A ZRÍNYI MIKLÓS NEMZETVÉDELMI EGYETEM KIADVÁNYA

A katonai kommunikációs rendszerek fejlődési irányai –kihívások és trendek a XXI. században

Nemzetközi szakmai tudományos konferencia anyaga

-2001-

Zrínyi Miklós Nemzetvédelmi Egyetem
Budapest, 2001. november 28.

Lektorálták a szervező bizottság tagjai:
Dr. habil. Sándor Miklós ezredes
Hamar Sándor mk. ezredes
Dr. László András alezredes
Dr. Rajnai Zoltán mk. őrnagy

Szerkesztette:
Fekete Károly mk. alezredes

Felelős kiadó: Dr. Szabó Miklós rektor
Készült a ZMNE nyomdájában, 200 példányban
Felelős nyomdai vezető: Kardos István

ISBN 963 00 8819 3

TARTALOMJEGYZÉK

A nemzetközi tudományos konferencia kommunikációs partnere:

Magyar Távközlési Részvénytársaság

A tudományos konferencia szponzorai:

- Unitronex Corp
- Thales
- Kapsch Telecom Kft
- Fercom Kft
- Siemens Telefongyár Kft
- CEOTRONICS AG
- Magyar Posta TETRA Rt
- UNIBIND HUNGARY Kft

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:
- Unitronex Corp.
- Thales
- Kapsch Telecom Kft
- Fercom Kft
- Siemens Telefongyár Kft
- CEOTRONICS AG
- Magyar Posta TETRA Rt
- UNIBIND HUNGARY Kft

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. László András alezredes
- 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.

A szakmai tudományos konferencia célja volt áttekinteni a kommunikációval kapcsolatos trendeket és kihívásokat a XXI. század elején. Elemezni kívánta a katonai kommunikáció (híradás) fejlődési irányait, a konvergencia megjelenési formáit.

További célja volt a katonai kommunikáció hadműveleti vezetés rendszerében elfoglalt helyének, szerepének értelmezése és képet adni a katonai képzés és felkészítés szakmaspecifikus jellemzőinek alakulásáról a haderő átalakítással összefüggésben megváltozott 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 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 nemzetközi szakmai tudományos konferencia plenáris és szekció előadásainak előzetesen beküldött változatából a nyomtatott formátumú különkiadvány mellé a konferenciát szervezők –korlátozott példányszámú- elektronikus formátumú, CD-n sokszorosított kiadványt is mellékeltek, melyen megjelentették az előző évi országos szakmai konferencia kiadványát is. A ZMNE Katonai kommunikációs rendszerszervező tanszékén a konferenci kiadvány elektronikus formátumú változatát illetően lehetőség van utólagosan felmerült igény kielégítésére.

A szervező bizottság

Jean-Louis DEBEURET

RÉSEAU TACTIQUE WAN DE NOUVELLE GÉNÉRATION RITA 2000

(THALES Communications - unité Réseaux - FRANCE)

Tout en reprenant les fonctionnalités (mobilité à la fois du réseau et des abonnés) qui ont fait le succès du RITA de 1ère génération, le réseau RITA 2000 rénove complètement la notion de réseau tactique terrestre, et constitue le cœur de la composante télécommunications du Champ de Bataille Numérisé. Il offre des services sécurisés en phonie et données, compatibles des standards civils (RNIS, IP, ATM,..) qui permettent la mise en œuvre des moyens les plus modernes maintenant en service dans les Postes de Commandement: bureautique opérationnelle, transmissions vidéo, visioconférences …

Une intégration technologique très poussée permet sa projection rapide sur des Théâtres d'opérations extérieurs, et diminue considérablement le personnel nécessaires à sa mise en œuvre. Son interopérabilité avec les réseaux fixes et tactiques, civils ou militaires, français ou de l'OTAN, permet de répondre aux nouveaux scénarios d'emploi multinationaux.

C'est le maillon indispensable de la chaîne de commandement, qui permet la transition du réseau opérationnel classique vers le concept de « Tactical Internet ».

Le nouveau contexte géostratégique, et les interventions récentes essentiellement sous forme de Forces Projetées, ont considérablement modifié le besoin en télécommunications sur les Théâtres d'opérations.

- Par exemple il y a nécessité d'assurer, dés les premiers instants de l'arrivée des éléments en zone opérationnelle, les liaisons indispensables au Commandement pour rendre compte de la situation aux autorités nationales, pour échanger la situation Renseignement la plus actualisée, et engager le processus Logistique. Cette urgence du besoin de communiquer a conduit à élaborer un système plus agile que le RITA de 1ère génération.
- De plus, la prolifération des Systèmes d'Information et de bureautique opérationnelle jusqu'aux plus bas échelons des troupes déployées en intervention appelait la mise en œuvre des technologies les plus performantes et les plus ouvertes.

Réalisé autour de ces principes, le Réseau de communication tactique de l'Armée de Terre RITA 2000 répond totalement aux besoins opérationnels de la période post 2000.

Qu'est ce que RITA 2000, et cela sert à qui et pourquoi faire ?

Mettons en situation un déploiement de Forces interaramées (éléments Terre / Air / Mer) pour y voir le rôle que tient RITA 2000.

- Les premiers éléments terrestres arrivent en zone opérationnelle avec un ensemble aéro-transportable RITA 2000 / Station satellite tactique. Le PC projeté dispose immédiatement sur site d'un réseau local multimédia à Haut Débit raccordé par une liaison SATCOM vers la métropole, et vers les autres éléments de l'intervention.
- Au fur et à mesure du déploiement de la Force, autour de ce premier élément de PC d'urgence viennent s'agréger les nœuds RITA 2000 qui constitueront un réseau tactique complet, pour desservir tant les usagers fixes des Postes de Commandement que les usagers mobiles dotés de postes de combat PR4G.
- Des interfaces de type STANAG sont installées vers les réseaux alliés, ainsi que des passerelles vers les réseaux civils locaux.
- Une autre zone RITA 2000 peut être constituée dans le même Théâtre, en mesure de raccorder directement le réseau MTBAd d'une base aérienne projetée, ou encore par moyen SATCOM constituer un réseau global avec les composantes aérienne et maritime de l'opération.
- Le système RITA 2000 est de plus en mesure d'étendre ses services jusqu'aux Postes de Commandement très tactiques en véhicules blindés et aux systèmes d'armes.

Le couple RITA 2000 / Stations SATCOM tactiques est parfaitement adapté à desservir un Théâtre d'opérations lacunaire, où les Forces Terrestres nationales n'occupent pas la totalité d'une région mais se concentrent sur les zones qui leur sont attribuées en fonction de leur mission, avec la possibilité de contingents alliés entre deux zones nationales.

par exemple :

- une zone de déploiement initial
- une zone logistique
- une zone opérationnelle principale
- des zones d'extension : lors de reconnaissances ou d'opérations dans la profondeur.

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

•Le réseau RITA 2000 utilise largement les standards civils, et offre aux usagers en opération des services multimédia IP et RNIS. Il constitue l'élément essentiel de la numérisation du champ de bataille.

•Comme nous le verrons 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 son transport en zone opérationnelle que pour sa mobilité sur zone

•Enfin dès sa conception 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 les PfP, mais été réalisé selon une architecture conforme aux standards TACOMs post 2000.

Pour présenter **le système RITA 2000** essayons d'abord de le positionner dans l'architecture générale des réseaux tactiques TACOMs post 2000.

Le modèle TACOMs post 2000 est proposé à 12 pays membres de l'Alliance par le consortium industriel TACONE, dont Thales est l'un des membres. Ce modèle segmente les communications tactiques en WAS, LAS, MS et systèmes terminaux des usagers

1. Le Wide Area System (WAS) est au cœur de cette architecture et assure particulièrement la fonction de transit.Le WAS se caractérise par un ensemble de réseaux à fortes contraintes, et disposant de ressources de transmission limitées (débit des artères). Les technologies mises en œuvre dans le WAS tendront donc à assurer:
   - l'utilisation maximum de la bande passante disponible ;
   - un overhead protocolaire minimum vis à vis des informations "utiles" transmises ;
   - l'assurance d'une QOS "militaire" alliant qualité des services et délais d'acheminement contraints (particulièrement en phonie et visio-phonie), et la priorité des usagers,
   - enfin l'interopérabilité avec les réseaux extérieurs civils et militaires.
2. Les Mobile Systems (MS) ce sont les réseaux radio de combat, qui peuvent être interconnectés par un backbone à « bande étroite » et constituer un Internet tactique.
3. Les réseaux de desserte et d'accès :
   - les LAS à très haut débit des postes de commandement importants, typiquement réalisés par un maillage de liaisons optiques, autour de commutateurs et de routeurs
   - et les LAS véhiculaires qui s'interconnectent pour constituer des PC tactiques.
4. Enfin les applications des usagers faisant largement appel aux services multimédia.

RITA 2000 se plaque exactement sur l'architecture TACOMs post 2000. Il offre une composante WAS de Transit, une composante LAS de desserte des

PC, une composante interface avec les systèmes mobiles selon les standards TACOMs post 2000.

RITA 2000 s'interface bien sûr avec les réseaux extérieurs du théâtre ou de la métropole. Il peut accéder directement, ou par l'intermédiaire de stations ARISTOTE, aux réseaux de satellites. Enfin il permet l'interopérabilité avec les réseaux alliés 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 l'armée de Terre, l'un des plus importants a été certainement de donner aux moyens de Transmissions une véritable capacité d'aérotransport. Les systèmes de communications tactiques de la génération des années 80, encore en service dans la grande majorité des armées occidentales, sont organisés en Sections de Transmissions constituées d'une trentaine d'hommes et d'une dizaine de véhicules. Le volume et le poids de ces moyens, les personnels nécessaires à leur mise en œuvre, sont peu compatibles avec les impératifs opérationnels d'une Réaction Rapide. Compte tenu des capacités d'aérotransport disponibles ils posent de véritables problèmes pour la planification et l'exécution d'un déploiement hors métropole. Avec des services offerts à la fois beaucoup plus variés et plus performants, l'élément de base de RITA 2000 se réduit à un simple véhicule de transmissions et un véhicule cargo, servis par et une demi douzaine de personnels. Un autre objectif particulièrement important de ce nouveau système de télécommunications tactiques, 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 État-majors. A travers cet exemple nous allons voir successivement les briques qui constituent le système de télécommunications tactiques RITA 2000.

- RITA 2000 est un réseau maillé de type WAN, dont l'objectif est de couvrir très rapidement une zone opérationnelle d'artères de télécommunications sécurisées. Les nœuds de ce maillage nous le verrons sont les CART : Centre d'Accès Radio et de Transit ;
- Les usagers, raccordés à ce maillage se situent dans des Postes de Commandement de taille différente suivant leur niveau :
    - ils se situent d'abord dans les Postes de Commandement Importants, tels que le sont les PC de Division, ou les PC de Forces multinationales, soit installés en shelters soit en bâtiments
    - ils se situent dans des Postes de Commandement Tactiques, plus compacts et composés de véhicules de commandement blindés, typiquement au niveau des Brigades

- les usagers de RITA 2000 sont aussi dans les Postes de Commandement mobiles au niveau des Régiments, qui constituent les unités de combat et de soutien, avec leurs Compagnies et Escadrons
- les usagers de RITA 2000 doivent être en mesure de coordonner leurs actions avec leurs alliés. Chaque élément du réseau est en mesure de s'interconnecter avec les réseaux alliés voisins.
- Quatre types de stations suffisent à remplir l'ensemble des fonctions de maillage, de raccordement des usagers et de gestion du réseau.

La fonction maillage est assurée par des nœuds de communication. Il s'agit de stations appelées CART : **C**entres d'**A**ccès **R**adio et de **T**ransit. Les CART utilisent des liaisons Hertziennes pour d'une part s'interconnecter et constituer le maillage de Transit, d 'autre part raccorder les Postes de Commandement.

Un programme séparé « Chaîne Hertzienne Future » va offrir au Réseau RITA 2000 des artères en Bande IV (jusqu'à 8 Mb/s) et le raccordement des Postes de Commandement en Bande V (qui pourront s'effectuer à des débits jusqu'à 34 Mb/s). 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 peuvent indifféremment appeler ou être appelés par les usagers du réseau RITA 2000, et si leur profile d'usager les y autorise, avec les usagers des réseaux d'infrastructure ou alliés qui sont raccordés à RITA 2000. Le système effectue le changement de raccordement d'une balise à une autre d'une manière transparente au cours de leurs déplacements. Les mobiles ont ainsi un service d'appel automatique de type radio-téléphone sécurisé :

- en Phonie,
- et en Transmissions de données.

La fonction d'interface d'accès et de desserte des abonnés est assurée par les stations "**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 pour assurer la même protection et la même mobilité que les unités qu'ils desservent.Dans les Postes de Commandement importants le CMAI est l'interface entre le réseau de transit et un réseau local LAS à très haut débit capable de desservir plusieurs centaines d'usagers. Pour des Postes de Commandement de taille plus réduite, le CMAI permet un accès direct potentiellement jusqu'à 80 usagers. Les artères de raccordement au réseau de transit pourront offrir des débits de 8 à 32 Mb/s (4x8 Mb/s) avec les faisceaux hertziens de la famille TRC 4000. C'est dans le domaine du raccordement des

unités très tactiques que le système évolue aujourd'hui, pour satisfaire les nouveaux types de déploiement des forces terrestres. Il s'agit d'offrir un support de transmissions significatif pour les unités situées dans des enclaves en dehors de la zone couverte par le WAS, voire en mouvement :

- d'abord avec une nouvelle station d'accès, en cours de définition, pour les unités déployées dans la profondeur. Dotée d'un terminal satellite tactique, elle sera l'interface entre le réseau de transit et le PC régimentaire. Elle devrait même permettre, mais avec des débits limités, de maintenir sa liaison SATCOM en cours de déplacement.
- ces besoins opérationnels émergeants appellent le développement d'interfaces « tout IP » entre le réseau de transit et les systèmes mobiles de l'avant constitués en Tactical Internet.

Abordons maintenant la fonction Local Area System de RITA 2000.

La desserte des PC importants est assurée par un réseau local LAS constitué de commutateurs Haut Débit et de routeurs, reliés en Fibres Optiques. La station CMAI, nous l'avons vu, assure 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. Il existe pourtant une différence fondamentale, on pourrait dire d'ergonomie, entre un Poste de Commandement et une entreprise : la taille d'un PC militaire en opération évolue, et les usagers veulent pouvoir obtenir leurs connexions en différents points d'accès du réseau.

Les contraintes opérationnelles de déploiement conduisent fréquemment ces 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 « wireless »,

- à des distances importantes, et avec des débits jusqu'à 32 Mb/s, par les moyens hertziens du programme CHF
- à l'avenir, sur de courtes distances avec des technologies Wireless LAN.**Les interfaces 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 État-majors. On peut citer : la bureautique opérationnelle, les téléphones et fax, la visioconférence, l'accès partagé à des bases de données opérationnelles, la conférence téléphonique, la continuité vers les usagers des réseaux extérieurs en particulier avec l'infrastructure nationale, et l'interconnexion avec des réseaux cellulaires type TETRA. Ceci 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. Toujours dans le domaine de prospectif, mais prévu d'être dans l'offre RITA 2000 à

court terme : les briques technologiques sont aujourd'hui disponibles pour donner à la station CMAI Tactique une capacité de raccordement par satellite.

Même éloignés de leurs bases, et en dehors de la couverture terrestre de la toile du réseau, les Postes de Commandement très tactiques pourront obtenir un raccordement immédiat au réseau RITA 2000, pendant les arrêts momentanés, voire avec des débits limités au cours leurs déplacements.

L'emploi du **RITA 2000** n'est pas limité aux seules interventions dites « conventionnelles », il peut bien sûr être déployé pour des opérations de maintien de la paix dans le cadre des Nations Unies, de coalitions « Partner for Peace », d'opérations de sécurité civile, voire pour des opérations en zone urbaine. Dans de telles opérations certains éléments des forces militaires ou de police utilisent des systèmes mobiles PMR (Professional Mobile radio). Toute station RITA 2000 peut 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 fixes et mobiles du **RITA 2000.**

Voici, pour conclure, le déploiement typique du système RITA 2000 pour desservir une zone de PC important : il s 'agit ici du PC du Commandement de la Composante Terrestre d'une opération de grande envergure (image 1).

- Arrivée d'un binôme station RITA 2000 / station SATCOM, et service immédiat d'un PC d'urgence
- Extension de la desserte 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, arrivée de mobiles, déploiement d'unités de protection, d'un hôpital de campagne, etc..
- Déploiement de la toile RITA 2000 adaptée à cette zone de PC

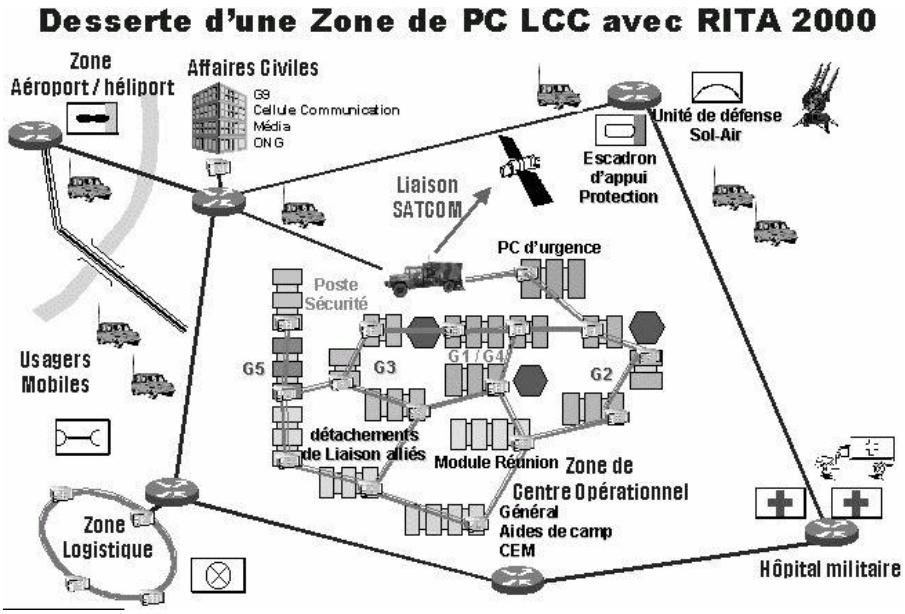


Figure 1.

Comme tout réseau de télécommunications, RITA 2000 dispose d'outils de gestion qui sont hébergés dans les stations CECORE (**CE**ntre de **CO**mmandement du **RE**seau) :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.

Bertalan Eged

SOFTWARE DEFINED RADIO CONCEPT FOR WIRELESS COMMUNICATION

Budapest University of Technology and Economics
Department of Microwave Telecommunications
Wireless Information Technology Laboratory
Goldmann ter 3. Budapest 1111 Hungary
T: +36-1-463-3614 F: +36-1-463-3289 beged@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.

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.

The idea behind Software Defined Radio (SDR) is not new, SDR technology was first demonstrated in a US Department of Defense project in 1995. [1], [2]

The Software Defined Radio Forum

Promotion of Software Defined Radio (SDR) technology is the reason the Software Defined Radio Forum was founded. The original name, the Modular Multifunction Information Transfer System (MMITS) Forum reflected the founders intention to address a broad interest area. When experience indicated that the MMITS name mystified many people, it was changed to SDR Forum, in spite of lack of a clear definition of what SDR meant. The term "Software Radio" and many variants with qualifiers such as "defined," "based," and other words, have been proposed to reflect various qualities of radio systems whose

functionality is partially implemented in software. (It should be noted that no functional radio system can be implemented without hardware.) [3]

The SDR Forum is an international industry association of 100+ organizations committed to enabling the wireless Internet and advanced capabilities for civil and military systems. The Forum is dedicated to promoting the development, deployment and use of software defined radio for advanced wireless systems. To that end, the Forum promotes the development of global standards for SDR technologies for use in modules, products and network systems in conjunction with existing commercial standards for wireless networks. [3]

The Forum's mission is to accelerate the proliferation of SDR technologies in wireless networks that support the needs of military, civil and commercial sectors. The Forum's charter is to: [3]

- Develop requirements and/or standards for SDR technologies. We intend to work independently and through liaison activities to ensure that the standards we develop are easily adaptable to existing and evolving standards for wireless systems.
- Bring together an international group of interested parties to promote global compatibility and interoperability in the wireless industry and to conduct cooperative research.
- Cooperatively address the unique security and regulatory needs of particular nations and/or market sectors while preserving common platforms and methodologies.

European activity

The European Commission recognised early that the benefits to be derived from a widespread adoption of SDR concepts were far reaching and would no doubt have profound implications for all mobile communications sector actors, namely manufacturers, operators, service providers, users, regulators, and standardisation bodies.

In 1996, in the scope of the Second Call for Proposals of the ACTS (Advanced Communication Technologies and Services) R&D program, one project was retained, FIRST (Flexible Integrated Radio Systems Technology), looking into intelligent multi-mode terminals.

In March 97, the European Commission (EC) organised the First European Workshop on Software Radio [4], trying to broaden the scope of the discussion. The workshop was instrumental in generating responses to the ACTS Third Call for Proposals, which included novel technological work in SR technologies. Two projects resulted in this area: SUNBEAM (Smart Universal Beam-forming) and SORT (Software Radio Technology), one dealing with the integration of smart array antennas in a "software radio base station", the other looking into base band issues, and namely channelisation.

The EC co-organised in June 98 the First International Workshop on Software Radio Technologies [5] with the, at the time, MMITS Forum, with the

objective of fostering the exchange of experience in the field, and explicitly of promoting a broader approach, extending beyond the terminal. The result fell far from what was expected.

Having in mind the objective of launching a European Initiative in this area, with a system, all encompassing perspective, the EC again organised in March 99 the First European Colloquium on Re-configurable Radio Systems and Networks, bringing together experts from many relevant areas, from DSPs to smart antennas, from algorithmic research to RF, from middleware and applications to network management.

At the Colloquium, the EC proposed a much broader, all encompassing approach than the one proposed by the SDR Forum. At that time their approach concentrates mainly on the terminal side (only recently was a working group formed to look into base station issues), while ours covers the whole system, extending through the network into service creation and application development.

The European Commission has played, in the area of Re-configurable Radio Systems and Networks, an important driving role. So, it is with some apprehension that they see quite a scattered approach to Clustering in areas that are relevant to the work that we have been promoting.

It should be obvious that without critical mass there is very little that can be accomplished. Furthermore, focusing on "specifics" leads to losing the overall perspective. This is particularly true in the area of Re-configurable Radio Systems and Networks.

Clustering is used to achieve a ‘consolidated added value’, promote collaborative work between projects: [8]

- Working in a common technical domain
- Working towards a common objective
- Aiming at co-ordinated dissemination of results

To support "action projects" contracted to assure work coherence

The reconfigurability cluster was founded and the the main objectives of the cluster on reconfigurability are: [9]

- To develop a vision on reconfigurability
- To provide a forum to consolidate the results of the participating projects
- To help with the identification of common interests of the projects and possible areas for cooperation among the projects

SDR Architecture

To communicate is to impart information from a source to a recipient by means of a medium. A conversation, a book, a TV broadcast, and a note on the refrigerator door are among the many forms of communication which abound in contemporary society. A substantial part of the world economy is involved in the business of communication. The many diverse segments of this society

provide vastly different perspectives. Department of Defense suppliers, magazine and newspaper publishers, motion picture producers, television and cable networks, wireline telephone companies, and cellular service providers have vastly different views of the meaning of communication, as well as divergent economic interests. In spite of this diversity.

The primary interest of the SDR Forum is in communication using radio technology. A Radio is a communication system employing wireless transmission of information by means of electromagnetic waves propagated through space. The two most salient characteristics of a radio communication link are mobility and networking. Mobility is the independence of the position of the terminal from the geographic location of the source. Unlike the services provided by a public address system or a wired telephone, by use of radio equipment the driver of a moving car can listen to a traffic report or conduct a telephone call. Networking is the linking of multiple radio stations to facilitate communication. It describes the means used to control which of many stations are involved in a particular communication, determination of connections between stations, and specification of which station (if any) is in control of the network. An important form of network is a tactical network, used to control operations of a fleet of vehicles, such as tanks, fire trucks, or taxis.

A wide variety of different types of radio links are in active service, characterized by different operating frequencies, different modulation techniques used to impose information on the radio waves, and different information coding formats or protocols.

SDR architecture is based upon a high-level generic model with specific functional blocks connected via open interface standards recommendations. The SDR architecture supports three specific domains: hand-held, mobile, and base-station (or fixed site). The software is implemented by controlling the characteristics of equipment/device subsystems through hierarchical and peer level modules that support scaleability and flexible extensions of applications. Modularity is the key to successful implementation software applications within open systems. Between modules are defined interfaces that are subject to standardization. Within a module the developer is free to implement functionality in the most effective way.

The following figure (Fig. 1.) illustrates a high-level hierarchical functional model for software defined radio (SDR) systems. Three views of increasing complexity are presented. The top-level view is a simple representation of an entire information transfer thread. The left side interface is the air interface. The right side interface is the wire side and user interface. The next level view identifies a fundamental ordered functional flow of four significant and necessary functional areas; (1) front end processing, (2) information security, (3) information processing, and (4) control. It is noted that diagrams and processes discussed within this document, unless otherwise specified, are two-way de-

vices (send and receive). Note that the functional model as shown in this figure is not intended to show data or signal flow.

The SDR Forum software reference model for an information transfer thread implemented as a software defined radio envisions multiple processing elements operating in parallel to implement the two paths. One path is for control, directives to individual system components needed to execute system operations such as increase volume, change frequency, switch antennas, or switch to a different air interface. The other path describes the flow of information carried by the radio signal.

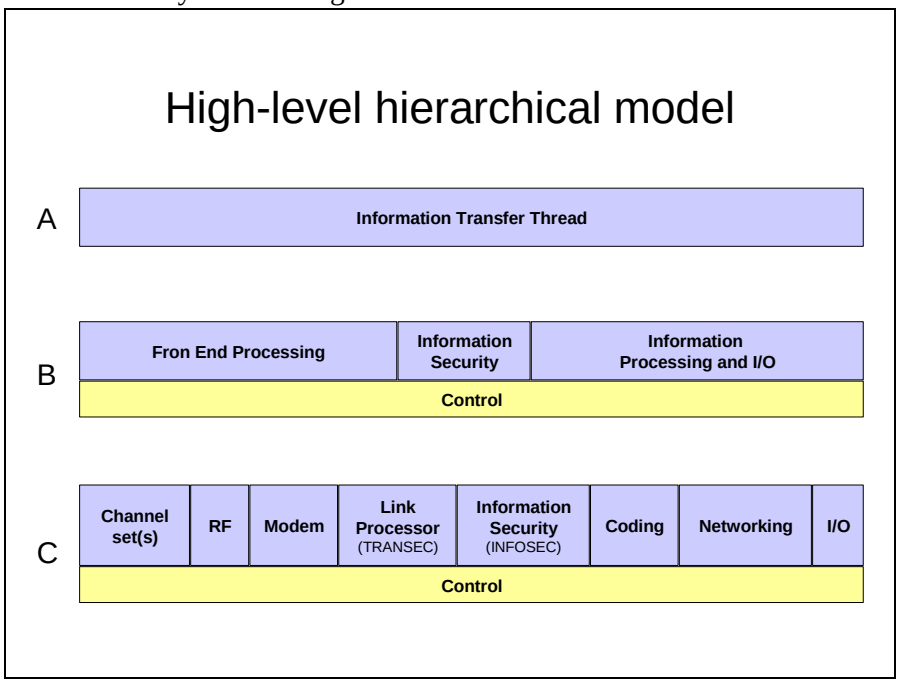


Figure 1.

Front end processing is that functional area of the end user device that consists generically of the physical air (or propagation medium) interface, the front-end radio frequency processing, and any frequency up and down conversion that is necessary. Also, modulation/demodulation processing is contained in this functional block area.

Information security is employed for the purpose of providing user privacy, authentication, and information protection. In the commercial environment, this protection is specified by the underlying service standard while in the defense environment, this protection is of a nature that must be consistent with the various Governmental doctrines and policies in effect.

Content or information processing is for the purpose of decomposing or recovering the embedded information containing data, control, and timing. Content processing and I/O functions map into path selection (including bridging, routing, and gateway), multiplexing, source coding (including vocoding, and video compression/expansion), signaling protocol, and I/O functions.

The block diagram of the radio functional model amounts to a partitioning of the black-box functions of the ideal software radio nodes introduced above into the specific functional components shown in the last level of Figure 1. and listed in Table 1.

Functional Component	**Allocated Functions**
Input and output	Human interface, narrow band conversion
Service and network support	Multiplexing, setup and control, data services, internetworking
Source coding and decoding	Audio, data, video, and fax interfaces
Information security	Authentication, nonrepuditation, privacy, data integrity
Link processing and transmission security	Hopping, spreading
Modem and IF processing	Baseband modem, timing recovery, equalization, channel waveforms, predistortion, beamforming, diversity combining,
RF access	Antenna , diversity, RF conversion
Channel sets	Simultaneity, multiband propagation
Multiple personalities	Multiband, multimode, interoperable

Table 1.

The SDR architecture consists of functions connected through open interfaces, and procedures for adding software specific tasks to each of the functional areas. The software necessary to operate is referred to as a software application. The following figure (Fig. 2.) shows the SDR open architecture of

seven independent subsystems interconnected by open interfaces. In this view the generalized SDR functional architecture has been particularized by equating a subsystem definition to each functional area. In general this is not the case; subsystems will be determined by implementation considerations. Interfaces exist for linking software application specific modules into each subsystem. Each subsystem contains hardware, firmware, an operating system, and software modules that may be common to more than one application. The application layer is modular, flexible, and software specific. The common software API layer, inferred in the following figure (Fig. 3.), is standardized with common functions having open and published interfaces. Peer-to-peer interfaces are neither required nor proscribed.

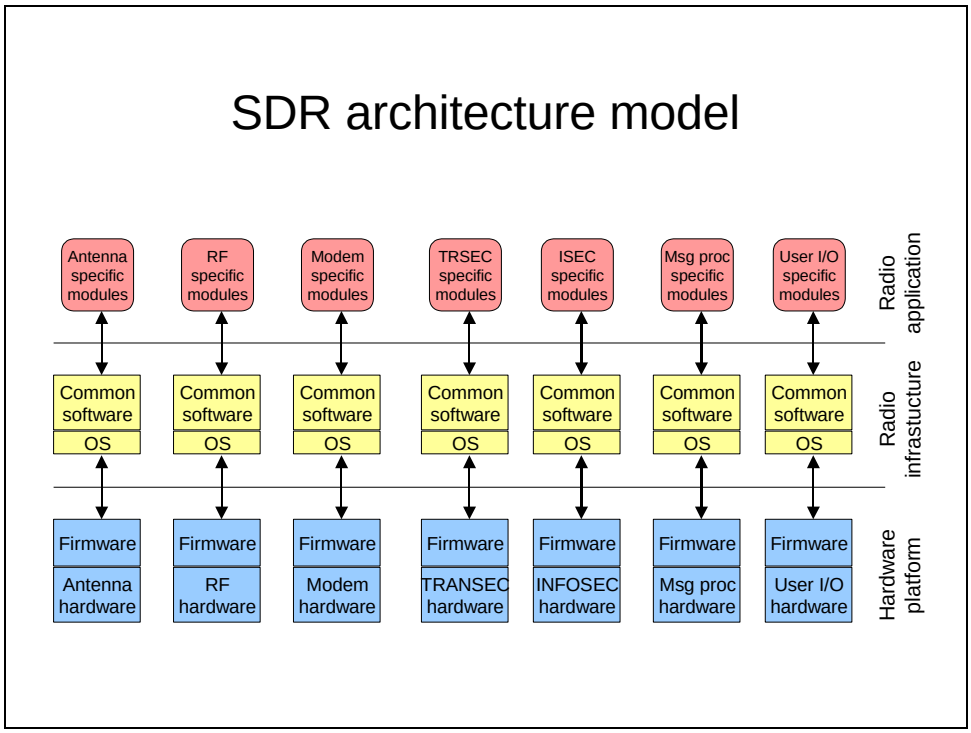


Figure 2.

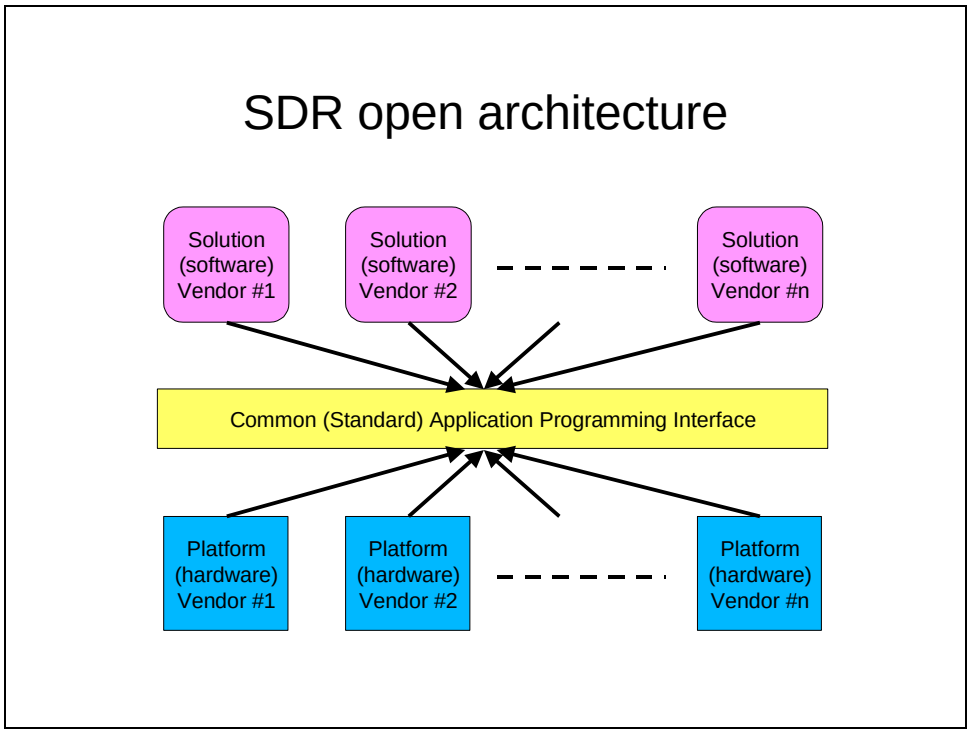


Figure 3.

Software Radio Definitions

In describing a cognitive space, it is often useful to start with extreme cases. One extreme of the software defined radio is a radio with no software at all. Such all-hardware systems were used for many years prior to the availability of digital semiconductor technology. The closest thing to software was a manual that told the operator what settings to use in order to change frequency or how to change from amplitude modulation to continuous wave operation. At the other extreme is something we can give the working title of "ultimate software radio." Use of the term "software radio" has been suggested for such a system. But in the absence of any qualifier, software radio would seem to apply to any system with any software at all, rather than implying the ideal or ultimate solution. We propose, then, to make that term generic, and use the term "software radio" to cover Tiers 1-4 as described below.

Tier 0. Hardware Radio

No provision is made for any changes of system attributes except by physical intervention by the user or a service technician. System operation is accomplished by use of switches, dials, and buttons, by physically opening the covers, or by replacing the unit. This category also applies to radios that have

some specific functions operated remotely by electromechanical means such as relays or servos. Internal use of software, firmware, or computer processing elements still fits this definition if they cannot be changed externally.

Tier 1. Software Controlled Radio

Radios in this category have control functionality implemented in software, but do not have the ability to change attributes, such as modulation and frequency band without changing hardware. This includes the SDR handheld model with a switcher and a group of independent or "velcro" radios in a common case.

Tier 2. Software Defined Radio

The Tier 2 system provides a broad operational range (e.g. 20-500MHz, 1-2GHz) under software control without hardware change. These systems are typically characterized by a separate antenna system followed by some wideband filtering, amplification, and down-conversion prior to receive analog-to-digital conversion. The transmission chain provides the reverse function of direct digital-to-analog conversion, analog up-conversion, filtering, and amplification. This front-end equipment represents a constraint on the frequency coverage of the system, and its performance. It may be necessary to switch antennas to obtain the entire frequency range. Except for these constraints, however, the system is fully capable of covering a substantial frequency range and of executing software to provide a variety of modulation techniques, wideband or narrow-band operation, communications security functions (such as hopping), and meet the waveform performance requirements of relevant legacy systems.

An SDR is also capable of storing a large number of waveforms or air interfaces, and of adding new ones to that storage through either disk or on-line load. Over-the-air software load is desirable, but not required in the definition. The system software should also be capable of applying new or replacement modules for added functionality or bug fixes without reloading the entire set of software.

Tier 3. Ideal Software Defined Radio

This system has all of the capabilities of the Tier 2 system, but eliminates analog amplification or heterodyne mixing prior to digital-analog conversion. It provides dramatically improved performance by eliminating analog sources of distortion and noise.

Tier 4. Ultimate Software Radio

This system description is intended for comparison purposes rather than implementation. It is a small lightweight component with very small current drain that can easily be incorporated into personal devices. It requires no external antenna, and no restrictions on operating frequency. It has a single connector that delivers the desired information in the desired format, typically digital. The connector also accepts information, uses it to modulate a signal,

and radiates that signal in the desired waveform or air interface. The ultimate software radio also accepts control information through its connector to operate and reconfigure the operating software. It can switch from one air interface format to another in milliseconds, use GPS to track the users location, store money using smartcard technology, or provide video so that the user can watch a local broadcast station or receive a satellite transmission. Further, it has a large amount internal processing capacity, so with appropriate software it can perform a wide range of adaptive services for its user.

SDR Functional interfaces

The following figure (Fig. 4.) presents the SDR functional interface diagram and demonstrates how the SDR Architecture extends to the definition of functional interfaces. A representative information flow format is provided at the top of the diagram. Actual representations will be implementation dependent. Interfaces are identified for information and control. For example, information transfer is effected throughout the functional flow within the SDR architecture to/from antenna-RF, RF-modem, modem-INFOSEC, and INFOSEC-Message Processing interfaces. Control and status is effected between the same interfaces as information and, in addition, control is effected between each functional module and one or more control points and interfaces. Auxiliary interfaces are also allowed, as shown on the diagram.

The actual user traffic (i.e. data and information) being transmitted follows the paths illustrated by the "I" in the figure. SDR works by providing control ("C") over each of the functional blocks as indicated by the Control function. As an example, the frequency at which a wireless signal is generated is determined by frequency generation in the RF function. Through the control capability, an SDR terminal would allow this frequency to be changed to accommodate different operating environments (such as moving between regions with different frequency assignments).

After identifying the functions to be accomplished in a software radio, one must define the interface points among the functional components. The notation RF waveform is shorthand for RF interface. The IF waveform includes most aspect of the air interface, but the signal have been filtered and converted to an IF that facilitates processing. In addition, IF processing may include A/D and D/A conversion. Baseband waveforms are almost always digital streams, they may also be sampled replicas of analog waveforms. The modem delivers what may be called decoded channel bits (“black” bits in INFOSEC jargon) to the transmission and information security functions if one is present. Information security then transform these protected bits into a clear bits (“red” bits). These bits maybe manipulated through a protocol stack in order to yield source

bits or network bits. Network bits conform to network protocol, while source bits are appropriate for a source decoder. The interface to a local user of voice, video, etc. includes an analog trasducer. Access to a remote sources is accomplished via a network interface. In addition these signal-processing interfaces, there are control interfaces mediated by the user or network. Personalities are downloaded to the radio via the software object interface. The simplest mechanism for maintaining radio software after deplymnt is the downloading of a complete binary image of the radio. A more flexible approach allows one to download a specific new function such as a specialized voice coder (vocoder).

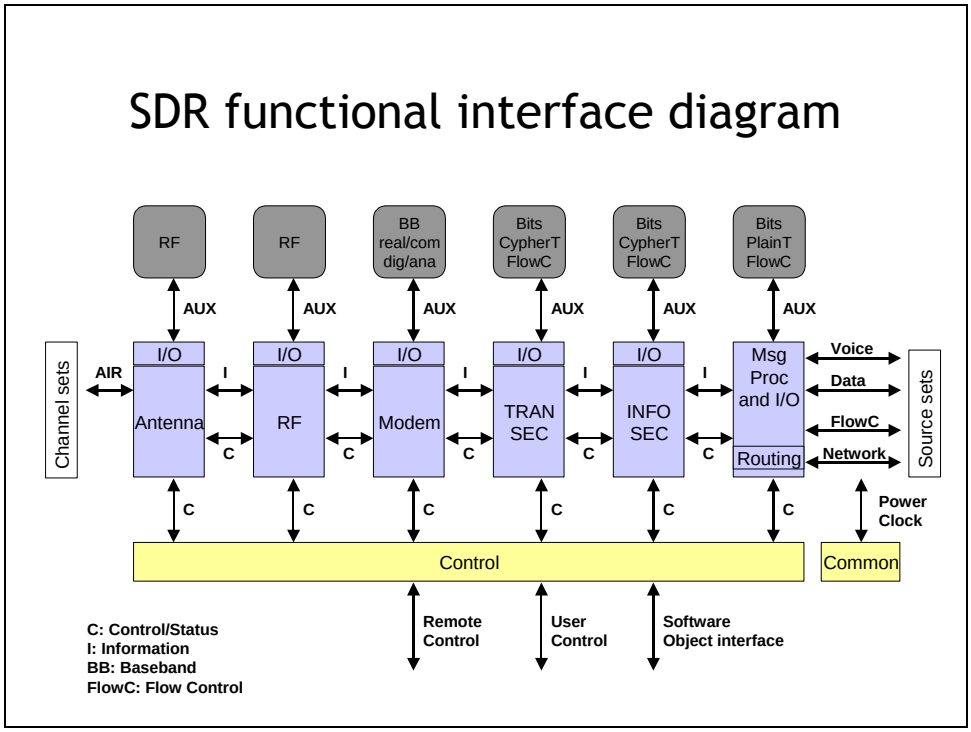


Figure 4.

These interfaces may be thought of as the “horizontal” interfaces of the software radio, since they are concateaned to form signal and control flows among sources and channels. They air future characterized in Table 2.

Interface	Characteristics
Analog stream	Audio, video, facsimile
Source bitsream	Coded bitstreams and packet. Converter, vocoder, data compression
Clear bitstream	Framed, multiplexed, forward error controlled, bitstreams and packets
Protected bitstream	Random challenge, authentication responses, public key, encripted bitstreams and packets
Baseband Waveform	Discrete time synchronous quantized sample streams (one per carrier)
IF Waveform	Composite, digitally preemphasized waveform ready to up-conversion
RF Waveform	Antenna , diversity, RF conversion
Channel sets	Power level, shape, adjacent channel interference, etc. are controlled
Network Interface	Packaged bitstreams may reqire asynchronous transfer mode (IP)
Joint Control	Control interfaces to all hardware and software initialization, fault recovery
Software Objects	Download from evolution support systems

Table 2.

In traditional radio engineering, the definition of such interfaces faciliated the design and development of the radio. Variation of these definitions from one design team (vendor) to another did not matter, provided the component suppliers and the system integrator all agreed. The idea of plug-and-play hardware and software modules has become popular in personal computing. The wireless industry seeks to benefit from the adaptation of plug-and-play technology to the software radio. This potentially elevates any functional partitioning to the role of architecture. Plug-and-play requires industry wide agreement on architecture.

Our current activity

Wireless Information Technology Lab runs active projects in the field of Software Defined Radio. It is our main interest to develop a general radio infrastructure as the base of application development. The focus is on the base band and RF front end functionality. Our hardware platform consists of tree main elements the base band unit, the frequency conversion and control unit. (Fig. 5.) The base band unit can be divided into two segment the DSP processor part and a high-speed interface between the digital up converters (DUC) and digital to analog converter (DAC). (Fig. 6.) The DUC contains 4 channel

including the serial port, RAM coefficient filter (RCF), cascade interpolation filter (CCI), numeric controlled oscillator (NCO) and final summing stage. (Fig. 7.) The experimental test platform is realized (Fig. 8.) and some typical modulation formats was implemented on the platform. (Fig. 9-12.)

Future plans include the extending the frequency range up to 2500MHz covering the most frequently used wireless mobile bands and developing the receiver architecture based on the SDR concept.

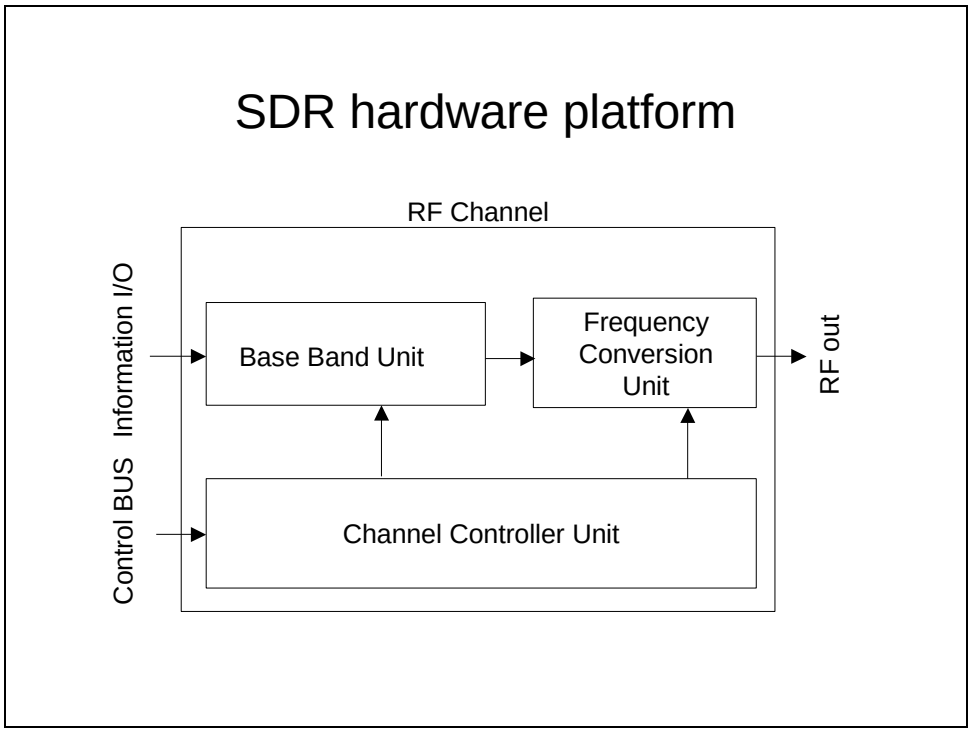


Figure 5.

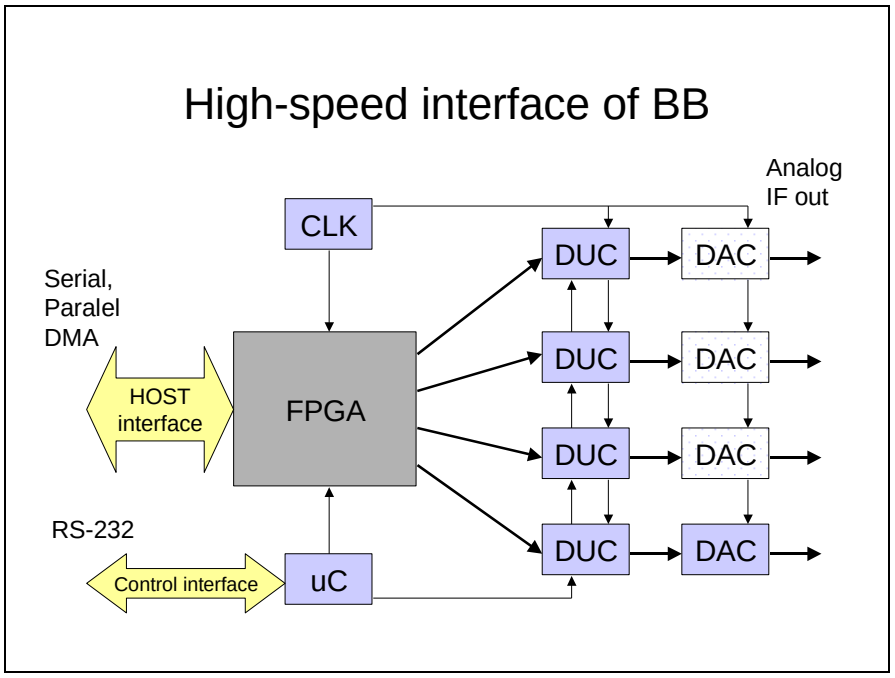


Figure 6.

