természeti kincsekben, s minden másban szerények a lehetőségei —, ha fejleszti az egyetlen kincsét, a kiművelt emberfők sokaságát, a teremtő, alkotó, cselekvő szürkeállományt.

Az invesztáció pénzbe kerül. Nagyon sok pénzbe. Egy ilyen kis nemzetnek, mint mi vagyunk ez egy óriási esély, egy nagy lehetőség a felemelkedésre, a régióból való kitörésünkre. Ahogy igaz ez az országra, sokszorosan igaz a hadseregre is!

És most térjünk vissza a kinek képzünk kérdésre.

A megrendelőnek — szerintem — nagy általános és szakmai műveltséggel rendelkező, szilárd katonai tudáson alapuló katonai vezetőkre van szüksége, ha a tisztképzést ragadjuk ki a képzés–felkészítés rendszeréből.

Olyan katonai vezetőre, aki mestere, művelője a hadi tudományoknak, és szakmájának.

Mindenki olyan szakembert kell, hogy képezzen, amire predesztinálva van.

Saját szakmámról beszélve, és nem átmutogatva a szomszéd zöldebb fűvére:

A Katonai kommunikációs rendszerszervező tanszék az egyetemi alapképzésben katonai vezetőket, nem mérnököket képez. Olyan katonai vezetőket, akik ismerik a szakma csínját-bínját, de elsődlegesen katonai vezetők! Amit a villamosmérnöki képzésben résztvevők elsajátítanak, azt az elméleti tudásanyagot elsajátítják ők is, sőt többet is. Ők 5 év alatt szerzik meg azt a tudást, amihez a főiskolát végzetteknek 7, illetve 8 év szükséges. Hosszútávon melyik a kifizetődőbb? Az olcsóbb? Baj az, ha a hadnagynak egyetemi végzettsége van és csak a karriertanfolyamokat kell elvégeznie ahhoz, hogy előrehaladása biztosított legyen? (Természetesen jó munkavégzés mellett.)

Most hatalmi szóval deklarálta a politika, igen a politika, mert véleményem szerint katona ilyet nem mond, hogy egyetemi végzettség csak alezredeseknek jár. Enyhén szólva nem értem.

Nem értem ezt a szűklátókörűséget, vagy nevezhetném bűnnek is, kicsinyes emberi bosszúnak is. Nem elég, hogy a rendfokozatokat — az egyes beosztási helyeket — visszavették az ún. piramis elv miatt, de a beosztásokhoz kapcsolódó iskolai végzettségeket is visszavonták. Miért kell félni?! attól, hogy a katona művelt, nagy tudással rendelkezik?

Miért nem rendelkezhet egyetemi végzettséggel és ismeretekkel pl. az a főhadnagy, akinek munkájához szükséges lenne az egyetemi szintű ismeret. Csak mást ne mondjak a digitális rendszerekben a hálózat-felügyeleten dolgozók, akiknek dönteniük kell, pl. a tábori rendszerekben hadműveleti kérdéseket érintve is, amelyeket tanfolyamokon nem lehet elsajátítani.

Mindenki végezze a saját munkáját. A műszaki egyetem képezzen mérnököt, a nemzetvédelmi egyetem katonai vezetőt.

Jelenlegi ismereteim szerint ma a polihisztorképzés nem megvalósítható, illetve nagyon-nagyon hosszú ideig tartó folyamatként lehetne csak számításba venni. Talán …

Ma specialistákat kell képezni. Olyan specialistákat, akiknek megfelelő alapismereteik vannak és képesekké válnak tovább- és átképezni magukat, új és új ismereteket, szakmaiakat és általánosakat szerezni, azokat alkotó módon felhasználni.

Milyen képzési struktúrát képzelek el ezután a sok mormorandusz után.

Az előbb már szóltam arról, hogy a szakmának elsődlegesen szakmailag jól képzett vezetőkre és nem mérnökökre van szüksége. Bár a kettő nem zárja ki egymást.

A másik argumentum a 4+2, illetve a 4+3 az mindig több mint az 5, mely a négyéves főiskolai és a kiegészítő egyetemi alapképzés nappali és levelező ideje, összevetve az ötéves egyetemi alapképzéssel.

A harmadik az, hogy egy magas szintű alapképzés után a tisztek rendszeresen részt vennének a különböző karriertanfolyamokon közös érdekeltség alapján — az egyén– és a hadsereg — nem elszakítva a családtól. Ha valaki vállalja a magasabb beosztást, akkor vállalja a képzést, vállalja a költözést és mindent, ami ezzel jár.

Milyen is lenne ez a képzés? Egy változata a következő kettő lehet:

Kommunikációs rendszerszervezők képzése

Ötéves egyetemi alapképzés, melyben a katonai alapképzésen túl általános–, általános katonai, rendvédelmi–, szakközös szakirányú ismeretek és szakmai gyakorlat szerepel:

- az általános ismeretek ~ 12%;
- az általános katonai rendvédelmi ismerek ~ 18%;
- szakmai ismeretek (szak és szakirányú) 70%-át

teszik ki a képzési időnek. A szakmai ismeretek magunkba foglalják a 4x4=16 hét csapat (szakmai) gyakorlatot is.

Mivel kommunikációs rendszerszervező a képzés, a szakmai órák jelentős informatikai ismereteket is magunkba foglalnak.

A továbblépés feltétele egy szakirányú továbbképzési szak indítása. Itt a tantárgyak, a szaktárgyak aránya közel azonos 50-50%. Kimunkálása most van folyamatban az informatikai tanszékkel közösen.

Szintén kidolgozás stádiumában van egy kommunikációs alapképzési szak kimunkálása, melyben az informatika és a hírközlés azonos súlyú.

Természetesen ennek a szakirányú továbbképzési szakának kimunkálásán is dolgozunk.

Miért van erre szükség?

A konvergenciáról más helyen már szóltam Az információs robbanás a hadsereget sem kerüli el. A parancsnoknak minél több használható, értékelhető, valós idejű információra van szüksége az eredményes tevékenység vezetésére. Az információ transzportálásához, az értékelés feltételrendszerének biztosításához járul hozzá az ICIS, az integrált kommunikációs és informatikai rendszer, amelyben elmosódnak a határvonalak és csak nagyon nehezen, mondvacsinált módon lehet megmondani, állítani, hogy hol végződik az egyik és hol kezdődik a másik.

Ezzel a képzési formával két nagyon fontos szakterület szakemberképzése valósulna meg. Képesek lennének mind a hírközlési, mind az informatikai szakfeladatok megoldására, a feladatok végrehajtására. A programozók és a

villamosmérnökök képzése továbbra is a szakirányú egyetemeken történne. Hozzá kell tenni viszont, hogy ez a létszám MH szinten sem jelentős, mintegy 15-30 főt tehet ki.

A tanulás ma már végig kell, hogy kísérje egész életünket. A következő években, évtizedekben óriási segélyt kínál az e-learning annak, aki hajlandó könyvet, vagy egyéb információhordozót a kezébe venni, hajlandó képezni magát, hajlandó tanulni.

Mi is ez? Miről van szó?

A hatékonyság növelésének egyik legfontosabb eleme a képzés. Ennek intenzifikációja egy külön tanulmányt érdemelne. Mivel az oktatás is — mint sok minden más — idő és pénzigényes tevékenység, ezért törekedni kell a lehető leghatékonyabb megvalósítására. Pl. a felkészítés ésszerű megtervezésével, az oktatandó, tanulmányozandó anyag gondos kiválogatásával, rendelkezésre álló idő hatékony kihasználásával, korszerű módszertan és segédeszközpark alkalmazásával, a tapasztalatok elemzésével, kutatásával stb., stb.

Különösen fontos szempont a hatékonyság saját szakterületünkön, ahol a megszerzett tudás 3-5 év alatt elavult, ráadásul félévente, évente frissítést igényel!

A hagyományos képzésben a tanár, az oktató és a hallgatók között teljes kommunikáció — kétirányú — alakul ki. Ez remek. Hátránya a jelentős idő– és költségráfordítás.

A távoktatás már régóta jelen van a képzési formák között, újabban megjelent változata a papírt és nyomdai kapacitást kímélő CD ROM alapú változata. Tanszékünkön jelenleg is folyik az oktatási anyagok CD-re „írása". A távoktatás nagy előnye a rugalmasság és az alacsony költségek, hátránya viszont az alacsony–szintű kommunikáció a tanár és a hallgatója között.

Az e-learning a két megoldás előnyeit egyesíti. A lényege az, hogy folyamatában az oktató és a hallgató között élő párbeszéd alakul ki az Internet és az Intranet rendszereken, hálózatokon keresztül és a tananyag is on-line módon jut el a hallgatókhoz.

Az e-learning fő területei a szinkron és az aszinkron e-learning.

A szinkron e-learning esetében a hallgatók és a tanár egy időben vesznek részt a képzésen. A résztvevők a számítógép monitorja előtt ülve látják a tanár által bemutatottakat és hallják a hozzájuk fűzött magyarázatot is. Interaktívan részt vehetnek az órán, jelentkezhetnek szóban és írásban, válaszolhatnak a tanár kérdéseire, teszteket tölthetnek ki stb., stb. Előnye, hogy a tanár és hallgatósága között magas fokú kommunikáció és interaktivitás alakul ki.

Legjobban ez a forma közelíti meg a tantermi oktatás hatékonyságát. Hátránya lehet az időbeni kötöttség.

Az aszinkron e-learning lényege az, hogy a tananyag online formában áll rendelkezésre. Az oktató és a hallgatók közötti kapcsolat intenzív, de az okta-

tás időben nincs szinkronizálva, a tananyag a megszabott időhatárokon belül egyéni ütemben sajátítható el.

A különböző tesztek, végrehajtandó feladatok jelentik a kommunikációt és az interaktivitást. E képzési formának legfőbb előnye a rugalmasság, hátránya az alacsonyabb kommunikációs szint.

Az e-learning felhasználásának feltétele egy multimédiás PC, amelyik Internet eléréssel rendelkezik. Az alkalmazások majd mindegyike szinte csak ingyenes, opcionális szoftvereket igényel, többségük már a már átlagos modemsebesség mellett is élvezhető minőséget ad.

A szervekre, a menedzsment-rendszerre, a hallgatók regisztrációjára, a tananyagokhoz való hozzáférésre, a vizsgák eredményeinek rögzítésére és még sok minden másra, ami a témához tartozik e tanulmányban nem akarok kitérni.

És még valamit a képzés jövőjéről

Természetesen szigorúan a magánvéleményem erről a kérdésről. Ha már új struktúrával el akarják sorvasztani a jelenlegi képzést a hadmérnöki — beindításával — mint ennek hangot is adtak az Egyetemi Tanács szeptemberi ülésén — akkor egy igazi, nagy lépést kellene megtenni, amely egy ilyen kis hadseregnek, mint a miénk, biztosan előnyére válna.

Elöljáróban el kell mondanom, 1.) hogy nem én találtam ki, 2.) ez a rendszer már hosszú évek óta működik, egy kicsi, de erős hadseregben — Görögországban.

A tisztjelöltek a négy éves főiskolai képzésben elsajátítják mindazokat a vezetői ismereteket, amelyeket egy katonai vezetőnek ismernie kell. Mesteri kezelőivé válnak az összes rendszeresített fegyvernek, minden harc– és gépjármű vezetését elsajátítják, nyelveket tanulnak, és fizikai felkészítésükre nagy hangsúlyt fektetnek. Az általános értelmiségi tárgyakról itt és most nem szólok.

Végzéskor — a hadsereg igényeinek megfelelően és a hallgatók előmenetele alapján döntik el, hogy ki, milyen beosztásba kerül, ki lesz lövész, tüzér, híradó stb. Ezt követően a tisztet különböző időtartalmú képzéseken vesznek részt és lesznek lövész, tüzér, híradó stb. parancsnokok.

Innen hasonló a felépítés → karriertanfolyamok, akadémia, vezérkari akadémia.

Igaz a főiskolán nem kapnak mérnöki diplomát a végzett hallgatók, de katonák lesznek, akik a hadsereg bármely! tiszti beosztására képesítettek a logisztikustól a harckocsizóig oda és vissza. Természetesen ez a szárazföldi haderőre igaz, a haditengerészetnek és légierőnek megvannak a saját iskoláik. A mérnököt, és egyéb speciális felkészültséget igénylő szakembereket a polgári egyetemek képezik a kor követelményeinek megfelelően, évtizedes, talán évszázados tapasztalatok alapján.

Szerintem ez is egy járható út lenne. Egy viszonylag olcsó járható út.

Befejezés

Égető, sürgető feladatok:

- ismételten át kellene tekinteni, ki kellene jelölni a tiszti és főtiszti munkaköröket;
- át kellene tekinteni, módosítani kellene az egyetemi végzettséghez kötött munkaköröket;
- a változásoknak megfelelően módosítani kellene az állománytáblákat;
- újra kell gondolni az előmeneteli és képzési (át– és továbbképzések) rendszerét, szükséges megteremteni a karriertanfolyamokat, az előrelépés, a továbbjutás feltételeit.

A képzési struktúra kialakítása érdekében újra kell gondolni a követelmény– és feladatrendszert.

A képzés többek között:

- szorosan kapcsolódjon az előmeneteli rendszerhez, de ne legyen a gátja;
- mindig a szervezet igényeit elégítse ki elsődlegesen!;
- biztosítsa a különböző beosztások közötti átjárhatóságot;
- bázisa legyen a korszerű oktatási módszerek alkalmazásának és fejlesztésének.

A képzés rendszerével meg kell valósítani az egész életre kiterjedő — lifelong — szakképzést.

Ennek egyik módszere lehet az e-learning.

Köszönöm a figyelmet!

MAROS Dóra[11]

MINŐSÉGBIZTOSÍTÁS A TÁVKÖZLÉSBEN

A magyar távközlési piac új kereteinek formálódásakor elengedhetetlen követelményként és elvárásként jelentkezik a minőségbiztosítás kérdése, amely nem pusztán a magyar fogyasztók és szolgáltatók érdekeinek védelmét jelenti, hanem az ország Európai Uniós csatlakozásának is egyik fontos eleme. A tanúsító szervezetek létrejötte a távközlés terén az Európai Unió gyakorlatának megfelelő piacfelügyeleti koncepció része. A koncepció a Távközlési törvényben és a hozzá kapcsolódó minisztériumi rendeletekben került kidolgozásra. A hazai piacon egyre gyakrabban, a nemzetközi tenderek (NATO, EU, stb.) esetében mindig kötelező feltétel a pályázó által a termékek tanúsítását igazoló okiratok bemutatása. A magyar vállalatok külföldi térnyeréséhez is elengedhetetlen feltétel a megfelelő minőségi garanciák felmutatása.

A tanúsító szervezet munkájának célja az azonosított minőségi paraméterekkel rendelkező termékek piacra jutásának, illetve szabad áramlásának biztosítása, ezen belül annak igazolása, hogy az általa tanúsított termékek megfelelnek-e a vonatkozó normatív dokumentumokban meghatározott lényegi követelményeknek, illetve a szolgáltató által önként vállalt minőségi paramétereknek. A tanúsító szervezet ennek megfelelően vizsgálja a távközlési szolgáltatás minden fontos elemét: az értékesítéstől és szerződéskötéstől a szolgáltatás nyújtásán és számlázásán keresztül az előfizetői szerződés felbontásáig. A tanúsítás kiterjed a távközlési szolgáltatás műszaki összetevőire éppúgy, mint annak ügyfélkapcsolati aspektusaira (például: reklamáció kezelés, hibaelhárítás).

A távközlési piac eddigi szerkezete szerint az előfizetők és a szolgáltatók közötti kapcsolat szabályozása a szabályozó hatóságokon keresztül történt. A tanúsító szervezet a piaci liberalizáció szellemének megfelelően új szereplőként jelent meg a távközlési piacon. A szervezet feladata az, hogy visszacsatolást nyújtson a szolgáltatóknak szolgáltatásuk minőségéről, továbbá, hogy az előfizetőknek biztosítékot adjon arról, hogy a szolgáltatás nyújtása valóban az előírásoknak megfelelően történik és a számlázott díj pontosan megegyezik az előfizetői szerződésben, illetve a jogszabályokban rögzített díjakkal.

A távközlési iparág fellendülése és az előfizetők számának folyamatos növekedése megkívánja, hogy a szolgáltatók igazolni tudják az előírásokban és az előfizetői szerződésekben lefektetett szabályoknak megfelelő szolgáltatásminőség nyújtását. Az előfizetők tehát nagyobb biztosítékkal rendelkeznek arról, hogy a szolgáltatás megfelel minden normatív követelménynek, minősé-

[11] Maros Dóra okleveles villamosmérnök, főiskolai adjunktus, Matrix Vizsgáló, Ellenőrző és Tanúsító Kft., tanúsítási igazgató

gi előírásnak, továbbá a szolgáltatás ellenértékeként kibocsátott számlák tartalma és a nyújtott szolgáltatások összhangban vannak. A hatóságokhoz eljutatott egyéni panaszok kezelésénél a tanúsítvány referenciaalapot jelenthet, így az esetek vizsgálata gyorsabban és hatékonyabban folytatható le.

A tanúsító szervezetnek függetlennek kell lennie gyártóktól, szolgáltatóktól és a hatósági szervektől egyaránt. Az auditorok nem érdekeltek a tanúsítás tárgyát képező szolgáltatással kapcsolatos semmiféle gyártásban, tervezésben vagy értékesítésben. Tanúsítási tevékenységét független, harmadik félként szigorú belső minőségi követelmények alapján, független távközlési szakértők és kijelölt laboratóriumok segítségével végzi.

A tanúsító szervezet működésének alapfeltétele, hogy a működése során birtokába jutott cég- és ügyféladatok messzemenő védelméről és szigorúan bizalmas kezeléséről gondoskodjon, erre működési engedélye és tevékenységének folyamatos hatósági ellenőrzése a garancia.

Nemzetközi gyakorlat távközlési szolgáltatások tanúsítására

Általánosan elmondható, hogy az EU tagállamaiban jogilag van szabályozva a távközlési szolgáltatások megfelelőség tanúsítása.

Irányelveket rögzítõ dokumentumok

1. Az **Európai Parlament és Tanács 98/10/EC 1998. február 26-i Irányelve** a nyílt hálózatellátás (ONP) alkalmazása versenykörnyezetben a telefonszolgáltatásra és a távközlési egyetemes szolgáltatásra történő alkalmazásáról.
2. **ETSI ETR 138** második kiadás (1997 december); Hálózati vonatkozások (NA); a beszédcélú távbeszélő szolgáltatás és az integrált szolgálatú digitális hálózat (ISDN) nyílt hálózatellátásának (ONP) szolgáltatásminőségi mutatói.
3. **TL9000**, Egységes távközlési minőségbiztosítási szabvány (USA)

A 98/10/EC Irányelv

Az irányelv a közcélú fix távbeszélő-hálózatokhoz és a közcélú fix távbeszélő szolgáltatásokhoz való nyílt és hatékony hozzáférésre és azok igénybevételét érintő feltételek harmonizálására vonatkozik a nyílt- és verseny piaci környezetben, a nyílt hálózatellátás (ONP) elvével összhangban.

ETR 18 ONP szolgáltatásminõségi (QoS) mutatók öt elve:

1. Az ONP QoS (Quality of Service) paramétereknek a nagyközönség által könnyen érthetőnek, valamint számára hasznosnak és fontosnak kell lenniük.
2. Valamennyi paraméter hálózati végpontban érvényes. Ahol lehetőség van mérésekre, azokat az ügyfél helyiségeiben, üzemben lévő vonalak felhasználásával kell végezni. A lehető legnagyobb mértékű valósághűség eléréshez, a megfelelőség igazolása érdekében, megfelelő számú próbahívást kell végezni, de amikor csak lehet, próbahívások helyett valós forgalmi adatokat kell felhasználni.

3. A paramétereknek alkalmasaknak kell lenniük független szervezetek által történő ellenőrzésre. Ez az ellenőrzés vagy a tanúsító szervezet által elvégzett közvetlen mérések (próbahívások) kiértékelésével, vagy az üzemeltető méréseinek hitelesítése és kiértékelése révén történhet.
4. A QoS értékek pontosságát olyan szinten kell megállapítani, amely ésszerű, minél egyszerűbb és minél alacsonyabb költségekkel járó mérési módszerekkel elérhető.
5. A paraméterek statisztikai és egyedi alkalmazásra egyaránt szolgálnak. A statisztikai értékeket egy egyszerű statisztikai függvény alkalmazásával lehet egyedi értékekké alakítani. A statisztikai függvényt szabványban vagy ajánlásban kell meghatározni. A szabványnak megfelelő útmutatást kell tartalmaznia arra nézve is, hogy miként kell kiválasztani a statisztikailag lényeges mintákat.

TL9000

A TL 9000 kézikönyv minőségi rendszer-követelmények fejezete 21 elemet sorol fel. Ezek közül 20 követelmény kisebb kiegészítésekkel megegyezik az ISO 9001-el. A 21. elem, mellyel kiegészítették az ügyfél elégedettséggel foglalkozik.

A TL 9000-nek a nemzetközileg elismert ISO 9001-gyel való összekapcsolásától azt várják, hogy javul a követelmények következetessége, javulnak a minőségbiztosítási rendszerek és csökkennek a költségek.

Hasonlóan az ISO9001-hez a TL 9000 szabvány is gondoskodik független harmadik fél általi tanúsítás lehetőségéről. A többféle tanúsítási opció a felhasználó számára azt jelenti, hogy a tevékenységéhez leginkább illő tanúsítási módot tudja kiválasztani.

A TL9000 szerinti tanúsítási opciók:

1. TL 9000-HW (hardver minőségi követelmények és hardver minőségmérés)
2. TL 9000-SW (szoftver minőségi követelmények és szoftver minőségmérés)
3. TL 9000-SC (szolgáltatás minőségi követelmények és szolgáltatás minőségmérés).

Szolgáltatásminőségi mutatóknak az a céljuk, hogy az ügyfelek számára kimutassák, hogy a távközlési szolgáltató az általa felkínált és folyamatosan biztosított szolgáltatást kvantitatív és kvalitatív mutatók tekintetében is magas színvonalon biztosítja. A különböző szolgáltatók által nyújtott azonos típusú távközlési szolgáltatások esetében, a korrekt összehasonlítás érdekében, a tanúsító szervezetnek az irányelveknek és szabályozásoknak megfelelően egységes definíciókat és mérési módszereket kell alkalmaznia. A szolgáltatásminőség meghatározása tekintetében az irányelvek egyben javasolják a minőségi mutatók egységes közzétételét, illetve a minőségi megfelelőség igazolása érdekében egy országon belül az egységes védjegy használatát is.

A beszédcélú távbeszélő szolgáltatás QoS mutatói a közcélú kapcsolt távbeszélő hálózaton (PSTN) ellátott távbeszélő szolgálatra vonatkoznak. Az ISDN-mutatók számos, az ISDN segítségével teljesített vonal- és csomagkapcsolt szolgáltatásra érvényesek.

Két példa a távközlési szolgáltatások megfelelõség tanúsítására az EU országaiban

Anglia

1984 óta törvény írja elő a **B**ritish **A**pproval **B**oard for **T**elecommunications (BABT) tanúsító szervezet által végrehajtott éves auditokat a számlázásra a mobil és vezetékes távközlési szolgáltatóknál.

Http://www.oftel.gov.uk (Metering kulcsszóval!)

Németország

Évente a számlázási megfelelősség igazolás előírt a Távközlési Fogyasztóvédelmi rendelet (TKV) 5.§ alapján. Ha ezt a távközlési szolgáltató nem teszi meg, vagy késve igazolja, akkor a hatóság szankciókat alkalmaz (pl. megfelelőség igazolás újra tanúsítással 6 hónapon belül).

A Tanúsítási munka szakaszai

A tanúsító szervezet által folytatott tanúsítási munka célja annak igazolása, hogy a távközlési szolgáltató által, az előfizetői számára biztosított szolgáltatás megfelel-e a hatóságok által kötelezően előírt, valamint a szolgáltató által önként felvállalt normatív dokumentumokban előírt követelményeknek.

A vizsgálatok alapját képező normatív dokumentumok a következők lehetnek:

1. Törvények, rendeletek, egyéb hatályos jogszabályok
2. Ajánlások, direktívák
3. Műszaki szabványok, előírások
4. Általános Szerződési Feltételek, Üzletszabályzat, Koncessziós és/vagy Egyetemes Szerződés
5. Vállalati belső szabályozások, utasítások
6. Egyéb minőségi tanúsítványok (pl. ISO, BABT, stb.)

A tanúsító szervezet által lefolytatott tanúsítási munka több, lényegében jól elkülöníthető szakaszra osztható:

1. Követelmények meghatározása
2. Mutatók és célértékek meghatározása
3. Vizsgálati program aktualizálása
4. Vizsgálatok végrehajtása
5. Eredmények összegzése
6. Értékelés

1. Követelmények meghatározása

A követelmények meghatározása során a tanúsító szervezet összegyűjti és elemzi a tanúsítási területhez kapcsolódó kötelező és önként vállalt követelményeket tartalmazó dokumentumokat.

A dokumentumok feldolgozása és kiértékelése kapcsán a tanúsítónak két kérdésben kell egyeztetnie a szolgáltatóval:

- A normatív dokumentumok listájáról,
- A normatív dokumentumok által meghatározott követelmények listájáról.

A követelmények meghatározásakor teljes körűen és tételesen kigyűjtésre kerülnek a normatív dokumentumokban szereplő, a tanúsítás során vizsgált követelmények. Ennek során az egyik legnehezebb kérdés a követelmények szelektálása a tanúsító szervezet kompetenciája szempontjából. Ez azt jelenti, hogy a tanúsító szervezet csak olyan szolgáltatásokat tanúsíthat, amelyek kijelölési okiratában szerepelnek (pl. Egyetemes távközlési szolgáltatások), illetve normatív dokumentumként csak azokat a szabályozásokat veheti figyelembe, amelyek ebben az okiratban felsorolásra kerültek és a tanúsítási munka idején még hatályosak. A kijelölési okiratban nem szereplő, illetve a kijelölés időpontjában még nem létező, de a tanúsítás alatt már hatályos jogszabályok normatív dokumentumként való elfogadása csak abban az esetben lehetséges, ha azt az illetékes hatóság (HÍF, stb.) a tanúsító cég illetve a szolgáltató kérésére elfogadta.

A tanúsítás első szakaszának eredményei az alábbiakban foglalhatók össze:

- A szolgáltatóra vonatkozó kötelező és a szolgáltató által önként felvállalt normatív dokumentumok és a normatív dokumentumok által előírt követelmények szolgáltató és tanúsító által elfogadott listájának meghatározása.
- Az egyeztetések során a szolgáltató specialistái megismerik a tanúsítási munka vonatkoztatási pontjait.
- A tanúsító szervezet a munka további lépései során fontos szolgáltató-specifikus információhoz jut.

2. Mutatók és célértékek meghatározása

A tanúsítás következő lépéseként a követelmények alapján a strukturált mutatórendszer és a mutatókhoz kapcsolódó célértékek – a mutató tekintetében elérendő mérőszámok – meghatározása, szolgáltatóval való egyeztetése következik.

A követelmények a távközlési szolgáltatás egy-egy aspektusára vonatkozó normatív előírások. Mint ilyenek, komplex műszaki, technikai és adminisztratív, illetve üzleti területek vonatkozásában érvényesíthetők. A szolgáltatónál végzett tanúsítás során a megfelelőség csak úgy vizsgálható, ha a követelmények és a szolgáltatás vonatkozó elemeinek összerendelése megtörténik Ez alapján egyfajta megfeleltetést kell létrehozni, azaz az normatív követelményeket rá kell vetíteni a szolgáltatást létrehozó vállalati területekre és tevékenységekre.

A tanúsítás során a követelmények teljesülését ezért úgy célszerű áttekinteni, hogy a konkrét követelmények kapcsán választ kapjunk a következő kérdésekre:

- A szolgáltatás mely lényegi jellemzőjére vagy jellemzőire vonatkozik?

- Az érintett jellemzők kapcsán milyen feltételeknek kell teljesülniük a követelmény szerint?

Az elemzés eredménye azon mutatók és célértékek meghatározása, amelyek kifejezik a követelmény lényegét és az elvárt szolgáltatásminőségi szintet, illetve konkrét vizsgálati területekre vonatkoztathatóak.

A mutatók és célértékek meghatározása tekintetében lényeges, hogy az egyeztetésekbe a szolgáltató szakemberei is aktívan be tudjanak kapcsolódni, és szakterületük, valamint a szolgáltatás létrehozásának konkrétan alkalmazott megoldása alapján fejthessék ki véleményüket a követelmények alkalmazhatóságának módjáról.

Példák kvantitatív és kvalitatív mutatókra

A távközlési szolgáltatások minőségi követelményrendszerében meghatározó elemként szerepel a számlázási rendszer pontossága és zártsága (biztonsága). A pontosságot olyan számszerűsíthető mutatókban lehet kifejezni amelyek jól reprezentálják a hívásadatok rögzítésének korrektségét, a számlaösszeg helyességét. A mutatók célértékei meghatározzák a számlázás pontosságának kritériumait és a minőségi megfelelőséget (vagy nem megfelelősséget). Ilyen mutatórendszert definiál a brit OTR 003 ajánlás, amelynek lényegi elemei a magyar HÍF 005/2001 Ajánlásban (A közcélú távbeszélő és közcélú mobil rádiótelefon szolgáltatások számlázási rendszerének helyessége és zártsága) is meg jelennek.

Pontosság *kvantitatív meghatározása a HÍF-005/2001 Ajánlás alapján:*

(a) A **pontatlanul mért idejű összeköttetések számaránya** nem lehet nagyobb mint az összes hívások egy tízezred része **(1:10000).**

(b) A **pozitív eltéréssel mért idejű összeköttetések számaránya** nem lehet nagyobb mint az összes hívások egy ötvenezred része **(1:50000).**

(c) Az összes **(a) pont szerint pontatlanul mért idejű összeköttetések teljes számlázási összege** nem haladhatja meg a szolgáltató által az adott hálózat előfizetői részére kiszámlázott kapcsolási és forgalmi díjak összegének az egy húszezred részét **(1:20000).**

(d) Az összes (b) pont szerint pontatlanul **mért idejű összeköttetések teljes számlázási összege** nem haladhatja meg a szolgáltató által az adott hálózat előfizetői részére kiszámlázott kapcsolási és forgalmi díjak összegének az egy százezred részét **(1:100000).**

(e) Időalapú díjazás alkalmazása esetén a szolgáltatás igénybevételének mérését olyan pontossággal kell végezni, hogy az egyes **összeköttetések tényleges időtartama és a hívásrekordban rögzített időtartam között az eltérés** a leghosszabb összeköttetési idő esetén **sem lehet nagyobb 1 sec-nál**, ha a hívó vezetékes szolgáltatási ponton, 2 sec-nál ha a hívó rádiós hozzáférési ponton keresztül csatlakozik a hálózatra.

(f) Az **összeköttetés kezdete/befejezése napi időpontjának meghatározása**, valamint a **napszakváltás időpontjának meghatározása 2 sec**

pontossággal történjen a csillagászati időhöz képest.

A zártság kvalitatív meghatározása Common Criteria és BS 7799 alapján:

- **Biztonsági megfelelősé:** a biztonság különböző jellemzőinek megadása. **Humán vagy szervezeti** biztonság, azaz a biztonsággal kapcsolatos szerepkörök kialakítása és a szervezetben lévő humán biztonsági problémák kezelésének rendszere; biztonsági tudatosság. **Szabályozási háttér**: biztonsági politika, az adatok, rendszerek biztonsági osztályozása, ellenőrzési rendszer, üzletmenet folytonossági terv. **Fizikai biztonság,** vagyis a telephelyek és objektumok védelmi szintjének kialakítása, a védelem megvalósítása. **Logikai biztonság**, amelynek része a digitális kapcsolóeszközökben, az informatikai rendszerekben és hálózatokban megvalósított védelem: hozzáférés-védelem, programcsere rend, mentési rendszer, vírusvédelem, naplózás és ellenőrzése, hálózati forgalom védelme, üzemeltetés szabályozottsága fejlesztéstől való elkülönítése. A rendszerek **életciklus folyamatában** megvalósított védelme.
- A **számlakezeléssel** kapcsolatos követelményeknek való megfelelőség az **Általános Szerződés Feltételek** fő jellemzői: a reklamációkezelés rendje és eljárása, illetve a számlareklamáció rendezésének módjai.

3. Vizsgálati program aktualizálása

A mutatók és célértékek meghatározása, és azok mindkét fél általi jóváhagyása után pontosan meghatározható, hogy a tanúsítás során milyen szakterületeket kell megvizsgálni, illetve milyen ezekhez kapcsoló jellemzőket kell adott esetben megmérni vagy ellenőrizni. A tanúsítási munka következő lépéseként a vizsgálatok módszerét, azok szolgáltatóra való testre szabását kell meghatározni.

A végleges és specifikus vizsgálati tervek elkészítésének kiindulási pontját a tanúsító szervezet által kidolgozott azon előzetes vizsgálati módszerek jelentik, amelyeket a tanúsító szervezet Vizsgálati Módszertan című dokumentumában rögzített.

Ezek az előzetes vizsgálati tervek a szükséges tipikus vizsgálatok leírását tartalmazzák, de mivel ezek nem szolgáltató specifikusak, ezért a tanúsítás során közvetlenül nem vagy csak részben alkalmazhatók.

A vizsgálati tervek konkrét tanúsítási munkára való adaptálásához a következő feladatokat kell elvégezni:

a) A követelmények és a mutatók-célértékek meghatározása során összegyűjtött szolgáltató-specifikus ismeretek beépítése.
b) A tervek egyeztetése a szolgáltató munkatársaival.
c) Végleges tervek és formanyomtatványok elkészítése.

Példák a vizsgálati tervek aktualizálása során figyelembe veendő szempontokra:

- A **hozzáférési hálózat** kapcsán a szolgáltató által alkalmazott védettségi

osztályba sorolás kritériumai, a hálózat nagysága, a hálózati elemek száma, típusa.

- A **kapcsoló központok** hívásadatgyűjtés pontosság kapcsán annak megvizsgálása, hogy milyen statisztikák állnak rendelkezésre, és azok milyen módon készülnek, mennyire alkalmazhatók a tanúsítás során. A szolgáltató végez-e teszthívásokat, ha igen milyen megoldással, azok mennyire hitelesek, a teszthívásoknak milyen paraméterei, eredményei állnak rendelkezésre, és milyen módon alkalmazhatók tanúsítás céljából.
- A **számlázó rendszer** pontosságára nézve a rendszer architektúra ismeretében a fő üzemeltetési, fejlesztési és biztonsági veszélyforrások és kontrollpontok azonosítása és a vizsgálatukhoz szükséges ellenőrzések kiválasztása.
- A **számlakezelés kapcsán** a felelős területek azonosítása, eljárásrendek és szabályozások egyeztetése, a rendelkezésre álló statisztikák megvizsgálása abból a szempontból, hogy mennyire alkalmasak a tanúsítás céljából. Lekérendő riportok meghatározása, interjú tervek elkészítése, stb.
- **A számlázási folyamat** kapcsán a részterületek kritikus kapcsolódási pontjainak meghatározása, felelősök, rendelkezésre álló szabályozások és kimutatások egyeztetése, interjú tervek elkészítése.

A tanúsítási munka e szakaszának eredménye a követelményeknek való megfelelőség tanúsításához szükséges, szolgáltató-specifikus vizsgálati tervek véglegesítése. A vizsgálati tervek mind a normatív szempontok, mind pedig a megvalósíthatóság szempontjából megfelelőek. Mivel a vizsgálati tervek és a vizsgálati módszerek a szolgáltató munkatársaival történt egyeztetés után véglegesíthetők, a vizsgálatok eredményét illetően várhatóan növekszik a pozitív szolgáltatói hozzáállás valószínűsége is.

4. Vizsgálatok végrehajtása

A követelményeknek való megfelelőség tanúsításához szükséges szolgáltató-specifikus vizsgálati tervek alapján a tanúsítás következő lépésében a szolgáltató és a tanúsító szervezet munkatársai lefolytatják az előírt vizsgálatokat.

A vizsgálatokat a szolgáltatóval egyeztetett vizsgálati tervek alapján kell elvégezni. A munkafázis fontossága miatt ügyelni kell arra, hogy a vizsgálatokat és az azok eredményét tartalmazó vizsgálati jelentéseket a tanúsító szervezet megfelelő kompetenciával rendelkező munkatársa (pl. tanúsítási igazgató) szakmai és formai szempontból folyamatosan ellenőrizze.

A vizsgálatokat végző auditor a vizsgálandó szakterület sajátosságaiból adódóan különböző módszerekkel győződik meg a szóban forgó szakterületeken elért minőségi szintről. A vizsgálatok során az auditor célja az, hogy a vizsgálandó területhez rendelt követelmény- és célértékrendszerre alapozva hiteles bizonyítékokat gyűjtsön össze a megfelelőség igazolására.

A vizsgálatok a következő módszerek alkalmazásával végezhetők el:

- A szolgáltatás minőség területén a szolgáltatónál korábban elvégzett belső

és külső auditok jelentéseinek áttekintése (pl ISO)

- Belső vállalati szabályozások, utasítások, eljárásrendek és a minőségbiztosítási rendszer dokumentáció áttekintése
- Fentiek végrehajtásának, gyakorlati alkalmazásának vizsgálata
- Műszaki tesztek, próbamérések
- Hitelességet igazoló okiratok bekérése (pl. Próbahívó, órapontosság, stb)
- Rendszertervek elemzése
- Elektronikus vagy papír alapú napló állományok elemzése
- Személyes interjúk
- Szemlék
- Statisztikák elemzése
- Élő ügyfél-esetek áttekintése (pl. Szolgáltatás életciklus)

Az egyes vizsgálati területek kapcsán a vizsgálati módszerek jól meghatározhatók. Azt hogy az egyes vizsgálati módszereket miként, illetve milyen súlyozással kell alkalmazni, az adott szolgáltatónál történő megvalósulás alapján lehet eldönteni. Ha például egy terület jól szabályozott, akkor kisebb hangsúllyal szerepelhet az interjúzás mint egy kevésbé szabályozott területen. A módszertan az irányokat jelöli meg, de a tanúsító dönti el, hogy egy-egy módszerre mennyire kíván támaszkodni.

A vizsgálati területek elemzését és a vizsgálatok eredményeit az auditorok a vizsgálati jelentésekben foglalják össze.

5. Eredmények összegzése

A tanúsítás e szakasza akkor kezdődik, amikor már elkészült az összes - tanúsító és szolgáltató által jóváhagyott - vizsgálati jelentés. A távközlési szolgáltatás komplexitása miatt ezen a ponton fontos munkalépést kell végrehajtani, a részterületekre vonatkozó eredmények összegzését. Ez biztosítja azt, hogy a szolgáltatást teljes folyamatában lehessen szemlélni.

Az egyes részterületekről készült részletes vizsgálati jelentések alapján készül el a véglegesített, összesített vizsgálati jelentés. A feladat abból áll, hogy az egyes területekért (pl. kapcsoló központok, számlázási rendszer, számlakezelés, számlázási folyamat) felelős munkatársak megvizsgálják, hogy az értékelés szempontjából milyen átfogó jellegű összefüggéseket kell figyelembe venni a szakterületeken belüli, illetve a szakterületek közti viszonylatban.

Példák az átfogó összefüggésekre:

- **Kapcsoló központok**

- A kvantitatív és kvalitatív jellegű vizsgálatok egymást kiegészíti-e,
- A kapcsoló központ és a számlázó rendszer beállításai megegyeznek-e.

- **Számlázó rendszer**

- A számlázás pontosságának vonatkozásában a kvantitatív és kvalitatív vizsgálatok egymást kiegészítik-e.
- A kvalitatív jellegű vizsgálatoknál az egyes veszélyforrásokkal szembeni

kontrollok gyengeségét ellensúlyozhatja-e más kontrollok erőssége a pontosság és a biztonság tekintetében.
- A számlaellenőrzés - mint ügyviteli folyamat - hatékonyságának értékelése a számlázó rendszer manuális feldolgozási kontrolljaként.

- **Számlakezelés**

- A személyes és telefonos ügyfélszolgálatok milyen információt tudnak nyújtani az olyan back-office jellegű tevékenységekről, mint például a bizonyítási eljárás.

- **Számlázási folyamat**

- A kapcsolástechnikai, informatikai és kapcsolódó műszaki területeken a teljesítmény-követés és a hozzá kapcsolódó hibaelhárítás együttes megfelelőségének vizsgálata.
- Tarifa beállítások implementálásának vizsgálata, mint a marketing, jogi, kapcsolástechni-kai, informatikai, marketingkommunikációs, ügyfélszolgálati területek együttműködését igénylő feladat.

A felvetődő kérdések és problémák átfogó jellege miatt e munkafázisban lényeges a különböző területekért felelős tanúsító és szolgáltató munkatársak együttműködése, a megállapítások egyeztetése.

A munka eredménye a részterületek vizsgálati jelentésein alapuló, átfogó vizsgálati jelentés, amely tartalmazza az egyes vizsgálatok lényeges elemeit, és amely az értékelési jelentés alapja.

6. Értékelés

A vizsgálati jelentéseket alapul véve, a témafelelős tanúsítók kiértékelik a kapott eredményeket a követelményrendszer és a mutatók célértékei alapján, és az egyes szakterületek tekintetében meghatározzák a szolgáltató megfelelőségi szintjét.

A megfelelőség esetén a tanúsító szervezet az értékelési jelentésben javaslatot tesz a tanúsítvány tartalmára és annak érvényességi idejére. Nem megfelelőség esetén részletes hibajegyzék készül.

Az értékelési jelentés elkészülte után, megfelelőség esetén a tanúsító szervezet a szolgáltató részére tanúsítási okiratot (Tanúsítványt) állít ki, amelyen feltünteti a vizsgált szolgáltatás megnevezését és a vizsgálatok alapját képező normatív dokumentumok listáját.

RÉVÉSZ Gyula

A HÍRADÓ SZAKBEOSZTÁSÚ SZERZŐDÉSES ÁLLOMÁNY KIKÉPZÉSI LEHETŐSÉGEI

„Semmi sem nehezebb annál, mint valamit elkezdeni,
semmi sem veszélyesebb, mint ezt véghezvinni,
semminek a kimenetele nem bizonytalanabb,
mint egy sor új dolog bevezetésébe belevágni.”
(Machiavelli)

Bevezetés

A nemzetközi tapasztalatok azt mutatják, hogy a haderő átalakítási folyamatokra a csökkentés, a strukturális átalakítás és a hatékonyság további növelése a jellemző. Ezen új keletű, a védelmi kiadások csökkentésére irányuló nyomások olyan időben jelentkeznek, amikor a Magyar Köztársaság és NATO-szövetségesei egyre több kontingens (IFOR, SFOR, KFOR) műveletet hajtanak végre, a katonai erők összetétele pedig egyre kisebbre zsugorodik.

- A NATO-t alkotó hadseregek 25–40 százalékkal csökkentek.
- Az Európában állomásozó amerikai erők több mint 66 százalékkal csökkentek és a korábbi 300 ezer főről mára összesen 100 ezer főre csökkentek.
- A tartalékok mozgósításának időszükséglete napokról hetekre és hónapokra emelkedett.

A Magyar Köztársaság fegyveres erői, ezen belül a Magyar Honvédség átalakítása, illetve fejlesztése is csak így mehet végbe, mert a nemzeti haderőfejlesztés célkitűzései így kerülhetnek összhangba a nemzetközi tendenciákkal. Eredményül pedig egy kisebb, rugalmasabb szervezetű, gazdaságosan működő haderő jöhet létre, mely olyan fegyveres erő, ami gyorsan bevethető, nagyrészt hivatásos katonákból áll, komplex, modern technikájú fegyverrendszerrel rendelkezik és többnemzetiségű keretben is alkalmazható.

Ennek kapcsán a 90-es években drasztikusan csökkent a honvédség létszáma, s így a behívottak száma is, először csak felmerül a sorkatonai szolgálat hosszának megváltoztatása, majd három alkalommal csökkent is. Ezen túl is történtek jelentős változások, szigorodtak a behíváskori kiválasztás követelményei, egyre nagyobb százalékban kerültek otthonukhoz közelebb a sorkatonák, megnőtt a szabadidő hossza, korlátozták a parancsnokok fegyelmezési eszközkészletét.

A politikai vezetés elgondolása alapján 2007-re megszűnik a sorozott állomány a katonai szervezeteknél, és tisztán hivatásos és szerződéses haderőről beszélhetünk.

Haderő átalakítás, új típusú honvédelem

A történelem során a háborúkat mindig ugyanazokkal a technológiákkal és technikákkal vívták meg, amelyeket a gazdaság megteremtésére is használtak. Az agrártársadalmak parasztseregekkel harcoltak, ha lehetőség volt rá, akkor aratás előtt vagy után.

Az ipari társadalom hozta el a fegyverek, tankok, repülőgépek tömegtermelését és hatalmas hadseregek szárazföldi, vízi és légi úton való mozgatását.

Ma, **az információ korában** a háborúk lefolytatásának módszerei forradalmasodnak.