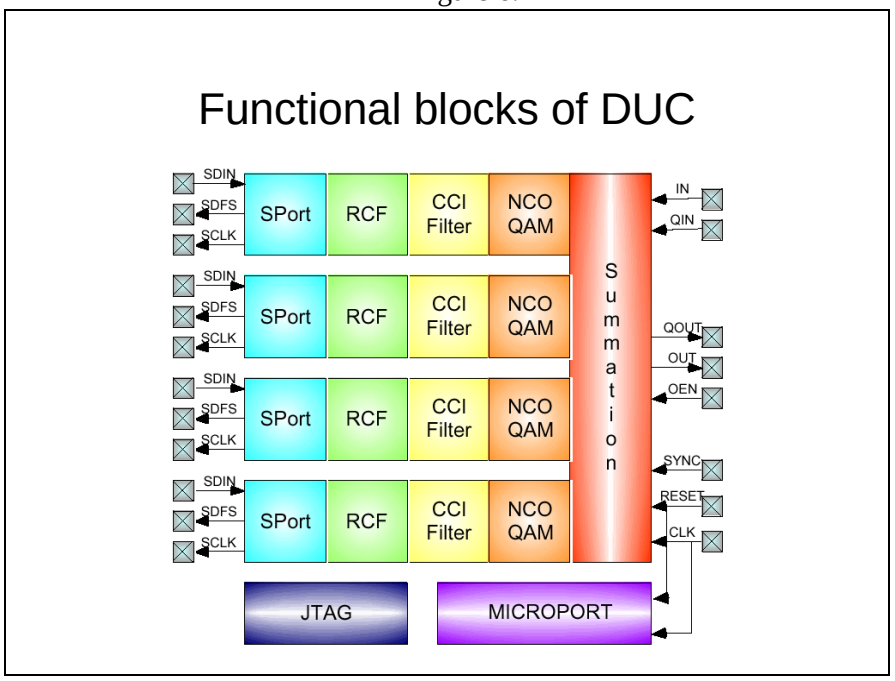


Figure 7.

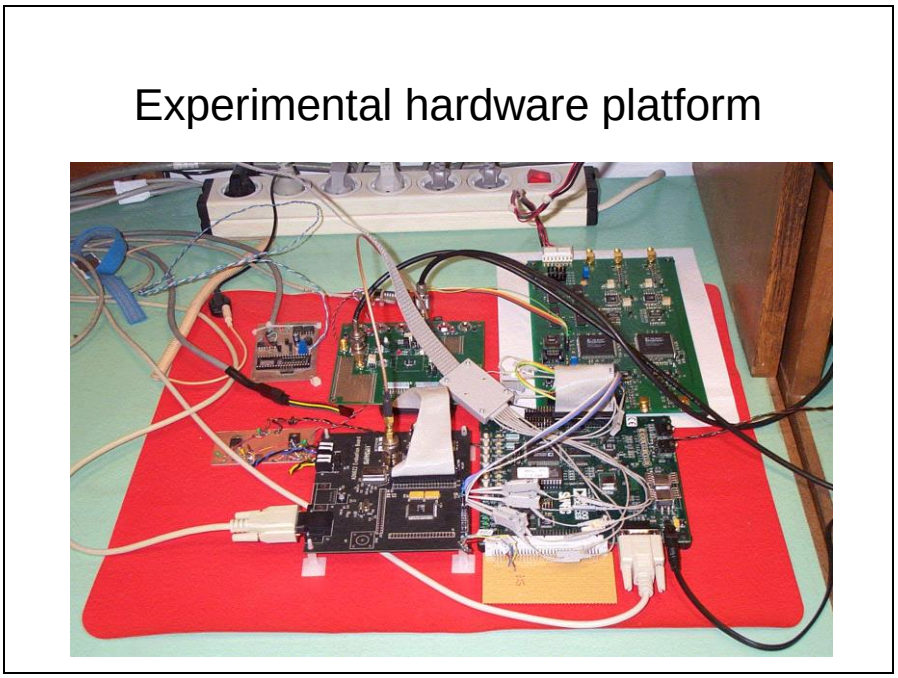


Figure 8.

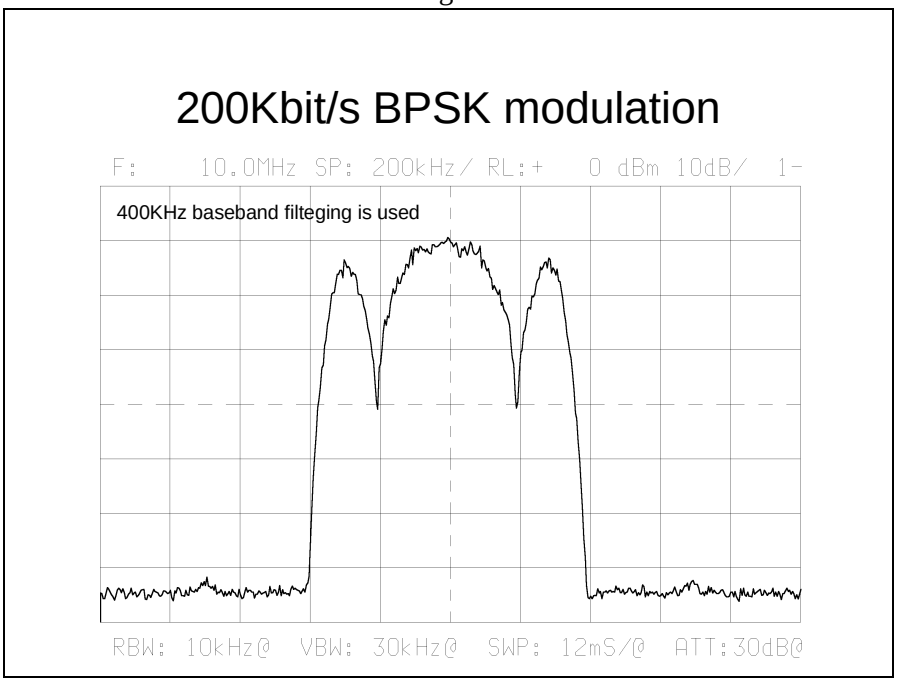


Figure 9.

Vector diagram of GSM/EDGE

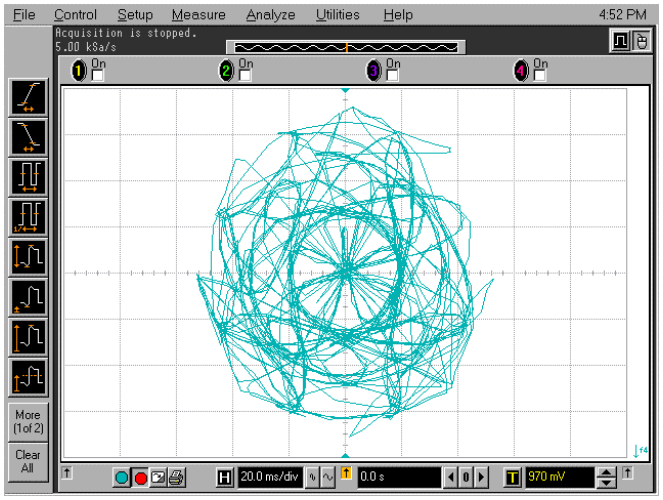


Figure 10.

Histogram of GSM/EDGE modulation

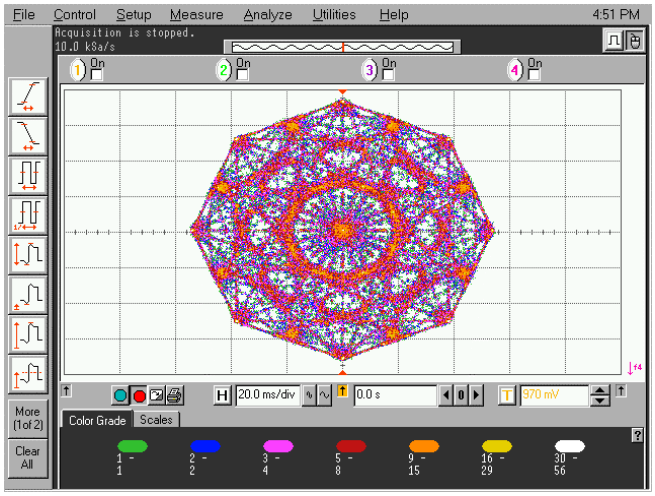


Figure 11.

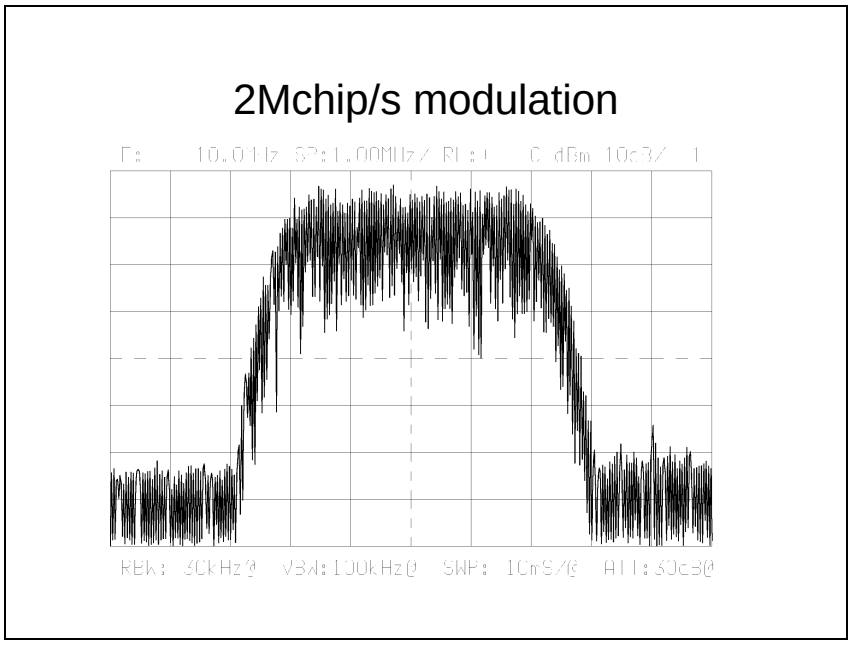


Figure 12.

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] Proceedings of the First Workshop on Software Radio, Brussels, May 1997.
[5] Proceedings of the First International Workshop on Software Radio Technologies, EC/MMITS Forum, Rhodes, June 1998.
[6] Re-configurable Radio Systems and Networks, Jorge M. Pereira, Editor, European Commission, DG XIII, London, Mar 1999.
[7] Jorge M. Pereira, "Beyond Software Radio, towards Re-configurability across the whole System and across Networks", Proceedings of VTC-Fall 99, Amsterdam, September 1999.
[8] IST Mobile, Satellite and Personal Communications, Concentrations and Clusters http://www.cordis.lu/ist/ka4/mobile/concertacluster.htm
[9] IST Mobile, Satellite and Personal Communications, Cluster on Reconfigurability http://www.cordis.lu/ist/ka4/mobile/reconfigurability2.htm
[10] Second European "Colloquium on Reconfigurable Radio" 18-19 October 2001 Athens, Greece, http://cnl.di.uoa.gr/colloquium/

Dr. Rajnai Zoltán
Article revu par Beatrix Fregan

LA NUMÉRISATION DANS L' ARMÉE DE TERRE

La numérisation de l'espace de bataille va permettre de doter le combattant, les chefs et les états-majors d'un outil commun d'information capable de donner en temps quasi réel, la même image de l'évolution de la situation et d'accélérer la prise de décision. Introduire ainsi l'informatique revient à doter une armée moderne d'un formidable multiplicateur d'efficacité et à la mettre en capacité d'acquérir la supériorité, non plus en se fondant exclusivement sur l'accumulation d'armes, de matériel et d'hommes, mais en recherchant l'emploi le plus performant possible des moyens les mieux adaptés à la situation. L'enjeu est immense puisqu'il s'agit, et c'est une attitude nouvelle, de ne pas hésiter à puiser dans les technologies civiles adéquates de l'information pour optimiser l'emploi des forces terrestres.

Les systèmes entièrement numérisés vont faciliter et renforcer la fonction d'interopérabilité avec les armées alliées, non seulement pour permettre l'articulation plus souple des unités avec leurs homologues étrangers lors d'opérations multinationales.

Des conditions opérationnelles nouvelles

La numérisation de l'espace de bataille permet d'optimiser l'emploi des forces terrestres en s'adaptant aux nouvelles conditions opérationnelles et en utilisant les technologies de l'information disponibles dans le civil. Le concept de numérisation de l'espace de bataille se fonde sur plusieurs constats. La plupart des théâtres d'opérations ne sont plus continus mais éclatés. Ils imposent une série d'engagements lacunaires au lieu d'un engagement linéaire classique. Les forces se projettent loin de leurs bases et, de plus en plus, dans le cadre d'une coalition multinationale qui pose le problème de l'interopérabilité des moyens alliés.

Les interventions de maîtrise de la violence, qui ont tendance à devenir majoritaires, impliquent une capacité moduler l'action militaire depuis la simple opération d'interposition jusqu'aux actions de rétorsion par le feu. La supériorité quantitative n'est plus le moyen privilégié de prendre l'ascendant sur un adversaire militaire. Cette logique trouve d'ailleurs ses limites budgétaires. Il est apparu, notamment pour des raisons de coût, qu'il était possible de fonder la puissance opérationnelle sur d'autres critères que l'accumulation pure et simple de moyens de combat. Il est vital de chercher à optimiser l'emploi des nouvelles générations de matériel existant — chars, hélicoptères, missiles, systémes d'artillerie sol-sol et sol-air, moyens de reconnaissance par drones notamment, etc. La connaissance en temps quasi réel de l'espace de bataille, de l'état des forces en présence, de leur évotution,

de leur environnement, rêve de tout grand soldat au cours de l'histoire, confère la supériorité en donnant un temps d' avance à celui qui sait et en lui offrant la certitude de conduire sa maneuvre en pleine efficacité opérationnelle.

L'effet Internet:

La technologie qui permet d'optimiser les moyens, de les rendre interopérables, de les moduler existe dans notre quotidien. Il s'agit de la technologie numérique symbolisée par internet et son réseau, ses banques de données, ses moteurs de recherche, internet qui accélère à la fois l'acquisition de l'information, son traitement et sa diffusion.

Il n'est pas question pour des moyens relevant du métier des armes et qui doivent garantir une absolue confidentialité ainsi qu'une fiabilité en ambiance de combat, de se brancher sur internet pour faire la guerre. Mais il est de bonne politique de puiser dans le vivier technologique civil pour accroître l'efficacité militaire. Il faut bien comprendre que la numérisation de l'espace de bataille ne se profile pas comme une fin en soi, mais qu'elle permet d'atteindre l'objectif qui est l'excellence opérationnelle; d'où l'idée d'insérer dans l'espace de bataille toute la panoplie numérique utile à l'acquisition du renseignement sur l'adversaire et l'environnement, à sa transmission, à son traitement et à sa diffusion ciblée vers les unités engagées. Il est évident que la numérisation va générer sur le théâtre d'opérations et, en particulier, au niveau des états-majors, un flux d'informations alimenté non seulement par les liaisons phoniques et les échanges de données, mais aussi par des éléments très divers d'imagerie. Ce flux devra être soigneusement traité, filtré, synthétisé pour rendre l'information utilisable en fonction des trois grands niveaux: stratégique, opératif et tactique. C' est pourquoi il faut choisir une diffusion horizontale de l'information par niveaux de commandement et non pas verticale, par spécialités selon la pratique américaine. Cette approche permet de rester en cohérence non seulement avec les moyens dont dispose la Nation, mais confère au chef sur le terrain, une capacité d'initiative. La numérisation représente certes un effort important, mais le fait qu'elle fasse appel des technologies civiles existantes, donc amorties sur de très grandes séries, permet de limiter l'impact budgétaire. De plus, l'investissement dans les technologies de l'information s'avère moins lourd que le lancement de programmes de conception et de réalisation destinés à remplacer les équipements militaires en service (opérationnels) aujourd'hui ou à accroître leurs performances.

Une question d'actualité: Qu' est-ce que la numérisation?

C'est une technologie qui apporte la capacité de transformer la voix, des données, des cartes, des photos, tous types d'informations, en signaux numériques, de les transmettre et de les recopier selon les besoins, sans subir de déformation. La numérisation permet aussi d'entrelacer les informations, par exemple la voix et des données sur un seul canal. Les données peuvent être

compressées pour occuper moins d'espace dans les transmissions. Ce concept va fédérer les systémes d'information et de communication. Il apporte un facteur multiplicateur d'efficacité. L'enjeu est donc trés important. Une élimination du doute et une augmentation de la vitesse de compréhension des situations, des renseignements transmis et traités quasiment en temps réel, des ordres plus vite répercutés. Avec la numérisation, les différentes armes de l'armée de Terre, et les forces alliées deviennent plus facilement interopérables car elle fluidifie les protocoles d'échange entre les différents systémes.

Un exemple concret de l'efficacité de cette technologie

Les informations de sources différentes pourront être corrélées rapidement. On peut imaginer plusieurs capteurs, une observation humaine, une image de drone, le radar détectant un même objectif. La transmission s'effectuera en instantané et s'inscrira presqu'aussitôt sur un écran d'état-major. Dans le système traditionnel, il faut un délai beaucoup plus long pour reporter ces infos sur une carte.

Mais il y a-t-il des risques dans les domaines de la numérisation?

La surinformation en fait partie. Chaque acteur à son niveau ne doit pas détenir en permanence la somme des informations sur l'espace de bataille mais disposer de ce dont il a besoin. Pour autant, l'ensemble des acteurs doit pouvoir se référer à une base de données unique. Ce qui implique que toutes les informations qui entrent et sortent de cette base soient validées par une cellule spécialisée au niveau du poste de commandement. A l'échelon d' une brigade ou d' un régiment et de ses composantes, la numérisation ne doit pas constituer une entrave à la liberté d'action au combat mais une aide, d'où la nécessité d'automatiser le maximum d'échanges et de réduire au strict minimum le nombre de touches à manipuler. Enfin, il ne faudrait pas que la «facilité» offerte par la numérisation incite les décideurs à attendre la prochaine information. Au lieu d'être accéléré, le processus serait alors retardé. L'échange automatique de données numériques n'interdit nullement le commandement à la voix. Il y a complémentarité. La numérisation doit permettre de mieux se consacrer la conduite du combat, en automatisant un certain nombre de tâches annexes, telles la fourniture de la position ou du potentiel.

L' effort de la numérisation continue est loin d'être neutre pour l'armée de Terre qui doit aboutir vers les années 2010-2015 à une généralisation de la numérisation. Sachant que les systémes qui seront en service dans une dizaine d'années n' auront rien à voir avec ceux d'aujourd'hui.

(D'après l'article de « Numérisation de l'espace de bataille » de l'Armées d'aujourd'hui)

Hans Helmut PEER

EINE EFFEKTIVE TRUPPE BRAUCHT PERKFEKTES KOMMUNKATIONSEQUIPMENT

Gut 10 Jahre nach dem Mauerfall und in Zeiten, in denen immer mehr Staaten des ehemaligen Warschauer Paktes in die Nato eintreten steht eine Reform dieser Streitkräfte unmittelbar bevor. „Kämpfende Truppe in Gefahr"

Um sich den neuem komplexen Herausforderungen stellen zu können brauchen sie eine hoch effiziente Truppe. Doch diese „kleinen & schlagkräftigen Einheiten" können nicht allein an der Güte ihrer Ausbildung, der Qualität des Trainings und an den zur Verfügung stehenden High Tech-Waffen gemessen werden.

Ohne professionelles Kommunikations-Equipment hat die verbleibende „aktive Truppe" zwar Arbeitsplätze, schwebt aber bei Kampf-, Sicherungs-und Ordnungseinsätzen in Lebensgefahr.

Nur perfekte Kommunikation schafft Sicherheit

Schlechtes Kommunikations Equipment führt nicht selten zu Mißverständnissen oder Rückfragen. Diese sind bei der kämpfenden Truppe im besten Falle zeitraubend oder störend-, in den schlimmsten Fällen tödlich. Ob Helmkommunikationssysteme zum Anschluß an Funkgeräte fürdas Heer, Headsets für Piloten oder Hör-Sprechsystem für die Bodenabfertigung bei der Luftwaffe. In allen Bereichen der Landesverteidigung oder bei künftigen Nato oder UN –Einsätzen haben die Länder ihren Soldaten gegenüber die Verplichtung bei der Beschaffung von Kommunikationselektronik als erstes an die persönliche Sicherheit zu denken.

Billig ist selten günstig.

Für Wirtschaftlichkeit eines Kommunikationssystem spielt der Anschaffungspreis eine untergeordnete Rolle. Entscheidend ist vielmehr, ob die vermeintlichen Ersparnisse bei Billinprodukten hierbei

nicht von den Folgekosten „aufgefresser” werden. Reparaturen oder noch schlimmere Ersatzinvestitionen verschlingen oft noch einmal den gleichhen Betrag der eigentlich budgetiert war und kosten Zeit.

Ceotronics und Soldaten im gleichen Boot.

Die optimale technische Ausstatung der Streitkräfte weltweit mit Kommunikationssystemen ist sehr wichtig.
Daher haben wir extra die Stelle des Produktmanagers Streitkräfte und Behörden geschaffen. Dieser berät die Entscheidungsträger beim Militär; individuell bei der Anschaffung von Audio-Video und Data-Kommunkationssystemen. Ebenso ist er direkter Ansprechpartner für Anregungen von Produktverbesserungen und Neuentwicklungen. Nur durch Investitionsentscheidungen, die Konsequenzen auf mehreren Ebenen berücksichtigen, kann es gelingen, die notwendige Ausrüstung der Streitkräfte zu erreichen. Entscheidungen sind gefragt die auf lange Sicht den Soldaten dienen und die optimale Sicherheit dieser gewährleisten.

Hóka Miklós

NEW CHALLANGES AND POSSIBILITIES IN RADIO COMMUNICATION

(The Joint Tactical Radio System)

Introduction

The move toward digitization, in several country's military has resulted over the last years in the development of a variety of new operational architectures and warfighting strategies. In such strategies as the Joint Vision 2010, Network-Centric Warfare, Tactical Internet/Digitized Battlefield, and nowadays the new Joint Vision 2020, the traditional focus of military operations is changing. There is an increasing emphasis on alternative military operations - joint/coalition operations, humanitarian efforts, peacekeeping missions, and other operations not traditionally associated with wartime. These new paradigms make new demands on the military particularly by:

- emphasizing interoperability;
- requiring flexible force structures;
- needing small logistics tails;
- being Command, Control and Communications (C3) intensive, including an emphasis on services such as situational awareness, precision targeting, and rapid tasking of assets; and
- networking and information transfer between disparate systems.

The Joint Tactical Radio System

This new goals and „visions" needed is to develop a family of affordable, high-capacity tactical radios to provide both line-of-sight and beyond-line-of-sight Command, Control, Communications, Computers and Intelligence (C4I) capabilities to the warfighters. This family of radios will cover an operating spectrum from 2 to 2000 MHz initially, and will be capable of transmitting voice, data and video. However, the Joint Tactical Radio System (JTRS) is not a one-size-fits-all system. Rather, it is a family of radios that are interoperable, affordable and scaleable. By building upon a common open architecture, JTRS will improve interoperability by providing the ability to share waveform software between radios, even radios in different physical domains.
The goal of the JTRS Joint Program Office (JPO) is to migrate today's legacy systems to systems compliant with the JTRS architecture. Legacy systems are typically single band, single mode radios that have limited or no networking capability. Consequently, legacy systems require complex solutions to be integrated into networks. Furthermore, the use of proprietary standards complicates interoperability. The solution is to migrate all legacy systems to

the JTRS open systems architecture. This will be a phased implementation that balances operational requirements, weapon system integration issues and funding constraints.

New technologies

The term "software radio" was coined in 1991 to signal the shift from the hardware-intensive digital radios of the 1980's to the multi-band multi-mode software-based radios planned for the year 2000 and beyond. Software programmable radio technology offers numerous advantages over the inflexible implementation of previous radio designs. It allows for improvements or enhancements without altering the radio hardware. It also allows users to acquire relatively generic hardware and tailor its capabilities to their individual needs by choosing software that fits their specific application; this is analogous to the flexibility inherent in today's personal computers.

This shift to software-based radios results from the advent and improvement of a variety of technologies, including:

- Increased speed and power of embedded processors, enabling modem functions to be performed by Digital Signal Processors (DSPs);
- Improved Analog-to-Digital Converters (ADCs), with higher conversion rates and increased dynamic operating ranges; and
- The development of object-oriented programming technologies, such as CORBA middleware, that permit software functionality to be independent of the underlying hardware.

These and other technologies have allowed high-performance software-based radios to become a reality.

Definition of a Software Radio

A radio performs a variety of functions in the process of converting voice or data information to and from a Radio Frequency (RF) signal. Nominally, these functions include:

- Processing the analog RF signal (e.g., amplification/deamplification, converting to/from Intermediate Frequencies (IFs), filtering, etc.);
- Waveform modulation/demodulation (including error correction, interleaving, etc.); and
- Processing of the baseband signal (e.g., adding networking protocols, routing to output devices, etc.).

A software radio is a radio whose waveform modulation/demodulation functions are defined in software. For a transmitter, this means that waveforms are generated as sampled digital signals, converted from digital to analog via a wideband Digital-to-Analog Converter (DAC), and then upconverted (possibly through an IF) to RF. Similarly, a receiver employs a wideband Analog-to-

Digital Converter (ADC) that captures all of the channels of the software radio node. The receiver then extracts, downconverts, and demodulates the waveform digitally. Software radios employ a combination of techniques that include multi-band antennas and Radio Frequency (RF) conversion, wide-band digital-to-analog, IF, and analog-to-digital conversion, base-band and digital signal processing functions.

Definition of an Architecture

The foundation of a software radio design, as with any digital system, is the architecture. This is especially true for the JTRS effort, as the architecture will be common, open, and used in a wide range of implementations. The term architecture can refer to either hardware or software; it may also refer to a combination of the two. The architecture of a system always defines its broad outlines and may define precise mechanisms as well. It contains the description of elements from which a system is built, the interactions that occur between those elements, the patterns that guide their composition, and the constraints imposed on those patterns. It describes a collection of components and their interactions - showing the topology of the system. It shows how different system elements correspond with one another to deliver the required system operational characteristics. Finally, it provides a rationale for design decisions and establishes the nature of the assumptions implicit in those decisions.

Architectures are comprised of three basic building blocks:

- Components (hardware and software) - the elements that form the foundation of re-use among a family of radios;
- Rules of composition - define and describe what components can fit together and how they fit together; and
- Rules of behavior - provide the semantics for the system, defining both the behaviors of components and the way they interact with one another.

The new warfighting paradigms, such as Joint Vision 2020, emphasize mobile, flexible networks that automatically adapt to the warfighter's needs. These paradigms, as expressed in the JTRS ORD, require mobile networking capabilities significantly beyond what is possible with currently fielded technology. JTRS networking protocols must support a variety of services, including automatic neighbor and link quality discovery, automatic network reconfiguration, quality-of-service guarantees, precedence and priority marking, and the automatic routing and relaying of traffic. In addition, these services must be supplied with efficient protocols that minimize overhead. The development and implementation of mobile networking protocols is a technical challenge to the JTRS effort. Current military networking technology predominately gives static, pre-planned legacy networks with only modest

capabilities for adaptation and forwarding between networks via gateways. Furthermore, commercial networking technology relies on significant fixed infrastructure to support mobile users, and it is unlikely that protocols meeting future military needs will result directly from commercial technologies.

Spectrum Management

The JTRS ORD requires that JTRS technologies support implementations that operate across the entire frequency range of 2 MHz to 2 GHz (although some implementations may only operate across portions of this range). However, the 2 MHz to 2 GHz portion of the electromagnetic spectrum is also used by commercial, civil, and other military systems. Under current spectrum management policy, spectrum usage must be allocated by spectrum management agencies to potential users before systems can transmit. Spectrum allocation is granted to military users only after extensive analysis, testing, and coordination with civilian and international agencies. In addition, spectrum allocation is often granted only on a restricted, temporary, or conditional basis. For instance, the use of L-band systems such as Link 16 and EPLRS are usually restricted or forbidden, except in small geographical areas under tight constraints, because of the possibility of interference with civilian air traffic control systems. The unprecedented capabilities of JTRS implementations give rise to several technological challenges, including the following:

- Each JTRS implementation type will have unique hardware, and in some cases, unique legacy waveform software. Under current spectrum management guidelines, each JTRS implementation would have to go through the entire spectrum allocation process for each legacy waveform. As implementations will generally include multiple legacy waveforms, this requirement likely places untenable testing and administrative burdens on JTRS implementations.

- Currently, operational compliance with spectrum allocation constraints is usually straightforward, as DoD receives a blanket allocation for a particular waveform. However, in some cases, allocations involve time and space limitations or other constraints that can make compliance operationally difficult. An example of this is Link 16, where usage must be tightly coordinated with civil authorities and other Link 16 users. JTRS implementations will be able to transmit over a wide range of frequencies, and this flexibility may make operational compliance significantly more problematic.

- Because JTRS waveforms reside in software modules, characteristics such as frequency, modulation scheme, and hopping pattern can be easily modified, perhaps to meet more stringent performance requirements or threat conditions. However, under current spectrum

management procedures, each modification of this type would require a new allocation permit, with attendant analysis, testing, and coordination among civil and international agencies. This would negate a significant new capability that will likely offer tremendous benefit to military users.

The Software Communications Architecture (SCA)

The JTRS effort will result in a family of tactical software radios, all built upon a common, open architecture. In view of its potential applicability across a wide range of communications devices, this architecture is known as the Software Communications Architecture (SCA). In addition to its use in JTRS applications, the SCA has been advocated as a standard for use in commercial applications by the Software Defined Radio (SDR) Forum. The SCA is currently under development, based on an initial baseline SCA framework established by the JTRS JPO.

SCA Goals

The JTRS requirements are promulgated in the JTRS Operational Requirements Document (ORD), itself derived from the JTRS Mission Needs Statement (MNS). These documents place stringent operational requirements on JTRS implementations, presenting significant technical challenges to the JTRS developers. Since no single implementation is capable of meeting all of the ORD requirements, JTRS is envisioned as a family of radios based upon a common architecture.

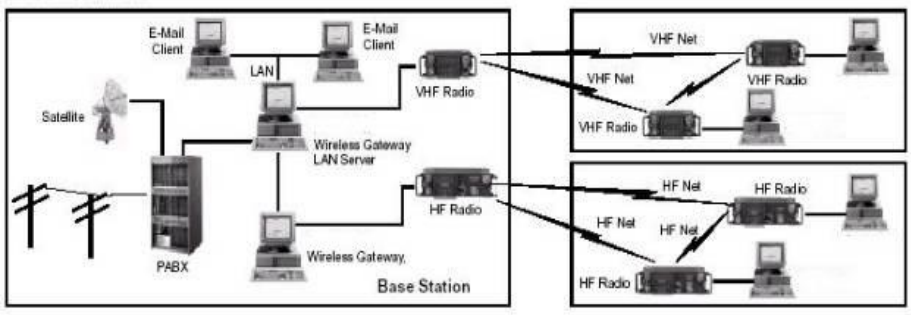


Figure 1. Sample Application of software radios

The ORD requirements for scalability, portability of waveforms and extensibility as technology evolves drive the need for a common Software Communications Architecture (SCA). These over-arching ORD requirements and the important technical requirements of radios impact the nature of this architecture and drive the technology solutions that will be employed to meet the needs of the JTRS users. The Table summarizes the eight goals to be met by the SCA.

Architecture Goal	Goal Description
1. Common Open Architecture	The use of an open, standardized architecture has the advantages of promoting competition, interoperability, technology insertion, quick upgrades, software reuse, extendibility, and scalability
2. Multiple Domains	The JTRS family of radios must be able to support operations in a wide variety of domains - airborne, fixed, maritime, vehicular, dismounted, and handheld
3. Multiple Bands, Multiple Modes	A JTRS radio replace a number of radios currently being over a wide range of frequencies - from 2 MHz to 2 GHz and to interoperate with radios operating in disparate portions of that spectrum. Cross-banding between modes and waveforms will be essential to ensure radio interoperability.
4. Compatibility with Legacy Systems	It is crucial that the JTRS architecture be developed so that JTRS implementations are capable of smoothly interacting with a wide variety of legacy equipment. This will require minimizing the impact of platform integration
5. Technology Insertion	The JTRS architecture must enable technology insertion, in which new technologies can be incorporated to improve performance, reduce cost and time to field, prevent obsolescence, and keep pace with commercial technologies.
6. Security	The JTRS architecture provides the basis for solving a number of long-standing issues related to tactical communications systems security: a programmable cryptographic capability, multiple independent levels of classification, streamlined security certification, and infrastructure elements include key management, software management, certificate management, and user identification and authentication.
7. Networking	JTRS architecture will also support emerging wideband networking capabilities for voice, data, and video.
8. Software Re-use / Common Waveform Software	The JTRS architecture should allow for the maximum possible reuse of software. The JTRS architecture will allow for the use of common waveform software among various implementations, with waveforms being portable from one implementation to the next.

Glossary

So that all concerned are familiar with the industry view of the software radio, the following definitions are provided. These were initially given in a brief to ITU-R TG 8/1 IMT-2000 Workshop, Isle of Jersey, 10 November 98.

Digital Radio - this does not necessarily mean that the radio is a software-defined radio. A radio may be digital but if the processing is performed by special purpose ASICs, it is not a software-defined radio. Even if the ASIC processing is under software control, the radio is not considered a software-defined radio unless the information channel processing is accomplished by software residing in programmable DSP chips.

Software-Defined Radio - a radio, in which the digitization is performed at an IF, may be baseband, for the receiver and at an IF or directly at RF for the transmitter. Conventional analog circuits, LNAs, mixers, Pas, etc. are still required.

Software Radio - a radio in which the digitization is at the antenna and all of the processing is performed by software residing in high-speed digital signal processors.

Bibliography:

1. **JOINT VISION 2020**
   Published by: US Government Printing Office, Washington DC, June 2000, www.dtic,mil/doctrine/jel/index.html
2. DR. DAVID S. ALBERTS :*Operations Other Than War: The Technological Dimension.* Washington, DC: National Defense University Press, 1995.
3. DR. DAVID S. ALBERTS : *Defensive Information Warfare* Washington, DC: National Defense University NDU Press Book 1996
4. DR. DAVID S. ALBERTS: *Network Centric Warfare (NCW)* Washington, DC: National Defense University NDU Press Book 1999
5. JOINT TACTICAL RADIO SYSTEM (JTRS) JOINT CONOPS VERSION 2.0 06/30/2000
6. Joint Tactical Radio System (JTRS) U.S. Army Signal Center and FORT GORDON www.gordon.army.mil/jtrs
7. Joint Tactical Radio (JTR) OPERATIONAL REQUIREMENTS DOCUMENT 23 mar 1998 www.jcs/j6/jtr23_mar

Fekete Károly

TOWARD THE WITHIN OF MILITARY CIS CONVERGENCE (IPV4 AND IPV6)

Key words: military communication system, information system, convergence, Ipv4 and Ipv6

The exponential growth of the various tipe of the communication and information systems in recent years has dramatically increased the demand for higher bandwiths and for attainability in military wide area networks. The recent solution has been to use Asynchronous Transfer Mode (ATM) at 2 Mbit/s (tactical level) to STM-1 (155 Mbit/s)and STM-4 (622 Mbit/s) (strategical level) rates.

The most efficient and perspective solution in military Communication and Information Systems (CIS) to support of military subscribers with high Quality of Services are ATM and the such new technologies as LAN Emulation, Voice over Internet protocol (VoIP) and Classical Internet Protocol over ATM (IPo-ATM).

The milestones of the Internet:

1971-The DARPA ARPANET becomes operational using Network Control Protocol (NCP).
1973-Development of the Internet Protocol version 4 (IPv4) begins.
1978-Principal Deputy Under Secretary of Defense for Research and Engineering (USDR&E), Gerald P. Dinneen, mandates the use of IPv4 for all DoD packet-oriented data networks.
1981-Plan for transitioning the ARPANET to TCP/IPv4 is published.
1983-The transition of the ARPANET to IPv4 was completed on January 1.
1983-IPv4 and TCP become MIL-STD-1777 and MIL-STD-1778 respectively.
1983-National Research Council Committee on Computer-Computer Communications Protocols is formed to arbitrate differences between the National Bureau of Standards (NBS) and the Department of Defense (DoD) on data communications protocols.
1985-The NRC committee recommends DOD move toward adoption of the OSI protocols as a co-standard with IPv4.
1987-ASDC3I, Donald C. Latham, mandates the use OSI protocols as a replacement for IPv4 within two years of the finalization of the federal Government Open Systems Interconnection Profile (GOSIP). Interoperation with existing IPv4 systems for their expected life times was also required.

1990-Internet governance transitions to the Commerce department andthe ARPANET is replaced by the National Science Foundation Network (NSFNET).
1992-Congress passes the Scientific and Advanced-Technology Act of 1992 allowing, for the first time, commercial traffic on the Internet.
1993-IP: Next Generation (IPng) White Paper Solicitation published in the IETF.
1994-IPNG protocol shoot-off.
1995-Dr. Steven Deering publishes the Internet Protocol, Version 6 (IPv6) Specification for the first time.
1998-Internet Corporation for Assigned Names and Numbers (ICANN) is formed to take over Internet administrative functions from the United States government.
2001-The Internet contains 120+ million hosts in 50+ countries worldwide.

Internet Trends

Because the underlaying infrastructure provided by carriers is Synchronous Digital Hierarchy (SDH) or Synchronous Optical Network (SONET) deployed over wide area fiber links, interest has grown in the IP. *"During the 11 September 2001 major terrorist attack on the United States, the Internet demonstrated that is capable of fulfilling its function as a means of communication during crisis. It must be considered an integral component of every communication infrastructure."*[1]

As we can see the most important characteristic of evolution of Internet are:

- Dramatic growth in the number of Internet connected devices.
- Accelerated technology development and deployment.
- Internet privatization and internationalization
- Proliferation of strong commercial encryption.
- Proliferation of 'Always On' and mobile internetworking.
- Proliferation of Quality of Service (QoS) and multicast

The Fig. 1. shows the number of the Internet is growing at a ridiculouslly fast rate but the number of available Internet Protocol version 4 (Ipv4) addresses is limited.

[1] Maurene Grey, Robert Batchelder, Joyce Graff: The Day the Internet Grew Up, 11 September 2001, Gartner, http://www3.gartner.com

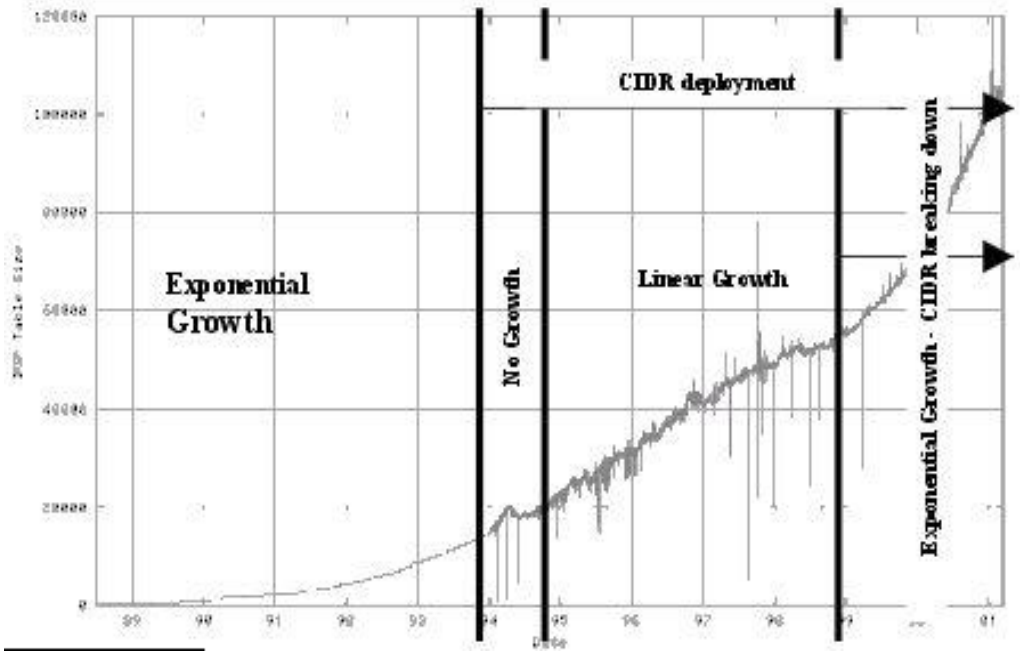


Fig. 1. The trends of Internet expansion in the last years. CIDR (Classless Inter-Domain Routing)

(Source: http://www.telstra.net/ops/bgptable.html)

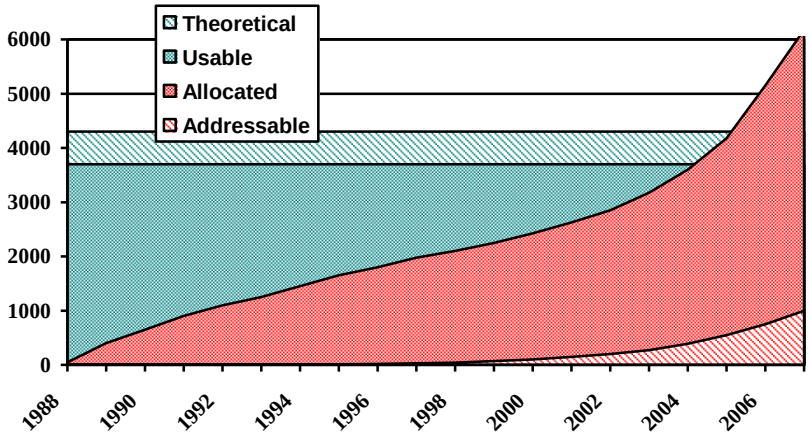


Fig. 2. The formation of theoretical, usable, allocated and addressable fields of Ipv4

As we know in 1990 IPv4 addresses being consumed at an alarming rate, projections show:

- Class B address space exhausted by 1994
- All IPv4 address space exhausted between 2005 – 2011 (Fig. 2.)

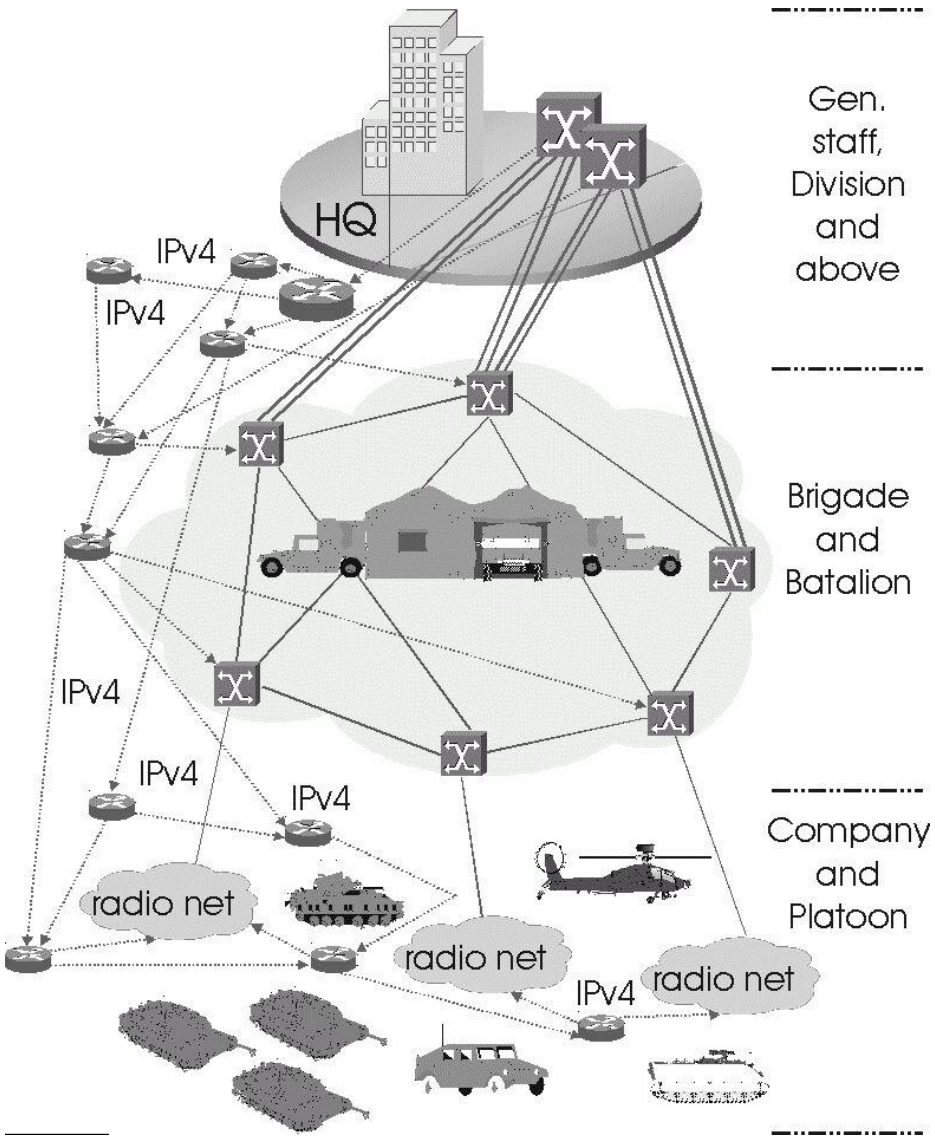


Fig. 3. The limited size of on line contact between of echelons based on Ipv4

Regarding to most military information applications they are principally client-server in nature for many reasons including IPv4 address deple-

tion/conservation. IPv4 Internet can't satisfy one or more of the requirements of many online military applications.

IPv4 Internet limits the size of the online contact in military CIS because of it's well known limitations on scalability and accessibility (Fig. 3.).

There are additional Telecommunication Management Network (TMN) problems with IP today.

The system administration is big enough and the military subscriber networks cannot be dynamically renumbered or configured. The security in CIS is optional; no single standard, no support for new protocols and difficult to add to the base IPv4 technology.

Interim measures helped, but address space consumption slowed, meanwhile Internet growth accelerated. Everything wanted to go to the Internet (1Billion mobile and Internet users by 2005). 90% of all new mobile phones will have Internet access by 2003.[2]

There are a lot of demands in front of Internet services in military CIS. The Internet products and services must be able to utilize the *full peer-to-peer capabilities of TCP/IP*, and must *scale* to many geographically distributed military subscribers. The military IP devices and services must have access to *strong security mechanisms* for authentication, data privacy and must support both *fixed and mobile* Internet devices such as special military sensors, cameras and LANs (Fig. 4.).

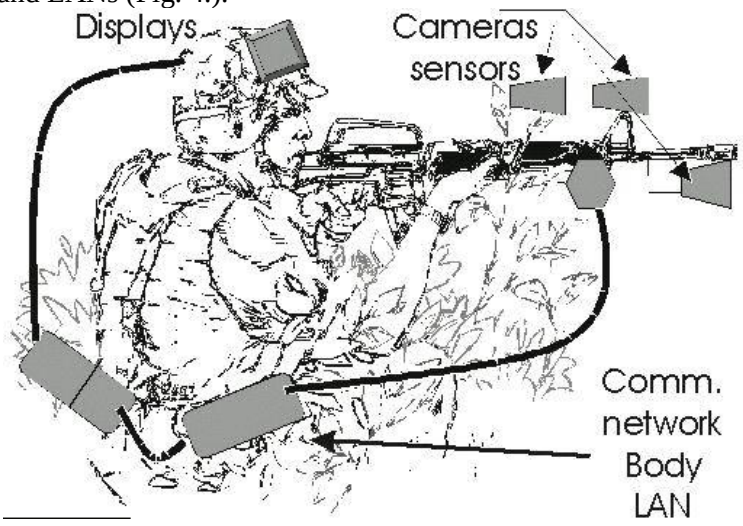


Fig. 4. Body LAN –as element of possible IP devices

In the application of military environment the products and services should be *cost-effective* to develop, test, deploy, and maintain and should be *afforda-*

[2] (Morgan Stanley Dean Witter, May 2000)

ble to the vast majority of NATO member-states. The instruments should require *little or no military user configuration* to effectively use and should utilize *open industry (ITU, RFC) and NATO (STANAG, EUROCOM) standards* to the greatest extent possible for extensibility.

Ipv6

Planning, designing and implementing common network infrastructures that support voice, data and multimedia services are critcal in military CIS in today's and tomorrow's environment. IP based technology is enabling the development of common integrated CIS network infrastructure for transporting any kind of military applications (Fig 5.).

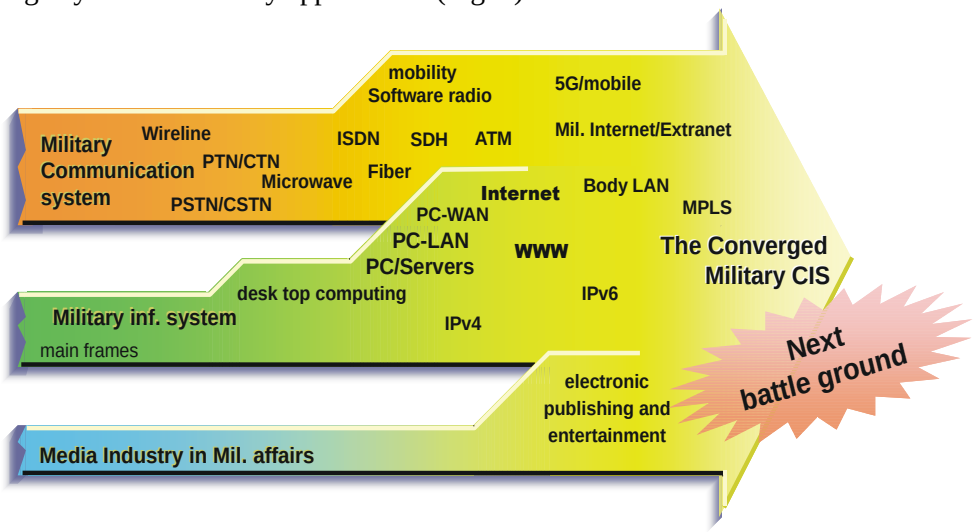


Fig. 5. Convergence in the field of military CIS

Considering the process of convergence there are some technical requirements of military CIS based on IP. The CIS must be able to utilize the full peer-to-peer capabilities of TCP/IP, and must possess real-time performance (typically <100 ms) where necessary to satisfy human perception or where required by the military application. CIS networks must utilize QoS and or resource reservation when real-time performance is required by the any application.

The products and services in CIS must *efficiently distribute information* to all subscribers and must have access to *strong security mechanisms* for authentication and data privacy. Commmunication and information services must possess *low packet loss* (typically <2%) and *low packet jitter*.

IPv6 Base Technology

The economic advantages of packet voice are driving both access and core voice networks away from circuit switching *towards packet*. The military communication and information specialists continues to debate whether the

future of these packets networks will based on ATM, pure IP, IPoATM, Internet Protocol over MultiProtocol Label Switching (IPoMPLS) or a combination thereof.

The Ipv6 has got the next Design Philosophy (Table 1.):

- Recognizable yet simplified header format
- Reduce common-case processing cost of packet handling
- Keep bandwidth overhead low in spite of increased size of the address
- Flexible and extensible support for option headers
- Design optimised for 64-bit architecture
- Headers are 64-bit aligned
- Fixed Size IPv6 Header
- Unlike IPv4 - Options not limited at 40 bytes
- Fewer fields in basic header
- faster processing of basic packets
- 64 Bit Alignment Header/Options
- Efficient option processing
- Option fields processed only when present
- Processing of most options limited performed only at destination

Table 1.

FEATURE	**IPv4**	**IPv6**
Address Length	32 bits	128 bits
IPSec Support	Optional	Required
QoS Support	Some	Better
Header Checksum	Yes	No
Link-Layer Address Resolution	ARP	Multicast Neighbor Discovery Messages
Uses Broadcast	Yes	No
Configuration	Manual	Automatic
Minimum MTU	576 Bytes	1280 Bytes

Accordintg to the Addressing Model (RFC 2373) of IPv6 the addresses assigned to interfaces (No change from IPv4 model) and interfaces typically have multiple addresses. The subnets associated with single link3. The IPv6 addresses have scope and lifetime. From point of view of Ipv6 TMN the IP address provides “Plug-and-Play” and Autoconfiguration capability. IPv6 Mobility is based on the base IPv6 was designed to support Mobility.

[3] A link is a link-layer (layer 2) domain e.g. LAN and the Multiple subnets on same link

Today, normal traffic on the Internet is transmitted in the clear, unencrypted. It is transmitted in standard formats using public protocols. It passes through switches and communication facilites that are publicly accessible. Under such conditions, almost any kind of attack is feasible. IPv6 mandates IP security and security features are standardized. All implementations must offer them extensions to the IP protocol suite (RFC 2401) authentication (packet signing) and encryption (data confidentiality). The defence in Ipv6 operates at the IP layer (so invisible to applications), protects all upper layer protocols and both end-to-end and router-to-router ("secure gateway"). IPv6 could provide robust and flexible security mechanisms when required.

IPv6 could bring about an explosion in the converged CIS by connecting every military subscibers, anywhere, independently from *Fixed and or Mobile* with efficient and scaleable transport services.

IPv6 could support cost-effective development of new and innovative military CIS applications (multimedia, body LAN, etc.).

IPv6, a Technical Solution for Future Military CIS

All the technical requirements for future military CIS can be satisfied, in the general case, with *the use of IPv6, IPsec, broadband, and with good design and management of CIS infrastructure and resources* (Fig. 6.). The technical requirements for future CIS cannot be satisfied, again in the general case, with the use of IPv4 or even a transitional IPv4/IPv6 gaming infrastructure. Protocol Translators, proxies, firewalls and other such "inline" devices will typically violate one or more of the technical requirements and add single points of failure, performance bottlenecks, and complexity.

The considerations of applications of Ipv6 in military CIS:

- Commercial of the Self (COTS) and Governmental of the Self GOTS software upgrades required
- CIS infrastructure upgrades, transition and interoperability testing may be required
- Increased support costs during the CIS upgrade.
- Evolving a prototype joint architecture.
- Interoperability with allies, coalition partners, government agencies, contractors, research institutions, and potential adversaries.

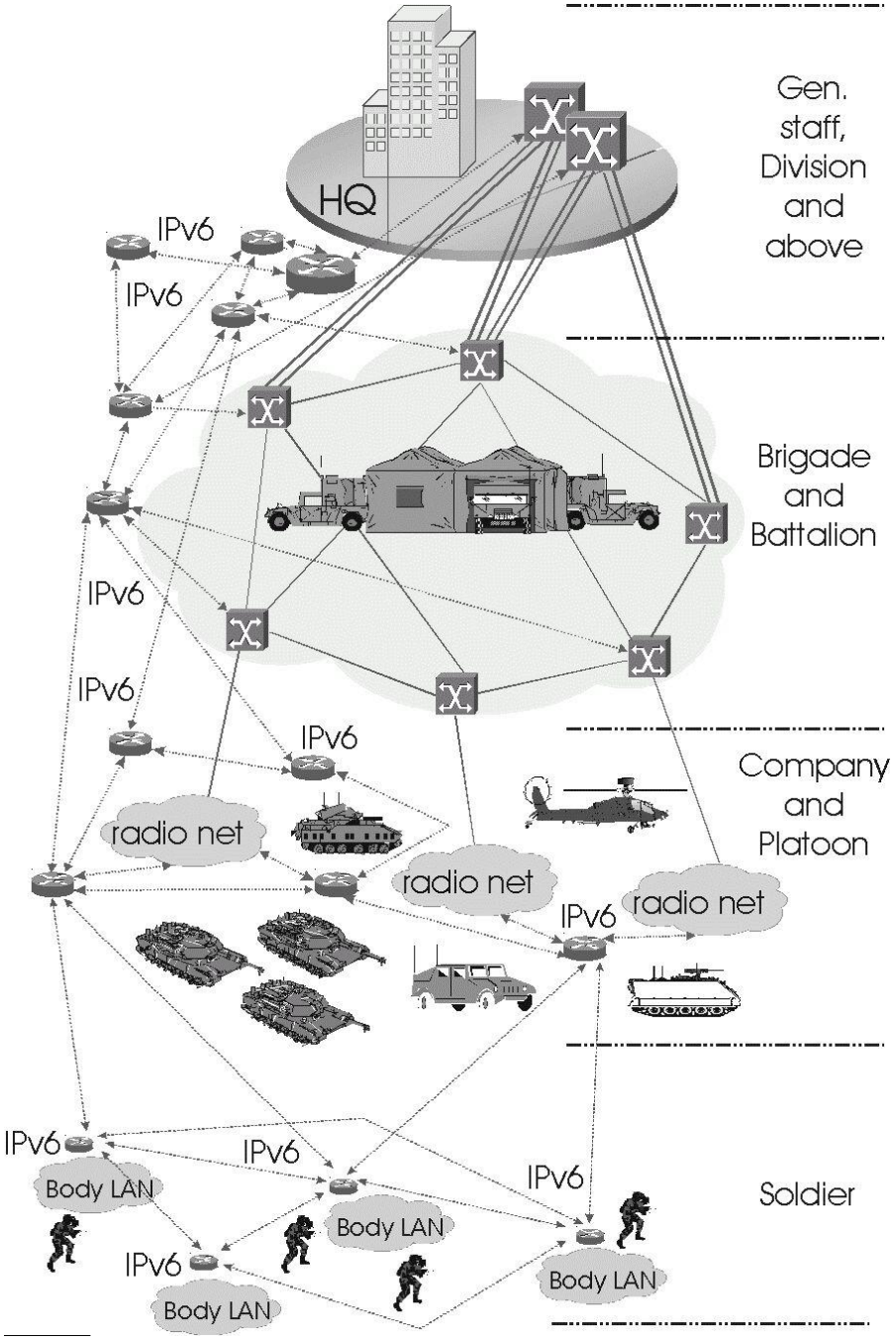


Fig. 6. The Ipv6 based CIS part with cooperation of strategical, mobile and tactical military CIS

References:

1. Maurene Grey, Robert Batchelder, Joyce Graff: The Day the Internet Grew Up, 11 September 2001, Gartner, http://www3.gartner.com
2. Simulation Interoperability Standardization Organization (SISO), http://www.sisostd.org/content.htm
3. Institute of Electrical and Electronics Engineers (IEEE), http://www.ieee.org
4. Federal Networking Council Resolution: Definition of "Internet", Oct. 24, 1995., HTTP://www.fnc.gov/Internet_res.html
5. Matáv-PanTel: Összekapcsolt hálózatok, VGA Monitor, 2001 október 12, pp. 4.
6. Scott Phillips: IP The Next Generation,
7. S. Bradner, A. Mankin: The Reccommendation for the IP Next Generation Protocol, RFC 1752, January 1995.
8. Robert E. Larson: Methods for Implementing IP on ATM Networks

Dr. Mezey Gyula

SECURITY AND DISTRIBUTED SYSTEMS

Zrínyi Miklós National Defence University
Budapest, Hungária krt.9-11.
MEZEY@ZMNE.HU

Key words: Structure of security objectives, security policies, security mechanisms.

1. Objectives

Security objectives: they are interdependent and cannot be taken in isolation.

Network (simplified hierarchical) structure exist among the objectives as follows :

Primary objectives: applicable both to stored data and messages in transit

Data confidentiality (based on access control),

Integrity (based on access control),

Availability (based on access control),

Primary communication objectives: applicable to communication between users/programs

Authentication (based on access control to protect the password file and encryption-based confidentiality if the access control fails)

Non-repudiation (based on identity authentication)

Secondary objectives: Access control (based on identity authentication)

Audit trail (based on identity authentication)

Security alarm

2. Security policies

2.1. Security policy

With regard to security risks an organization's security policy plans for dealing with those risks in accordance with the overall high-level security objectives of the respective organization. Main issues of the plan :What assets are to be protected (see 3.4. access control),

What are the threats to these assets,

Which threats are to be eliminated.

2.2. Security interaction policy :

Security interface acceptable to, and agreed upon by all parties in an interaction within the organization. These are important, because the information systems in an organisation are generally heterogeneous, incompatible and operated to a variety of security policies, instead of a centrally managed policy and standards.

2.2. Inter-organizational security interaction policy :

If at least one of the parties is from outside the organization.

3. Security mechanisms

3.1. Physical security mechanisms

Physical, electronic, and human security of components of the system :

Physical security of components of the system : Preventive measures (phys.access control)

Detection and deterrence,

Recovery

Electronic security of components of the system :Prevention against interference/Malfunction

Electromagnetic radiation/Passive eavesdropping The solution is tempest proofing devices

Human security : Regime measures. Not tackled here

3.2. Communication security mechanisms

Traffic padding : mainly in military systems

Encryption :

Link encryption : covers only the communication links, but not the processors

End-to-end encryption : directly between only the initiating and target systems

Network encryption : covers a whole network, but not the gateways

By hardware unit : the link to the unit is not covered, so physical protection needed

Encryption **algorithms** :

Symmetric (a single secret) key /difficult key management/

PKI asymmetric (a related pair of keys, the encrypting key is public, so key management is easier, although the decrypting key is secret)

Hibrid systems (PKI for key distribution, symmetric key for message security)

3.3. Authentication mechanisms

User authentication : verifying the claimed identity of a human user based on some

Information known only to the human beeing (passwords, etc) or

Tokens (one-time password generator, card,) in only possession

Person's characteristics (signature, fingerprint, etc).

In open distributed systems there needs to be a **system** AC policy. It has two main prerequisits :Unique user identifiersandUser authentication.

Normal users logging in from terminals and workstations within the organization premises tipically use passwords, and system AC policy focuses standards for passwords.

But in case (whether staff or external) logging in from outside the organization premises a higher level (one-time password generator) of authentication is required.

Message authentication : verifying the claimed originator and non-alteration of a message

Message authentication code (MAC)

Using asymmetric keys non-repudiation is met as well (based on identity authentication)

Data AC policy has four prerequisits :

- All of the organization's data are protected by logical access control (AC)
- Access is permitted only when authorized by the data owner
- Definition of ownership of all elements of the organization's data
- The strength of AC protection is defined according to a decision.

3.4. Logical access control mechanisms

In case of multi-user systems physical access control is impossible. A security policy on the low-level is specified as a set of logical access control rules (AR).

An AR states what (O) operations are permitted between two domains (U=users, T=target objects) of elements in the system. In addition to an existing AR, compatibility between the interfaces of T and U is also necessary.

An AR states that any user in the U domain is authorized to perform any element in the O operation set on any of the target objects of the T domain. An AR names neither the users, nor the target objects, so the allowed in case of a particular user to a particular object is not in the relation. Instead, an AR is formulated using domain names so that the AR remains stabil and valid for the present members of the domains, and not affected by the changes in the the domain membership.

An operation request is authorized if and only if at least an AR exist which applies to it. No default access is allowed to users.

But some compound operations may require more than one AR-s.

It is also possible, that more than one AR satisfies the request and that becomes important when a user access grant is removed. It may be not enough to remove only the obvious AR.

Access permissions are granted or removed by AR operations. Permitted AR-operations themselves are controlled by AC (or authorization) policy constraints (which are also AR-s). So all in all, access control (AC) policy is represented by a set of 3-relation (U,O,T) triples. The set of AR-s was characterized by TCSEC (1985 DoD) as:

Discretionary or mandatory.

- Discretionary AC : allows users to specify and control sharing of objects with other users. AR-s in the system – and so the AC policy itself - may be altered.
- Mandatory AC : AR-s are built into the system and cannot be altered, except by installing a new version of the system. The set of built in AR-s applies universally and has priority over all other (discretionary AC) policies in the system, if any.

Implementation of the AR-s can be : ACL (access control lists)
orauthenticated capabilities (tokens, passwords, etc)
or an authorization server.

Ferenc Kubinszky4, Zoltán Lázár5

PERFORMANCE ANALYSIS OF IEEE 802.11 BASED AD HOC NETWORKS

Technical University of Budapest
Depatment of Microwave Telecommunications
Wireless Information Technology Lab[6]

Abstract

The original motivations for mobile adhoc network are found in the military need for battlefield survivability. In battlefield environment the military cannot rely on access to a fixed, preplaced communications infrastructure. Due to this technology if the participating nodes which communicate with other nodes are not in the communication range or not in the line of sight they use a multihop (store-and-forward) packet routing to exchange messages between the users. Our goal is to demonstrate the feature of multihop wireless networks. This is why performance analysis and scalability tests were done.

Introduction

Within the last few years there has been a surge of interest in mobile ad hoc networks (MANET). A MANET is defined as a collection of mobile platforms or nodes where each node is free to move about arbitrarily. Each node logically consists of a router that may have multiple hosts and that also may have multiple wireless communications devices. The term of MANET describes distributed, mobile wireless, multihop networks that operate without the benefit of any existing infrastructure except for the nodes themselves.

The acronym MANET is relatively new, but the concept of mobile packet radio networks, where every node in the network is mobile and where wireless multihop (store-and-forward) routing is utilised, is not. Since the early 1970s, not long after the initial development of the packet switching technology that grew into what we now know as the internet, the U.S. Department of Defense (DoD) sponsored research to enable packet switching technology to operate without the restrictions of fixed or wired infrastructure.

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

Motivation to develop MANET

One of the original motivations for MANET is found in the military need for battlefield survivability. To survive under battlefield conditions, warfighters and their mobile platforms must be able to move about freely without any of the restrictions imposed by wired communication devices. Thus, the need for battlefield survivability translates into a mobile wireless communications system for coordinating group actions which operates in a distributed manner, avoiding single points of failure such as centralised control stations.

An additional motivation for MANET is that the military cannot rely on access to a fixed, preplaced communications infrastructure in battlefield environment. In some regions there is no terrestrial communications infrastructure (desert, jungle). In the other regions, access is unavailable because of destruction of or damage to the local communications infrastructure.

The third motivation is the store-and-forward principle. If the nodes which communicate with each other are not in communication range or not in the line of sight a multihop (store-and-forward) packet routing must be used to exchange messages between the users.

History

Packet switching technology, first demonstrated by the ARPANet in the 1960s, provided great promise for dinamically sharing bandwidth among multiple users, and it offered a means for adaptive routing traffic in response to changing network conditions and user demands. Recognising the advantages of packet switching in a mobile wireless environment, in 1972 DARPA initiated a research effort to develop and demonstrate a packet radio network (PRNet). The PRNet was to provide an efficient means of sharing a broadcast radio channel as well as coping with changing and incomplete connectivity.

DARPA Packet Radio Network

In 1972, when the DARPA PRNet program was initiated, packet switching had just recently been demonstrated as an efficient means for sharing bandwidth using store-and-forward routing to provide reliable computer communications. Although the initial PRNet protocols used a centralised control station, the core PRNet concept quickly evolved into a distributed architecture consisting of a network of broadcast radios with minimal central control, using multihop store-and-forward routing techniques to create end-

user connectivity from incomplete radio connectivity. Broadcast radios were used for three reasons:

- Mobile user do not need pointing antennas
- The simpler channel management in that no coordinated frequency allocations are needed beyond the setting of the frequency for the network
- Theoretical results indicated that for bursty traffic it is better to share a larger channel dynamically than to divide it into subchannels

The PRNet used a combination of the Aloha and Carrier Sense Multiple Access approaches. The spread spectrum approach helped mitigate multipath fading and aided in discriminating between signals from different radios. The challenge was then to develop network management algorithm that would provide the needed connectivity assessment, route determination, and packet forwarding functions in a continually changing environment with no centralised control.

The initial version of the radios and associated controllers were large, power hungry and limited in their processing. Due to this reasons the DARPA initiated the Survivable Radio Networks (SURAN) program in 1983.

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 some 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 because the nodes usually are 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. Some digital security and privacy keys are needed for these applications.

IEEE 802.11 wireless standard

The IEEE 802.11 standard deals with wireless LANs by defining Physical Layer (PHY) options for wireless transmission and the Medium Access Control (MAC) layer protocol. The PHY layer corresponds directly to the lowest layer defined by the International Standards Organisation in its 7-layer Open System Interconnect (OSI) network model. The MAC layers corresponds to the lower half of the second layer of that same model with Logical Link Control (LLC) functions making the upper half of OSI layer 2.

The IEEE 802.11 standard defines the protocol for two types of networks: Ad-hoc and client/server networks. An Ad-hoc network is a simple network where communications are established between multiple stations in a given coverage area without the use of an access point or server. The standard specifies the etiquette that each station must observe so that they all have fair access to the wireless media. It provides methods for arbitrating requests to use the media to ensure that throughput is maximised for all of the users in the base service set. The client/server network uses an access point that controls the allocation of transmit time for all stations and allows mobile stations to roam. The access point is used to handle traffic from the mobile radio to the wired or wireless backbone of the client/server network. This arrangement allows for point coordination of all of the stations in the basic service area and ensures proper handling of the data traffic. The access point routes data between the stations and other wireless stations or to and from the network server.

The fundamental access method of the 802.11 MAC is known as Carrier Sense Multiple Access with collision avoidance, or CSMA/CA. CSMA/CA works by a "listen before talk scheme". This means that a station must first check the radio channel to determine if another station is transmitting. If the medium is not busy, transmission may proceed. The CSMA/CA scheme implements a minimum time gap between frames from a given user. Once a frame has been sent from a given transmitting station, that station must wait until the time gap is up to try to transmit again. Once the time has passed, the station selects a random amount of time (called a back off interval) to wait before "listening" again, to verify a clear channel on which to transmit. If the channel is still busy, another back off interval is selected that is less than the first. This process is repeated until the waiting time approaches zero and the station is allowed to transmit. This type of multiple access ensures fair channel sharing while avoiding collisions.

At the physical layer, two RF transmission methods and one infrared are defined. Operation of the WLAN in unlicensed RF bands requires spread spectrum modulation to meet the requirements for operation in most countries.

Physical layers

a.) Infra-Red

One infrared standard is supported and it operates in the 850-to-950nm band with peak power of 2 W. The modulation for infrared is accomplished using either 4 or 16-level pulse-positioning modulation. The physical layer supports two data rates; 1 and 2Mbps.

b.) Direct Sequencing Spread Spectrum (DSSS)

The IEEE standard supports DSSS (Direct Sequence Spread Spectrum) for use with DBPSK (Differential Binary Phase Shift Keying) modulation at a 1 Mbps data rate, or DQPSK (Differential Quadrature Phase Shift Keying) modulation at a 2 Mbps data rate. The general band plan consists of five overlapping 26 MHz sub-bands centered at 2.412, 2.427, 2.442, 2.457, and 2.470 GHz. This scheme is used in an attempt to combat interference and selective fading.

The DSSS physical layer uses an 11-bit Barker Sequence to spread the data before it is transmitted. Each bit transmitted is modulated by the 11-bit sequence. This process spreads the RF energy across a wider bandwidth than

would be required to transmit the raw data. The processing gain of the system is defined as 10x the log of the ratio of spreading rate (also know as the chip rate) to the data:

$$10 \log \frac{BW_{chip}}{BW_{data}}$$

The receiver de-spreads the RF input to recover the original data. The advantage of this technique is that it reduces the effect of narrow band sources of interference. This sequence (with the 11bit sequence) provides 10.4dB of processing gain which meets the minimum requirements for the rules set forth by the FCC. The spreading architecture used in the direct sequence physical layer is not to be confused with CDMA. All 802.11 compliant products utilise the same PN code and therefore do not have a set of codes available as it is required for CDMA operation.

c.) Frequency Hopping Spread Spectrum (FHSS)

FHSS (Frequency Hopping Spread Spectrum) is supported under 802.11 with 2-4 level GFSK (Gaussian Frequency Shift Keying) modulation and two hopping patterns with data rates of 1 Mbps and 2 Mbps. Under this scheme, the band is divided into 79 sub-bands with 1 MHz bandwidth each. Each sub-band is subject to a minimum rate of 2.5 hops/s using any of three possible hop patterns (22 hops in a given pattern). The minimum hop rate ensures that each packet sent could be transmitted in a single hop so that destroyed information could be recovered in another hop. This allows an effective frequency diversity that provides excellent transmission characteristics.

Each of the physical layers use their own unique header to synchronise the receiver and to determine signal modulation format and data packet length. The physical layer headers are always transmitted at 1Mbps. Predefined fields in the headers provide the option to increase the data rate to 2 Mbps for the actual data packet.

The MAC layer

The MAC layer specification for 802.11 has similarities to the 802.3 Ether-net wire line standard. The protocol for 802.11 uses a protocol scheme know as carrier-sense, multiple access, collision avoidance (CSMA/CA). This protocol avoids collisions instead of detecting a collision like the algorithm used in 802.3. It is difficult to detect collisions in an RF transmission network

and it is for this reason that collision avoidance is used. The MAC layer operates together with the physical layer by sampling the energy over the medium where transmitting data. The physical layer uses a clear channel assessment (CCA) algorithm to determine if the channel is clear. This is accomplished by measuring the RF energy at the antenna and determining the strength of the received signal. This measured signal is commonly known as RSSI. If the received signal strength is below a specified threshold the channel is declared clear and the MAC layer is given the clear channel status for data transmission. If the RF energy is above the threshold, data transmissions are deferred in accordance with the protocol rules. The standard provides another option for CCA that can be alone or with the RSSI measurement. Carrier sense can be used to determine if the channel is available. This technique is more selective sense since it verifies that the signal is the same carrier type as 802.11 transmitters. The best method to use depends upon the levels of interference in the operating environment. The CSMA/CA protocol allows for options the can minimize collisions by using request to send (RTS), clear-to-send (CTS), data and acknowledge (ACK) transmission frames, in a sequential fashion. Communications is established when one of the wireless nodes sends a short message RTS frame. The RTS frame includes the destination and the length of message. The message duration is known as the network allocation vector (NAV). The NAV alerts all others in the medium, to back off for the duration of the transmission. The receiving station issues a CTS frame which echoes the senders address and the NAV. If the CTS frame is not received, it is assumed that a collision occurred and the RTS process starts over. After the data frame is received, an ACK frame is sent back verifying a successful data transmission.

A common limitation with wireless LAN systems is the "hidden node" problem. This can disrupt 40% or more of the communications in a highly loaded LAN environment. It occurs when there is a station in a service set that cannot detect the transmission of another station to detect that the media is busy. In figure 1 stations A and B can communicate. However an obstruction prevents station C from receiving station A and it cannot determine when the channel is busy. Therefore both stations A and C could try to transmit at the same time to station B. The use of RTS, CTS, Data and ACK sequences helps to prevent the disruptions caused by this problem.

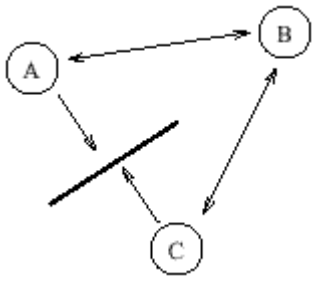


Figure 1.: Hidden node

Security provisions are addressed in the standard as an optional feature for those concerned about eaves dropping. The data security is accomplished by a complex encryption technique know as the Wired Equivalent Privacy Algorithm (WEP). WEP is based on protecting the transmitted data over the RF medium using a 64-bit seed key and the RC4 encryption algorithm. WEP, when enabled, only protects the data packet information and does not protect the physical layer header so that other stations on the network can listen to the control data needed to manage the network. However, the other stations cannot decrypt the data portions of the packet.

Power management is supported at the MAC level for those applications requiring mobility under battery operation. Provisions are made in the protocol for the portable stations to go to low power "sleep" mode during a time interval defined by the base station.

Routing in mobile ad hoc networks

A number of new routing protocols have been developed by considering the MANET attributes. Routing protocols in wired networks generally use link state or distance vector algorithms. Both of them require periodic updates which is not a good idea in a mobile network. In link state routing each router broadcasts to all other routers in the network. In distance vector algorithms each router broadcasts only to its neighbour routers.

There are two main groups of the new protocols in the mobile area, the pro-active and reactive. Pro-active means that the routing protocol constantly tries to track the route changes in the changing network. 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 also known as on-demand protocols.

Dynamic Source Routing (DSR)

Source routing algorithms have been used in wired networks using dynamically built or statically defined routes, and have also been used with statically defined routes in TAPR (Tucson Amateur Packet Radio) wireless networks. In DSR as in all source routing algorithms the sender of a packet determines the complete sequence of nodes through which to forward the packet. The sender puts the list of the route into the header of the packet to identify each node of the hop sequence. In DSR there are no periodic router advertisements, instead when a new route is needed from a host to another, it dynamically determines on cached information and on the result of a route discovery protocol a route to the destination. Since DSR doesn't use any periodic update messages, using it can reduce the network bandwidth overhead especially during periods when there is no significant host movement in the network. By using DSR some battery power can be conserved on the mobile hosts, the mobile devices can put themselves into sleep or power saving mode. In addition, conventional routing protocols may compute some routes which do not work. A radio wave channel might be asymmetric, due to differing propagation or interference patterns.

Basic Operation

To send a packet to another host, the sender constructs a source route in the packet's header, giving the address of each host in the desired route to reach the destination host. The sender transmits the packet to the first hop in the route. When a host receives a packet it simply transmits the packet to the next hop in the source route, except if this host is the destination. Once a packet reaches its destination, it is delivered to the network layer for further processing.

Each mobile host in the ad-hoc network maintains a route cache in which it caches source routes that it has learned. When a host wants to send a packet, it first checks its route cache for a source route to the destination. If a route is found, the sender uses this route to transmit the packet. If no proper route is found, the sender may attempt to discover one by using route discovery. Each entry in the cache has an expiration period, after which the entry is deleted.

Route Discovery

Route discovery allows any host in the ad hoc network to dynamically discover a route in the network, whether the destination is directly reachable or through one or more intermediate hops. When a node needs a new route, it broadcasts a route request packet which may be received by the other nodes in radio transmission range. The route request packet identifies the target host. When a route discovery is successful the source host receives a route reply

packet in which there is a recorded list of the sequence of network hops to the destination named route record. Each route request packet has a unique request id in order to detect duplicate route requests received and to avoid to resend.

Route Maintenance

Since there are no periodic route updates, many mobile networks use hop-by-hop acknowledgment to detect link failures immediately, and may correct the route, or send a route error packet back to the sender.

Ad-hoc On-Demand Distance Vector (AODV) Routing

AODV is also a distance vector algorithm but operates only on-demand. In this protocol there are no periodic route updates as in the conventional distance vector algorithms. The route is only set up when a packet has to be sent from a node to another. The route is maintained by only the nodes between the two end nodes in the path.

The primary objectives of AODV are:

- To broadcast discovery packet only when necessary
- To distinguish between local connectivity management (neighbourhood detection) and general topology maintenance
- To disseminate information about route changes only in local connectivity to those node that need the information

AODV uses a broadcast route discovery mechanism, similar to DSR, but instead of source routing, AODV relies on dynamically established route table entries at intermediate nodes, conserving link bandwidth by reduced packet overhead. To maintain the most recent routing information between nodes, AODV borrows the concept of destination sequence numbers from DSDV. With the combination of these two techniques AODV is band efficient, responsive to topology changes and ensures loop-free routing.

Path Discovery

The Path Discovery process is initiated whenever a node needs to send a packet to another, and it has no routing information in its routing table. Every RREQ (Route Request) packet can be uniquely identified by the following fields:

< source_addr, source_sequence_#, broadcast_id, dest_addr,
dest_sequence_#, hop_cnt >

When a source issues a new broadcast the broadcast_id is incremented. Each neighbour either satisfies the RREQ by sending back a route reply (RREP), or rebroadcasts the RREQ and increments its hop_cnt. When a node receives a RREQ which has been received before, it simply drops it. If a node

cannot satisfy an RREQ, it keeps track of the following information in order to implement the reverse path setup:

- Destination IP address
- Source IP address
- Broadcast_id
- Expiration time for reverse path route entry
- Source node's sequence number.

Reverse Route Setup

Each node receiving an RREQ sets up a reverse route back to the source of the route request to deliver back the route reply (RREP) message. Not all the reverse routes will be used so their lifetime is less than the ordinary route lifetime to be avoid filling up the routing table with unused entries.

In figure 2 there is an ad hoc network formed by eight nodes. Node A wants to send a packet to node E and it has not got the valid route to the destination. A route request is initiated (broadcasted) and it propagates through the network by flooding it. All the nodes receiving the RREQ set up a reverse route to node A pointing to the next hop towards it (this next hop is the prev hop of the RREQ).

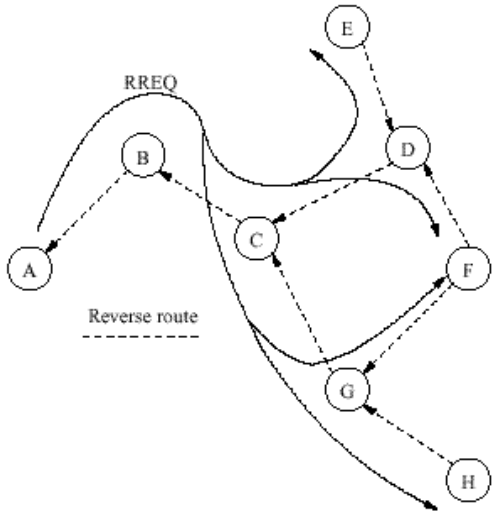


Figure 2.: Reverse route setup in AODV

Forward Route Setup

As the RREQ reaches its destination, or a node which has a valid route to that destination, an RREP will be initiated (unicasted), and sent back along the

reverse route to the original node. Each node receiving the RREP sets up the forward route by adding an entry to the destination. The reverse route also updated with longer lifetime.

Figure 3 shows the same network as figure 2 after the RREP has been sent back from node E to node A. The forward route has been set up, while the unused reverse routes deleted after a timeout period.

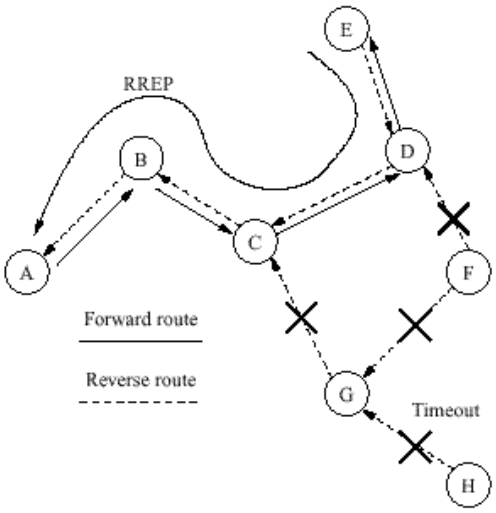


Figure 3.: Forward route setup in AODV

Route Table Management

Each mobile node maintains a route table entry for each destination of interest with the following information in it:

- Destination
- Next Hop
- Number of hops
- Sequence number of destination
- Active neighbours for this route
- Expiration time for this entry

Each time a route entry is used its timeout data is renewed by the current time plus a timeout period called active_route_timeout. If a new route is offered to a node, it compares the destination sequence numbers, and the route with the greater number is selected. If the sequence numbers are the same, the route with the smaller hop count is chosen.

Path Maintenance

Movement of nodes not lying along an active path does not affect the routing. If the source node moves during an active session, it can re-initiate the route discovery procedure. When either the destination or an intermediate node moves, a special RREP is sent to the affected source nodes.

Local Connectivity Management

For local connectivity management or neighbourhood checking, AODV uses hello messages, or learns from RREQ broadcasts. The hello message is a special RREQ packet, containing its identity and sequence number. The hello messages are not re-broadcasted by the neighbours. The neighbour that received a hello message, updates its local connectivity information.

The hello messages can be used to determine if the link to a neighbour is bidirectional or not. For this purpose, a hello message can contain a list of nodes that the sender can hear. To save the bandwidth this is optional.

Scalability tests

This section describes basic scalability tests. They are not complete, some other tests have to be done, but they can show some interesting points. First of all it has to be mentioned that the scenarios in these tests have 20 nodes on an 1000x1000m field and the transmitter range is 250m. All the parameters used during scalability tests are shown in Table 1.

Parameter	Value
Node type	Mobile
Transmitter range	250 m
Number of nodes	20
Environment size	1000x1000 m
Link type	Wireless
Link bandwidth	2 Mbit/s
Simulation time	180 s
Moving node speed Variable,	1. . . 20 m/s
Background traffic type	CBR
Number of background CBR source	4
Traffic rate Variable,	1. . . 50 pkt/s
Packet size	512 bytes

Table 1.: Parameters used during scalability tests

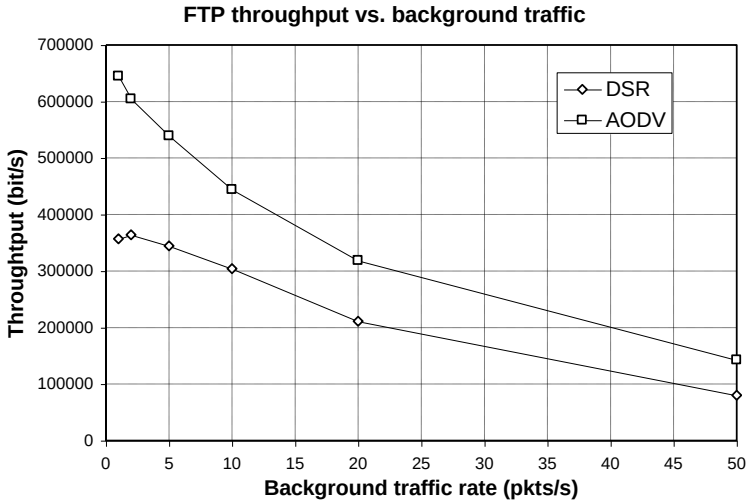


Figure 4.: FTP throughput vs. background traffic

Figure 4 shows the simulated end-to-end FTP throughput between two nodes. At this test a 1400byte files were downloaded continuously between the two nodes from the first second to the end of the simulation time at different movement speeds and background traffic rates. When the background traffic increases, the FTP throughput generally decreases as the Figure 4 shows.

FTP throughput versus path length

In this test I examined the FTP throughput of a multi-hop mobile network with increasing path lengths. The test scenario is shown by figure 5. The first node is the FTP server and the last node is the destination.

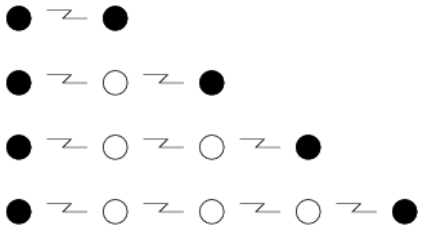


Figure 5.: The test scenario

The mobile nodes use radio the interface described in IEEE 802.11 to communicate with each other. They use Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) to share the channel. When a node wants to

send a packet to the wireless medium, it first listens to the channel. If no other nodes are heard, the node can start to transmit its own packet, but before doing this it will send a short message, the Network Allocation Vector (NAV) to inform other nodes about how long the channel will be used. Furthermore a radio interface cannot listen and transmit at the same time.

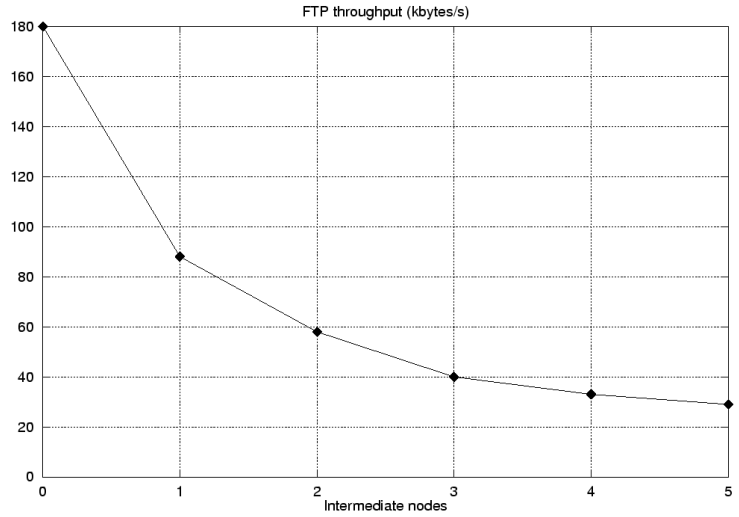


Figure 6.: FTP throughput vs. path length

The FTP throughput versus increasing path lengths is shown by the diagram in figure 6. An exponential-like decreasing can be observed on the throughput with increasing number of hops along the path. This is because the basic behaviour of CSMA/CA systems. When a node sends a packet neither of its neighbours can send, because the channel is occupied. When there are only two nodes with no intermediate nodes (one hop) this effect will not cause too much problem in an FTP download (almost a one-way communication). With one intermediate node, when this node sends a packet, the source is blocked and vice versa. In other words the source blocks the second node, and the second node can block the source. With two or mode intermediate nodes the mechanism can be extrapolated. Each node blocks the previous and the next node in the path. Fortunately, the effect of these newly incoming bottlenecks is quickly decreasing, so the throughput of the network will convergate to a level between somewhere 20 and 30 kbytes/s. This test clearly shows that the throughput on an (almost) one way communication channel can fall back far below the nominal throughput of the link. In the case when there are more sources in a small network this effect can show up more dramatically.

Round trip time on a changing scenario

In this test the one hop delay has been examined on a simple network shown by figure 7. The two communicating nodes are the moving node (down) and the grey coloured node (fifth from left). A normal, one second delay ping is used to measure the round trip time.

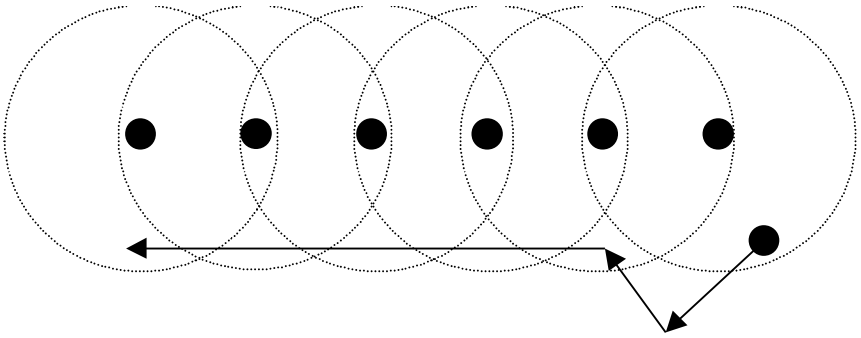


Figure 7.: Scenario

The results can be seen in figure 8. In the beginning there is one intermediate node in the path between the two nodes. The round trip time (RTT) is approximately 10 ms.

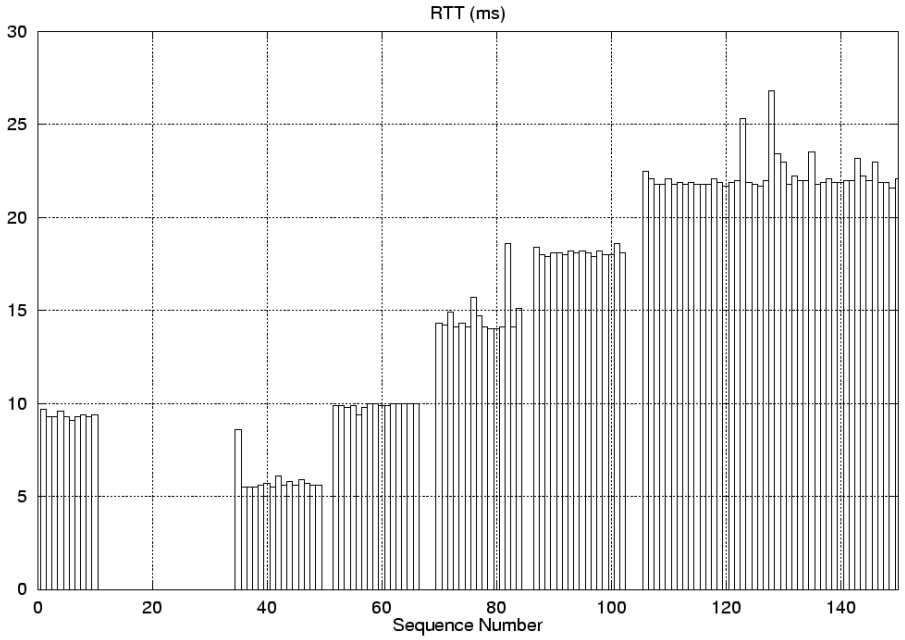


Figure 8.: Round Trip Time vs. ping sequence number

The first big gap in the diagram is because the node moves out of range from the other nodes. The next phase is a one hop route without any intermediate nodes. The RTT is approximately 6 ms. The next phase is a two hop route again. After that there is a three hop route, where the RTT is about 14 ms. With this 'equations' the two parameter can be computed. Note that the values are RTTs, so they are two times as much as in a one way route. The small gaps are caused by AODV latency before finding that a link is broken and the latency of finding a new route. AODV decides that a link is broken when the number of (serially) missing hello messages from a former neighbour exceeds the maximum hello loss value. The hello message interval is set 1 second, and the allowed hello loss value is 2, which means that AODV has minimum two and maximum three seconds of latency before recognise a broken link.

Mobility test

The goal of this test is to demonstrate the efficiency of two routing protocol in case of changing the network topology dynamically. The parameters of the network scenario were the following:

Parameter Value	
Node type	Mobile
Transmitter range	250 m
Number of nodes	20
Environment size	1000x1000 m
Link type	Wireless
Link bandwidth	2 Mbit/s
Simulation time	180 s
Moving node speed Variable,	1. . . 20 m/s
Background traffic type	CBR
Number of background CBR source	4
Traffic rate Variable,	10 pkt/s
Packet size	512 bytes

In this simulation the efficiency of the AODV and DSR routing protocol have been examined on a simple network where the mobility factor is changing. The results are shown in figure 9. As we can see the AODV protocol has better throughput than DSR because AODV only deal with searching new route when it is necessary. In case of low mobility the protocols

can find better transmission route. If the mobility is higher the protocols have to search new routes frequently than before. Due to protocol overhead the throughput is degraded.

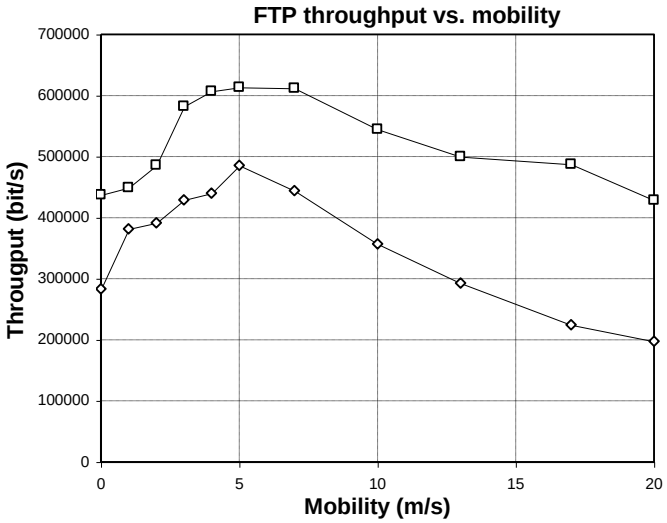


Figure 9.: FTP throughput vs. mobility

When the mobility is 5 m/s the throughput is maximal. Generally, it is not a typical value rather the feature of this scenario.

Conclusion

The simulation results demonstrate the efficiency of two routing protocol in case of mobility, hop length and round trip time. We can observe that the reactive protocols more efficient than the pro-active ones because reactive protocol only tries to find a route when it is needed. However, the pro-active protocols have bigger overhead.

Pándi Erik

CONTROLLING THE USE OF THE INTERNET AND IP-BASED SYSTEMS IN THE HOME AFFAIRS SECTOR

Preamble: The integration process in the fields of communication and information-technology services and technologies during the second half of the last century also affect and form the customs of the contemporary society. In the so called *information society* conception information takes a special part in both the life of the individual and the operation of the organization; therefore to break the existing doubtfulness, more information shall be gathered in large volume. IP-based communication has a more and more significant part in the domestic governmental work and the operation of the defense sectors as well; an example of which is that the Ministry of the Interior elaborated and issued its direction in relation to the tasks concerning the application of the Internet by sectors. The present publication sums up the development of the Internet, furthermore the national and domestic trends of its improvement and the main definitions of the measure elaborated, originating from the controlling activity of the home affairs sector.

Internet – the beginning

The development of the Internet started on the basis of the order of the U.S. defense department, approximately at the end of the 1960s. The main purpose was the endurance of the military leadership in case of an atomic strike, that is the central command should not be disabled if partial systems are dropped. In addition a further demand was that information sent through the system should not be traceable.

The theoretic solution originated from the setting up of the model of a decentralized network, that is an information system consisting of nodes, in which the nodes that can be handled as equal points are free to send, receive and forward data towards each other. The messages themselves are divided into small, individually addressed packets by the sender node; which are put together by the recipient node. These packets are dispatched by the sender not simultaneously and in different routes, furthermore on one route several partial messages are forwarded at the same time, which makes impossible the acquirement of the messages by the enemy. As a matter of fact the accidental destruction of a route does not cause any trouble, as the forwarding nodes can choose from several routes.

At the beginning of the technological development (1971) there were only four nodes:

1. University of California in Los Angeles;

2. Stanford Research Institute;
3. University of California in Santa Barbara;
4. University of Utah in Salt Lake City.

The network was called Advanced Research Project Agency Network (ARPANet), in which the group of users was extended gradually by the participants of the research. Approximately from 1973 onwards the researchers began to test communication protocols, with the assistance of which systems operating according to different standards could be also connected to this network. The series of experiments were called Interneting, from which the denomination Internet is coming.