Ahhoz, hogy az új biztonságpolitikai környezetben is számottevőek tudjunk maradni, a katonáknak alkalmazkodniuk kell az új feladatokhoz, amelyek a békefenntartástól a hagyományos hadműveletekig terjednek. A technika és technológia fejlődése, a megnőtt adatmennyiség lehetővé teszi kevesebb katona alkalmazását a harcmező nagyobb területeinek lefogásához.

Az Öböl-háború, valamint a Jugoszlávia elleni háború során benyomást kaphattunk arról, hogyan változtatják meg a harcmezőt a precíziós, modern fegyverek. A precíziós fegyverek kulcsa az információ gyors begyűjtése, feldolgozása és továbbítása, mely igen magas szinten képzett katonákat igényel.

Ma a CNN jóvoltából egy tiszt, tiszthelyettes vagy katona harctéri döntését világszerte milliók nézhetik élőben. A katonákat a helyes döntések meghozatalára kell nevelni, és fel kell őket hatalmazni, hogy a döntéseik alapján intézkedhessenek.

Tekintve, hogy az információ és a technológia mind a kis és nagy nemzetek számára elérhetőek, létrejöhetnek aszimmetrikus hadszínterek, ahol a kis nemzet a technológia vékony rétegénél is nagyobb eséllyel vehet részt a küzdelemben (lásd, Izrael).

A korlátozottan rendelkezésünkre álló forrásainkat, beszerzési összegeinket a legmodernebb, kereskedelmi forgalomban beszerezhető berendezések vásárlására kell fordítanunk. Nem elegendő átstrukturálni a szervezeteket, a haderő átalakítás többet jelent a régi technológiák új információs technológiákra való puszta felváltásánál. Szükség van a belső szervezeti követelményeknek az információs forradalom kívánalmai szerinti bevezetésére is.

Ma a magyar politikai erők többsége az atlanti és európai védelem jövendő megfelelő katonai eszközének a hivatásos hadsereget tekinti. Ennek ellenére, sokan igen hasznosnak, sőt elengedhetetlennek tartják a sorkatonai szolgálat fenntartását, mivel a hivatásos hadsereg megteremtésével, hivatalosítanák a civilek és a hadsereg közötti szakadékot.

Ismerjük be, hogy a katonai szolgálat soha nem volt sem általános, sem pedig egyenlően kötelező. Mindig megvoltak a kibúvók, tulajdonképpen a kü-

lönböző társadalmi rétegek és különböző etnikai hovatartozású személyek keveredését segítette elő, mesterségesen és kötelezően.

A hivatásos állomány körében is növekszik a kötelező katonai szolgálat eltörlését támogatók tábora, ugyanakkor politikai oldalról erősödni látszanak azok a hangok, melyek a szolgálat szocializációs szerepét igyekeznek feltüntetni, egyrészt a hazaszeretetre, másrészt a munkára való nevelés tekintetében. Ez az érv a gazdasági és társadalmi környezet változásával megdőlt.

Mivel az új informatikai technológiák elmossák a harcászati, a hadműveleti és a hadászati döntések közötti különbségeket. Ugyanis a hidegháború utáni időszakban a különböző polgárháborúk és krízishelyzetek megoldásához olyan katonai alakulatokra van szükség, amelyek kisebb létszámúak ugyan, de nagyon jól kiképzett mobil erők, gyorsan és könnyen bevethetők.

Figyelembe véve századunk végén a véres konfliktusok típusainak átalakulását, a magyar társadalomnak végül is olyan katonai konfliktusra kell keresnie a megfelelő választ, melyek földrajzi értelemben közel vannak Magyarországhoz (lásd, a volt Jugoszlávia területe) és amelyek esetében valós szükséglet mutatkozik a katonai, diplomáciai vagy humanitárius akciókra.

Az ENSZ és az EBESZ különböző válságkezelő katonai és polgári misszióinak tapasztalataira támaszkodva ezeket a nemzetközi akciókat növekvő érdeklődés övezi.

A fenti gondolatsor is mutatja, hogy a sorkatonai szolgálat számtalan társadalminak tekinthető problémát vet fel. Az új legénységi szisztéma, melyben a szerződéses katonai szolgálat lenne kizárólagos, vagy döntően meghatározó, olyan jelentős mértékben átalakítja a hadsereg és a társadalom viszonyát, ami kihat a gazdasági, pénzügyi, munkaerő piaci, egészségügyi, közoktatási, kulturális viszonyokra.

Profi hadsereget Magyarországon

A sorkatonai szolgálat megszüntetése esetén technikai korszerűsítést hajthatunk végre és igen jelentős forrásokat mozgósíthatunk a toborzásra, a képzésre, a megbecsült visszavonulás, illetve társadalomba való visszaillesztés lehetőségének érdekében.

Az egyre nagyobb számban megnyerendő önkéntesek magas iskolázottsággal, erős motivációval kell, hogy rendelkezzenek és minden társadalmi osztályából, annak minden régiójából kívánatos, hogy jelentkezzenek. Természetesen a minőség, a hatékonyság emelésével párhuzamosan, figyelembe kell venni a védelmi költségvetés realitásait.

A jelenlegi biztonsági kihívások nem teszik szükségessé a nagy létszámú hadsereget, többek között ezért van szükség minél előbb egy profi hadsereg megteremtésére. A leszerelési tárgyalások a hagyományos fegyverek jelentős csökkentését eredményezték, és mindenekelőtt a szárazföldi haderőt érintően a védekezés mellett egyre nagyobb hangsúlyt kapott a mozgékonyság, a gyors alkalmazás. Ebből adódóan a jelenlegi hadsereget kell hivatásossá tenni, ezál-

tal a kötelező katonai szolgálat rendszerét fel lehetne függeszteni, csakis a magyar létérdekek veszélyeztetése, vagy nagyobb krízis és háborús helyzet esetén lenne szükség a sorkötelezettség újbóli bevezetésére.

A katonák kiképzettsége a NATO-tagországok vezetőinek körében legnyilvánvalóbb követelmények egyike. A „NATO-elvek" szerint nincs jól vagy kevésbé jól kiképzett katona, csak **megfelelően kiképzett katona** van!

A katonának alanyi jogon jár, egyben kötelessége is a mindenkori legmagasabb szintű kiképzés azért, hogy önmagát, társait, a hazáját, szövetségesét megvédhesse, ez igaz a szerződéses katonákra is.

Éppen ezért a honvédség vezetésének az egyik legsürgősebb feladata a Magyar Honvédség önkéntes, „profi" haderővé történő átalakítása koncepciójának a kidolgozása. Csak így lehet minden mai haderő átalakítási mozzanat előremutató és sikeres.

Ez lehetővé teszi az új eszközkezelő állomány korszerű kiképzését, összekovácsolását, s ha szükséges, sikeres harci alkalmazását is.

Mivel a válságkezelő, az azonnali, a gyors készenlétű és az ENSZ-feladatok teljesítésére kijelölt katonai szervezeteknél már ma is jelentős mennyiségű a korszerű technika, értelemszerű, hogy ott már most indokolt a teljesen önkéntes állományra való áttérés megkezdése.

Az önkéntesség arányának növelését megkívánja a magasabb színvonalú technikai eszközök rendszerbe állítása, az új típusú, bonyolult katonai feladatok megoldása.

Híradó szakbeosztású szerződéses állomány

A szerződéses állomány beosztásba helyezése, a vezetői és a személyügyi tevékenység fontos eleme.

A személyzeti tevékenység klasszikusan két fő szakmai területbe sorolható:

- kiválasztás
- fejlesztés

A kiválasztásnál fontos, hogy a szervezet határozza meg, milyen ismeretre, személyiségre van szükség az adott beosztás betöltéséhez.

A fejlesztés magába foglalja a képzést, motiválást és az értékelést. Ezek a területek meghatározóan összetartoznak, hiszen nem lehet úgy tervezni valamilyen képzést, hogy ne tudjuk pontosan, mely területeken kell az ismereteket bővíteni, milyen módszerek hatékonyak, illetve milyen adottságai, képességei vannak a képzendőnek.

Az ösztönzésnek, motiválásnak kölcsönös kapcsolatban kell lennie a teljesítményértékeléssel. Az értékelés az elért teljesítményt hasonlítja össze a szervezet által megfogalmazott szintekkel. A szervezet a számára előnyös viselkedést, eredményességet elismerheti, jutalmazhatja, az előnyteleneket szankcionálhatja.

A teljesítményértékelés segítségével a szervezet visszajelzést kap és ad tagjai teljesítményéről. A teljesítményértékelés (minősítés) kialakításakor figye-

lembe kell venni, milyen kérdésekre szeretnének választ kapni az értékelés során.

A jövőbeli kép vizsgálata során a következő kérdésekre kell választ adni:

- milyen jövőbeni állapotot kíván elérni a szervezet?
- milyen alapvető képességekkel rendelkezik?
- milyen tevékenységekkel kell, illetve akar foglalkozni?
- milyen tevékenységekkel számolhat a jövőben?

Az emberi erőforrás gazdálkodáshoz kapcsolódó feladatok, a megfelelő képességekkel rendelkező és elkötelezett emberek kiválasztására, a munkakörük meghatározására, az oktatásukra, továbbképzésükre, a teljesítmények értékelésére, a fegyelmi és más munkahelyi gondok kezelésére.

A motiváció során alkalmazható gyakorlati lépések, a pozitív megerősítés, negatív megerősítés, büntetés, megszüntetés, munkakörbővítés, munkaerőgazdagítás, rotáció, teljesítmény, jutalmazás; előmenetel biztosítása, fejlődési lehetőség, pályaív bemutatás.

A szerződéses állomány képzése

Jelenleg a szerződéses katona felkészítését, kiképzését az alakulat hajtja végre, ahová szerződése köti. A szerződéskötés feltétele a háromhavi próbaidő kikötése.

A jövőben a sorkatonai beosztások fokozatosan megszüntetésre kerülnek, helyettük szerződéses beosztások kerülnek rendszeresítésre. A szerződéses állománnyal kevesebb a fegyelmi probléma, hiszen ők önszántukból kerültek a rendszerbe, a sorozott állománnyal szemben. A jövőben a szerződéses állomány felkészítését is a kiképző központok hajtanák végre az első három hónapban.

Figyelembe véve a kétéves szerződés lehetőségét, ennek megfelelően a Szolgálati Törvényben biztosított alap- és pótszabadságot, a kiképzésre rendelkezésre álló idő 21 hónap.

A rendelkezésre álló idő felosztása:

- 1-3. hónap általános katonai ismeretek frissítése, szakfelkészítés szakaszszintig,
- 4. hónap század foglalkozások,
- 5-6. hónap szakasz-tárgykörök feldolgozása,
- 7-9. hónap századszintű feladatok végrehajtása,
- 10-11. hónap zászlóaljszintű feladatok végrehajtása,
- 12. hónap zászlóaljszintű ellenőrzésen való részvétel,
- 13-19. hónap szinten tartás
- 20. hónaptól speciális képzés, átképzés

A szerződéses állománnyal kapcsolatos általános rendelékezések

A katonai pályájukat megkezdő szerződésesek számára egymással összhangban lévő követelményrendszert kell megfogalmazni és felállítani.

A követelményeknek a hatályos magyar jogszabályokra, a katonai életet szabályzó belső rendelkezésekre és azon NATO dokumentumokra kell épülnie, melyek meghatározzák a Magyar Honvédséggel és ezen belül a Szárazföldi haderőnemmel szemben támasztott szövetségi elvárásokat, illetve eljárási rendeket.

A követelményrendszer magába foglalja az általános műveltségi és általános katonai, valamint az általános (híradó) szakmai műveltség követelményeit, melyeket minden pályakezdőnek - állománykategóriájának megfelelő mélységben – ismernie kell, illetve képesnek kell lennie alkalmazni.

A követelményrendszernek továbbá tartalmaznia kell az egyes híradó beosztások, illetve a pályakezdő tervezett első beosztásának megfelelő specifikus szakmai követelményeket.

A tanintézetek a megfogalmazott követelmények alapján kidolgozzák az oktatási tematikákat, megszervezik az oktatást, az adott témakörökben magas szintű ismeretekkel rendelkező oktatói állományt biztosítanak a képzés végrehajtásához.

A végrehajtott képzés eredményeként a pályakezdő rövid beilleszkedés és a helyi sajátosságok megismerése után képes lesz a beosztása teljes értékű ellátására.

Követelmények megfogalmazása

Általános képességek, elvárások a szerződéses pályakezdővel szemben:

Alapvető és meghatározó elvárás a hazához és a nemzethez való feltétlen hűség, a politikamentesség, a katonai szimbólumok és az egyenruha iránti tisztelet, valamint a katonai hivatás iránti elkötelezettség.

A pályakezdő rendelkezzen:

- megfelelő fizikai, pszichikai felkészültséggel,
- katonai professzionizmussal,
- döntés előkészítő, döntéshozói képességgel,
- megfelelő vezetői ismeretekkel,
- karrier orientációval,
- képességgel mások érdekeinek képviseletére,
- az önművelődés, önképzés igényével,
- kommunikációs képességgel,
- elhivatottsággal hivatása iránt.

A pályakezdő híradó szerződésessel szemben támasztott követelmények:

Általános műveltség és általános katonai ismeretek területén:

A szakmai képzés eredményeként ismerje:

- a magyarság történetét, ezen belül hadtörténelmünk főbb eseményeit.
- a katonai híradás fejlődésének főbb mozzanatait, a magyar katonai és polgári híradás fejlődéstörténetét.
- az Alkotmány, a Honvédelmi törvényt, a Szolgálati törvényt, a szerződéses katonákra vonatkozó törvényeket, legyen képes e jogszabályok előírásainak gyakorlati alkalmazására.
- a Magyar Honvédség feladatát, felépítését, a haderőnemek és fegyvernemek, fontosabb szakcsapatok rendeltetését, főbb feladatrendszerét.
- a Szárazföldi Parancsnokság szervezetét, alárendeltjeit, azok feladatait, a parancsnokság vezetési rendjét.
- a nemzetközi hadijog előírásait, legyen képes azok alkalmazására.
- az ENSZ/NATO/EU szervezetét, főbb feladatait, infrastruktúráját.
- a NATO tagállamok hadseregei által használt katonai rendfokozatokat, fontosabb beosztásokat és megszólításokat.
- a NATO-ban alkalmazott híradó jeleket és jelzéseket, térképen a jelzéseket, valamint a különféle munkaokmányokon, híradó vázlatparancsokon. Ismerje meg az alkalmazott rövidítéseket, amelyekkel munkája során találkozhat.
- a kiépített és kiépítésre kerülő védelmi építmények (pl: EÁP-ok., óvóhelyek, tüzelőállások, vezetési pontok,) telepítésének rendjét, használatát, berendezéseinek alkalmazását.
- legyen képes az elfogadott társadalmi etikett szerinti megjelenésre, megnyilvánulásokra

A pályakezdő szerződéses rendelkezzen:

- erkölcsi bizonyítvánnyal
- szakbeosztási kötelezettség esetén nemzetbiztonsági vizsgálattal
- alapfokú állami nyelvvizsgával,
- személy és teher gépjármű jogosítvány
- általános katonai ismeretekkel és készségekkel,

A pályakezdő szerződéses legyen képes:

- egyéni lőfegyvereinek készség szintű kezelésére,
- a személyi számítógép felhasználói szintű alkalmazására.

- az alapvető híradó technikai eszközök kezelésére. Legyen tisztában a NATO közös gyakorlatok során végrehajtandó információ továbbítási eljárások és módszerek legfontosabb alapfogalmaival.
- híradó technikai eszközök álcázásával kapcsolatos feladatok irányítására, végrehajtására
- fizikai felkészültsége olyan szintű legyen, hogy a fizikai követelményeknek legalább megfelelő szinten eleget tudjon tenni. Legyen felkészítve az alapvető önvédelmi fogások alkalmazására.
- a szolgálati, az alaki szabályzat és az öltözködési utasítás előírásait ismerje és legyen képes azok gyakorlati alkalmazására.
- tudjon szabályosan parancsot és vezényszavakat kiadni, azok végrehajtását megkövetelni.
- munka és környezet védelmi ismeretei olyan szintűek legyenek melyek az első beosztáshoz szükségesek.
- az ön-és kölcsönös segélynyújtás készségszintű végrehajtására úgy legyen kiképezve, hogy azt a gyakorlatban alkalmazni tudja.

Általános híradó szakkövetelmények szerződésesek számára:

- rendelkezzen szakirányú végzettséggel.
- ismerje a híradó szolgálat rendeltetését, fő területeit, helyét és szerepét Magyar Honvédségben, illetve a Szárazföldi haderőn belül.
- legyen tisztában a forgalmazás szabályaival, illetve a NATO híradó forgalmazási rendszabályainak és terminológiájának alkalmazásában.
- ismerje az alegységénél rendszeresített híradó technikai eszközöket, azok alkalmazási lehetőségeit, illetve főbb harcászat-technikai adatait.
- ismerje a híradó katonákra vonatkozó kiképzési norma feladatokat.
- rendelkezzen REH alapismeretekkel.
- ismerje a híradó állomáshoz előírt okmányokat , azok vezetésének szabályait.
- ismerje a híradó állomások szolgálati személyeinek feladatát.
- ismerje a híradó állomások technikai kiszolgálásának szabályait.
- ismerje és tudja alkalmazni a híradó állomás álcázási szabályait.

Ismerje:

- szakasz szintig azon terveket, amelyek, annak riasztásához, a személyi állománynak visszahívásához, az eszközei kiegészítéséhez, a tartalékosaik mozgósításához, mindezek fogadásához, az áttelepüléshez szükségesek.
- a szakasz békeidős működéséhez szükséges dokumentumok felépítését, elemeit.

- a szakasz békeidős feladatai végrehajtásához szükséges dokumentumokat.
- ismerje a különféle feladatok végrehajtásához szükséges egyéni és kollektív felszereléseket és anyagokat, legyen képes ezen felszerelések készség szintű alkalmazására.
- a szakcsapatnál rendszeresített lőszer, rakéta anyagok rendeltetését, valamint a hajtó illetve kenőanyagok sajátosságait, használati jellemzőit.
- a nukleáris, biológiai és vegyi védelemmel ellátott járművek, létesítmények védelmi lehetőségeit és azok alkalmazását.
- az áttelepülésre történő felkészülés mozzanatait, a tevékenység rendjét.
- áttelepülés előkészítésének szabályait, a települési hellyel szemben támasztott követelményeket.
- az áttelepülés végrehajtásának rendjét, annak minden oldalú biztosítási mozzanatait.
- az előírt jelentések megtételének rendjét.
- az elöljáró irányába történő jelentések megtételének szabályait, azok tartalmát.
- az információs biztonság rendszabályait és legyen képes azokat a mindennapi tevékenység során hatékonyan alkalmazni

HOFFMANN Imre

SÚLYOS BALESETEK, KATASZTRÓFÁK BEVETÉSIRÁNYÍTÁSA, DÖNTÉS-ELŐKÉSZÍTÉSE, TÁMOGATÁSA A MEGELŐZÉSBEN, A VÉDEKEZÉSBEN RÉSZTVEVŐK KOORDINÁLÁSA, IRÁNYÍTÁSA ÉS VEZETÉSÉNEK KOMMUNIKÁCIÓS, INFORMATIKAI, TÉRINFORMATIKAI FELADATAI

Tisztelt Hölgyeim, és Uraim!

Tisztelt Konferencia!

Előadásomban a felkérésnek megfelelően kívánom bemutatni a *2000. január elsején törvény alapján két előd szervezetből létrehozott szervezet a BM OKF területi szervének, a Jász-Nagykun-Szolnok Megyei Katasztrófavédelmi Igazgatóság* alkalmazását, az irányítás és a vezetés megyei szintű feladatait. A megyei Tűzoltó és Polgárivédelmi parancsnokságok összevonásával létrejött egy, olyan új szervezet, amely képessé vált a kor kihívásainak megfelelni. Alapvetően mindkét előd szervezet az állampolgárok, a lakosság biztonságát és védelmét szolgálták. Nincs ez ma sem másként, de nap mint nap újabb kihívásoknak való megfelelés szükségessé tette az összevonást. Az egyre gyakoribb súlyos balesetek és katasztrófák (természeti, civilizációs) megelőzése, a mentési és helyreállítási feladatok komplexitásából adódóan az eseményekben „résztvevők" növekedett száma bonyolult irányítást és vezetést igényel. Amint a képen láthatják (2. dia.) az igazgatóság „NORMÁL" időszakban, a mindennapi tevékenysége során állandó kapcsolatban van:

- BM. OKF-gal,
- a MVB elnökével,
- a települések polgármestereivel közvetlenül vagy a Polgárivédelmi kirendeltségeken keresztül közvetve,
- az együttműködőkkel és monitoring rendszereikkel,
- a Polgárivédelmi kirendeltségekkel és irodákkal,
- a hivatásos, önkéntes köztestületi és önkéntes tűzoltó
- gyesületekkel,
- a szomszédos Megyei Katasztrófavédelmi Igazgatóságokkal,
- valamint különböző polgári és karitatív szervekkel

A normál időszak alapvetően a megelőzés és a felkészülés feladatainak elvégzését tartalmazza. Szükségesnek tartom kiemelni, hogy az igazgatóság diszpécser szolgálata, a hivatásos és önkéntes tűzoltóságok folyamatos „ÉLES" készenléti helyzetben (kettő, illetve nyolcperces riasztási készséggel)

látják el tűzoltási és műszaki mentési feladataikat. Ez azt jelenti, hogy éves átlagban naponta megyei szinten, 15-20 esetben vonulnak tűzesethez illetve balesethez.

A sajátosságból adódik, hogy az irányítás és a vezetés rendszere, annak technikai feltételének folyamatosan jól és megbízhatóan kell működnie.

A 3. dia. és a 4. dia. a hivatásos, és önkéntes tűzoltóságokat, valamint a Polgárivédelmi kirendeltségeket, irodákat működési terület szerinti elhelyezkedés szerint láthatják.

A 5. dia. a Megyei Katasztrófavédelmi Igazgatóság működési folyamatábrája látható veszély/katasztrófa helyzetben.

Az irányítás és vezetés rendjében minőségi változás történik, ugyanis az állandó diszpécser szolgálat által RIASZTOTT Területi Katasztrófa-elhárítási Információs Központ kerül felállításra részlegesen vagy teljes állománnyal. A kialakult veszélyhelyzettől függően kerül aktivizálásra a Megyei Védelmi Bizottság Védekezési Munkacsoportja az Operatív Törzs (6. dia), a Helyi Védelmi Bizottságok, Pv. szervezetek, Polgári és karitatív szervek.

Az 7. dián keresztül kívánom bemutatni egy Megyei Katasztrófavédelmi Igazgatóság híradó rendszerét.

Az Igazgatóság URH rendszere két külön álló rendszerből épül fel:

A tűzoltóságoknál meglévő híradórendszer:

A tűzoltóságoknál lévő rendszer un. szimplex üzemmódban működik (ugyanazon a frekvencián ad-vesz és forgalmazás közben az azonos csatornán lévő rádiók mindenki által hallhatók, ezért hívóneveket és hívószámokat szükséges alkalmazni illetve a rádióforgalom egyszerre csak egy adó és egy vevő között lehetséges). A használt típusok: MOTOROLA GM-300 (stabil-, mobil eszköz, teljesítményük 20 - 45W között

van), MOTOROLA GP-300 (kézi eszköz, teljesítménye 5 – 10W között van). Ez a típus egyszerre több rádió rendszert képes lekezelni (megfelelő programozás után), illetve automata figyelő funkciója segítségével hangolja magát arra a frekvenciára, amelyiken forgalmazást észlel. Ezenkívül rendszerben van még a KENWOOD és a YAESU különböző típusa (főleg az önkéntes tűzoltóságoknál). A stabil eszközök központi ügyeleten vannak telepítve és nagy hatótávolságukat kiépített antenna biztosítja. Így az ügyeletek képesek egymás elérésére, melynek jelentősége a kölcsönös segítségnyújtáskor értékelődik fel. A mobil eszközök különböző járművekbe építettek és hatótávolságukat a járműre szerelt antenna magassága-, és a jármű pillanatnyi helyzete határolja be. Ez biztosítja vonulás és beavatkozás közben a központi ügyelettel az állandó kapcsolatot. A kézi eszközök közvetlenül a beavatkozás helyszínén biztosítják a kapcsolatot (legyen az földi, légi) az abban résztvevők és a beavatkozást biztosítók között. A rádió forgalom a stabil, a mobil, és a kézi eszközök között biztosított.

Polgárivédelmi híradórendszer:

A PV egységeknél lévő rendszer un. duplex üzemmódban működik (egy frekvencián ad, egy másikon pedig vesz és forgalmazás közben csak az a személy hallja az adást akit hívtak / ”szelektív hívás” /). Ez azt jelenti, hogy az előre meghatározott hívószámot aktivizálva (adás) csak az a rádió fogja észlelni, amelyik ezzel a hívószámmal rendelkezik, tehát így egyszerre több hívás is kezdeményezhető a másik zavarása nélkül. A használt típusok: BRG gyártmányú (stabil-, mobil eszköz, teljesítményük 10 - 25W között van), YAESU (kézi eszköz, teljesítménye 0.5 – 10W között van).

A stabil eszközök központi ügyeleten-, PV kirendeltségeken-, önkormányzatoknál vannak telepítve és nagy hatótávolságukat kiépített antenna biztosítja. Így azok képesek egymás elérésére akár veszélyhelyzetben is. A mobil eszközök itt is különböző járművekbe építettek és hatótávolságukat a járműre szerelt antenna magassága-, és a jármű pillanatnyi helyzete határolja be. Ez biztosítja vonulás és beavatkozás közben az állandó kapcsolatot. A kézi eszközök közvetlenül a beavatkozás helyszínén biztosítják a kapcsolatot az abban résztvevők és a beavatkozást biztosítók között. A rádió forgalom mind a stabil, mind a mobil, mind a kézi eszközök között biztosított.

A 8. dián jól látható, hogy az egész megyét a mobil átjátszóval képesek vagyunk átfogni.

A rádiók mellett fontos szerepe van telefonnak, a FAX és E-amil kapcsolatnak.

A jelenlegi rendszerek mellett már volt módunk és lehetőségünk veszélyhelyzetben kipróbálni a TETRA rádiórendszert. A 9-12 diákon jól látható, hogy a trönkölt rádiórendszer alkalmazása esetén biztosítottá válik a bevetésirányítás. A jelentősége az események kezelésében nagyszámú együttműködők közötti kommunikáció feltételének gyors létrehozásában és fenntartásában van.

Döntés-előkészítés, döntés-támogatás.

Előadásomban már tettem említést a döntés-elkészítésről és a döntéstámogatásról. Jász-Nagykun-Szolnok-Megyében 1999-ben és 2000-ben több természeti és civilizációs katasztrófa, valamint katasztrófa helyzet alakult ki. A döntéshozóknak szüksége volt pontos jól előkészített javaslatokra és ezt rövid idő alatt kellett biztosítani. A meglévő adatbázisok, tervek – légyen papíron, vagy Excel táblázatban- nem biztosították a gyors és megbízható döntéselőkészítést. A kommunikáció eszközei, az informatika, a térinformatika meglévő lehetőségeit kihasználva kialakítottuk az interaktív adatbázisunkat.

13. dia:

Az interaktív térinformatikai adatbázis bemutatására feltételezés alapján Tiszapüspöki, Fegyvernek, Szajol, Örményes, Kuncsorba, települések teljes megelőző kitelepítésével, valamint Törökszentmikós egy kisebb területének kitelepítésével kell számolnunk.

Az egyszerűbb áttekinthetőség, az útvonalak megjeleníthetősége miatt a kitelepítési tervezését két képre bontottuk.

14-15. dia kitelepítési adatok táblázat:

Az előbb említett, térképpel összekapcsolt adatbázisok lehetővé teszik a gyors, szemléletes elemzések végrehajtását. A három térképen kijelölt (sárga) település adatai az összesítő táblázatból azonnal automatikusan kijelölődnek, előrehozhatók és helyben összesíthetők.

kitelepítési útvonal táblázat:

A kitelepítési útvonal meghatározása után az azonnal térképre vihető, ha szükséges megjelölhetők és a Rendőrség részére átadhatók a szükséges útlezárási pontok.

befogadási adatok táblázat:

A kijelölt befogadási helyekről is azonnal előhozható az adataikat tartalmazó táblázat, amelyről azonnal leolvasható, hogy esetlegesen milyen kiegészítő készletekről (fekvőhelyek, ivóvíz, étkeztetés, stb.) kell gondoskodni a befogadóhelyek számára.

16-20 dia

-A szolgáltatott adatok alapján megjeleníthető a kérdéses területen a védekezésben maradók (pirossal), a várhatóan saját elhatározásból nem kitelepülők aránya (narancssárga) a lakosság létszámához (zöld) képest.

Itt kell megjegyeznünk, hogy adott esetben ilyen és ehhez hasonló adatok illetéktelen kezekbe kerülve alkalmasak lehetnek pánikkeltésre. Ezért rendkívül fontos az egész hálózat és minden elemének védelme, az adatforgalom titkosítása.

21. dia

A térinformatikai szoftverek lehetőségeit kihasználva természetesen az adatbázisok szemléletes, a döntést megkönnyítő elemzésére sok lehetőség adódik.

Jelen példánkon továbbhaladva, az állatállomány befogadásának tervezése a következő lépés:

A kitelepítendő állatállomány adatait a szoftver segítségével, az összetételt és a nagyságrendeket szemléltető grafikonokon is megtekinthetjük településenként.

22. dia

A számosállatok befogadási lehetőségeinek bemutatására néhány pillanat alatt átállíthatjuk a térképünket, ahonnan a mennyiséggel arányos színmélységekből következtethetünk a befogadóképességekre.

23-24. dia

Szintén a 2000. év tapasztalata, hogy a baromfiállomány kitelepítését a nagy létszámú tenyésztőtelepeknél, a különleges szállítási igény biztosítása miatt teljesen külön kell kezelni, egyébként igen nagy elhullással kell számol-

ni. A kitelepítendő baromfiállományt is egy arányosan színezett tematikus térkép segítségével képernyőre kérhetjük.

25. dia

Az előzőekben bemutatotthoz hasonlóan a térkép mögötti adattáblázatból természetesen azonnal meghatározható a kérdéses területen a kitelepítés első, és második üteméhez a személyszállító eszköz igény, legyen a szóló autóbusz, csuklós autóbusz, vagy ahol a lehetséges vasúti személyvagon.

26. kép:

A befogadóhelyek készletpótlási igénye is lekérdezhető. A jelen tematikus térképen például a látható, hogy az egyes befogadó települések intézményi elhelyezés és szükségtáborhely kialakításával történő elhelyezés esetén mennyi fekvőhelyet igényelnek a központi készletből.

27. kép:

Másik fontos kérdés árvízi veszélyeztetettségnél a várható elöntési területen lévő veszélyes anyagokat tároló, felhasználó üzemek, veszélyes hulladék lerakók, növényvédő szer raktárak, dögkutak helyének pontos ismerete. A képen éppen a területen lévő veszélyes üzemek helye látszik.

28. kép:

A következő képen, pedig azt láthatjuk, hogy egy-egy pontra rámutatva természetesen azonnal lekérhetjük az üzem adatait: elérhetőségeit, a tárolt anyagok fajtáit mennyiségét.

Bemutatom az interaktív térinformatikai adatbázis következő alkalmazási lehetőségét egy belterületi földmunkák során feltételezetten feltárt, fel nem robbant II. Világháborúból visszamaradt robbanótest hatástalanítása során elvégzendő feladatok tervezését.

29. dia

A helyi katasztrófa helyzetek kezelése a Helyi Védelmi Bizottság feladata. A védelmi bizottság vezetője a polgármester, tagjai a helyi szintű szervezetek vezetői munkatársai, akik segítik a polgármester döntéseinek előkészítését, végrehajtását.

Egy helyzet kezelésében a megfelelő döntés meghozatalának döntő momentuma az információ gyűjtése, rendszerezése, a döntésben résztvevők részére történő továbbítása.

Ezen információk jelentik a tervezés alapjait, ezeken nyugszanak az egyes alternatívák. Ezek az információk jelentik az alap adatait az erő-eszközszámításnak, a végrehajtáshoz szükséges idő meghatározásának.

30-31. dia

Tiszafüreden a város 1: 1000 léptékű vektorizált térképét használtuk fel.

A lépték nagyságból is látható, hogy igen részletes térképről van szó, melyen az egyes azonos célú térképi objektumok rétegekre szervezve jelennek meg. A térképet tehát objektumok, rétegek rendszere, egysége alkotja

Minden térképi objektumhoz adatbázis kapcsolat hozható létre, így a továbbiakban az objektum megtalálható a kapcsolt adatok, illetve az egyes részadatok is megtalálhatók az objektumok alapján.

Ha például olyan objektumot keresek, amelynek térképi elhelyezkedését nem, de valamely rész adatát ismerem, az objektum megtalálható. Ha azonos adattal rendelkező több objektum is van, mind megjelenik a térképen. Ugyanígy fordítva.

Több objektum, adatsor megjelenésekor a szükséges elemzéseket már el lehet végezni.

32. dia

Tiszafüred térképéhez kapcsolódó adatbázist úgy alakítottuk ki, hogy több célra felhasználható alapadatok rendszere álljon össze.

Az egyes rétegeken lévő objektumokat más-más adatbázis tartalommal láttuk el. Ezen a dián a lakóépületek adatai láthatók.

Így egyrészt az épületek megtalálásához szükséges adatok kerültek az adatbázisba, másrészt az épületekben lakók számadatai, illetve járulékos adatai.

A járulékos adatoknál olyan adatok is megjelennek, amelyek a végrehajtás folyamatos ellenőrzése során keletkeznek majd.

Az adatbázist egy un. házi szabvány alapján építettük fel, előre gondolva az elemzések elvégzésére.

Az adatbázis folyamatosan bővíthető a felmerülő igények alapján.

33. dia

Ezen a dián, a lakóépületeken túli másik nagyon lényeges terület a középületek adatbázis felépítése látható, melynek elkészítése során szintén az univerzalitásra törekedtünk. Az alapadatokon túlmenően szintén „házi szabvány szerint” feltüntettük az egyes középületnél a funkcióját (oktatás, orvosi ellátás, élelmiszer kereskedelem, élelmiszer előállítás, melegkonyha, építőanyag előállítás, építőanyag kereskedelem, stb.), valamint az épületben, a vállalkozás telephelyén mekkora létszám, hogyan helyezhető el. Így más esetben is (rendkívüli hó, árvíz, belvíz) felhasználható az adatbázis.

34-42. dia

Az elemzések videó filmje esetünkben egy adott pont köré rajzolt 600 méter sugarú körbe eső lakó és középületek összességének leválogatását mutatja. A befogadó helyek adatainak elemzéséről készített diákon az elemzés egy-egy fázisa látható

Az útvonal meghatározásáról készült diákon az útvonal rajza, valamint a robbanótest szállítása során veszélyeztetett sáv szélessége látható. Az elemzés során az is kiderült, hogy az érintett sávban veszélyes üzem is található, a dián az üzem adatai láthatók

43. dia

A forgalomelterelés elemzése: a dián látható a térkép egy része, a forgalom irányító pontok elhelyezkedésével, adataival. Ezen pontok jelentősége a lakos-

ság, a járművek mozgásának irányításában, de egy esetleges veszélyes anyag szállítmány figyelemmel kísérésében is jelentős

Tisztelt Hölgyeim, és Uraim!

Tisztelt Konferencia!

KÖSZÖNÖM MEGTISZTELŐ FIGYELMÜKET!

SIPOS Mihály

A MAGYAR ELEKTRONIKAI IPAR A RENDSZERVÁLTÁS UTÁN

A 2002. év immár a hatodik éve az ipari, ezen belül pedig a feldolgozóipari termelés lendületes növekedésének. Ez leginkább a tágabb értelemben vett gépipar eredményeinek köszönhető. Az iparág szárnyalása azt jelzi, hogy a magyar gazdaságnak van egy egészséges magja, amit elsősorban annak köszönhetünk, hogy itt meghatározó mértékben és a legelsők között zajlottak le a szükséges változások. Tény, hogy az egész ipart tekintve egyedül csak a gépipar volt képes arra, hogy nemcsak elérje, de túl is szárnyalja az 1989-es termelési szintet, a többi ágazat sajnos még nem képes erre. Vagyis nincs szó általános növekedésről, hanem csak néhány szakágazat boomjáról. A gépiparon belül az egyik legdinamikusabban fejlődő szakágazat az elektronikai ipar. Az iparágat az elmúlt 10-12 évben az alábbiak jellemezték:

Mint az hazánk legújabb kori történelméből közismert, az 1980-as évek közepére a magyar gazdaság egésze válságba került. A korábban elért életszínvonal csak nagy áldozatokkal, tekintélyes eladósodottság árán volt tartható. Ez a krízis vezetett el a gazdasági és politikai rendszerváltáshoz.

Ekkortájt a híradástechnikai, elektronikai iparágat meghatározó módon Budapest központú voltság, illetve a felső utasításra létrehozott vidéki telephelyek jellemezte. Ettől eltérést alig egy-két vállalat mutatott: pl. a Videoton Székesfehérvárott. A vállalatok KGST és Varsói Szerződés orientáltak voltak, ugyanakkor fejlesztéseik a COCOM restrikcióktól sújtottak. Ez végső soron azt jelentette, hogy nem tudtak bekapcsolódni az igazi nemzetközi munkamegosztásba. Ennek következtében a rendszerváltást követően – a régi piacok elvesztése, illetve az újakra való alacsony penetráció miatt – az iparág termelése 1989. és 1993. között 40 %-kal csökkent. A termelés visszaesése különösen 1990-ben és ’91-ben volt erőteljes, amelyet 1992-ben stagnálás követett. Megkezdődött a vállalatok tulajdonosi szerkezetének átalakítása.

1993-ban megindult egy szerény növekedés, az iparág termelése némileg nőtt, az exportteljesítmény azonban még csökkent. 1994-ben a magyar ipar képes volt kihasználni a szerény nyugat-európai konjunktúrát, de a szerkezetváltás folyamatában még csak a kezdeti lépéseknél tartott. Új tulajdonosi formák jöttek létre.

Bár 1995-től kezdve felgyorsult az iparági szerkezetváltás, 1997. volt az első igazi éve a gazdaság növekedésének. A korszerű technológiák hazai bevezetése csak a befektetések növekedése mellett képzelhető el tartósan és hosszú távon. A hazai korlátozott (sőt, elégtelen) tőkeforrások miatt döntő szerep jutott és jut továbbra is ezen a téren a külföldi tőkének. Az új tulajdonosi kör meghatározóan külföldi szakmai befektető. Jellemző módon tehát ezek azok az

évek, amikor megjelentek hazánkban azok a multinacionális cégek is, amelyek termelésükkel és exportjukkal a nemzetgazdaság fő erejét alkotják.

Ettől kezdve az ipari növekedés forrása a gépipar, amelyen belül kiemelkedő szerepe van az elektronikai iparnak és háttériparának; a termelés 45-50%-kal növekedett. Ezt a növekedést változatlanul az export dinamikus bővülése alapozta meg. Az élénk fejlődést alapvetően a Magyarországon befektető multinacionális vállalatok biztosítják, amelyek száma napjainkban is tovább gyarapszik.

Az újonnan hazánkba érkező elektronikai cégek egészen a legutóbbi időkig jellemző módon két földrajzi területen koncentrálódtak: Budapest vonzáskörzetében és a Dunántúlon. Ez utóbbi esetében – a már említett Székesfehérvár kivételével – új termelési struktúrák, eddig ott nem látott iparág létrejöttéről beszélhetünk. Ezzel megindult egy földrajzi (a volt jugoszláv, illetve az osztrák határ mint politikai/gazdasági barrier), infrastrukturális (korábban eltérőek voltak a domináns fő szállítási és közlekedési irányok) szempontból hátrányos pozíciójú tájegység fejlődése. 2000-től pedig egy újabb térségben, Kelet-Magyarországon indulnak be új beruházások.