The communication system of the Internet is the TCP/IP, which is a combination of two earlier systems, the so called TCP (Transmission Control Protocol) and the IP (Internet Protocol). The TCP breaks up the messages into units by the sender, and puts together the messages by the recipient, we can say it controls data exchange. The IP executes addressing of the information packets and ensures that each message reaches the addressee through more nodes, even through more different computer networks.

The TCP/IP system, that is open to everybody ensured that the closed system consisting of four nodes at the beginning became nowadays a world-wide network. A significant feature of the improvement is that according to some surveys 80% of the information exchange of the U.S. army is carried on through the Internet.

During the successful research-development process the military-type sub-system was definitely detached, therefore with the material support of the National Science Foundation the NSFNet was established. It can be presumed that NSFNet was the last integrated main Internet network, as it is pertaining to the world-wide network, that it does not have any kind of central network-management. Control is only present upon the distribution of addresses, represented by the Internet Society (ISOC) and the Internet Architecture Board (IAB). The name of the main network in Europe is Ebone, while the Hungarian is called Hbone.

The Internet is a huge treasury of open information, the network of information-technology equipment connected to the network, the development of which was enormous in the last few years. It is very difficult to estimate the number of organizations and individuals connected to the network, but according to some estimates 400-1000 new web pages are published each day. The number of joining individuals and persons is approx. 800 million-1 milliard, the number of interconnected networks can be about 40-50 thousand.

Unfortunately the deviation between the surveys so far is large, according to some estimations the volume of overall information can reach 2-10 terabyte (10^{12}). One terabyte is 1 million megabyte, or one-million times one-million

characters. In an average library there is a 3-terabyte data volume (300 thousand books).

All in all, we can say that the Internet has proved practical adaptability during its improvement, which is clearly supported by the accelerated appearance of commercial subscribers and Internet suppliers. Nowadays the information reachable and supplied through the network – *due to its volume* – cannot be indifferent to the life of the individual and the operation of the organization, therefore the provision of access in a long-term can be for the benefit of all of us.

Preparing for the electronic governmental work

By the end of the twentieth century the development trends of information-technology converging with telecommunication have revalued the part of the information-technology sector in the fields of communication. The literature of the last few years has already outlined the information society of the future, and the structure of it, which will be basically determined by the prevalence of telecommunication and information-technology (with a new phrase 'info-communication') equipment, networks and services.

In Hungary at the beginning of the present governmental period the Prime Minister's Office (Miniszterelnöki Hivatal - MeH) has published the governmental conception stipulating the principles of supplying the information society. For the establishment of the *"supplying state and administration"* the Prime Minister's Office intends to advance the governmental use of information-technology, the essence of this conception is the following:

- the state, as an active participant of the society – *executing and ensuring its administrative functions* – applies information-technology in the interest of its own efficiency;
- the state, as the maintainer of democracy and constitutional personal rights tends to establish personal and regional equality of chances;
- the state, as the owner of information determining the future, and the one having the infrastructure proper for strategic analysis, affects the conditions of the development of the information society in a directive way.

For assisting better social integration the administration with its services and the data gathered and presented by it shall provide equal chances for its citizens and for this purpose the administration shall be also altering:

- it shall operate effectively, that is its organization and procedures shall be well-arranged, it shall provide reliable data and services quicker and cheaper;
- it shall operate in a way, that its civil services are accessible expansively and universally, in the meantime it shall ensure proper legal safety and guarantees.

All in all, the strategic aim of the Prime Minister's Office is the setting up of administration without any paperwork, one-stage transactions, common construction and electronic citizens' consultation. In relation to administration without any paperwork a purpose to be reached is the organization of governmental and administrational information work on a digital base, in which the ministries, offices and the data bases of them will be connected. With the integrated data bases set up in this way the connecting of governmental and municipality information will be possible. According to the technical conception of one-stage transactions with the application of the data bases the connection between the citizen and the administration can be interactive.

During the planning and organizing of the network needed for the technical effectuation of the conception outlined above, serious problems arose due to the scattered build-up of the state and private communication networks; the present government intends to solve this problem with the setting up of a new system, the so called Egységes Kormányzati Gerinchálózat (EKG) – Unified Governmental Main Line Network. Apart from the existing troubles, in co-ordination with the international trends and the governmental conceptions, the Ministry of the Interior (BM) monitoring and controlling the administration of Hungary has also worked out its own conceptions concerning the method of setting up and applying the Internet and the IP-based networks, which is stipulated in the document of Reg. No. 63-470/1999 BM.

Sectoral control of modern information-technology developments and the application of them

The Ministry intends to advance for the expansion of the essence of sectoral information-technology in two fields:

- increasing the efficiency of the design and control systems;
- strengthening the serving feature of information-technology.

As in the case of classic telecommunication, in the field of information-technology the serving feature is stressed, therefore the solving of the support of the demands and tasks determined by the professional guidance is the main requirement. As the basis of the information-technology system to be set up and developed is the totality of various professional expectations, there will be common tasks upon development, like:

- expansion of defense applications (registration system at the frontier, finger-print registering and identification system);
- the reconstruction of information-technology supply background (basic domestic records, head information system, duty-system);
- in co-operation with the sectoral telecommunication organizations the setting up of an integrated network infrastructure, supporting the information-technology applications;

- setting up of applications concerning public authenticity (the achievement of safety in the electronic information-exchange);
- the establishment and development of administrative services (the setting up of civil information systems with the establishment of local administrative information-technology centers).

Consequently we can see that parallel with the central strategy the Ministry of the Interior intends to establish the technological base of the electronic governmental work in its plans as well; for which the Ministry plans to improve both its telecommunication and information-technology infrastructures. Beside the elaboration of the conceptions of technological improvement the effects of the surroundings of administration mean significant challenge. In their everyday work both the provost services (police, border-guards, disaster-protection) controlled by the Minister of the Interior and the organizations supporting ministry operation are compelled to apply Internet as a source and for information, or use the network for forwarding data.

As consecutive approach is rather peculiar to the administrative organizations due to their inability, the sectoral regulation of electronic operation – demanded earlier by the surroundings – was only executed in the middle of this year, upon the issuing of the **BM directive No. 36/2001**.

III.1 The structure of the measure

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.

III.2 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.

III.3 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 ambiency 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.

Summary

The present publication sums up the steps taken in relation to the introduction of the Internet and the communication procedures serving it. It can be ascertained, that using the applications based on the Internet and IP-based networks the Ministry of the Interior, representing the domestic defense sector, tries to connect up properly into the model of the electronic governmental system, reflecting governmental conceptions.

Prospectively, in the life of the 21st century society information and quick access to data will take a significant part; therefore the operation of the defense sectors functioning as part of the administration cannot be independent of the info-communication ambiency.

The control ambiency of the Ministry of the Interior shall of course go ahead in a direction, that - according to the civil trends – the problems arising in the fields of sectoral communication and information-technology should become resolvable in a common way. When this process is launched, an internal professional and organizational integration could be reached in the middle-run already, that could assist the early feasibility of governmental conceptions on an administrative level.

Fekete Károly

VOIP IN MILITARY COMMUNICATION SYSTEM

Overview

Military communications has always been a weak point in the real time voice- and data communication. The ability of computers to generate information has increased multiple magnitudes in the past ten years; however military communications has not kept pace. Further, the enhanced weapons available to the enemy has made interoperability between the services and the various functional areas vital.

One of the leading tendencies in military telecommunication development is joining of this scientific and technical sphere together with information science. It became possible due to the fact that a computer does not just operate with the data but it can transfer and receive them as well. The modern military communication and information system (CIS) networks are based on the methods of packet transfer and commutation. They use a simple idea of presentation of any kind of information (data, images, speech, sound, service and controlling messages) as a numerical order which is divided into small parts called packets that have the necessary information for their identification, routing, errors correction etc provided. This approach allows to transfer all kinds of information, use different means to transfer the data and use universal military commutation systems.

Under the conditions of unlimited networks and unlimited channel capacity the development of such networks is a pure technical problem. The scientific and technical problems emerge when we come across the resource boundedness. Moreover, these problems differ depending on the kind of information, and they require the specialists in the military CIS topic.

Planning, designing and implementing common military CIS network infrastructures that support voice, data and multimedia services are critical to the success in today's and tomorrow's environment. Internet Protocol (IP) based technology is enabling the development of a common integrated military network infrastructure for transporting voice applications.

The convergence of the public switched telephone network (PSTN) and Internet protocol (IP) data networks promises exciting opportunities for local and long-distance wireline and wireless carriers, Internet service providers (ISPs), equipment manufacturers. An important step in the fulfillment of this promise is the extension of military communication and information network (CIN) capabilities to and from IP networks. This integration of CIN and IP technologies represents a significant breakthrough in the ongoing convergence of voice and data networks.

This tutorial contrasts a few alternative architectures for an CIN/ Voice over IP (VoIP) integrated network, considering the advantages and disadvantages of each.

Voice over IP

While the PSTN and military STN evolved into a CIN, data networks evolved in tandem. With the creation of the World Wide Web (WWW), the Internet exploded into a global network of research, business, and personal users. As a result, *IP has become the de facto standard for data networking*. Unlike the circuit-switched architecture of the most military CIN, IP networks are data packet networks. The computers on the network are all interconnected by persistent connections, the bandwidth of which is shared by all active military users. As the network gets busier, each user will remain connected but will experience performance degradation.

Although military CIN and IP networks are fundamentally different in terms of routing and performance, it is possible for the networks to be connected, exchanging voice and data traffic. Figure 1 depicts the first generation of technology to achieve this integration.

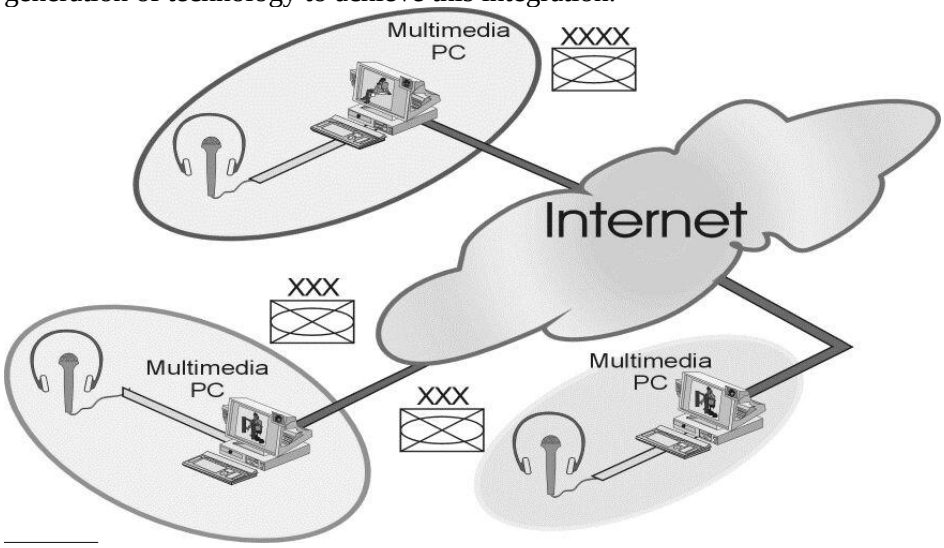


Fig. 1. The first generation of technology integration in military CIS and IP

VoIP QoS issues

The advantages of reduced cost and bandwidth savings of carrying voice-over-packet networks are associated with some quality-of-service (QoS) issues unique to packet networks.

Delay

Delay causes two problems: echo and talker overlap. Echo becomes a significant problem when the round-trip delay becomes greater than 50

milliseconds. As echo is perceived as a significant quality problem, voice-over-packet systems must address the need for echo control and implement some means of echo cancellation.

Talker overlap of military users (or the problem of one talker stepping on the other talker's speech) becomes significant if the one-way delay becomes greater than 250 milliseconds. The end-to-end delay budget is therefore the major constraint and driving requirement for reducing delay through a packet network.

The following are sources of delay in an end-to-end, voice-over-packet call:

Accumulation Delay (Sometimes Called Algorithmic Delay)

This delay is caused by the need to collect a frame of voice samples to be processed by the voice coder. It is related to the type of voice coder used and varies from a single sample time (.125 microseconds) to many milliseconds. A representative list of standard voice coders and their frame times follows:

G.726 adaptive differential pulse-code modulation (ADPCM) (16, 24, 32, 40 kbps)—0.125 microseconds

G.728 LD–code excited linear prediction (CELP)(16 kbps)—2.5 milliseconds

G.729 CS–ACELP (8 kbps)—10 milliseconds

G.723.1 Multirate Coder (5.3, 6.3 kbps)—30 milliseconds

Processing Delay

This delay is caused by the actual process of encoding and collecting the encoded samples into a packet for transmission over the packet network. The encoding delay is a function of both the processor execution time and the type of algorithm used. Often, multiple voice-coder frames will be collected in a single packet to reduce the packet network overhead. For example, three frames of G.729 code words, equaling 30 milliseconds of speech, may be collected and packed into a single packet.

Network Delay

This delay is caused by the physical medium and protocols used to transmit the voice data and by the buffers used to remove packet jitter on the receive side. Network delay is a function of the capacity of the links in the network and the processing that occurs as the packets transit the network. The jitter buffers add delay, which is used to remove the packet-delay variation to which each packet is subjected as it transits the packet network. This delay can be a significant part of the overall delay, as packet-delay variations can be as high as 70 to 100 milliseconds in some frame-relay and IP networks.

Jitter

The delay problem is compounded by the need to remove jitter, a variable int The convertion must not distort a voice signal much, and the transmission mode must keep the exchange of information between abonents in a real-time mode.erpacket timing caused by the network a packet traverses. Removing

jitter requires collecting packets and holding them long enough to allow the slowest packets to arrive in time to be played in the correct sequence. This causes additional delay.

Lost-Packet Compensation

Lost packets can be an even more severe problem, depending on the type of packet network that is being used. Because IP networks do not guarantee service, they will usually exhibit a much higher incidence of lost voice packets than military ATM networks. In current IP networks, all voice frames are treated like data. Under peak loads and congestion, voice frames will be dropped equally with data frames. The data frames, however, are not time sensitive, and dropped packets can be appropriately corrected through the process of retransmission. Lost voice packets, however, cannot be dealt with in this manner.

The gateway in military CIS.

The gateway is a basis of IP-telephony. It converts service signals and data from military PBX into the Internet packets and back.

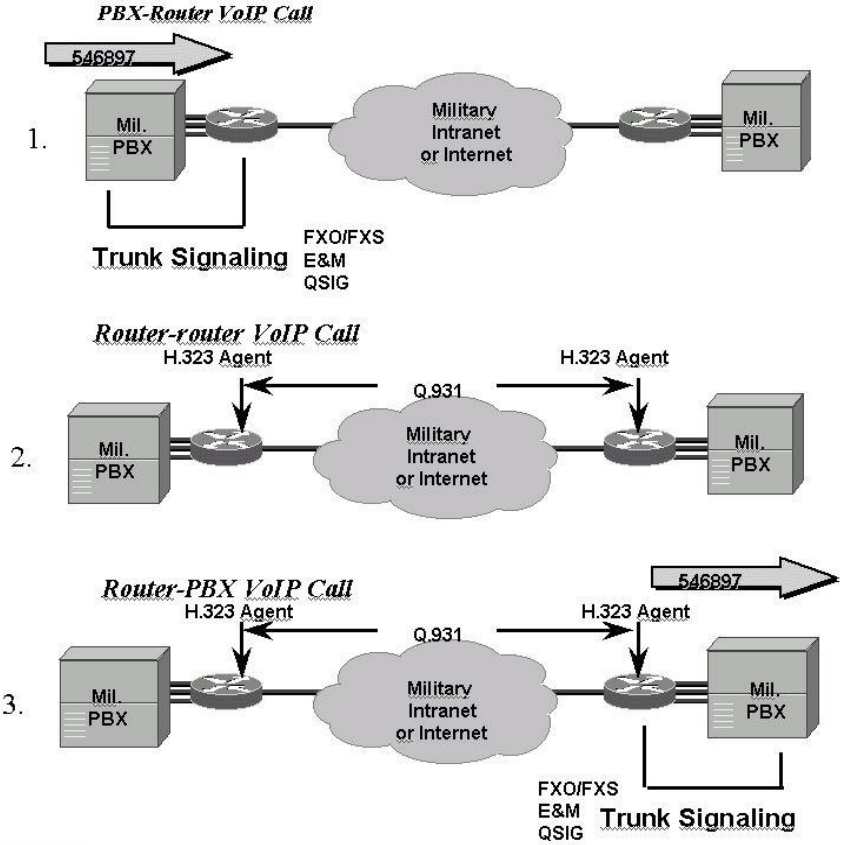


Fig. 2. The phase of voice transfer on military intranet/internet

The functions of gateway at the point to point connection (Fig. 2.):

- Realization of physical interface with network.
- Detection and generation of signals of military users signaling
- Convertion of signals of military users signaling into data packets and back.
- Connection of military users.
- Transmission of signaling and voice packets.
- Disconnection of military users.

The most functions of gateways with the architecture TCP/IP are carried out in the applied processes.

Gateway realization for IP-telephony

As we mentioned in the beginning all IP-telephony systems can be divided into the basic schemes: for PC-users and users of a telephone network (via the Internet without PC usage).

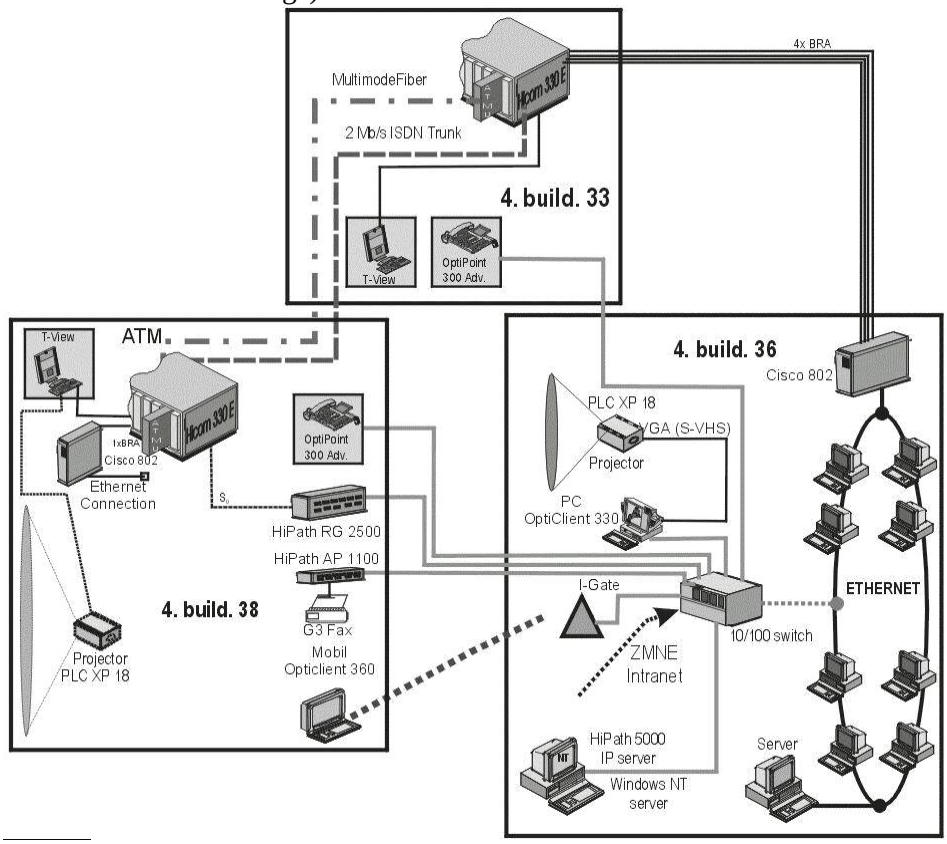


Fig. 3. The part of VoIP and ATM based architecture of military CIS on National Defense University Hungary.

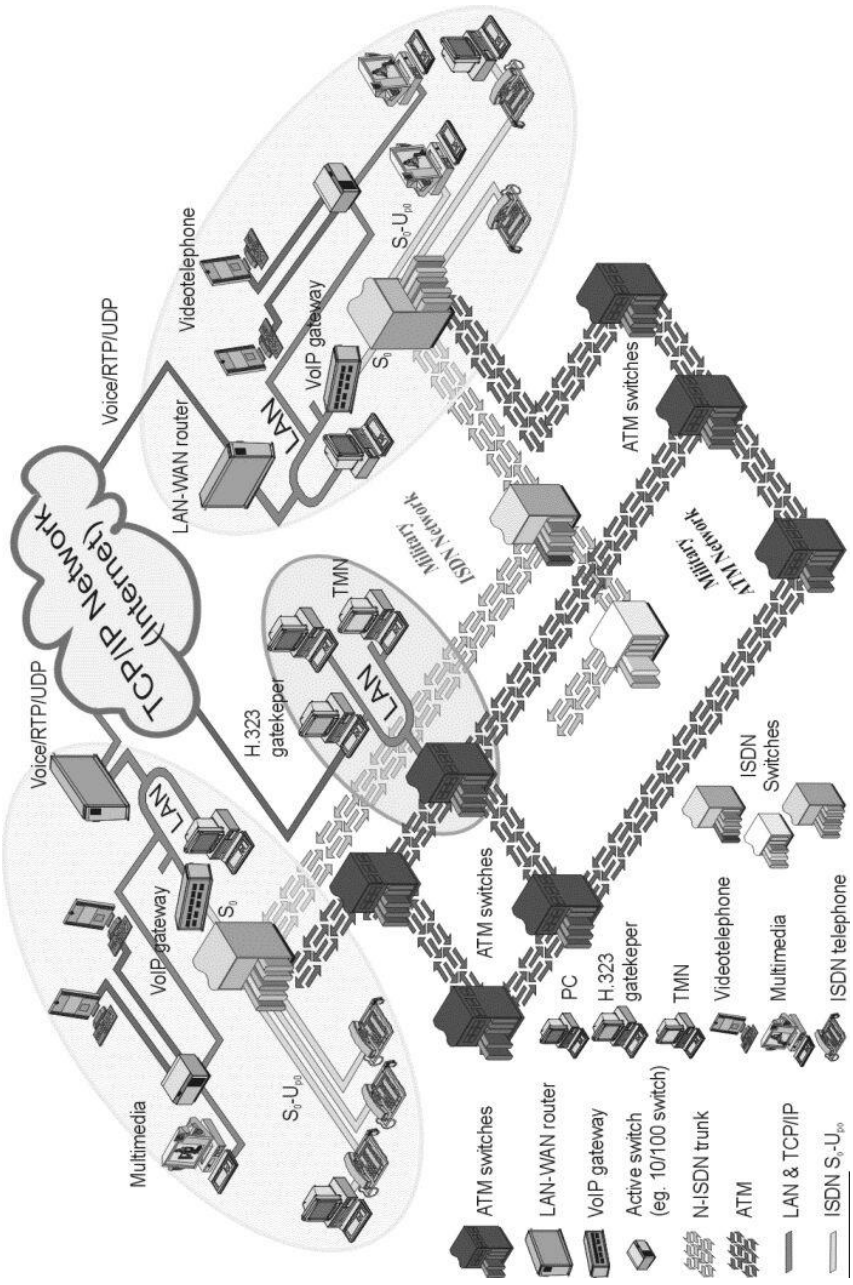


Fig. 4. Recommended VoIP completion of ATM based military CIS

The first scheme in military CIS has two variants of realization: software (when all procedures are carried out by the PC with a built-in soundcard), and

soft hardware (when DSP card is installed in the PC that fulfils the basic functions and unloads the PC for other operation).

The second variant is may be the variant of National Defense University where was established a special project. The first part of competition intended to doing research of military communication system on ATM base. The second part of competition want to study of possibility VoIP applications in military CIN (Fig. 3.).

Recommendation

With special regard to increasing of voice- and data flow and regard to spreading of sophisticated communication and information services, such as multimedia, and sensors in military CIS we can recommend the completion of military CIN, based on ATM and N-ISDN (Fig. 4.).

The most important parts of confoguration of VoIP completed military CIS are:

- ATM switches (military or common governmental property)
- N-ISDN switches
- LAN-WAN routers
- VoIP gateways
- H.323 gatekeeper
- TMN workstation
- Multimedia equipments (PCs, projectors and videotelephones)

SECURITY ISSUES IN MOBILE AD-HOC NETWORKS

Kata Molnár
Budapest Polytechnics Kandó Kálmán
Faculty of Electrical Engineering
kmolnar@k2.jozsef.kando.hu

László Zömbik
Ericsson Research, Hungary
Conformance Center
laszlo.zombik@ericsson.com

Abstract

The idea of ad-hoc network has been outlined to the military due to the sporadically spread troops in the battlefield are needed to keep contact to each other and the HQ. In the ad-hoc solution the messages are forwarded to the destination via the other troops' communication equipment. In this case several fundamental security question rises since the approach of the ad-hoc network is quite different from the usual centralised or semi-centralised infrastructure. For example the malicious node not only capable to eavesdrop or block the communication, but even the enemy might seamlessly get those equipment on which the communication flows between the other troops and the HQ.

1. Ad-hoc networks

The need of ad-hoc network [Ad-hoc] had been dated back to the ancient times when the commanders of the army wanted to communicate to distant troops or the emperor independent of their location. For example the Indians had invented the "smoke signalling network". In a dedicated fireplace on top of the hill and a warrior could inform the surrounding troops and the neighbouring tribes about the danger. However the security of this kind of communication was not strong since the enemy was not only able to read the messages but with capturing the fireplaces could block or even they could send misleading messages.

The idea of the ad-hoc networks in the XXI. century is remained the same. Those networks are created for one specific purpose with no predefined rules; nodes connect and serve a collective goal. The network is entirely distributed so any node failure should not affect the system significantly.

Ad-hoc networks not rely on the actual bearer, although nowadays the most ad-hoc networks are based on radio technology. In this case the nodes became even capable for mobility.

Therefore security properties of mobile ad-hoc networks (MANET) are descended from the mobility of the nodes and the distributed features of the ad-hoc networks. Mobility provides location freedom so the user is able to communicate anywhere within the network. Ad-hoc attribute due to the co-operative nodes and distributed feature provides high availability in a continually changing environment.

The properties of the infrastructure seem to provide only advantages, but in several cases those features became disadvantages for security.

Mobile Ad-hoc Implementations

The two most widespread mobile Ad-hoc implementations are the IEEE 802.11 [80211] and the Bluetooth [Bluetooth].

IEEE 802.11 (WaveLAN) has been designed to support client/server based and ad-hoc networks. The access method is CSMA/CD (Carrier Sense Multiple Access with Collision Detection). The physical layer uses two unlicensed RF bands and one infrared frequency. Unlicensed frequency bands requires spread spectrum modulation to achieve meet the quality requirements.

Bluetooth has been designed for replace the wire with radio technology. Therefore mostly uses for single hop wireless connections. In Bluetooth the medium access is master-slave based. A master node and its slaves forms a piconet. A Bluetooth unit can connect into more than one piconet at any time but it can be a master in only one piconet. A unit that participates in multiple piconets can serve as a bridge thus allowing the piconets to form a larger network, which is referred to as a scatternet.

2. Security Goals

Communication networks should provide the following security services for reliable and secure information transport:

Confidentiality ensures that certain information never discloses to any unauthorised entities. Sensitive information traverses along a communication network must be equipped with confidentiality. Such a sensitive information can be user data (e.g. tactical or strategic military information) or system signalling, for example routing information.

Leakage of that information can lead destructive consequences; endanger the aim of the infrastructure and the privacy of the user.

Confidentiality can be provided hop-by-hop or peer-to-peer basis. In the former case some sensitive information might also be shared between authorised entities along the path (e.g. routing) while the latter case the sensitive information must only be shared between the endpoints.

In Ad-hoc networks confidentiality between the communicating peers is needed for protecting the user information against eavesdroppers along the path. Since in Ad-hoc network the probability of compromise of an intermediate node (e.g. the enemy capture the node) is not negligible therefore confidentiality of user sensitive data should have peer-to-peer.

Significant confidentiality can be reached using message encryption lower lever can be reached with steanography (e.g. Public Switched Telephone Networks).

Integrity ensures that the information being transferred is neither altered by malicious nodes nor corrupted due to link errors. There are several integrity definitions: data, correctness and source integrity [RFC2828]. Data integrity provides that data has not been changed, destroyed, or lost in an unauthorised or accidental manner. Correctness integrity ensures accuracy and consistency of the information that data values represent, rather than of the data itself. This can be important e.g. for accounting or for critical applications. The source integrity is the degree of confidence that can be placed in information based on the trustworthiness of its sources.

Authentication guarantees a node to ensure the identity of data or identity of peer communicates with. It consists of two steps. First the peer presents an identifier to the security system, second presents or generates authentication information that corroborates the binding between the peer and the identifier. Data origin authentication is the corroboration that the source of data received is as claimed. Peer entity authentication is the certification that a peer entity in an association is the one claimed.

Non repudiation is a protection against false denial of involvement in a communication. This service is useful for detection and isolation of compromised nodes.

Availability ***ensures that the system or its resources remains being accessible and usable despite simple fails or denial of service attacks. In the ad-hoc network a denial of service attack could target at any layer. On the physical and medium access layer the attacker uses interference, on the network layer routing table manipulation causes network malfunctions and on higher layers services became target for attacks [AdHocSec].***

Key management ***ensures of handling and controlling cryptographic keys and related material during their life cycle in a cryptographic system, including generating, distributing, storing, loading, auditing, and destroying the material.***

Other ***(e.g.*** **Authorisation** ***a right or a permission that is granted to a system entity to access a system resource).***

3. Threats in the mobile ad-hoc environment

In a distributed mobile network - where the routers also capable mobility, where no centralised point exists, where the environment (neighbours) also

changes, some network elements became corrupted and malicious nodes tries to cause damages - hard to establish proper security.

Due to the mobile ad-hoc network properties several threats exists. The most important problems are highlighted in this section.

3.1 Denial of Service Attacks

The Denial of Service Attacks (DoS) decrease service availability or even prevents of authorised access to a system resource or delays of system operations and functions. The attacker typically floods the system large amounts corrupt, outdated, or correct but vast resource consuming queries. Since the resources of mobile equipment in ad-hoc network are assumed to fairly limited this threat is significant.

3.1.1 CPU Overloading

The target is to decrease service availability due to CPU overloading and even crash the node. Sending large amount of CPU consuming queries (e.g. the message processing requires decryption) due to the limited CPU capacity the equipment became useless for its purpose.

3.1.2 Battery Exhaustion

A CPU consuming task can reduce the life of the battery too. Battery life is critical parameter for many portable devices since the weight and size of the equipment depends on the lifetime of battery therefore many techniques are used to maximise it [SecIssues]. Those techniques are based on that the CPU and radio receivers are turned to sleep mode. If the attacker prevents the node from going power saving mode the device became unavailable prematurely.

3.1.3 Interference in Radio Medium

The interference on physical medium also DoS attack. The adversary could emit noise in the physical medium, which causes large number of information loss. In that case it is hard to identify the scramble of the attacker from the natural noise of the medium. This is even problematic in the case of radio medium.

3.1.4 Flood of Physical Medium (collision)

Flooding the medium with MAC (Medium Access Control) messages prevent the nodes to access the medium. This can be accomplished by sending bad messages or neglect the medium access rules. Open systems are usually based on that nodes work cooperatively and this behaviour is crucial if they share a specific medium. This is an important problem in mobile ad-hoc case because nodes share a specific frequency range; if a node plays destructively communication became impossible.

3.1.5 Fill of Routing Table with Invalid Entries

A mobile device has to collect information to deduce several properties of the ad-hoc network. The most important parameter is the routing information. Using its routing table the node appoints a path or direction to send the

message to its destination. Due to the changing environment it must be refreshed frequently so routing table should always up to date.

If a malicious node broadcasts wrong routes then message path might be altered to wrong direction. This leads to loss and performance degradation.

(If the adversary exhibits oneself as the solution of all routing problems than it can control which messages are forwarded and which are not. Even it became capable eavesdrop the communication flow.)

3.2 Impersonation

3.2.1 Endpoint Impersonation

The malicious node can simulate that it is the node with the other party wanted to communicate. If no authentication exist in the system then it is a trivial attack.

However gaining the endpoint credentials (which is unique and definitely determine the user) the authentication procedure can be fooled. Therefore the authentication must contain an identification step but also a verification step which corroborates the binding between the entity and the identifier. This step since no centralised infrastructure exists to trust and to store data necessary for verification (e.g. on-line CA where CRL – Certificate Revocation Lists can be obtained) is quite difficult. Since the probability of mobile node compromise is not negligible this is a menacing threat.

3.2.2 Man in the Middle

A form of active wiretapping attack in which the attacker intercepts and modifies communicated data in order to simulate to the peers that he is the opposite peer.

3.3 Confidentiality Violation

3.3.1 Passive Eavesdropping

Malicious node listens on the shared medium to catch others communication. Due to the usage of radio medium the physical area of the shared medium is larger than necessary. Therefore employing this kind of attack is easy.

3.3.2 Active Eavesdropping (e.g. using routing manipulation or man-in the-middle)

In the mobile ad-hoc network several active attacks can be employed, the two most important are based on the routing manipulation and the man in the middle attack.

Man in the middle attack: a form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data in order to masquerade as one or more of the entities involved in a communication association.

Routing manipulation: the adversary distributes routing information so the path of the communication alters in that way it goes trough oneself. Then the communication can be eavesdropped.

3.3.3 Code Breaking

Eavesdrop attack might fail if the nodes uses encrypted communication. Although using week algorithms or selecting improper parameters (e.g. key expiration time or even the improper key) the communication became vulnerable against code breaking attacks.

3.4 Message Alteration

A malicious node can influence the message has been sent to the destination.

3.4.1 Message Insertion

A new message has been inserted to confuse the nodes, alter the meaning of the information or mount a DoS attack.

3.4.2 Message Annihilation

An important information has been removed from the network by physical signal interference, collision on the link layer, or it has been silently discarded. If a malicious node broadcasts wrong routes then message path might be altered to wrong direction.

3.4.3 Message Alteration

Contents or meaning of the message has been modified.

3.5 Message Repudiation

Denial by a system entity that it was involved in a communication. If messages can be denied than later an investigation cannot decide that the node itself or other (malicious) entity behaved as logged. For IDS (Intrusion Detection System), accounting and critical communication non-repudiation is required.

3.6 Anonymity Violation

3.6.1 Neighbour Discovery

Malicious nodes which capable to process the communication protocol are able to collect some information about the neighbouring nodes [QuestFor] due to the access medium is shared and identifications (e.g. unique host address) is readable. Therefore identification or localisation of the target host became easy.

3.6.2 Sending Credentials

Node sends authentication credentials to another peer to identify oneself. This credential provides information for the peer, but due to the shared medium the identification is disclosed to the eavesdroppers too.

3.7 Unauthorised Physical Access

3.7.1 Hardware Tampering

Unauthorised person gets access to the equipment, where hardware modification, hardware destruction, hardware steal (e.g. one-time key generator) or compromising of information has been made. The protection of physical access is weak (devices are not behind a closed door in the server room) in the mobile ad-hoc networks.

3.7.2 Software Tampering

Unauthorised person gets access to the equipment and modifies or compromise substantial information (e.g. gets private or shared secret key). A subset of this threat is when the adversary installs viruses, trojans, etc. to the node.

3.8 Attacks based on Shared Radio Resources

3.8.1 DoS Attacks

Attacker blocks the medium with radio interference or malformed link layer (MAC) messages.

3.8.2 Eavesdrop

Attacker gets into the radio transmission range and collects information.

3.9 Lack of Centralised Trusted and Well-secured Network Element

In the mobile ad-hoc environment it is assumed that there is no trusted centralised secure network element. The advantage of this is that the system is not vulnerable when a node with centralised functionality brakes down or became compromised. The authentication procedure in distributed system cannot easily handled since there is no trusted network element (e.g. online Certificate Authority or Key Distribution Centre) which guarantees proper authentication.

3.10 Distributed Architecture

If a node is found malicious in one part of the ad-hoc network then the exposed node moves to another part of the network where they have no criminal record of the adversary. In that case even one attacker could threat the ad-hoc system.

3.11 Routing Manipulation

3.11.1 Wrong Directions

The ad-hoc networks rely on the routing information to a great extent. Offering wrong directions to the node cause increased delay or message loss.

3.11.2 Routing Alteration

The attacker alters the path of the communication to across its territory. Then several attacks can be mounted.

3.12 Compromise of Keys

Attacker could obtain secret information (key), which is an input parameter that varies the transformation performed by a cryptographic algorithm. Not only the key to the actual encrypted communication, but the authentication and integrity protection key can also be compromised.

3.12.1 Hardware Tamper

During unauthorised physical access to the equipment the keys can be picked out.

3.12.2 Code Breaking

Using weak algorithms or using keys for long time or on too much byte keys can be deduced for the attacker by cryptanalysis.

4. Countermeasures

The following steps have to be made to prevent the threats in the mobile ad-hoc network environment. Although some threats are not significant in some cases (e.g. a military mobile hardware device not requires protection against viruses) but the most important preventive procedures are presented.

4.1 Blocking DoS attacks

4.1.1 Issues

If the target of Denial of Service attack is the shared resource, than the defence is quite hard. In that case the limited shared resource is occupied therefore this affects all nodes shares the resource. In mobile ad-hoc case the radio medium is a limited shared resource. With steanography nodes are protected against interference on physical layer, but in the medium access level protection hardly can be reached.

If the Denial of Service attack targets not shared resources but dedicated nodes then handling of this kind of attack is easier but it also requires some intelligence in the node.

In some cases intelligence is not enough due to the received and collected information are not sufficient to make proper decisions. For example in mobile ad-hoc network it is hard to decide whether a malicious node sent wrong routing information intentionally or the network topology changed in that way that the routing entries became obsoleted.

4.1.2 Rule based Filtering

In that case the node first applies the messages to a specific rules and if and only if the rule accepts further process continues. For example a rules specifies that the number of specific connections are limited. In that case flooding the node with connection attempts will be refused and therefore crash of the node is avoided.

4.1.3 Intelligent Filtering

Intrusion Detection Systems (IDS) can identify that behaviour of a node is different than expected. In that case those malicious nodes are placed on suspicious lists. If a malicious node act aggressively the communication with that node is terminated.

4.1.4 Steanography (Spread Spectrum Modulation)

In a shared medium cryptography can be solution for privacy and steanography against Denial of Service attacks. In that case the communication in physical layer became hidden for attacker. In order attacker not to be able to mount brute force attack on the whole physical medium the price of this kind of attack must be high. This can be achieved with Spread Spectrum Modulation e.g. DSSS (Direct Sequencing Spread Spectrum) where the useful information is expanded to a large frequency scale.

4.2 Against Impersonation

4.2.1 Authentication

Proper authentication ensures protection against impersonation and against man in the middle attacks. However if identification credentials are compromised then an authentication process not always capable to identify the problem.

4.2.2 Identification of Compromised Endpoint

After successful authentication if a node behaves maliciously the responsibility of IDS to identify and if necessary reconsider the result of the authentication. In order to the malicious node became identifiable non-repudiation is required.

4.3 Confidentiality

4.3.1 Against Passive Eavesdropping

The communication has to be armoured with suitably strong coding mechanism (usage of encryption algorithms).

4.3.2 Neutralise Active Eavesdropping

Secure routing and encryption of the communication is needed. A routing should use authentication mechanisms too, to identify the nodes from the routing table was received.

4.3.3 Countermeasures against Code Breaking

Any encryption can be broken if it is used improperly. Frequently changed keys and strong encryption mechanisms prevent the attacker to break the code with its available resources.

4.4 Integrity Protection

Several mathematical algorithms exist which generates an integrity check value from a data flow. This value gives great confidence that hardly exist another sequence of data, which has the same integrity value or if exist pretty different.

With this method link errors can be revealed, but man-in the middle attacks are not.

Therefore authentication must be added to the integrity check so that the integrity value not just ensures that the message was not altered, but it was not modified since the source.

4.5 Non-Repudiation

In order to reveal compromised nodes non-repudiation is desired. It can be accomplished as some unique token “stamps” the messages. This can be public/private keypairs, but even symmetric keys.

4.6 Keeping Anonymity

4.6.1 Authentication of node vs. authentication of user or higher level applications

Link layer level node authentication must not reveal the identity or other private information of the user or higher level application. Also the authentication and communication in the lower layer should minimise that risk

the attacker could deduce the set of devices which the user might use. For example avoid that the neighbours can easily collect information.

4.6.2 Hiding Identities

The authentication phase should reveal some information about the node identity. This information can be useful for attacks, which targets one specific entity. However there are existing methods, e.g. Zero knowledge proofs [Scheiner] ensure proper authentication without uncovering the identity of the entity.

4.7 Countermeasures against Physical Access

4.7.1 Physical Protection

Proper physical protection is not typical for mobile ad-hoc equipment. Therefore other tricks should be used to make effective tamper impossible (e.g. usage of password for the console). But the attacker with hardware tamper could get the secret for authentication and communication.

4.7.2 Key Expiration and frequent and proper authentication

In order to avoid the usage of obtained secret of communication frequent key change and proper authentication (check whether the requestor is not a compromised node) is needed.

4.7.3 Identification of Compromised Endpoint

If the tamperer obtains the identification credentials for authentication, IDS might identify that the node is compromised. In that case non-repudiation is needed.

Also with frequent authentication with up to date lists of compromised nodes the malicious node can be excluded easily.

4.8 Radio Resource Protection

Radio resource requires protection against eavesdrop with encrypted communication channels and secure routes. Also protection against DoS attacks should be ensured.

4.9 Distribution of the Centralised Trust Infrastructure

Although no secure centralised trusted infrastructure in ad-hoc networks, there are methods to provide similar and robust functions than a KDC (Key Distribution Centre) or CA (Certificate Authority) provides. The solution relies on the Threshold Cryptography [AdHocSec], which allows a n number of nodes to share the ability to perform a cryptographic operation (e.g. creating or verifying digital signatures) so that any t nodes from the n node can perform the operation jointly. In that case even t-1 nodes can be compromised the result of the function still remain proper.

4.10 Collective Mind

If the whole ad-hoc network each node collects and distributes information then this collective knowledge prevents malicious nodes after recognition of them to move into another part of the network and there hose adversaries continue its task.

4.11 Protection of Routing

If the routing information is received only from trusted network elements or trusted nodes can only be found on the path discovery than the routing can be supposed to be secure.

Onion Routing collects public keys of the trusted nodes along the path. The message then is encrypted with those public keys so that with the farthest node key first and the closest node key least. Then the message is sent to that path where the routers unpack and forward toward the appointed destination.

The procedure provides not just trusted but also confidential routing.

4.12 Key Management

Key management has to ensure proper frequent key changes, and key distributions. It should be based on Diffie-Hellman algorithm [AdhocKey] since generally no shared secret exists. However DH requires proper authentication.

5. Mobile Ad-Hoc Implementations for Security

5.1 WEP

The wired Equivalent Privacy was designed to achieve as quality of security as in the wired environment exists [WEP].

Soon it is realised that WEP provides no security at all since practical attacks against WEP are succeeded regardless of the key size or the cipher. In particular, as currently defined, WEP's usage of encryption is a fundamentally unsound construction; the WEP encapsulation remains insecure whether its key length is 1 bit or 1000 or any other size whatsoever, and the same remains true when any other stream cipher replaces RC4. The weakness stems from WEP's usage of its initialisation vector. This vulnerability prevents the WEP encapsulation from providing a meaningful notion of privacy at any key size.

The deficiency of the WEP encapsulation design arises from attempts to adapt RC4 to an environment for which it is poorly suited.

WEP also uses a CRC for integrity check. However there are differences between data error detection from secure integrity check. The latter uses not only bit error detection, but gives unambiguous evidence that the information was sent from the presumed source and no modification had been done [RC4], [NoClothes], [Unsafe].

5.2 Bluetooth

5.2.1 Bluetooth security

The security of Bluetooth relies on four entities: the device address, which is, consists of 48 bit and unique for each device; the authentication key (128 bit random number); the encryption key (8-128 bit) and a random number RND. The authentication key is used for authentication while the encryption key is used for encryption.

Bluetooth has three security modes. Mode 1 provides no security, Mode 2 provides service level enforced while Mode 3 provides link level enforced

security. Between security Mode 2 and 3 the difference is that in Mode 3 Bluetooth device initiates security procedures before the channel is established.

In Bluetooth a device can be trusted or untrusted. A service either requires no security or requires authentication or requires authentication and authorisation too.

There are several link keys in Bluetooth: the unit, initialisation, combination and master key. The unit key is generated when the device is in operation for the first time and stored to non-volatile memory. The initialisation key is needed when two devices have no prior engagements (no unit or combination keys). In that case the PIN code (1-16 bytes) is entered. The combination key is used if the devices have decided to use one. In that case they generate and exchanges securely. The master key is the only temporary key created from two random numbers.

The Bluetooth uses Challenge-Response authentication [Bluetooth].

5.2.2 Problems in security of Bluetooth

The Bluetooth Stream cipher E0 can be broken in certain circumstances.

There are usability problems with the PIN code since either user must enter twice every time connect to the device or place physically to each device. The former raises usability the latter security concerns.

Also the strength of the initialisation key is based on the PIN codes. The regular length is 4 digit of the PIN code, which provide poor quality for protection.

Unit key is used as link keys if the peer lacks of resources. In that case assume node A has no resource to generate other keys, therefore node A will communicate with node B and C with the same key. In that case node C can fool node B, as he is node A and vice versa [BTSec].

6. Conclusion

In the mobile Ad-hoc environment the number of existing threats are much more than the other wired or wireless systems. Also several security mechanisms which was outstanding in the wired or centralised mobile environment is useless due to ad-hoc environment is not have those assumptions. If security is established in the MAC layer, then system requires some non ad-hoc properties due to security cannot be implemented without either confidentiality or integrity or authentication. And those require some pre-placed secret.

Layer 2 (link level) security methods can only be served with the upper layer security services. In the upper layer not the equipment but the services and users are the targets of security and those are the ones require protection. Also the users change terminals therefore theirs access points also varying and the lower layer security protocols are not suitable for that ad-hoc environment.

Lower layers also more vulnerable to attacks too. They are vulnerable against DoS attacks.

Due to resource problem the algorithms are also weaker so they are usually vulnerable even against other attacks.

References

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

[80211] ISO/IEC 8802-11: 1999 IEEE Standards for Information Technology - Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Network - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

[Bluetooth] The Bluetooth Specification v.1.0B http://www.bluetooth.com/developer/specification/specification.asp

[WEP] ISO/IEC 8802-11, Chapter 8.

[NoClothes] W. Arbaugh, N. Shankar, J. Wan Your 802.11 Wireless Network has No Clothes, 2001

[Unsafe] Jesse R. Walker: Unsafe at any key size; An analysis of the WEP encapsulation, 2000.

[SecIssues] F. Stajano, R. Anderson: The resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks, 1999 AT&T Software Symposium

[BTSec] J. T. Vainio: Bluetooth Security, 2000. http://www.niksula.cs.hut.fi/~jiitv/bluesec.html

[AdhocKey] M. Hietalahti: Key Establishment in Ad-hoc Networks

[AdHocSec] L. Zhou, Z. J. Haas: Securing Ad-hoc Networks, IEEE Network Nov/Dec 1999.

[QuestFor] J.-P. Hubaux, L. Buttyan, S. Capkun: The Quest for Security in Mobile Ad Hoc Networks, MobiHOC 2001.

[RC4] Fluhrer, Mantin, Shamir: Weaknesses in the Key Scheduling Algorithm of RC4

[RFC2828] R. Shirey: Internet Security Glossary, RFC 2828 May 2000.

[Schneier] Bruce Schneier: Applied Cryptography, Second edition, John Wihley 1996.

Kassai Károly

RESPONSIBILITY FOR A SECURE CIS[7]

In last ten years Republic of Hungary was developed a new security environment in Europe. The political, social, economical and military radical changes and technological development has taken a new situation for us.

Like most of the states Hungary also has a comprehensive approach to the security. Beside several traditional and new elements of security the information security[8] has an increasing role.

The information for the governments, business, military and other organizations is more and more valuable. The efficiency and security of data transmission and processing systems are playing an increasing important role in the functioning of state structures and society.

However, the information environment includes a lot of organizations, persons, networks, computers and other devices. Among these elements there are some cooperative partners but there are enemies, too.

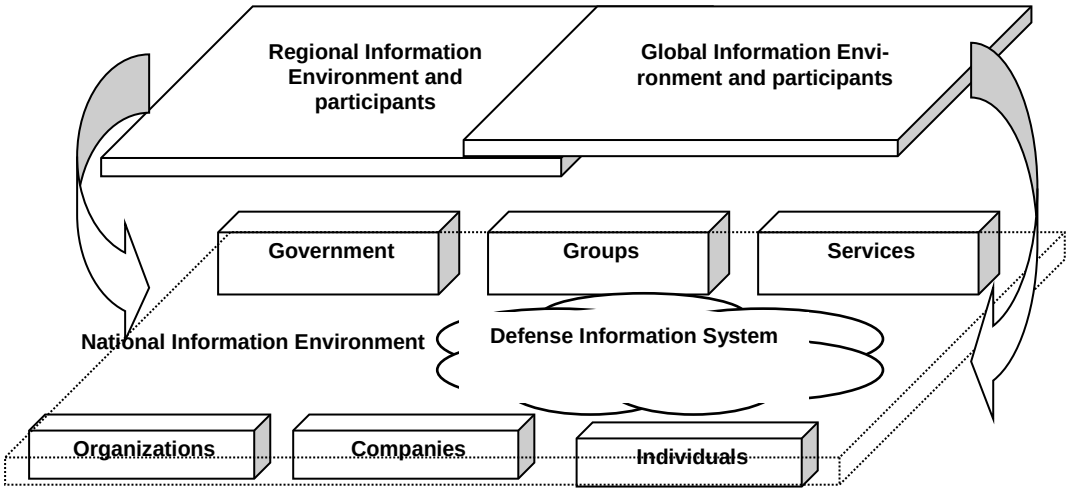


Figure 1: The environment of Defense Information System

[7] Communications and information system (CIS): assembly of equipment, methods and procedures, and if necessary persons, organized so as to accomplish specific information conveyance and processing functions (AAP 6(V). Hungary defense Force (HDF) hasn't a conventional CIS because the voice, fax, teletype systems are separated from the informatics systems.

[8] Information security: The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users (JP 3 - 13).

The information revolution is useful, but there are some aims and interests, which are hostile to national or international communication system. Thus, we must protect our information and information systems.

The technological progress, the scope of risks and sources of danger have increased and grown more complex. For instance the financial, energetically systems, the various administrative networks, air traffic control systems, as well as the greatest number of military communication systems includes a lot of elements which easy to attack.

The defense of information and information systems is a difficult and complex issue. There are some information, which help somebody to penetrate and to disable electronic and information systems, so the target of attack is not only the sensitive (or classified) information but also several information from the communication systems or elements of system.

The dangers

The *critical infrastructures* (including telecommunications, energy, financial, transportation etc. systems) are vulnerable to computer and physical attacks. This attack is not a conventional attack already.

The aggressor (or intruder) may be an educated engineer, who knows a lot of information about computer technology, or a hacker who has a high-level equipment or a curious student who now has to study the programming of computer, but may be a terrorist or armed criminal.

While teenagers, and children work on computer at home and at the school, we have old systems and equipment, so the protection of conservative (documental)- or electrical information is a difficult problem.

The main danger against the military CIS is the new part of warfare: the *information warfare (IW)*.[9] There is a lot of equipment, method and technology (e.g. network centric warfare, computer network attack), which helps to compromise the information or keep back operation of information network. The computer viruses are getting more and more dangerous, and may be virtually undetectable by conventional antiviral software. Trojan horses, logic bombs and other malicious software are appearing on our systems, and require improved countermeasures and careful security procedures.

There isn't a warning signal before the attack against a communication network and the attacker's aims and technology are often unknown.

The attack may be a *combined action* and may affect more points of network at one time. The support system of CIS, the links and the switches of the network, the controls of network have complicated elements, which have to cooperate. If the cooperation stops in the network, the network can't provide

[9] Information warfare: information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. (JP 3-13)

services for users and a lot of communication systems can't work. If there isn't appropriate contact among the units, a lot of information that is gathered about the battlefield, the enemy, the weather, the units, the reserves etc. by reconnaissance systems and sensors can't be processed, so the cycle of decision became longer and the risk of actions grows.

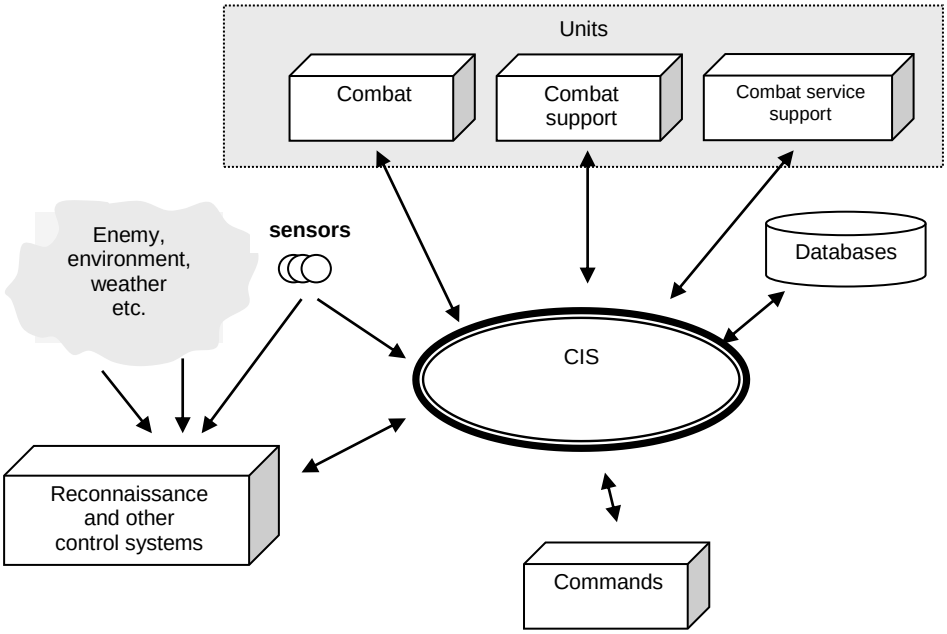


Figure 2: The users of CIS

The enemy is *not only outside* the network. Most of the sources say, that insiders commit 80-85 percents of computer crimes with validated access to the resources of the systems. Insiders abuse of their authorization or make mistakes.

A lot of people can access to several point of network during the maintenance, repairing and up-date inside the organization. Because of the comprehensive dangers the communication network has *security management* beside the fault, performance, accounting, and configuration management.

During the work the users and the operators make mistakes, too. A password on a piece of paper, a floppy on the desk without supervision or a copy of a sheet of paper cause trouble to the absent-minded user or the management of the security. In another occasion an untrained user uses malicious software or an operator makes a mistake and break down the network or a part of network.

Without the human factor there are also some dangers, which threaten the information or the information systems. In a critical moment a power cut, a fire, a hardware trouble, an interruption of transmission or a mistake of the network supervision is an obstacle of information flow.

The task

Because a lot of information is in danger, we have to protect all elements of CIS by appropriate protection equipments and methods.

The modern information security system has three main areas: the *documental* security, the *electrical information* security and the *technically secure area.*

This information security system based on four pillars:

- physical security;
- personal security;
- document security and
- procedural security.

In these pillars there are some special field that have to realize the availability, integrity and confidence of information. These fields are *the communication security* (include transmission, cryptographic and emission security) and *the computer security* (include hardware, software, and firmware security).

Nowadays, when we have to build a new communication infrastructure for the Hungarian Defense Force, we have to study and collect a lot of information about the goal, the task, the structure and the weakness of modern information systems then we will have a well-constructed, powerful and cost-effective system.

Therefore we have to plan carefully the CIS and have to form a good supervisor and control system, and we have to use preventive, corrective and controlled maintenance system and have to build a powerful instruction and practice system.

We have to build a lot of well-matched security elements based on a central security point of view into CIS. The security isn't based on the great number of protective elements but the harmony and the quality. The hardware and software components and the policy of security system can't be changed permanently.

All organizations must have procedures and guidelines in a written security policy. An effective security policy covers three things: technology (how often the systems are updated and how it can be accessed by people and processes), people (password procedures, user's responsibilities and acceptable use of the equipment of organization) and processes (emergency response, changing the access control when an employee resigns, reporting the violations and drawing the conclusion of them).

Each command, unit, and branch of service must have it's own security management. The security management has to coordinate the goal, task and

structure of protection of information against the sabotage, tampering, denial of service, espionage, fraud, misuse, misappropriation, access by unauthorized person, snuffing, eavesdropping, and so on.

The security management has to know and understand the task of units (or other organization), the threats, the risks, the vulnerability of information system. So the management can make a comprehensive security program for peacetime, conflict and war.

This security program will control the system, analyses the risks and determines the view and tasks of the security training. It's impossible to work on modern communication systems without appropriate qualification. The users' responsibility is protecting that information from unauthorized disclosure. Users have to understand the function of equipment, have to have knowledge of computer programs and have to keep the rules of security. Individuals have to be trained

- to know the weakness in information systems;
- to be informed of the threats, vulnerabilities of information systems;
- to recognize the vulnerability of information systems;
- to take the necessary measures to protect the generated, stored, processed, transferred information;
- to recognize the compromise and to know the action of protection.
- to understand and be practiced in the execution of emergency plan.

The efficiency and security of data transmission and processing systems are playing an increasingly important role in the functioning of state structures and society. We have to plan, maintenance and develop good security programs for the information security because the military force have a lot of arms, equipments and material, which are dangerous in unauthorized persons' hands.

References

1) NATO glossary of terms and definitions AAP-6 (V)
2) NATO TACOM Post architecture, http://194.7.79.15/Volume02/Annex_A-00.htm
3) Joint Doctrine for Information Operations JP 3-13
4) Maintenance philosophy for telecommunication networks C C I T T M .20
5) Information Operations FM 100-6

Zömbik László

USING THE INTERNET FOR DEFENCE IN THE XXI CENTURY

Ericsson Research, Hungary
laszlo.zombik@ericsson.com

Abstract

Under the ARPA project of US Defense of Department a research communication network born. From the so-called ARPANET outgrew the Internet. Since the beginning till nowadays the number of the hosts is powerfully increasing. The Internet Protocol (IP) and other IP based protocols provide not just robust, but effective information transfer.

At certain circumstances the Internet, this civilian infrastructure, can be used for military or intelligence communication. In this document a framework describes in which circumstances can the Internet based communication be used for this purposes.

Future directions of evolution of the Internet will also be considered in order to show the way of the seamless usage of the Internet for military and intelligence communication in the XXI century.

1. The past of the Internet

In the beginning the Internet was not a commercial communication network, it was born form a research network sponsored by military. In order to be capable to understand the future of the Internet and also to understand how can it be used for defense purposes we have to look back on the past.

1957 USSR launches Sputnik, first artificial earth satellite. In response, US form the Advanced Research Projects Agency (ARPA) within the Department of Defense (DoD) to establish US lead in science and technology applicable to the military. [Timeline]

1962 Idea of packet switching networks presented.

1965 Two research lab in Santa Monica and in MIT are directly linked (without packet switches)

1967 First design paper on ARPANET

1968 Packet-switching network presented to the ARPA

1971 15 nodes (23 hosts) connected containing MIT, Harvard, Stanford and NASA/Ames. The email program had been invented.

1973 First international connections to the ARPANET: London and Royal Radar Establishment, Norway.

1979 Packet Radio Network (PRNET) experiment starts with DARPA funding. Most communications take place between mobile vans. The experiment connected to ARPANET.

1982 The Transmission Control Protocol (TCP) and the Internet Protocol (IP) introduced, as the protocol suite, commonly known as TCP/IP, for ARPANET. This leads to one of the first definitions of an "internet" as a connected set of networks, specifically those using TCP/IP, and "Internet" as connected TCP/IP internets. DoD declares TCP/IP suite to be standard for DoD.

1983 ARPANET split into ARPANET and MILNET; the latter became integrated with the Defense Data Network created the previous year.

1984 Number of hosts breaks over 1,000.

1988 2. November - Internet worm burrows through the Net, affecting approximately 6,000 of the 60,000 hosts on the Internet. CERT (Computer Emergency Response Team) formed by DARPA in response to the needs exhibited during the worm incident. The goal of CERT is to study Internet security vulnerabilities, handle computer security incidents, publish security alerts, research long-term changes in networked systems, and develop information and training to help improve security of hosts. From this year other countries also connects to the network.

1989 Number of hosts breaks 100,000 limit. [Timeline2]

1990 ARPANET ceases to exist. The first commercial Internet provider starts dial-up access services. The first remotely operated machine, which is not a computer but the Internet Toaster, is hooked up to the Internet.

1991 World-wide Web (WWW) released. PGP (Pretty Good Privacy) released. Hungary connects to the Internet.

1992 Number of hosts breaks over 1,000,000.

1995 WWW surpasses ftp-data. The first official Internet wiretap was successful in helping the US Secret Service.

1996 Internet phones catch the attention; the toll of the long-distance calls starts to fall. Various ISPs suffer Denial of Service (DoS) attacks. US Government sites are hacked into and their content changed, including CIA, Department of Justice, Air Force.

1999 The first full-service bank available only on the Net opens for business. First large-scale Cyberwar takes place simultaneously with the war in Serbia/Kosovo. Activists' Net-wide target the world's financial centers on 18 June timed to coincide with the G8 Summit.

2000 Time services around the world report the New Year as 19100 on 1 Jan. Massive denial of service attack is launched against major web sites, including Yahoo, Amazon, and eBay.

2. Future of the Internet

A military sponsored research network became a communication network between research centres. The next step in the evolution was the network access for commercial use. This made it possible that nowadays nearly everywhere in the World one can connect and surf on the net. Enormous information became available which affected the society. It is natural nowadays that we are sending emails, surfing on the net, reading the news, listening to radio or making phone calls.

There are existing trends, which shows the place of the Internet in the near future.

It is seen that nowadays due to the globalisation and the increased needs of the customers the telecommunication, data communication, multimedia and the other parts of informatics industry are integrating.

Since the appearance of the voice over IP applications the telecommunication vigorously merges and even in the far future might became part of the data communication, especially the Internet services.

The other multimedia applications (e.g. video) also follow that direction.

Therefore one can say that the Internet Protocol (IP) can be a general network protocol in the future. The new Internet Protocol (IPv6) is designed to meet for those requirements.

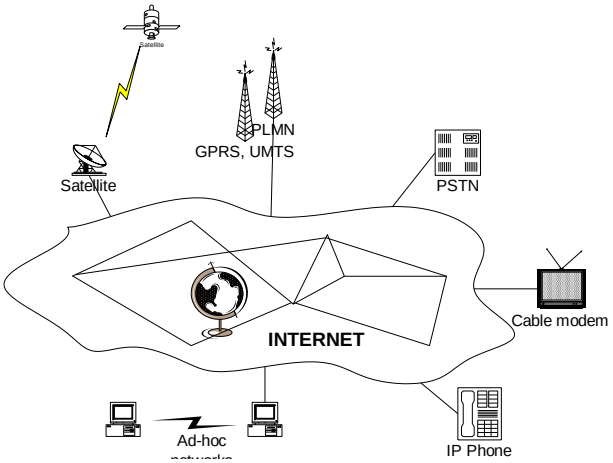


Figure 2.1 Internet over the World

Although IP can be a general unified transport protocol, but various physical layer supports is required. Therefore for example the research interest of the data communication over the power cables, over high-voltage long-range wires had been grown. Since those are the existing networks which have the longest lines, which are enmesh the world and reach and ends at the users.

Nowadays there are existing solutions for Internet access not with just direct (Ethernet) link or phone modem (analogue, ISDN, etc.) access, but Internet access can be reached on cable television (cable modem) on microwave links too.

Over the Public Land Mobile Network (PLMN) also capable to establish connection to the Internet. Examples can be the GPRS on GSM, and UMTS. There are other short-range, ad-hoc radio networks e.g. 802.11 WLAN, or Bluetooth. For long-range or high-speed communication the fiber optic can be used. On those areas where no other access found satellite communication can be solution.

The Internet will make changes in housekeeping too. The home network connects to the Internet, therefore the status can be inquired or the home can be remotely controlled. To reach this a well-developed communication network is required like nowadays' power lines.

Not just electronic toys, computers, printers or telephones will connect into the home network infrastructure, but other equipment like microwave ovens, cookers, bulbs, etc. Therefore the gas cooker can be checked whether it was switched off, or the bulb can be ordered to be switched off remotely, even from other side of the world or the alarm system can give status whether everything is fine at home.

3. The Dark Side

In the Internet community likewise as in the human societies destructive members exist. Since the mid-nineties the malicious attacks became unbearable. The attacks endangered the trust of the benevolent users, which could cause the Internet became a cyberspace of lunatic users.

The menace was dangerous, since the protocols and the architecture basically followed the "be nice" rule. For example the task of the ping command to check whether the host of the other party is connected or not. So if the other host acts nice, and it answers to the query. But this can be the method for an attack if mounting a flood of these ping requests might make the other party's host to crash.

Also the basic, widely used network services (e.g. ftp, telnet, etc.) provided no protection against eavesdroppers. Therefore access to the system resources could be easy.

In the other hand nowadays with the available algorithms one can encrypt traffic in such a way that there is hardly breakable for even the highly trained government forces. Therefore it could be a good opportunity for criminals.

From those reasons law control is required for the Internet, describe what and how can the cyberspace be used. It is very hard to establish and execute regulations since the Internet is spread out into countries.

Due to the regulations by the laws and the secure procedures not grew with the technical capabilities and the users' needs the Internet became untrusted.

However this network can be used for military or intelligence communication due to it is widespread, robust, effective and secure communication can be deployed. The following chapter describes the advantages of the IP based communication chapter 5 gives guidelines about the usage of Internet and chapter 6 contains some existing security procedures and services for protecting the communication over the IP.

4. Internet and defense

The XXI century is the century of communication everybody can be reachable irrespective of distance. Electronic tools can be remotely controlled even if it is not wired to any network. This requires a multiply connected backbone network.

This network is for commercial use and since nowadays trends show this is based on IP. Due to those network elements are civilian objects and due to the large number of nodes it may not be military targets. Since the IP was designed to handle link and node breakdowns it gives robust transport architecture. Also since those are not military objects there are not primary targets. In addition destroying those objects might cause different political situation too.

This architecture is cheap since the development and maintenance cost is not paid by military. Also since protocols are well known and the mass-production of hardware makes low cost and easy-to-build equipment.

Besides localisation can be harder than the pure radio-based equipment, since with the radio-wave emission the spot of radio tools can be easily determined. Note that IP equipment may use radio link too.

Due to the enormous access points it can be used for military intelligence for example to place and watch the situation on a web camera. The solution is cheap already. Another possible usage can be the monitoring of blocked nodes or broken lines. From that information the line of the battle might be deduced.

There is one mayor disadvantage of that architecture, the power failure. In that case nodes can stop its services and important lines can go offline. Since the communication does not highly consumer power some back-up batteries UPSs can resolve the power for short time outages. Power generators can give long-range power supply, installing them into main or important nodes, is reasonably.

Note that a disconnected sub network can also be used for communication between troops, and dynamic connection can also be established (with e.g. directed radio link) after critical node failure. The network protocol (IP) can easily adapt to the changed circumstances.

Therefore on the IP based transport network military intelligence containing identification, location is easy to deploy. Also it is useful for troops to communicating (including voice, video or data) with each other or the base.

5. Integrating the labelled secure network onto the untrusted

The military communication network must be a secure one anybody except the authorised endpoints must have access for any information. With standalone network infrastructure (e.g. separated military mobile network) this requirement can be easily reached. From that solution it follows that the physically separated network can be very well identified target for enemy forces.

On the other hand if the military communication aggregated with other civilian communication traffic can easily observed by the enemy intelligence and might be decrypted. (For example if the military network uses the same frequency range and protocol – e.g. it uses one channel in the GSM range and communicating through GSM messages.)

In addition if the military communication is implemented just only on the aggregated infrastructure this network might easier be identified than the standalone since the procedures are well known. Therefore those became similarly to the standalone primary targets for the enemy. This solution also has weaker penalty for spying.

In order to provide robust communication network under attack where nodes can go offline the system should contain both solutions. Therefore the standalone communication can be for the main communication and the aggregated infrastructure for backup and intelligence communication. In that case the primary targets are the network elements of the standalone communications. Secondary targets can be the backup infrastructure which destruction with the primary might cause high cost for the attacker.

Note that the civilian networks in the XXI century became very complex multiply connected graphs and the network protocols can easily handle link or node failures. Therefore they can be good bearers for backup communication. (Figure 5.1)

To reach this the backup network must be implemented and prepared before any combat situation. Therefore it must be built in “peace” when the civilian hackers can hit or identify and also might publicate the information they could reach. In order to handle this risk network designers can deploy decoy hosts with well-known name and some services. Those works as a honey-pot for the attackers therefore not just attract them but information about its methods and behaviour can be collected. In the background some no-name well-secured hosts can provide the required backup services. Those should be fix and always prepared nodes. Besides the hot-standby nodes, some not connected but ready for on-line communication nodes should be placed. These can provide surprise for those enemies that can even chart the network of hot-standby nodes. (Figure 5.2)

Also the maintenance of backup network can be easier since there are more experts repairing the civilian infrastructure. This can be a task of civil defence.

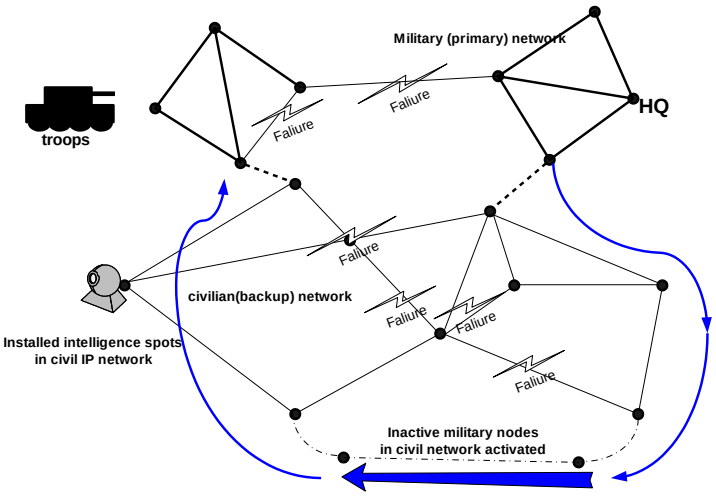


Figure 5.1 military and civilian network when military networks damaged the backup civilian network can be used

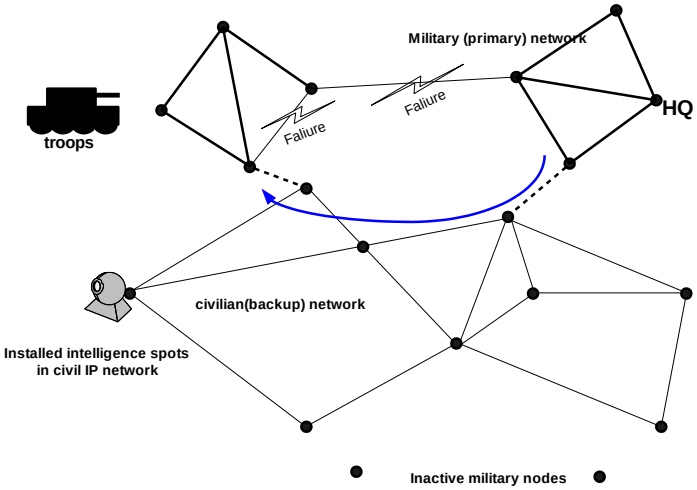


Figure 5.2 military and civilian network when military and civilian networks are damaged the inactive nodes can be used

6. Security mechanisms on IP

There are existing security procedures and services for protecting the communication over the Internet. Due to the protocols are flexible and usually not depend on each other some can be applied some can be modified in order to provide labelled security communication. Usage of these protocols beneficial since a malicious user primarily searching for some "strange" protocol. Although the protocols or the message headers are standard contains should be protected with stronger cryptographic algorithms.

Also usage of widely used security protocols, which are tested against hackers every day provides less risk due to those protocols are refined when a new security risk rises. Some protocols, which are widely used in the Internet, will be introduced. The cryptographic algorithms will not be described here since those are always changing due to the computational power is increasing and due to it might be algorithms found which provides less computational task for the cracker.

In order to provide secure communication in between two nodes key negotiation and security protocol, based on the negotiated keys, required. The key management provides procedures with the peers can identify some secret information (keys) and other parameters (e.g. expiration of key) in order to secure communication became realisable. Security protocol gives framework for cryptographic algorithms with using the given secrets to provide private, authenticated, replay protected and integrity checked communication.

6.1 Security traffic protocols

6.1.1 IPSec

IPSec [IPSec] uses two traffic security protocols, the Authentication Header (AH) [AH] and the Encapsulating Security Payload (ESP) [ESP].

The IP Authentication Header provides connectionless integrity, data origin authentication, and an optional anti-replay service.

The Encapsulating Security Payload protocol may provide confidentiality (encryption), and limited traffic flow confidentiality. It also may provide connectionless integrity, data origin authentication, and an anti-replay service. (One or the other set of these security services must be applied whenever ESP is invoked.)

A simplex connection, that affords security services to the traffic carried by it, is called Security Association (SA). Security Associations can be used between two hosts. In that case IPSec is used in Transport mode. If Security Associations applied to an IP tunnel then IPSec in tunnel mode. Usually the latter mode is used between two VPNs. (Figure 6.1)

On each node Security Association Database (SAD) and Security Policy Database (SPD) exists. The Security Association Database contains parameters that are associated with each (active) security association. The Security Policy

Database specifies the policies that determine the disposition of all IP traffic inbound or outbound from a host or security gateway.

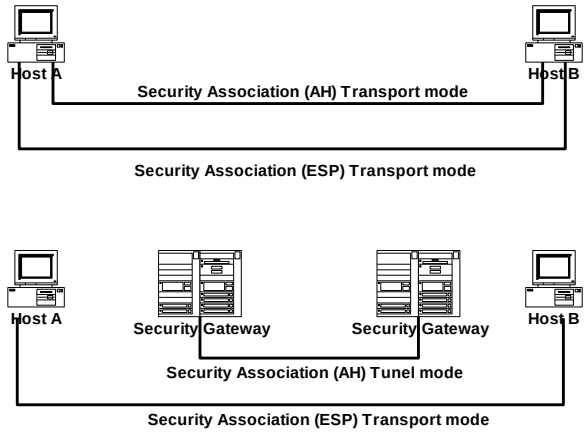


Figure 6.1 IPSec in transport and tunnel mode

6.1.2 SSL and TLS

The primary goal of the TLS [TLS] Protocol is to provide privacy and data integrity between two communicating applications. The protocol is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol. At the lowest level, layered on top of some reliable transport protocol (e.g., TCP [TCP]), is the TLS Record Protocol.

Record Protocol provides connection security that the connection is private and reliable. Symmetric cryptography is used for data encryption integrity check is used for detecting malicious modifications and peer identity is authenticated to check that the communicating parties are they claim to be.

The Handshake Protocol is used to allow peers to agree upon security parameters for the record layer, authenticate themselves, instantiate negotiated security parameters, and notify error conditions to each other.

The SSL (Secure Socket Layer) [SSL] was the ancestor of TLS. Therefore the services and goals of SSL is similar to TLS.

6.2 Key management protocols

6.2.1 Kerberos V.

The Kerberos [KerverosV] is designed to provide easy key distribution in client-server architecture with using a common trusted node, which called Key Distribution Centre (KDC). The Key Distribution Centre consists of two parts the Authentication Server (AS) and the Ticket Granting Server (TGS).

The client, who wants to communicate with the server, authenticates with using the pre-shared secret in between the client and the KDC. The Authentication Server then gives a key for communication with Ticket

Granting Server and a ticket. The ticket will be the authentication to the TGS. Then the TGS gives keys for the server, with which the client wants to communicate, and a ticket for authenticating to the server. The tickets contain a key for communication to the client.

6.2.2 ISAKMP

The Internet Security Association and Key Management Protocol (ISAKMP) [ISAKMP] defines procedures and packet formats to establish, negotiate, modify and delete Security Associations (SA). SAs contain all the information required for execution of various network security services, such as the IP layer services (such as header authentication and payload encapsulation), transport or application layer services, or self-protection of negotiation traffic. ISAKMP defines payloads for exchanging key generation and authentication data. These formats provide a consistent framework for transferring key and authentication data which is independent of the key generation technique, encryption algorithm and authentication mechanism.

6.2.3 IKE

The purpose of the Internet Key Exchange [IKE] protocol is to negotiate, and provide authenticated keying material for, security associations in a protected manner. ISAKMP is designed to be key exchange independent; that is, it is designed to support many different key exchanges, like IKE.

6.3 Nodes for security

There are nodes in the IP world, which have dedicated security services. Here some essential objects are listed.

6.3.1 Security Gateway

A node provides IPSec encapsulation or decapsulation for packets. At the Security Gateway starts or ends an IPSec tunnel.

6.3.2 Firewall

Either packet filter or application level filter machine. If firewall is used in packet filter mode than certain packets will be passed some are not according to the source, destination IP address, services or direction.

The application level filtering firewall not only checks the IP header of the packet but it makes sure that the message is suitable for the specified protocol.

6.3.3 Proxy

The proxy is an application level translator, which resides in between communicating peers and hides the other party's identification. The path in between the peers cannot be established due to firewalls, without communicating through the proxy.

6.3.4 Honeypots

Nodes in the network attract interests of malicious users, which try to hack, crack or break down the node. The goal is that the attackers became misleaded, and therefore divert attention from other key hosts. Also the behaviour and

identification of the malicious user can be deduced. In that way the host registers and sends to a trusted machine every tries of improper behaviour.

7. Conclusion

The XXI century is the century of war of information. This is true not just for military but even for civilian area. The information became the primary weapon and with blocking or spreading war can be won. In this paper the idea of usage of a globally available fault tolerant civilian data communication network (IP network) for military communication purpose is described.

References

[IPSec] S. Kent, R. Atkinson: Security Architecture for the Internet Protocol. November 1998. RFC 2401

[AH] S. Kent, R. Atkinson: IP Authentication Header. RFC 2402

[ESP] S. Kent, R. Atkinson: IP Encapsulating Security Payload (ESP).

[SSL] Alan O. Freier, Philip Karlton, Paul C. Kocher, "The SSL Protocol Version 3.0 " Internet Draft, draft-freier-ssl-version3-02.txt, November 1996.

[TLS] T. Dierks, C. Allen: The TLS Protocol Version 1.0. RFC 2246.

[ISAKMP] D. Maughan, M. Schertler, M. Schneider, J. Turner: Internet Security Association and Key Management Protocol RFC 2408

[IKE] D. Harkins, D. Carrel: The Internet Key Exchange (IKE). RFC 2409

[KerberosV] J. Kohl, C. Neuman: The Kerberos Network Authentication Service (V5) RFC 1510

[Timeline] R. Zakon: Hobbes' Internet Timeline RFC 2235

[Timeline2] http://www.zakon.org/robert/internet/timeline/

Ternyák István

A MAGYAR KATONAI KOMMUNIKÁCIÓ LEHETSÉGES FEJLŐDÉSI IRÁNYAI

A magyar katonai kommunikáció lehetséges fejlődési irányainak vizsgálatánál számba kell vennünk:

- a katonai információtechnológia lehetséges fejlődési irányait;
- a magyar polgári és katonai információtechnológia jelenlegi helyzetét, mint kiindulási alapot;
- a Magyar Honvédség jövőbeni alkalmazásának lehetséges feladatait, a vállalt szövetségi kötelezettségeket;
- saját döntési lehetőségeinket, amelyekkel elősegíthetjük, vagy éppen lassíthatjuk a fejlődést.

1. A katonai információtechnológia lehetséges fejlődési irányai.

Az információtechnológia szűkebb értelemben a híradástechnika, a számítástechnika és a média technológiáinak és piacainak konvergenciája. Szinonim fogalomként használják az informatika (IT ipar) megnevezést is.

Tágabb értelemben az információtechnológia a híradástechnika, a számítástechnika, a műsorszórás és média ipar, a szélesebb értelemben vett ipar, továbbá a szolgáltató ipar – egészségügy, oktatás, bankszféra, kiskereskedelem – technológiáinak és piacainak konvergenciája.

Magyarország Nemzeti Informatikai Stratégiája megállapítja: „A számítástechnika és a távközlés technikai konvergenciát mutat.” Alapját a digitalizálás teremti meg, amelynek során minden fajta információ (kép, hang, szín, szám, stb.) elektronikusan reprezentáltan számjeggyé (digitekké) alakul, amelyeket nagy biztonsággal képesek a számítógépek tárolni, feldolgozni, illetve a távközlési hálózatok továbbítani. A harmadik pólus az információ tartalmának integrálódása (elektronikus média).

Az utóbbi évtizedek információtechnológiai fejlődésének két vívmánya – az Internet és a mobiltelefon – egyesül a mobil Internetben. A mobiltelefonjaink egyre inkább kisméretű számítógépekre hasonlítanak majd, illetve beépített kamerával rendelkeznek és zene lejátszására is képesek lesznek. Ezekkel a mobilokkal az emberek e-mailezhetnek, szörfözhetnek a Weben, híreket olvashatnak, tanulhatnak, segítséget kérhetnek, stb. bárhol és bármikor.

Otthonainkban (hivatalokban) a kiépített távközlő és/vagy kábeltévé/műholdas TV-hálózatokon keresztül ugyanezek a szolgáltatások állnak rendelkezésre (a nagyobb sávszélesség és felhasználói készülékek segítségével) még komfortosabban.

A technológiai konvergenciák eredményeként létrejövő információs (infokommunikációs) értéklánc elemei között horizontális és vertikális integráció (átrendeződés) valósul meg. Nő a „megfoghatatlan”, a virtuális szerepe.

Az információtechnológia fejlődése az emberiség története során eddig semmilyen más technológiánál nem tapasztalt szédületes sebességet ért el. Ez a lehetőségek szinte korlátlan kiteljesedésével párhuzamosan rendkívül nehéz helyzetbe hozza mind az információrendszerek tervezőit, alkalmazóit, mint az információtechnológia előállítóit, szolgáltatóit. Komoly kihívást jelentenek napjainkban a rendkívül gyors eszközcsalád változások, amelyek komolyan befolyásolják mind a polgári, mind a katonai rendszerek hosszú távra szóló fejlesztéseit. Az ismert amerikai számítógépes szoftverfejlesztő mérnökről elnevezett Moore-törvény szerint a számítógépek teljesítménye kétévenként megduplázódik. Szédületes tempóban nő a számítógépek műveleti sebessége, a tárolók kapacitása. Folytatódik a miniatürizálás, ami elősegíti az intelligens fegyverrendszerek, robotok fejlesztését. Tudósok értékelése szerint az információ technológia forradalmi fejlődésének harmadik szakaszában vagyunk. Az első szakaszt a mikrochipek, a másodikat a lézertechnológia megjelenése jellemzi. Az első lehetővé tette a PC-k, a második az Internet elterjedését. A harmadik szakaszt az érzékelők, sensorok teljes világunkat behálózó megjelenése fogja jellemezni, ami az adatgyűjtést, adatszerzés automatizálása révén minden eddiginél hatékonyabbá teszi információs rendszereinket.

A biológiai, orvostudományi és az információtechnológiai kutatások konvergenciájának eredményei jelenleg beláthatatlanok, egy példaként az ember-gép kapcsolat mindkét oldalának összehangolt vizsgálata azonban – már ma is számos újdonsággal szolgál.

A **katonai információtechnológia** a híradás (kommunikáció), a számítástechnika és az információs rendszerek (katonai informatika), az érzékelő (információforrások, szenzorok, navigációs és IFF eszközök) és a fegyverirányító rendszerek technológiáinak, szervezeteinek és alkalmazásainak konvergenciája.

A védelmi szférában – a technológiai fejlődésre alapozva – új, komplex, a katonai gondolkodásmódot gyökeresen megváltoztató fogalmak és tevékenységek jelentek meg, amelyek átformálták a doktrínákat, szervezeteinket, céljainkat, prioritásainkat, az elérendő képességeket és azokhoz vezető utak módjainak, módszereinek és erőforrásainak tervezését.

A mobil és globális kommunikáció (például katonai műholdas) egyesítése katonai célra az Internet technológiával lehetővé teszi a katonai erő vezetését és irányítását bárhol, bármikor. A COTS (kereskedelemben kapható) technikák kiterjedt katonai alkalmazása elősegíti a polgári és katonai (védelmi) infrastruktúrák összekapcsolását, az erőforrások együttes felhasználását védelmi célokra.

Meghatározó képességgé válik az információs fölény kivívásának képessége. A tevékenység, amivel a fölény kivívható információs hadviselés az állam szintjén, a vezetési-irányítási hadviselés a katonai szinten, a tér, ahol vívják az információs hadszíntér, vagy kibernetikus tér. A kibernetikus (virtuá-

lis) és fizikai térben a küzdelem az információra összpontosul, annak meglétére, hiányára, adekvátságára, tárgyhoz tartozására, időbeniségére, megbízhatóságára és pontosságára. Célpontjai azok a folyamatok, szervezeti és technikai rendszerek, amelyekben az információ gyűjtése, továbbítása, tárolása, feldolgozása és elosztása, továbbá védelme folyik. Eszközei kibővülnek a hadviselés hagyományos (tűz, csapás, manőver) eszközein túl az információs hadviselés speciális eszközeivel, úgy, mint a hálózat-központú hadviselés elemei.

Átértékelődik a hagyományos katonai erő fogalma. A tűzerő, a manőverező készség és védettség, a kiválóan kiképzett katona a kor szintjén álló információrendszerek (érzékelők, IFF, helymeghatározás, Internet, kommunikáció, védettség, alkalmazások) hiányában nem lesz képes eszközeinek alkalmazására, mert mielőbb azokat használni tudná, harcképtelenné teszik. Az információtechnológia katonai alkalmazása átértékeli magát a katonákról alkotott képet is. Az Internet korszakban született gyerekek „anyanyelvi szinten" értik az információtechnikát, kiképzésük során csak a speciális katonai ismereteket kell megtanulniuk.

Aki nem beszéli az „internetes nyelvet", vagyis nem tudja kezelni a számítógépet az gyakorlatilag csak kisegítő katona lehet, aki nem fog rendelkezni az információtechnológia eszközeivel és azok professzionális alkalmazására nem lesz felkészítve csak „áldozat" lehet.

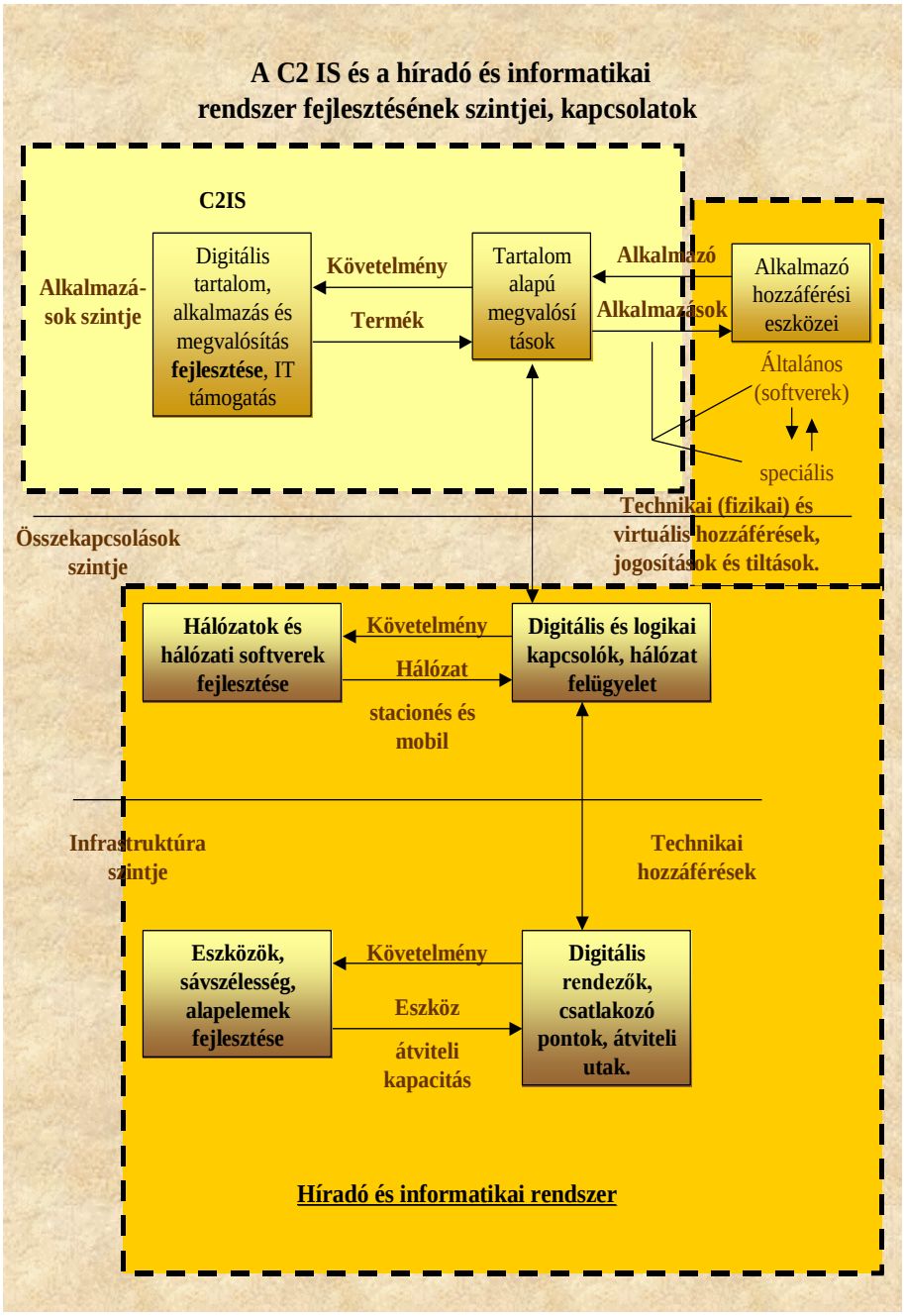
A kommunikáció, a számítástechnika és a katonai alkalmazások konvergenciája a fejlődés (fejlesztés) új formáját eredményezi. (1. sz. ábra)

Az ábrán a C2IS vezetési, irányítási információrendszert, vagyis alkalmazást jelent. Az alkalmazó hozzáférési eszközei és a technikai hozzáférés eszközei egyre többször azonosak, ilyen például a softwer rádió, vagy egy számítógép kommunikátorral.

Az ábra tartalmának azonban van egy másik fontos üzenete is. A fejlesztés logikus sorrendje:

- alkalmazói, hadműveleti követelmények meghatározása, vagyis annak, hogy mit és hogyan akar a vezető; (TARTALOM)
- a rendszerrel szembeni követelmények, vagyis annak meghatározása, hogy kik és milyen módon vesznek részt a műveletben;

és végül a technikai rendszer felépítésének meghatározása.



A három szint között a kapcsolat természetesen nem merev, kölcsönös egyeztetésük nélkülözhetetlen, ugyanakkor jelenlétük, közreműködésük elengedhetetlen.

A résztvevőknek ismerni kell egymás nyelvét, a parancsnoknak – mint a hadműveleti követelmények meghatározójának – ismerni kell az információtechnológia alkalmazását, lehetőségeit, képesnek kell lenni azt használni a vezetés ciklusában.

Az információtechnika szakértőinak tudni kell „parancsnokul".

Feltehető a kérdés, *kiből lesz a jövő katonai vezetője?*

A jelen informatikusaiból (információrendszer szakértőiből), úgy, hogy megtanulnak vezetni, vagy éppen fordítva? A jelen fiatal katonai vezetői tanulják meg az informatikát? A valószínű válasz: is-is.

Milyen lesz a jövő katonája, tiszthelyettese?

A folyamatos létszámcsökkentések nem teszik lehetővé, hogy az alegységben, vagy harcjármű személyzetben minden szakterület külön szakértővel képviselje magát. Így nem lesz külön gépjárművezető, híradó katona stb, a parancsnoknak az alegysége, harcjárműve minden eszközéhez érteni kell, amelynek elengedhetetlen részét képezik az információtechnikai eszközök is. A kérdést nem így kell feltenni, hogy lőni tanuljon meg a katona, vagy például számítógépet kezelni? Mindkettőt, - és még sok minden mást is – magabiztosan kell tudnia.

2. **A magyar polgári és katonai információtechnológia jelenlegi helyzete.**

A magyar haderő elmúlt 25 éves történetében az informatikának (információtechnológiának) különös története van, fejlődése ellentmondásoktól, szakmai tévedésektől sem mentes kacskaringós út.

> A Varsói Szerződésben a 70-es években tömegesen megjelentek a fegyvernemi automatizált vezetési rendszerek, ugyanakkor a haderőnemek fegyvernemeinek rendszerei egymással sem beszéltek, nemhogy összhaderőnemi együttműködésre lettek volna képesek. A rendszerek a mikroelektronikát (integrált áramköröket) nem, vagy csak nagyon kis mértékben használták. A hálózatok kapacitását az alacsony sávszélességű, analóg híradás korlátozta.

A 80-as években ugyan megjelentek a haderőnemi automatizált vezetési rendszerek prototípusai (PASZUV, TACSVER, UNIVERZÁL, PIRAMIDA stb.) azonban a 60-as évek technológiájára alapozódtak.

A rendszerváltáshoz a 60-as, 70-es évek analóg híradó, repülőtéri navigációs és leszállító, IFF, valamint légvédelem automatizált vezetési rendszereivel érkeztünk. Az eszközök nagy része műszakilag és erkölcsileg elavult.

A döntéshozók formálisan kifejezték ugyan az informatika fontosságát, felismerték a híradás és számítástechnika konvergenciáját, azonban a fejlesztésre érdemi döntés nem született. A helyzetet bonyolította a híradó, informatikai és elektronikai hadviselési szakemberek viszonya, a konvergenciát valamennyien csak a saját dominanciájukkal tudták elképzelni. Az egyébként is szűkös szellemi és anyagi kapacitásokat egymás gyengítésére, egyedi megoldások menedzselésére és nem együtt használták fel.

Miközben a rendszerváltást követően, amíg a polgári távközlés és informatika – a piac jótékony hatásának köszönhetően – a meglevő anomáliák ellenére – dinamikus fejlődésnek indult, addig a katonai informatika néhány üde kivételtől eltekintve egyedi, egymástól független stand-alone megoldásra költötte az egyébként is szűkös erőforrásait. Az informatika nem volt a hadseregben „értékteremtő", így a folyamatos átszervezések közben presztisét és szakértőinek többségét elvesztette, a meglevő automatizált vezetési rendszerek többségét kivonták a hadrendből.

A számtalan előny mellett nálunk a személyi számítógépek tömeges alkalmazása több negatív jelenséggel párosult. csökkent a központosítás, háttérbe szorult az egységes kódrendszerek alkalmazása, tért nyertek a párhuzamos fejlesztések. Az egységesítés helyett teret nyertek az önálló kódrendszerek, sok esetben ugyanazokra az objektumokra vonatkozóan.

Igénylik az egyes számítástechnikai szakemberek mesterségbeli tudását, „kézügyességét", de kevés helyen igénylik az informatikát, mind rendszerelméleten alapuló tudományágat, amely választ adhatna az egymástól elszigetelt, önálló rendszerek egységesítésének, integrálásának kérdéseire.

Amíg a 70-es években a katonai híradás és a számítástechnika azonos, vagy egyes esetekben magasabb színvonalon állt, mint a polgári, addig napjainkra a helyzet a polgári távközlés és informatika egyértelmű fölényét mutatja. Hazánkban a hagyományos vezetékes távközlés óriási fejlődésen ment át, a piac liberalizálódása megkezdődött, az előkészítés alatt álló Hírközlési Törvény végső célnak a teljes liberalizációt jelöli meg. A MATÁV mellett több mint 25 koncessziós társaság létezik. A kábeltelevíziózás és az Internet területén kínálati piac alakult ki.

A mobiltelefonia (WESTEL – 450, -900, PANNON, VODAFON) – a 450, 900 és 1800 MHz-es frekvenciasávokat használva – óriási ütemben fejlődik ,adott a technikai és szolgáltatói feltétel a mobiltelefon és az Internet integrációjának 2-3 éven belüli piacra kerülésére. Döntés született a TETRA kormányzati rendszerként való telepítésére.

Magyarországon jelen van a világ számos meghatározó cége; nagyszámú az informatikai cégek jelenléte. A vállalatok egy része mögött jelentős hazai műszaki háttér (szoftverház, fejlesztő, gyártó) áll.