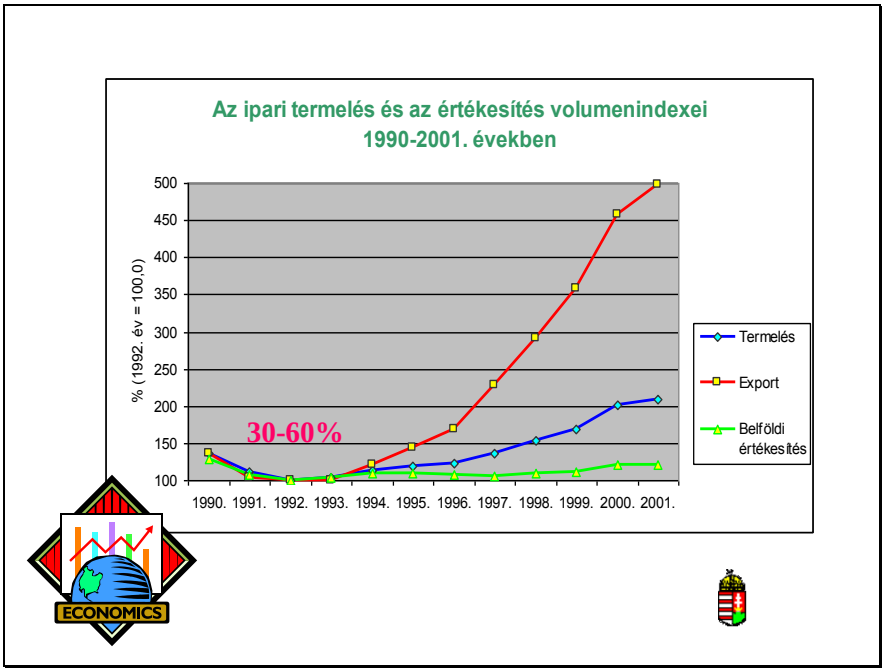
A magyar elektronikai ipar a rendszerváltás után

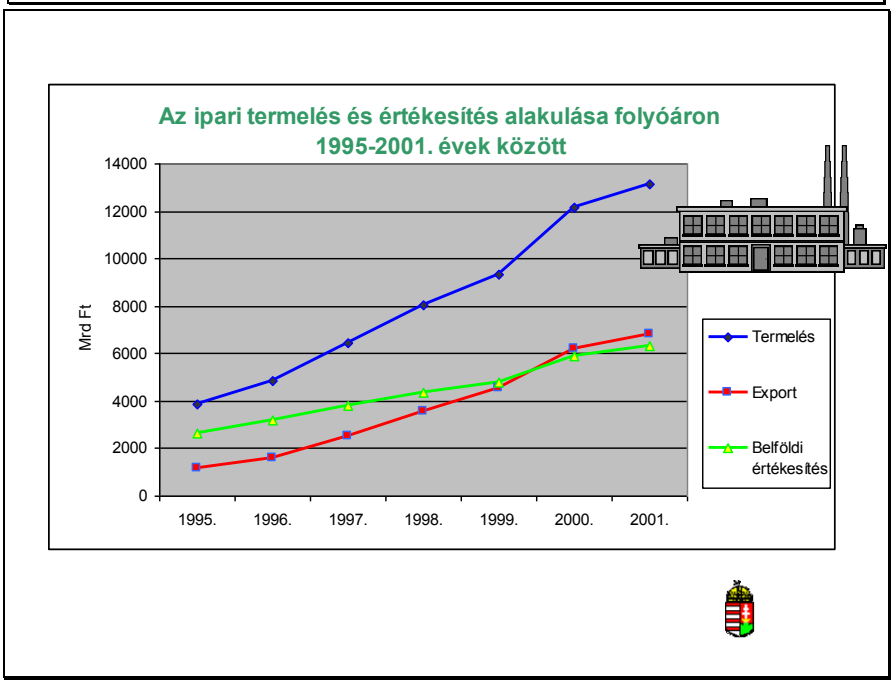
GAZDASÁGI ÉS KÖZLEKEDÉSI MINISZTÉRIUM IPARI FŐOSZTÁLY

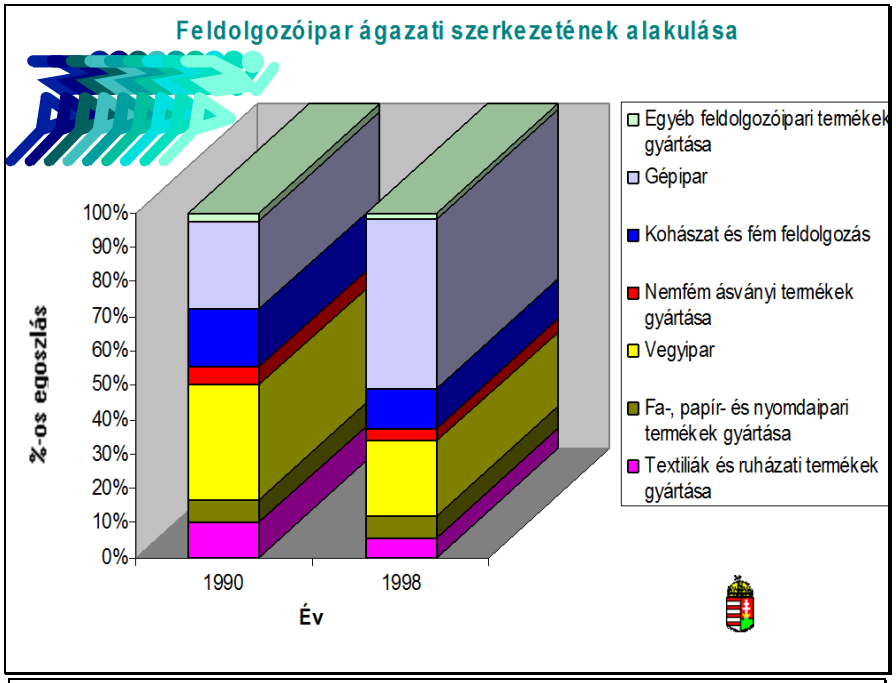
1880 Budapest Pf. 111

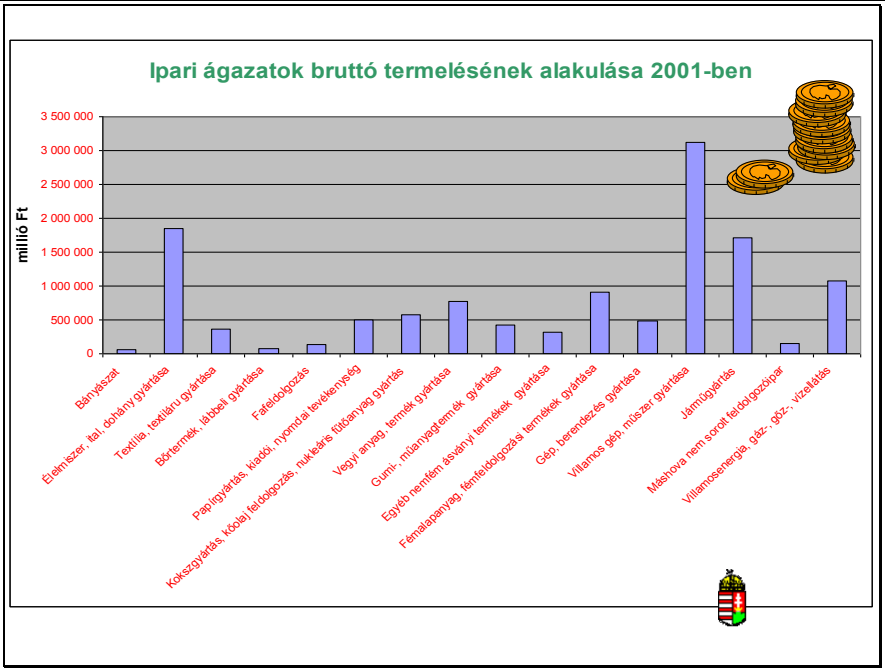
Előadó: Sipos Mihály osztályvezető

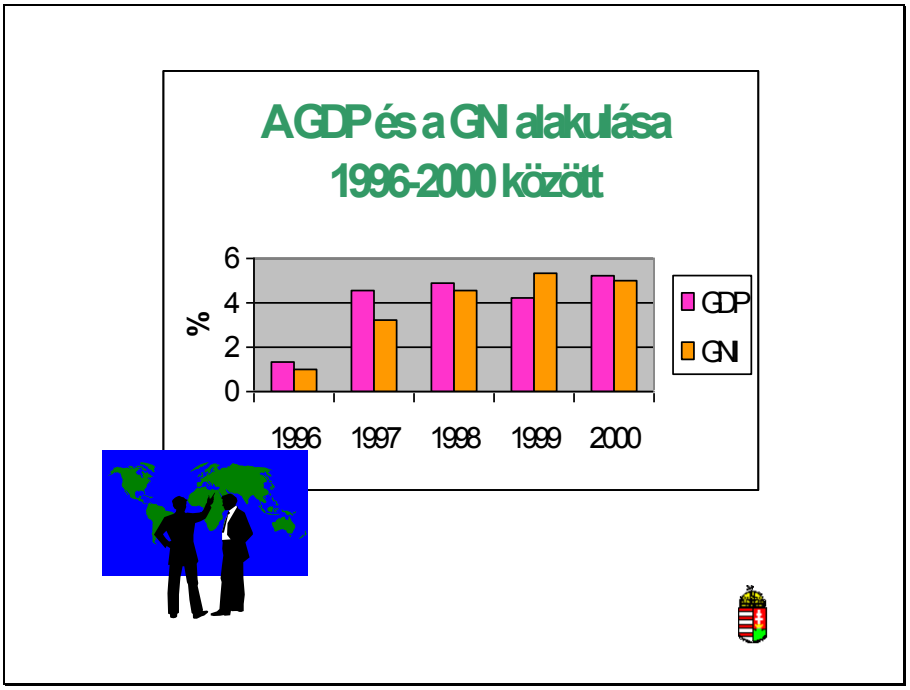
E-mail: mihaly.sipos@gmv.gov.hu telefon:472-8629

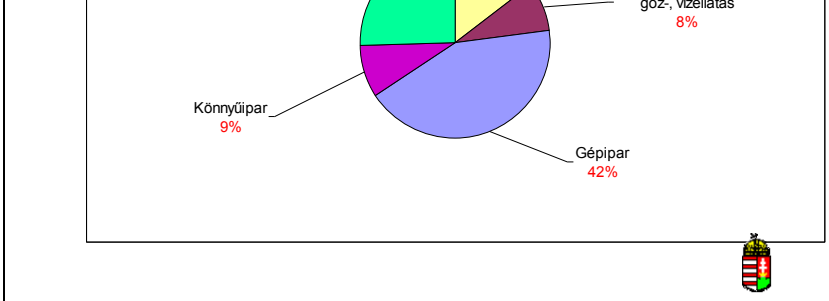

Az ipari termelés és az értékesítés volumenindexei
1990-2001. években
% (1992. év = 100,0)
500
450
400
350
300
250
200
150
100
30-60%
1990. 1991. 1992. 1993. 1994. 1995. 1996. 1997. 1998. 1999. 2000. 2001.
Termelés
Export
Belföldi értékesítés
ECONOMICS


Az ipari termelés és értékesítés alakulása folyóáron
1995-2001. évek között
Mrd Ft
14000
12000
10000
8000
6000
4000
2000
0
1995.
1996.
1997.
1998.
1999.
2000.
2001.
Termelés
Export
Belföldi értékesítés


Feldolgozóipar ágazati szerkezetének alakulása
%-os egoszlás
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
1990
1998
Év
Egyéb feldolgozóipari termékek gyártása
Gépipar
Kohászat és fém feldolgozás
Nemfém ásványi termékek gyártása
Vegyipar
Fa-, papír- és nyomdaipari termékek gyártása
Textiliák és ruházati termékek gyártása


Ipari ágazatok bruttó termelésének alakulása 2001-ben
millió Ft
3 500 000
3 000 000
2 500 000
2 000 000
1 500 000
1 000 000
500 000
0
Bányászat
Élelmiszer, ital, dohány gyártása
Textília, textiláru gyártása
Bőrtermék, lábbeli gyártása
Fafeldolgozás
Papíripar, kiadói, nyomdai tevékenység
Kokszgyártás, kőolaj feldolgozás, nukleáris fűtőanyag gyártás
Vegyi anyag, termék gyártása
Gumi-, műanyagtermék gyártása
Egyéb nemfém ásványi termékek gyártása
Fémalapanyag, fémfeldolgozási termékek gyártása
Gép, berendezés gyártása
Villamos gép, műszer gyártása
Járműgyártás
Máshova nem sorolt feldolgozóipar
Villamosenergia, gáz-, gőz-, vízellátás


A GDP és a GN alakulása
1996-2000 között
6
4
2
0
%
1996
1997
1998
1999
2000
GDP
GN


Az ipar bruttó termelési értékének
megoszlása 2001-ben
Élelmiszer, ital,
dohány gyártása
15%
Egyéb ipar
26%
Villamosenergia, gáz-
gőz-, vízellátás
8%
Könnyűipar
9%
Gépipar
42%

A gépipar súlya az ország bruttó kibocsátásában

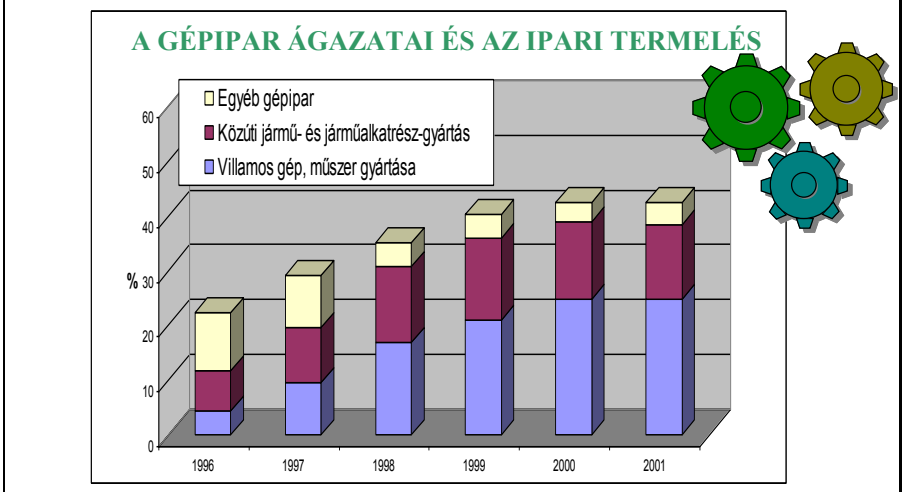
Termelés : Szolgáltatás = 55 : 45

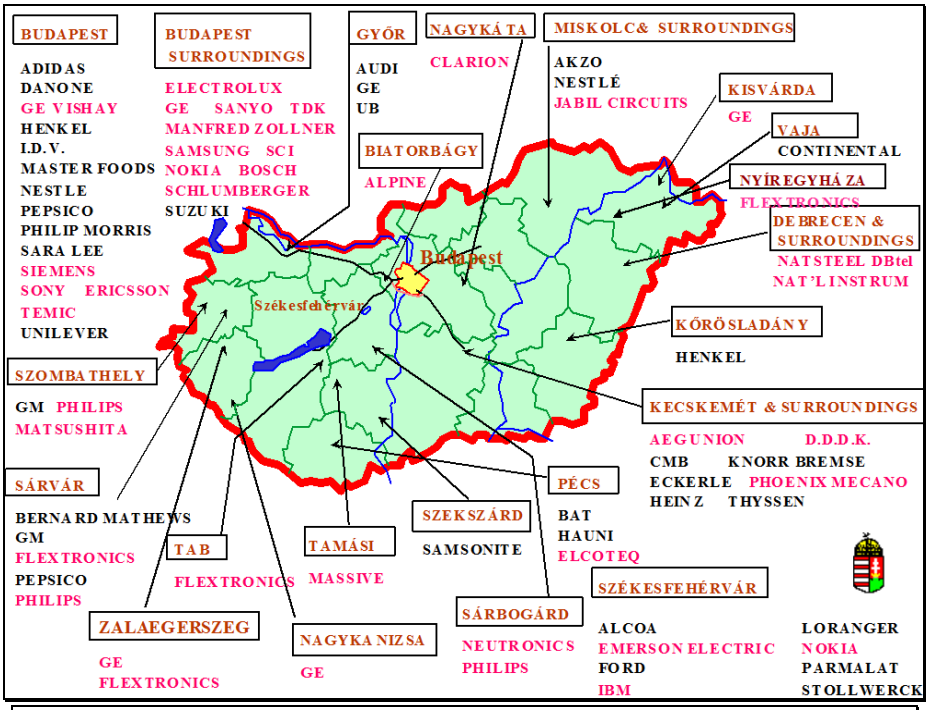
A termelésből:

Ipar: 82%, mezőgazdaság 9%, építőipar 9 %

Iparból: gépipar 42 %,

azaz a termelés 34-35 %-a!!!!




BUDAPEST
ADIDAS
DANONE
GE VISHAY
HENKEL
I.D.V.
MASTER FOODS
NESTLE
PEPSICO
PHILIP MORRIS
SARA LEE
SIEMENS
SONY ERICSSON
TEMIC
UNILEVER
BUDAPEST SURROUNDINGS
ELECTROLUX
GE SANYO TDK
MANFRED ZOLLNER
SAMSUNG SCI
NOKIA BOSCH
SCHLUMBERGER
SUZUKI
GYŐR
AUDI
GE
UB
NAGYKÁTA
CLARION
MISKOLC& SURROUNDINGS
AKZO
NESTLÉ
JABIL CIRCUITS
KISVÁRDA
GE
VAJA
CONTINENTAL
BIATORBÁGY
ALPINE
NYÍREGYHÁZA
FLEXTRONICS
DEBRECEN & SURROUNDINGS
NATSTEEL DBtel
NAT'L INSTRUM
Budapest
Székesfehérvár
KÖRÖSLADÁNY
HENKEL
SZOMBATHELY
GM PHILIPS
MATSUSHITA
KECSKEMÉT & SURROUNDINGS
AEGUNION
D.D.D.K.
CMB
KNORR BREMSE
ECKERLE
PHOENIX MECANO
HEINZ
THYSSEN
SÁRVÁR
BERNARD MATHEWS
GM
FLEXTRONICS
PEPSICO
PHILIPS
TAB
FLEXTRONICS
TAMÁSI
MASSIVE
SZEKSZÁRD
SAMSONITE
PÉCS
BAT
HAUNI
ELCOTEQ
SZÉKESFEHÉRVÁR
ALCOA
EMERSON ELECTRIC
FORD
IBM
LORANGER
NOKIA
PARMALAT
STOLLWERCK
ZALAEGERSZEG
GE
FLEXTRONICS
NAGYKANIZSA
GE
SÁRBOGÁRD
NEUTRONICS
PHILIPS


Köszönöm megtisztelő figyelmüket!

186

Dr. KOCZKA Ferenc

A HUSZONNEGYEDIK ÓRÁBAN… INFORMÁCIÓVÉDELMI SZAKÁLLOMÁNY KÉPZÉSE A ZMNE KATONAI TÁVKÖZLÉSI ÉS TELEMATIKAI TANSZÉKÉN

Bevezetés

A Magyar Honvédség információs környezete átalakulóban van és a közeljövőben a haderő életének valamennyi területére kihat a vezetési és információs rendszerek gyorsütemű fejlesztése. Ezen rendszerek kiépítése és üzemeltetése felértékeli az információvédelem szerepét. A rendszerek korszerűsítésében testet öltő információs technológiaváltással együtt a humán erőforrás felkészítésében is alapvető változások szükségesek.

Magyarország a NATO szövetségi rendszeréhez történő csatlakozáskor kötelezettséget vállalt a minősített adatok védelmére, a NATO Biztonsági Szabályzatában meghatározottak szerint. Az információk védelme, az információs rendszer biztonsága szerves része az általános biztonságnak, ezért követelményeit az általános biztonság komplex rendszerének részeként kell meghatározni. Ennek szellemében kell fejleszteni az információvédelem állami rendszerét, korszerűsíteni az információvédelmi eszközöket, üzemeltetésük ellenőrzését, működtetésük rendszerének auditálását és kialakítani az információvédelmi szakemberek képzésének és felkészítésének egységes rendszerét.

A feladat végrehajtása érdekében a HM HVK Vezetési Csoportfőnökség Biztonsági Osztálya elkészítette az információvédelmi szakemberképzés elgondolását [1]. Ennek megfelelően 2002. novemberében – kezdetben még csak tanfolyami formában – a ZMNE BJKMFK Katonai Távközlési és Telematikai Tanszékén megkezdődik a megrendelő szakmai követelményeit kielégítő képzés.

A cikk írójának nem célja az elgondolás ismertetése, sokkal inkább – mint felsőoktatási menedzser – ezen elgondolásból saját szervezetére (tanszék, főiskolai kar) háruló feladatok áttekintése, az információvédelmi oktatási kultúra ismételt meghonosítása a Nemzetvédelmi Egyetemen, a Magyar Honvédség igényeinek mind magasabb szintű kielégítése érdekében.

Röviden a Katonai Távközlési és Telematikai Tanszékről

A tanszék ZMNE Bolyai János Katonai Műszaki Főiskolai Kar oktatási szervezeti egysége. Alaprendeltetése a tiszti hallgatók főiskolai szintű képzése. A tanszéken belül három szakcsoport feladata a szakirányú - híradó, rádielektronikai felderítő és az elektronikai hadviselés - felkészítés.

A Híradó Szakcsoport – 10 fős létszámmal – végzi az alap nappali és levelező képzési formákban tanuló híradó tancsoportok képzését. Végzett hallgatóink a tiszti kinevezési okmány mellett, híradó (távközlési) szakirányú villa-

mosmérnöki oklevelet vehetnek át. A szakcsoport alaprendeltetéséből adódó feladatai mellett végzi:

- a más szakokon tanulmányokat folytató főiskolai hallgatók híradó szakirányú képzését,
- tartalékos híradótisztek képzését (szakirányú polgári egyetemet és főiskolát végzettek), 2 tancsoport/év leterheltséggel,
- híradótisztek, tiszthelyettesek és közalkalmazottak szakmai továbbképzését 2-4 hét időtartamban, 4-6 tancsoport/év leterheltséggel,
- tiszti karriertanfolyamok (fhdgy., szds.) tananyagának kidolgozását, a képzés végrehajtását 2 tancsoport/év leterheltséggel.

A tanszék, a Híradó Szakcsoport azonosult a megrendelő – HVK Vezetési Csoportfőnökség, MH Elektronikai Szolgálatfőnökség – az irányú elvárásaival, hogy vegyen részt a rendszerbe állításra tervezett és rendszerbe állított infokommunikációs eszközök üzemeltetésére és üzemben tartására történő felkészítésben, működjön egyfajta szakmai továbbképző központként is. Ez a feladat az utóbbi években egyre hangsúlyosabb, melyet az itt leírtak is erősítenek.

A tanszék javuló infrastrukturális feltételekkel kezdte meg az új tanévet, melynek során három kiemelt területen kíván jelentősen előrelépni. Ezek az információvédelmi képzés, a mikrohullámú rádióberendezések oktatásához szükséges infrastruktúra és tananyagalkotás, valamint a híradó gyakorlati képzés. Mindhárom területen a kitűzött cél elérése javítja a képzés minőségét, de közülük is kiemelkedik az információvédelmi szakállomány képzése, mely átmeneti szüneteltetés után ismét megjelenik az alapfokú tisztképzést végző szervezet képzési struktúrájában.

Az információvédelmi képzés beillesztése a főiskolai kar képzési struktúrájába

„A főiskolai kar felvállalja az infokommunikációs eszközök alkalmazásához kapcsolódó képzési, át- és továbbképzési feladatokat” [2]. Az információvédelmi képzés bevezetése nem más, mint az intézményfejlesztési terv jövőképében megfogalmazottak konkrét, gyakorlati végrehajtása. A kar tervezett képzési struktúrájába az információvédelmi képzés elméletileg gond nélkül beilleszthető.

A tanszék, az egyetem felvállalta az információvédelmi képzés menedzselését, mely az előkészítés, bevezetés és a végrehajtás fázisaiban megbízható támogatást ad a szakterületen oktatók számára. Ez megnyilvánul:

- az információvédelmi képzési infrastruktúra beépítéséhez szükséges elhelyezési és kommunikációs feltételek biztosításában,
- az oktatói állomány munkafeltételeinek kialakításában,
- a képzés végrehajtásához – az információvédelmi eszközök rendszerben történő üzemeltetéséhez – szükséges távközlő, valamint informatikai hálózatok rendelkezésre bocsátásában,

- a képzési okmányok kidolgozásának segítésében, különös tekintettel a főiskolai kimenetű információvédelmi szakirány indításában, képzésének megszervezésében,
- a képzések végrehajtásához szükséges hallgatói szolgáltatások biztosításában.

Mindez elképzelhetetlen lett volna az egyetem és a HM HVK J-6 korábban kialakult jó együttműködése nélkül.

Általános információvédelmi képzés

Az általános információvédelmi képzés fegyvernemi hovatartozástól függetlenül segíti az állományt a bizalmas, illetve minősített információkkal történő napi munka végzésében, illetve vezetőként az információs biztonság feltételeinek kialakításában, a szabályszerű működés fenntartásában.

A Vezetési Csoportfőnökségnek mint megrendelőnek el kell érni, hogy a tiszti állomány információvédelmi felkészítését a főiskolai képzés időszakában kezdjék meg minden alapképzési szakon. Ezt célszerűen az MH PK VKF 35/1997. (HK10) intézkedésének módosításával lehet elérni, mert az abban jelenleg szereplő egymondatos utalás a titokvédelmi rendszabályok alkalmazóképes ismeretére nem fedi le ezen a területen tisztjeinktől elvárt tudást, a személyi, fizikai, dokumentum és az elektronikus információ biztonság követelményeinek kielégítéséhez kapcsolódó ismereteket és gyakorlati jártasságokat.

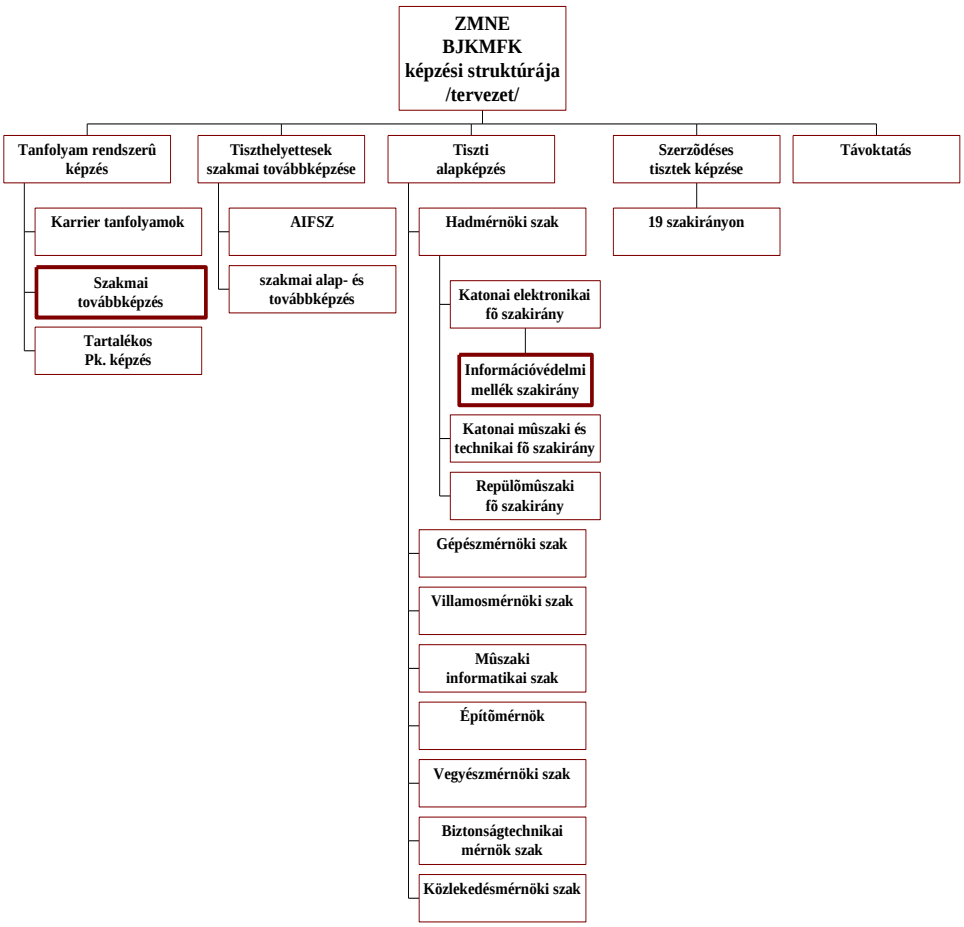
Információvédelmi szakképzés

Tiszti alapképzés információvédelmi mellékszakirányon

Információvédelmi tisztek alapképzésben történő felkészítésére elsősorban a szakindításra tervezett hadmérnöki szakon van lehetőség, a katonai elektronikai fő szakirányon belül, információvédelmi mellék szakirányon. Az 1. ábrán vastagított kerettel jeleztem az iformációvédelmi szakmai követelményeket kielégítő képzési formákat.

A hadmérnöki szak kifejezetten a megrendelői igények kielégítése érdekében kerül alapításra és nyolcadik szakként a mérnöktiszt-képzés struktúrájába. A szak képzésének lényege, hogy megfelel a műszaki felsőoktatás képesítési követelményeinek [3], de ugyanakkor a csapatok kis létszámú és differenciált tiszti igényeit is gazdaságosan elégíti ki. Ennek érdekében például a katonai elektronikai fő szakirányon folyó képzés az első három évben egységes és csak negyedikben, a csapatok egy évvel előre jelzett igényeinek megfelelő létszámban választhatnak a hallgatók mellék szakirányt. Jelenlegi elgondolás [4], szerint a következő képzési kínálatból lehet választani: légvédelmi rakétatechnikai, lokátortechnikai, híradó, információvédelmi, rádióelektronikai felderítő, elektronikai hadviselés, informatikai.

A legkorábban 2004-ben indítható hadmérnök-képzés keretében szakmailag korrekt módon biztosítható tiszti alapképzésben, az információvédelmi beosztásokra történő felkészítés. Ezzel egyidejűleg a mérnöktiszti oklevél egzisztenciális biztonságot is ad tulajdonosa számára. A szakindításban egyetértés van az egyetem és a főiskolai kar között, hiszen az új szak biztosítja a lineáris képzés megvalósításának lehetőségét, így az első három egységesen végrehajtott képzési év után – megrendelői igény esetén – a hallgató azonnal megkezdheti az egyetemi végzettséget biztosító további két évet. A megrendelő joga eldönteni, hogy az alapképzésben (2.2.1. pont), vagy tanfolyami rendszerben (2.2.2. pont) látja célszerűbbnek a képzés végrehajtását.



1.ábra

2.1.1. Információvédelmi tisztek szakképzése tanfolyami rendszerben

Hadmérnök-képzésben az első kibocsátásra leghamarabb 2008-ban kerülhet sor. Addig nem várhat az információvédelmi ágazat, tehát a jelenlegi képzési rendszerre alapozva, tanfolyami rendszerben kell biztosítani a szaktiszti állomány utánpótlását, felkészítését.

Az információvédelmi szakállomány tevékenysége szorosan kapcsolódik a távközlési és az informatikai szakterülethez. Munkája során együtt kell működjön a katonai és polgári távközlési- és informatikai szolgáltatókkal, valamint a NATO információbiztonsági szerveivel és azok rendszereivel. Ahhoz, hogy ebben a közegben a beosztásuknak megfelelően eredményesen tevékenykedhessenek, a tiszteknek rendelkezniük kell:

- híradó (távközlési), vagy informatikai szakirányú főiskolai végzettséggel és
- angol nyelvismerettel. Az információvédelmi beosztások ellátásához szükséges végzettséget a ZMNE BJKMFK villamosmérnöki szak **híradó szakirányán**, illetve **műszaki informatikai szakán** célszerű elsajátítani.

Ebben az átmeneti időszakban (2008-ig) a beiskolázásra tervezett hallgatói létszámokat – a képzést felügyelő szakmai főnökségekkel egyeztetve – a feltöltetlen információvédelmi hadnagyi beosztások függvényében növelni kell.

Az információvédelemmel kapcsolatos speciális szakismeretek oktatására később, tanfolyamrendszerben célszerű sort keríteni. A Magyar Honvédségnél eltöltött egy-két év gyakorlat után az információvédelmi terület iránt érdeklődő, arra javasolt és alkalmas (kockázatmentes nemzetbiztonsági felülvizsgálati eredmény) tisztek információvédelmi szakképzés keretében kerülnek át- és továbbképzésre, melynek elvégzése után tervezőkként, irányítókként, illetve felügyelőkként tölthetnek be beosztásokat [1].

Tiszthelyettesek információvédelmi szakképzése tanfolyami rendszerben

Tiszthelyettesek információvédelmi szakképzése tanfolyami rendszerben a tisztek – 2.2.2. pontban leírt – felkészítésével analóg módon valósulna meg. Tehát a híradó, vagy informatikai szakon végzett tiszthelyettes néhány év csapatgyakorlat után tanfolyami rendszerben szerezné meg az információvédelmi beosztások ellátásához szükséges szakmai ismereteket, gyakorlati jártasságokat. A ZMNE Katonai Távközlési és Telematikai Tanszéke felkészült (és jelenleg is folytat) a tiszthelyettesi szaktanfolyamok végrehajtására, amennyiben erre megrendelést kap.

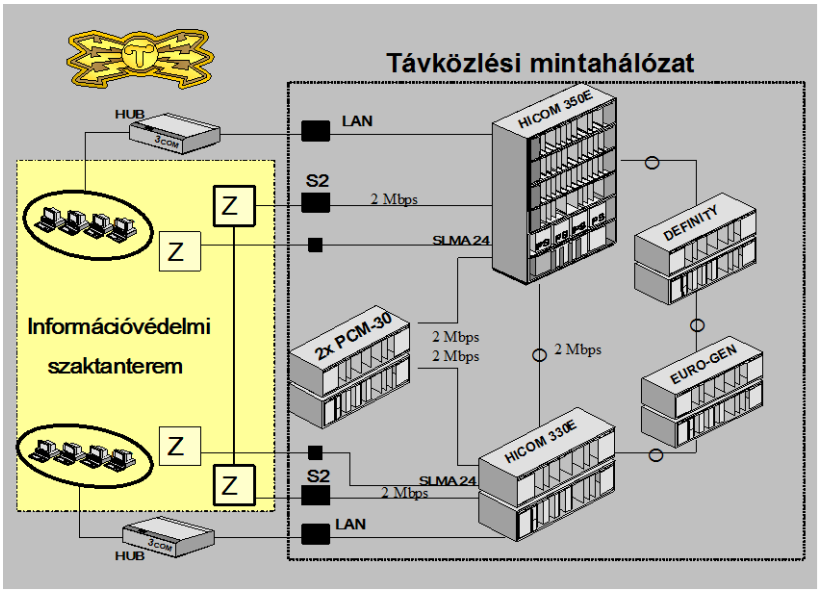
Végzés után a tiszthelyettesek kezelőkként, vagy nyilvántartókként kerülnek információvédelmi beosztásokba.

A Katonai Távközlési és Telematikai Tanszék képzési infrastruktúrájának felhasználása az információvédelmi szakképzésben

A tanszék a több lépcsőben végrehajtott korszerűsítés eredményeképp üzembe helyezett telematikai rendszer szaktantermek révén alkalmassá vált a

Magyar Honvédségnél rendszeresített és rendszeresítésre tervezett korszerű infokommunikációs eszközök üzemeltetésének és üzemben tartásának oktatására.

2. ábra



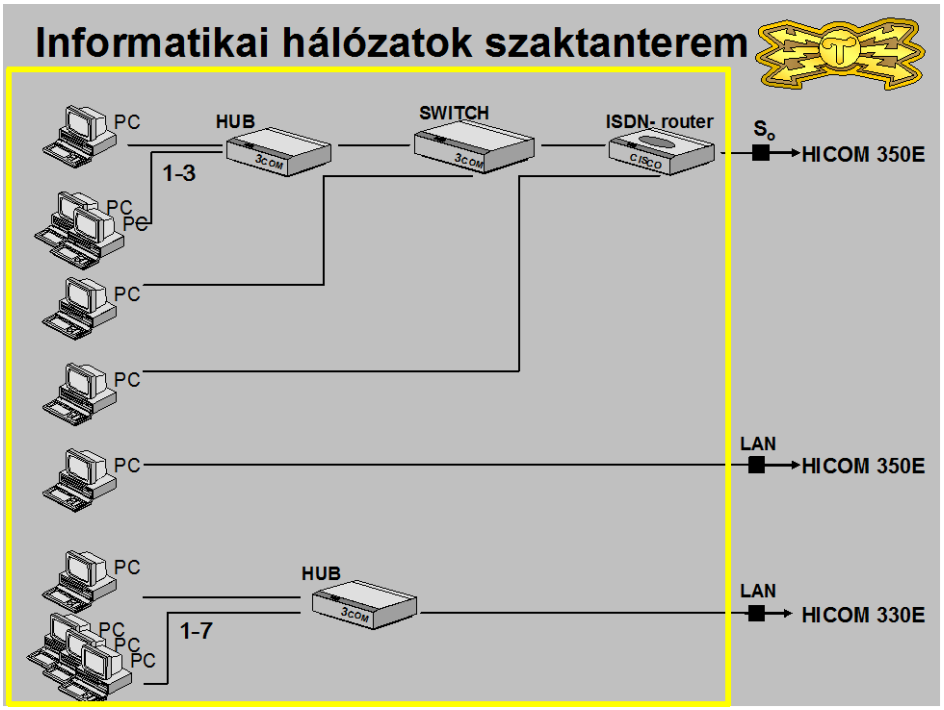
3. ábra

4. ábra

A fejlesztés révén kialakult négy alközpontos távközlési mintahálózat (2. és 3. ábra) alkalmassá vált az egyedi alközpontok oktatásán túl a hálózati felépítés és működés bemutatatására, az üzemeltetési jártasságok kialakítására. Ehhez szervesen kapcsolódnak az információvédelem biztosításának szakfeladatai, illetve azok gyakorlati végrehajtása. Itt elsősorban az összeköttetés védelem feladataihoz, az egyedi és csoportos rejtjelző (titkosító) eszközök távközlő hálózaton (rendszerben) történő üzemeltetéséhez kapcsolódó jártasságok kialakítása történik meg (3. ábra). Emellett a rendszer lehetőséget biztosít kisebb tancsoportok esetén az informatikai védelem gyakorlati feladatainak végrehajtására is.

Az információvédelmi szaktanterem informatikai eszközei között meg kell jelennie a tábori körülmények között is alkalmazható ellenőrzött kisugárzású számítógépeknek, a tantermi és kapcsolódó hálózatok kiépítésénél pedig törekedni kell a biztonságos hálózat követelményeinek kielégítésére. A Siemens TEMPEST technológiával készült számítógépei és FUTURAWay kábelezési rendszere megfelel ezen elvárásoknak.

Az informatikai biztonság oktatásához, a kapcsolódó gyakorlati jártasságok kialakításához a telematikai rendszer egy másik eleme, az informatikai hálózatok szaktanterem biztosít kedvező feltételeket (4. és 5. ábra).



5. ábra

A tantermi számítógépek (21 munkaállomás) egy stacioner helyi hálózathoz csatlakoznak és ez összekapcsolásra került a tanszéki és a főiskolai hálózatokkal. Ilyen módon a hallgatók egyéni oktatásán túl biztosított a ZMNE INTRANET és az INTERNET hálózatok elérése.

A tanterem stacioner hálózatának „szétszedésével", pótlólagos hálózati hardver elemek felhasználásával a szaktanterem lehetőséget biztosít (5. ábra):

- kisebb, egyenként 4-8 munkahelyes LAN-ok kialakítására (HUB, SWITCH),
- ezen kisebb hálózatok hálózati szoftvereinek telepítésére és a LAN-ok közötti kommunikáció biztosítására,
- a LAN-ok informatikai és távközlő csatornán (rádió, optikai, modem, ISDN) történő összekapcsolására, mely jól szimulálja a tábori (pl.: dandár fő harcálláspont) viszonyok között kialakított informatikai hálózatokon folyó munkát,
- a LAN-ok HICOM 350E, 330E digitális kapcsolóközpontokhoz történő csatlakoztatására, a LAN-ok központokon keresztül történő összekapcsolására.

A szaktanterem az informatikai védelem gyakorlati feladatai közül az alábbiakat képes kiszolgálni:

- személyi számítógépek biztonsági beállításai:
    - több felhasználó használ egy gépet: személyes beállítások, saját könyvtárak, policy editor telepítése és használata,
    - információ biztonság erőforrások megosztása esetén,
- szoftveres tűzfalak telepítése, konfigurálása. Csomag szűrő és alkalmazása, átjáró előnyei és hátrányai,
- vírusok és egyéb számítógépes kórokozók működési elve. A makrovírusok lehetőségei. Vírusok elleni védekezés módjai, gyakorlati megvalósításuk,
- informatikai védelem a hálózati eszköz (HUB, SWITCH, router) helyes megválasztásával, programozásával,
- összetett hálózatok létrehozása és ellenőrzése szoftveres protokollanalizátorral (hardver analizátor és teszter beszerzése pótlólagos beruházást igényel),
- informatikai hálózatok forgalmának figyelése információvédelmi szempontból fontos paraméterek alapján, szoftver és hardver eszközökkel.

Az információvédelmi képzési kultúra ismételt meghonosításával egy előremutató, egyre nagyobb jelentőségű feladatra történő felkészítés feltételei jönnek létre a katonai felsőoktatásban. A Nemzetvédelmi Egyetem a képzés megkezdésével is bizonyítja rugalmas reagálását a valós megrendelői igények kielégítésére. Meggyőződésem, hogy a fegyveres erők és a nemzetbiztonsági szolgálatok munkaerőpiacán az elkövetkező években egyre keresettebb lesz a felsőfokú végzettségű információvédelmi szakember.

A képzés megkezdése problémákat vet fel, elsősorban a főállású oktatói helyek túlterheltsége, hiánya miatt. Meg kell próbálni ebből a hátrányos helyzetből előnyt kovácsolni. Ez pedig a viszonylag nagy számú külső előadó által biztosított gyakorlat- orientált felkészítésben, a valós felhasználói igények kielégítésében jelentkezhet. További előnyös hatásként információvédelmi területen megjelennek azok az integrált felkészítésű szaktisztek, akik képesek a távközlési és informatikai hálózatok együttes üzemeltetésével járó műszaki problémák felismerésére és elhárítására, az információvédelem és a rendszer üzemeltetés biztonságának egyidejű megvalósítására.

A biztonság kincs, érték, mint a bizalom. A NATO tagországok egymás iránti bizalma rendülhet meg a titkokra vonatkozó előírások sérülésével, a védendő információk nem megfelelő kezelésével. Tudott dolog, hogy a titkok korrekt megtartására nem lehet születni, ezt meg kell tanulni és ennek nincs alternatívája. Annak sem, hogy az erre való felkészítés, az ismeretek frissítése, szinten tartása tudatos, rendszeres tevékenységgé kell hogy váljon [5].

A felhasznált irodalom jegyzéke:

[1] Mayer Csaba: A Magyar Honvédség információvédelmi képzésének elgondolása, HM HVK Vezetési Csoportfőnökség, 2002. szeptember
[2] Intézmény fejlesztési terv, Budapest, ZMNE BJKMFK, 2000. július
[3] l57/1996. (X. 22.) Kormányrendelet a műszaki felsőoktatás alapképzési szakjainak képesítési követelményeiről
[4] A ZMNE BJKMFK főigazgatójának éves beszámoló jelentése a kar 2001/2002 évben végzett munkájáról, Budapest, ZMNE BJKMFK Főigazgatói Hivatal, 2002. szeptember
[5] Kuti Ferenc, Kollár Antal: Biztonság és titokvédelem a NATO szabályai szerint, Budapest, Honvéd Kiadó, 1999

TESSEDIK Tamás

A TÁVBESZÉLŐ SZOLGÁLTATÓ VÁLLALATOK NEMZETBIZTONSÁGI ÉS NEMZETVÉDELMI KÖTELEZETTSÉGEIT MEGHATÁROZÓ JOG REND

Bevezetés

A távbeszélő cégeket funkcióik alapján többféle képen lehet csoportosítani. Nemzetbiztonsági szempontból, azonban alapvetően két részre oszthatóak, úgy mint piaci szereplők (front vagy elsődleges funkció) és biztonsági szereplők (back vagy másodlagos funkció). Az elsődleges és másodlagos funkciók meghatározását kizárólag az adott nemzet biztonsági pozíciója határozza meg.

A biztonsági pozíció meghatározásához szükség van a biztonság fogalmának és kockázati skálájának meghatározására. Egy nemzet biztonságának és fenyegetettségének kérdésével számos tudományág foglalkozik.

(*Itt az előadásomban a biztonság elfogadott, és jelenleg is alkalmazott fogalmak rendszerét rendszerét foglalom össze.*

1. sz. ábra egy állam és az azt érintő fenyegetettségi tényezők kapcsolati viszonya.)

A hírközlő és távbeszélő szolgáltatók piaci céljaik megvalósítása mellett felelősen vesznek részt a biztonsági és védelmi feladatok megvalósításaiban is. A felelőség vállalás kölcsönös biztonságnyújtás a szolgáltató és az állam között. E viszonyrendszert a mindenkori jogrend szabályozza.

(*2. sz. ábra a szolgáltató és az állam viszonyáról, a jogrendszer aspektusából)*

A továbbiakban e jog rendszer hatás mechanizmusának összefoglalására teszek kísérletet, kizárólag, mint biztonsági szakember.

A távbeszélő szolgáltatók biztonsági feladatait meghatározó Törvények

A távbeszélő (szélesebb körben hírközlő és telekommunikációs) cégek működését az alkotmányon alapuló jogrendszeren belül is a hírközlésről szóló törvény határozza meg. A hírközlésről szóló törvény egy keret törvény, amely összefoglalja a mindenkori telekommunikáció működtetéséhez szükséges feltételeket. Ebből eredően nem terjedhet ki minden szabályozó elvre, ezért más további törvényekkel együtt alakít ki szabályozó rendszert. E törvények együttesen képzik a nemzet biztonságát szavatoló törvények rendszerét. Az említésre kerülő taxatívák, természetesen önmagukban is nomenklaturák, melyek érintik a nemzet védelmi és biztonsági feladataihoz kapcsolódó stratégiai és operatív folyamatainak szabályait. Mind ezekkel együtt az igazi kihívás ezek együttes kezelése.

Ebben a kontextusban a szolgáltató kizárólag jogkövetőnek (adaptív) tűnik, viszont nem hagyható figyelmen kívül, hogy ugyanakkor indíttatásából és

alapításának célja alapján piaci szereplő, aki támogatója a nemzet biztonságának.

(3 sz. ábra a szolgáltatók, mint piaci szereplők a védelem és biztonság szempontjából, valamint a törvények függvényében.

Törvényi tételek felsorolása:(fő címekben)

- Honvédelem, honvédelmi felkészítés,
- Lakosság riasztása, tájékoztatása
- Polgári védelem, katasztrófák elleni védekezés, veszélyhelyzetek
- Hírközlés
- Rendőrség, nemzetbiztonság,
- Titokvédelem,
- Törvénnyel kihirdetett, nemzetközi (NATO, Nyugat-európai Unió) szerződések
- Adatvédelmi törvény.

Mind ezen törvény számos végrehajtási kormányrendelettel vált végrehajthatóvá.

A biztonsági feladatok megoldásai ezen törvények és kormányrendeletek speciális rendszerében válnak olvashatóvá.

HÓKA Miklós

A HARCÁSZATI INFORMÁCIÓELOSZTÁS MEGFONTOLÁSAI

Az információ – hatalom, idézik sokan a jól ismert szlogent. Én ezt kiegészítem: az információ – fegyverként is funkcionál. Bármely fegyveres konfliktusban, történjen az belátható terepszakaszon, hegyek között vagy a nagyvárosok utcáin, a harcmező tele van zajjal, átláthatatlan történések zajlanak nagyon rövid idő alatt, és lényeges jellemző, hogy sohasem elég a rendelkezésre álló információ.

Amire a modern katonának harcban szüksége van, – a lőfegyverén és az ahhoz való lőszeren kívül –, az a valós idejű felderítési adat, harctéri azonosító jel, zavar- és információvédett összeköttetés az elöljáróval vagy a társakkal, hogy túlélje a háború okozta ködöt, amit a káosz generál harc közben. Tudnia kell, merre vannak a támogató erők, merre mozog az ellenség, milyen útvonalon kerülje ki őket és csatlakozzon társaihoz, stb.

A parancsnokok, vezetők, de a harcoló egyének is igénylik a valós idejű adatokból álló komplex harcmező értékelést, amely csak a hálózatba kötött elemek összehangolt információáramlási képességei alapján alakulhat ki. A különböző típusú harctéri azonosító rendszerek integrálása a kommunikációs hálózatokba, a fegyverre szerelt lézertávmérő, azonosító, célmegjelölő funkciók, a nagypontosságú helymeghatározó és navigációs rendszerek egy, hatékonyan kialakított hálózatba foglalása már napjaink jellemzője. A komplett harctéri kép kialakítása olyan integrált számítási, azonosító, és megjelenítő funkcióval bíró eszközökkel történik, amelyek adatokat szolgáltatnak a harc minden fázisában, kiszámíthatóvá és modellezhetővé teszik például a tűz és manővertámogatást, a légitámogatást, és végső soron a túlélés lehetőségét, a veszteségek minimalizálását.

A hadseregekkel szembeni kihívások megváltozott jellege, illetve a gyors ütemű műszaki haladás következtében a jövőben az alakulatok mérete és létszáma csökkenő, míg hatékonysága növekvő tendenciát fog mutatni. A komplex hatású, digitális eszközrendszerekkel és fegyverzettel olyan feladatok oldhatók meg kisebb létszámmal, amelyek eddig csak a tömeghadsereggel voltak megvalósíthatók.

Alapvetően a vezetés – irányítás részére kerül kiépítésre egy digitális információs hálózat, a Harcászati Internet, amely támogatja a harcászati rendszerek működtetését és folyamatos figyelemmel kisérését. Ennek a hálózatnak elsősorban rugalmasnak kell lennie, toldás és hézagmentesnek, és megfelelő

kommunikációs csatlakozást kell, hogy biztosítson az egész hadsereg harcászati felhasználói részére.

A legtöbb ország haderejének különböző szintjei közötti adatelosztás megszervezése elsőrendű feladat, a katonai műveletek sikeres végrehajtása érdekében.

A Harcászati Internet jellegű hálózatoknál a legfőbb probléma az információ -, adatmegosztás – sávszélesség korlátok közötti arány megválasztásából adódik. A legmagasabb szinten általában a civil/üzleti szféra vezetékes hálózatain történik az információs rendszer kialakítása, és fix telepítésű műveleti központok között kerül megvalósításra az információ áramoltatás. A művelet végrehajtói szinteken, a hadtest, dandár és ezek alatt megjelenő vezetési pontok összeköttetéseinek stabil biztosítására viszont egy tábori híradórendszer kerül kiépítésre, a veszélyeztetettség szintje szerinti nagyságban, és annak trönk kapcsolatai felhasználásával történik az információ-megosztás. Szükségessé válik az alacsonyabb szinteken keletkező információk megosztása a magasabb szintű elemek vezetési pontjaival, műveleti központjaival, illetve a különböző parancsok, műveleti előírások lejuttatása a harcászati, végrehajtási szintekre. Ez az elvárás maga után vonja a két (állandó és tábori), funkcionálisan elkülönülő rendszerszint kapcsolódási lehetőségeinek fix kiépítését.

Harcászati szinten a vezetési pontok munkaállomásainak (harcjármű parancsnokok, szakaszparancsnokok, stb. munkahelyei) a csatlakoztatása a legfőbb probléma, hiszen ezt mobil, harci körülmények között, vezeték nélküli csatornák kialakításával kell megoldani a harcjárművek és a harcászati szintű vezetési pontok között. A végrehajtói szinteken rádiókészülékek hálózatba szervezett elemei biztosítják az összeköttetést a harcjárművek között, és stabil adatátjátszást kell megoldani a Harcászati Internet előnyeinek kihasználásához. A viszonylag keskeny sávszélességben dolgozó harcászati rádiók (jellemzően 50kHz, 25kHz vagy még ennél is kevesebb) komoly gátját képezhetik a folyamatos, nagy adattömegek áramoltatásának.

A korlátozott anyagi lehetőségek arra kényszerítik a hálózattervezőket, hogy ésszerű erőforrás-gazdálkodás kertében alakítsák ki a harci körülmények között működő, műveletorientált harcászati szintű hálózatokat, kihasználva a fejlesztések során megalkotott digitális rádiók képességeit, de figyelembe véve a még rendszerben lévő, szerényebb képességű analóg rádiókat is.

Egy olyan kombinált hálózati topológia kialakítása a cél, ahol a felhasznált szoftver és hardver elemek megfelelően működnek szinte bármilyen sávszélesség korlátozás között.

A hálózati topológia meghatározása

A harcjárművekben funkcionáló kapcsolóelemek egymáshoz csatlakoztatása kétféle, ma ismeretes módszerrel lehetséges: az ügyfél – kiszolgáló (kliens –

szerver)[12] alapú hálózatban, vagy az egyenrangú elemek (peer –to – peer)[13] csatlakozásának hálózatán.

A kliens – szerver topológiában az alárendelt szerepet játszó (beosztott) harcjárművek kliensként funkcionálnak, és hálózati routereken[14] keresztül küldik információikat más járműveknek, egy szerver (fő munkaállomás) segítségével. Az információk, üzenetek minden esetben a szerveren keresztül jutnak el a címzettekhez. Gondot jelenthet viszont a kliens járművek „leszakadása" a hálózatról, mozgás közben. Ez a probléma csak igen gondos és körültekintő hálózatszervezéssel kerülhető el, és ez a rugalmas harci csoportosítások kialakítási lehetőségének rovására mehet. A kliens – szerver hálózat tagjai egy csoportban kell, hogy maradjanak a stabil összeköttetéshez, a teljes művelet teljesítése közben. Amennyiben a szakaszparancsnoki harcjármű a szerver, akkor annak meghibásodása, kiesése esetén a kliens járművek kapcsolat nélkül maradnak, vagy leállnak a parancsnoki járművel együtt, veszélyeztetve a harci dinamikát. Ekkor az egész szakasz kommunikációs képessége megszűnhet, de legalábbis jelentős kiesés várható ezen a téren. Képzeljük el ugyanezt az esetet zászlóalj szinten! Be kell látni, hogy a kliens szerver topológiával nehéz mobil, harc-túlélő kommunikációs kapcsolatokat létrehozni, kivéve, ha a körülmények mindenképpen biztosítják a hálózati struktúra működőképes fenntartását. Megfontolandó az a tény, hogy általában éppen a harci körülmények azok, amelyek jellemzői a gyors, váratlan, előre nem látható események bekövetkezése

Az egyenrangú elemek összekapcsolásával kialakított hálózatban viszont minden harcjárműnek saját szervere van, és az információ a környező harcjárművek kapcsolatain keresztül jut el a címzetthez. A peer – to – peer hálózatok kevésbé sebezhetők, mivel nem csak egy szerver van a hálózatban. Itt is jelentkezik azonban megoldandó probléma, amely főleg a szervezetlenségben nyilvánul meg. Ha a Harcászati Internet egy önálló, óriási egyenrangú elemek összekapcsolásából álló hálózat, rendkívüli módon rendezetlenné válik az információkezelés. Ekkor a hálózatunk egy sor, külső kapcsolódású rádióból álló rádióhálózattá válik. Annak meghatározására, hogy ki van jelen a hálózaton, ki kell alakítani egy eljárást az önazonosításra.

---

[12] Ügyfél-kiszolgáló kapcsolat**:** A hálózati eszközök kapcsolatában az egyik megoldási mód a kliens-szerver mód, ahol van egy kitüntetett, általában a hálózatba kapcsolt gépeknél nagyobb teljesítményű gép (a szerver) amelynek feladata a többi gépről (kliensektől) érkező kérések kiszolgálása. Valójában mind a szerver mind a kliens a gépeken futó programok formájában jelennek meg, amelyek a gépek közötti összeköttetést kihasználva végzik a munkájukat.

[13] Peer-to-peer kapcsolat**:** egyenrangú, vagy peer-to-peer hálózatokról beszélünk, amikor minden gép egyenrangú, és erőforrásainak egy részét bocsátja a hálózaton keresztül a többi gép számára. Ilyen hálózatokban is elképzelhető, hogy az egyik gép csak szerverként működik. Lényeges, hogy nem a gépek információ-szolgáltatásban nyújtott szerepe a döntő, hanem az, hogy az egyenrangúság értelmében bármelyik lehet ügyfél és szolgáltató.

[14] Router: útvonal-választó, forgalomirányító.

Mikor egy számítógépet bekapcsolunk, és az fellép a hálózatra, bejelentkezik, és a hálózat a címzés alapján állapítja meg a gép helyét, valamint a kapcsolódás módját is. Az állomások üzenetei folyamatosan áramlanak a hálózaton, így az üzenetküldő elem „be tud hallgatni" a folyamatokba, jelezni tudja, hogy jelen van, és képes kilistázni a lehetséges (már csatlakozott) címzetteket. Ez az önazonosítási eljárás, melynek során minden csatlakozó számítógép egy fix címzéssel rendelkezik, és amely a kommunikációs hierarchia kialakítását is megkönnyíti.

A peer – to – peer hálózatoknak van még egy nagy előnyük a kliens – szerver típussal szemben, a szervezeti rugalmas átcsoportosítás lehetősége. A kliens – szerver hálózatban, egy új kliens beléptetéséhez át kell programozni a szervert és a routereket, míg az egyenrangú hálózatban csak egy rádiócsatornát kell megváltoztatni, és az új tag „beköszönése" már a csatlakozást is jelenti egyben. Az utóbbi eljárás sokkal közelebb áll a katonai műveletek dinamikus változás követéséhez, amely a mobil kommunikációs hálózatok egyik elvárása. Ezen túl, az egyenrangú hálózat rendelkezik azzal az előreprogramozható képességgel is, hogy segítsen, amikor két tagállomás nem képes egymással kommunikálni: egy harmadik állomás meghatározásával elérhető az automatikus üzenetátjátszás a címzetthez.

A hálózati topológia kialakításának lényeges kérdése a rendelkezésre álló sávszélesség. Egy kliens – szerver hálózatban az üzenetátjátszás a szállítási protokoll/Internet protokoll (TCP/IP)[15] szabványokat használja fel. Így elég rugalmasan, a Földön jelenlévő bármely számítógépet meghatározhatunk a címazonosítás alapján, viszont ez elég nagy sávszélességű átvitelt igényel, mivel az azonosítási információk adatcsomagjai külön azonosító biteket szállítanak magukkal (az OSI modell[16] kialakításának megfelelően).

Egy alacsony költségvetésből kialakított Harcászati Internetnél tekintettel kell lenni arra is, hogy a régebbi típusú harcászati rádiók még nem képesek felismerni a TCP/IP protokollokat. Ennek feloldására talán a legegyszerűbb módszer, ha szoftveresen „megtisztítjuk" az üzenetet a TCP/IP jelzésbitektől, mielőtt azt egy keskeny sávszélességű ultrarövid hullámú (URH) harcászati rádión továbbítjuk, és a bitazonosítókat egyszerű rádiócímzésekre cseréljük. A

[15] Protokollok, a hálózati kommunikációt leíró szabályok rendszere. Protokollokat használnak a hálózatokban egymással kommunikáló számítógépek és programok is. A TCP/IP is protokollok egy gyűjteménye, amelynek minden tagja az információ Interneten történő közlekedését szabályozza.

[16] OSI modell, a Nemzetközi Szabványügyi Szervezet (ISO) által kidolgozott referenciamodellt (ISO OSI hivatkozási modell, röviden: OSI modell) értik alatta, amely a különböző nyílt hálózatok, rendszerek összekapcsolására vonatkozik (olyan rendszerek, amelyek nyitottak más rendszerekkel való kommunikációra). A modell szerint a hálózatot legjobban úgy lehet megvalósítani, hogy azt a feladatok szerint egymástól független különböző rétegekre osztjuk, ahol aztán az egyes rétegek egymással kommunikálnak.

csatlakozási képességek ugyanazok maradnak, de csak a legszükségesebb sávszélességet kívánja meg az üzenettovábbítás.

Az adatelosztás megfontolásai

Miután meghatároztuk a kialakítandó hálózat topológiáját, meg kell fontolni, milyen módszerekkel és eljárásokkal biztosíthatjuk az adatelosztást.

Amikor elhatározzuk, hogy minden információt mindenhová eljuttatunk, általában két nehézség megjelenésével kell számolni. Először is, nagy valószínűséggel az URH rádiók sávszélessége nem fogja támogatni a nagy mennyiségű adattovábbítást. A második probléma a harc megvívásának tetőpontján a harcászati parancsnoknál jelentkezik. Ekkor a parancsnoknak címzett helyzetjelentések miatt a hálózat maximális teljesítőképessége határán kell, hogy üzemeljen, de akár „be is dugulhat", és éppen a legfontosabb pillanatokban.[17]. Valamilyen módszerrel le kell vezetni a felgyülemlett üzenethalmazt, megakadályozni a hálózat elzáródását, és ez nem egyszerű feladat.

Ésszerű döntéshozatal során ki kell alakítani a megosztásra szánt információk körét. Mely információkra van egyáltalán szükség? Szükséges – e tudnia például a dandárparancsnoknak, hogy a szomszédos dandár egy szállító járműje éppen milyen pozíciót foglal el a hadszíntéren? Valószínűleg nem. Viszont, ha éppen erre az információra van szükség, akkor az hogyan érhető el a legegyszerűbben?

Az ilyen és ehhez hasonló problémák megoldására megfogalmazott adatelosztási módnak az ellenütemű jelzőt adhatjuk, mivel a „húzd meg – ereszd meg" elvet követi (push and pull). Ahelyett, hogy minden információt, minden időben megosztanánk, csak a saját adatbázisunkat frissítjük a számunkra szükséges információkkal, illetve a saját továbbfejlesztett, frissített információinkat osztjuk meg másokkal. Az állandó vagy rövid időnkénti (pl.: 10 másodpercenkénti) adatfrissítés nagyobb sávszélességet foglal le folyamatosan, mint az ennél nagyobb időintervallum választása. Ha meghatároztuk az információink elévülési idejét, (amely természetesen nagyon kicsi is lehet), akkor már nincs meg a kényszer a szinte folyamatos adatfrissítésre. Általában a parancsnok felelőssége meghatározni ennek fontosságát, és szükségességét, valamint kiosztani az állandó, fenntartott sávszélességet, a legmagasabb prioritást kívánó információk továbbításához.

Az olyan adatok aktualitása, mint egy harcjármű pozíciója, harcképessége a harctéren meghatározó, hiszen a harcászati helyzetismeret kiemelten kezeli a saját csapataink helyzetének folyamatos nyomon követését. Az alacsony szintű (pl.: zászlóalj) Harcászati Internetben viszont ez az elvárás csak jelentős sávszélesség lekötésével alkotható meg. Ha túl sokat használunk fel a rendelkezésre álló sávszélességből erre az egy funkcióra (a harcjárművek pozíciói),

[17] Erre példa is történt a Szerbia elleni NATO műveletek során (1999), amikor a szerb hackerek által előállított több ezer, automatikusan generált üzenet, jelentősen megterhelte azokat a harcászati információs rendszereket, amelyek a nyílt célú Internetet (is) felhasználva működtek.

akkor a hálózat jelsebessége is le fog csökkenni. Ennek figyelembevételével kell megfelelő egyensúlyt kialakítani a rádiós üzenetküldések mennyiségi megszorításainak szervezésénél.

Információgyűjtés az adatfrissítéshez

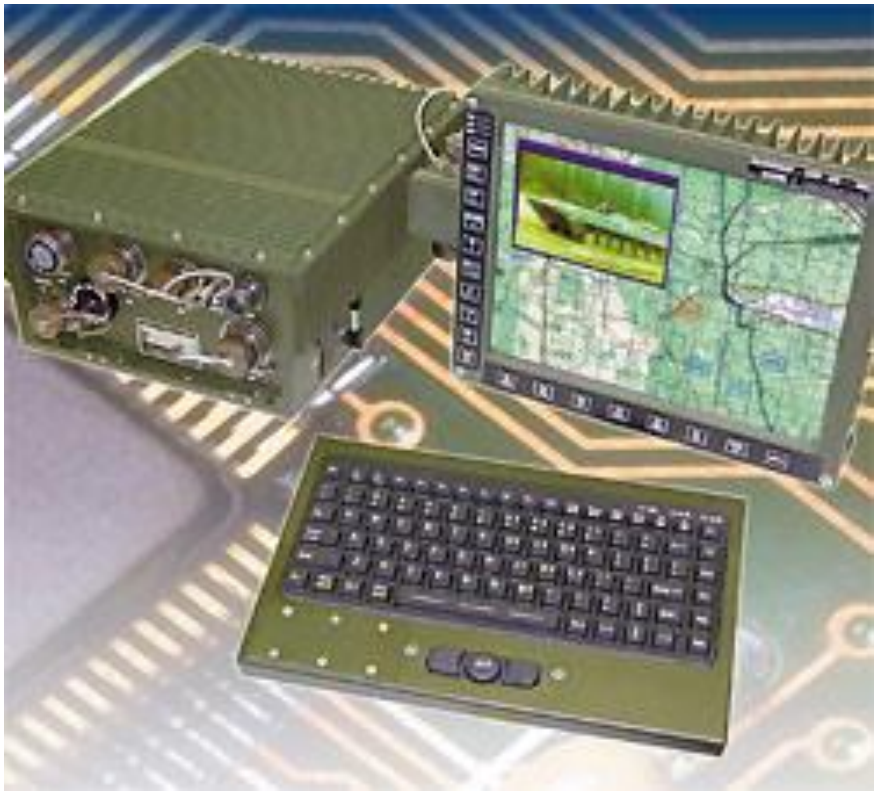
Meghatározhatjuk, hogy a harcjárművekre vonatkozó helyzeti információk a hálózaton minden percben vagy ennél is rövidebb idő alatt érkezzenek. Ez a legrosszabb módja az információgyűjtésnek, ugyanis a legtöbb katonai egység vagy jármű döntően egy helyben áll (a manőverek, menetek kivételével), és így csak a sávszélességet pazaroljuk el. A helyzetváltoztatásra vonatkozó információkat célszerű csak a tényleges mozgást végrehajtó elemek esetében meghatározni, és csak ekkor kérni egy rövid üzenetet az új pozíció pontosításához. A mobil harcászati rendszer szolgáltatásai között meg kell jelenjen az a lehetőség, hogy az elmozdult jármű egy automatikus üzenetküldéssel legyen képes helyzetének pontosítására.

Ide tartozhat még egy szervezési eljárás megvalósítása. A kijelölt figyelőállomás harcászati monitorán is megjelenő, struktúrába szervezett „borítékokat" hozunk létre, amelyek mindegyike egy – egy megfigyelt célobjektumhoz, járműhöz tartozik. Az általuk küldött helyzetváltoztatásra vonatkozó üzenetek ezekben kerülnek tárolásra, így időrendben is sorba rendezhetők a mozgások változásai. Továbbá lehetőség nyílik esetlegesen a járművek üzemanyag fogyasztásának a regisztrálására, valamint az üzemképesség helyzetismeretéhez is. Így a logisztikai támogatás egy része is megvalósítható némi rendszer továbbfejlesztés révén…

Sokféleképpen megoszthatjuk a pozicionáló információkat a saját rádióhálónkban, de még mindig van gond a többi rádióhálóval való megosztás kérdéseiben. Ekkor is a parancsnok döntése a meghatározó: milyen adatoknak, információknak legyen prioritása, a harcászati helyzetnek legyen az elsődlegesen megjelenítendő és információelosztási szerepe, illetve az ellenség vagy a saját csapataink jellemzőire vonatkozó információknak. Mint parancsnok, kiválasztom a fontos információt és kihelyezem a monitor munkaasztalára. Ez mind felfelé, mind lefelé és oldalirányban is automatikusan biztosítja a megosztást, olyan gyakran, ahogy a sávszélesség megengedi. Ugyanazon időben az elöljárók felé és az egyenrangú állomások felé szabad sávszélességgel rendelkezem a saját számítógépem részére, a számomra fontos információk megkeresésére.

Harcászati helyzetismeret

A hálózati információ megosztás és gyűjtés egyensúlyának helyes megválasztása biztosítja a parancsnokoknak, hogy kialakítsák a harcászati helyzetismeretet, miközben minimalizálják a sávszélesség kitöltését.



1.ábra. A Harcászati Internet eszközei a harcászati helyzetismeret kialakításához

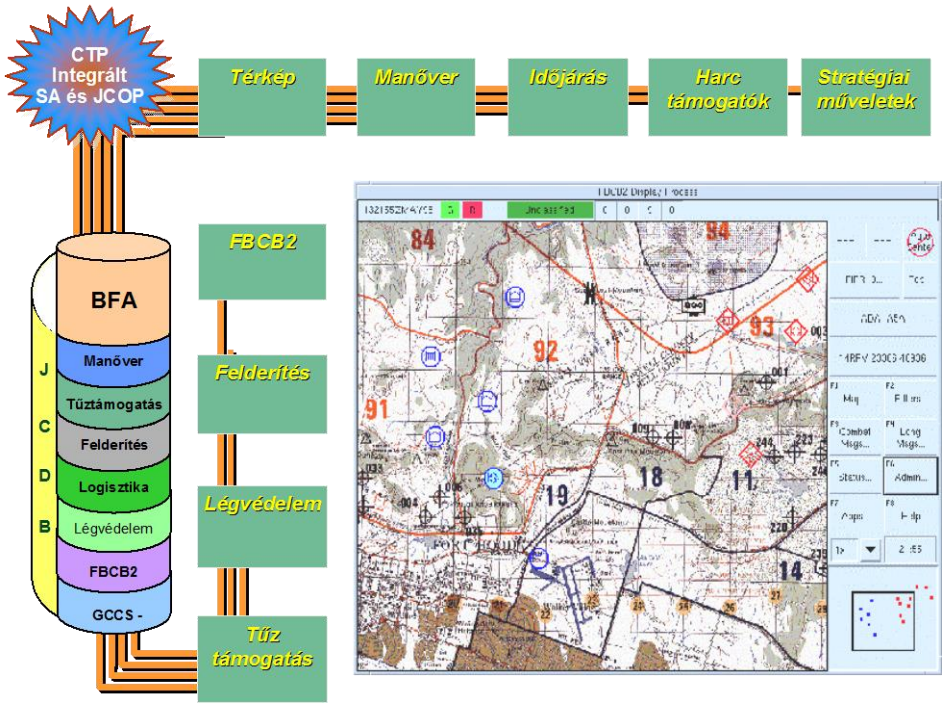
Felmerül a kérdés, hogy a hálózat képes – e minden felhasználó számára ugyanúgy megjeleníteni a harcászati képet? A válasz az, hogy igen is meg nem is. Technikailag lehetséges, de ez mindenkor adott beosztástól és szubjektív értékeléstől függ: ki, hogyan értékeli a harctéri helyzetet. Ide tartozik még az emberi szem egyik jellegzetessége is, hogy általában a központi mozgásokra fókuszál főként, ugyanakkor a perifériákra kevésbé.

A Harcászati Internet amellett, hogy fókuszba képes helyezni a legfontosabb változásokat és tudnivalókat a harci helyzetről, még a perifériás helyzetismeret meghatározására is képes. A harcászati információs rendszer „húzd meg – ereszd meg” típusú, ellenütemű eszköztára azt is jelenti egyben, hogy gyorsan képesek vagyunk a harcászati helyzet általunk kívánt összetevőire fókuszálni.

Nem biztos, hogy a harctól távol eső történések hatással vannak adott helyen vívott harctevékenységünkre. Igaz lehet ez a megállapítás, ha csak a közvetlen tevékenységünket befolyásoló részösszetevőkre koncentrálunk. Ugyan-

akkor egy hálózaton mindig ki kell alakítani a hierarchikus viszonyok kapcsolatrendszerét is. Az információk megjelennek dandár szint felett is, hiszen szükség van rájuk a különböző kimutatásokhoz és a magasabb szintű adatbázis frissítésekhez. A harcászati információs rendszerhez kapcsolt felderítő szenzorok, a felderítő csoportok adatainak megjelenése, stb. biztosítják, hogy – többek között – csapataink megóvás-támogatása (pl.: riasztások, veszélyre figyelmeztető jelzések formájában) is szerepet kapjon a harcászati helyzetismeret pontos kialakításában. Az ilyen típusú információkra szükség van jó néhány kilométerre a harctevékenységtől is, és oda küldhetők, ahol éppen szükség van rájuk.

Egyik jellemző példája ennek az USA hadsereg 1. digitális dandárjánál rendszerbeállított eszközcsalád, mely a Harcászati Internet adatmegjelenítésére egy multifunkciós terminált használ.



2.ábra. A multifunkciós harcászati terminál által megjeleníthető Közös Harcászati Kép (CTP)

Közös harcászati adatbázisokból (Joint Common Database, JCDB) valós időben megjeleníthető adatok, harctéri azonosító rendszerek jelei, digitális térképek, időjárás előrejelzés stb. adják meg a valós Harcászati Kép kialakításának lehetőségét, amely egy integrált harctéri helyzetismeretet (Situational Awareness, SA) kombinál az összhaderőnemi közös feladatokkal (Joint Common Operations, JCOP).

A helyesen megválasztott információáramoltatási hierarchia kialakítása még korlátozott sávszélesség mellett is biztosítani fogja, hogy az információ a megfelelő időben, a megfelelő helyre, a megfelelő személynek legyen továbbítva. A hálózaton így biztosítható minden információ szükségszerinti megosztása, és olyan, koncentrikus körökbe rendezett harcászati helyzetismeret részösszetevők jelennek meg, amelyek a parancsnokok számára tisztán és időtakarékosan jelentkeznek. Ez pedig oda vezethet, hogy egy csökkentett létszámú haderő valóban megvalósíthatja képességeinek növelését a kommunikáció vonatkozásában.

Felhasznált irodalom

- Daintry Duffy: Information is a weapon
  Intenet: www. infowar. com/mil_c4i. shtml
- Dr. Munk Sándor: Az informatika eszközrendszere, ZMNE jegyzet, (J–1082), Budapest, 1998.
- Tactical Internet on limited funds, Computerdevices Co.Ltd. (CANADA)
  Internet: www.computerdevices.com

208

EGRI Gábor, VARGÁNÉ ÁDÁM Gabriella

LEGÚJABB HÁLÓZATI FEJLESZTÉSEK A BM TÁVKÖZLÉSÉBEN

Egri Gábor r. alezredes, Vargáné Ádám Gabriella r. százados
O R F K
HÍRADÁSTECHNIKAI SZOLGÁLAT

A rendőri/belügyi munka során a kommunikációnak - mint általában a szervezetek vezetési rendszere egyik elemének - igen jelentős szerepe van. A mai kor által nyújtott korszerű távközlési és informatikai eszközök lehetőséget biztosítanak a különleges szakmai munka magas színvonalú kiszolgálására. Ezek között kiemelt jelentőségű a különböző szolgáltatások és integrált alkalmazások elterjedése és használatba vétele.

Az előző években szervezett hasonló konferenciákon a belügyi szakmai munkát kiszolgáló speciális híradástechnikai projektekről számoltunk be. Ezek teremtették meg az alapokat a korszerű informatikai – távközlési belügyi infrastruktúra létrehozásához.

Ennek az infrastruktúrának a felépítése is felbontható:

- átviteli vagy transzport síkra
- kapcsolási vagy útvonal választási (routing) síkra
- alkalmazások síkjára.

A jelen előadás a fenti bontás első két elemével foglalkozik.

1. Átviteli vagy transzporthálózat.

Ez a hálózat funkcióját tekintve a kommunikáció átviteli közegét képviseli. Felépítését, átviteli technológiáját tekintve két alapvetően különböző részre osztható, amely a belügyi ágazat sajátos szervezeti tagozódásához és területi elhelyezkedéséhez is illeszkedik:

a) budapesti hálózat
b) országos kiterjesztés.

1.a) A budapesti átviteli hálózat döntően optikai összeköttetéseket tartalmazó, gyűrű kialakítású topológián alapul. Fő csomópontjait képezik a Budapesten elhelyezkedő belügyi objektumok, ezek közül kiemelve:

- BM központi épülete;
- RIK (ORFK, BRFK, Pest MRFK) központi épülete;
- BM Központi Adat-, Nyilvántartó- és Választási Hivatal épületei;
- Rádió-távközlési Főközpont Hármashatár-hegy;
- Határőrség Országos Parancsnokság központi épülete;
- Katasztrófavédelem Országos Parancsnokság központi épülete;

- Bevándorlási és Állampolgársági Hivatal központi épülete.

A hálózat nagysebességű digitális átvitelt biztosít a különféle felhasználóknak, beszéd- és adattovábbítás céljából.

1.b). Az átviteli hálózat országos kiterjesztése alapvetően mikrohullámú összeköttetésekből kialakított hurok topológiát tartalmaz. Fő csomópontjait a közigazgatás és rendvédelmi szervek megyei egységei képezik, de egyes megyék esetén eltérő mértékben és különböző átviteli kapacitással. Ezen csomópontok alapvetően a megyei rendőr-főkapitányságok bázisán lettek kialakítva és kapcsolódnak hozzájuk a különféle szervezetek (Megyei Közigazgatási Hivatal, okmányirodák, Megyei Katasztrófavédelmi Igazgatóság, Határőr Igazgatóság, esetenként rendőrség területi szervei).

2. Kapcsolási, vagy routing hálózat

E funkciókat külön-külön hálózat-részek valósítják meg a beszéd-, illetve az adatátvitel esetén.

A beszédátvitel kapcsolási síkjait a 4 szintű hierarchiára bontott távkezelő központok rendszere valósítja meg. Ebben a rendszerben a következő funkcionálisan eltérő kapcsolóelemek találhatók, az egész országos hálózat teljes vertikumát tekintve:

- főgyűjtő gócközpontok (2 db)
- gyűjtő gócközpontok (7 db)
- góc központok (11 db)
- területi (kapitánysági) sík.

A távbeszélő hálózat digitalizálásáról az előző évi konferencián már részletesen esett szó.

Az adatátviteli hálózat fejlesztésének előzményei közé tartozik, hogy a Belügyminisztérium ilyen célra rendkívül elavult (X. 25), alacsony kapacitású rendszerrel rendelkezett. A hálózat kialakítása - az akkori viszonyoknak megfelelően készült, ugyanakkor ez napjainkra rugalmatlanná vált és ezáltal korlátokat jelent. Ezzel párhuzamosan azonban a felhasználók egyre fokozottabb sávszélességet és alkalmazhatóságot igényeltek, miközben az átvitel alapját képező infrastruktúra jelentős fejlődésen ment keresztül.

Ezek alapján célkitűzésünk egy korszerű, központilag menedzselt, garantált szolgáltatást biztosító, megbízható, felhasználó- és üzemeltető barát szolgáltatói hálózat kialakítására irányult.

A rendelkezésre álló infrastruktúra hatékony kihasználása érdekében olyan technológiát kellett választanunk, amely:

alkalmas nagy kiterjedésű (országosan több szervezetet kiszolgáló) hálózat kialakítására, ugyanakkor lehetővé teszi a rendszer-elemek számának növekedését;

- nem korlátozza a hálózati kapcsolatok számának növekedését, a jövőbeni kiterjesztést;
- biztonságos kommunikációt tesz lehetővé;

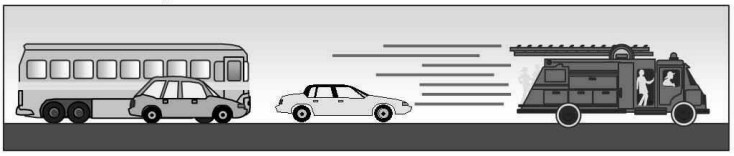
- az egységes központi menedzsment megbízható üzemviteli információkat szolgáltat;
- biztosítja a változások folyamatos kezelhetőségét;
- költség-hatékony működést eredményez az egységes hálózat platformján, ugyanakkor a felhasználók számára (virtuálisan) önálló hálózatként funkcionál.

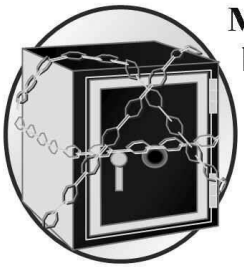
Az adatátvitel céljára az MPLS technológián alapuló hálózat kialakítására került sor. E technológia biztosítja az egymástól szervezetileg független, de a tevékenységük során szorosan együttműködő szervezeti egységek önálló alkalmazásainak kiszolgálását. A közös infrastruktúra biztosításával önálló alrendszerek alakíthatók ki, amelyek maradéktalanul kiszolgálják a felhasználók igényeit, biztosítva az önálló hálózat részek elkülönülését. Természetesen a ”felhasználók” fogalom itt nem általános civil, vagy üzleti partner kapcsolatot jelent, hanem a kormányzat részét jelentő belügyi szakterület alárendeltségébe tartozó szervezetet. Ebből fakadóan egy sor biztonsági aspektus is jelentkezik. Gondoskodni kell az információ biztonságáról és hitelességéről. Meg kell oldani a hálózat biztonságát fizikai értelemben, valamint rendelkezésre állás értelemben is.

E hálózat kialakítását mutatják a következő előadási vázlatok

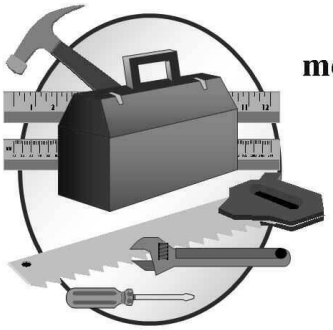
IP alapú hálózatok lehetőségei

Quality of Service





Magasfokú biztonság



Egyszerű menedzsment

IP alapú hálózatok lehetőségei

- Multiservice hálózatok kiépítésének lehetősége
- Gyors konvergenciával rendelkező protokollok
- De! CPU igénybevétel

(bejövő csomagfogadás,előfeldolgozás,routing,klasszifikáció, sorbanállítás(QoS)

Szolgáltatói hálózat fő feladatai

- A szolgáltatói hálózatnak ne kelljen kezelnie az „ügyfél” routokat
- Szolgáltató részére gyors telepítési lehetőséget nyújtson
- Sok telephelyű ügyfelek részére is megoldást jelentsen
- QoS- különféle IP szolgáltatásokat tudjon

MPLS előnyei

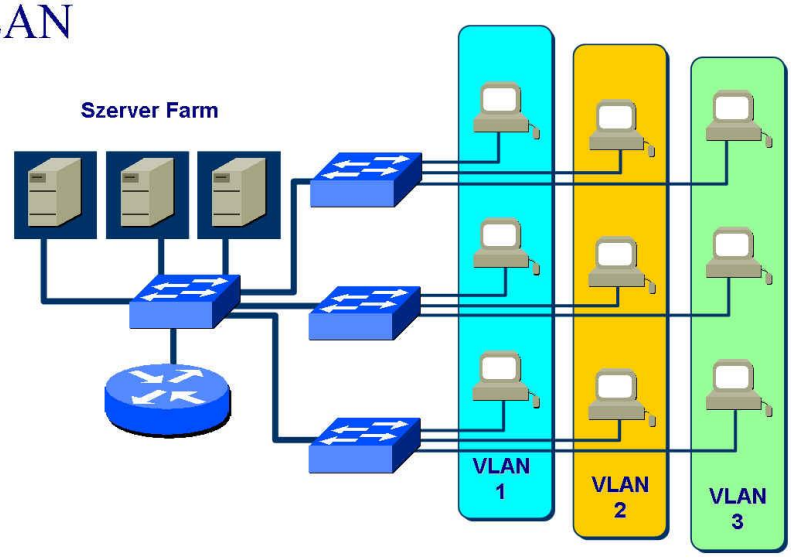
- Nem kell nagy routing táblák alapján továbbítani a csomagokat,
- Gyors rerouting hiba esetén;
- Egyszerű konfiguráció;
- VPN lehetőségek

Virtuális Privát Hálózatok (VPN)

- Közös erőforrások használata különböző szervezetek részéről
- Lehetővé teszi a hálózatot használó szervezetek elkülönítését
- VPN-eken belül tetszőleges címtartományok
- Különböző VPN-eken belül azonos címtartományok

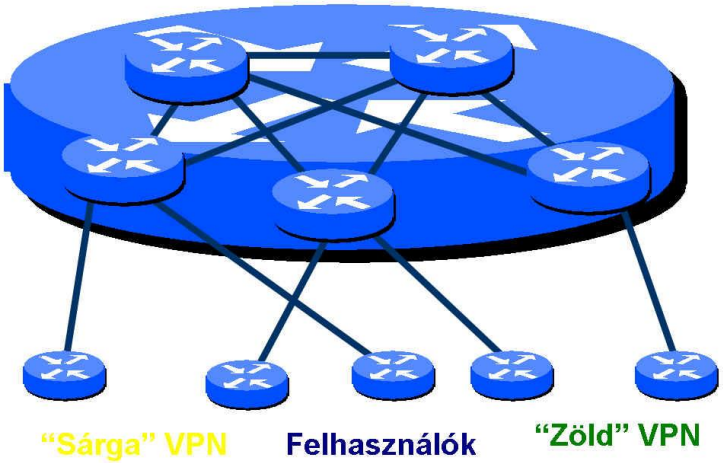
MPLS VPN funkcionális felépítése

- VLAN

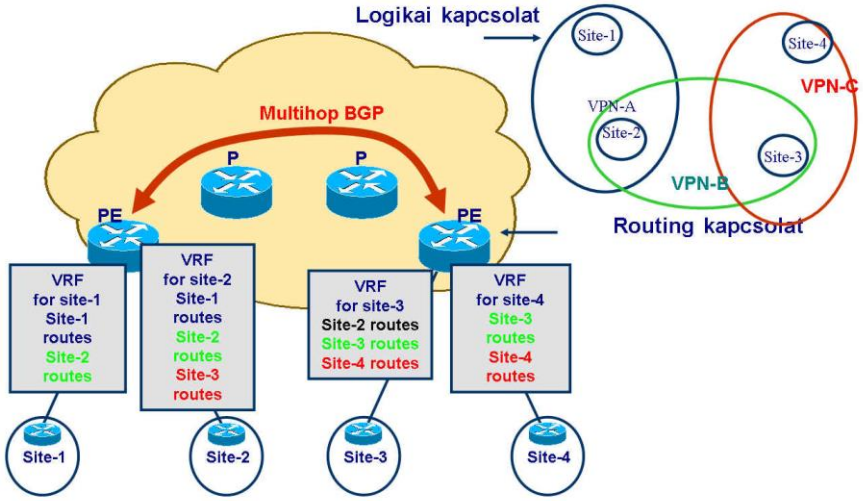


MPLS VPN technológiai analógia

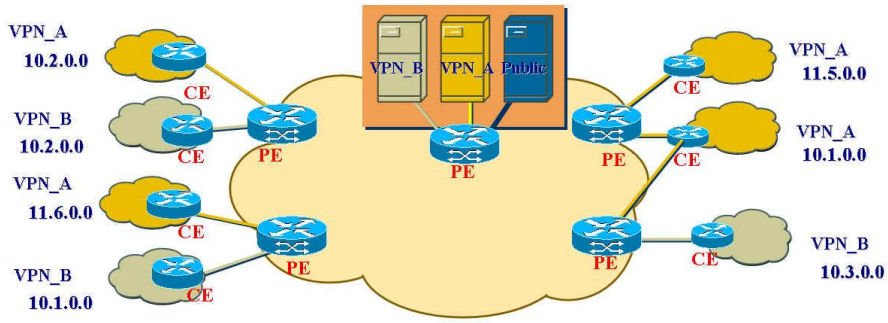
- Virtuális router



MPLS VPN mechanizmus
VRF és routing példa



Közös erőforrások elérése

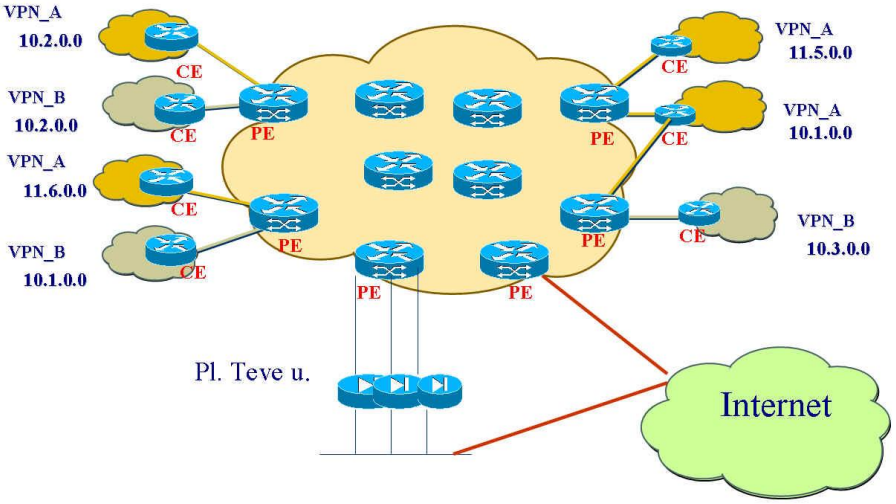


- **Privát felhasználású szerverek**
- **Publikus felhasználású szerverek**
- **A szerver címe csak a használók VPN-jéből "látszik"**

MPLS alkalmazások

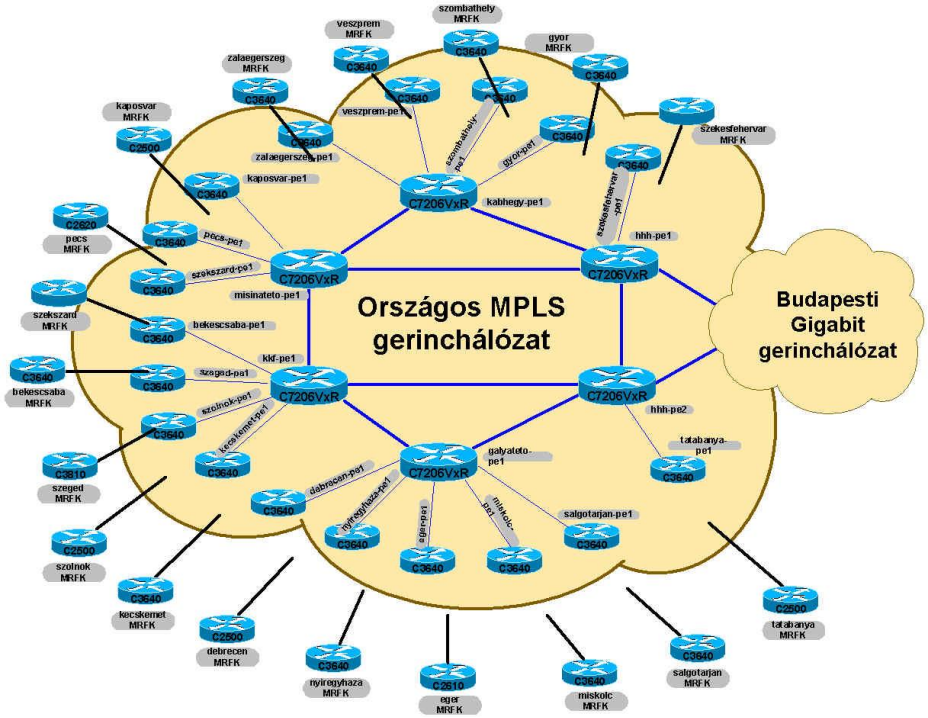
- QoS biztosítása
  - Valósidejű alkalmazások (VoIP, Video)
  - Fontos alkalmazások kiemelt kezelése (Robotzsaru)
  - „Nem lényeges” forgalom elnyomása
- Traffic Engineering (TE) – a gerincben
  - Optimalizált kihasználtság, forgalomirányítás
  - Gyors útvonalválasztás hiba esetén (fast reroute)
- MPLS VPN
  - VPN szolgáltatások gyors megvalósítása L2-nek megfelelő biztonsággal
- Class-of – Service (CoS)
  - A fontos szolgáltatásoknak a megfelelő prioritás biztosítható a kívánt késleltetés elérése érdekében

MPLS és az Internet



Országos routeres MPLS hálózat

- Redundáns gerinchálózat
- 2Mbps a végpontokig
- Minden megyében az MRFK-n a végpont
- Egyszerűen bővíthető
- Egységes menedzsment
- Költséghatékony

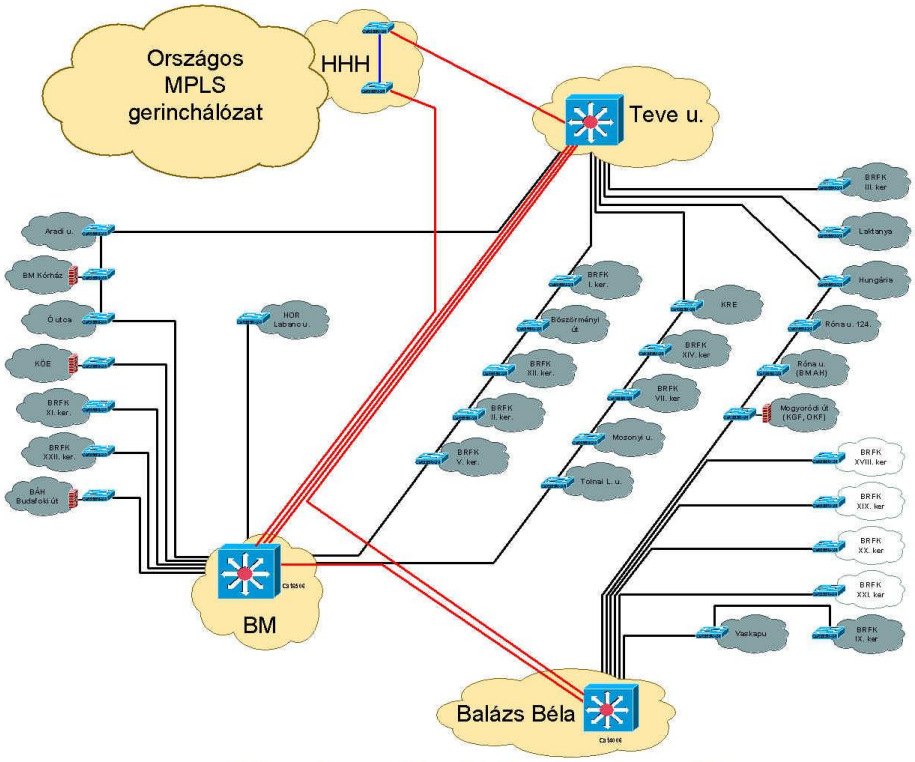


Budapesti Gigabit Ethernet hálózat

- Követelmények:
  - Nagy sebesség (több Gbps)
  - Magas szintű rendelkezésre állás
  - Elérhetőség minden BM szerv számára
  - Meglévő infrastruktúra felhasználása
  - VLAN technológia támogatás
  - Layer3 funkcionalitás
  - QoS támogatása
  - Egységes menedzsment rendszer - egységes

Előnyei

- Alkalmazkodik a kiépített optikai hálózat nyomvonalához
  - optikai hálózat folyamatos bővítés alatt
- Gigabit Etherchannel technológia (egyszerűen bővíthető)
- A központi kapcsolók és a kisebb objektumokat kiszolgáló kapcsolók gyűrűket alkotnak.