A Magyar Köztársaság NATO taggá válásával vállalta, hogy különböző képességeket hoz létre és azokat a Szövetség rendelkezésére bocsátja. A felajánlott képességek meghatározó része információtechnológiai fejlesztésekkel jár. Ezek a vezetési, irányítási, stratégiai és tábori híradó és informatikai rendszerek, a légierő vezetési, irányítási rendszere (3D radarok, ASOC, ICC, stb.), a megerősítő erőket fogadó repülőterek navigációs és leszállító rendszerei, védett levegő-föld-levegő rádiókapcsolatok, információvédelem, funkcionális vezetési, irányítási, információrendszerek (logisztikai, mozgáskoordináló,

egészségügyi, BICES – felderítő -, stb.), IFF és S mód, valamint szimulációs és számítógépes gyakoroltató rendszerek, a teljesség igénye nélkül.

Pénzügyi korlátok miatt időben későbbre tervezett (2006 után) a felderítő (pilótanélküli és személyzet nélküli földi érzékelők) és elektronikai hadviselési rendszerek fejlesztése, azonban szakmai okok miatt (felderítési adat nélkül nincs hatékony vezetési rendszer, az elektronikai hadviselési képesség ma már elengedhetetlen összetevője a haderőknek) ezek módosításra kerülhetnek.

A Magyar Honvédség számára „a piac" a NATO tagsággal és vele egyidőben Koszovóval jelentkezett. Bebizonyosodott, hogy a hadsereg gyökeres átalakítás, modernizálás nélkül nem alkalmas alaprendeltetéséből adódó feladatai végrehajtására. (A kivétel talán a felderítés.)

A megfogalmazott és jóváhagyott fejlesztési célok között – összhangban a NATO ajánlásokkal – a híradó és informatikai rendszer fejlesztése prioritást kapott.

Többéves előkészítő munka eredményeként a honvédelmi miniszter **2000 áprilisában elfogadta „A honvédelmi tárca híradó és informatikai rendszerei fejlesztésének programját."**

A fejlesztés öt programot tartalmaz:

- az állandó híradó és informatikai rendszer;
- a tábori híradó rendszer;
- a tábori informatikai rendszer;
- a repülések navigációs és leszállító, valamint az IFF rendszer (beleértve „S" mód) és
- az információvédelem fejlesztésének programjait.

A programokban mintegy 15 különböző projekt (URH rádiók, kapcsolástechnika, informatikai hálózat, IFF, stb.) található.

A programok a NATO fejlesztési célokra (FG-k) épülnek, 2006-ig éves bontásban eszköz, komplexum szintig költségekkel együtt tartalmazzák a fejlesztési feladatokat. A programok indításához szükséges pénz rendelkezésre áll, 2006-ig mintegy 50 milliárd Ft garantált biztosítása van tervezve.

3. A Magyar Honvédség jövőbeni alkalmazásának lehetséges feladatai, vállalt szövetségi kötelezettségek.

Magyarországot jelenleg és a belátható jövőben **semmilyen katonai veszély** nem fenyegeti. Az enyhülési és leszerelési folyamat eredményeképpen létrejött **strukturális támadóképtelenség**, valamint a váratlan támadások elhárítását lehetővé tevő **információcsere** gyakorlatilag kizárta és kizárja egy esetleges katonai támadás veszélyét. Jelenleg nincs olyan ország, mely hazánkkal, mint a NATO tagjával szemben bármely igényét katonai erővel tehetné érvényesíthetővé!

Az eltelt időszakban alapvetően **megváltozott a katonai tevékenység jellege.** A hatótávolság megnövekedése és a felderítő-reagáló eszközök elterjedé-

se következtében egyre csökkent a közvetlen harcérintkezés formájában megjelenő harctevékenység esélye.

Az érdekek és értékek képviseletének és megvédésének **van** más, **hatékonyabb** módszere, mint a **klasszikus háború.**

Megváltozott a veszély és a fenyegetés jellege. Előtérbe kerültek a **nemzetiségi, etnikai, vallási ellentétekből eredő helyi jellegű** feszültségek, konfliktusok, fokozódott a **migráció,** a **kábítószer-kereskedelem,** a **tömegpusztító fegyverek** ellenőrizhetetlenné vált elterjedésének a veszélye.

A legfontosabb katonai tevékenység a közeljövőben a nemzetközi szerződések alapján végrehajtott **békefenntartás** lesz. Egyre jobban elfogadottá válik a **nemzetközi katonai munka- és feladatmegosztás,** és a **többnemzetiségű alakulatok** létrehozása. A békefenntartás a **hadseregek jövője**, a konfliktushelyzetek áldozatok, veszteségek nélküli rendezése, a polgári lakosság biztonságának, életfeltételeinek megvédése.

Előtérbe került a **„testreszabás"** a katonai szférában is. Az elérendő cél a saját adottságoknak és feltételeknek, a **szövetségi tagságból eredő ajánlásoknak és elvárásoknak** legjobban megfelelő rendszer kialakítása. A korszerű technológia – információtechnológiai – katonai célra történő alkalmazása gazdaságos és egyben képességnövelő.

A kommunikációs követelmények meghatározásához szükséges egyszerűsítéssel az MH jövőbeni feladatai lehetnek:

- az ország légterének ellenőrzése, azonosított légihelyzetkép (RAP) kialakítása nemzeti és NATO célra, léti járőrszolgálat (Air Policing) biztosítása, kutató-mentő szolgálat biztosítása;
- válságkezelés a határainkhoz közeli konfliktus esetén (döntően dandár szintű kötelékkel), válságkezelésben részt vevő NATO erők részére bázisok biztosítása;
- részvétel katasztrófa elhárításban; bekapcsolódás a NATO polgári veszélyhelyzeti rendszerében;
- maximálisan zászlóalj szintű kötelékekkel részvétel különféle többnemzetiségű (döntően NATO/EU vezette) békefenntartó műveletekben;
- a felajánlott erőkkel részvétel NATO V. Cikkely szerinti műveletekben (kicsi az esélye), az erők felkészítése a vállalt képességek elérésére;
- kis kötelékekkel való részvétel szélsőséges időjárási körülmények közötti többnemzetiségű műveletekben. (ehhez az állomány és technikai különleges felkészítése szükséges)

A felsorolt feladatokból két jellemző elemet emelnék ki nemzeti és nemzetközi **együttműködő** környezetben **alegységszintű kötelékek** tevékenysége várható.

Belátható időn belül az EU tagjai leszünk, amely szintén bizonyos erők (képességek) felajánlásával fog járni. Országunk szavahihetőségének megőrzése megköveteli, hogy vállalásainknak (ha kisebb-nagyobb időcsúszásokkal

is) eleget tegyünk, hogy legyenek felajánlható erőink a NATO és az EU részére, hogy képesek legyünk érdemben hozzájárulni a szövetségek védelmi erőihez. Ezek a hiteles képességek meghatározó mértékben leggyorsabban és leggazdaságosabban az információtechnológia alkalmazásával hozhatók létre, illetve anélkül nem hozhatók létre.

4. Saját lehetőségeink

Az információs társadalom és ezen belül az információs hadviselés fejlődési tendenciáinak szem előtt tartásával nekünk a jelenlegi és a várható, de hazai körülmények által behatárolt feltételek alapján kell a követendő „stratégiát" kidolgozni.

Az információtechnológia fejlődés egy folyamat, mely **kikerülhetetlen, a NATO-ban vállalt kötelezettségeink** is ebbe az irányba mutatnak. Minél később csatlakozunk ehhez a fejlődési folyamathoz, annál nagyobb hátrányt kell behozni, és annál nagyobb anyagi ráfordítással kell számolnunk.

Magyarország nem fog vezető szerephez jutni ezen a területen. Ugyanakkor rendelkezik olyan **tapasztalat- és tudáspotenciállal,** mely lehetővé teszi a már kifejlesztett rendszerek magasszintű alkalmazását, a hazai „testreszabását", és továbbfejlesztését. Elsődleges feladat az ismeretek és tapasztalatok megszerzése, bővítése, a szükséges tennivalók hosszú távú megtervezése, és az alkalmazás gyakorlati feltételeinek megteremtése.

A társadalom támogatása, együttműködése nélkül nem lehet hadsereget építeni. Miközben az ipari-gazdasági szférában egyre inkább **terjed az elektronika,** a sorköteles korosztály szinte a „középkornak" megfelelő körülmények között tölti el szolgálati idejét. A hadsereg társadalmi elfogadottságának, **támogatásának feltétele,** hogy a társadalom a hadsereget önön részének tekintse és **közösséget vállaljon** vele.

Amikor az információtechnológiai kihívásokat elemezzük, akkor a kihívásokat nem kizárólag és szó szerinti értelemben, a technológia világában keressük. Megítélésünk szerint a kihívások az alábbi főbb területeken jelentkeznek:

A honvédelmi ágazat és a Magyar Honvédség számára az informatikai rendszer korszerűsítésének szükségessége adódik:

- a környezeti feltételekből, azaz abból, hogy meg kell teremtenie, és fenn kell tartania az együttműködési képességét a Szövetséggel, lépést kell tartania az államigazgatás és védelmi igazgatás nemzeti rendszereivel, a nemzetgazdaság résztvevőivel;
- gazdasági, költségvetési kényszerből, mivel a nemzetgazdaság és a társadalom által a haderő finanszírozására elismert és biztosított erőforrások mértéke megköveteli az anyagi-technikai, szervezeti és humán erőforrások takarékos igénybevételét;
- az országvédelem hatékonyságának erősítésére vonatkozó társadalmi elvárásból, amely szükségessé teszi a haderőnek mind a katasztrófa-, válság-

helyzetben, mind a béke- és hadműveletekben való alkalmazási képességének növelését.

A konvergencia olyan meghatározó trendnek látszik, amelynek ellenében menetelni nem célszerű. A Konvergencia – függetlenül attól, hogy milyen okok eredményezték – nemcsak technológia, technikai eredmény, hanem gondolkodási, cselekvési mód is.

A kommunikáció, számítástechnika és a katonai alkalmazások egy közös irányba terelése az művelő szakemberek együttes tevékenységével érhető el a leghatékonyabban.

Nálunk elsősorban a törzsek és a logisztikai szervezetek kialakításában történtek ezirányú lépések (6-os blokkok, elektronikai szolgálat); ugyanakkor az alkotórészek érdemi összehangolása még csak kezdeti szakaszban van.

A ZMNE-n folyó oktatás sem a konvergencia figyelembevételével folyik, van kommunikációs rendszerszervező, informatikai és elektronikai hadviselési szakember képzés. A jövőben – már zászlóalj harccsoport szinten is – egy egységes információ rendszert kell tervezni, szervezni és üzemeltetni, amelyhez lesz egy tiszt (menedzser) a tervezéshez – szervezéshez, egy az üzemeltetés irányításához, néhány tiszthelyettes és zászlós, a többi katona (remélhetőleg szerződéses).

Melyik intézmény és mikor készíti fel ezeket a szaktiszteket egy összetett rendszer menedzselésére, továbbá a parancsnokokat annak alkalmazására?

Akkor amikor a magyar katonai kommunikáció jövőjéről beszélünk és a kulcskérdésnek, a legkritikusabbnak a humán oldalt tartom. Az biztos, hogy a kommunikáció – akár akarjuk, akár nem – az információtechnológia egyik meghatározó tartópillére lesz, nélküle nincs semmilyen információrendszer, önállósága, a korábbi (jelenlegi) értelemben vett szakmai önállósága jelentősen csökken. Ráadásul úgy csökken, hogy jelentősége, a vele szemben támasztott követelmény, összetettsége és bonyolultsága egyre nő.

Amilyen mértékben a beszéd és papír alapú vezetés adat- kép - grafika multimédia alapúvá válik, olyan értelemben változik a klasszikus híradás (kommunikáció) helye és szerepe is, válik részévé egy digitalizált rendszernek.

Az általánosan elterjedt nézetektől eltérően amiben hiányt szenvedünk az az idő és a szakértelem, a szükséges pénz biztosítható.

A szakértelmet a hazai tudományos és oktató, szolgáltató és termelő cégektől meg lehet vásárolni. Nemzeti vezérléssel – a nemzetközi katonai és polgári tapasztalatok széleskörű alkalmazásával – egy átfogó, katonai információtechnológia egészét felölelő koncepciót, valamint a koncepcióba illeszkedő részletes fejlesztési tervet kell kidolgozni, pontosabban a meglevő terveket kell aktualizálni. A piacon fellelhető legmodernebb technológiák – döntősen COTS – alkalmazásával, az infrastruktúra, a hozzáférési és alkalmazási rendszerek egyidejű, feladat centrikus fejlesztésével az időbeni lemaradásunk ledolgozható lesz.

A fejlesztéseket először a felajánlott erők felkészítésére, „tudás alapú” kiképzésre kell használni, majd az egész haderőre ki kell terjeszteni.

Amit nem lehet megvásárolni az a hozzáértő tiszt, zászlós, tiszthelyettes, az ki – át – tovább kell képezni.

Ismereteim szerint a képzési rendszer átalakítása nem teljesen az információtechnológia által követelt irányba mutat.

HM tárca vezető szakmai szerveinek képviselőiből – NATO mintára – célszerű egy testületet, testület alatt különböző szakbizottságokat kialakítani, amely a vezetés, irányítás, híradás és informatika fejlesztésének fő elemeit, illetve szakmai részleteit határozná meg. A testület vezetője a területért felelős helyettes államtitkár, illetve vezérkar főnök helyettes lehetne társelnökként.

Talán meglepő, hogy a magyar katonai kommunikáció jövője szempontjából nem a technikai, hanem humán oldalt hangsúlyozom. Felkészült szakemberek a megfelelően kialakított és működtetett szakmai fórumokon – a hazai és nemzetközi vérkeringés részeseiként – képesek az optimális fejlődési irány meghatározására, szükség szerint annak módosítására.

Dr. Somos András

A KATONAI KOMMUNIKÁCIÓ ÉS A HÍRKÖZLÉS FELKÉSZÍTÉSÉNEK VISZONYA

Mindenek előtt értelmezzük az előadás tárgyát képező fogalmakat (**katonai kommunikáció és hírközlés felkészítése).**

A katonai kommunikáció alatt azt az információtovábbítást értem, amely a katonai szervezetek közötti vezetési és együttműködési kapcsolatokban az állandó és tábori eszközökkel szervezett távközlő rendszereken folyik békében, veszélyhelyzetben vagy fegyveres küzdelemben.

A hírközlés felkészítésének fogalmából a **hírközlés** alatt „küldemény, adat, jel, kép, hang, vagy bármilyen információ hírközlő infrastruktúra segítségével történő továbbítását, vételét" értjük; más szavakkal ide soroljuk a távközlést, a postai szolgáltatást, a frekvenciagazdálkodást, a műsorszórást és zártcélú hálózatok üzemeltetését is.

A **felkészítés** alatt pedig a hírközlési tevékenységet végző szervezetek és eszközök (rendszerek, hálózatok) alkalmassá tételét arra, hogy minősített időszakban is megfeleljenek a velük szemben támasztott azon kormányzati, védelmi, nemzetbiztonsági, lakossági igényeknek, amelyek több szempontból eltérhetnek a békeidőszakitól.

A katonai kommunikációt optimális esetben olyan komplex hálózati rendszer biztosítja, amely egységes alapon felépült, de legalábbis azonos interfészekkel rendelkező állandó telepítésű és tábori (mobil) híradó, illetve informatikai eszközökből épül fel. A katonai kommunikációs rendszer egyes meghatározó jellemzői (szervezése, felhasználása, biztonsága, információvédelme, felügyelete, irányítási módja, együttműködése más rendszerekkel, stb.) alapvetően eltérnek más hálózatokétól. A katonai kommunikációs rendszer nem nélkülözheti a közcélú távközlő hálózatok igénybevételét, az azokhoz történő csatlakozást. Ilyenek a közcélú távbeszélő, rádiótelefon, adatátviteli (Internet) szolgáltatások, illetve ezek fizikai hálózata. Ide tartozhatnak a műsorszóró (szétosztó) és a műholdas hálózatok, valamint más zárcélú, vagy elkülönült hálózatok is.

A katonai kommunikációs rendszer állandó telepítésű és üzemeltetésü részét a jogszabályok zártcélú hálózatnak nevezik. Ilyenek lehetnek még az államigazgatás más konkrét területein is (kormányzat, rendvédelem, nemzetbiztonsági szolgálat, igazságszolgáltatás). A zártcélú hálózatok közötti együttműködés biztosítása fontos feladat, mint ahogy az a NATO egyes rendszereihez való csatlakozás is.

Az elmondottakból következik, hogy a katonai kommunikációs rendszer mind az állandóan működő, mind a tábori eszközeit (alrendszereit) tekint-

ve sok szállal (műszaki, jogi, gazdasági szálakkal) kapcsolódik az ország hírközlését biztosító elemekhez a hagyományos és informatikai szolgáltatások tekintetében. Ez képezi az **egyik motivációs** oldalát annak, hogy a távközlés (hírközlés) veszélyhelyzeti felkészítése mindig is egyik lényeges eleme volt az ország felkészítésének (országmozgósítás, hadszíntérelőkészítés, stb.) és a követelmények, igények egy részét a katonai igénybevétel szolgáltatta. Bár meg kell jegyezni, hogy a konkrét követelmény támasztással mindig gondok voltak.

Tudomásom szerint az MH perspektív kommunikációs rendszerének koncepciója egységes (állandó és tábori), ISDN szolgáltatású digitális rendszer létrehozását tartalmazza, amely kielégíti a HM, az MH vezetési, irányítási, informatikai és információvédelmi követelményeit, igényeit, együttműködik a közcélú hálózatokkal, más zárcélú hálózatokkal és a NATO rendszereivel. Ilyen körülmények között felül kell vizsgálni a korábbi elveket és a katonai kommunikációs rendszer felőli igényeket, főképpen két terület vonatkozásában:

- az egyes (közcélú) hírközlési szolgáltatások állandó jellegű igénybevételének rendje, módja, fajtája, helye, stb. hazai és nemzetközi viszonylatban;
- a tábori (mobil) eszközök közcélú hálózathoz történő csatlakozásával összefüggő igények, azok békeidőben történő előkészítése érdekében.

A **felkészülés másik** motivációs oldala, hogy az ország egységes (egységessé tehető) hírközlését alkalmassá kell tenni az alkotmányban és egyéb jogszabályokban megfogalmazott veszélyhelyzetek, katasztrófa helyzetek kezelésére. A polgári védelemről szóló 1996. évi törvény szerint ez a kategória „a szükséghelyzetet el nem érő, az állampolgárok élet- és vagyonbiztonságát, vagy a környezetet veszélyeztető természeti csapás, illetőleg ipari baleset okozta állapot”. Az 1999. évi katasztrófatörvény szerint „a minősített helyzetek kihirdetését el nem érő mértékű olyan állapot vagy helyzet, amely az emberek életét, egészségét, anyagi értékeit, a lakosság alapvető ellátását, a természeti környezetet veszélyezteti, károsítja…”

A **felkészülés harmadik** motivációs oldala, hogy az ország NATO tagságából eredően részesei vagyunk a polgári/katonai együttműködésnek a Polgári Veszélyhelyzeti Tervezés (CEP) keretében, amelynek munkája egy főbizottságban (SCPC) és 9 bizottságban folyik. Ezek közül a harmadik a hírközlési kérdésekkel foglalkozó Polgári Távközlési Tervező Bizottság (CCPC). A polgári távközlésbe a NATO értelmezés szerint a katonai kommunikációs eszközök és szolgáltatások kivételével a magyar „hírközlés” fogalomköre tartozik.

A CCPC mint nemzetközi szervezet – amelynek munkájában minden NATO tagállam, így Magyarország képviselői is résztvesznek – a hírközlés veszélyhelyzeti felkészítésének általános kérdéseivel foglalkozik, „azon intézkedésekkel, amelyek célszerű mértékig már békeidőben szükségesek a távköz-

lés folyamatos biztosításához válság és háború idején, polgári és katonai célokra" (Idézet a CCPC AC/121 szabályzatából).

Mindezekhez a hírközlés szabályozott és folyamatos veszélyhelyzeti felkészítése szükséges. E tevékenység szervezettebbé, hatékonyabbá tételéhez kedvező feltételeket teremt (teremthet) az új hírközlési törvény és az abban szereplő felhatalmazások birtokában kidolgozandó alacsonyabb szintű jogszabályok.

A Kormány által 1998.-ban elfogadott és ma is érvényben lévőnek tekinthető „Hírközléspolitika" c. okmány a kormányzati célú távközlés címszó alatt néhány pontban megfogalmazza a hírközlés honvédelmi feladatainak magas színvonalú ellátását szolgáló célkitűzéseket. Ilyenek:

a) a közcélú hálózatok, elsődlegesen a gerinchálózat biztonságának növelése, zavarérzékenységének csökkentése, a honvédelmi érdekből történő hozzáférés lehetőségének biztosítása;
b) a honvédelmi feladatokban résztvevő hírközlési szervek kijelölése és feladataik meghatározása;
c) felkészülés a NATO tagságból eredő védelmi igények kielégítési módszereinek, eljárási rendjének átvételére. (Ez 1998. évi okmány, a belépés pedig 1999 márciusában történt.)

A Hírközléspolitika tartalmazza egyébként az egységes hírközlési törvény kidolgozásának célkitűzését és nagybani elveit is.

Mint ismeretes, az Eht-nek titulált hírközlési törvény előkészítését a KHVM kezdte el és kidolgozta annak téziseit, amelyet a Kormány 1999. decemberében hagyott jóvá. A tézisek szerint az Eht. célja – többek között – a hálózatok egységének, veszélyhelyzeti felkészítésének, biztonságának, a szolgáltatók együttműködésének biztosítása, a hálózatok minősített időszaki felkészítésében az állami szerepvállalás meghatározása.

Az Eht. több változatban történő kidolgozása és egyeztetése 2000. közepétől az újonnan létrejött MeH Informatikai Kormánybiztosság irányításával folytatódott. A végleges törvényjavaslatot a Kormány 2001. márciusában nyújtotta be az Országgyűlésnek, amely azt XL. számon 2001. június 12.-én fogadta el.

<u>Azok számára, akik nem ismernék</u>: van egy 50/1998. Korm. rendelet a zártcélú hálózatokról. A rendelet kidolgozása az 1992. évi távközlési törvény felhatalmazásán alapult és több évig tartott; első része meghatározza a zártcélú hálózatok létesítésének, üzemeltetésének, fenntartásának, finanszírozásának rendjét, a hálózatgazdák feladatait; második része (IV. fejezete és melléklete) meghatározza a távközlés honvédelmi felkészítésének rendjét, állami és önkormányzati feladatait, a távközlés minősített időszaki alkalmazásának elveit.

A Hírközléspolitikában és a Tézisekben foglaltaknak megfelelően, továbbá figyelembe véve a zártcélú távközlő hálózatokra vonatkozó 50/1998 Korm. rendelet meglétét és tartalmát, az Eht. előkészítése és államigazgatási

véleményezése során a következő elveket követtük (a nemzetbiztonsági szolgálatokat érintő kérdésekkel nem foglalkozom):

d) a jogszabály céljai sorában a védelmi szabályozás megjelenítése;
e) az állami feladatok között a hírközlés felkészítéséért viselt felelősség megfogalmazása;
f) az állami feladatokat ténylegesen végrehajtó Kormányra és a szakminiszterre háruló feladatok részletesebb meghatározása;
g) a szolgáltatók alapvető kötelezettségeinek megfogalmazása (tervezés, tartalékképzés, együttműködés);
h) felhatalmazás rendeleti szabályozásra:

a Kormány számára:

- a zártcélú hálózatokra vonatkozó szabályokra;
- a hírközlés veszélyhelyzeti felkészítésének elveire, szabályaira, állami feladataira.

a szakminiszter számára:

- a honvédelmi feladatok végrehajtásába bevont hírközlési szervek kijelölése és feladataik meghatározása (a Hvt. 1993. évi megjelenése óta csak részben végrehajtott feladat).

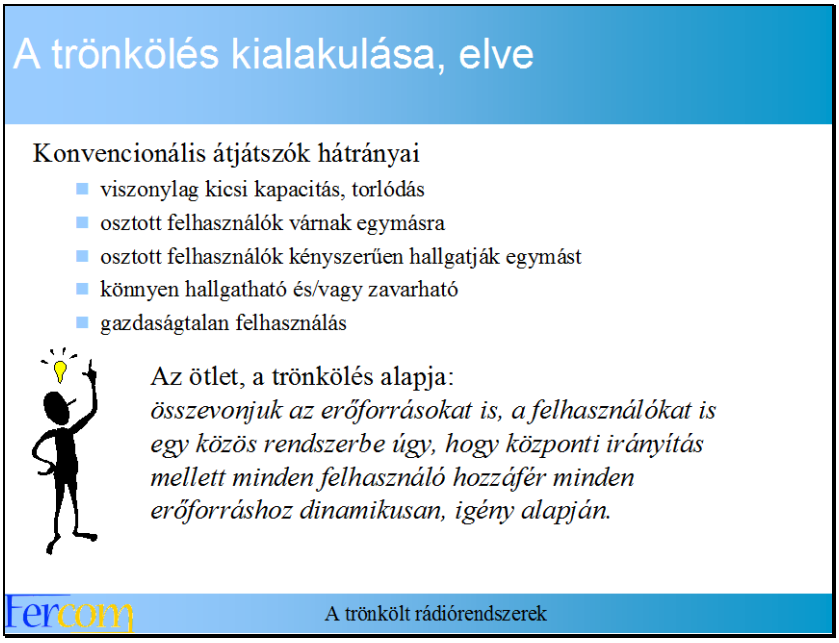
A fenti célkitűzések döntő mértékben érvényesülnek az Eht-ben, amelynek keret-törvény jellege miatt nagy szerep hárul a kiegészítő jogszabályokra. A keret jelleg ellenére a további jogi szabályozás alapelveit és felhatalmazásait a törvény megfelelően tartalmazza.

Visszatérve az előadás tárgyára és előző részére, levonhatjuk azt a következtetést, hogy:

- megmaradhat és korszerűsödhet az MH kommunikációs rendszere, ezen belül az állandó telepítésű hálózata, mint az MH zártcélú hálózata; a jogi kereteket a jelenlegi 131/2001 rendelettet módosító 50/1998. Korm. rendelet első része, vagy annak korszerűsített, aktualizált változata adhatja;
- az ötvenes rendelet második része alapján készült külön kormányrendelettel szabályozható a hírközlés felkészítése a honvédelem (a katonai kommunikációs rendszer) mai, aktualizált igényeinek figyelembe vételével és a NATO tagságból eredő, jelenleg már jobban ismert elvi és gyakorlati szempontokkal összhangban;
- miniszteri rendelet szintjén konkretizálhatók a veszélyhelyzeti felkészítés feladatai a szolgáltatók számára, ha az Eht-ban megfogalmazott piaci átalakulások megtörténtek, vagy azok menete már látható.

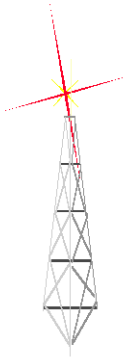
Koncz Mihály

A MOTOROLA TRÖNKÖLT RÁDIÓRENDSZEREK



A trönkölés elemei

- központi vezérlő
  - erőforrás-gazdálkodás
  - felhasználói és infrastruktúra adatbázis
  - nem trönkölt rendszerek felé interface
- átjátszók
  - beszédátvitel
- szervezőcsatorna
  - vezérlő és készülékek közti kommunikáció
- végkészülékek
  - a kommunikáció eszköze felhasználói oldalon
- konzolok
  - diszpécseri pult
  - havária beavatkozó terminálok



A Motorola trönkölt megoldások

- StartSite – egy telephely, kis csatornaszám
- SmartNet – egy telephely, nagy csatornaszám
- SmartZone – sok telephely, nagy csatornaszám
- SZ Omnilink – korlátlan telephely, nagy csatornaszám

- 2^{16} felhasználó
- 2^{12} logikai csoport
- 28 csatorna telephelyenként
- csoportkommunikáció 0,3 – 0,5 sec alatt
- az átjátszók kihasználtsága statisztikailag egyenletes
  - nincs túlterhelt átjátszó
  - nincs kihasználatlan átjátszó

A trönkölés felhasználói szolgáltatásai

- egynyomógombos azonnali kommunikáció
- rugalmas csoportképzés
- jelzéshagyás, priváthívás, telefonhívás lehetőségek
- külső és belső belehallgatás elleni védelem
- kizárólagosság érzése
- elveszett készülékek kitiltása
- foglaltságok kezelése

A trönkölés operátori szolgáltatásai

- frekvencia-takarékos kommunikáció
- könnyű, egyszerű bővítés, végkészülékeket nem érinti
- redundancia, üzembiztonság
- korábbi rendszerek integrálhatósága
- a rendszer Tetra rendszerbe integrálható
- felhasználói adatbázis, jogosultságok kezelése
- automatikus készülék, csoport és telephely azonosítás
- beszéd és aktivitás naplózhatóság, automatikus számlázás

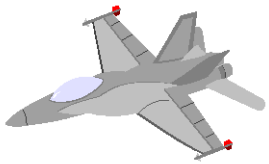
A trönkölés előnyei

- a munkatársak azonnali, mobil elérhetősége
  - gazdaságosabb üzemvitel
  - magasabb fokú szervezettség
  - megnövekedett üzembiztonság és hatékonyság
- saját, független kommunikációs infrastruktura, redundancia
- egyéb kommunikációs költségek csökkenése
- szolgáltatónak fizetendő havidíj ellenében nincs engedélyezési procedura, nincs frekvenciakijelölés, nincs karbantartási költség

Működő katonai trönkölt rendszerek

A Fercom Kft telepített és jelenleg is üzemeltet
Motorola SmartNet rádiórendszert az alábbi repülőtereken :

- Pápa
- Kecskemét
- Szentkirályszabadja



- mindenütt 5 csatorna, kb 65 rádió
- alkalomjellegűen, pl. repnap, akár 100 rádióval bővítve
- Sztkirsz. telefonkapcsolat próbajelleggel

Alkalmazási lehetőségek

A rendszert nagyfokú megbízhatósága ideálissá teszi adatátvitelre.

- Paks, LTRR, sziréna távkezelés
- Lehetőségek
  - fénytechnika kezelése 
  - meteorológiai adatgyűjtés és továbbítás
  - objektum-felügyeleti információk
  - GPS AVL alkalmazások

Köszönöm a figyelmet !

Fercom

MOTOROLA
Authorized Distributor

1036 Bp. Lajos u. 78.
www.fercom.hu
info@mail.fercom.hu

Dr. Mráz István

A VEZETÉS INFORMÁCIÓS TÁMOGATÁSÁNAK VEZETŐI KÖVETELMÉNYEI

A vezetés színvonalát, hatékonyságát, általa pedig a katonai tevékenységek eredményességét számos tényező befolyásolja. Közöttük fontos a szerepe a vezető[10] és a vezetési szervek tájékozottságának, helyzetismeretének, információellátásuk minőségének.

A vezetés információs hátterének megteremtése – információs támogatása – előrelátóan szervezett és működtetett információs rendszert igényel. Vezetői követelményeinek széleskörű egyeztetés és viták során kell formálódnia, amelyben jelentős szerepet kell kapnia és vállalnia a nyilvánosságnak. Az előkészítő munkában felszínre kell kerülnie mindazon személyek véleményének és javaslatainak, akik valamilyen formában kapcsolatba kerülnek az információs rendszerrel és részt is kívánnak venni a kialakításában.

Ez az előadás a vezetői információs rendszer néhány általános kérdését kívánja felvetni. Olyan elvi-elméleti jellegű megfontolásokat, amelyek a szerző véleménye szerint előbbre vihetik kiépítésének megalapozását, érdemi tervezésének előkészítéséhez szükséges vezetői követelmények kialakítását.

Az előadás a szerző egyéni véleményét tükrözi. A téma újszerűségéből és feltáratlanságából eredően nem törekedhet sem a teljességre, sem a hibátlanságra. Inkább vállalja azonban a tévedés vagy a kiforratlanság következményeit, mintsem elhallgasson a szerző által fontosnak ítélt kérdéseket és az azokra adható lehetséges válaszokat. Az anyag már akkor betölti szerepét, ha a követelmények kidolgozásának részévé válik és annak egyik építőköve lesz, amelyet a későbbi vizsgálatok kritikával illetnek, vitatnak és végül meghaladnak.

A vezetési rendszer olyan összetevőinek, mint a *kommunikációs* és az *informatikai bázis*, megkülönböztetett helye és szerepe van az információs rendszer fejlesztésében és működtetésében. Kapcsolataik a vezetéssel és egymással sajátos tartalommal bírnak, amelyek feltárásától nem tekinthetnek el az *információs rendszerre* vonatkozó vizsgálatok.

FŐBB TÉNYEZŐK, KAPCSOLATOK, PRIORITÁSOK

A *kommunikáció* és az *informatika* napjainkra a vezetés létfontosságú támogató elemeivé váltak. Dimenziót adnak a vezetés funkcionális oldalának, ugyanakkor nélkülük gyakorlatilag nem beszélhetünk korszerű vezetésről. [11]

[10] Az előadás a vezető fogalmát általános értelemben használja. Érti alatta a haderő parancsnoki, a szolgálati és szakmai elöljárói beosztásait, függetlenül azok szintjétől és szakterületi sajátosságaitól.

[11] A kommunikáció és a híradás integráns elemként történő kezelése igen határozott az amerikai haderő vezetés-felfogásában. Pl.: „ *A hatékony parancsnoklás*

Az előző megállapítás igazságtartalma aligha kérdőjelezhető meg. Mondandója – bár eléggé általános – elégségesnek és alkalmasnak tűnik néhány *következtetetés levonására*. Nevezetesen:

- A vezetéstámogatás - vezetés viszonylatában az utóbbi a meghatározó elem. A vezetés tartalmi, minőségi jellemzőiből és működési sajátosságaiból származtathatóak a támogató elemekkel szembeni alapkövetelmények.
- A legáltalánosabb követelmények a kommunikációs és informatikai alapokkal szemben a vezetésből fakadnak, illetve kell, hogy fakadjanak. Első megközelítésben a felépítés, a működési paraméterek, a kapcsolatok és a szolgáltatások milyensége, színvonala azok a területek, amelyekben vezetés-centrikus megoldásokat kell keresni és megvalósítani.
- Felelősségi sávja és hatásköre alapján a vezetés széleskörű és sokoldalúan összetett tevékenységi forma. Belső struktúrája távolról sem homogén jellegű. Elemei közül elsősorban azok a meghatározóak – követelménytámasztóak –, amelyek a haderő fő feladataihoz, a hadászati-hadműveleti folyamataihoz kötődnek. Minden más vezetési részterületnek és tevékenységi iránynak e folyamatok mentén kell a prioritásokat keresni és megtalálni.12

A vezetéstámogatás bonyolult és sokösszetevős rendszer. Követelményeinek meghatározása egyetlen személy – a vezető – által egysíkú és reménytelen vállalkozás lenne. Ebből adódik, hogy a vezetői követelmények kialakítása széleskörű csapatmunkát kíván. Résztvevőinek szem előtt kell tartani egyrészt a vezetés fent hangsúlyozott prioritásait, másrészt az általuk képviselt szakterületek szakmai szempontjait. evidens

Annak megítélése, hogy a bevezetőben hozott megállapítás mennyire kézenfekvő (netán elkoptatott), csakis elvi-elméleti síkon lehet kérdéses. A gyakorlatban, a mindennapjaink során nem ritka, hogy ez a *szoros* és *határozott irányú* kötődés nem, vagy nem az igényeknek megfelelően működik. Számos esetben tapasztalható, hogy a támogató elemek a vezetés igényeitől, a vezető akaratától és szándékaitól függetlenül funkcionálnak. Jóllehet, ebben több ok is szerepet játszhat, a vezetés-vezetéstámogatás valós viszonyában jelentkező gondok azonban a tapasztalatok szerint nagyobbrészt a *vezetői követelmények hiányára* vagy *elégtelenségére* vezethetők vissza.

…megbízható, biztonságos és interoperábilis híradást követel." 3-0. Egyesített kiadvány – Egyesített Hadműveletek Doktrínája USA 1995. február. Kéziratos fordítás 43. oldal. Más helyen: *„A vezetés négy fő összetevője …a vezetettek, a vezető, a helyzet és a kommunikáció."* FM 22-100 Katonai vezetés. HVK Euro-atlanti Integrációs Munkacsoport Budapest, 1997. 17. oldal

[12] A hadászati-hadműveleti szempontok érvényre juttatásának fontosságát és lehetőségeit vizsgálja SZŰCS Gáspár A hadászati-hadműveleti vezetés integrált számítógépes rendszeréről c. munkájában. (Új Honvédségi Szemle 1997/2. szám. 132-136. o.)

Nem minden tanulságtól mentesek pl. azok a felmérések, amelyek szerint a polgári életben az információs rendszer egészével vagy annak főbb elemeivel a felhasználók igen sokszor elégedetlenek. A fenntartásaik okait elemezve a szakirodalom legnagyobb arányban a felhasználói követelmények oldaláról mutat ki hiányosságokat: a panaszok okainak több mint fele adódik a szakmai felhasználói követelmények *meghatározásának* vagy *érvényesítésének hiányosságaiból*.[13]

FONTOSSÁGI ÉS IDŐSZERŰSÉGI SZEMPONTOK

A Magyar Honvédség vezetésének rendjét, a vezetéstámogatás helyzetét, az információs rendszer fejlesztésének szempontjait és követelményeit napjainkban több tényező befolyásolja. Közülük a legidőszerűbbek és a legfontosabbak:

- A legközvetlenebb hatású és igényű tényező a haderő vezetésének napirenden lévő korszerűsítése, ennek részeként pedig a Honvédelmi Minisztérium (HM) és a Honvéd Vezérkar (HVK) integrációjának befejező szakasza. Az átalakítások eredményeként ez év végére új minőségű felső vezetési rend alakul ki. Csökken a haderő vezetési szintjeinek száma, és átrendeződés következik be az egyes szintek hatás- és feladatkörei között. A kidolgozás fázisában van a HM információ-kapcsolati rendszere. Mindezek sürgető jelleggel és a gyakorlat oldaláról igénylik a változásokat mind a vezetés folyamataiban, mind annak információs támogatásában.
- A vezetői információk (a vezetők informáltságának) felértékelődése szélesebb síkon is időszerűséggel bír. Nemzetközi téren az új szövetségi kötődésünk, a biztonsággal és annak katonai garanciáival kapcsolatos elvek változása, a béketeremtő és békefenntartó műveletek tapasztalatai azok a főbb tényezők, amelyek új megvilágításba helyezték a katonai vezetés és az információs támogatás elméleti és gyakorlati kérdéseit. Megerősítették, hogy az új viszonyok igen nagy mennyiségű adat és információ uralását igénylik a katonai vezetéstől, melyhez sürgető egy új minőséget képviselő, korszerű vezetői információs rendszer kialakítása.
- Az ország biztonságának veszélyeztetésében és a katonai erő, mint biztonsági tényező szerepének értékelésében beálló változások a békefeladatok súlyponteltolódását eredményezik és a vezetés megújításának irányába hatnak. A fegyveres erők fő feladata változatlan: „ …Magyarország szuverenitásának és területi épségének védelme és

[13] Kutatások tapasztalatai alapján a felhasználói elégedetlenségek – a programok és az információs rendszerek kifogásolt hibái – az esetek 56%-ában az *alkalmazói követelmények elégtelen meghatározására*, 27%-ban tervezési hiányosságokra, 7%-ban programozói és kódolási hibákra és 10%-ban egyéb okokra vezethetők vissza. Forrás: MOLNÁR Bálint: Bevezetés a rendszerelemzésbe. Aula kiadó Budapest, 1996. 12. o. és RAFFAI Mária: Információrendszer-fejlesztés. Novadat Kiadó Győr, 1999. 253. o.

…hozzájárulás a Szövetség kollektív védelméhez."14 Ennek hangsúlyozása mellet is számolni lehet azzal, hogy a jövőben mindinkább a nemzetközi szerződésekben vállalt katonai kötelezettségek teljesítésében, a béketámogató műveletekben és a humanitárius segítségnyújtásban, a szövetséges csapatok manővereinek, szállításainak támogatásában, a válsághelyzetek megoldásában, valamint a katasztrófa-elhárításban történő képesség-alapú részvétel képezi a béke-tevékenység súlyponti elemeit.15 Előtérbe kerül a határainkon kívüli tevékenység.16 E sajátos műveleti és igénybevételi formák a korábbiakhoz képest újszerű vezetési és információs elveket és gyakorlatot igényelnek.

- Hazai vonatkozásban a honvédelmi és a biztonságpolitika filozófiájának újragondolása, alapelveinek újrafogalmazása, a civil kormányzati ellenőrzés szerepének növelése, valamint a működési és finanszírozási viszonyok újraértékelése jelenti a legnagyobb kihívást – és lehetőséget – a vezetéssel, a vezetés információs támogatásával szemben.
- Hangsúlyos mozgatóerő napjaink technikai forradalma, amely mindenekelőtt információs-technológiai forradalomként jellemezhető. Ebből eredően a legközvetlenebb kapcsolatban van a katonai vezetéssel, annak valamennyi funkcionális elemével és a vezetést támogató összetevőkkel.
- A várható alkalmazási, felhasználási és igénybevételi feladatokban történt változások a haderő stratégiai átalakítását igénylik.17 Mindezek újszerű vezetési és alkalmazási elveken alapuló tevékenységi rendet követelnek.18 Ismeret- és szemléletváltás zajlik a magyar haderőben mind

[14] Az Országgyűlés 94/1998. (XII. 29.) OGY határozata a Magyar Köztársaság biztonság- és védelempolitikájának alapelveiről. 14. pont.

[15] Dr. KŐSZEGVÁRI - Dr. SZTERNÁK - MAGYAR : A XXI. századi hadviselés. /A században várható biztonsági kihívások, konfliktusok és háborúk; hadviselési elképzelések; haderő struktúrák és feladatok/. Egyetemi jegyzet. Zrínyi Miklós Nemzetvédelmi Egyetem Doktori Iskola. Budapest 2000. és PADOS Ferenc alezredes: A Magyar Köztársaság veszélyeztetésének lehetséges esetei és fegyveres ereje alkalmazásának elvei, politikai következményei. Doktori (PhD) értekezés-tervezet. ZMNE Budapest, 2001.

[16] "*...napjaink katonája nagy valószínűséggel hazáján kívül kerül alkalmazásra."* (CHRIS Donelly: A katonák felkészítése a XXI. századra. NATO tükör. 2000 nyár/ősz 29. o.)

[17]Az Országgyűlés 61/2000. (VI. 21.) OGY határozata a Magyar Honvédség átalakításának irányairól. 2. pont.

[18] A közép és kelet-európai haderőkkel szembeni újszerű kihívásokat, az alkalmazási sajátosságokat és azok vezetésre gyakorolt hatásait elemzi CHRIS Donelly: A katonák felkészítése a XXI. századra c. munkájában. (NATO tükör 2000 nyár/ősz 28-31. oldal.).

Hasonló következtetésre jut több hazai kutató is. Lásd: PADOS Ferenc alezredes: A Magyar Köztársaság veszélyeztetésének lehetséges esetei és fegyveres ereje alkalma-

harcászati, mind hadműveleti, mind pedig stratégiai szinten. Az új doktrinális alapelvek megfogalmazása ugyanúgy része ennek, mint a vezetés- és szervezéstudomány legújabb eredményeinek adaptálása és az információs rendszerek megújítása.

A fenti tényezők súlyából és minőségi jegyeiből adódik, hogy azok *stratégiai jellegű változásokat* tesznek szükségessé a katonai vezetésben és a vezetés támogató elemeiben. Minőségileg új vezetési struktúrát igényelnek új működési renddel, új híradó és informatikai lehetőségekkel és ezek alapjain új információs rendszerrel.

A KÖVETELMÉNYTÁMASZTÁS ÁLTALÁNOS ALAPJAI

A vezetői követelmények legáltalánosabb forrásait a vezetésre, annak rendszerére és működésére vonatkozó *alapelvekben, szándékokban,* az ezekre vonatkozóan *egyeztetett nézetekben és megállapodásokban* (konvenciókban) kell keresni. Vizsgálatuk során nem kerülhető meg a vezetés néhány *stratégiai jellegű problémája* sem.

VEZETÉSFELFOGÁS 2001

Az előadás alkalmazásában a *katonai vezetés* (továbbiakban: vezetés) az alárendeltek befolyásolásának folyamata a vezetők részéről a katonai tevékenység sikere, a feladat eredményes végrehajtása érdekében.[19] Jogot és kötelezettséget, hatáskört és felelősséget testesít meg, amelyeket az egyszemélyi vezetőre ruháznak a *célkitűzések* és *követelmények* meghatározása, a katonai *szervezetek* és az *állomány kialakítása*, hatékony *működtetése*, az alárendeltek tevékenységének *szabályozása, irányítása* és *ellenőrzése* céljából.[20] Lényeges eleme a törvényileg biztosított és ellenőrzött *jog* (a vezető hatalma) a vezetői akarat és szándék megfogalmazására, kinyilvánítására és végigvitelére a célkitűzések teljesítése érdekében. Magába foglalja az alárendelt erők (egységek) *alkalmazásának jogkörét* és *felelősségét.*

A *katonai irányítás* azt a hatáskört és felelősséget öleli fel, amelyet a vezető az alárendelt szervezetek tevékenységének *egyes összetevői* (egy része, egy fázisa) vagy a *megerősítő erők* felett gyakorol. Vezetési tevékenység, melynek

---

zásának elvei, politikai következményei. Doktori (PhD) értekezés-tervezet. ZMNE Budapest, 2001. 110. o., VÉGH Ferenc vezérezredes: A Magyar Honvédség feladatai és struktúrája az ezredforduló után, a biztonság alakulásának függvényében. Doktori (PhD) értekezés. Budapest, 1999. 128. o.

[19] „*A vezetés joghatóság és egy személyre van ruházva. Úgy lehet leírni, mint egy folyamatot, amelynek során a parancsnok az akaratát és szándékát keresztülviszi az alárendeltre abból a célból, hogy egy konkrét tevékenység megtörténjen*." (Szövetséges Összhaderőnemi Doktrína AJP-01 1997. szeptemberi kiadás 0402. pont.)

[20] „*Command = parancsnokság; vezetés; parancs: a fegyveres erők egy személyére a katonai erők irányítása, vezetése és koordinálása céljából ráruházott felelőssége*." (NATO szakkifejezések és meghatározások szógyűjteménye ADP-6 (U) HVK Euroatlanti Integrációs Munkacsoport kiadványa Bp., 1996.)

révén a törzs bevonásával szervezi, koordinálja az alárendeltek és a megerősítő erők tevékenységét.[21]

Az irányítás általában *tipizált* (tipizálható) *eljárásokat* jelent az információs, a kommunikációs, a híradó, az informatikai és más vezetéstechnikai rendszerek, eszközök széles körű alkalmazásával.

A vezetés és irányítás egymással szoros kapcsolatban lévő fogalmak, de nem szinonimák. A vezetés *szélesebb* és *komplexebb* tevékenység, magába foglalja az irányítás funkcióit. A vezetés szorosan kötődik a *vezető személyéhez*, az irányításban nagyobb a súlya a törzs tevékenységének. A vezetői szándék és akarat lényegében az irányítás feladat-meghatározó, szervező és koordináló funkciói révén realizálódik.

A MAGYAR HONVÉDSÉG KATONAI VEZETÉSI STRATÉGIÁJA

A Magyar Köztársaság katonai stratégiájában tervezettként megfogalmazott célkitűzésekkel és követelményekkel összhangban a *nemzeti katonai vezetési stratégia* alapvető célkitűzése lehet a szövetségi követelményekkel és az ország gazdasági lehetőségeivel összhangban lévő, a kor színvonalán élenjáró nemzeti katonai vezetési rendszer megteremtése és fenntartása.

A vezetési rendszer mind elvi-elméleti alapjaiban, mind struktúrájában és működési rendjében biztosítja a haderő egészének és részeinek vezetését a béke-felkészítés során, a szűkebb vagy szélesebb régióban bekövetkező és az országunkat, a szövetségeseinket vagy az érdekeinket veszélyeztető válságok, fegyveres konfliktusok megelőzése, lokalizálása, visszaszorítása és kezelése folyamán. Kiterjedtebb fegyveres konfliktus esetén megteremti a vezetés feltételeit a mozgósításhoz, az aktív katonai műveletekhez, az ország védelméhez és a szövetséges védelmi célok teljesítéséhez.[22]

A VEZETÉS FUNKCIÓI

A vezető funkcionális feladatai – vezetési funkciók – közül az információigény és a működési követelmények szempontjából *tervezés és szabályozás*, a

[21] *„Az irányítás a parancsnok által gyakorolt jogkör, ... folyamat, amelyen keresztül a parancsnok a törzs segítségével megszervezi, utasítja és koordinálja a hozzá beosztott kötelékek tevékenységét."* (AJP-01, 0402 pont).