Technikai jellemzők

- Full Gigabit Ethernet megoldás
- Teljeskörű Layer3 switching
- Korszerű eszközök (Cisco Catalyst család)
- Együttműködés az MPLS hálózattal
- Egységes biztonságos menedzsment
- Magasszintű megbízhatóság – redundancia,(terhelés megosztás)

Virtuális LAN architectúra

- Hálózati forgalom elkülönítése
- LAN –ok között átjárás nincs(alaphelyzetben)
- Átjárás Layer3 switchekkel
  - Teve u
  - BM központi épület
  - Balázs Béla u.
  - többi objektumban Layer3 lehetőség

DOBOS Attila

GYORS REAGÁLÁS A KATONAI TÁVKÖZLÉSBEN

Joggal merülhet fel az olvasókban a kérdés, hogy mit tudhat egy „civil” cég a katonai távközlésről és miért pont a reagálóképességgel foglalkozik.

A Siemens Nemzeti Vállalatcsoport tagjai – Siemens Rt, Siemens Telefongyár Kft – több éve „közeli kapcsolatban” vannak a Magyar Honvédség zártcélú távközlő hálózatával. A hálózat gerincét képező HICOM központok üzemeltetése és fejlesztése során több gondolat merült fel bennünk, amelyet ezúton szeretnénk közzétenni.

A Magyar Honvédség zártcélú hálózatának rendeletetése többféle módon fogalmazható meg. Talán a legegyszerűbb a civil megközelítés: a vezetési rendszer részeként biztosítani a szükséges információk áramlását mindig és minden körülmények között. A szükséges információk szöveg, beszéd, vagy adat formájában, írott, illetve elektronikus formában jelennek meg. A körülmények a kialakult helyzettől függően igen változatosak lehetnek: békeállapotban stabilan telepített vezetés pontok közötti ideális állapotnak mondhatótól a harctéri, tábori körülmények között folyamatosan települő és áttelepülő vezetési pontok közötti körülményekig.

További terhet jelent a hálózatnak a valós idejű átvitel biztosítása, az átvitt információk védelme, az átjárás biztosítása más hálózatok felé, a folyamatos felügyelet biztosítása, valamint a nemzetbiztonsági követelményeknek való megfelelés.

A fentieket természetesen folyamatosan biztosítani kell és az esetlegesen bekövetkező változások negatív hatásait minél jobban csökkenteni.

Építsük fel az alábbi funkcionális alapmodellt és vizsgáljuk ez alapján a hálózattal kapcsolatos elvárásokat.

Az azonos rendeltetés miatt tekintsük egységes rendszernek a stabilan telepített és a tábori körülmények között folyamatosan változó hálózatot.

A legfontosabb elvárás a nagy sebességű transzparens átvitel folyamatos biztosítása mind a távközlési, mind az informatikai alkalmazások számára. A stabilan telepített berendezéseknek folyamatos és dinamikusan kezelt kapcsolatokkal kell rendelkezniük, amelyek a megfelelő védelmez is biztosítják. Megfelelő pontokon berendezések és dedikált erőforrások szükségesek a más hálózatokhoz történő kapcsolódáshoz, valamint szükség esetén a hálózat tábori körülmények közé történő kiterjesztésére.

A tábori hálózat telepítése és üzemeltetése során biztosítani kell valamenynyi szolgáltatást, amely a stabil hálózatban rendelkezésre áll.

A teljes rendszert folyamatosan menedzselni szükséges, reagálva az esetleges változásokra.

Megoldások a Siemenstől:

1. A jelenleg rendszerbe lévő HICOM központok képesek a zárt célú hálózat egységes rendszerré történő integrálására az alábbiak szerint:

- az átviteli kapacitások dinamikus menedzselése,
- tranzit központ funkciók ellátása,
- interfészek biztosítása más hálózatok felé,
- informatikai hálózatok integrálása sávszélesség allokálása mellett,

2. A hálózat védelmét biztosító titkosító berendezések telepítése és felügyelete:

- csoportos titkosító berendezések az átviteli utak védelmére (64kbps – nX2 Mbps)
- titkosító eszközök virtuálisan kialakított hálózatok – LAN, WAN – védelmére,
- végponti titkosító berendezések,
- az alkalmazott berendezések teljes felügyelete és integrált menedzsmentje

3. Védett, biztonságos informatikai hálózatok létesítése:

- komplex kábelezési rendszer, biztonságos technológiával,
- TEMPEST munkaállomások és hálózati eszközök önálló fejlesztése és gyártása,
- teljes körű üzemeltetés, fenntartás, felügyelet

4. A stabil hálózat kiterjesztése tábori rendszer felé:

- tábori kivitelű HICOM fejlesztése (MIL STD 810F, és MSZK 067 N7 szerint)
- a tábori rendszer integrálása
- teljesen azonos szolgáltatások és felületek,
- integrálás a hálózat felügyeleti rendszerbe,

5. Transzporthálózat biztosítása tábori körülmények között:

- tábori berendezések valamennyi sávra (Band I-IV-V), nagy sávszélesség biztosításával,
- mobil antennatornyok és speciális konténerek biztosítása.

6. Informatikai hálózatok tábori körülmények között:

- speciális katonai számítógépek forgalmazása, igény esetén fejlesztése,
- katonai kivitelű passzív elemek (réz és optikai kábelek, rendezők)

7. Harcászati rádiórendszerek:

- magas műszaki színvonalú berendezések szállítása,
- teljes integráció a vezetékes hálózatokkal,
- egyéni fejlesztési lehetőségek

8. Teljes rendszerintegráció:

- stabil és tábori rendszer integrációja, menedzsment rendszerek egységesítése
- beépítés gép- és harcjárművekbe,
- valamennyi folyamat teljes szoftveres támogatása, célszoftverek fejlesztése

Hogyan jelentkezik a reagálóképesség problémája?

Békeállapotban a stabil hálózat szükséges átalakítása, erőforrások dedikálása egy jól felépített hálózat felügyeleti központból megoldható. Amennyiben ez a központ megfelelően integrált, úgy a teljes hálózat – kapcsolók, átviteli utak – felügyelete biztosított.

A tábori rendszer telepítése esetén, a szükséges bejelentkezések után ez a felügyelet tovább terjeszthető, biztosítva ezzel az immár kiterjesztett hálózat működőképességét.

A vezetési rendszer elemeként az esetleges erőforrásokkal végrehajtott manővereket az így kialakított központ jól támogatja.

Természetesen gondoskodni kell a központ duplikálásáról akár teljes, akár részfeladatok átvételére képes központok kialakításával.

A fentiek képességek kihasználásával kialakításra kerülő rendszer tökéletesen képes megfelelni az alaprendeltetésének. A központosított felügyelet és menedzsment biztosítja azt a reagálóképességet, amely a rendszer biztonságát adja.

A Magyar Honvédség a rendszerváltás óta folyamatosan alakul át. A jelenlegi szövetségi rendszerben a tárca vezetése már több alkalommal hangsúlyozta, hogy a kisebb létszámú, speciális szakfeladatokat – műszaki, egészségügyi - ellátó szervezeti egységek fejlesztése kiemelt jelentőséggel bír.

Igazán nagy szakmai kihívást jelent egy ilyen többnemzetiségű szervezetben tevékenykedő csoport híradásának tervezése és biztosítása. Olyan berendezésekkel kell ellátni, amelyek amellett, hogy teljesen biztosítják az adott helyszínen települőkkel az együttműködést, biztosítják a teljes – vagy előre

definiált – jogú hozzáférést. A felhasznált átviteli közeg – műholdas, vagy rádiócsatorna – megfelelő védelméről is gondoskodni kell.

A vezetési rendszer alapját képező, ilyen módon felépített rendszer igen értékes információkat tartalmaz és szállít. Ezen információk megszerzése és birtoklása, esetleg a rendszerbe hamis információk bejutatása a teljes vezetési rendszert megbéníthatja.

Az ilyen jellegű „információs hadviselés" napjainkban egyre elterjedtebb. Elemzők és szakértők állítják, hogy bármilyen vezetési rendszer – és ezen keresztül haderők – ilyen módszerrel megbéníthatóak. A védekezés az ilyen jellegű tevékenység ellen igen bonyolult. A fizikai, személyi biztonságot tovább lehet növelni megfelelő szervezéssel. Azonban ha az információt továbbító rendszer egységes, jól védett és rendelkezik további szabadsági fokokkal, megbízhatóan láthatja el feladatát.

A gyors reagáló képesség fontossága ebben jelentkezik egy „civil" szemével nézve. Egy egységes és biztonságos, védett rendszernek további védelmet nyújt az, ha működés közben képes – a működést nem befolyásoló módon – átalakulni. Felderített átviteli utak, információ források és végpontok áthelyezése, eszközök - kapacitások átterhelése, kódok és eljárások változtatása igen hatékony eszközei lehetnek a védekezésnek. Magának a védekezésnek is igen fontos mozzanata lehet az ilyen jellegű reagálás.

Remélem sikerült a gyors reagálási képesség ilyen irányú megközelítésével felkelteni az érdeklődést. Különösen fontosnak tartom ezt egy olyan rendszer esetében, amely a hagyományosan értelmezett gyors reagálású erőket igénylő feladatokat hivatott támogatni.

Kihasználva saját és partnervállalatainak kapacitásait és képességeit a Siemens képes egy ilyen rendszer kialakításra, üzemeltetésére és igény esetén továbbfejlesztésére.

HODOSI Lajos

A BÉKEMŰVELETEK MŰSZAKI TÁMOGATÁSI SZAKFELADATAINAK HÍRADÓ BIZTOSÍTÁSA AZ IFOR-SFOR TAPASZTALATOK TÜKRÉBEN

1996-tól 2002-ig az IFOR-SFOR feladatok végzésében a műszaki szakfeladatok híradó biztosítása kiemelt jelentőséggel bírtak.

A minden oldalú biztosítás egyik fő eleme a híradó biztosítás, mely a feladatok sikeres végrehajtásának elengedhetetlen része.

Úgy gondolom, hogy a gyakorlati tapasztalatokat célszerű összefoglalni e területen is és egy rövid következtetést, levonni a felmerült problémákról.

Az előadásomban a műszaki támogatás híradó biztosítását fogom bemutatni a MIOB feladatai között, és röviden szólok ennek a feladatnak a jelentőségéről is.

A műszaki támogatás híradó biztosítását két területen fogom megvizsgálni a menetek során, majd az ideiglenes táborok kitelepítése működtetése folyamán, amikor is egy szakfeladatot hajt végre egy kijelölt alegység.

A műszaki támogatás híradó biztosítása a békeműveletekben [18]

A híradó biztosítás a vezetés általános része, de békeműveletekben igen fontos biztosítási feladatként jelentkezik. Az 1. ábra ezt mutatja be.

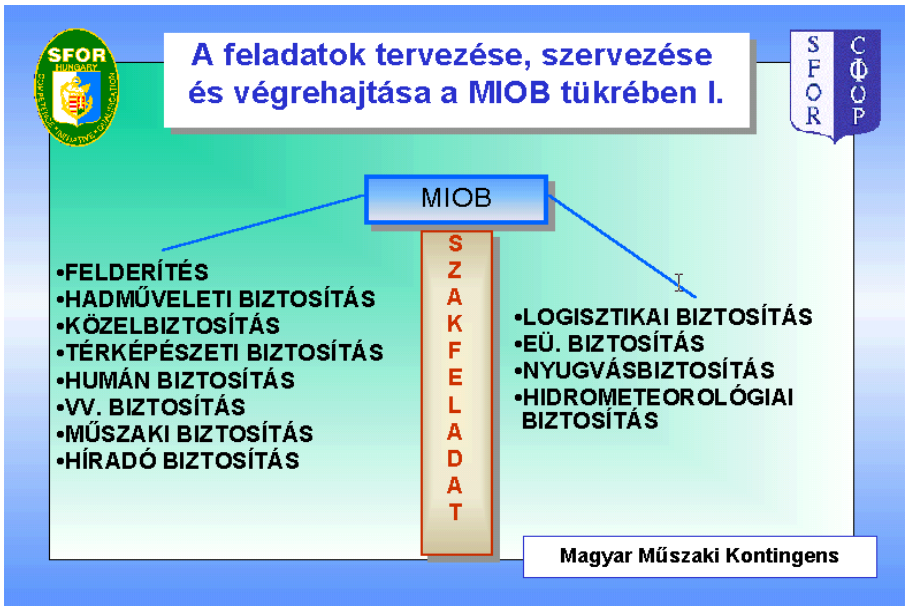
A műszaki támogatás híradó biztosítási feladatai eltérést mutatnak a hagyományos harc-hadműveléthez képest, mivel a békeműveletek során másképpen kell megtervezni ezt a biztosítási fajtát. Az ellenőrzésbe minden esetben bevonják a logisztikai főnököt, a híradó főnököt, a segélyhelyparancsnokot, kiemelt műszaki munkák esetén a kontingens főmérnökét is.

A következőkben egy szakfeladaton keresztül fogom bemutatni a közelbiztosítás feladatait. Egy konkrét munka végrehajtása több ismeretet ad az állomány biztosítási feladatairól, mintha konkrét adatokat sorolnék fel.

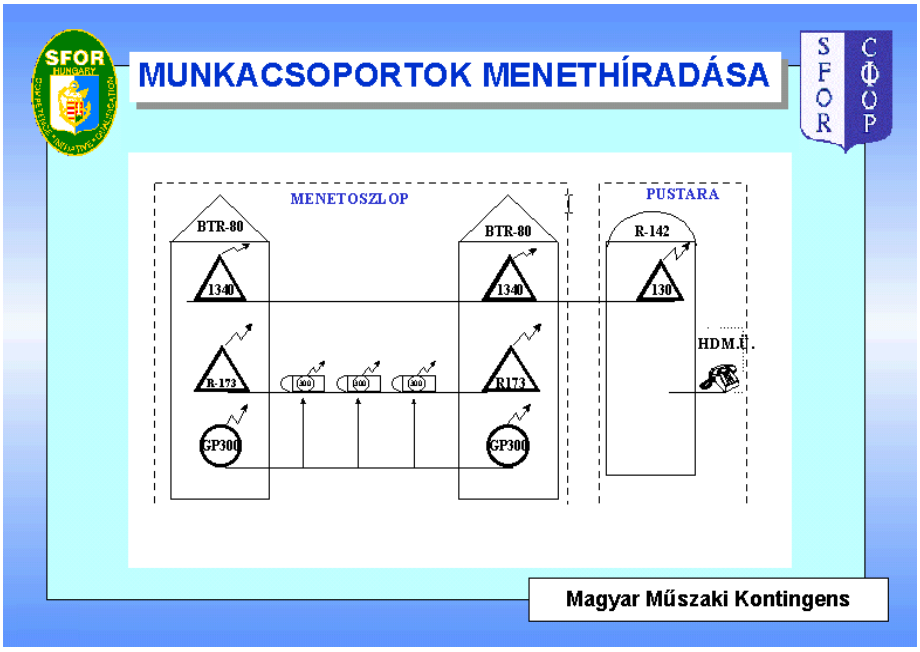
A közelbiztosítási feladatok végrehajtása a menet közelbiztosításával kezdődik. Ennek első üteme a menetrend összeállítása. A MMK a menetrend felépítésénél — más nemzetek és saját tapasztalatokat feldolgozva — az alábbi rendező elvet célszerű követni.

---

18 Kovács Tibor: A béketeremtő és békefenntartó kötelékek működésének gyakorlati tapasztalatai, Tanulmány, ZMNE, Bp., 2001. alapján.



1. ábra: Híradó biztosítás a MIOB-on belül[19]



2. ábra: Munkacsoportok menethíradása[20]

[19] U.o. 99. o.

A menetoszlopokat lehetőleg kettő harcjárművel biztosítják. Az egyik harcjármű (BTR–80), mint terepkutató harcjármű az oszlop élén, azt 300–500 méterrel megelőzve halad. Feladata a menetvonalon lévő akadályok időben történő felderítése, folyamatos adatszolgáltatás a parancsnok részére az esetleges veszélyhelyzetekről, közlekedési körülményekről, akadályokról és az esetleges demonstrációkról. Amennyiben az oszlop továbbhaladása nem biztosított, az oszlopfordítás ideje alatt, biztosítási feladatot hajt végre.

A parancsnok az oszlopot a terepkutató harcjármű mögött vezeti, felhasználva a tőle kapott információkat. Tisztázatlan helyzet esetén az oszlopot megállítva, a THJ fedezete alatt szemrevételezi a kialakult helyzetet, és látottak alapján dönt a további tevékenységről. A menetrendben a parancsnokot a műszaki járművek követik. Mivel méretük, tömegük és felépítményeik általában nem teszik lehetővé gyors haladásukat, ezért elhelyezésük lehetővé teszi, hogy a parancsnok folyamatosan kontrolálja mozgásukat, és ehhez igazítsa az oszlop sebességét.

Az oszlop közepén vagy utolsó harmadában foglal helyet az üzemanyag ellátó csoport. Ebből adódóan egy esetleges — a menetoszlop ellen irányuló— támadás ellen jobban védve van, mintha az oszlop végén helyezkedne el. Ebben az esetben a kigyulladt üzemanyag lehetetlenné tenné az oszlopfordítást is! Ugyan ez az elv érvényesül abban az esetben is, ha egy közúti balesetet feltételezünk, hiszen az oszlop végén lévő tartálykocsival előforduló baleset megsokszorozhatja az egyébként súlyos eset következményeit.

Az oszlop utolsó harmadában kap helyet a mentő gépkocsi. Baleset, sérülés esetén az oszlop mellett bármely gépkocsit meg tudja közelíteni anélkül, hogy nagyobb manővert kelljen végrehajtania.

Az oszlop végén lévő harcjármű előtt foglal helyet a javító-vontató csoport járművei, majd az oszlopot szintén egy BTR–80 harcjármű zárja, mely végrehajtja a menetoszlop végbiztosítását, illetve az oszlop megállása esetén személyzete végrehajtja a forgalomszabályozó feladatokat.

Az előzőekben ismertetett menetrend felépítés a közelbiztosítási feladatok megszervezésén kívül a megbízható híradás megszervezését és végrehajtását is biztosítja.

Az oszlop elején és végén lévő harcjárművek rádió eszközei biztosítják az információáramlást:

- az oszlop eleje és vége;
- a menetoszlop és az alaptábor között.
- Az oszlop- és gépjárműparancsnokok a hírhálóba a kontingensnél rendszeresített MOTOROLA GP 300 típusú rádióval vannak bekötve, me-

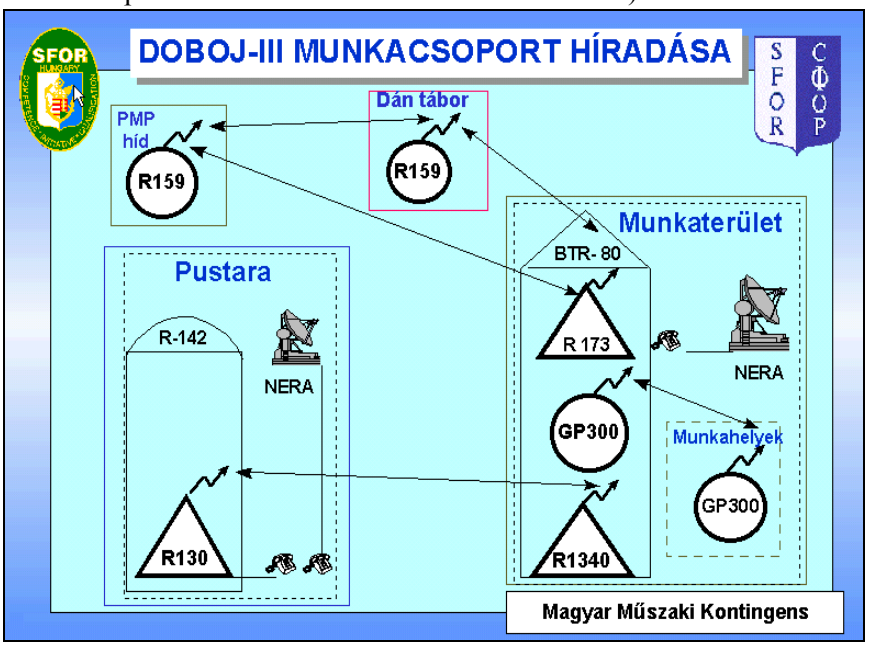
[20] U.o. 82. o.

lyeken veszik az oszlopparancsnok utasításait, a harcjárművek illetve a parancsnokok és a biztosítók által leadott veszélyjelzéseket.

A menethíradás ilyen módon történő megszervezése az alábbi előnyöket biztosítja:[21]

- az oszlopparancsnok folyamatosan információkhoz jut — az oszlop hosszától függetlenül — az egyes járművek helyzetéről, az esetleges meghibásodásokról;
- az előző gondolatból adódóan bármikor be tud avatkozni az oszlop menetébe;
- a tagállomások folyamatosan értesülnek az oszlopban történtekről, készek a veszélyjelzések vételére;
- az oszlop mozgása során is van lehetőség az alaptábor és a menetoszlop közötti kétoldalú információáramlásra;
- a két harcjármű alkalmazása lehetővé teszi az összeköttetés dublírozását az alaptábor felé, mely szintén növeli a menetoszlop biztonságát.

(A munkacsoportok menethíradását a 3. ábra szemlélteti).



3. ábra: Doboj III Munkacsoport híradása[22]

[21] U.0. alapján.

[22] U.o. 89. o.

A munkahelyek közelbiztosítása[23]

A munkahelyek közelbiztosításának megszervezésére és végrehajtására a munkacsoportok biztonsága szempontjából szintén meghatározó kérdés. Feladatainak tartalmát az alábbi körülmények határozzák meg:

- mely ország területén kerül végrehajtásra a feladat;
- a munkavégzés időtartama;
- a munkacsoport nagysága, összetétele;
- a feladat végrehajtás közvetlen környezete;
- a munka jellege.

A körülményeket figyelembe véve a közelbiztosítás feladatai több ütemben kerülnek végrehajtásra. A befolyásoló körülmények függvényében ezen ütemek feladatainak sorrendjei, felcserélődhet, esetleg egyes feladatok el is maradhatnak.

A közelbiztosítás mellett az állomány biztonságát a jól szervezett, megbízható híradás is elősegíti.

A munkaterületre történő kiérkezést követően a híradó rendszer felállítása az elsődleges feladatok közé tartozik.

A hírrendszer kialakításánál az alábbi rendező elveket célszerű figyelembe venni:

- biztosítson folyamatos, kétoldalú, dublírozott összeköttetést a munkaterület és az alaptábor között;
- biztosítson összeköttetést a munkaterület és (ha vannak ilyenek) a kihelyezett részlegek között;
- a munkaterületen belül (természetesen annak nagyságától függően) az egyes részlegek és a parancsnok között.

A munkaterület és az alaptábor között a folyamatos híradó összeköttetést a BTR–80 harcjárművek rádió eszközei, valamint a telepített NERA típusú műholdas telefonkészülék biztosította a Doboj híd építése során.

Mivel a munkaterületen kívül két kihelyezett részleg is tevékenykedett, velük az összeköttetés R–159 típusú URH rádiókon keresztül valósult meg.

A munkaterület nagysága megkívánta, hogy a parancsnok és a különböző részlegek között is legyen összeköttetés. Ezt a GP 300 típusú rádiók alkalmazásával biztosították.

(A DOBOJ III. munkacsoport híradásának rendszerét a 3. ábra szemlélteti.)

Az előzőekben ismertetett hírháló az alábbi előnyöket biztosította:

- folyamatos információ áramlást az alaptábor és a munkaterület között, mely elősegítette a munkacsoport biztonságát érintő

[23] U.o. alapján

közlemények adását-vételét úgy mint a munkavégzéssel kapcsolatos közlemények továbbítását;
- a két kihelyezett részleg értesítését, információk, adatok, vészjelzések adását és vételét;
- a munkaterületen lévő részleg tevékenységének irányítását, összehangolását, riasztását.

A szakfeladatok végrehajtásából levont következtetések

A békeműveletek tervezése, végrehajtása eltér mind a háborús, mind a békevezetési rendtől.

A feladatok előkészítésére elegendő idő áll rendelkezésre, de e közben több cselekvési változatú, minden körülményt figyelembe vevő tervező, szervezőmunkát kell elvégezni.

A parancsnoki- és törzsmunkát részletekre menően kell végrehajtani, melybe annak megkezdésétől célszerű bevonni a végrehajtó részleg parancsnokát is.

A szakfeladatok kidolgozásával párhuzamosan, arra épülően, részletesen ki kell dolgozni a mindenoldalú biztosítás feladatait is.

A végrehajtásba bevont szak- és biztosító állomány felkészítését — a konkrét feladatra— minden esetben célszerű végrehajtani.

A felkészítés során a hangsúlyt a feladat megértésére, a MIOB főbb területeinek ismertetésére, és az ezekkel összefüggő, ismétlődő jellegű ismeretekre kell tenni.

A feladatra történt felkészülés ellenőrzését minden esetben végre kell hajtani.

A munkacsoportot úgy kell összeállítani, hogy biztosítási feladatok végrehajtásával a szakállományt ne terheljük, ennek következtében — az esetek többségében — előfordul, hogy a biztosító állomány létszáma nagyobb lesz, mint a végrehajtóké.

A biztosítási feladatokat két időszakra célszerű felbontani:
- a menet;
- feladat végrehajtás időszakára.

Az felhasznált híradó eszközök kompatibilitásának problémái

Az alkalmazott híradó eszközök a követezőek voltak a műszaki kontingensnél:
- Motorola GP 300;
- BTR–80 harcjárművek rádió eszközei;
- NERA típusú műholdas telefonkészülék.

Az eszközök egyike sem volt alkalmas más országok híradó eszközeivel való kapcsolatra ezért csak az összekötő tisztek útján lehetett kommunikálni. Részükre biztosítottak megfelelő típusú rádiót.

A GP 300 kis hatótávolságú néhány kilométerig alkalmas az összeköttetésre és elsősorban menetek és munkatáborok közötti híradásra célszerű alkalmazni.

A BTR-80-ban lévő rádiók (R-130, R-123) csak a hasonló típusú rádiókkal kompatibilisek más NATO országok készülékeivel nem, bár a hatótávolságuk tereptől függően ezt lehetővé tenné. Meg kell jegyezni, hogy Boszniában a nagy hegyek jelentősen csökkentették a teljesítményüket ezeknek a híradóeszközöknek.

NERA típusú műholdas telefonkészülék ez egy viszonylag korszerű eszköz, de sajnos ez sem volt kompatíbilis a békefenntartásban résztvevő országok hasonló típusú műholdas rendszereivel. Előnye, hogy bárhol alkalmazható az időjárástól és a tereptől függetlenül.

Ezek az eszközök nem képesek biztosítani az elöljárókkal, a külföldi nemzetek katonáival esetleges közös feladat végzése során a híradó kapcsolatot.

Milyen megoldásokkal javítható ez a probléma a jövőben?

Köztudott, hogy az anyagiak a legfőbb meghatározói a korszerűsítésnek, de ebben az esetben elkerülhetetlen a jövőbeni fejlesztés.

Következő javaslatokat gyűjtöttem össze a szakemberekkel való konzultációim során. A rádiótelefon lehet az egyik megoldás, ha a területen megfelelő üzemeltető biztosítja a szolgáltatást.

A következő olyan műholdas rendszerre való csatlakozás, mely kompatíbilis más résztvevő országok eszközeivel.

Esetleg egy saját hazai korszerű rendszer, mely kompatíbilis és képes a megfelelő szolgáltatás nyújtani akár békefeladatok végzésekor is. Az egyik ilyen típus lehet a fejlesztés alatt álló TETRA rendszer. Információim szerint ez a terület prioritást élvez. A jövőben komoly fejlesztés várható a híradó eszközök korszerűsítésében, melyre jelentős összeget különítettek el.

Végezetül szeretnék egy megoldást ismertetni. A Belga békefenntartók a Francia műholdas rendszerre csatlakoztak és az ő eszközeiket, használták az összeköttetés biztosítására. Ez egyrészt kompatibilitást biztosított és anyagilag is gazdaságosabb volt a Belgáknak, mintha egy külön rendszert építettek volna ki.

Ezek az országok az Internet adata lehetőségeket is kihasználták. Külön rendszert alkalmaztak a katonák saját internetes levelezéseire és egyéb civil felhasználásra, míg a katonai felhasználásra egy zárt, védett hálózatot alkalmaztak.

Befejezés

A műszaki kontingens híradó biztosítása megfelelő tervező-szervező munkával sikeresen végrehajtásra került, de számos nehézséget kellett megoldaniuk a szakembereknek.

Az híradó eszközök nagy része elavult, nem kompatibilisek más nemzetekével (NATO és ENSZ országokra gondolok).

A jövőben szükséges lesz a korszerűsítés és az együttalkalmazhatóság (kompatibilitás) megoldása.

Az általam leírtak csak egy kis szelete a híradó biztosításnak a békeműveletekben, de úgy gondolom, hogy gondolatébresztőnek nem haszontalan e rövid áttekintése a témának.

A tapasztalatok összegyűjtése véleményem szerint hasznos lehet a jövő szempontjából mind a tervező- szervezőmunka tekintetében is.

Végezetül szeretném megköszönni a kutatáshoz nyújtott segítségüket témavezetőmnek, (Dr. Kovács Tibornak) és a híradó kollégáknak is, akikkel hasznos konzultációkat folytattam.

Irodalomjegyzék:

Kovács Tibor: A béketeremtő és békefenntartó kötelékek működésének gyakorlati tapasztalatai, Tanulmány, ZMNE, Bp., 2001.

Magyarok az IFOR-ban, SFOR-ban, Zrínyi kiadó, Bp., 1997.

Szabó Sándor - Padányi József: A harc-hadművelet és békefenntartó műveletek műszaki támogatásának összehasonlító elemzése: Tanulmány, ZMNE, Bp., 2000.

Padányi József: A békefenntartó műveletek műszaki támogatása, Tanulmány, Nemzetvédelmi Egyetemi Közlemény, 5. évf. 2. szám, ZMNE, Bp., 2001.

A MH Harcszabályzata I. rész, A MH kiadványa, Bp., 1993.

A Motorola cég portálja: www.motorola.com.

MÁRKI László

A DIGITÁLIS TECHNOLÓGIA HASZNÁLATÁNAK LEHETŐSÉGEI A TÁVOKTATÁSBAN

Márki László
markil@ahrt.hu www.ahrt.hu
www.edunio.com

Az Antenna Hungária Rt. a szaki.net projekt egyik konzorciumi tagjaként részt vállalt a nyitott szakképzés támogatására létrehozott kísérleti jellegű oktatási infrastruktúra létrehozásában. A kísérlet során egy zárt, nagysebességű oktatási hálózatot hozott létre, amellyel az ország három oktatási intézményét kötötte össze egy központtal. Ezen a hálózaton nagysebességgel multimédia oktatási anyagok terjesztése, használata vált lehetővé, továbbá biztosítottá vált ennek adminisztrációs és konzultációs lehetősége. Az infrastuktúrát a NYITSZAK alapítvány szakértői korszerűnek minősítették. Sajnos anyagi okok miatt a program nem folytatódott, s így már nem valósulhattak meg az eredetileg kitűzött célok.

Hosszas előkészítő munkát és a megfelelő partnerek megtalálását követően 2001 márciusában az Antenna Hungária Rt. egyik leányvállalatának, az Antel Invest Kft.-nek a keretein belül felállított egy távoktatással foglalkozó csoportot. A csoport feladata volt a korábbi távoktatási program folytatása, illetve kiterjesztése, valamint a gyorsan változó elektronikus távoktatási piacon meghatározó részesedés megszerzése. Ennek jegyében 2001 áprilisában az Antenna Hungária Rt. vezetésével és három partnercéggel megalakult az Edunio távoktatási konzorcium.

Az **Antenna Hungária Rt. által alapított és vezetett Edunio távoktatási konzorcium** azzal a céllal jött létre, hogy **a magyar elektronikus távoktatási piacon széleskörű kompetenciáinak birtokában komplex szolgáltatásokat nyújtson ügyfelei részére**, s néhány éven belül piacvezetővé váljon ezen a piacon. A konzorcium tagjai az Antenna Hungária Rt., az OGYS Consulting Kft., az Eduweb Távoktatási Rt. és az Antenna Multimédia Rt.

Az **Antenna Hungária Rt.** informatikai és kommunikációs szolgáltatásai révén teljes körű műszaki hátteret biztosít az elektronikus távoktatási szolgáltatásokhoz, az **OGYS Consulting Kft.** a konzorciumon belül elsősorban elektronikus távoktatási tanácsadást, projekttámogatást és minőségbiztosítási szolgáltatásokat nyújt, az **Eduweb Távoktatási Rt.** az általa kifejlesztett Eduweb távoktatási keretrendszert és ahhoz kapcsolódó műszaki, oktatási szolgáltatá-

sokat és tananyagfejlesztést, míg az **Antenna Multimédia Rt.** főként az oktatási anyagok multimédiás elemeit készíti el.

Az Antenna Hungária Rt. és az Edunio távoktatási konzorcium a távoktatási szolgáltatásokat és lehetőségeket megalapozó piaci tanulmányok alapján az alábbi fontos felismerésre jutott: a „száraz" tisztán szöveges tananyagok nem használhatóak hatékonyan internetes környezetben. Ezzel szemben az internet lehetővé teszi képekkel, videókkal, hangokkal, interaktív elemekkel gazdagított tananyagok megjelenését is, ami hatékonyabb az egyszerű szöveges vagy maximum képekkel illusztrált hagyományos tananyagnál. A multimédiás elemekben gazdag tananyag viszont egyrészt modern internetes hozzáférést és nagy sávszélességet igényel a tartalom továbbítása során.

Az elektronikus távoktatás potenciális fogyasztói körét megvizsgálva az internet ellátottság alapvetően jónak mondható, ugyanakkor a sávszélességről ez már nem mondható el. A multimédiás oktatási tartalmak pedig jelentős sávszélességigénnyel bírnak. Pl. a videók használata a szűk sávszélesség miatt jelenleg az esetek többségében gyakorlatilag lehetetlen.

A fenti probléma megoldását keresve az AH szakemberei elsősorban az adatszórásban láttak jelentős potenciált. Az adatszórás tekintetében pedig a DVB (Digital Video Broadcasting – digitális műsorszórás) technológia tűnik ígéretesnek. Az AH nagyszabású kutatási programot indított a DVB-T alkalmazási lehetőségeinek vizsgálatára, amelyen belül két alprojekt csak a DVB-T távoktatásban történő alkalmazásának lehetőségeit kutatja. Az egyik projekt egy tanulmány keretében arra kereste a választ, hogy a digitális technológia, illetve az interaktív televízió hogyan alkalmazható oktatási célra, ezen belül a vizsgálat három nagy részterületet ölelt fel:

- a nagy sávszélességből eredő előnyök vizsgálata,
- pilot rendszer kiépítése a technológia tesztelésére,
- adatszórási lehetőségek vizsgálata.

A nagy sávszélesség tekintetében a lehetőségek sokkal korlátozottabbak, mint gondoltuk. A DVB-T technológia esetében az adattovábbításra használható összes sávszélesség mértéke még nem eldöntött, de feltételezésünk szerint egy országos, nyílt internetszolgáltatást nem fog tudni kiszolgálni.

A DVB-T elektronikus távoktatásban használható adatszórási potenciáljának vizsgálatára az egyik projekt keretében kiépítésre kerül egy pilot rendszer, amely szimulálja az elektronikus távoktatás technikai környezetét. A pilot rendszeren belül a felhasználók felé az adattovábbítás a DVB protokollon történik. A rendszer tesztelése bizonyította, hogy a DVB technológia lehetővé teszi nagy mennyiségű adat viszonylag gyorsan történő szórását (továbbítását). Ez pedig alkalmassá teszi távoktatási alkalmazását is elsősorban a nagy terjedelmű oktatási anyagok továbbítására. Az anyagok továbbítását követően a felhasználó már szabadon használhatja ezt a tartalmat.

A DVB-T projekt kapcsán a digitális technológia alkalmazhatóságának vizsgálatán túl az interaktív televíziózás oktatási felhasználása is kiemelt kutatási téma. A téma melletti döntést erősen motiválta, hogy a televíziót már korábban is alkalmazták az oktatásban, a digitális televíziózás pedig csak kiterjesztette a korábbi lehetőségeket, elsősorban az interaktivitás megjelenésével. A DVB-T projekt keretében elkészülő tanulmány külön is elemzi a hagyományos televíziózás oktatásban való használatát, s az ott alkalmazott módszertani elemek, valamint az interaktivitás alkalmazási területeit.

Az elméleti kutatások eredményeként megszületett tanulmány arra a következtetésre jutott, hogy a technikai lehetőségek nagyon korlátozottak, s alkalmazásonként bonyolult programok készítésére van szükség a technológia távoktatási alkalmazásához. A DVB-T technológia alkalmazása a távoktatásban ugyanakkor kiterjeszti a multimédiás és videó anyagok felhasználásának lehetőségeit.

A tanulmány alapvetően technológiai és oktatástechnikai szempontból közelítette meg a DVB-T alkalmazásának lehetőségét, és nem vizsgálta a valós felhasználói igényeket, valamint a fenti technológiák gazdaságosságát. A gazdaságossági kérdések és a felhasználói igények vizsgálata későbbi tanulmányok feladata lesz.

Az elektronikus távoktatásban a DVB-T technológia alkalmazásának nemzetközi példái, valamint ezek elemzése érdekes részét képezte a tanulmánynak, mivel a példák azt mutatják, hogy érdemes erőfeszítéseket tenni e technológia alkalmazási lehetőségének vizsgálatára.

A 6 ország részvételével, EU támogatással létrehozott SMART EDU például a DVB-S technológiát alkalmazza távoktatási célokra, így biztosította a teljes képernyős VHS minőség az átvitelét. A visszirány a SMART EDU esetében tetszőleges internetkapcsolat lehet.

Az amerikai AVAYA a Syberstar műholdas rendszerét használja e-learning szolgáltatások nyújtására, s adatszórás segítségével juttatja el az oktatási tartalmakat a helyi szerverekre.

A norvég TANDBERG Television pedig internet alapú streaming megoldást alkalmaz a digitális televíziózásról szóló oktatási anyagok továbbítására.

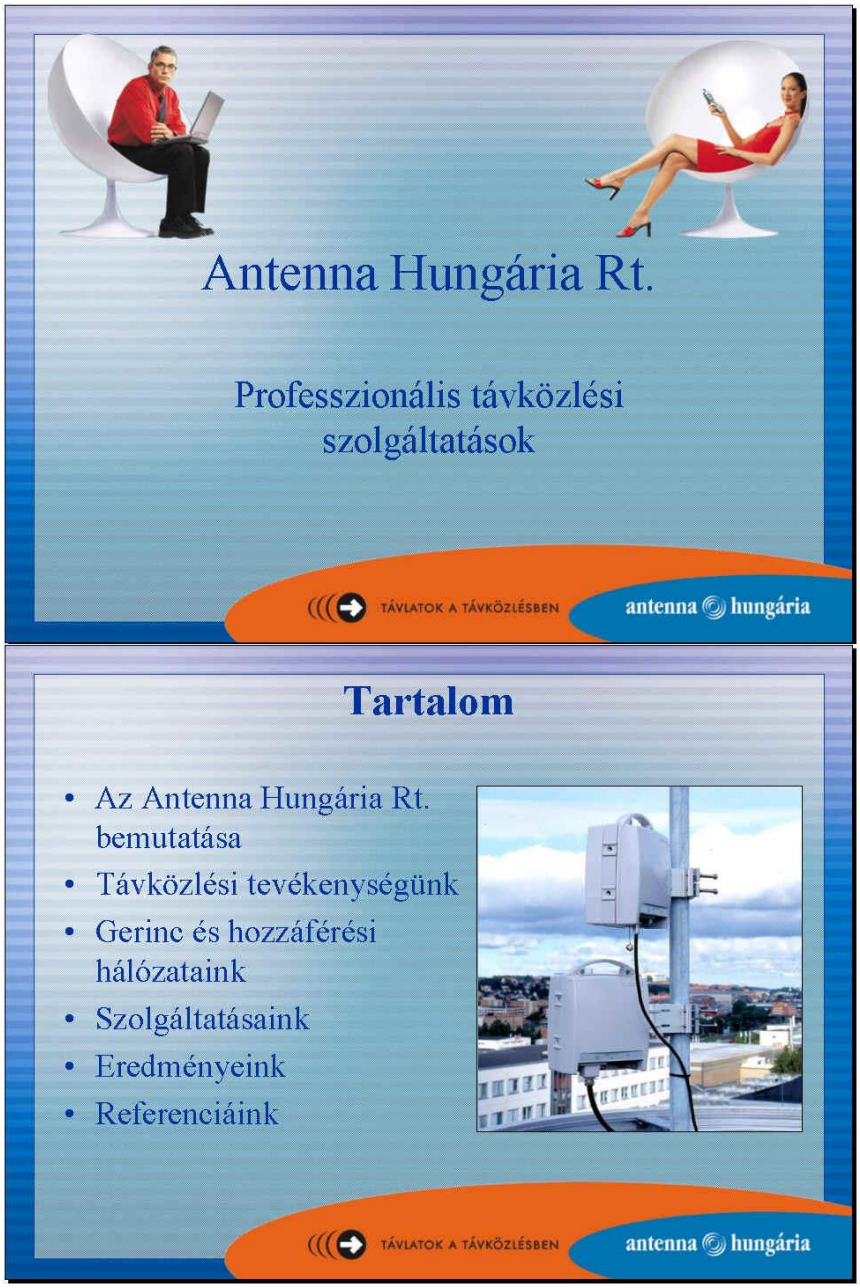
Mint az a fenti példákból is kitűnik, a DVB-T és egyáltalán az adatszórás technológiája alkalmazásának van helye az elektronikus távoktatásban. Elsősorban ott, ahol nagyméretű és gyakran változó oktatási tartalmakat kell eljuttatni földrajzilag egymástól távol eső helyekre.

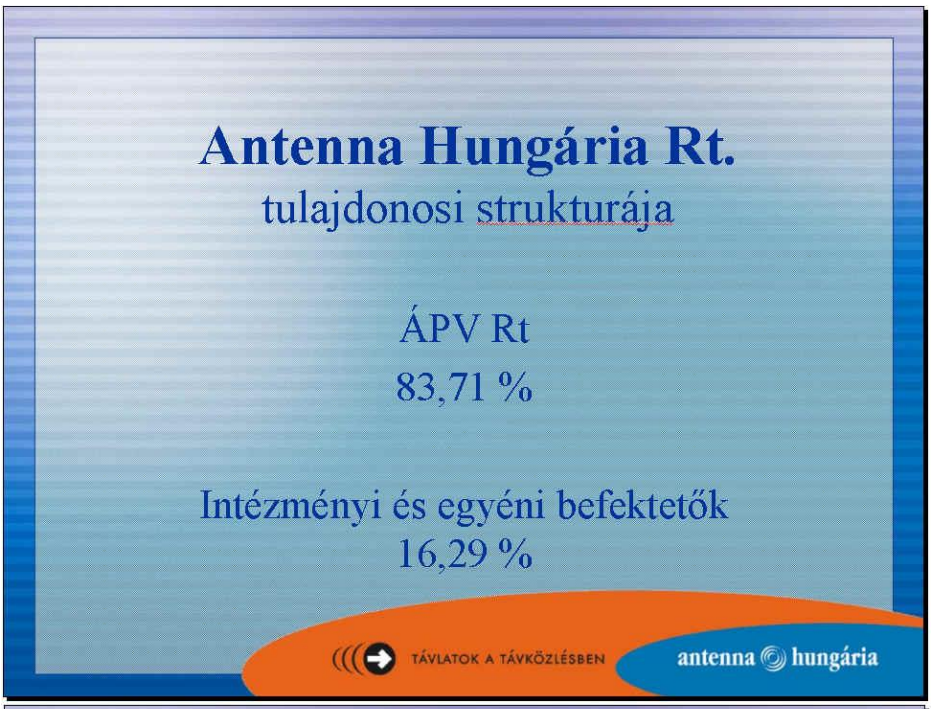
Köszönöm a figyelmet!

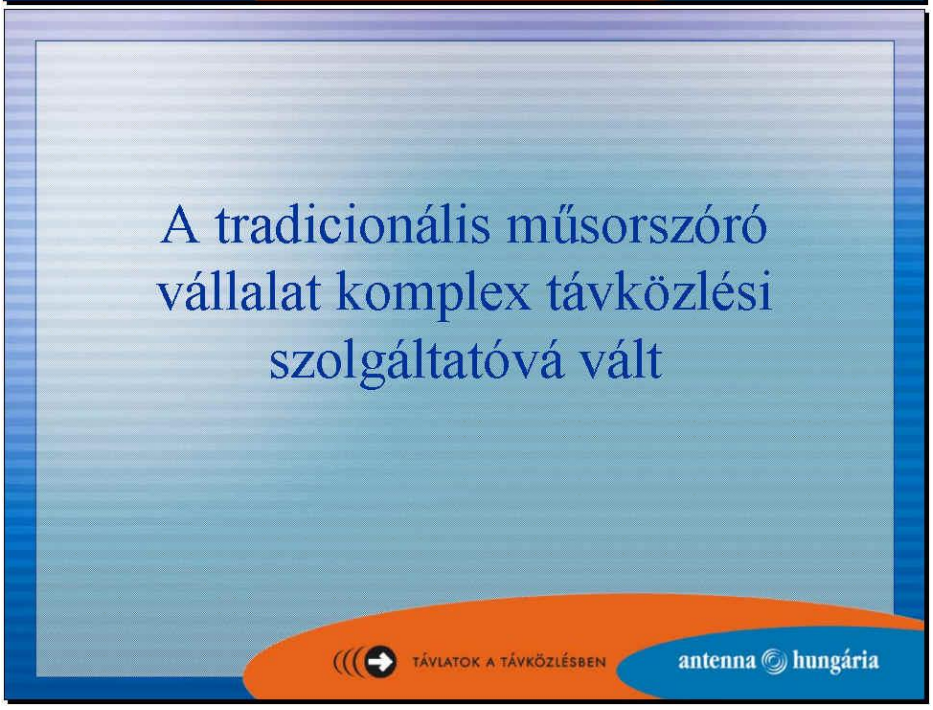
236

MOLNÁR Sándor

PROFESSZIONÁLIS TÁVKÖZLÉSI SZOLGÁLTATÁSOK

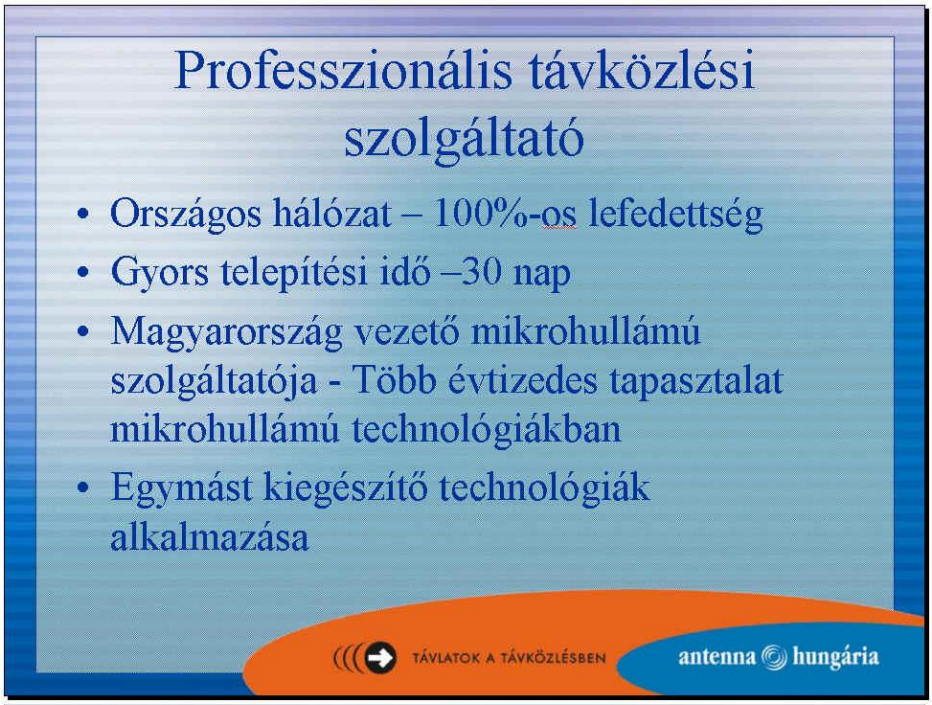


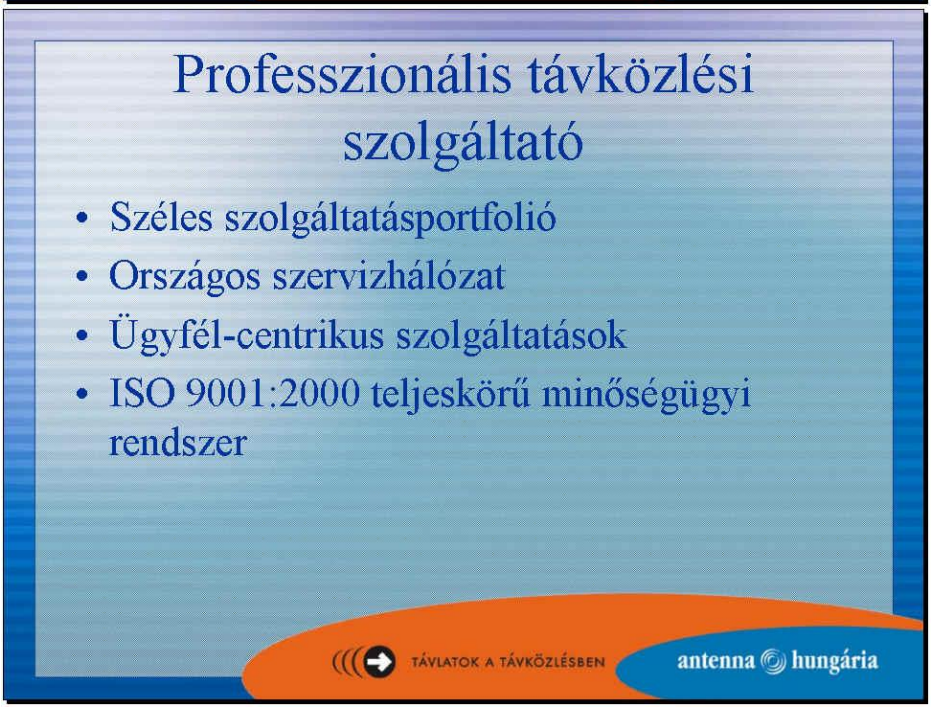

Antenna Hungária Rt.
tulajdonosi strukturája
ÁPV Rt
83,71 %
Intézményi és egyéni befektetők
16,29 %
TÁVLATOK A TÁVKÖZLÉSBEN
antenna hungária


A tradicionális műsorszóró vállalat komplex távközlési szolgáltatóvá vált
TÁVLATOK A TÁVKÖZLÉSBEN
antenna hungária


Az Antenna Hungária csoport
V.R.A.M. Rt.
(Vodafone)
Antenna Hungária Rt.
Tevékenysége:
új típusú, értéknövelt médiaszolgáltatásokat
Tevékenysége:
Informatikai outsourcing (MSP, ASP).
Tevékenysége:
saját optikai hálózatán
digitális jelek átvitelét végzi.
és távközlési fejlesztés,
tervezés, gyártás és szolgáltatás.
TÁVLATOK A TÁVKÖZLÉSBEN
antenna hungária


Távközlési történetünk
1998
1999
2000
2001
2002
1998:
- gerinchálózat kiépítése,
- alapszolgáltatások
indítása
1999:
- ügyfél igénnyel párhuzamosan
elérési hálózat építés,
- Vodafone indulása
2000:
- szolgáltatás bővítés,
- Vodafone igények
dinamikus fejlődése
- gerinchálózat bővítése
2001:
- moduláció generálta
árbevétel növekedés,
- 3,5GHz-es licensz
- Románia irányú
fejlesztés
2002:
- értéknövelt
szolgáltatások
bevezetése
- Pandant
szolgáltatás
megújítása
TÁVLATOK A TÁVKÖZLÉSBEN
antenna hungária


Professzionális távközlési szolgáltató
• Országos hálózat – 100%-os lefedettség
• Gyors telepítési idő –30 nap
• Magyarország vezető mikrohullámú szolgáltatója - Több évtizedes tapasztalat mikrohullámú technológiákban
• Egymást kiegészítő technológiák alkalmazása
TÁVLATOK A TÁVKÖZLÉSBEN
antenna hungária


Professzionális távközlési szolgáltató
• Széles szolgáltatásportfolió
• Országos szervizhálózat
• Ügyfél-centrikus szolgáltatások
• ISO 9001:2000 teljeskörű minőségügyi rendszer
TÁVLATOK A TÁVKÖZLÉSBEN
antenna hungária

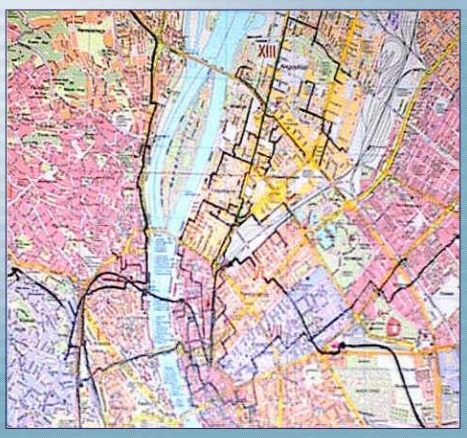
Országos hálózatunk

- Digitális mikrohullámú gerinchálózat
  Már meglévő szabad kapacitás
- Országos lefedettség
  Gyors csatlakozási lehetőség
- Domborzatilag kiemelt stratégiájú helyek
  Jó átlátás
- SDH rendszerű, topológiája 9 gyűrűből áll
  Nagy megbízhatóság

TÁVLATOK A TÁVKÖZLÉSBEN

antenna hungária

Budapesti hálózatunk

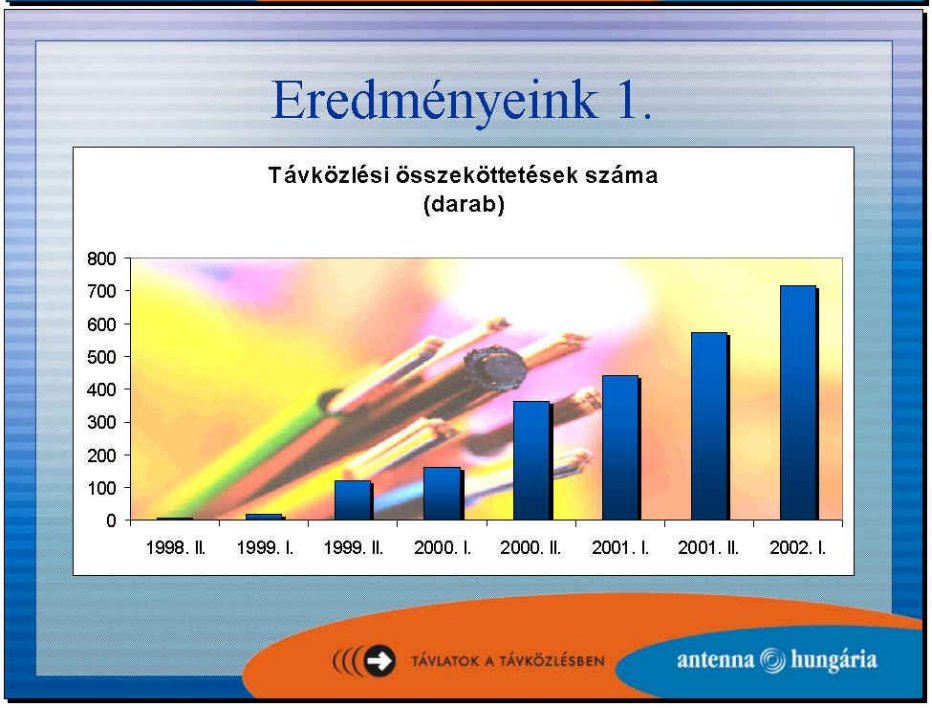


- Közel 200 kilométer hosszúságú optikai hálózat
- Az optimális gerinchálózati topológia
- Lefedettség Budapest teljes területén (1,5 és 3,5 GHz-es) mikrohullámú hálózattal

TÁVLATOK A TÁVKÖZLÉSBEN

antenna hungária


Szolgáltatásaink
Érték
E-Commerce
Alkalmazás Fejlesztés
Web Hosting
Műholdas flottakövetés
IP VPN
Műholdas járművédelem
VOIP
IP átvitel
Műsorjeltovábbítás
VSAT
Bérelt vonali Internet szolgáltatás
Sötét Szál
Menedzselt bérelt vonal
Nagykereskedelmi szektor
Üzleti és intézményi szektor
TÁVLATOK A TÁVKÖZLÉSBEN
antenna hungária


Eredményeink 1.
Távközlési összeköttetések száma
(darab)
800
700
600
500
400
300
200
100
0
1998. II.
1999. I.
1999. II.
2000. I.
2000. II.
2001. I.
2001. II.
2002. I.
TÁVLATOK A TÁVKÖZLÉSBEN
antenna hungária

Eredményeink 2.

	1998	1999	2000	2001	2002 (terv)
Az értékesítés nettó árbevétele	664 168	750 016	1 797 706	4 725 000	5 137 000

TÁVLATOK A TÁVKÖZLÉSBEN antenna hungária

Referenciáink

- bankok, pénzintézetek (**OTP Bank, Takarékbank, Postabank, Konzumbank, Budapest Bank**),
- termelő és szolgáltató vállalatok (**Pécsi Dohánygyár, Dunapack, EGIS, KITE, Hilltop Neszmély, ÖMV, Shell**),
- elektronikus média (**Magyar Rádió, UPC**),
- távközlési (**Vodafone, Pannon GSM, Nokia, V-com, Pantel, GIRO, Fornax**) és
- Internet szolgáltatók (**Externet, TV NET, Nextra, Alarmix, Drávanet, Telnet, Szabinet**), valamint a
- kormányzati szféra intézményei (**HÍF, Magyar Honvédség, PSZÁF, Hungarocontrol /LRI/, Szerencsejáték Rt.**).

TÁVLATOK A TÁVKÖZLÉSBEN antenna hungária

244

Dr. SZÉP József

A NATO ÉS A MAGYAR C3

Azonos rendeltetésű szervezeti elemek összehasonlítása

A NATO csatlakozást követő évek sok változást hoztak a híradó és informatikai szakterület életében. Szervezetek szűntek meg és új erővonalak mentén új szervezetek jöttek létre állítólag NATO mintára.

Ez a megállapítás annál is érdekesebb, mivel a NATO, ahová felvételt nyertünk – hiszen tűzzel, vassal ide törekedtünk - referenciaszervezetként állt és áll ma is előttünk egy messze nem tökéletes, de működőképes NATO C3 Board szervezettel, amelyet szándékom szerint össze kívánok hasonlítani a magyar hasonló tevékenységet folytató rendszerrel. Az összehasonlítás célja arra a kérdésre választ adni, hogy vajon célszerű-e ezt a helyzetet fenntartani vagy elérkezett az idő a „NATO mintára történő tényleges átszervezésnek". Nem szándékom a fejlesztésekben, beszerzésekben szerepet játszó számos egyéb szervezet megnevezésével, tevékenységével foglalkozni, csak a „szűkebb értelemben vett „szakma" szervezeti alapjaival.

A bemutatást két alapvető körben kívánom elvégezni. Elsősorban ismertetem a NATO híradó, informatikai, egyéb elektronikai tevékenységét irányító szervezetét, röviden bemutatom alrendszerének főbb elemeit. Másodsorban megnevesítem a szakterületeket és megkeresem azokat a szervezeteket, amelyek hasonló vagy azonos célú tevékenységet folytatnak Magyarországon, amennyiben egyáltalán léteznek.

1. Híradó terminológia

Mielőtt rátérnék a szervezetek összehasonlítására még egy alapvető apróságra kívánok rámutatni, nevezetesen a katonai híradó terminológiára. Napjainkra kuszaság alakult ki ezen a területen. A híradás, a híradócsapat, híradóközpont stb. fogalmak évszázados hagyományokra tekintenek vissza. Az informatikai alkalmazások szükségszerű térnyerésével, sokakban azonban disszonanciát vált ki a híradás, híradórendszer stb. kifejezések következetes használata, mivel sokan a jelenlegi tábori hírrendszer képességére és eszközparkjára asszociálnak, és jogosan vetik fel, hogy ez a terminológia csak elvétve tesz utalást az automatizálásra az információs rendszerekre. Van olyan megközelítés, amely –nem helytelenül – tágabb értelemben kommunikációról, kommunikációs rendszerről beszél. Ezzel párhuzamosan megjelent a NATO terminológia is, amely egyes esetekben teljesen új – C2, C3, CCIS, interoperabilitás stb. – kifejezéseket hozott az elfogadott vagy már meghonosodott magyar katonai híradó terminológia palettájára.

Intermezzóként a híradó terminológiával kapcsolatos - természetesen vitatható – magánvéleményem illusztrálására egy számomra szimpatikus példa bemutatásával szeretnék hozzájárulni és a terminológiára érzékeny szakértők figyelmébe ajánlani.

Példaként említem az USA fegyveres erők erre utaló magatartását, amely mind a ma napig tradícióból a „Signal" magyarul „Jel" kifejezést használja a katonai híradás tartalmi kifejezésére, mivel a XIX. században létrehozott „Signal Corps" jelzőcsapatok" valóban jelzőeszközöket használtak a vizuális kommunikációra (piros és fehér zászlót nappal, illetve piros és fehér lámpát éjjel). A „Signal Soldier" azaz „Jelző Katona" mind a mai napig a két zászlóból készített fegyvernemi jelzést viseli a hajtókáján. Ugye senki nem merné azt állítani, hogy az USA híradó és informatikai, valamint fegyverirányítási rendszerei jelenleg nem a világelső kategóriába tartoznának, és mégis ragaszkodnak a fülnek elavultan csengő „Signal Officer" „híradótiszt", „Signal Troops" „híradóalegységek", „Signal Corps" „híradócsapatok" fogalmak használatához. Az átviteli rendszer a jelzőrendszer, az információ a jel, a kommunikáció pedig a jelcserét megvalósító cselekvés. Az informatikának, mint tudományterületnek minden vívmányát felhasználják és beleértik a régies kifejezésbe. Senkinek nem okoz lelki traumát, és senki nem kívánja magát híradótisztnek, vagy informatikai tisztnek tituláltatni, mivel a hierarchiában nem jelent sem előnyt, sem hátrányt, egyszerűen csak a rendszer működtetésében elfoglalt szakmai tevékenységre utal.

Analóg módon a magyar „hír" szó az én interpretációmban az információ maga, amelyet valamilyen átviteli rendszeren, „híradó rendszer" valamilyen átvitelre alkalmas formában továbbításra „adásra" és az emberi érzésszervek által feldolgozható módon megjelenítésre kerül azon felek számára, aki a „hírváltást", azaz az információcserét végrehajtják, más szóval a kommunikációt, mint cselekvést folytatják. Aki az erre szolgáló technikai rendszert működteti az nem más, mint a „híradó katona", „híradószervezet" és ezen a gondolatsoron így tovább.

Annál is inkább javaslom a katonai „híradás" és az ebből származtatott kifejezések megtartását, mivel véleményem szerint a híradás fent vázolt tradicionális kifejezése egyike a valóban létező nem mondvacsinált katonai hagyományainknak.

Viszont vitán felül kétségtelen tény, hogy a magyar katonai híradó terminológia megrekedt egy majd húsz év előtti szinten és rendbetétele több mint időszerű, mondhatni megkésett szükségszerűség. Írásomban a tradicionális híradó, illetve a híradás és informatika kifejezéseket egyaránt használom, ahol azt szükségesnek ítéltem arra nézve, hogy véletlenül se vesszen el az értelme az információkezelés, az információtárolás, információmegjelenítés legmodernebb eljárásait képviselő szakterületnek.

Az egyes felszínre kerülő NATO híradó terminológiák értelmezésére a jobb megértés kedvéért az adott szövegkörnyezetben térek ki.

2. A NATO C3 Board rendeltetése, struktúrája

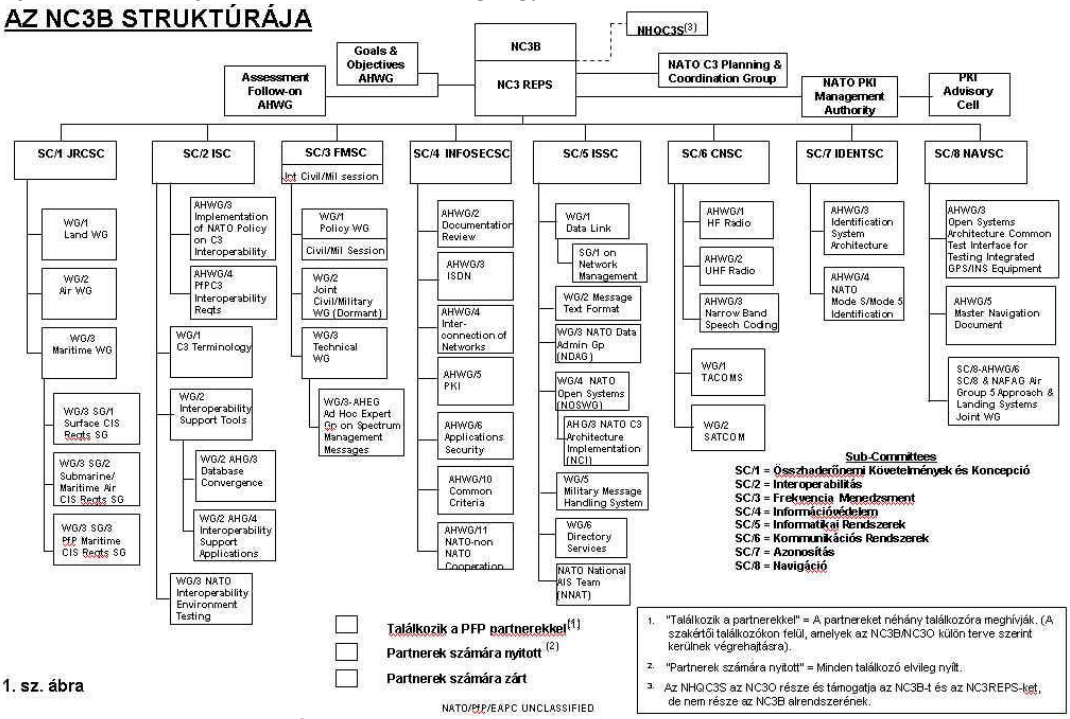
Az NATO jelenleg működő C3 szervezetét 1996-ban hozták létre, amikor világossá vált, hogy az iszonyatos sebességgel fejlődő, ezzel párhuzamosan egyre bonyolultabb, szerteágazó távközlési, informatikai, elektronikai rendszerek vezetése, fejlesztése egységes koncepció, követelménytámasztás, szabvány nélkül nem folytatható. A koalíció híradása a „Sivatagi Viharban", a NATO hadászati, harcászati híradása a jugoszláviai műveletekben enyhén szólva megbukott. Megszületett az Észak-atlanti Tanács és a hadászati parancsnokságok racionalizálásra vonatkozó igénye, amelynek következtében létrejött a célkitűzést végrehajtani hivatott szervezet.

Mielőtt rátérnék a szervezet, és a szervezeti elemei rövid ismertetésére elérkezett az idő, hogy a NATO híradó terminológiájából a C2, C3 kifejezésnél álljunk meg egy pillanatra. Két szélesen elterjedt és elfogadott, eltérő tartalmú értelmezés van. A NATO értelmezésű C3, angol nyelven a „Consultation Command and Control", magyarul a Konzultáció, Vezetés és Irányítás kifejezést takarja. Tartalmát tekintve nem azonos a másik C3, azaz angol nyelven a „Command Control and Communications", magyarul Vezetés, Irányítás és Kommunikáció kifejezéssel. A Magyarországon az alapvető probléma a „Command and Control" „Vezetés és Irányítás" C2 értelmezése körül alakult ki a NATO csatlakozás előtt. Félreértelmezésből, vagy hozzá nem értésből – a klasszikus vezetés fogalomkörét keverték össze, a vezetési mechanizmust automatikus adatfeldolgozással, megjelenítéssel, tárolással támogató technikai rendszerrel, amely tény, hogy a vezetési és irányítási rendszer alrendszere. [Lásd AAP –31(A)].

A NATO legfelső szintje katonai értelemben nem vezet. A katonai vezetés a hadászati parancsnokok dolga. A NATO, mint politikai szervezet konzultál, megbeszél, megoldást keres. Ezért van az, hogy a konzultációt helyezi előtérbe, de az előbb említett olyan (NATO) C3 technikai rendszer felhasználásával valósítja meg, amelyben túlsúlyos a globális, statikus, konzultáció lefolytatására alkalmas elem. A másik, a nemzeti C3 egy országon belül hadászati, hadműveleti, harcászati vezetési és irányítási információs rendszereket takar, amelyekben a statikus és mobil elemek egyaránt megtalálhatók és alapvető feladata a katonai műveletek támogatása. Az Észak-atlanti Tanács ezt a mindkét tevékenységet támogató (konzultáció és katonai műveletek), technikai rendszer fejlesztését, felügyeletét rendelte minden járulékos problémájával, specifikumával együtt egy szervezet felelősségi körébe.

A NATO teljes vertikumában (politikai és katonai) konzultációs, vezetési és irányítási ügyekben kizárólagos joggal és felelősséggel eljáró legfelső szintű multinacionális irányító testület a **N**ATO **C3 B**oard, azaz a NATO C3 Igazgatóság (a továbbiakban NC3B), amely közvetlenül az Észak-atlanti Tanács és a

Védelmi Tervező Bizottság alárendeltségébe tartozik, azok a nevében jogosult eljárni. Struktúráját, tekintve a NATO legnagyobb szervezete.



1. sz. ábra

Tanáccsal látja el az Észak-atlanti Tanácsot, a Védelem Tervező Bizottságot és a Katonai Bizottságot az összes tagállam érdekét szolgáló kérdésekben, egyúttal a NATO C3 Szervezet igazgatótanácsaként funkcionál. Az NC3B évente két alkalommal 2 napot ülésezik. Tagjai a nemzetek vezető beosztású szakmai képviselői, a hadászati parancsnokságok J6 főnökei, az NC3A, a NACOSA vezetői, a Katonai Bizottság, valamint a légi vezetéssel, pénzügygyel, légvédelemmel, és a biztonsággal foglalkozó NATO főbizottság képviselője. Egyike azon kevés főbizottságoknak, ahová minden nemzet két főt delegálhat, a rendkívül szerteágazó C3 szakterületet átfogására. Ez a két személy az, akinek a nemzet nevében joga van nyilatkozni és az úgynevezett „Silence Procedure" azaz a „hallgatási eljárás" szabályait betartva megakadályozni egy nemzeti érdeket sértő konszenzust.

Az NC3B állandó elnöke a NATO főtitkár védelempolitikai támogatásáért felelős helyettese. Két társelnöke van, amelyek közül az egyik a mindenkori NATO Központ C3 Törzs (a továbbiakban NHQC3S) igazgatója, a másik nemzeti jelölést követően a nemzetek által kerül megválasztásra. Mindkettő vezérőrnagy rendfokozattal rendelkezik. Az NHQC3S a NATO Nemzetközi Törzs állományába tartozik. Magába foglalja az NC3B összes alárendelt albizottságának elnökét, és a megfelelő létszámú szakértői, hadműveleti tiszti,

illetve adminisztratív állományt. Az NHQC3S politikai részről a védelem támogatásért felelős főtitkárhelyettes, katonai részről a Nemzetközi Katonai Törzs igazgatójának napi irányítás alatt áll, viszont az NC3B döntéseinek végrehajtó szerve, az ezzel kapcsolatos adminisztratív tevékenységet hajtja végre.

Az NC3B üléseinek szünetében - gyakorlatilag egész évben - az NC3B jogkörét a Nemzeti C3 Képviselői Csoport (Group of National C3 Representatives) gyakorolja. Minden nemzet két fő nemzeti C3 képviselőt (a továbbiakban NC3 képviselő) jogosult delegálni a már fent említett széleskörű tevékenység átfogására, amellyel a nemzetek alapvetően élnek. A komolyabb apparátussal, nagyobb befolyással bíró vagy bírni vágyó nemzetek híradó csoportokat, híradó szolgálatokat tartanak fent, melynek az élén az NC3 képviselő áll. Az NC3B igazgatók felhatalmazása alapján az NC3 képviselőnek jogában áll a nemzet nevében állást foglalni és joga van „Silence Procedure" eljárás szabályainak betartásával megakadályozni a nemzet érdekeit sértő állásfoglalást, illetve jobbító szándékát egy adott ügyben érvényre juttatni. Az NC3B felhatalmazása alapján ez a testület jogosult a Board nevében a NATO teljes egészét érintő C3 vonatkozású döntéseket hozni és irányítani a NATO C3 Szervezet szerves részét képező **N**ATO **C**onsultation **C**ommand and **C**ontrol **A**gency-t (a továbbiakban NC3A), illetve a **NA**TO **C**IS **O**perating and **S**upport **A**gency-t (a továbbiakban NACOSA) szervezeteket. Egy rövid kitérővel tekintsük át a két említett szervezet feladatát, és a nevesítsük meg a magyar megfelelőjét. Mindkettő referenciaértékű szervezet, amely a NATO életében kulcsfontosságú szerepet tölt be.

Az NC3A adja a tudományos támogatást, az NC3B felelősségi körébe tartozó híradó, informatikai, és egyéb elektronikai rendszerek műszaki tervezésére, végzi az eszközök, rendszerek beszerzését, rendszerbeállítását. Csak érdekességképen már hat magyar mérnök dolgozik az NC3A hágai részlegében, ami a Magyarország, a magyar szellem számára egyfajta elismerés, mivel a részünkre csak egy kvótás hely biztosított. Sajnos Magyarországon ennek a komplex tevékenységnek megfelelő szervezet nem működik. A műszaki tervezéstől a rendszerbeállításig számos szervezet bábáskodik a magyar szférában. Az eredményességükre nem kívánok eben az írásban szót vesztegetni.

A NACOSA a NATO távközlési rendszereit üzemeltető szervezete. Az MH-ban ennek a szerepkörnek az MH Híradó Parancsnokság felel meg. A NACOSA egyre nehezebben képes eleget tenni alaprendeltetésének a magasan képzett kezelői állomány egyre növekvő hiányának köszönhetően. A nemzetek ugyanis nem akarják feltölteni a kezelői beosztásokat. Mindenki azt várja, hogy a másik nemzet majd megteszi. A nyelvismeretet tekintve a NACOSA már ott tart, hogy nem vizsgálja az angol nyelvtudás szintjét, csak legyen valaki, aki a jó irányba fordítja a kapcsolót.

Visszatérve az NC3B struktúrához a Board alárendeltségébe nyolc albizottság tartozik, amelyek mindegyike alárendelt munkacsoportok, illetve ad-hoc

munkacsoportok alrendszeréből áll. A nyolc albizottság a következő funkcionális területeket öleli fel:

- Összhaderőnemi követelmények és koncepció
- Interoperabilitás
- Frekvenciamenedzsment
- Információvédelem
- Informatikai Rendszerek
- Kommunikációs rendszerek
- Azonosító rendszerek
- Navigáció

Az albizottságok alá rendelt munkacsoportok összlétszáma száma 46, bár ez időnként az ad-hoc munkacsoportok létrehozása vagy feloszlatása miatt változik. Az NC3 képviselők közvetlenül irányítják a NATO Nyilvános Kulcsú Infrastruktúra Menedzsment Hatóságot és a NATO C3 Tervező és Koordinációs Csoportot. Az NC3B struktúra szigorúan hierarchikus. Érdekessége ennek a struktúrának, hogy a legalacsonyabb szinten elhelyezkedő munkacsoportok képviselik a legmagasabb szintű speciális műszaki tudást, míg a magasabb szinteken levő szférákban egyre nagyobb teret nyer a globális rendszerszemlélethez, valamint irányelvek kidolgozásához szükséges képesség. Az 1. sz. ábrán az NC3B szervezeti struktúrája látható. Az ábrán az NC3B felépítménye teljes részletességgel jelenik meg.

A szervezeti felépítés és a magyar rendszerrel való összehasonlítás szempontjából az albizottságok a mérvadók. Ezek tükrözik hűen azt a feladatkört, amelyet az NC3B végez, illetve szolgálnak alapul nemzeti szervezetekkel történő összehasonlításra. A teljesség igénye nélkül ismertetett NC3B főbb szervezeti elemeinek áttekintése után vessünk egy pillantást a „magyar C3 Board" arhitektúrájára. Tekintsük át hol vannak azok a magyar híradó szervezetek, amelyek partnerként kezelik a NATO C3 ügyeket, megjelenítik a magyar érdekeket az NC3B alárendelt szakmai bizottságaiban. Nézzük meg röviden, hogyan történik a NATO-tól kapott információk feldolgozása, terítése, a magyar híradó és informatikai fejlesztési tervekbe történő adoptálása, a magyar NC3B igazgatók tájékoztatása.

3. A magyar helyzetkép

Nem szándékom a jelenlegi status quo történelmi háttérről beszélni, mert az egy külön elemzést érdemelne meg, hogy mi történt, mi és ki játszott szerepet a létrehozásában, és hogy vezetett lépésről lépésre a mai helyzet kialakulásáig. Szándékom szerint felvállalni csak azt kívánom, hogy az előzőekben vázolt NATO szakmai szub-struktúrát követve rámutassak, vajon létezik-e magyar megfelelője, illetve rámutassak azokra a deviáns szervezeti elemekre és magatartásra, amelyek a jelenlegi status quo folytatását véleményem szerint a jövőben tarthatatlanná teszik. Kívánom ezt megtenni abban a logikai sorrendben, ahogy az NC3B albizottságai követik egymást.

a. Összhaderőnemi híradó követelmények és koncepció

Funkcionális tevékenységét tekintve nem más, mint a híradó szolgálatoknál korábban jól ismert híradó hadműveleti osztály, alosztály szervezete. Ez a szervezet az, - amely hivatott a sokak számára ismerősen csengő híradó hadműveleti követelmények, híradó normatívák, és a hírrendszer telepítéséhez, vezetéséhez, fenntartásához, az elektronikai biztosítás, ellátás megszervezéséhez, tervezéséhez szükséges elvi követelmények kidolgozására. A napjainkban divatossá vált kifejezéssel élve doktrínaformáló szervezet.

Ez az a szervezet, amely az összhaderőnemi, haderőnemi követelményekhez magát a hírrendszer leírását fogalmazza meg, amely normálisan működő országokban minden nemű katonai híradó és informatikai, elektronikai rendszerfejlesztés alapokmánya.

Sem a HM IHF, sem a HM-HVK VCSF-ség állományában nem található meg tisztán ilyen feladatrendszerű szervezet. Valaha a Magyar Honvédség teljes vertikumában működött, mielőtt teljesen felszámolásra került. Amíg, az NC3B-ben működő szervezet szárazföldi, haditengerészeti és légierő munkacsoport tagozódásban haderőnemi alárendelt komponensekből épül fel, amelyek a haderőnemek sajátos helyzetét, működési környezetét figyelembe véve jelenítik meg, dolgozzák ki a haderőnemi specifikus mutatókat, amelyek alapkövetelményei a Board összes többi albizottságának, addig HM, MH szervezetében ilyen szervezet egyszerűen nem létezik.

Az NC3B-nál történő képviseletet a HM-HVK VCSF, Híradóosztály látja el öröklési alapon, mivel az osztály jogelődje a Híradó Csoportfőnökség volt és annak az állományában működött a híradó hadműveleti osztály.

b. Interoperabilitás

Természetesen ilyen tevékenységet megvalósító szervezet sincs sem a HM IHF, sem a HM-HVK VCSF-ség állományában, következésképpen ilyen irányú tevékenység nem folyik sem a HM, sem az MH egyetlen szervezetében sem. Öröklött hagyományaink a témában nincsenek.

Az interoperabilitás jelentéstartalmát tekintve nyilvánvaló, hogy a volt VSZ katonai tömbjében fel sem merült. Az egységes elgondolások alapján fejlesztett rendszerekben kevés kivételtől eltekintve gyakorlatilag azonos típusú, azonos gyártmányú, azonos interfészű eszközök voltak, amelyek esetében bár voltak kisebb a nemzetek által használt csatlakozókábelek fejeiben, alapvetően azonban az analóg átviteltechnika szabványainak megfeleltek és az interoperabilitás definíciójával összhangban más rendszerek részére szolgáltatást nyújtottak, illetve azoktól fogadtak, úgy, hogy egymás működését nem zavarták. Így a majdhogy kizárólagosan analóg rendszerekben, rendkívül alacsonyfokú automatizálás mellett interoperabilitással foglalkozó terület kialakítására nem volt igény sem szükségszerűség.

A különböző nemzetek által gyártott híradó rendszerek, eltérő szabványok, eltérő protokollok, interfészek, vagy eltérő generációs, eltérő technológiájú

digitális rendszerek alkalmazása esetén az interoperabilitás kutatása, a tesztkörnyezet megteremtése, egységes szabványok létrehozása egy NATO méretű, gazdasági érdekeket is megjelenítő koalícióban elengedhetetlen. Mi még nem tapasztaltuk meg komolyan a stacioner vagy tábori digitális hírrendszer koalíciós környezetben történő rendszerbekapcsolásának buktatóit nem lévén ilyen rendszerünk. De lassan közeledik már az idő, amikor szembesülünk a való világgal, de akkor kapkodni interoperabilitási kutatások után már késő lesz.

A képviseletet mind a HM IHF, mind a HM-HVK VCSF-ség biztosítja. Rutinszerűen jelenthetem, hogy a NATO-tól kapott interoperabilitással foglalkozó dokumentumok nem kerültek fordításra, az MH szervezetében csapatszintre vagy akár haderőnemi szintre még eredetiben sem kerültek kiadásra.

c. Frekvenciamenedzsment

Ismét egy olyan szervezeti elemhez értünk el, amely sem a HM IHF, sem a HM-HVK VCSF-ség állományában nem található meg. Érdekesebb azonban a helyzet, mivel három szervezet is munkálkodik az adott területen. Kettő a frekvenciagazdálkodással (polgári és kormányzati) a harmadik a katonai frekvencia-felhasználás tervezésével foglalkozik. Érdemes néhány szót vesztegetni az itt kialakult helyzetre.

A kezdetek kezdetén a Kormányzati Frekvenciagazdálkodási Hivatal (KFGH) szerezte meg a jogot az MH képviseletére az NC3B-nak alárendelt Frekvenciamenedzsment Albizottságban. A HM IHF főosztályvezetőjének, illetve a HM-HVK VCSF-ség csoportfőnökének - az NC3B igazgatóknak - gyakorlatilag jelentési kötelezettséggel nem tartozik, mivel egyrészt nincs olyan szabályzó, amely a jelentésre kötelezné az ülést követően, hogy milyen ügyben, milyen álláspontot képviselt, másrészt a kormányzati frekvencia felhasználók felett hatósági jogkört gyakorló szervezet. Teljesen ellentétes egymással, hogy az országot reprezentáló, a NATO szintjén az Észak-atlanti Tanács nevében intézkedési, döntési jogkörrel rendelkező NC3B igazgatókat nem köteles tájékoztatni, viszont a nekik alárendelt albizottságban ellátja a képviseletet, ugyanakkor Magyarországon a felettes szervei felett hatósági jogkört gyakorol.

A katonai frekvenciamenedzsmenttel foglalkozni hivatott szervezet a HM, MH állományában sincs. A katonai frekvencia-felhasználás tervezése a HM-HVK Felderítő Csoportfőnökség, Elektronikai Hadviselési Osztály felelősségi körébe tartozik. Ugyanakkor az MH-án belül a rádióelektronikai kisugárzás ellenőrzését, az elektronikai védelmet végző végrehajtó szervezete az MH HIP állományában található. Az EHV viszont az NC3B Frekvenciamenedzsment Albizottság munkájában nem vesz részt, így tevékenysége kizárólag az MH –án belülre korlátozódik.

Érdemes elgondolkozni azon, hogy miért nincs a katonai frekvenciafelhasználással foglalkozó szervezet sem szolgálatilag sem szakmailag alárendelve a hírrendszer működéséért felelős szervezet vezetőjének, (a végrehajtó

szerve viszont igen!). Említésre méltó még, hogy haderőnemi szinten katonai frekvencia-felhasználással foglalkozó szervezeti elem nincs az MH-ban. A NATO-tól kapott frekvenciamenedzsmenttel kapcsolatos dokumentumok, haderőnemi szintre nem kerültek kiadásra, nem kerültek fordításra, az érintett vezetők nincsenek tájékoztatva.

A frekvenciamenedzsment terén nem egyértelműen a szakterület hiánya a domináns, hanem alárendeltsége, a jogosítványok, a feladatmegosztás kérdése. A civil-katonai munkacsoportban jelenleg Miniszterelnöki Hivatal képviselője jeleníti meg a polgári érdekeket.

d. Információvédelem

Ezen a téren is ellentmondásos a helyzet. A HVK VCSF-ség létrehozásakor megosztásra került az addig funkcionáló információvédelmi osztály. Egy részét a HM Információ és Dokumentumvédelmi Főosztály szívta magába, míg a másik fele beolvasztásra került a HVK VCSF-ségen belül akkor felállt Biztonsági Osztályba. Az Információvédelmi Albizottságon felül, kivétel nélkül minden alárendelt ad-hoc munkacsoportban a HM Információ és Dokumentumvédelmi Főosztály képviselteti magát. Jelentési kötelezettséggel az albizottságban, illetve a munkacsoportokban folyó tevékenységéről nem tartozik a HM IHF és a HM-HVK VCSF vezetői felé.

Mivel a HM-HVK VCSF-ség rendelkezik egy furcsa összetételű - információvédelmi téren megnyirbált jogosítványokkal rendelkező - Biztonsági Osztállyal, az NC3B-tól minden okmány részére is megküldésre kerül. A HM IHF nem kap a dokumentumokból. Megállapítható, hogy az információvédelem terén sem egyértelműen a szakterület nem léte domináns, hanem itt is az alárendeltsége, a jogosítványa, a feladatmegosztás kérdése.

e. Informatikai Rendszerek

A HM-HVK VCSF-ség szervezetében megtalálható informatikai osztály egyre agilisabban, hatékonyabban kezd funkcionálni. Az informatikai hálózatok fejlesztésében végzett szerepük, tevékenységük, hatékonyságuk részletes értékelése nem célom a szervezeti anomáliák ismertetése során. A HM és a HM-HVK egyaránt képviselteti magát az NC3B illetékes albizottságában, illetve kölcsönös munkamegosztás alapján a munkacsoportokban is.

f. Híradó hálózatok

A szakterület kezelését a HM-HVK VCSF-ség állományában egy híradó osztályszintű szervezet végzi. Alaprendeltetése mellett minden olyan tevékenység ezen az osztályon maradt, ami a HM-HVK VCSF-ség többi elem nem tud, vagy nem akar elvégezni, illetve korábbi szerepkörénél fogva ráöröklődött, nevezetesen az interoperabilitás, hadászati védelem híradó tervezése, védett vezetési rendszerek, híradó hadművelet, híradó kiképzés (kamarai jogkörrel), M-kieg, navigáció, légi vezetési rendszerek, doktrínaszerkesztés, NATO DCI és DPQ, futár- és tábori posta.

És még egy érdekesség, ami még egy szögből megvilágítja a katonai frekvencia-felhasználás hollétének kérdését. Mivel a kommunikációs célú frekvenciát használó eszközök, így a rádiók, rádió-relék alkalmazásának tervezése, a rádióhálók és irányok táblázatának elkészítése a híradó osztályon (mint már említettem nincs hadműveleti osztály) történik bármilyen hihetetlen, de ez az osztály valósítja meg a valós frekvencia-kiosztás is a Magyar Honvédség teljes egészében, mivel a HM-HVK Felderítő Csoportfőnökség erre nem hajlandó.

Az osztály görgeti maga előtt az MH hosszú híradó fejlesztési tervét is. Ellátja a képviseletet az NC3B összhaderőnemi követelmények és koncepció, az interoperabilitás, a híradó rendszerek és a navigáció albizottságaiban.

g. Azonosító rendszerek

A HM vagy HM-HVK szinten sincs rá szervezet. Az Azonosító Rendszerek Albizottság az NC3B szerves része, viszont a képviselet ellátását Magyarországon a HM-HVK Hadműveleti Csoportfőnökség felelősségi körébe utalták. Az albizottság mindkét munkacsoportjába viszont az MH ÖLTP –től került egy képviselő kijelölésre. Az MH ÖLTP szakembere tartós kiküldetésre NATO beosztásba került. Jelentési, tájékoztatási rend nem működik. Az okmányok feldolgozása nem történik meg. Az azonosítás, azon belül az IFF Magyarországon gyakorlatilag halott terület.

h. Navigációs rendszerek

HM vagy HM-HVK szinten nincs rá szervezet. A képviseletet a HM-HVK VCSF Híradóosztály egy főtisztje látja el. Ez véletlenül a múltat jól ismerő utolsó aktív szakemberek egyike. A kapott információ feldolgozásra nehézkes. Az okmányok eredetiben az MH LEP részére is megküldésre kerülnek.

4. Összegzés

Számszerűen bizonyítható, hogy az NC3B felelősségi körébe tartozó nyolc funkcionális szervezeti elem közül négy területre – híradó hadművelet, interoperabilitás, azonosítás, navigáció - nincs Magyarországon felelős szervezet (a szakterületek 50%-a), ezen felül további kettő hatósági jogkört, illetve felettes szerv szerepet gyakorol a szakmai felettese felett.

Nyilvánvalónak tűnik, hogy az egymástól nem ritkán független szervezetek között szerteszét szórt feladatkörök összefogására, követelménytámasztásra, felelősség és jogkör gyakorlására az arra illetékes vezetőknek jelen szabályzók megléte mellett alig, gyakorlatilag nincs lehetősége. Szakmai jelentési rendszer mind a mai napig nem került kialakításra. Az információtovábbítás, a feldolgozás kevés kivételtől eltekintve alacsony színvonalú.

A NATO és a létező magyar C3 szakmai szervezetek közötti összehasonlítás eredményeként azt a megállapítást kell tennem, hogy jelen felállásban sem külön-külön, sem együttesen nem képesek az NC3B felelősségi körébe tartozó szakterületek lefedésére, kezelésére. Meggyőződésem, hogy amennyiben a kialakult állapot felszámolására nem tesznek lépéseket, akkor prognosztizálhatatlan jövőképpel kell a szakmának szembenéznie.