Control = irányítás, vezetés, ellenőrzés: Egy parancsnok által az alárendelt, vagy normális esetben nem az ő parancsnoksága alá tartozó szervezetek tevékenységeinek része felett gyakorolt jogkör, mely felöleli a parancsok vagy irányelvek végrehajtási felelősségét. (AAP-6 U)

[22] A Magyar Honvédség összhaderőnemi vezetési doktrínája. (Kézirat) HVK Vezetési Főcsoportfőnökség 2000. és MRÁZ István: A Magyar Köztársaság Nemzeti Katonai Stratégiája kialakításának jelenlegi helyzete és hatása a haderő átalakítására. Új Honvédségi Szemle 2001/10. szám 15-23. o.

szervezés, az *irányítás* és az *ellenőrzés* tekinthető alapvetőnek és jellemzőnek.[23]

A *tervezés és szabályozás* a helyzetadatok értékelésére, a célok és követelmények megfogalmazására, a feladatok előírására, a környezettel való kapcsolatra, az erőforrások előteremtésére és alkalmazási, felhasználási módjára vonatkozó döntések sorozata. Lényege: a szándékolt állapot megvalósítása, a kitűzött helyzet elérése érdekében a vezetői célkitűzések feladatokra, részfeladatokra, szervezetekre, időre, helyre történő kibontása, elrendelése és tervbe foglalása.

A tervezés során vázolják és végiggondolják a kitűzött cél elérésének lehetséges változatait, elemzik azokat és kiválasztják a legkedvezőbb változatot. A tervezésnek viszonylag kötött rendje, ebből eredően sajátos információigénye van. Többnyire a döntés-előkészítéssel egy időben kezdődik, lényegi szakasza a döntés után és annak révén, a tervek jóváhagyásával fejeződik be.

A *szervezés* a katonai szervezetek létrehozására, működésük feltételeinek megteremtésére és összehangolására irányul. A szervezés ennek megfelelően legalább két részre tagolható: a szervezetek és a tevékenység szervezésére. Mindkét terület a szervezés központi elemével, a munka- és feladatmegosztással kapcsolatos. Az állandó jellegű és az alkalmi szervezetek létrehozása vagy a feladatokhoz történő igazítása közvetlenül szolgálja a szervezeteken belüli munkamegosztást. A tevékenység szervezése pedig a szükségleteknek megfelelően, a helyzethez igazodva teremti meg a célszerű erőforrás-elosztás feltételeit.

Az előzőeknek megfelelően a szervezés egyrészt a mindennapos tevékenység feltételeinek biztosításával kapcsolatos általános teendőket, másrészt a szervezeti struktúrák alakításával kapcsolatos szervezési szakfeladatokat jelenti. A mindennapos operatív szervezői tevékenység a munka összehangolását foglalja magában, eredménye a tervszerűség és a szervezettség. A szakfeladatok a szervezeti elemek harmóniájának biztosítására, a szervezetek külső és belső körülményekhez történő igazítására irányul.

Az *irányítás* központi eleme a valós tevékenység, annak szolgálja a tervszerű megvalósítását. Összetett funkció, magába foglal olyan elemeket, mint a koordinálás, a feltételek biztosítása, a részfolyamatok célirányosságának ellenőrzése, valamint a szükséges korrekciók bevitele.

Az irányítás, a koordináció lényege az egyeztetés és összehangolás a tevékenységek tervszerűsége, szervezettsége és eredményessége érdekében. Az erőforrások, a tennivalók és a feltételek összehangolására irányul. Célja, hogy

[23] Dr KÓTHAY János: A vezetéstudomány helye, szerepe, nézetrendszere. és Dr MEZEY Gyula kandidátus: Folyamatok, biztonság, adatminőség. Az MH új békevezetési rendszere c. tudományos konferencia anyaga. Hadtudományi Tájékoztató 1998/4. szám 51-63. és 178-185. o.

a közösen végzett feladatok a legkisebb ráfordítással, kellő időben, a közös cél érdekének megfelelően, eredményesen kerüljenek végrehajtásra. A koordináció elsősorban a résztevékenységek összehangolását szolgálja.

Az *ellenőrzés* általános célja a vezetés tájékoztatása a kitűzött és a tényleges helyzet/tevékenység egybeeséséről vagy eltéréséről és a kialakult állapotokról. Fontos a szerepe a vezetői szándékok megvalósításában, a döntések helytállóságának igazolásában, a tevékenység hatékonyságának mérésében, a követelmények és az elért eredmények egybevetésében. Eszköze a hibák, a tévedések, mulasztások visszajelzésének, megállapítja azok okait és javaslatot tesz kijavításuk módjára.

Az ellenőrzés fontos információforrás. Nélküle a vezető nem rendelkezne elegendő és kellően objektív információval a szervezet helyzetéről, az abban zajló folyamatokról. A szervezet tagjai, a munkacsoportok, az egyes szervezeti egységek az ellenőrzés értékelő része nélkül felszínesebb visszajelzést kapnának munkájuk eredményességéről és hiányosságairól.[24]

A VEZETÉS FOLYAMAT

A vezetési funkciók a gyakorlatban folyamatjelleggel jutnak érvényre. Olyan főbb tevékenységek sora jelzi a folyamat teljes ciklusát, mint a *célok kitűzése*, az *információgyűjtés,* a *helyzetértékelés*, a *döntés*, valamint a *feladat meghatározása*. Valamennyi vezetési funkcióban a folyamatelemek láncolata és többnyire együttes eredménye jelentkezik.

Minden vezetési folyamatelem *döntés-centrikus*. A vezető feladatai között az egyik legfontosabb és legnagyobb felelősséggel járó feladat a döntések meghozatala. Megalapozása *hatékony információs rendszert* igényel teljes körű, naprakész adatokkal, információkkal és korszerű döntés-előkészítő eljárásokkal.

A döntés a vezetés *egyik legjellemzőbb*, egyben legkockázatosabb *funkciója*. A döntés lényege a lehetőségek közötti választás, amely utasítás, intézkedés, jóváhagyás, egyetértés, kiadmányozás vagy más formában jelenhet meg. Döntési jogosultsággal a vezető rendelkezik, akinek joga és kötelessége a hatáskörén belül döntéseket hozni.

A döntések *kötelező* (cselekvési és magatartási szabályok) vagy *ajánlás* (irányelv) jellegűek lehetnek. Legfontosabb típusai a döntésnek az *általános* (normatív) szabály és az *egyedi* (konkrét) rendelkezés.

A VEZETÉS RENDSZERE

A vezető tevékenységét, feladatainak ellátását és a vezető szervezetek (törzsek) működését a vezetési rendszer támogatja. Az előadás alkalmazásában

[24] A tárgyalt funkciókkal kapcsolatban lényeges hangsúlyozni: külön-külön történt felsorolásukból úgy tűnhet, hogy azok a valóságban is elkülönültek. A tagolásuk azonban csupán a vizsgálatuk szempontjából engedhető meg, a gyakorlatban a funkciók szorosan összekapcsolódnak és átmennek egymásba. Így például, valamennyi funkció az információra épül; a tervezés lényegére nézve döntések sorozata.

jelenti a vezetési feltételek létrehozásához és működtetéséhez szükséges *szervezeti, erőforrás- és eszközrendszereket,* működési (alkalmazási, eljárási) rendjük *elméletét és gyakorlatát*.

A vezetési rendszerrészek (alrendszerek) közül a vezetői követelmények szempontjából az *információs,* a *kommunikációs*, (híradó) és az *informatikai* rendszer bír megkülönböztetett jelentőséggel.

INTEGRÁLT INFORMÁCIÓS INFRASTRUKTÚRA

Az előadás nem tartja a tárgykörébe tartozónak és nem vizsgálja a vezetési rendszer elemeinek konvergenciáját, a híradó és az informatikai bázisra épülő katonai *integrált információs infrastruktúra* (I^3) kialakításának és működtetésének lehetőségeit. Tekintettel azonban a témában élenjáró külföldi és hazai polgári és katonai kutatások tapasztalataira, e kérdéskör a közeljövőben már az MH viszonylatában sem kerülhető meg.

Előrejelzések szerint a vezetés hatékonyságának növelése a jövőben egységes *információs infrastruktúra* alapján képzelhető el, amely integrálja az *informatikai infrastruktúrát*, a kapcsolatait hordozó *kommunikációs technológiát*, a felhasználók igényeihez igazodó *alkalmazásokat,* az *ismereteket* és egyéb elemeket. Az *infokommunikációs eszközök* és az alkalmazásukon alapuló *integrált vezetéstámogatás* új minőségként történő alkalmazása még számos nyitott kérdés megválaszolását, az érintett szakterületek széles körű és tudományos igényű elemzéseit igényli.

Az információs rendszer lényegére nézve *egységes*. Legalábbis a vezetés számára nyújtott szolgáltatási felületei vonatkozásában az. Ebből pedig adódik, hogy idegen tőle minden felosztási szándék, és a rá vonatkozó vezetői követelményeket is integráló szemlélet kell, hogy jellemezze. Az információs támogatás vezetői követelményei egységben kell, hogy kezeljék az információs rendszert. Ez a szintetizáló törekvés harmonizál az *integrált információs infrastruktúrán* alapuló szemlélettel.

Az integrált információs infrastruktúra tágabb környezete a *vezetési rendszer*. Legáltalánosabban, legszélesebb síkon ez ad keretet a vezetői követelményeknek.

VEZETŐI KÖVETELMÉNYEK

Az információs rendszer vezetői követelményei egyrészt a felső vezetési szint *információigényének* maradéktalan kiszolgálására, másrészt az élenjáró informatikai és kommunikációs technikával támogatott *feldolgozó és adatátviteli rendszer kialakítására* irányulnak. A rendszerfejlesztés során ezeken túl figyelemmel kell lenni néhány követelménytámasztó *általános alapelvre* is.

AZ INFORMÁCIÓS RENDSZER KORSZERŰSÍTÉSÉNEK ÁLTALÁNOS ELVEI

Az információs rendszer korszerűsítésére vonatkozó javaslatok kialakításához az alábbi *alapelvek* szolgálhatnak támpontul:

- Az információs rendszer kiszolgáló/támogató jellegének elve. Az információs rendszer és annak egyetlen eleme sem célja, hanem eszköze a

vezetésnek. Az információs rendszert az MH alapvető feladataiból, a vezetés funkcióival és hatáskörével összhangban kell levezetni, figyelemmel a kapcsolódó területek részéről jelentkező követelményekre.

- A felső szintű vezetés felelősségének elve. Az információs rendszer kialakítása felső szinten az ágazati szintű vezetés felelőssége és hatásköre. Az információs támogatás stratégiai kérdéseit ágazati szinten kell megválaszolni, szerepére, fejlesztésének céljaira és irányaira, a megvalósítás tennivalóira és a felhasználható erőforrásokra védelmi ágazati szinten kell elhatározást hozni, figyelemmel a katonai-szakmai javaslatokra és a szakterületi testületek állásfoglalásaira. Csupán ebből az alapállásból biztosítható a rendszerszemlélet, a harmonikus fejlődés és a költséghatékonyság szempontjainak, valamint a vonatkozó kormányhatározat25 előírásának érvényesítése.
- A szervezeti önállóság elve. A katonai szervezetek önállósága az egyeztetett stratégia keretein belül érvényesül az informatikai fejlesztések helyi tervezése és megvalósítása területén.
- A feladat, a felelősség és az erőforrások együttes kezelésének elve. A több szervezet közös érdekeltségében megoldandó feladatok esetén az egyes szervezetek részfeladatait, felelősségeit és a megoldáshoz biztosított erőforrásokat egymással összhangban kell meghatározni.
- A tervszerűség és az összehangoltság elve. A katonai szervezetek információs fejlesztéseinek kiszámíthatóságát, összehangoltságát a központi információs fejlesztési tervre épülő szervezeti információs fejlesztési tervek biztosítják. Eszközeit a katonai szervezetek önálló információs fejlesztési tervei képezik, amelyek végrehajtásáért a készítő katonai szervezet vezetője felelős.
- Biztonság elve. Az adatbiztonságra vonatkozó követelmények, az adatok elvesztése, meghibásodása és megrongálása elleni védelmét szolgálják. Vonatkoznak mind a technikai, mind pedig a szervezési feladatokra, úgy az adatállományok, mint a feldolgozási rendszer megóvására. Az adatbiztonság érdekében a vezetői követelményeknek olyan főbb területekre kell rendszabályokat foganatosítani, mint az adatminőség biztonsága, az adatátviteli hibák elleni védelem, a biztonsági mentések, másolatok készítése, a biztonságos tárolás, a visszaállíthatóság feltételeinek megteremtése, a hozzáférési jogosultság és illetékesség szabályozása, a számítógépvírusok elleni védelem.
- A végrehajthatóság és a végrehajtás támogatásának elve. Minden fejlesztési terv annyit ér, amennyit megvalósítanak belőle. Az információs fejlesztés jogszabályi, pénzügyi és technikai szempontból reális kell, hogy

[25] A Kormány 1066/1999. (VI. 11.) határozata az államigazgatási informatika koordinációjának továbbfejlesztéséről. 2. pont.

legyen. A megvalósításához szükséges erőforrásokat a jóváhagyó felelős vezetőnek kell biztosítania.

- A kapcsolódó rendszerek illeszthetőségének elve. A felső szintű vezetés információs rendszerei fontos hazai és külföldi rendszerekhez kapcsolódnak (pl. NATO-hálózatok, kormányzati levelező rendszert, védelmi felkészítésben és országvédelemben résztvevő szervezetek stb.). Az illeszthetőség érdekében a felek részéről elengedhetetlen a rendszerekre vonatkozó szabványokhoz, előírásaihoz történő igazodás.
- A nyílt rendszerépítés elve. A beszerzés-politikában olyan elveket kell követni, amelyek meggátolják az egyes szállítók monopolhelyzetbe kerülését és fenntartják a versenyhelyzetet a költségek csökkentése érdekében.

A KATONAI FELSŐ VEZETÉS INFORMÁCIÓIGÉNYÉNEK JELLEMZŐI

A katonai felső vezetés információigénye (továbbiakban: információigény) többféle aspektusból vizsgálható. Közülük a *jogszabályokban* és *belső rendelkezésekben* meghatározott *funkcionális feladatok* végrehajtásához szükséges (formális) információbázis igénye tekinthető elsődlegesnek.

Az információigénynek első megközelítésben két, viszonylagosan elkülöníthető forrása van. Úgymint a *saját oldali* (belső), valamint *a külső igények*.

A *belső igények* a haderő szervezeteihez, helyzetéhez, tevékenységéhez és működéséhez kötődnek és vonatkoznak a saját és az alárendelt katonai szervezetek helyzetére, tevékenységére, működésére, a saját katonaföldrajzi környezet adataira.

A *külső igények* a tágabb környezet helyzetéhez, folyamataihoz kapcsolódnak, különös tekintettel a szövetségi viszonyokra, a kormányzati és országos hatáskörű szervekkel történő együttműködésre, az információs társadalmi törekvésekre, a biztonsági helyzet alakulására és a tágabb régió katonaföldrajzi adottságaira.

Lényeges hangsúlyozni, hogy a saját oldali igény szinte valamennyi összetevője és folyamata *kétirányú információáramlást* jelez. A felhasználók és a szolgáltatók kölcsönösen – egymással szemben – jelentkeznek információ igénnyel és szolgáltatási kötelezettséggel.

A külső igények egy része nyílt jellegű és szabadon hozzáférhető információra vonatkozik, más része viszont speciális módon megszerezhető, védett adatokra, információkra irányul.

Súlya és szerepe alapján békében a *belső információigény* a meghatározó. Ez az igény kapcsolódik közvetlenül a HVK rendeltetéséhez, funkcionális feladataihoz. További információigénnyel jár a vezetési szervezet munkájának koordinálása, a szervezeti elemek közötti kölcsönös tájékoztatás és a belső informálódás.

A HONVÉD VEZÉRKAR FŐNÖK FELADATKÖRÉHEZ KÖTŐDŐ INFORMÁCIÓIGÉNY

Az információigény meghatározásához és leírásához a legfontosabb szempontot a katonai vezetés legalapvetőbb sajátossága adja. Nevezetesen: a honvédség *egyszemélyi felelős vezetés* alatt álló szervezet. A honvédség katonai tevékenységét a honvéd vezérkar főnök (HVKF) vezeti. Prioritása van azoknak az igényeknek, amelyek a haderő törvényes működtetéséért, a jogszabályokban, határozatokban, utasításokban, illetőleg a Kormány és a honvédelmi miniszter által egyedileg megállapított feladatokért viselt felelősségéhez és a belőle fakadó vezérkar főnöki feladatokhoz kötődnek.

A HVKF vezetői felelősségéhez, tevékenységéhez kötődő információigény és az általa meghatározott információs kör mindenekelőtt:

- MH szintű, hadászati és összhaderőnemi jelleggel bír;
- összefogottan, a teljesség igényével jellemzi a haderő helyzetét, alkalmazhatóságát;
- bemutatja a honvédség felkészítésének, béketevékenységének helyzetét, folyamatait;
- megalapozza az egyszemélyi vezetői feladatkörét érintő kormányzati döntések előkészítését;
- támogatja az ország fegyveres védelemre történő felkészítésével összefüggő követelmények meghatározását, a honvédelemben résztvevő szervek feladatainak megállapítását;
- biztosítja a minősített időszakok vezetési rendjére vonatkozó döntések meghozatalát;
- reális alapot ad az alárendelt katonai szervezetekkel szembeni követelmények megfogalmazásához, feladataik meghatározásához, tevékenységük értékeléséhez;
- megalapozza a hatósági feladatokhoz kapcsolódó döntéshozatalt.

A fentiekből következtethető, hogy a HVKF vezetői információigénye igen *széleskörű* és *sokoldalú*, ugyanakkor szakszerűen *válogatott* és mesterien *összefogott* információbázist jelöl. Teljesítése körültekintő, alapos és sokirányú információgyűjtő, elemző, értékelő tevékenységet követel a HVK-tól. Az igények kielégítésére kialakított információs rendszernek biztosítania kell a fenti követelmények mennyiségi és minőségi kielégítését.

A HVKF információigénye kisebb részben *általános*, nagyobbrészt *egy-egy helyzethez, eseményhez kötődik*. Az időszerű vezetői döntések meghozatalához kötődő információk rendre egy-egy vezetési aktushoz vagy annak valamely fázisához kötődnek. Nem elhanyagolható ugyanakkor az állandó (folyamatos) jellegű igénye sem az általános tájékozódás és tájékoztatás céljából.

A HVK SZINTJÉN JELENTKEZŐ INFORMÁCIÓIGÉNY

A HVKF személyes vezetői tevékenysége – annak információ- szükséglete – lényegében a HVK szintjén is meghatározza az információigényt. A vezérkar

főnök információigényének döntő hányadát a HVK szervek által gyűjtött, értékelt, elemzett és összegzett információk elégítik ki.

Lényeges sajátossága a vezérkar információigényének, hogy az a honvédség fő tevékenységi területeihez kapcsolódva, *szakági tagozódásban* jelentkezik. A HVK rendeltetésére, fő feladataira épülő szervezeti tagozódással összhangban a vezérkari információigény *szakterületeit adják*:

- a személyügyi szakterület a béke és háborús humán erőforrás biztosítással, személyügyi, kiegészítő, humánszolgálati és képzési feladatokkal kapcsolatos szakmai igényekkel;
- a felderítő szakterület a hadászati, a hadműveleti-harcászati felderítés tervezésével, szervezésével, irányításával, a felderítési adatok gyűjtésével, értékelésével, a katonai felső vezetés és a haderőnemi vezérkarok tájékoztatásával, az elektronikai hadviselési feladatokkal kapcsolatos igényekkel;
- a hadműveleti szakterület a haderő hadászati-hadműveleti szükségleteinek összhaderőnemi tervezésére, az alkalmazás, a készenlét fokozás, a felkészítés és kiképzés, a helyőrségi, a katonai rendészeti és őrzésvédelmi, a szabványosítási, a doktrinális és a civil-katonai kapcsolatok követelményeinek kidolgozására, tervezésére vonatkozó igényekkel;
- a logisztikai szakterület a honvédség logisztikai biztosításának tervezéséhez, szervezéséhez és irányításához, valamint a költségvetési tervezés koordinálásához szükséges igényekkel;
- a védelmi tervezési szakterület az MH fejlesztésére, korszerűsítésére, a hadseregépítés hosszú és középtávú célkitűzéseire, fő irányaira, követelményeire és feladataira vonatkozó felső szintű igényekkel;
- a vezetési szakterület a béke- és háborús általános vezetési és irányítási, az ellenőrzési, a híradó, az informatikai és a biztonsági feladatok általános elveinek, követelményeinek, szabályozóinak felső szintű tervezéséhez, a kapcsolódó tevékenységek koordinálásához és szakmai irányításához kötődő igényekkel.

A felsorolt területeken túl az *egészségügyi*, valamint a *szárazföldi* és a *légierő haderőnemi* és a *logisztikai támogatási* szakterületre vonatkozó információs elvárások teszik teljessé a felső szintű vezetés információigényét.

A szakterületi információigény szinte valamennyi eleme tovább strukturálható a vezetés funkciói és a folyamat-elemei szerint.

FUNKCIONÁLIS KÖVETELMÉNYEK

Az előadás értelmezésében a vezetői követelmények az információs rendszer alkalmazásával, *funkcionálásával* kapcsolatos *általános felhasználói elvárások*, melyeket a katonai vezetők a szakterületi vezetők, technikai és műszaki fejlesztők közreműködésével az információs rendszer tartalmi oldalával, funkcionális működésével szemben támasztanak, s amelyek kielégítése lehetővé

teszi a hatékony alkalmazását. A vezetői követelmények a *szakmai követelményekkel együtt* képezik a rendszertervezés és megvalósítás alapjait.

A kialakításra kerülő rendszernek a *vezetés igényeire* kell épülnie. A döntési és az információs szintek összhangjának követelményéből adódik, hogy az adott vezetési szintnek behatárolható, önálló rendszerrészként is vizsgálhatónak és működőképesnek kell maradnia.[26]

A HVK információs rendszerének viszonylagos önállóságát a honvédségi (tárca-) szintű, egységes információs rendszer kialakítása esetén, annak keretében is meg kell őrizni.

A rendszer adatbázisainak egyaránt tartalmazniuk kell *a béke- és a minősített időszakok* vezetéséhez szükséges adatokat. A követelményt mindenekelőtt annak belátása és elfogadása indokolja, hogy mindkét időszakot egyenrangúan kell támogatnia, amelyből adódóan mind az infrastruktúra, mind a programok vonatkozásában egységes rendszerként épül fel és működik. Szigorúan elhatárolt ugyanakkor a két terület egymástól az adatok tárolása, a hozzáférés engedélyezése és a biztonsági-védelmi megoldások szempontjából.

Az információs rendszer biztonságának tekintetében alapkövetelmény, hogy a minősített adatokat feldolgozó alrendszerek még többszörösen védett áttételeken sem kapcsolódhatnak a nyílt rendszerekhez.

A felső szintű vezetés információs rendszerének a haderő helyzetének és tevékenységének *valamennyi lényeges területéről* adatot, információt kell szolgáltatnia. Az információs adatbázisnak, adatfeldolgozási rendszernek a vezetési szinten meghozandó döntések információs hátttereként minden adatot, információt, feldolgozási eljárást, tárolási, archiválási lehetőséget biztosítania kell.

ÁLTALÁNOS FELHASZNÁLÓI ELVÁRÁSOK

Az információs rendszerrel szembeni *általános elvárások* (követelmények) a rendeltetés, az adatok, információk időbelisége és a tartalma, valamint a kimenő adatok megjelenítése és formája alapján tagolható.

Az információs rendszer *rendeltetéséhez, alapvető feladataihoz* kapcsolódó elvárások lényege, hogy az adatoknak és információknak támogatniuk kell a haderő stratégiai átalakítását, alkalmazásának, tevékenységének és működésének tervezését, a vezetők tájékoztatását. Ezen túl segíteniük kell a napi operatív feladatok végrehajtását, a tevékenység összehangolását, lehetővé téve az érintett partnerek közötti a kommunikációt.

Az információk *időbeliségére* vonatkozó követelmények azt fogalmazzák meg, hogy az adatok folyamatosan vagy az előírt szükséges gyakorisággal rendelkezésre álljanak és azok az aktuális, a valós állapotot tükrözzék.

[26] SZŰCS Gáspár: A hadászati-hadműveleti vezetés integrált számítógépes rendszeréről. Új Honvédségi Szemle 1997/2. szám.

Az *adatok tartalmára* vonatkozó követelmények a pontosságukra, a teljességükre és a hitelességükre vonatkoznak. A pontosság kritériuma a reális helyzettel való összhangot fejezi ki.

A *formai* megkötések a kimenő adatokra (táblázatos vagy grafikus állományra, listákra) vonatkoznak, függetlenül azok megjelenési formájától. Lényeges szempont a kezelhetőség, az egyszerűség, az áttekinthetőség és a célszerű elrendezés.

KÖVETKEZTETÉSEK

- Az információs rendszer vezetői követelményeire irányuló vizsgálatoknál abból a kell kiindulni, hogy a katonai felső vezetés – a Honvéd Vezérkar – szintjén mind a vezetést, mind pedig annak információs hátterét elvek, szabályok és törvényszerűségek jellemzik, amelyek viszonylagos önállósággal kezelhetők és kutatható rendszerrészt képeznek. A vezérkar vezetői információs rendszere szerves elemét képezi a védelmi ágazat szintjén egységes információs rendszernek. Felépítésének, működési sajátosságainak és kapcsolatainak feltárása során soha nem szabad szem elől téveszteni a rendszerhatárokat és az azokon keresztül kapcsolódó rendszerkörnyezetet.
- A vezetői információs rendszert a kapcsolódó tudományterületek általános alapelveiből és követelményeiből kiindulva kell vizsgálni és kialakítani. Az elvi-elméleti megközelítés alapvető a tudományos értékű és időálló megoldások kimunkálása szempontjából.
- Korunk átalakult biztonsági viszonyai, a NATO szövetségi rendszeréhez történő csatlakozásunk, a honvédelem helyének, szerepének és a haderő működési feltételeinek újragondolása minőségileg új kihívásokat és feltételeket közvetít a honvédség vezetésével, annak információs támogatásával szemben.
- A magyar haderőt a fő feladataival összhangban új tartalmú katonai-biztonságpolitikai feladatokra és újszerű nem katonai fenyegetések és veszélyhelyzetek megelőzésére vagy felszámolására kell felkészíteni. Jelentősen növekednek a követelmények a nem háborús műveletekre irányuló békevezetés előrelátásával, megalapozottságával és rugalmasságával szemben. Mind jobban előtérben marad a béketámogató műveletekben történő részvétel. Mindezek elodázhatatlanul és sürgető jelleggel igénylik az információellátás és tájékoztatás rendszerének új alapokra helyezését.
- A haderő információs rendszerének egységes stratégia, működési rend és infrastruktúra alapján kell állnia. A HVK vezetői információs rendszer szerves része az MH szinten egységesnek elgondolt információs rendszernek. Kialakítását a Honvéd Vezérkar szintjén kell megalapozni, kezdeményezni és koordinálni valamennyi érintett fél bevonásával.

- Az információs rendszer átalakításának elvi koncepciója, a megvalósítás gyakorlata figyelemmel kell, hogy legyen a jelenleg reálisan létező információs alapokra, a szellemi bázisra, a működtetés hagyományaira, az infrastruktúrára.
- Az átalakítás stratégiája hosszabb időszakra is kellő távlatokat kell, hogy teremtsen. Az új minőség hosszabb távon, több szakasz alakul ki. Minden szakasza pontosan körülhatárolható, egymásra épülő részcélok teljesítése érdekében folyik.

Összegzett tanulságként megállapítható, hogy az új vezetői információs rendszert *integrált jelleggel, egységes* elgondolás szerint kialakított és működtetett *adatbázisra* építve, kellően *tagolt* és *viszonylagosan önálló funkcionális alrendszerek* működtetésével, a szövetségi és a hazai viszonylatban is a mindenkori *élvonalba tartozó kommunikációs* és *informatikai eszközrendszeren* célszerű kialakítani.

IRODALOMJEGYZÉK

1. A Kormány 2204/2001. Határozata a Magyar Köztársaság a Magyar Honvédség irányításának és felsőszintű vezetésének rendjéről.
2. A Magyar Honvédség összhaderőnemi vezetési doktrínája. (Kézirat) HVK Vezetési Főcsoportfőnökség 2000.
3. NATO szakkifejezések és meghatározások szógyűjteménye. AAP-6 (U). HVK Védelmi Tervezési Főcsoportfőnökség kiadványa. Budapest 1999. (Az 1998. évi NATO kiadás fordítása).
4. Dr. BANA István: Az SSADM rendszerszervezési módszertan. LSI Oktatóközpont Budapest, 1994.
5. GORZA Jenő: Elgondolás a Magyar Honvédség informatikai fejlesztésére. Új Honvédségi Szemle 1999/7. füzet.
6. Dr. HALASSY Béla: Az adatbázis-tervezés alapjai és titkai. IDG Magyarországi Lapkiadó Vállalat Kft. Budapest, 1994.
7. MRÁZ I.: A katonai felső szintű vezetés információs rendszerének korszerűsítése I., II., és III. rész. Új Honvédségi Szemle 2001/7. szám 26-46. oldal, 2001/8. szám 32-52. oldal és 2001/9. szám 28-47. oldal,
8. MRÁZ I.: A Magyar Honvédség felső szintű vezetésének információigénye és az információs rendszer fejlesztésének iránya. ZMNE Repülőtiszti Intézet Repüléstudományi Közlemények XII. évfolyam 29. szám 2000. 275-288. oldal.
9. MUNK Sándor: Katonai informatika. Jegyzet a ZMNE hallgatói számára Budapest, 1997.
10. PINTÉR István: Katonai vezetés és szervezéselmélet. Egyetemi jegyzet. Budapest, ZMNE 2000.
11. RAFFAI Mária: Információrendszer-fejlesztés. Novadat Kiadó Győr, 1999.
12. SZŰCS Gáspár ezredes: A katonai vezetés harcászati szintje információfeldolgozásának korszerűsítése. PhD értekezés. ZMNE Budapest, 2000. június.

Dr. Rajnai Zoltán

A HADSZÍNTÉR DIGITALIZÁLÁSA

Napjainkban a csapatok törzseiben, egységeiben, alegységeiben tevékenykedők, a feladatok kidolgozásában és végrehajtásában közreműködők munkájuk során különböző irodai alkalmazású kommunikációs eszközöket (számítógépek, híradó berendezések), rendszereket (LAN, strukturált hálózatok, stb.) használnak. Ezen törzsek, parancsnokok jogos elvárása, hogy hadműveleti feladatok előkészítése, kidolgozása és végrehajtása során a hadműveleti területen is képesek legyenek hasonló, esetenként még több szolgáltatás és adatbázis igénybevételére, mint béke elhelyezési körleteikben, helyőrségeikben. Mint ahogy egy vállalatnál a számítógépes és kommunikációs hálózat, az Internethez történő hozzáférés és alkalmazás, vagy az IP[27] alapú telefónia biztosítja a feltételeket az információk megszerzésére, tárolására és továbbítására a felhasználók felé, úgy azonosítható ezzel egy laktanya, vagy helyőrség információs rendszere is. Kimondhatjuk tehát, hogy egy (polgári) vállalati rendszer és egy katonai rendszer között jelentős eltérés csak a rendszerek speciális, hierarhizált tulajdonságaiban van. Maga a rendszer, annak felépítése, üzemeltetése, eszközrendszere megegyezik. Ebből következően megállapítható, hogy a honvédség által alkalmazott hálózatok struktúrája, szolgáltatásai hasonlóak egy vállalati rendszerhez, amit hadműveleti területen éppúgy alkalmazni kívánnak a felhasználók, mint standard körülmények között. De vajon képesek vagyunk-e biztosítani mindezeket hadműveleti területen és alkalmazás közben? Erre kell keresni a megoldásokat és a lehetőségeket.

Az ATM alapú hálózat alkalmazásának szükségessége

Az elektronikai technológia, a távközlési- és informatikai eszközök és rendszerek robbanásszerű fejlődése következtében a NATO tagállamokban megkezdődött a PCM alapú rendszerek leváltása egy korszerűbb, nagyobb adatátviteli sebességet biztosító tábori digitális hálózatokra

A hadműveleti és harcászati vezetés szintjén a multimédiás szolgáltatások kiemelt szerepet kapnak, ahol a hang- és adatátvitel mellett a videokonferencia szolgáltatások nagyfokú igénybevétele történik. Ehhez azonban már csak elégséges feltétel lesz a PCM alapú tábori hálózat, ahol elsősorban a polgári kivitelű CB telefonok, militarizált LB telefonok és a G3 szabványtípus követelményeit kielégítő FAX berendezések találhatók a végberendezések szintjén, míg ISDN szolgáltatásokra alkalmas adapter csatlakoztatása esetén a kapcsolóközpontokhoz illesztett multimédiás számítógépek és videokonferencia terminálok

[27] Internet protokol

biztosíthatnak szolgáltatásokat. A hadműveleti-harcászati vezetés azonban az információkat reál- (valós)[28] időben kívánja feldolgozni és felhasználni, ezért azt nagy átvitelt nagysebességű hálózaton kell továbbítani magas szintű szolgáltatási minőséggel (QoS[29]). A nagy felbontású képek, videokonferenciák és egyéb jellegű információk egyidejű továbbítása esetén a szükséges csatornakapacitás esetenként már a néhány tíz Mb/s-os jelfolyam sebességet is megköveteli. Erre a feladatra az ATM technológia nagyon megfelelő. Ez a technológia nem más, mint a széles sávú ISDN (B-ISDN[30]) megvalósításának lehetősége, amely biztosíthatja a hálózati videózás, a mozgóképes multimédiás elektronikus küldemények továbbítását, LAN hálózatok összekapcsolását és a nagysebességű átvitelt csomagkapcsolt formában. Az ATM hálózat adatátviteli sebessége 155 MB/s[31], ami a keskenysávú ISDN sávszélességének 2500-szorosa.

Nyugat-Európában több ország is felismerte ezt a problémát, melynek kiküszöbölésére az ATM[32] alapú kommunikációs rendszereket kezdték rendszerbe állítani. Ilyen rendszert alakított ki haderejében Franciaország, a vezetési pontok kommunikációs hálózatában Németország, az USA, majd Belgium, Nagy-Britannia, és Olaszország is. Ezekben a NATO tagországokban felismerték a reális idejű adattovábbítás, a több résztvevős videokonferenciák és konferenciabeszélgetések jelentősségét. Az ilyen jellegű összeköttetéseket tömegesen alkalmazták például az Öböl-háború idején is. A kommunikációs feltételek biztosításához tehát rendelkezésre állnak a polgári életben az említett jellegű összeköttetések biztosításához szükséges távközlő és informatikai eszközök, így ezek alkalmazása, katonai körülményekhez történő igazítása lesz a kommunikációs rendszerek kialakításának előfeltétele, melynek során például a szélsőséges hőmérsékleti viszonyoknak, a rázkódásnak kell megfeleltetni az eszközöket.

A hadműveleti helyzetek gyors változása nem teszi tehát lehetővé a vezetési pontok hálózatainak hosszú idejű kiépítését és telepítését, konfigurálását, vagy áttelepítését, ezért ki kell alakítani a minimális telepítési idejű rendszert, a kezelők rövid idő alatti telepítési és beállítási feladatait, vagyis a lehető legnagyobb automatizáltságra kell törekedni. Ennek lehetőségét is nagymértékben képesek biztosítani a polgári kereskedelemben vásárolható eszközök, melyek megfelelnek a Plug and Play (PnP)[33] automatikus ki- és belépési rendszer lét-

[28] kis késleltetési idővel

[29] Quality of Service – Szolgálat minősége, az ATM szabvány által definiált paraméterek

[30] Broadband Integrated Services Digital Network

[31] pontosan 155,52 Mb/s

[32] ATM= Aszinkron transzfer mód

[33] Plug and Play (PnP) = Csatlakozás és alkalmazás

rehozásának. Ezt, ha egy konkrét helyzetre, a válságkezelésre vizsgáljuk megállapítható:

- a zászlóalj harccsoportok és a dandár operatív csoport vezetési pont hírközpontja települ a válságkezelés kezdeti időszakában;
- a helyzet további eszkalálódása után már a dandár szervezetének más cellái[34], az összfegyvernemi-, fegyvernemi- és szakalegységek is alkalmazásra kerülhetnek;
- a hadtest és a dandár tábori vezetési pontjai fokozatosan települnek ki a hadműveleti területre, és a teljes hadrend folyamatosan alakul ki. Az újonnan belépő cellák saját információs rendszereikkel kívánnak csatlakozni, vagy éppen leválni a hálózatról. Ezek a változások rendszer szinten nem jelenthetnek semmilyen befolyásoló hatást a hálózat működésére éppúgy, mint ha egy-egy kapcsolóközpont, vagy router meghibásodna.

A hálózat kialakításakor tehát egy olyan protokollt kell kiválasztani, amely a speciális katonai tényezőket figyelembe veszi, mint például a nagy adatátviteli sebesség, a könnyű kezelhetőség, a nagyfokú automatizáltság, a speciális dimenziók a rendszer felépítésében és működésében pedig kiszolgálják a felhasználókat igényeiknek megfelelően.

Az ATM alapú rácsrendszer felépítése

A NATO Katonai Bizottsága a „Tactical Communications Post-2000" (TACOM post-2000) megnevezéssel egy új architektúra típust javasolt a szárazföldi erők harcászati (mobil) kommunikációs rendszereihez. Ezt a nyugati haderők többségében már elfogadták, és rendszereiket ez alapján alakítják át, modernizálják. Ez az architektúra típus a hadműveleti erők számára lehetővé teszi:

- a vezetési (parancsnoki) lánc folytonosságát a hadtesttől a zászlóalj-, század szintekig;
- az információs rendszerek összekapcsolhatóságát minden szinten;
- az összekapcsolt hálózatok interoperabilitását a nemzeti törzsek szintjétől a hadműveleti feladatokat végrehajtó csapatokig, és a szövetséges erők nemzetei között is a kommunikációs eszközök széles skáláján.

Az ATM alapú hálózathoz csatlakozó hadtest-, dandár-, ezred- és zászlóalj vezetési pontok azonos képességekkel (jelfolyamokkal) csatlakoznak hírközpontjaikkal ehhez a rendszerhez az alacsonyabb vezetési szintek (pl.: század, harcrendi elemek) mobil felhasználóként rádióállomások alkalmazásával rádiótelefon jellegű kapcsolattal tartanak folyamatos összeköttetést a hálózaton keresztül az elöljáró szervezetekkel és más felhasználókkal.

[34] a törzs (S1-S6) vezetési, irányítási részei (lásd: Rövidítések)

A csomópontokból tehát a hálózat kialakítása érdekében biztosítani kell a szomszédos csomópontok irányába mikrohullámú összeköttetéseket, és képesnek kell lenniük a különböző szintű csatlakozó hírközpontok mikrohullámú berendezéseinek fogadására is. A hálózat csomópontjai egymástól 15-30 km-re települhetnek a hadműveleti területen, és ezeket több helyen illeszteni kell a stacioner területi hálózat csomópontjaihoz, valamint más NATO tagország kommunikációs rendszerével, és a polgári távközlési objektumokkal történő együttműködési képességre is alkalmassá kell tenni azokat.

A vezetési pontok belső kommunikációs hálózata

Az ATM alapú hálózat kialakításánál nagyon fontos a vezetési pontok belső kommunikációs rendszerének meghatározása, majd az erre épülő hadműveleti-harcászati csatlakozási sík felépítése. A vezetési pontok belső hálózatánál biztosítani kell, hogy a katonai szervezet törzscellái (G1-G6, S1-S6, stb.) egyidőben és széles körben alkalmazhassanak informatikai eszközökkel támogatott multimédiás kapcsolatokat a döntéselőkészítés, az elhatározás, és az adattovábbítás során, valamint ezzel párhuzamosan a digitális távbeszélő szolgáltatásokat ugyanazon kommunikációs hálózaton keresztül vehessék igénybe, hiszen a korszerű kommunikációs rendszereknek ezeket a szolgáltatásokat egy hálózaton belül kell biztosítania az informatikai és a távközlő hálózatok integrálásával. Ehhez olyan kapcsolókat kell kialakítani, melyek képesek analóg- és digitális trönköket, számítógép hálózatokat fogadni NATO STANAG-eknek és polgári szabványoknak megfelelően, valamint biztosítani szabvány Ethernet típusú kapcsolatot számítógépek, munkaállomások, hub-ok[35], szerverek[36] és routerek[37] részére. Ezeket a berendezéseket egy készülékbe építve olyan kapcsolókat kaphatunk, melyek egyidőben képesek:

- ATM kapcsolóként,
- Fast Ethernet[38] és IP[39] kapcsolóként, valamint
- Hagyományos PABX kapcsolóként üzemelni.

Az így kialakított berendezések a szolgáltatások jellegéből adódóan multimédiás kapcsolóknak (továbbiakban MUK) nevezhetők.

A vezetési pontokon a harcvezetésben és a hadműveletek különböző biztosítási feladatainak tervezésében, szervezésében és végrehajtásában részt vevő felhasználók igénye azonban nem csak az, hogy az informatikai hálózaton keresztül saját szervezetük törzsének más felhasználóival tarthassanak kapcsolatot, hanem igényük van arra is, hogy ezzel egyidőben, fizikailag egy másik

[35] elosztó egységek a számítógépes hálózatot használó munkaállomások csatlakoztatására

[36] a (helyi) hálózatok központi kiszolgáló egysége

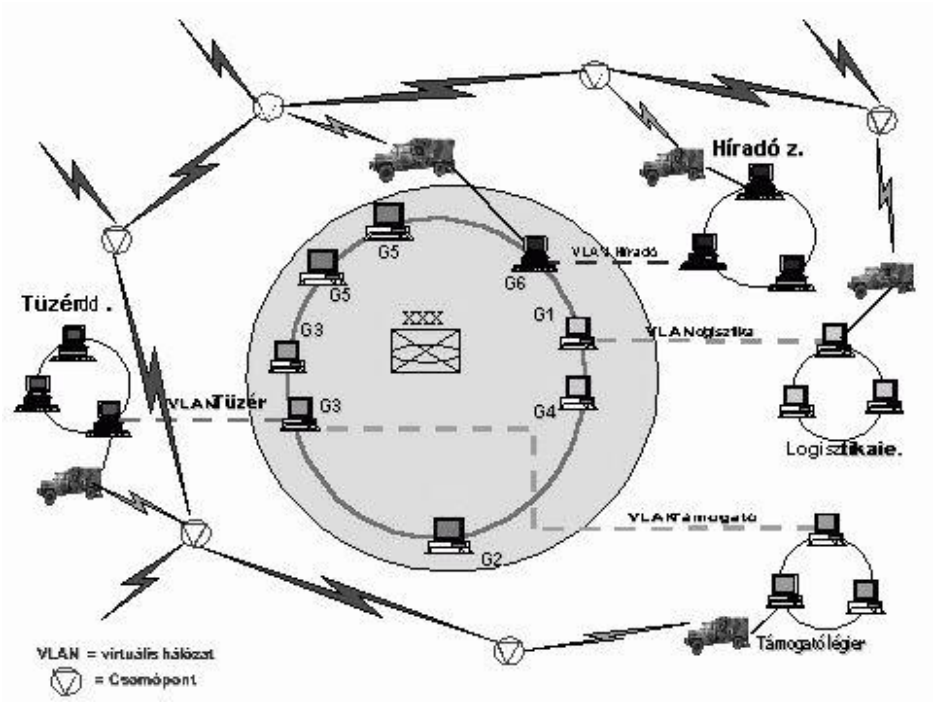
[37] útvonal-meghatározó, útvonal-kijelölő, útvonal-választó egység

[38] gyors helyi hálózat

[39] Internet protokoll

LAN hálózathoz csatlakoztatott felhasználóval cserélhessenek információt munkaállomásaikról, vagy adhassanak utasításokat. Egy konkrét példán keresztül bemutatva: a hadtest G3 (hadművelet) cella hálózatában dolgozó tüzér főnökség nem csak a hadtest törzs más felhasználóival kíván adatcserét és információs csatornákat, hanem a hadműveleti feladat végrehajtásában részt vevő tüzér egység vezetéséhez is adatokat szeretne részükre továbbítani, vagy tőlük kapni. Ezek a csapatok azonban termináljaikat saját törzsük informatikai hálózatához kapcsolva alkalmazzák, melyek egy-egy másik önálló LAN hálózatot jelentenek. Az ATM technológia alkalmazása esetén ezeket a hálózatokat nem szükséges közvetlen fizikai kapcsolattal összekötni, hanem elegendő egy közös csomóponti hálózathoz kapcsolni. Ezért a kapcsolatok realizálásához a vezetési pontokon egy-egy híradó állomásra van szükség, mint átviteli utat biztosító elemre, a csomóponti hálózathoz történő csatlakozás érdekében. Ezzel azonban még csak az adattovábbítás lehetősége biztosított. A további probléma feloldására az ATM rendszer megoldási lehetőséget a korábban említett virtuális áramkörök, és kapcsolatok létesítésével nyújt. Így megvalósítható a különböző vezetési szintek fizikailag közvetlenül össze nem kötött (nem azonos LAN hálózatban üzemelő) számítógépeinek és felhasználóinak kapcsolata logikai összeköttetések felhasználásával a **közös csomóponti hálózat** használatával. A különböző LAN hálózatok termináljai közötti kommunikációhoz tehát nincs szükség fizikai kapcsolat kiépítésére, mert a csomóponti hálózat tölti be ezt a szerepet. E szolgáltatás katonai alkalmazásának vizsgálatát segíti az ábra, ahol a gépesített hadtest vezetési pontjának virtuális hálózatkialakításának részlete látható egy lehetséges változatban.

A hadtest LAN hálózata optikai kábellel kiépített gyűrű struktúrában kerül telepítésre. A vezetési ponton a törzs felhasználói (G1-G6) saját termináljaikat e hálózatba integrálva használják, ugyanakkor az alárendelt fegyvernemi- és szakalegységekkel, a csapatok vezetési pontjaival az egyes cellák képesek virtuálisan (a valóságban fizikailag közvetlenül össze nem kötötten) hálózatot kialakítani. (Az egyes VLAN rövidítések az ábrán a virtuális hálózat kialakítási lehetőségére utalnak, ahol az ábrázolt sejtek önálló LAN hálózatai mellett jelenik meg a virtuális kapcsolat.) E módszer alkalmazásával a hálózati szolgáltatásokon és a virtuális kapcsolatokon kívül továbbra is biztosított a saját törzseken belül üzemeltetett katonai üzenetkezelő rendszer (MMHS) funkcionális működtetése is.



A virtuális hálózat kialakítási lehetősége (részlet)

A virtuális hálózat tehát a LAN hálózat mellett képes biztosítani az elöljáró fegyvernemi- és szolgálati ág főnökök virtuális csatornáit, melyek a beszéd kapcsolat mellett a multimédiás szolgáltatásokra is vonatkoznak. A vezetési pontokon e rendszerszolgáltatás biztosítására tehát a cellák felhasználói részére tehát olyan berendezés szükséges, amelyik lehetővé teszi az ATM technológia szolgáltatásainak igénybevételét a beszéd-, kép- és adatátvitel területén egyaránt. Ezt a szerepet a **multimédiás kapcsoló egységek** (MUK) tölthetik be az ATM alapú tábori kommunikációs hálózatokban. Ezek a berendezések biztosítják a csatlakozási felületet a hálózati elemek (munkaállomások) részére, valamint lehetőséget adnak az átviteli utat biztosító híradó állomás szükség szerinti csatlakoztatására is. A multimédiás kapcsolók között, és a csomóponti hálózathoz csatlakozó híradó állomás között a nagysebességű adatátvitel érdekében tábori kivitelű optikai kábelek szükségesek, melyek lehetőséget adnak a hálózaton belüli 155 Mb/s jelátvitelre, így a hagyományos szolgáltatások mellett a multimédiás szolgáltatások is biztosítottak lesznek a felhasználók részére. Egy így kialakított hadtest vezetési pont kommunikációs igényei kiszolgálására létrehozott LAN hálózat elvi felépítését mutatja az ábra, ahol a cellák egymáshoz kapcsolt rendszere mellett az átviteli utat biztosító híradó állomás

is megtalálható. Ez a változat akár egy védett vezetési ponton, béke elhelyezési körletben (laktanyában), vagy tábori körülmények között is megvalósítható.

A cellákban található, egymáshoz kapcsolt multimédiás kapcsolók biztosítják tehát a felhasználói terminálok és más kommunikációs eszközök csatlakoztatását, így összességében egy vegyes topológiájú[40] információs hálózatot alakítanak ki, ahol a vezetési cellák munkaállomásai csillagtopológiát alkotnak, addig a multimédiás kapcsolók a LAN hálózaton belül gyűrű- és csillag topológiában helyezkednek el.