Meggyőződésem továbbá, hogy ha a szervezetek nem alakulnak hazai és nemzetközi szinten is jogosítvánnyal rendelkező szervezetté, és nem kapják meg a források feletti rendelkezési jogot, addig a kusza, összevisszaszabályozott magyar struktúrában soha, senki, semmiért nem tehető felelőssé.

Meggyőződésem az is, hogy mindaddig, amíg a szervezeti alapok, a jog és hatáskörök nem kerülnek rendezésre, addig a fejlesztés, beruházás, rendszerbeállítás és fenntartás körül kialakult állapotok nem szűnnek meg.

Bármilyen is legyen az új struktúra az csak jobb lehet, amennyiben le tudja kezelni a felelősségi körébe tartozó feladatokat. A múlt és jelen tapasztalatait elemezve egyetlen dolog markánsan kiemelhető. Jolly Joker vezetőkre, szervezetekre ebben a szakmában pedig nincs igény. Csak integrált szervezet, pontosan meghatározott feladat és jogkör, jól koncentrált és menedzselt szaktudás és a kollektív csapatmunka lehet megoldás semmi más. A megújulás reményében Dr. Lindner Miklós nyá. vörgy. az MH volt híradófőnökének a szavait szeretném mindenki számára célzás értékkel idézni:

„Ez a szakma nem tűri a sztárokat.”

256

GERGELY Péter

AZ INFORMATIKAI KÉPZÉS RENDSZERE A MAGYAR HONVÉDSÉGBEN

Az elmúlt évtizedben az informatika robbanásszerű fejlődésének lehettünk tanúi. Túlzás nélkül állítható, hogy mára nincs olyan területe az életnek ahol a számítástechnika ne játszana valamilyen szerepet. A fejlődés természetes következménye, hogy a honvédség is mint felhasználó egyre több területen használja ki a számítógépek nyújtotta lehetőségeket.

Az átalakulóban levő honvédség és a XXI. század kihívásainak megfelelni akaró katona számára – legyen az tiszt, tiszthelyettes, szerződéses, vagy sorállományú – elengedhetetlenül fontos, hogy az informatika terén is rendelkezzen a megfelelő szintű ismeretekkel. Úgy vélem nem szorul különösebb magyarázatra, hogy a szervezet számára miért fontos az informatika minél szélesebb körben való alkalmazása. A Magyar Honvédség hosszú távú fejlesztési programjának is egyik eleme az informatikai rendszerek fejlesztése és bővítése. Ezen a téren sem elég azonban a technikai fejlesztések végrehajtása, kiemelten fontos a korszerű eszközöket megfelelő hatékonysággal kezelni képes személyi állomány felkészítése. A tapasztalatok azt mutatják, hogy sajnos jócskán van mit pótolnunk a képzettség terén, azonban biztató jel, hogy az érdeklődés és a fogadókészség a személyi állomány részéről nem hiányzik.

2001.év augusztusában a MK Miniszterelnöki Hivatala a Magyar Honvédség tizenegy alakulata részére biztosította számítástechnikai oktató kabinetek kialakítását. A kiépített kabinetek, alakulatonként egy vagy két tanteremben elhelyezve, komplett számítástechnikai rendszert foglalnak magukba: egy darab szerverrel és harminckettő darab munkaállomással *(1.sz. ábra).* A rendszerhez tartozik továbbá egy nagy teljesítményű színes tintasugaras nyomtató, egy lapolvasó, egy HP notebook és egy projector. Valamennyi munkaállomás Hp Vectra típusú számítógép, Windows 2000 Professional operációs rendszerrel telepítve.

Géptípus	Darabszám	Processzor / Mhz	Memória	HDD
HP Netserver	**1**	**P III / 933**	**512 Mb**	**40Gb**
HP Vectra	**4**	**P III / 933**	**256 Mb**	**20 Gb**
HP Vectra	**26**	**Celeron / 766**	**128 Mb**	**20 Gb**
HP Omnibook	**1**	**P III / 800**	**128 Mb**	**20 Gb**

1. ábra A rendelkezésre álló számítógépek adatai

A tantermek technikai átadását követően az informatikai alapképzés új kiképzési ágként beépítésre került a MH kiképzési rendszerébe. A képzés

beindításának célja, hogy a katonák – elsősorban a hátrányos helyzetű és számítástechnikai ismeretekkel nem rendelkezők – a sorkatonai szolgálat ideje alatt alapszintű ismereteket szerezzenek a számítógépek kezelése és alkalmazása terén.

A Savaria Kiképző Központban 2001. szeptember hónapban kísérleti jelleggel indítottuk be az informatikai képzést. Az első időszak tapasztalatainak felhasználásával decembertől megkezdődtek a rendszeres foglalkozások a kiadott kiképzési tematika alapján. A számítástechnikai alapismeretek kiképzési ág hat tárgykört foglal magába, mindösszesen 22 óra időtartamban. A kiképző központokban az alapkiképzés időszakában, amely a jelenleg érvényben levő 2+4 hónapos kiképzési és váltási rendnek megfelelően 4 hétig tart és 180 kiképzési órát tartalmaz *(2.sz. ábra),* a számítástechnikai alapismeretek I. tárgykör 1-3. foglalkozásait oktatjuk 3×2 óra időtartamban. A fennmaradó tárgykörök foglalkozásain a katonák, az átcsoportosítást követően az eredeti egységüknél vesznek részt.

KIKÉPZŐ KÖZPONTBAN		EREDETI EGYSÉGNÉL
ALAPKIKÉPZÉS	SZAKALAPOZÓ KIKÉPZÉS	KÖTELÉK KIKÉPZÉS
4 HÉT (120 ÓRA) NAPI 6 ÓRA KIKÉPZÉS	3 HÉT (120 ÓRA) NAPI 8 ÓRA KIKÉPZÉS	4 HÓNAP

2. ábra A kiképzés rendszere

Az informatikai alapképzés gyakorlati megvalósítása a Savaria Kiképző Központban az alábbiak szerint történik. A bevonulást követően az első kiképzési napon megkezdődik a sorkatonák oktatása. A képzés az alapkiképzés során tantermek 100%-os kihasználtsága mellett folyik. Mivel a kiképző központokban a két hónapos bevonultatási rendnek megfelelően alkalmanként 1500-2000 kiképzendő katona teljesít szolgálatot, a kialakított oktató kabinetek kapacitása egyidejűleg 30 fő részére teszi lehetővé az oktatást és az alapkiképzés időszakában naponta 6 kiképzési óra tervezhető, ezért a rendelkezésre álló idő nem teszi lehetővé valamennyi tárgykör ezen időszakban történő oktatását. A tervezés során igazodva a többi kiképzési ághoz, az alegységparancsnokok úgynevezett báziselosztási tervben kapják meg, hogy az adott alegység mely napokon vesz részt informatikai képzésen. A tantermek kialakításának megfelelően általában szakasz kötelékben történik az oktatás. Azon szakaszok részére amelyek az alapkiképzés során csak az I. tárgykör 1-2. foglalkozásain vettek részt, a szakalapozó képzés idejére tervezzük a 3. foglalkozást.

Az első foglalkozáson az oktatók felmérik a kiképzendő állományt az informatikai ismeretek szintjéről. A tapasztalatok szerint rendkívül nagy az eltérés a kiképzendők körében. Nagyon sok katona itt találkozik először számítógéppel – ez leginkább az általános felkészítésű kiképző zászlóalj alegységeire jellemző – és természetesen előfordulnak felsőfokú informatikai képzettséggel rendelkező katonák is, első sorban a híradó kiképző zászlóalj kötelékében. Ilyen körülmények között nehéz úgy oktatást tartani, hogy az is megértse

az elhangzottakat, aki életében először ül számítógép elé és az se érezze elfecsérelt időnek az oktatást, aki már rendelkezik bizonyos fokú előképzettséggel. Célravezető megoldás az ilyen katonák bevonása az oktatásba oly módon, hogy a gyakorlati foglalkozások során segítenek azoknak a társaiknak, akiknek az alapműveletek végrehajtása nehézséget okoz. Ezzel a módszerrel elfoglaltságot kapnak azok is, akik egyébként unalmasnak tartanák a foglalkozásokat és az oktató is lendületesebben tud haladni a tananyaggal, ha nem kell minduntalan megállni és valamely katonának személyesen megmutatni a helyes műveletet. Itt kell megjegyeznem, hogy a kiképzési programban rendelkezésre álló idő egyébként is szűkre szabott. A 3×2 óra idő alatt sajnos csak alapszintű ismeretek elsajátítására van lehetőség még a legintenzívebb foglalkozásvezetés mellett is.

Az informatikai alapképzés I. tárgykör 1. foglalkozása a „Számítógép típusok”, elméleti foglalkozás. A foglalkozásvezetők a rendelkezésre álló projector segítségével Power Point vetítés keretében oktatják a számítógépek felépítését, részeit és működési elvét. A 2. és 3. foglalkozások már gyakorlati jellegűek. Ezeken a foglalkozásokon sajátítják el a kiképzendők a számítógép be- és kikapcsolásának helyes sorrendjét, megismerkednek az operációs rendszerrel, annak felépítésével és működésével, valamint megtanulják az alapvető fájlkezelési műveleteket. A kialakult gyakorlatnak megfelelően az oktatók a tanári gép képét kivetítik a teremben és így a katonák folyamatosan figyelemmel kísérhetik, hogy az adott feladatot hogyan kell végrehajtani. Ezzel a módszerrel gyorsabb és eredményesebb a meghatározott műveletek elsajátítása. A kiképző központban az I. tárgykör oktatása, a 3. foglalkozás keretében felméréssel zárul. A kiképzendők az oktatói csoport által a tananyag alapján összeállított tesztet töltenek ki. A dolgozatok kiértékelése segítséget nyújt a későbbiekben az oktatói csoport részére, hogy melyek azok a területek amelyekre az oktatás során nagyobb hangsúlyt kell fektetni. Jelenleg a tesztek kitöltése és kiértékelése papíron történik. Az oktató kabinetben ugyan rendelkezésre áll a Phoenix 2 oktatói program amely lehetővé tenné az elektronikus úton történő vizsgáztatást és értékelést, azonban a telepítést végző vállalat még nem végezte el az összes beállítást így a programot jelenleg a képzésben nem tudjuk felhasználni.

A sorállomány informatikai alapképzése mellett az oktató kabinetek számos más felhasználási lehetőséggel rendelkeznek. Mint azt a bevezetőben említettem, fontos hogy a hivatásos és szerződéses állomány is kellő ismereteket és jártasságot szerezzen a számítástechnika terén. A tervek szerint sorállomány létszámának fokozatos csökkentésével párhuzamosan növekedni fog a szerződéses katonák aránya. A Savaria Kiképző Központban jelenleg is folyik a Magyar Honvédség különböző alakulataihoz bevonult szerződéses katonák emelt szintű alap és szakalapozó kiképzése. Jelenleg ezen állomány részére még nincs beépítve a kiképzési programba az informatikai képzés, azonban

úgy vélem, hogy a jelenlegi sorkatonák képzéséhez hasonlóan meg kellene kezdeni a szerződéses katonák informatikai képzését is. A jelenlegi kiképzendő létszám mellett természetesen ez csak a szakalapozó képzés időtartamában, vagy pedig délutáni foglalkozások keretében képzelhető el, azonban a sorállomány csökkenésével a tanterem kapacitás növekedése is nagyobb mozgásteret fog engedélyezni a képzés tervezésében.

A kiképző központ hivatásos állománya részére 2002 február hónaptól ECDL tanfolyamot szerveztünk. Két csoportban harminc fő vehetett részt a foglalkozásokon heti két alkalommal délutánonként, s ebből a harminc főből a tanfolyam végén huszonöten tettek eredményes vizsgát. Örvendetes, hogy a hivatásos állomány körében nagy az érdeklődés a számítástechnikai ismeretek iránt, így tervezzük további tanfolyamok szervezését is. Évente két tanfolyammal tervezve, 2-3 éven belül az állomány nagy részének biztosítható a szükséges informatikai ismeretek megszerzése.

Végezetül, de nem utolsó sorban említem az informatikai szaktantermek lehetőségeit az internet megismertetése és használata terén. A felmérések alapján valamennyi állománykategória körében ez lenne az egyik legnépszerűbb felhasználási terület. Sajnos az internet hozzáférés megteremtése terén komolyabb eredményeket nem sikerült mindezidáig elérni, pedig a számítástechnika alkalmazásának ez a rendkívül látványosan fejlődő területe már ma is kiemelkedő jelentőségű.

TOMKÓ József

FALCON II. -MINT A SZÁRAZFÖLDI CSAPATOK HÍRADÁSÁNAK ALAPJA

HARRIS

Falcon II.™ - mint a szárazföldi csapatok híradásának alapja

HARRIS

Áttekintés

HARRIS

- A Falcon II termékcsalád sikere
- A termékcsalád előnye
- Röviden mindegyik Falcon II rádióról
  - fejlett funkciók
  - a jövő
- Befejezés

A FALCON™ II sikere

HARRIS

- A Falcon II lett a taktikai rádiók legfontosabb családja
- Hagyományosan uralja a HF piacot
- A „U.K. Bowman” ajánlat alapját képezi
  - Hamarosan U.S. Army szabvánnyá válhat (IBCT)
- A Harris előnye 1.6 - 512 MHz sávban
  - A Harris JTRS manpack kiindulópontja

U.S. Interim Brigade Combat Team (IBCT)

HARRIS

- Harris szállíthatta a HF rádiókat az Interim Brigade Combat Team (IBCT) számára
  - A Rockwell Collins-szal szemben lett kiválasztva
  - Az első 10 Brigád már hadrendbe állítva
  - A U.S. hadseregének FBCB2 rendszerével bizonyítottan együttműködőképes
- A HF rádió kulcsfontosságú a U.S. Army jövője szempontjából
  - Nagyobb operatív területet biztosít
  - Összeköti a kisebb, szétszórt egységeket
  - Folyamatos helyzetjelentés a kisebb csapategységeknél
  - A JTRS programra is átterjed

FALCON™ II sikerek

HARRIS

Algéria	Macedónia
Brunei	Németország
Bulgária	Lengyelország
Dánia	Szlovákia
Lettország	Törökország
Litvánia	U.K.
Hollandia	U.S.
Új-Zéland	Egy. Arab Emirátusok
Románia	Üzbegisztán
Singapur	**Magyarország (Falcon I)**
Spanyol Marinák	

FALCON™ II termékcsalád

HARRIS

FALCON™ II termékcsalád

HARRIS

- HF hordozható

- VHF hordozható

- VHF kézi rádió NEW!

- UHF hordozható NEW!

- Többsávos hordozható

- Többsávos kézirádió NEW!

A termékcsalád előnyei

HARRIS

- Egy szállító
  - a felhasználó teljes taktikai rádió igényét kiszolgáló megoldást kínál
  - leegyszerűsíti a képzési és logisztikai feladatokat
- Együttműködő-képesség
  - Titkosított és nyílt adat és beszéd együttműködő-képesség a termékcsaládok tagjai között
- Kiterjesztett frekvencia sávok
  - A feladat végrehajtásához szükséges rádiók száma csökken
  - Megkönnyíti az együttműködést

A termékcsalád előnyei

A termékcsalád előnyei

Programozhatóság

- Második generációs programozható rádió
  software defined radio (SDR)

- Adat vagy Ethernet porton keresztül feljavítható (upgrade)
  - Megnövekedett élettartam
  - "Biztos vásárlás"
  - Az igények változásával a kezdeti olcsó, egyszerű készülék feljavítható

- Csökkentett élettartam-költségek

FALCON™ II taktikai rádiók

HARRIS

FALCON™ II termékcsalád

HARRIS

RF-5800H HF Hordozható

Megnövelt híradástechnikai megbízhatóság.

Mindenáron.

Fejlett funkciók:
- ***9600 bps modem (MIL-STD-110B)*** *
- ***UTM formátum GPS számára*** *
- Nagyobb frekvencia-tartomány (1.6 to 60 MHz)
- Digitális titkosítás (Citadel)
- Felhasználói egyedi titkosítás (Citadel)
- Beépített GPS
- ALE a MIL-STD-188-141A szerint
- LPC600 & LPC2400 digitális hangminőség
- Digitális alapú ECCM (vs. analog)
- Software továbbfejlesztési lehetőség

1. típusú titkosítás:
-AN/PRC-150(C)

A jövő:
- Magasabbszintű digitális hangminőség (MELP)
- ***STANAG 4538 ALE!!!***
- Következő generációs LPI/LPD
- Hálózat

****Új funkció***

Falcon I Radios in HHDF

HARRIS

AN/PRC-138 / RF-5200

Együttműködik a RF-5800H modellel

- Szabványosított világszerte
  - Több mint 13,000 egység rendszerbe állítva
  - Több mint 50 egység HHDF
- Fejlett belső funkciók
  - MIL-STD ALE (MIL-STD-188-141A)
  - Nagysebességű modem (2400 bps)
  - ECCM
- Számos rendszerkonfiguráció
  - 20 W ... 1 kW
  - Manpack, gépjármű, hordozható és bázisállomás modellek
  - Titkosítás
  - LPC-10 digitális hang

RF-5800H Rendszerkonfigurációk

HARRIS

Hordozható

- Max. mozgathatóság
- Nagytávolságú felderítés
- Fedett működés
- 20 Watt

Fix/Hordozható

- Főhadiszállás
- Komm. bunkerek
- Gyors hadrafoghatóság
- Hajófedélzet
- 20, 125, 150, 400 W rendszerek

Gépjármű

- Páncélozott rendszerek
- Puhakerekű járművek
- Repülőgépek
- 20, 125, 150, 400 W rendszerek

FALCON™ II termékcsalád

HARRIS

RF-5800V VHF Hordozható

Gyorsabban,messzebbre.

Kisebb és teljesen titkosított.

Fejlett funkciók:
- ***300 ugrás másodpercenként ECCM ****
- ***UTM formátum GPS számára ****
- Nagyobb frekvencia-tartomány (30 to 108 MHz)
- Digitális titkosítás (Citadel)
- Felhasználói egyedi titkosítás (Citadel)
- Beépített GPS
- 64 kbps modem
-Software továbbfejlesztési lehetőség

A jövő:
- GPS pozíció küldése
- Vezetéknélküli másolhatóság
- Hálózat

** Új funkciók*

FALCON™ II termékcsalád

HARRIS

RF-5800V-HH kézirádió

NEW!

Megbízható és biztonságos taktikai hírközlés egy kis, strapabíró kézirádióval

Fejlett funkciók:
- Digitális titkosítás (Citadel)
- ECCM szabvány (100 ugrás/sec.)
- Együttműködő képesség a HF, VHF és többsávos manpack egységekkel nyílt és titkosított módban is
- Együttműködő képesség a VHF és többsávos egységekkel frekvenciaugrás módban (100 ugrás/sec.)
- Digitális hang és adat mód (16 kbps)
- Nagy teljesítmény (5 W)
- Vezetéknélküli másolhatóság
- Nagyobb frekvencia-tartomány (30 to 108 MHz)
- Software továbbfejlesztési lehetőség

A jövő:
- 300 ugrás/sec. ECCM
- Hálózat

Elérhetőség:
- már rendelhető

FALCON™ II termékcsalád

HARRIS

NEW!

RF-5800U-MP UHF Hordozható

Kiemelkedő fontosságú Föld-Lég rádió

Fejlett funkciók:
- VHF és UHF folyamatos fedés: 90 - 420 MHz
- 5 kHz, 8.33 kHz, 12.5 kHz és 25 kHz csatornaraszter minden szabványt kielégít
- Többsávos scan és átjátszás (digitális/analog fordítás)
- Felhasználói egyedi titkosítás (Citadel)
- Beépített GPS
- 50W gépjármű-csatlakozóval
- Software továbbfejlesztési lehetőség

Elérhetőség:
– már rendelhető

FALCON™ II termékcsalád

HARRIS

RF-5800M-MP Többsávos Hordozható

Egy Rádió,
Többsávú
Többcélú

Fejlett funkciók:
- ***Vezetéknélküli másolhatóság*** *
- ***50W gépjármű-csatlakozóval*** *
- 30 - 512 MHz folyamatos sávátfogás
- Titkosított sávközti átjátszás
- Felhasználói egyedi titkosítás (Citadel)
- Beépített GPS
- 64 kbps nagysebességű adat
- Quicklook 1A ECCM
- Software továbbfejlesztési lehetőség

1. típusú titkosítás:
- U.S. Nomenclature: AN/PRC-117F(C)

A jövő:
- Hálózat
- Havequick II ECCM

*** Új funkciók***

FALCON™ II termékcsalád

HARRIS

NEW!

RF-5800M-HH Kézirádió

Fejlett funkciók:
- 30 - 512 MHz sávátfogás egy kis csomagban
- 0.1 - 5 W teljesítmény
- Citadel™ titkosítás
- 100 programozható csatorna
- Digitális beszéd és adat átvitel
- Együttműködő képesség a Falcon II termékcsaláddal titkosított és frek.ugrásos üzemmódokban is
- Quicklook 1A ECCM

Elérhetőség:
- 2001 Decemberétől

Az elérhető legfejlettebb

többsávú kézirádió

Vezetéknélküli üzenettovábbítás

HARRIS

Vezetéknélküli e-mail

HARRIS

- Software alkalmazások
  - Windows NT és 2000
  - automatikus e-mail továbbítás többféle médián ke
  - interface TCP/IP LAN és RF rádió között
  - nagyteljesítményű protokol a Harris rádiókhoz
  - ***STANAG 5066 megfelelő !!!***

- Szokásos PC hardwaren fut
- HF, VHF, UHF, telefon, INMARSAT kapcsolatok
- Két termék
  - Szerver: RF-6750W - LAN interface
  - Kliens: RF-6710W - végpont

Harris Általános Képátviteli Rendszer (HUITS)

HARRIS

Harris Universal Imaging Transmission System (HUITS)

HUITS képernyő

Micro Videokép Terminal (MVIT)

- Nagyfelbontású színes képek begyűjtése, átvitele, feldolgozása
- Hibamentes átvitel rádión
- Optimalizált protokol a kis sávszélességű átvitelhez
- Windows NT/2000

Összefoglalás

HARRIS

Falcon II *termékcsalád*

- Taktikai rádiócsalád teljes skálája
- A piac kipróbált, megbízható vezetője
- Software alapú, a jövőbeni fejlődést támogató

a 21. századi taktikai kommunikáció eszköze

HARRIS

Dr. habil SÁNDOR Miklós, GYARMATI Tamás

TÁVKÖZLÉSI SZOLGÁLTATÁSOK A SZOLGÁLTATÓ SZEMSZÖGÉBŐL

Az elmúlt időszakban közhellyé vált, hogy hamarosan elérkezik az információs társadalom kora. Ennek már a mindennapi életben is kezdenek mutatkozni az eredményei. Banki szolgáltatások egész sora érhető el telefonon, értéknövelt kommunikációs szolgáltatások széles választéka várja a fizetőképes keresletet, és egy világméretű számítógépes hálózat lassan itthon is bárki számára elérhetővé válik.

A nagy gyártók nem beszélnek többé számítástechnikáról, csupán informatikáról, ami jelzi, hogy többé nem számítógépekben, hanem információban kell gondolkozni. Egyre több területen hódítanak az elosztott rendszerek, mind az információ tárolásában, mind feldolgozásában. Ezzel egy időben a globális informatikai infrastruktúra - egy világméretű integrált hálózat- elérhető közelségbe került. Mindezek a változások elsősorban a hálózatok fejlődését vonták, vonják maguk után. Ennek megfelelően az informatika területén a számítógépes- és kommunikációs hálózatok válnak központi fontosságúvá.

A számítógépes hálózatok tervezésekor, megvalósításakor a legnagyobb probléma a különálló helyi hálózatok egymással, ill. az Internettel való összekapcsolása. Manapság már a kis gazdálkodó szervezetek és a magánvállalkozók számára is elérhető árkategóriába került az ISDN, ami kézenfekvő megoldást kínál a fenti probléma megoldására. Számítógéphálózatok ISDN-en keresztüli összekapcsolásához mindössze ISDN routerekre van szükség.

A távközlési szolgáltatók jelenleg egy másik szolgáltatást is ajánlanak az Internetre való kapcsolódáshoz, az ADSL-t. Ezzel azokat a felhasználókat célozzák meg, akik állandó kapcsolatot igényelnek, és több időt töltenek az információszerzéssel. Ez esetben a szolgáltató szintén egy routert helyez el a felhasználónál.

Több telephelyes szervezeteknél az egyes egységek közötti kapcsolat kialakítása a feladat. Sok esetben a felhasználó, pl. a Magyar Honvédség maga is rendelkezik egy elkülönült távközlő hálózattal, melynek a többi hálózatokkal való összekapcsolása a feladat. A Magyar Honvédség minden távközlési vállalat számára kiemelt ügyfélnek számít, így különleges elbírálásban részesül.

A konvergencia hatása a távközlési piac szereplőire

Tehát az információs társadalom egyre inkább realitássá válik. Fejlődését az a gyors technológiai változás táplálja, amely az információs iparágakat is

átalakítja. Ennek az átalakulásnak a jellege és sebessége új kihívásokat jelenthet a döntéshozók számára.

Az egyik legjelentősebb tényező az ugyanazon technológiáknak a különböző - nevezetesen a távközlési, a média és az információ-technológiai (IT) - szektorok általi egyre nagyobb mértékű alkalmazása. E konvergencia bizonyítéka az elmúlt években csak megerősödött az Internet térhódításával és azzal, hogy a meglévő hálózatok egyre nagyobb mértékben képesek a távközlési és műsorszóró szolgáltatások továbbítására.

A konvergencia jelensége viszonylag új keletű és számos eltérő álláspont alakult ki arra nézve, hogy mik a konvergencia vonatkozásai a társadalom és a gazdasági tevékenység tekintetében. Széles körben elfogadott, hogy a digitális elektronika és a szoftver területén elért fejlesztések megteremtik a technológiai potenciált az információs szolgáltatások nyújtásával és felhasználásával kapcsolatos új megközelítés számára. Már kevésbé egyeznek a vélemények arra nézve, hogy ezek a fejlesztések milyen mértékben változtatják meg a jelenlegi gyakorlatokat és milyen időn belül. A konvergencia a meglévő távközlési, média és információ-technológiai szolgáltatások teljes és gyors átalakulásához vezet olymódon, hogy ezek a jelenleg elkülönült szolgáltatási csoportok egymásba olvadnak, lényegében elmosva a korábban köztük fennálló világos megkülönböztetéseket.

A jelenleg elkülönült szektorok specifikus jellege korlátozza a szolgáltatási konvegencia terjedelmét, és a médiaszakma - a társadalmon belüli társadalmi, kulturális és erkölcsi értékek hordozójaként - szerepe független a fogyasztók elérése érdekében alapul szolgáló technológiától. Ez azt jelentené, hogy a gazdasági feltételeknek, valamint az információs szolgáltatások tartalmának szabályozását el kellene különíteni a hatékonyság és a minőség biztosítása érdekében. Az új szolgáltatások kialakulásától és a jelenlegi szolgáltatások fejlődésétől az átfogó információs piac bővülését várják. Mindez új lehetőségeket biztosít a gazdasági növekedés és a foglalkoztatás számára. Ugyanakkor az új kommunikációs szolgáltatási környezet lehetőségeket biztosít az európai polgárok életminőségének javításához azáltal, hogy bővíti a fogyasztói választékot, hogy lehetővé teszi a hozzáférést az információs társadalom által kínált előnyökhöz, és hogy elősegíti a kulturális sokféleséget.

Ezek a fejlemények tehát pozitívak Európa gazdasági és társadalmi fejlődése számára, és ezeket ezért ösztönözni kell.

A termékfejlesztés külső és belső okai

A távközlési szolgáltatók figyelembe véve tevékenységüket, ezáltal kényszeríve vannak az újabb termékek és megoldások kifejlesztésére.

Belső kényszer a tulajdonosi elvárásoknak való megfelelés, mely a pénzügyi mutatókban, a vállalat részvényeinek változásában nyilvánul meg. A tőzsdén lévő vállalatok állandó megfigyelésével a pénzügyi elemzők gerjesztik

a fejlődést, ösztönözve a résztvevőket az állandó megújulásra, fejlesztésre, és a távközlési piac tortájából minél nagyobb szelet kihasítására.

Külső kényszer a vállalatok számára a versenytársak megjelenése a különböző új piacokon. Magyarországon példa erre az IP hálózatok kialakítása, mely során a Pantel előnyt szerzett a Matávval szemben.

A termékfejlesztés során meg kell határozni a célpiacot mely várhatóan a fejlesztés lezárása után is igényt tart a szolgáltatásra.

A fejlesztési projekt indításakor egy projekt terv készül, amelyben meg kell határozni a következőket:

- A fejlesztés kapcsolata a vállalati szintű stratégiájával,
- műszaki tartalom,
- a szolgáltatások területi kiterjesztése,
- bevezetés ütemezése,
- kapcsolat a meglévő projektekkel, főbb hatások,
- pénzügyi elemzés,
- kockázatelemzés,
- megvalósítás javasolt lépései és ütemezésük.

Az elkészült fejlesztési tervet alapul véve egy döntés születik, a folyamat indításáról, a felelősök meghatározásáról, és a költségek és erőforrások allokálásáról. A megvalósítás során folyamatosan figyelni és tartani kell az előzőekben meghatározott időütemezést és a költségeket.

A fejlesztésben részt vesznek a vállalat különböző területeiről érkezett megbízottak. Ezekből különböző alteamek létesülnek, melyek: műszaki, szolgáltatási, oktatási, stb.

Az egyes alteamek elkészítik a fejlesztési projektből levezetve a saját projekt ütemezésüket igazodva a fő időpontokhoz.

Ha a fejlesztés külső beszállítókat igényel, akkor az azokkal való kapcsolattartást is meg kell szervezni, adott esetben tendert kell kiírni.

Ezzel egyidejűleg a szolgáltatás nyújtásában résztvevőket képzésben kell részesíteni, hogy mire a barátságos teszt elindul, mindenki tudja mi a folyamat és abban mi a feladata. A szolgáltatás végső kialakításához fel kell használni a teszt alatt összegyűlt tapasztalatokat is.

A komplex megoldás elengedhetetlen feltétele az ügyféllel való kommunikáció. Ebben nagy szerepe van az ügyfélmenedzsereknek és a kommunikációs terv elkészítőinek. A termék piacra vitelét már a végső kialakítás előtt meg kell kezdeni reklámokkal, road-show szervezésével, és a különböző médiában való megjelenéssel.

Ha a szolgáltatásnak egyetlen felhasználója van, akkor a megoldás egyedi, ilyenformán a különböző kommunikációs csatornák felhasználása is személyre szabott.

Különleges szempontok a nemzetvédelem számára nyújtott távközlési megoldásoknál:

A nemzetvédelem területén egyre bonyolultabb és nagy kiterjedésű informatikai rendszerek alakulnak ki. Az intézmények tevékenységét és működését mind intenzívebben támogatják informatikai alkalmazások. Ezzel együtt emelkedik az informatikai biztonság szerepe és jelentősége.

Az informatikai biztonságpolitika, stratégia, a biztonsági vizsgálatok és a védelmi intézkedések viszonylatában.

A megvalósítás középpontjában a védendő alapérték, amely esetünkben az adatok által hordozott információ áll, amelyet az érték környezetét alkotó rendszerelemek vesznek körül. Általában a támadások a rendszerelemekre hatnak közvetlenül és az ezeken megvalósított védelem által realizált védelmi képességektől függően veszélyetetett a védendő érték. A megvalósított védelemnek zártnak, teljes körűnek, a kockázatokkal arányosnak és időben folyamatosan biztosítottnak kell lennie.

Egy szervezetnél az informatikai biztonsági rendszer kialakításának kezdeti fázisában kialakítandó meg kell fogalmazni a szervezet és az informatikai biztonság viszonyának elveit, valamint védelmi rendszerre vonatkozó jövőképet és ki kell alakítani annak megvalósítási útját leíró biztonsági stratégiát. Ezen dokumentumok képezik a kiindulási alapot a későbbiekben a fizikai, a logikai és az adminisztratív védelmi rendszer tervezésének és megvalósításának.

A konkrét fenyegetéseket általánosabban megfogalmazó alapfenyegetések:

- a bizalmasság elvesztése,
- a sértetlenség elvesztése,
- a hitelesség elvesztése,
- a rendelkezésre állás elvesztése,
- a funkcionalitás elvesztése.

Ezek elhárítása az általános védelmi célokként értelmezendő.

Az alapfenyegetések figyelembe vételével az informatikai biztonsági követelmények felállítása két alapterületen történt meg, az informatikai rendszerek információvédelme, illetve megbízható működése területein. Az információvédelem alapvetően a bizalmasság, a sértetlenség és a hitelesség elvesztése elleni védelmet, a megbízható működés a rendelkezésre állás és a funkcionalitás elvesztése elleni védelmet foglalja magába.

Egy eklatáns példa ezeknek az elveknek az alkalmazására a központtól távoli telephely kialakítása, mely helyen helyi hálózaton működő terminálok, szerver, behívóhálózat, bérelt és kapcsolt adatvonalak, távbeszélő vonalak, alközpont, Web-es alkalmazások működnek.

BUCSAI Ferenc

AZ MH ŐR- ÉS BIZTOSÍTÓ ZÁSZLÓALJ VEZETÉSÉT BIZTOSÍTÓ KOMMUNIKÁCIÓS TEVÉKENYSÉG

Az MH Őr- és biztosító zászlóalj vezetését biztosító kommunikációs tevékenység

(2001. Január 4. – 2001 július 11.)

Ea: Bucsai Ferenc alezredes MH 62. BM gl.dd.
híradó és informatikai főnők

Amiről beszélni szeretnék:

1. Az ÖBZ megalakulása
2. A zászlóalj alárendeltsége, a parancsnoklás rendje
3. Híradó tevékenység.

A KFOR alegység megalakításának alapja

- **Az Országgyűlés 1999. június 15-i 55/1999. számú határozata, a SZFVKF, és a 3. g. ho. parancsnok intézkedései alapján megkezdődött a KFOR erők felállítása és felkészítése.**

- **Országgyűlési határozat alapján a maximális létszám 350 fő.**

- **A kiképzés végrehajtása Táborfalván 1999. 06. 17 - 1999. 07.14.**

A zászlóalj felkészítése

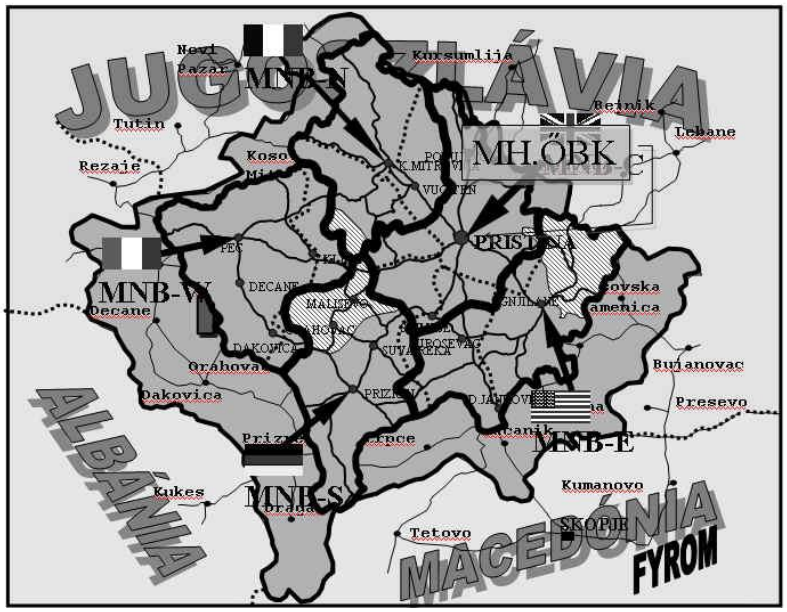
- **- állománytábla kialakítása;**
- **- személyi állomány kiválogatása;**
- **- technikai eszközök és anyagok előkészítése;**

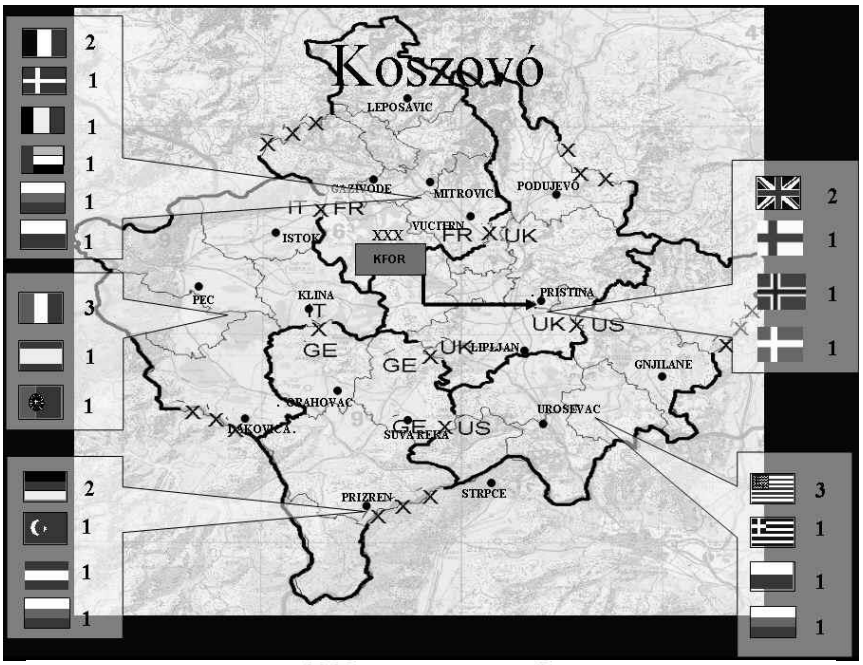
- **Általános felkészítés (minden katona számára)**
  1999.06.17 - 06.24.,
- **Szak- és speciális felkészítés (szakcsoportokban HCOM, R-142):**
  1999.06.25 - 07.06.,
- **Záró gyakorlat végrehajtása**
  1999.07.07 - 07.08.,

Átcsoportosítás

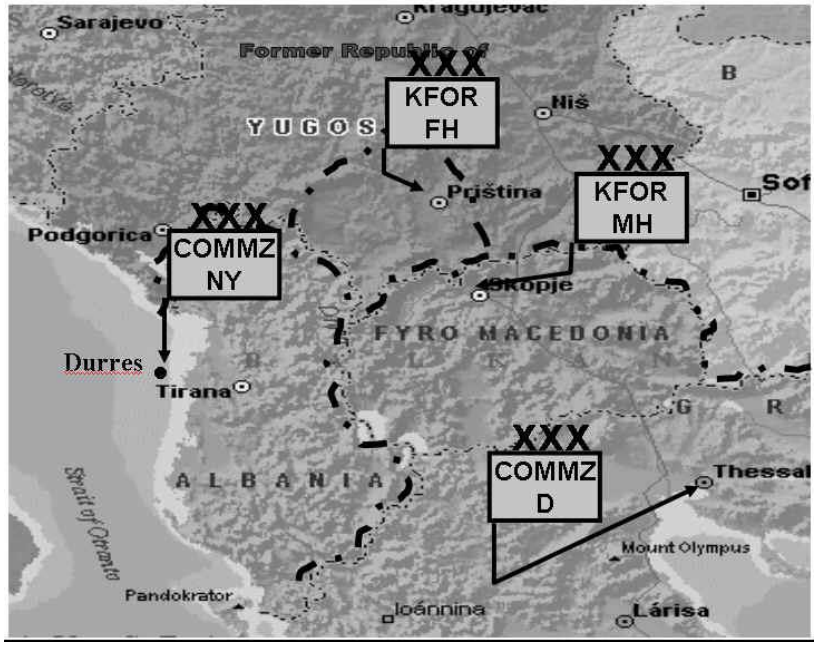
- 5 szerelvény;
- 324 fő;
- 110 db technikai eszköz;
- 830 tonna anyag.
- Átcsoportosítás befejezve 1999.08.02.

Koszovó




Koszovó
LEPOSAVIC
MITROVIC
PODUJEVÓ
VUCITERN
ISTOK
KFOR
PEC
KLINA
PRIŠTINA
GNJILANE
GRAHOVAC
UROSEVAC
DAKOVICA
SUVA REKA
PRIZREN
STRPCE
2
1
1
1
1
1
3
1
1
2
1
1
1
2
1
1
1
3
1
1
1

Koszovó


Sarajevo
Former Republic of
YUGOS
XXX
KFOR
FH
Niš
B
XXX
KFOR
MH
Sof
Priština
XXX
COMMZ
NY
Podgorica
Skopje
FYRO MACEDONIA
Durres
Tirana
XXX
COMMZ
D
ALBANIA
Thessal
Strait of Otranto
Mount Olympus
Pandokrator
Ioánnina
Lárisa

Pristina

A bázis kialakítása

A konténer-tábor kialakítása





Személyi felszerelés


Fő feladatok

Őrzésvédelem

Külső kapu

Fő feladatok

Őrzésvédelem
Főépület

MP asztal

Fő feladatok

Készenlét

Fő feladatok

Bármilyen feladatra alkalmazható az angol szektoron belül.
- **konvojkísérésre,**
- **blokkírozásra,**
- **tömeg oszlatásra,**
- **mobil EÁP feladatra**
- **egyes objektumok őrzés-védelmének megerősítésére.**

Készenléti szakasz

Fő feladatok

Szállítmány-kísérés

Konvoj kísérés
(4 bizt. gépjárműnél több)
Szállítmány kísérés
(4 bizt. gépjárműnél kevesebb)

Fő feladatok

A zászlóalj felépítése

- parancsnokság;
- törzs;
- ÖB alegységek;
- támogató és log. alegységek

A vezetési részleg helye és szerepe

- Közvetlenül a z. TÖF-nek van alárendelve;
- Állománya 2 fő:
  - részleg parancsnok (mb. ESZF);
  - Ügykezelő-gépíró.

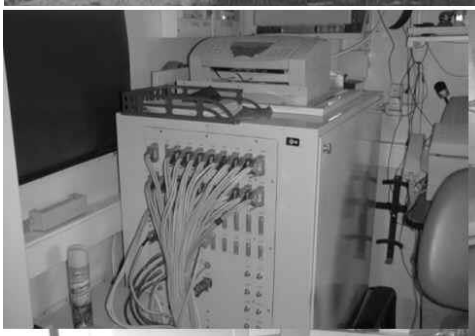
- Rendeltetése:
  - híradó és informatikai feladatok tervezése; szervezése, anyagok nyilvántartása;
  - ügyviteli tevékenység végzése;
  - küldemények továbbítása.

Zászlóalj híradó központ

Összetétele:

- HICOM távbeszélő központ;
- R-142 rádió állomás;
- ELN átjátszó állomás; (MOTOROLA);
- Távbeszélő pont.

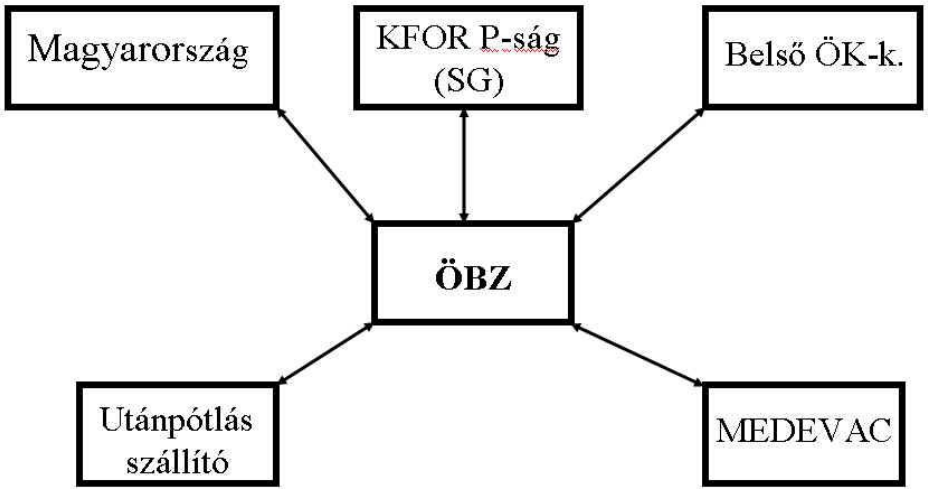
A híradó központ

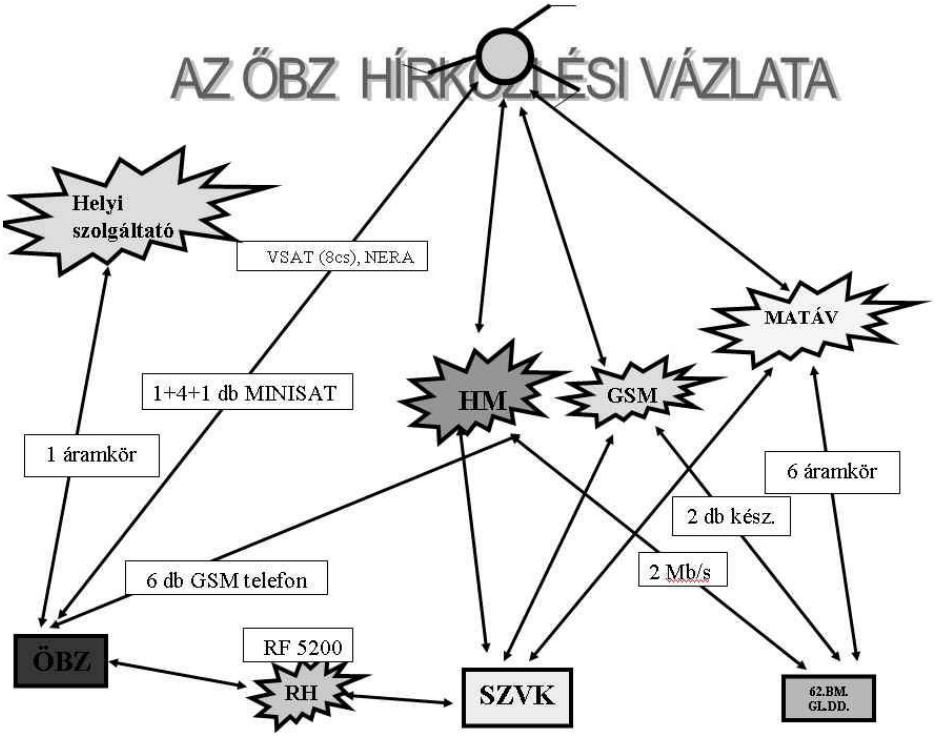


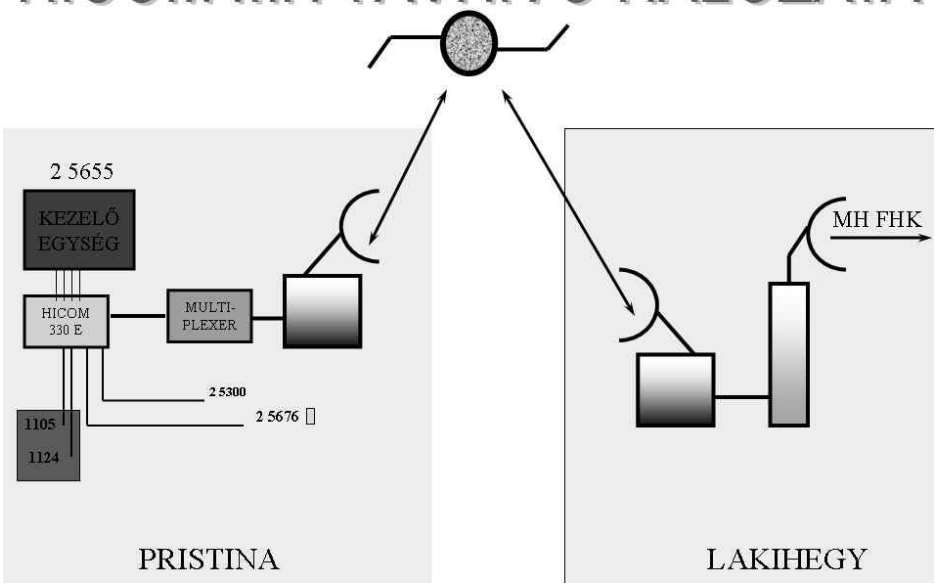
A mobil HICOM

Az ügyeletes központ kezelő

Az üzemelő összeköttetések irányai

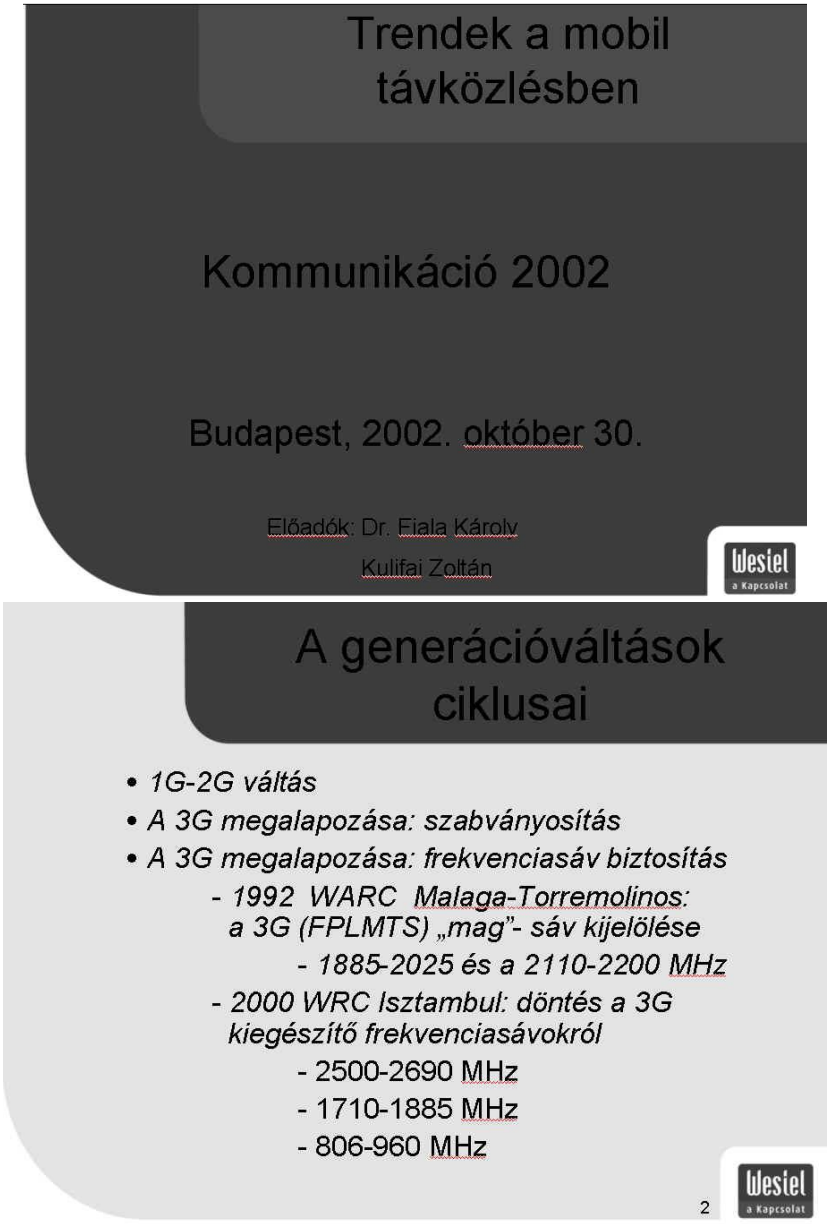



AZ ŐBZ HÍRKÖZLÉSI VÁZLATA
Helyi szolgáltató
VSAT (8cs), NERA
MATÁV
HM
GSM
1+4+1 db MINISAT
1 áramkör
6 áramkör
2 db kész.
2 Mb/s
6 db GSM telefon
RF 5200
ÖBZ
RH
SZVK
62.BM. GL.DD.


HICOM MH TÁVHÍVÓ HÁLÓZATA
2 5655
KEZELŐ EGYSÉG
HICOM 330 E
MULTI-PLEXER
2 5300
2 5676
1105
1124
MH FHK
PRISTINA
LAKIHEGY

Dr. FIALA Károly, KULIFAI Zoltán

TRENDEK A MOBIL TÁVKÖZLÉSBEN



Az eredeti 3G koncepció: revolúció

- **Globalitás**
  - *– globálisan harmonizált frekvenciasáv*
  - *– globálisan elfogadott szabvány*
  - *– globális terminál mobilitás – globális roaming*
  - *– globális ellátottság*
  - *– globális piac a gyártóknak*

3

Az eredeti 3G koncepció: revolúció

- **Új szolgáltatások és képességek**
  - *megnövelt felhasználói adatsebesség*
  - *beszéd (áramkörkapcsolt) + csomagkapcsolt adatátvitel + multimédiás szolgáltatások*
  - *IN alapú szolgáltatás-alkotó környezet és szolgáltatás hordozhatóság*
  - *flexibilis rádiós hordozószolgáltatások*
    - *igény szerinti sávszélesség*
    - *aszimmetrikus adatsebességek*
  - *magas QoS, összemérhető a fix hálózatokéval*
  - *könnyebb kezelhetőség*

4

Az eredeti 3G koncepció: revolúció

- **Sokféle környezetben való alkalmazhatóság**
  - *belvárosi, városi, rurál, és kies környezetek*
  - *fix és mobil felhasználók*
    - *integrált műholdas/földi hálózatok*
    - *adaptív terminálok*
- **Evolúció és migráció**
  - *evolúció a 3G rendszeren belül*
  - *szolgáltatások kompatibilitása a PSTN/ISDN hálózatokéval*
  - *együttműködés (IWF) a 2G hálózatokkal*
  - *nyílt architektúra*

5

Westel a Kapcsolat

Mi lett az eredeti koncepcióból ?

- *1996 :UMTS Task Force jelentés*
- *egy szabvány helyett: IMT- 2000 szabványcsalád*
- *IMT- 2000 : 5 rádió hozzáférési technológia*
- *Internet robbanásszerű fejlődése*
- *műholdas hálózatok kudarca*

6

Westel a Kapcsolat

Az ígéretek és a valóság

- **A beváltott ígéretek**
  - *frekvenciasáv biztosítás: teljes siker az EK országaiban*
  - *szabványosítás: 3GPP példátlan méretű sikeres globális együttműködés*
- **Ami félresikerült a 3G-vel kapcsolatban**
  - *helytelen időzítés, túl korai bevezetési időpont*
  - *felfokozott, túlzott várakozások*
  - *az árverés, mint engedélyeztetési forma kudarca*

7

A jövő mégis a 3G-é

- A fejlődés nem áll meg, a 2,5G-ről idővel szükségszerűen tovább kell lépni valamelyik IMT- 2000 szabványcsaládba tartozó 3 G-technológiára. (A 3G technológiák versenyének győztese várhatóan a UMTS lesz.)
- A 3G egy évtizedre kiterjedő, világméretű munkával létrehozott szilárd alapokon áll, mind a szabványosítás, mind a frekvenciasáv biztosítás területén.
- A 3G elterjedése időben és térben lassan elhúzódó folyamat lesz, ebből adódóan hosszú együttélés várható a 2,5 G technológiákkal.
- A 2,5 G platformon kifejlesztett 3G típusú szolgáltatásokkal és alkalmazásokkal helyre fog állni a technológia és a piac megbomlott egyensúlya a 3G vonatkozásában. Mire a 3G technológia kiforrottá válik, addig a piaci elfogadottsághoz szükséges szolgáltatások és alkalmazások rendelkezésre fognak állni.
- A 3G bevezetése a mobil szektor konszolidációja irányában hat, továbbá új típusú együttműködések kialakulását ösztönzi a komplexebbé váló piac szereplői között.

8

GSM adatkommunikációs felhasználási lehetőségek

- **SMS (Short Message Service)**
- **vonalkapcsolt adatkommunikáció**
  CSD (Circuit Switched Data)
- **csomagkapcsolt adatkommunikáció**
  GPRS (General Packet Radio Service)

9

SMS

- **SMS (Short Message Service)**
  elszórt adatküldés — max 160 karakter,
  nem alkalmas sűrű információváltásra

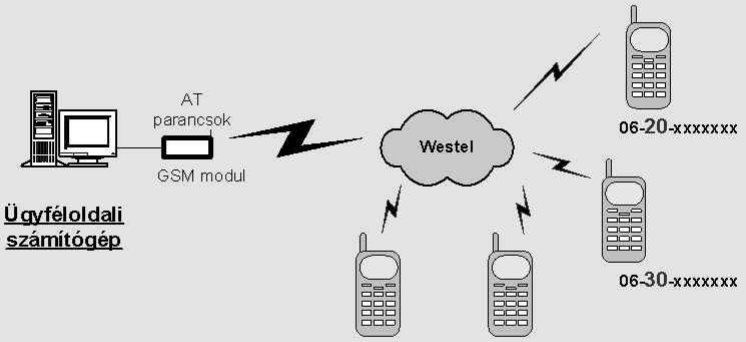
10

SMS felhasználás

- E-mail notifikáció
- jelentés
- vállalati telefonkönyv
- pénzügyi alkalmazások
- gépjárműfigyelés
- adatgyűjtés, távfelügyelet
- folyamatirányítás
- promóció
- rendezvényszervezés

11

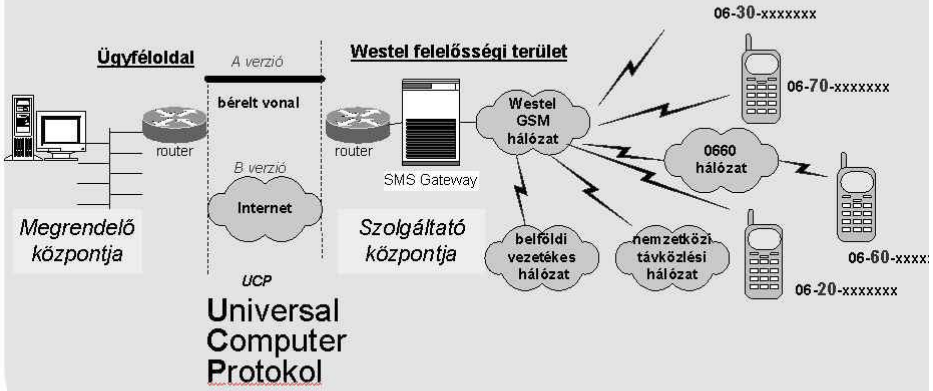
SMS küldés GSM modullal



SIM kártya kapacitása:
720 üzenet/óra

12

TömegesSMS



SMSC teljes kiküldési kapacitás: **280 SMS/ sec**

Rendszerkapacitás ügyfélre nézve: **2000 SMS/óra**

13

CSD

- **SMS (Short Message Service)**
  elszórt adatküldés — max 160 karakter, nem alkalmas sűrű információváltásra
- **vonalkapcsolt adatkommunikáció**
  CSD (Circuit Switched Data)
  folyamatos adatküldés — max 9,6 kbps, 30 sec feljelentkezés

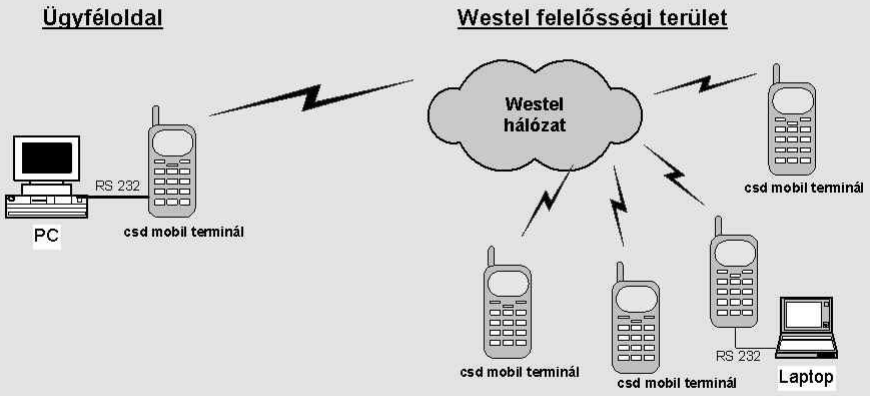
14

CSD felhasználás

- Irodán kívüli vállalati elektronikus levelezés
- információs adatbázis elérése
- Felső vezetői irodai felhasználás
- Távfelügyelet
- Azonosítási-ellenőrzési rendszer felhasználói
- Készlet nyilvántartási rendszer

15

CSD küldés GSM modullal



16

CSD küldés modem pool-on keresztül

17

GPRS

- **SMS (Short Message Service)**
  elszórt adatküldés max 160 karakter,
  nem alkalmas sűrű információváltásra

- **vonalkapcsolt adatkommunikáció**
  CSD (Circuit Switched Data)
  folyamatos adatküldés max 9,6 kbps, 30 sec feljelentkezés

- **csomagkapcsolt adatkommunikáció**
  GPRS (General Packet Radio Service)
  folyamatos és elszórt adatküldés ált. 30/10 kbps, 10 sec feljelentkezés

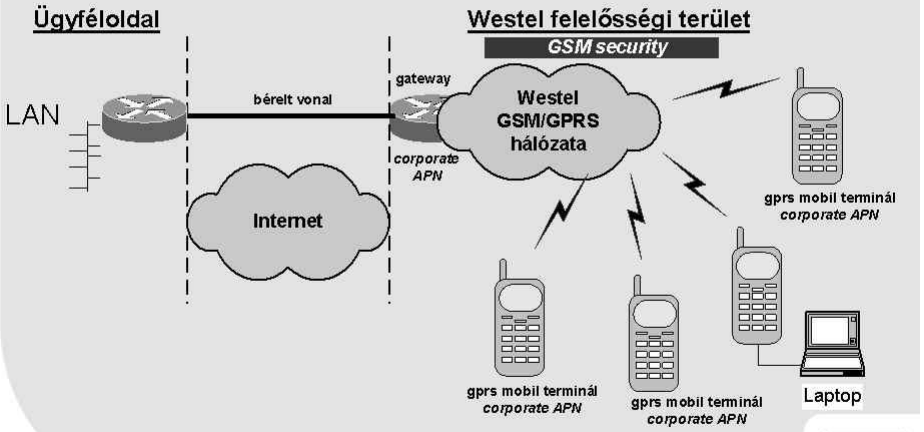
18

GPRS felhasználás

- **Telemetria (always-on és adatmennyiség alapú számla)**
  - gépjárműkövetés
  - vagyonvédelem
  - mérőberendezések adatainak továbbítása
  - fuvarirányítási rendszer (taxitársaságok)
- **office jellegű elérés (gyorsaság)**
  - készletnyilvántartási rendszer
  - belső levelező szerver és belső adatbázis elérése

19

GPRS LAN ACCESS



20

MAGYAR Sándor

A FORGALOMFELÜGYELET JELENTŐSÉGE
A MAGYAR HONVÉDSÉG
HÁLÓZATFELÜGYELETI RENDSZERÉBEN

A FORGALOMFELÜGYELET JELENTŐSÉGE
A MAGYAR HONVÉDSÉG
HÁLÓZATFELÜGYELETI RENDSZERÉBEN

EA: Magyar Sándor

A nemzetközi szabványokra támaszkodva a hálózatfelügyelet következő alrendszereket különíti el:

- hiba (fault) menedzsment;
- teljesítmény (performance) menedzsment;
- nyilvántartás (accounting) menedzsment;
- konfiguráció (configuration) menedzsment;
- biztonsági (security) menedzsment.

A hálózatfelügyelet főbb szükséges elemei:

- Parancsnokság
- Országos Hálózatfelügyelet (hálózati operátorok a nap 24 órájában végzik a felügyeleti tevékenységet)
- Forgalomelemző és díjszámláló részleg
- Szervizrészleg

Forgalomelemzés célja:

- A monitorozással a hálózat teljesítményének (erős, gyenge pontjainak) megismerése.
- A szükséges változtatások megtervezése (útvonaltervezés).
- A teljesítményben előforduló „hibák" kiküszöbölése.
- A rosszul beállított átviteli rendszerek kiszűrése.
- Költség- forgalom optimalizálás, teljesítmény menedzsment.

A kapcsolóközpontok és átviteli utak teljesítményének a hálózatra történő optimatizálása.

Forgalomelemző és díjszámláló részleg :

- Általános forgalmi kimutatásokat készít. A szükséges változtatások megtervezése (útvonaltervezés).
- Adatszolgáltatást nyújt a hálózat tervezéséhez.
- Forgalomelemzésnél folyamatosan figyelemmel kíséri az átvitel beszéd és adat jellegű összetételének arányát. Az beszéd/adat arány kritikus mértékben történő változásánál az hálózati operátorral együttműködve megkezdi a hiba behatárolását.

A következő kimutatások készítése:

- Fővonal csoport rendelkezésre állás grafikon.
- Forgalmas órák grafikonja.
- Idő-terhelés grafikon fővonalra.
- Idő-terhelés grafikon fővonal csoportra.
- Fővonal-terhelés grafikon.
- Fővonal csoport- terhelés grafikon.

Célszerű nyomon követni:

Felhasználók, a „jogosult felhasználók", az átviteli utakat egyidejűleg használók számát.

Költséghatékony útvonalválasztás :

- Az év elejétől érvénybe lépett törvényi háttér (2001.évi XL törvény a Hírközlésről) megengedi a zártcélú hálózatból a közcélú hálózatba történő kilépésnél a LCR alkalmazását. Mivel ez egy hálózati szintű feladat ezért nagy szerep jut a forgalomelemző és díjszámláló résznek.
- A forgalomelemző részlegnek kell (és tudja) megvizsgálni az érintett hálózati átviteli utak és közcélú kilépési útvonalak forgalmi terheltségét. LCR tervezésénél figyelembe kell az átviteli utak terheltségének növekedését.
- A Központosított költségvetés szükségessé válik.
- Díjszámláló részleg feladata megnő.

Következtetések:

- A hálózatfelügyelet egy komplex, együttes tevékenység részei szervesen együttműködnek.
- A hálózatfelügyeletnek a forgalomelemző és díjszámláló része az a szervezeti elem amely javaslatot tesz a hálózat teljesítményének optimalizálására.
- A Magyar Honvédség rendelkezésére álló költségkeretek szükségessé teszik a hálózat saját, bérelt és kapcsolt vonali, sávszélességének racionális kihasználását.
- LCR bevezetése csökkenti a Magyar Honvédség távközlési költségeit.

AGÁRDI Ferenc, ZARÁNDY István

AZ MVM RT. TÁVKÖZLÉS FEJLESZTÉSI PROJEKTJE

MVM MAGYAR VILLAMOS MÜVEK RT.
AZ ÁRAM FORRÁSA

Az MVM Rt. távközlés fejlesztési projektje

előadók:

Agárdi Ferenc	*MVM Rt.*
Zarándy István	*KAPSCH*

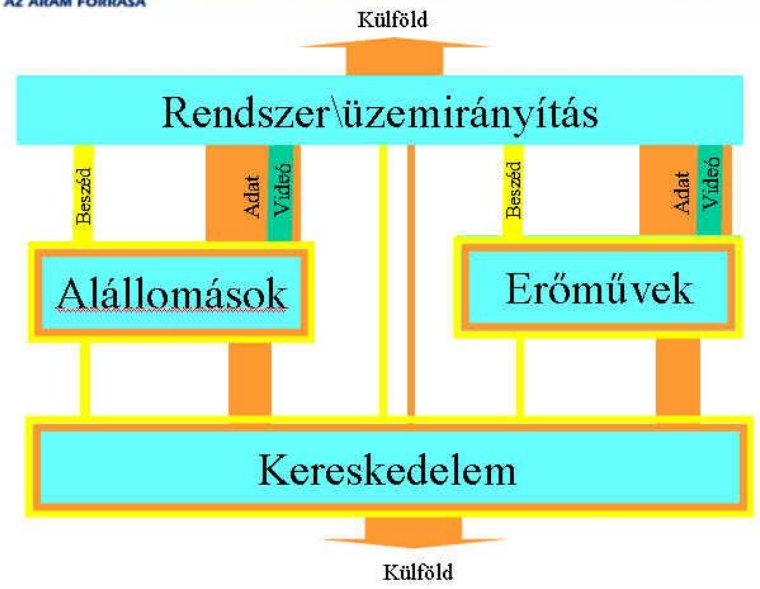
MVM MAGYAR VILLAMOS MÜVEK RT.
AZ ÁRAM FORRÁSA
kapsch >>>

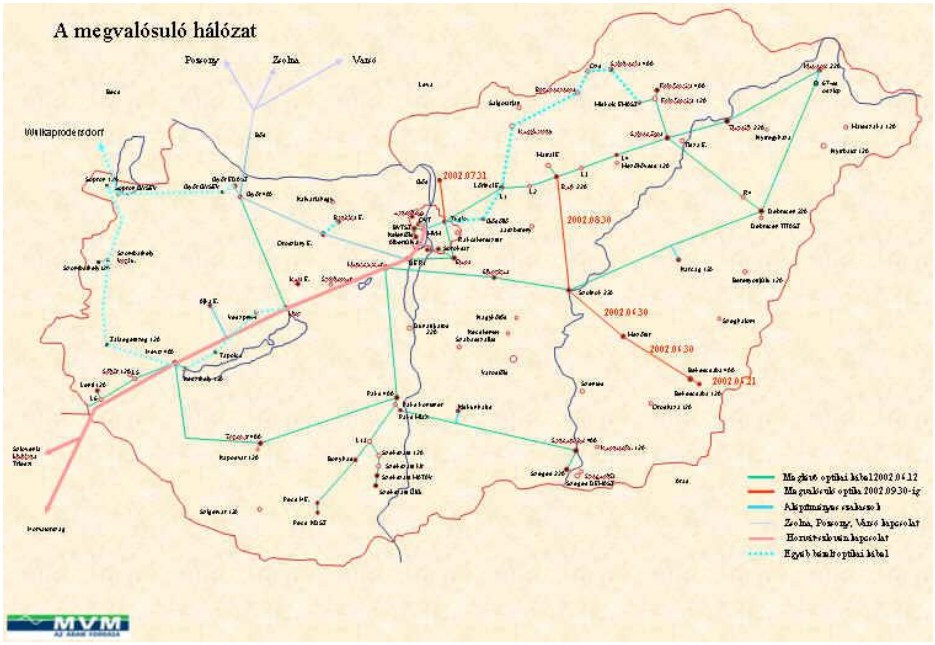
Felhasználói (tulajdonosi) szempontok.
Előzmények, kapcsolódások, üzleti tervek

Műszaki érdekességek

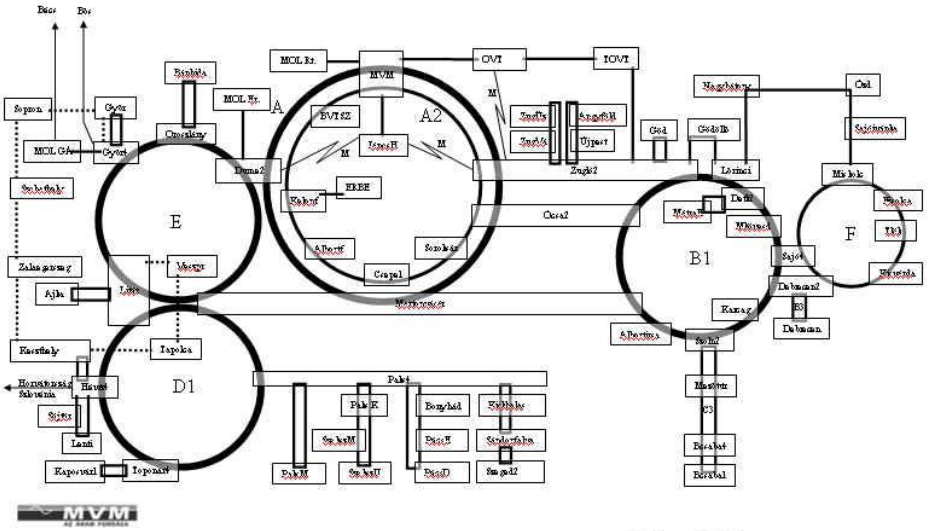
projekt folyamatok

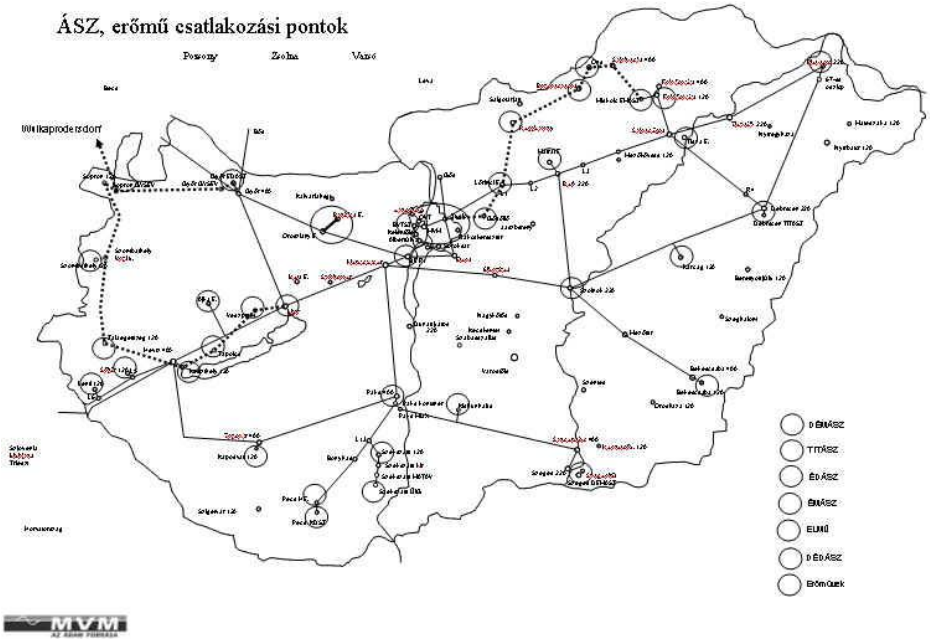
MVM MAGYAR VILLAMOS MÜVEK RT.
AZ ÁRAM FORRÁSA

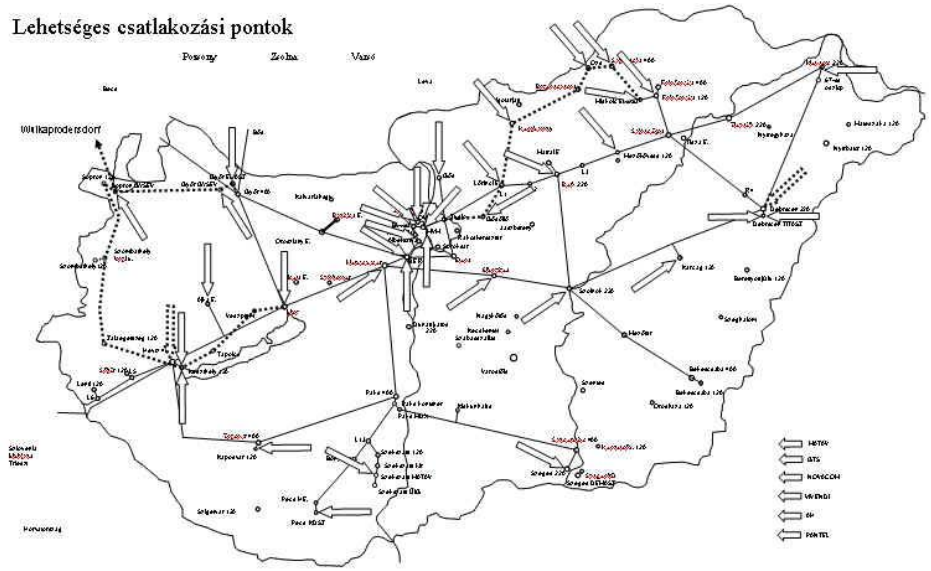




SDH hálózat kialakítása







MVM

kapsch >>>

Összetett műszaki tartalom

- *SDH*
- *DWDM*
- *PDH*
- *Hálózat menedzsment*
- *Védelmi jelátvitel*
- *Helyszínek előkészítése (preinstalláció)*

kapsch >>>

Kulcsrakész

- Hálózat tervezés
- Terület felmérés
- Állomási (installációs) tervezés
- Meglévő hálózatelemek integrálása
- Berendezés szállítás (import + hazai szállítók)
- Installáció
- Üzembehelyezés
- Oktatás/betanítás
- Garancia

kapsch >>>

Projekt felelősség

- Műszaki felelősség
- Határidő felelősség
- Üzembiztonság
- Pénzügyi felelősség
- Illeszkedés az optikai hálózat építéséhez (~1000 km új szakasz)

kapsch >>>

A projekt számokban

- *Gyűrűk száma: 4 x STM16; 10x STM 4; 11x STM1*
- *Állomások száma: 65 db.*
- *2 x Hot stand-by menedzsment állomás*

kapsch >>>

Műszaki tartalom I.

Nortel Optera Metro család

- *TN-1X (és a korábban szállított eszközök)*
- *TN-4XE*
- *TN-16XE*

Nortel DWDM

- *Optera Metro (OM 5200)*

ascom PDH

- *UMUX 1500*
- *FOX-U (korábban üzembe helyezett)*

Védelmi jelátvitel eszközei

- *FOX 515 (Ascom/ABB speciális illesztőkártyával)*

kapsch >>>

Műszaki tartalom II.

Menedzsment eszközök

- Lokális menedzsment hozzáférés
- Két menedzsment helyszín (a felhasználó szervezeti megosztásának megfelelően)
- hot stand-by
- X-terminal (2 x)
- EC-1
- Preside (INM)
- UNEM (UCST helyi hozzáféréshez)

❖ menedzsment kommunikációs hálózat

❖ riasztás kezelés

kapsch >>>

Projekt menedzsment I.

Projekt szervezeti modellek konfliktusa

- Elvárások a Megrendelő részéről (erős projekt gyakorlat és projekt szervezet az MVM-nél)
- Projekt szervezet

→ a Vállalkozónál
→ a Szállító(k)nál
→ az alvállalkozó(k)nál

- Minőségterv > minden résztvevőnél

kapsch >>>

Projekt menedzsment II.

Megrendelő részéről:

- *illeszkedés az optikai hálózat kiépítéséhez> TFP másik projektje*
- *helyszínek biztosítása > idegen tulajdonosok*
- *adatszolgáltatás > felmérések szükségesek*
- *mérnökiroda, szakértők*

Vállalkozó részéről

- *tervszállítás és zsüriztetés*
- *alvállalkozók, alvállalkozók koordinálása*
- *ütemezés, ütemes munka, ütemes fizetés*
- *helyszínfüggő (belépés, késedelem >>>átütemezés)*
- *beszámolók „előrehaladási jelentés"*

Közös döntések

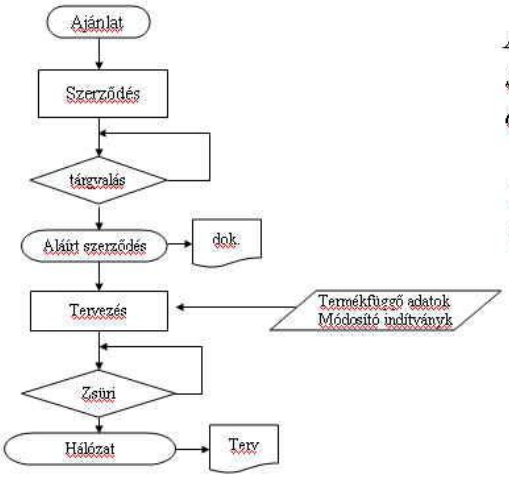
kapsch >>>

Üzembehelyezés, rendelkezésre állási próbák, átvételi vizsgálatok

- *Hideg szereléshez kapcsolódó vizsgálatok (alvállalkozó, dokumentált)*
- *Üzembehelyezési viszgálatok: a Vállalkozó felelőssége, dokumentált*
- *Rendelkezésre állási próbák (állomásra ill. gyűrűre): közös felelősség, közös program*
- *Integrált rendelkezésre állási próba*
- *További 'ad hoc' vizsgálatok (szúrópróba szerűen, nehezen ütemezhető)*

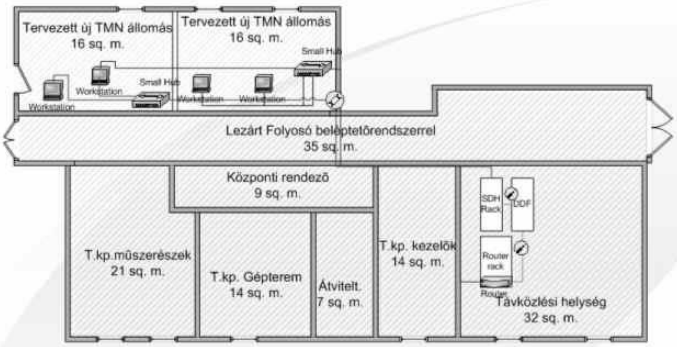
kapsch >>>

Szerződés folyamata



A tervezés eredményeként a szerződés tartalma változhat az ajánlathoz képest !!

Változatlan: a szerződés összege és a határidők.



	Project	Magyar Villamos Müvek Rt.
		SDH / PDH TMN system
Location	Budapest, Iskola u.	KAPSCH

314

DRENYOVSZKI János

A LÉGIERŐ PARANCSNOKSÁG HÍRADÁSÁNAK AKTUÁLIS KÉRDÉSEI

A Légierő Parancsnokság híradásának aktuális kérdései

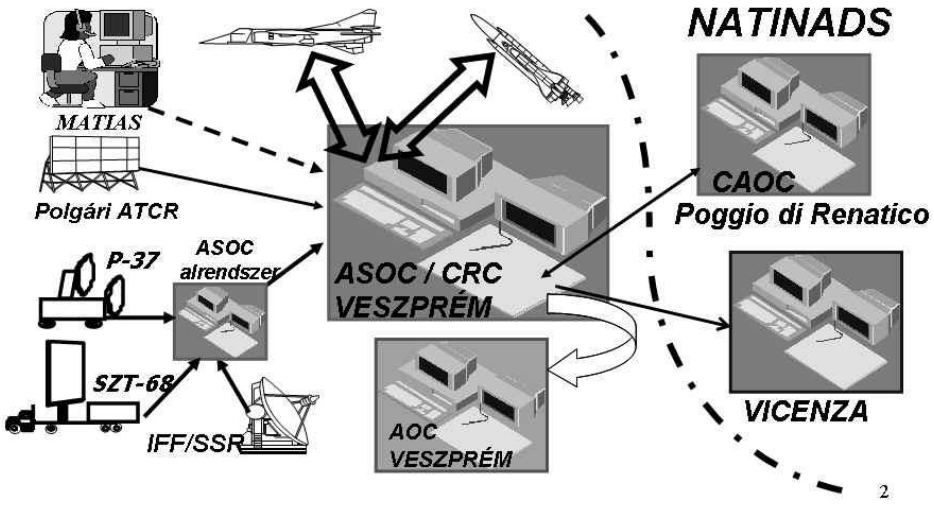
Drenyovszki János alezredes
MH Légierő Parancsnokság, Vezetési Főnökség, kiemelt híradó főtiszt

A Magyar Köztársaság NATO csatlakozása előtt, 1998 második felében a Magyar Honvédség és az akkori Légierő Vezérkar híradó szolgálatai előtt egy új, eddig számunkra szokatlan, de várt kihívás körvonalazódott.

A Légierő Vezérkar veszprémi harcálláspontján elkezdődött az úgynevezett „légtérszuverenitási hadműveleti központ" /Air Suverinity Operations Centre/ - továbbiakban ASOC – telepítése.

A megfogalmazott hadműveleti követelmények alapján az ASOC feladata a valós idejű légihelyzet kép /Recognized Air Picture- RAP/ előállítása, a Magyar Köztársaság légterében tartózkodó repülőszerkezetek azonosítása, erről tájékoztatás az elöljáró szervezet felé, valamint szükség esetén feladatszabás a légierő „aktív" – vadász és légvédelmi rakéta – fegyvernemei számára. (1. ábra)

A RAP LÉTREHOZÁSA ÉS TOVÁBBÍTÁSA

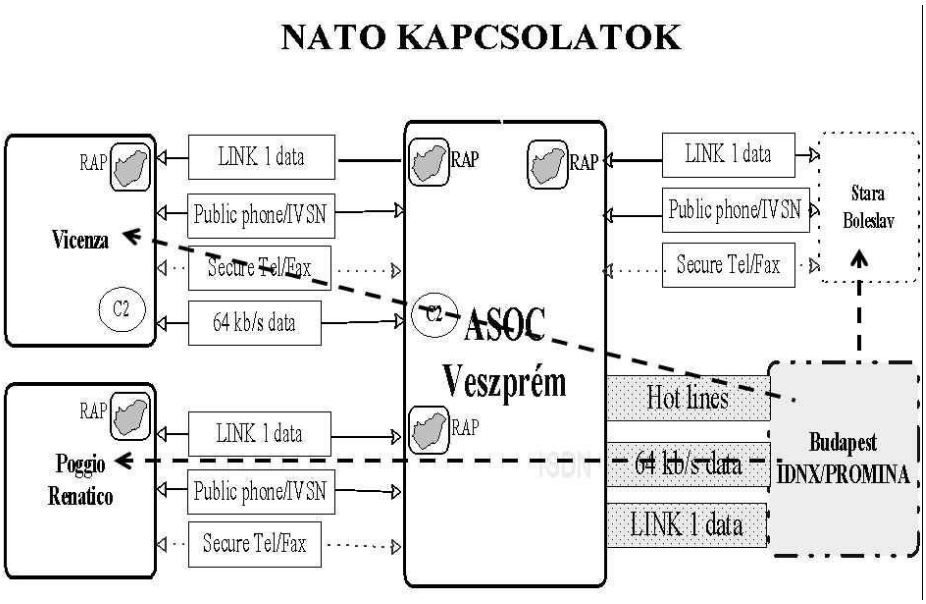


A feladatrendszer láthatóvá tette, hogy a korábbi légvédelmi értesítési, tájékoztatási rendszereket fel kell váltani egy számunkra új, automatizált adattovábbítási rendszerrel.

A várható feladatokból látszott, hogy a Magyar Honvédség – ezen belül a légierő híradása korszerűsítése elodázhatatlan.

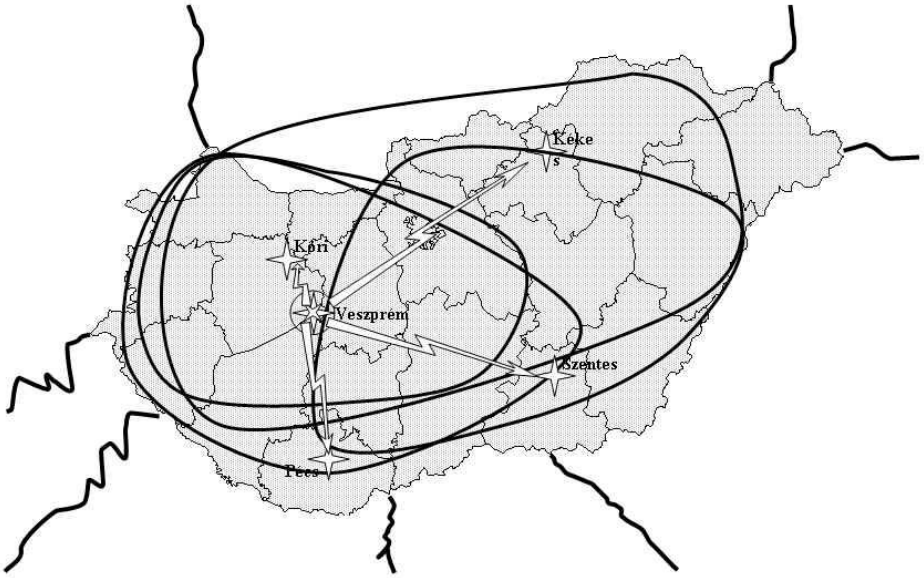
A fejlesztés 1998 decemberében megkezdődött - és a mai napig tart – az első digitális kapcsolóközpontok telepítésével.

Az első feladat – a valósidejű légihelyzet előállítása elsődleges és másodlagos adatainak eljuttatása szükséges Kup, Juta, Medin, Városföld, Békéscsaba, Debrecen helyszínekről. (2. ábra)



Az elfogó vadászrepülőgépek irányítására kiépítésre került Kőrishegy, Pécs, Szentes, Kékes helyszínekkel – Veszprémből történő távvezérléssel – a föld – levegő – föld hangkommunikációs rendszer, felváltva a korábbi sok-sok helyszínen telepített vadászirányító pontokat (VIP). A helyszínek „körültekintő" kiválasztásával a rádiólefedettség 1000m-es repülési magasságon az ország területén mintegy 95 %-os. (4. ábra)

RÁDIÓTÁVVEZÉRLŐ RENDSZER



A fejlesztés természetesen nem állt meg. Napjainkban kerül kiépítésre a Légierő Parancsnokság Hadműveleti Központja és valamennyi alárendeltje között az Integrált Vezetés Irányítás (ICC) rendszerét biztosító kommunikáció.

További feladataink a háromdimenziós radarok telepítésével egyidőben a radaradatok eljuttatásához és a helyszíneken telepítésre kerülő föld – levegő – föld híradást biztosító eszközök távműködtetéséhez szükséges kommunikáció kiépítése.

A Magyar Honvédség mobil hírközlési rendszerének állapotát azt hiszem nem kell részletezni. A Légierő számára is fontos feladat e terület fejlesztésének megkezdése, hiszen a kitelepülő légvédelmi rakéta, mobil radarcsoportok, valamint a Szárazföldi csapatok hadrendjébe települő Előrevont Légiirányító (tiszt, pont) (Forward Air Controller – FAC) irányítása, adatokkal való ellátása a jelen helyzetben nehézkes.

Nem érintettem a Légierőt nagyban befolyásoló repülőtéri navigációs rendszereinket.

Röviden azonban megemlítem, hogy a Kecskeméti Repülőbázis fénytechnikai és közelkörzeti irányító rendszere NATO és polgári szabványoknak megfelelően korszerűsített. Ezen a területen a továbblépést nagymértékben meghatározza a beszerzésre kerülő repülőgép fedélzeti navigációs rendszere.

Tisztelt konferencia ennyiben kívántam összefoglalni a Légierő Parancsnokság híradásának jelenlegi helyzetét, felvázolva röviden a továbblépés irányát.

318