A csillag topológiában minden egyes elem egy-egy közös kapcsolóhoz csatlakozik, így ennek előnye az egyszerű és gyors telepíthetőség, valamint az, hogy az egyes terminálok meghibásodása nincs hatással a topológiában található más munkaállomás működésére, így a hálózat megbízhatóan használható. A multimédiás kapcsolók önállóan is működőképesek, a kapcsolók telepítésével rugalmasan bővíthető hálózat alakul ki PnP[41] rendszerben vagyis a hálózathoz történő csatlakoztatásuk és az onnan történő kilépésük automatikus; a hálózat érzékeli az újabb becsatlakozó kapcsolók megjelenését, vagy távozását és a felhasználói hálózatot a rendszer automatikus konfigurálással alakítja ki. Egyes kapcsolók esetenkénti meghibásodása ez esetben nem okoz problémát a hálózat szintjén, mert a rendszer ettől függetlenül tovább üzemel, kiesés csak az adott kapcsolóhoz tartozó végberendezéseknél lehet. Egy-egy vezetési ponton a multimédiás kapcsolók száma elsősorban nem annak nagyságától, hanem a vezetési pontokon lévő felhasználók számától és az alkalmazott végberendezések számától függ. Így például dandár vezetési ponton már egy-kettő, hadtest vezetési ponton három-négy multimédiás kapcsoló is elégséges a vezetési ponton települt cellák összeköttetései minden fajtájának biztosítására.

Ezeknek a multimédiás kapcsolóknak biztosítaniuk kell egyidőben 10-12 munkaállomás (PC) fogadását, 10-12 (szükség esetén információvédelemmel ellátott) analóg távbeszélő- és/vagy G3 típusú FAX berendezés csatlakoztatását, 3-4 S_0 összeköttetés létesítését (ISDN digitális telefon, G4 típusú FAX, videokonferencia terminál, stb.), valamint 3-4 ATM (155Mb/s) irány fogadását optikai kábelen. Ezeknek a csatlakozási felületeknek meg kell felelniük mind a polgári, mind a NATO csatlakozások normáinak (STANAG 5040, 4206, 4249). A vezetési pontokon található kapcsolók egymással optikai kábellel kerülnek összekötésre, így azok képesek biztosítani a nagysebességű adatátvitelt a munkaállomások és felhasználók között, és egyúttal biztosítják az Internet protokoll alapú (IP) és a virtuális hálózati szolgáltatásokat egyaránt. A hadtest vezetési pontokon a törzs celláinak munkaállomásai mellett a multimé-

[40] topológia: A számítógépes hálózatban a munkaállomások és kiszolgáló elemek fizikai és logikai eléhelyezkedése

[41] Plug and Play

diás kapcsolókhoz kell csatlakoztatni a különböző szervereket[42] (pl.: E-mail), valamint a C3I rendszer teljes körű működését biztosító adatbázis szervert is. E rendszerben a törzs cellák azon munkaállomásai láthatók, amelyek a virtuális LAN hálózatokban üzemelhetnek, vagyis az alárendeltek felhasználóival tarthatnak információs kapcsolatot. A virtuális hálózati munkaállomások mellett azonban üzemeltetni kell az INTERNET/INTRANET szervereket. Ennek oka az, hogy a helyi LAN hálózatokról kilépést kell biztosítani más hálózatokba is, illetve tudni kell fogadnia más felhasználók csatlakozását, ezért tűzfalakkal ellátott szerverek szükségesek, melyek az illetéktelen belépőket kizárják a hálózati felhasználásból. A vezetési pontok informatikai hálózatának eszközparkján kívül ugyanez a kapcsoló látja el az irodai alkalmazású munkaállomások LAN hálózatban történő üzemeltetését, a videokonferencia szerverek, az analóg és digitális mellékek működőképességének biztosítását.

A gépesített hadtest vezetési pontján ennek egy lehetséges változatát mutatja be az ábra, ahol már a helyi LAN hálózat elemein és a kommunikáció más eszközein kívül megjelenik a hírközpont állomás csatlakozó eleme is, amelyik a vezetési pont hírközpontot illeszti a csomóponti hálózathoz. Ez a hírközpont állomás csatlakozási felületeit tekintve szintén a polgári és NATO szabványok által előírt standard-eken alapul, így lehetőség adódik a rácsrendszer csatlakoztatására civil távközlési szolgáltatók, NATO rendszerek és más NATO tagország harcászati szintű rendszereihez éppúgy, mint a stacioner területi hálózat elemeihez.

A tábori alaphírhálózat korszerűsítése során további cél lehet a híradó állomások típusszámának csökkentése, ami azt eredményezi, hogy megszűnik a vezetési pont hírközpontok nagy mérete, az ott található híradó állomások nagy száma, és helyüket korszerű, digitális eszközöket tartalmazó típusgépjárművek váltják fel. Ezeket a híradó állomásokat – *jó kialakítás esetén*- fel lehet használni csomóponti hírközpontok, vezetési pont hírközpontok és esetenként stacioner telepítésű területi hálózat elemeiként a kommunikációs rendszer kialakítására, így homogén, néhány híradó típusállomásból álló rendszer jön létre, ahol csak a hordozó járművek jellege és a digitális kapcsoló központok konfigurációja kell, hogy változzon a csapatok alkalmazásának, a résztvevő felhasználók számának megfelelően. Így a csomóponti- és a vezetési pont hírközpontok típusállomásaiból egyenszilárd kommunikációs rendszer építhető fel.

[42] a helyi hálózatok központi kiszolgáló egysége

Dr. Koczka Ferenc

AZ ALAPFOKÚ HÍRADÓTISZT-KÉPZÉS ELEMZÉSE, JAVASLATOK A FEJLESZTÉS FŐ IRÁNYAIRA

Bevezetés

A **hírközlés** az utóbbi évtizedben soha nem tapasztalt ütemben fejlődött és ez nem csak a szektor működését szabályozó jogi környezet, a működtetésért felelős szervezetek átalakítását kényszerítette ki, hanem intenzív fejlődést generált a hírközlési szektor munkarőpiacára beszállítóként dolgozó közép- és felsőfokú oktatási intézmények képzésében is.

A XXI. század elején a hírközlés jelentős kihívása a liberalizáció, a konvergencia és a globalizáció. E három jelenség várhatóan soha nem látott, forradalmi változást fog előidézni az emberiség történetében, aminek következményei ma még fel sem becsülhetők. A hírközlés és ezen belül különösen a **távközlés** területén végbemenő és prognosztizálható fejlődés, a szolgáltatások és technológiák integrációja, az informatika, a távközlés egyre szorosabb összekapcsolódása egyértelművé teszi, hogy a hírközlési infrastruktúra nemzetgazdasági és társadalmi jelentősége egyre meghatározóbb lesz a jövőben. Az ezredforduló utáni társadalom fejlődése már elsősorban a hírközlésre és a vele szoros kapcsolatban lévő informatikára épül.

A Kormány a nemzeti **hírközléspolitikai** célok megfogalmazásánál különös figyelmet szentelt azoknak a folyamatoknak, amelyek elősegítik az ország nemzetbiztonsági és NATO tagságunkkal is összefüggő védelmi igényeinek érvényesítését [1]. Ennek értelmében középtávon növelni kell a közcélú hálózatok honvédelmi érdekből történő hozzáférhetőségét, melynek megvalósítása több szempontból is előnyös hatást gyakorolhat a Magyar Honvédség távközlési infrastruktúrájára.

A hírközléspolitikai célokkal összhangban a MEH Informatikai Kormánybiztossága kidolgozta a **nemzeti információs társadalom stratégiáját** [2], melyen belül az Oktatási Program céljainak megvalósítása a katonai felsőoktatás részére is feladatokat határoz meg. A folytonosan változó információs gazdaságban a munka világa is átalakul. Az infokommunikációs eszközök rohamos fejlődése, használatuk gyors elterjedése tartalmában és eszközrendszerében is új kihívások elé állítja a modern kor emberét. Alapkövetelmény lesz az „élethosszig tartó tanulás”. A felsőoktatási intézményeknek változtatni kell oktatási filozófiájukon. A **hallgatóközpontú oktatás** során az „élethosszig tartó tanulás”-t kell modellezni (Főtantárgy az élet.), azaz már a képzés során olyan oktatási-tanulási metodikát kell kialakítani, hogy a hallgató a végzést követően – megszerzett tudására alapozva - önállóan szervezze saját továbbképzését, tudásának piacképes szinten tartását.

Az MH szempontjából a **katonai felsőoktatás stratégiai ágazat.** A fiatal tiszti réteg meghatározó a Magyar Honvédség és a Határőrség állományában az információs társadalomra történő felkészülés, az új haditechnikai eszközök és rendszerek fogadása terén [3]. A csapatoknál szolgálatot teljesítő állomány a frissen végzett mérnöktisztektől várja azon új munkamódszerek meghonosítását, melyek az infokommunikációs eszközök és rendszerek szolgáltatásainak magas színvonalú igénybevételén alapulnak. Nem utolsósorban a fiatal mérnöktisztektől várják a segítséget egy-egy konkrét alkalmazás megismeréséhez, a rendszerben bekövetkezett hiba behatárolásához és elhárításához. Így személyükön keresztül a honvédelmi vezetés katalizálhatja az új infokommunikációs eszközök és rendszerek alkalmazását, szolgáltatásaik mind teljesebb igénybevételét.

A Magyar Honvédség hosszú távú átalakításának irányairól szóló OGY határozatnak [4] megfelelően a Zrínyi Miklós Nemzetvédelmi Egyetemnek végre kellett hajtania a szervezeti átalakítást, mely a főiskolai karon - a létszámcsökkentéssel egyidejűleg – az öt szakirányú képzést folytató villamosmérnöki tanszék, két tanszékbe történő összevonását eredményezte. Így jött létre a Katonai Távközlési és Telematikai Tanszék a korábbi Elektronikai-harc, Híradó és a Rádióelektronikai felderítő Tanszékek bázisán.

A teljesség igénye nélkül arra vállalkozom, hogy a kialakult új helyzetben elvégezzem az alapfokú híradótiszt-képzés belső elemzését, környezetének vizsgálatát és ezek alapján javaslatokat fogalmazzak meg a fejlesztés lehetséges irányaira, lehetőséget adva munkatársaimnak, megrendelőinknek segítő szándékú javaslataik megtételére.

1. Az alapfokú híradótiszt-képzés belső elemzése, környezetének vizsgálata a SWOT módszer alkalmazásával.

A fejlesztési irányok, lehetőségek (a fejlesztés stratégiájának) meghatározása előtt célszerű önvizsgálatot végezni, elemezni a szervezet környezetét. A vizsgálat módszeréül egyszerűsége miatt a SWOT analízist[1] választottam, melyet az alábbi főbb témakörökre fókuszáltam:

- képzési kínálat,
- a képzés szervezete,
- humán erőforrások,
- képzési infrastruktúra.

1.1. Képzési kínálat

Helyzetleírás:

Alaprendeltetésünk a híradótiszti hallgatók főiskolai szintű képzése alap nappali (AN) és alap levelező (AL) képzési formákban. Végzett hallgatóink a tiszti kinevezési okmány mellett, híradó (távközlési) szakirányú villamosmérnöki oklevelet vehetnek át. Tanszékünk biztosítja az MH Híradó Szolgálata

tiszti utánpótlásának meghatározó hányadát, de rendszeresen helyezünk beosztásba végzett híradótiszteket az MH Elektronikai Szolgálat és a Határőrség Távközlési és Informatikai Főosztály alárendelt szervezeteihez is.

A Katonai Távközlési és Telematikai Tanszék Híradó Szakcsoportja **alaprendeltetéséből adódó feladatai mellett** végzi:

- a más szakokon tanulmányokat folytató hallgatók híradó szakirányú képzését,
- tartalékos híradótisztek képzését (a szakirányú polgári egyetemet és főiskolát végzettek számára),
- híradótisztek, tiszthelyettesek és közalkalmazottak szakmai továbbképzését, 1 hét – 2 hónap időtartamban. Azonosultunk a megrendelő - HVK Vezetési Csoportfőnökség, MH Elektronikai Szolgálatfőnökség - az irányú elvárásával, hogy tanszékünk vegyen részt a rendszerbe állításra tervezett és rendszerbe állított híradó eszközök üzemeltetésére és üzemben tartására történő felkészítésben, működjön egyfajta **szakmai továbbképző központ**ként is. Ez a feladat az utóbbi években egyre hangsúlyosabb.

SWOT

Erősségek: *a képzési kínálat összhangja a megrendelő elvárásaival.*

Gyengeségek: *a képzési kínálat további bővítését korlátozza az oktatói órakapacitás (létszám).*

*A **SWOT analízis**[1]* az 1960-as években a Harvard Business School-ról indult stratégiaalkotást segítő vizsgálati módszer. Feltérképezi, hogy a ***szervezeten belül*** mi jelent biztos alapot (erősségek = Strengths), mik szorulnak javításra (gyengeségek = Weaknesses); a ***szervezeten kívül*** melyek a lehetőségek, kihívások (Opportunities), és milyen veszélyek (Threats) fenyegetik a fejlődést, az optimális működést. A ~ célja, hogy biztosítsa a szervezet környezetéhez viszonyított helyzetének pontos definiálását, illetve elősegítse a célok eléréséhez vezető akciók (feladatok) meghatározását.

Kihívások:

- *a megrendelő – összhangban az új híradó eszközök Magyar Honvédségben történő rendszeresítésének ütemével – elvárja, hogy a tanszék szakmai továbbképző központként funkcionáljon,*
- *megkezdődnek a tiszti és a tiszthelyettesi életpálya modellhez kapcsolódó tanfolyamok (A tanfolyamok mérnök-műszaki részének végrehajtása,.*
- *bevezetésre kerül a távoktatási képzési forma (nemzetőr képzés, távközlési szakmérnök-képzés).*

Fenyegetettségek:

- *kielégítetlen megrendelői igények,*
- *támogatási források elapadása,*

- *a tanszék (a szakcsoportok) jelenlegi szakmai színvonalának és presztízsének csökkenése.*

1.2. A képzés szervezete

Helyzetleírás:

A Nemzetvédelmi Egyetemen ez évben végrehajtott 34 %-os létszámleépítéssel egyidejűleg a Főiskolai Karon az Elektronikai-harc, a Híradó és a Rádióelektronikai felderítő Tanszékek összevonásra kerültek a **Katonai Távközlési és Telematikai Tanszék** szervezetébe, illetve a Légvédelmi rakéta és tűzér, valamint a Lokátortechnikai Tanszékek, a Katonai Folyamatszabályozási és Mikrohullámú Tanszék szervezetébe. Az átszervezés sok feszültséggel járt. Az eredetileg több tanszék összevonását megcélzó javaslatból más tanszékeknek sikerült "kifarolni", így az a furcsa helyzet állt elő, hogy a karon az AN és AL képzési fomákban résztvevő tiszti hallgatói tancsoportok 47 %-át (2000/2001 tanév) ez a két összevont tanszék képezte.

Ebből a hátrányos, több szakirány számára presztízsveszteséget okozó helyzetből "jól" kijönni nehéz, majdnem lehetetlen. A tanszék irányítási rendje a következő oldalon látható ábra szerint alakult.

SWOT

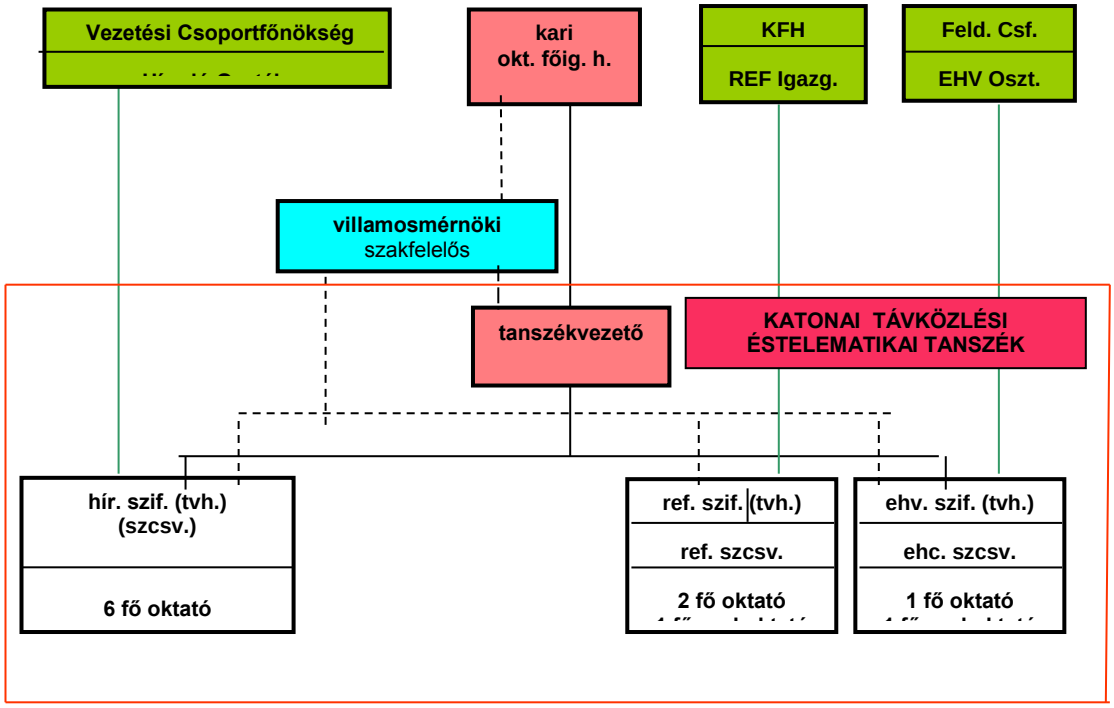
Erősségek:

- *a megnövekedett létszámú (20 fős) oktatási szervezeti egység, optimális (100 % körüli) leterheltség esetén lehetővé teszi – a tanszék szakmai kompetenciájába tartozó – nagyobb képzési feladatok önálló megoldását, egyes tantárgyak tananyagának több oktatóval történő lefedését,*
- *az egyes szakirányokon lökésszerűen jelentkező képzési igényeket a nagyobb szervezet rugalmasabban tudja kielégíteni,*
- *a nagyobb oktatói létszám – az oktatás megzavarása nélkül – lehetővé teszi 1-1 fő intenzív tanfolyami, vagy tudományos képzését, mely elősegíti az oktatók minőségének javítását.*

Gyengeségek:

- *nagy tanszéki óraadói leterheltség (2001/2002 tanévben 140 %)akadályozza a szakirányok közös képzési tevékenységi területének kialakítását, anulálja az erősségek érvényesítését,*
- *az oktatói állomány egy részének ellenállása nem ösztönzi az együttműködést.*

A KTTT organogramja



Kihívások:

- *mindhárom szakirányon közös tananyag oktatása,*
- *a meglévő korszerű képzési infrastruktúra (informatikai hálózatok szaktanterem, digitális kapcsolástechnikai szaktanterem) kihasználása,*
- *pályázatokon történő közös indulás, mely az elbírálás során előnyösebb helyzetbe hozhat bennünket és a pályázati beruházások megvalósítása során a terhelés jobban megosztható,*
- *a villamosmérnöki levelező képzés közbülső akkreditációs eljárása a 2003/2004 tanévben.*

Fenyegetettségek:

- *helytelen szervezeti működés esetén a tanszék nem tud adekvát módon reagálni a képzési igényekre, megrendelésekre, a szükségesnél nagyobb ellátatlan képzési területek alakulnak ki,*
- *a három szakirány (hír., ref., ehv.) együttműködő szakmai főnöksége ragaszkodik a specializáció jelenlegi mértékéhez, óraszámaihoz.*

1.3. Humán erőforrások

A humán erőforrások tárgyalásánál külön kell választani a képzési folyamat - mint bipoláris tevékenység - két oldalán elhelyezkedő főiskolai oktatók és a hallgatók vizsgálatát.

1.3.1. Tanszéki oktatók

Helyzetleírás:

A tanszék oktatói létszáma 14 fő, ebből 4 fő dr.univ., 3 fő levelező doktorandusz hallgató, 2 fő tervezi - a megalakuló ZMNE Katonai Műszaki Doktori Iskoláján - a tudományos fokozat megszerzését. Magas óratartási kötelezettségeik eddig nem tették lehetővé doktori képzésben történő részvételüket.

A tanszék oktatói állománya innovatív, amit az utóbbi két évben – a pályázati támogatások felhasználásával is – megvalósított, mintegy 35 MFt-os képzési infrastruktúra beszerzés, beépítés menedzselése is bizonyít. A tanszék képzett, gyakorlat-orientált felkészültségű oktatókat alkalmaz, akik katonai-szakmai tudásukon túl jártasak a képzési folyamatok szervezésében, az informatikai eszközök oktatásban és mérnöki szakterületen történő hatékony alkalmazásában. Kétharmaduk többdiplomás, piacképes diplomakombinációkkal. Az állomány fele két közép- vagy felsőfokú nyelvvizsgával rendelkezik, ám ez csak 1-2 fő esetében párosul aktiv verbális nyelvtudással. Pályán maradásuk életkorukkal, elhivatottságukkal, a tanszéken kialakult jó munkahelyi légkörrel magyarázható.

SWOT

Erősségek:

- *felkészült, tapasztalt, aktív, innovatív oktatói állomány,*
- *intenzív törekvés a tudományos fokozat megszerzésére.*

Gyengeségek:

- *rossz a korösszetétel, kevés a fiatal oktató,*
- *nincs a tanszéken tudományos fokozattal rendelkező oktató,*
- *alacsony szintű idegen nyelvű szóbeli kommunikációs készség.*

Kihívások:

- *a hírközlés (távközlés, katonai híradás) gyorsan változó ismereteivel,*
- *a villamosmérnöki szak akkreditációs követelményeknek történő megfeleltetése (tudományos fokozat megszerzésével is hozzájárulni),*
- *a „hallgató központú” képzés eszköz, tananyag és oktató módszertani feltételeinek biztosítása.*

Fenyegetettségek:

- a jelenlegi munkaköri jegyzék nem biztosítja a minőségi oktatói utánpótlás kinevelését,
- *oktatók elöregedése,*
- *kontaktusok hiánya a NATO tagországokkal.*

1.3.2. Híradótiszti hallgatók

Helyzetleírás:

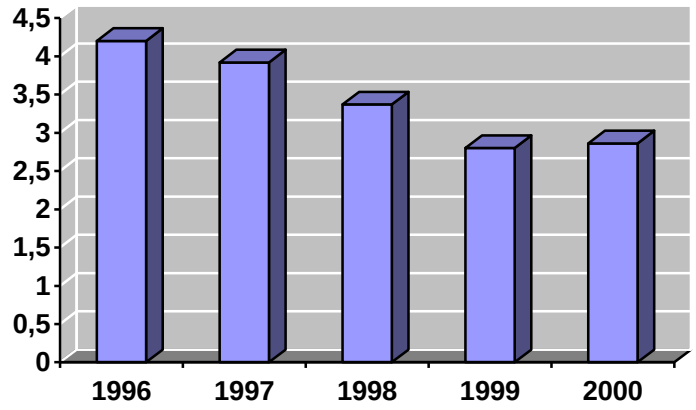
A főiskolai kar a megrendelői (katonai) elvárásokra rugalmasan reagáló, a műszaki felsőoktatás követelményeinek folyamatosan megfelelő intézmény, amely a katonai (tiszti) felkészítés mellett főiskolai szintű **mérnökképzés**t folytat. A főiskolai kar jellegéből fakad, hogy a képzésben a tanítás és tanulás harmonikus egysége mellett **meghatározó a katonai vezetőt jellemző magatartásformák** kialakítása.

A híradótiszt végzi a MH híradásának (távközlő és informatikai hálózatainak) és FRISZ biztosításának tervezését, szervezését, a végrehajtás irányítását. Szakmai tevékenysége során kapcsolatba kerül távközlési szolgáltatókkal és azok hálózataival, valamint a NATO híradó és informatikai szervezeteivel és rendszereivel. Ahhoz, hogy ebben a közegben operatív munkát végezhessen rendelkeznie kell:

– híradó (távközlési) szakirányú villamosmérnöki tudással,
– tárgyalóképes angol nyelvismerettel,
– általános és szakinformatikai ismeretekkel, jártasságokkal.

Tehát a katonai (tiszti) felkészítés és híradó (távközlési) szakirányú villamosmérnöki végzettség magas követelményeket támasztanak a főiskolai képzésre jelentkezőkkel szemben. Ugyanakkor a hivatásos tiszti pálya presztízse, vonzereje, anyagi megbecsülése az utóbbi években csökkent és ez megmutatkozik a beiskolázott híradó hallgatók minőségében is, ahogy azt az alábbi táblázat is mutatja.

A felvételt nyert híradó hallgatók matematika (és fizika) érettségi átlaga

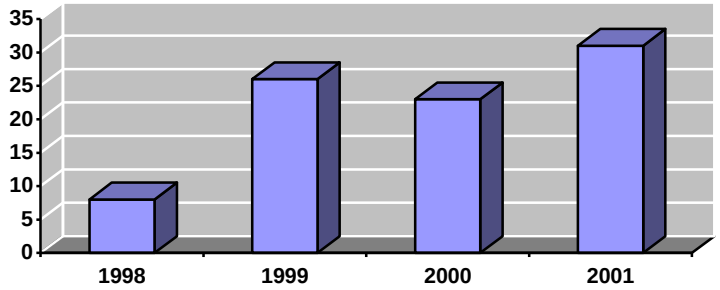


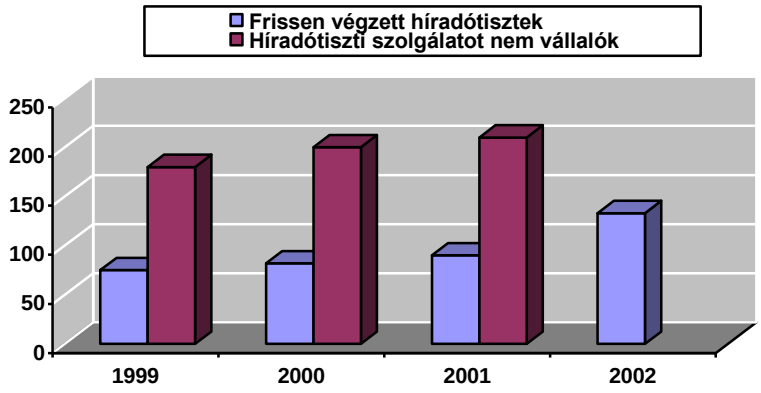
De ugyanezen probléma mutatkozik:

- a merítési bázis csökkenésében, mely oda vezetett, hogy 2001 évben már nem tudtuk teljesen feltölteni a híradó hallgatói keretlétszámot, illetve

- növekszik a záróvizsga után hivatásos tiszti szolgálatot nem vállaló híradó hallgatók aránya. Sajnálatosan pozitív visszaigazolása mindez „termékeink” – a végzett hallgatók –piacképességéről. Nem a legjobbak mennek el az első körben, hanem a specialisták, akikre nagy szükség lenne a híradó rendszer üzemeltetésében (Több meghatározó híradó szervezet híradótiszti feltöltöttsége 40-60 % között mozog). De ugyanezen elvándorlásnak vagyunk tanúi a Honvédségen belül is, amikor egy-egy tehetséges mérnök bajtársunkat csupán nyelvismerete okán alapképzettségétől eltérő – mérnöki tudást nem igénylő – beosztásokban foglalkoztatják.

Hivatásos tiszti szolgálatot nem vállaló végzett híradó hallgatók százalékos aránya





Havi bruttó fizetések összehasonlítása

Ezek a negatív tendenciák, részben vagy egészben jellemzőek más szakokon és szakirányokon is. Három évvel tisztté avatásuk után a mérnök informatikusok 10, a villamos-mérnökök 40, a gépészmérnökök 60 %-a található meg a Magyar Honvédség állományában.

SWOT

Erősségek:

- *jó minőségű képzés (oktatók, általános és képzési infrastruktúra, intézményi szolgáltatások).*

Gyengeségek:

- *csökkenő merítési bázis és tanulmányi felkészültség (érettségi átlag).*

Kihívások:

- *új szolgálati törvény,*
- *tiszti pálya presztízsének emelkedése.*

Fenyegetettségek:

- *a magyar munkaerő piac elszívó hatása,*
- *veszélybe kerül a híradótiszti utánpótlás, állandósul az alegységparancsnoki tiszti hiány, túlterheltség miatti fokozott pályaelhagyás a fiatal tisztek körében.*

1.4. Képzési infrastruktúra

Helyzetleírás:

A tanszék oktatói kihasználva a megrendelői támogatásokat és a távközlési szakirányú képzést segítő pályázati lehetőségeket az utóbbi években jelentősen korszerűsítették a **képzést támogató infrastruktúrát.** Ennek eredményeként valósult meg:

- a 46 munkahelyes tanszéki LAN,
- a hallgatói Internet kabinet,
- az oktatók és munkatársak 100 % feletti ellátása asztali számítógépekkel (laptopokkal),
- a digitális átviteltechnikai szaktanterem (multimédiás tanári munkahellyel),
- a Siemens HICOM 300 E kapcsolástechnikai rendszer szaktanterem (multimédiás tanári munkahellyel).

A képzésünket **támogató gazdasági szervezetek** elsősorban a távközlési piac azon szereplői köréből kerülnek ki, akik üzleti lehetőséget látnak az MH távközlési és informatikai rendszereinek korszerűsítésében. Ezek a Siemens Telefongyár Kft., TOTALTEL Távközléstechnikai Kft., Matáv Rt., Rohde&Schwarz. A képzés iránytartásához szükséges legkorszerűbb katonai és polgári távközlési technológiákat, eszközöket tőlük szerezzük be. Külön ki kell emelnem a HVK Vezetési Csoportfőnökség, valamint a MEH Informatikai Kormánybiztosság nagyvonalú támogatását távközlési és informatikai fejlesztéseinkhez. Ezen kapcsolatainknak tudható be, hogy a szakterületünkön lépést tudtunk tartani a korszerű beszéd- és adatkommunikációs technológiákkal.

A tanszék a megrendelői igények kielégítése, a korszerű infokommunikációs technológiák oktatása érdekében elébe kíván menni a felhasználói igényeknek úgy a főiskolai képzésben, mint az eszközorientált szaktanfolyamok végrehajtásában. Ennek megfelelően 2003-ig az alábbi fejlesztéseket tervezzük:

- ***Informatikai hálózatok szaktanterem***, mely alkalmas a tábori informatikai hálózatok leképezésére, modellezésére, üzemeltetési, programozási feladatainak gyakorlására, adatátviteli eszközökhöz történő csatlakoztatások végrehajtására. A szaktanterem átadása 2001. novemberében várható.
  Bekerülési összeg: 13 + 3 MFt (rendelkezésre áll).
  Forrás: pályázat.
- ***Digitális átviteltechnikai és ISDN mérőhelyek*** kialakítása. A mérőhelyek beüzemelése 2001. novemberében tervezett.
  Bekerülési összeg: 12,6 MFt (rendelkezésre áll).
  Forrás: pályázat.
- ***Mikrohullámú szaktanterem***, mely alkalmas az MH mikruhullámú hálózatában üzemelő és a tábori hírrendszerben rendszeresítésre kerülő mikrohullámú lecsatlakozó eszközök működése elméletének oktatására, nagyfrekvenciás és adatátviteli paramétereinek mérésére. A szaktanterem átadása 2002 második felében tervezett.
  Bekerülési összeg: 16 MFt.
  Forrás: 4 MFt Totaltel támogatás eszközben
  12 MFt pályázat.
- ***Harcászati rádiók szaktanterem***, mely alkalmas a Magyar Honvédségben rendszeresítésre kerülő korszerű RH, URH rádiók oktatására úgy a főiskolai, mint a tanfolyami képzésben. A szaktanterem lehetővé teszi rádiófrekvenciás mérések végrehajtását, rádiófrekvenciás csatornák vizsgálatát, rádió berendezések számítógépes tesztelését.
  Bekerülési összeg: 15 MFt. (Az összeg nem tartalmazza a harcászati rádiók árát.)
  Forrás: megrendelői támogatás

Az 1.4. pontban vázolt viszonylagosan kedvező helyzet csak a tantermi beépített híradó és informatikai eszközökre vonatkozik. Jelenleg az egyetem – és így tanszékünk is – összesen csak öt mobil híradó komplexummal rendelkezik papíron és ezekhez sincs hozzárendelve üzemben tartó, kiszolgáló állomány. E tekintetben továbbra is a híradócsapatokra vagyunk utalva.

SWOT
Erősségek:

- *az új híradó és informatikai eszközök rendszerbe állítását – a híradótiszti hallgatók képzése szempontjából – megalapozó tantermi infrastruktúra,*
- *kampusz kedvező földrajzi elhelyezkedése, általános infrastruktúrája, mely alkalmassá teszi országos – MH szintű – képzési feladatok végrehajtására,*
- *a tanszéken szervezett korábbi szakmai tanfolyamok egy főre vetített képzési költsége lényegesen kedvezőbb, mintha azokat polgári szervezeteknél hajtották volna végre.*

Gyengeségek:

- *kevés mobil híradó komplexum,*
- *a mobil eszközöket üzemben tartó, kiszolgáló állomány hiánya.*

Kihívások:

- *gyorsuló ütemű rendszerbe állítások (a képzési háttér, infrastruktúra megteremtése.*

Fenyegetettségek:

- *a képzési infrastruktúra fejlesztés nem tart lépést a fejlesztésekkel,*
- *az infokommunikációs eszközök és különösen a műszerek rendkívül magas beszerzési ára.*

2. Javaslatok az alapfokú híradótiszt-képzés fejlesztésének fő irányaira

A javaslataim a tanszék néhány alapkompetenciáján nyugszanak, melyek garantálják a megrendelői igények megfelelő minőségben történő kielégítését. Ezek:

– a híradótiszt-képzésben megszerzett 50, a mérnöktiszt-képzésben felhalmozott mintegy 30 éves tapasztalat,
– a kvalifikált, innovatív oktatói állomány és
– a beépített képzési infrastruktúra elfogadható korszerűsége.

2.1. Képzési kínálat:

A tanszék képzési kínálatában középtávon hangsúlyosabbá válik a tanfolyami képzés, beindul a távoktatási képzési forma, megjelenhet – más szakokhoz hasonlóan – az akkreditált iskolai rendszerű felsőfokú szakképzés, elsősorban a tiszthelyettesek részére. Az új szolgálati törvény tervezet ismeretében megállapítható, hogy a mérnöktiszti utánpótlást az MH részére (döntő mértékben) továbbra is a Nemzetvédelmi Egyetem (BJKMFK) fogja biztosítani.

A tanszék óraadói kapacitása korlátozott. Új képzési formák indítására, változatlan oktatói létszám esetén csak akkor van lehetőség, ha

– a megrendelők hozzájárulásával növeljük a villamosmérnöki szakon, illetve (a hír., ráf., ehv. szakirányokon) közös óraszámot és így óraadói kapacitások szabadíthatók fel,
– a tanszék felvállalja a külső óraadók bevonásával járó minőségi kockázatot, a szervezési feladatokat, a kar pedig az ezzel járó többletkiadásokat.

2.2. A képzés szervezete

A villamosmérnöki tanszékek számának csökkentését, az új szervezetek működését - az egy éves tevékenység tapasztalatainak figyelembevételével - 2002 júniusában kell elemezni és javaslatot tenni szervezeti korrekcióra, vagy az eredeti helyzet visszaállítására. Az összevonás előnyeit - a jelenlegi óraleterheltségek mellett - nem, vagy csak nagyon korlátozottan lehet érvényesíteni. Kérdés, hogy ilyen módon érdemes-e fenntartani az összevont tanszékeket, célszerű-e, hogy az alap nappali és levelező tiszti hallgatói tancsoportok 47%-át e két összevont tanszék képezze? A kérdés megfogalmazásában benne van a szerző véleménye.

2.3. Humán erőforrások

A tanszék **oktatói állományából** öt fő szakmai teljesítménye reális esélyt ad a tudományos fokozat 2-3 éven belüli megszerzésére. Ezeket az erőfeszítéseket a munkáltatónak is támogatni kell. Új oktatói pályázatok elbírálásánál egyik kiemelt szempont legyen a magas szintű informatikai ismeretekkel és jártasságokkal bíró, fiatal, angol nyelven jól kommunikáló oktatók beillesztése a tanszéki szervezetbe. Az okleveles villamosmérnöki / katonai egyetemi végzettséggel rendelkező oktatói állományt a 4/3-5/2 arányszámok között kell tartani a képzés jelenlegi óraszám-arányait alapul véve.

A vizsgálat egyik legkritikusabb szegmense a **hallgatói állomány** minősége, mely az utóbbi öt évben süllyedt erre a szintre. A honvédelmi vezetés – többek között - toborzó irodák felállításával, az új szolgálati törvény életbe léptetésével kívánja megoldani a tiszti hivatás presztízsének emelését. Ennek hatása a potenciális jelentkezők körére meglehetősen lassú. A kar, illetve a tanszék feladata, hogy ezen előnyös intézkedésekről szóló információkat közvetlenül juttassa el a címzettekhez (nyílt nap, Innovadidact, látogatás középiskolákba). Azzal tisztába kell lenni, hogy villamosmérnöki szakon a polgári élet továbbra is erőteljes elszívó hatást gyakorol végzettjeinkre. A Magyar Honvédségnek a mérnöktiszti utánpótlást elsősorban a pályán tartás oldaláról kell megoldania.

2.4. Képzési infrastruktúra

A főiskolai szintű képzés gyakorlat-orientált, így a mérnöktiszt-képzés a szakma gyakorlati műveléséhez szükséges tudás, valamint a katonai vezetőt jellemző magatartásformák kialakítását célozza meg. Ennek megfelelően eszközigényes. Azért, hogy a cél megvalósítható legyen - az új rendszeresítésekkel összhangban - az eddigieknél lényegesen nagyobb volumenű megrendelői eszköztámogatás szükséges. Ezek a beruházások gyorsan megtérülnek az át- és továbbképzési költségeknél jelentkező megtakarításokban. Középtávon szeretnénk eljutni oda, hogy a típusmodell eszközök teljes mértékben a híradó és informatikai szolgálatoknál rendszeresített, alkalmazott eszközök közül kerüljenek ki.

Mivel az egyetemen nem látok lehetőséget híradó kiszolgáló alegység működtetésére, egyes gyakorlati, üzemeltetési feladatok végrehajtására – hasonlóan az elektronikai hadviselés, illetve rádióelektronikai felderítő tisztképzéshez – tancsapat igénybevételét kell biztosítani.

A mérőműszerek magas bekerülési költsége (optikai labor ~100 MFt.), valamint az kis hallgatói létszám miatt, célszerűnek látszik néhány laboratóriumi mérést külső gazdasági szervezetektől megvásárolni. Ugyanakkor a villamosmérnöki szakon (8 szakirány) szükséges – nem túl nagy költségvonzatú - alapmérések eszközhátterét biztosítani kell.

A tanszék oktatói az utóbbi tíz évben hatékony pályázati munkával biztosították a képzés szinten tartásához szükséges forrásokat. Ezek továbbra is jól szolgálhatják a képzési infrastruktúra fejlesztését, kiegészítve a volumenében nagyobb megrendelői beruházásokat.

Irodalomjegyzék:

[1] 1071/1998. (V. 22) Korm. határozat a hírközléspolitikáról

[2] Nemzeti információs társadalom stratégiája, MEH Informatikai Kormánybiztosság, 2001

[3] Dr. Koczka Ferenc: Híradótiszt-képzés változó társadalmi, műszaki felsőoktatási és honvédségi környezetben ZMNE, Országos tudományos konferencia, 2000. 10. 14.

[4] 61/2000. (VI. 21.) OGY határozat a Magyar Honvédség hosszú távú átalakításának irányairól

Kassai Károly

AZ INFORMÁCIÓVÉDELEM ÚJSZERŰ MEGKÖZELÍTÉSE

Napjainkban a gyorsan fejlődő technológiának és technikának megfelelően az információs műveleteket egyre korszerűbb rendszerek szolgálják ki. Megkezdődött a rendszerek integrációja, amelyek a különböző forrásokból eredő adatok fúziója révén egyre feldolgozottabb és összetettebb információk elérését teszik lehetővé. Az új módszerek nagymértékben támogatják a különböző műveletek hatásainak mérlegelését, korszerűsítik a döntési folyamatot.

Ez a kedvező folyamat csak akkor ér valamit, ha a hagyományos és elektronikus információk védelmét olyan eszközök és módszerek valósítják meg, amelyek hatékonyan akadályozzák az illetéktelen megismerést, gátolják a rendszerekbe történő behatolást. Az információ biztonság fontosságát a világon rengeteg tényező indokolja, amely az államok biztonsági- és katonai stratégiáiban is fellelhető. Ehhez hasonlóan a Magyar Köztársaság biztonság- és védelempolitikai alapelvei között szerepel:

> „A Magyar Köztársaság a biztonságot átfogó módon értelmezi, amely a hagyományos politikai és katonai tényezőkön túl magában foglalja a széles értelembe vett biztonság egyéb – gazdasági és pénzügyi, emberi jogi és kisebbségi, információs és technológiai, környezeti, valamint nemzetközi jogi – dimenziót is.” [43]

Elmondható, hogy a Magyar Honvédség az információs műveletek területén a fejlődés szakaszába került.

Megkezdődött a zártcélú hálózat kapcsolóelemeinek digitalizálása, a mikrohullámú gerinchálózat kiterjesztése, összekapcsolva a frekvencia migrációval.

Napirenden van a különböző távközlési szolgáltatók által biztosított digitális szolgáltatások között lassan elszigetelődött, elavult tábori hírrendszer felváltása is. A források által megalapozott tervekben már körvonalazódott az LB- és géptávíró vonalak, vivős rendszerek és kézi kapcsolásos központok helyett egy rács szervezésű, korszerű szolgáltatásokat biztosító híradó és informatikai rendszer.

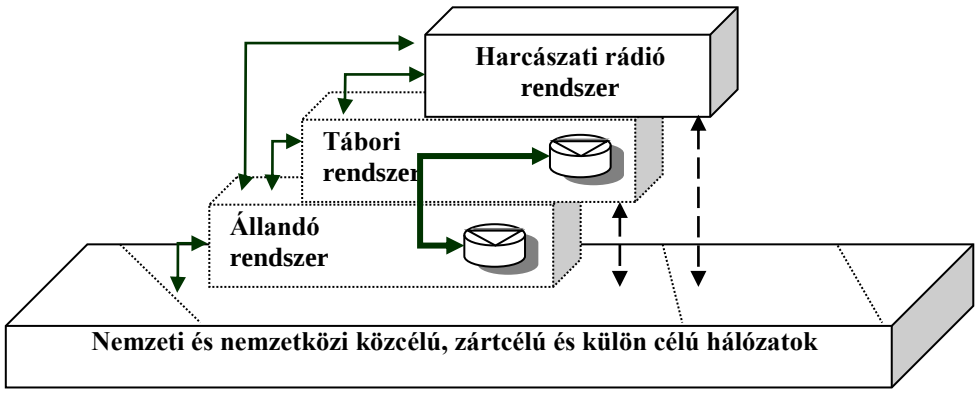
Megszűnik a föld levegő híradás eddigi elkülönülése, és a repülésirányító tornyok, harcálláspontok igényeit is az integrált rendszer fogja kiszolgálni. A régen tapasztalt analóg lokátorok tömegét kiváltó korszerű légtér megjelenítési és irányítási rendszer alapjai már megvannak és megkezdődött a NATO integrált légvédelmi rendszeréhez csatlakozó beruházások tervezése.

[43] 94/1998 (XII. 29) OGY határozat 1. pont.

Korszerű informatikai szolgáltatások kezdenek megjelenni, és a régi számítógép és szoftver hiány helyett lassan gyarapodó eszközparkkal és terebélyesedő hálózatokkal lehet találkozni. Megtörténtek az első lépések a papír alapú irodai szolgáltatások csökkentésére és korszerűsítésére.

A kor színvonalának megfelelő rádiók a harcászati híradó és informatikai rendszer támogatásával a megszokott távbeszélő szolgáltatások mellett kép- és adatátvitel, valamint navigációs feladatokat is lehetővé tesznek terepen, vagy mozgás közben is.

A digitális kapcsolóelemek és átviteli utak, korszerű végberendezések rendszerének felügyeleti és irányítási mechanizmusa is nagyságrendekkel fog változni. Az analóg rendszer rengeteg paraméterét feszített munkatempóban felügyelő és vezérlő, hierarchikusan kialakított híradó vezetési pontok rendjét korszerű és hatékony hálózatvezérlés fogja támogatni.



1. sz. ábra: A Magyar Honvédség tervezett híradó és informatikai rendszere (logikai vázlat)

A korszerű információ átviteli-, feldolgozási-, tárolási- és megjelenítési módszerek mellett a világban megjelentek az információs műveleteket hatásosan támadó eszközök és módszerek is. Különböző technikájú optikai, akusztikus, elektronikus és egyéb módszerekkel egyre szélesebb érzékelési tartományban gyűjthetők az egyének és szervezetek számára nélkülözhetetlen információk. Az információk illetéktelen megszerzése, az információs folyamatok megzavarása, a rendszerekbe megtévesztő információk bejuttatása már a modern hadviselés egyik legfontosabb részévé vált.

Az új kommunikációs lehetőségek megjelenésével párhuzamosan a Magyar Honvédségnek is számtalan olyan veszéllyel kell szembenéznie, amelyek korábban nem, vagy csak kis mértékben fenyegették információs rendszereinket.

Az egyre korszerűbb végberendezések, hálózati szolgálatok és szolgáltatások kiemelik a teljes átviteli úton történő *fizikai védelmet* az állandó és tábori objektumokban egyaránt. A hozzáférés felügyelete és ellenőrzése *a biztonsági*

területek rendjén alapul. A ki és belépések ellenőrzése, a biztonsági területek technikai védelme, a helyiségek határoló felületeinek és nyílászáróinak megerősítése és érzékelőkkel történő felszerelése, a biztonsági tárolók és egyebek már nem a régen megszokott mechanikus elemeken nyugszanak. A biometrikus azonosítási módszerekre épülő beléptető rendszerek, az elektronikus zárak a jogosultság ellenőrzése mellett képesek egy központ felé továbbítani az eseményeket, ami tárolással kiegészítve az elemzés új lehetőségeit teremti meg. Az intelligens irodaház (épület) kialakítás lényege, hogy az érzékelhető, távvezérelhető események (távbeszélő és adatátviteli rendszer, energia, világítás, fűtés, beépített mozgás-, és behatolás érzékelők, kamerák, tűzjelzők stb.) egy rendszer elemeit képezzék, ami a fenntartási feladatok gyorsítása, a gazdaságosság mellett a biztonságra is jótékony hatással van.

Mivel a korszerű érzékelők lehetővé teszik az elektromos jelenségek kisebb-nagyobb távolságról történő észlelését és rögzítését, szükség van a végberendezések, kapcsolóelemek kompromittáló kisugárzásának kézbentartására is. A kommunikációs eszközök aktív és passzív védelmi elemekkel történő felszerelése, a helyiségek árnyékolása, a másodlagos sugárzási lehetőségek csillapítása mind olyan megoldások, amelyek a helyi sajátosságoknak megfelelő biztonsági távolságok kialakításával hatékonyan gátolhatják a passzív módszerrel történő jogosulatlan információgyűjtést.

Mivel az információk feldolgozása és felhasználása nem csak helyben történik, így a védelmi eszközök mellé természetesen felsorakozik a *rejtjelzés* is, mint a tárolás és továbbítás egyik fontos védelmi eszköze.

Fontos tudni, hogy a rejtjelzés ereje nem egyedül a misztikus algoritmus, hanem még a rejtjelzési tevékenység általános védelmi rendszerének erőssége és a kulcsrendszer védelmének együttese. A csúcstechnika megjelent a rejtjelzés területén is, így nem véletlen, hogy egyre komolyabb támadási módszerek fejlődnek, amelyek az átviteli utak rejtjelzés előtti, vagy visszaalakítás utáni nyílt információ ellen irányulnak.

A rejtjelzett kapcsolatokat is többfajta támadás érheti, ami ellen további lépések szükségesek. Az *átviteli utak védelme* olyan hálózati szintű védelmet jelent, amely az alkalmazott protokoll belső lehetőségeit használja fel védelemre. Így könnyebben megvalósítható az azonosítás, a feladó és a továbbított adatok hitelesítése, lehetetlenné téve a továbbított információk visszajátszását, az illetéktelen beékelődést a kommunikációs felek közé. Ezt kiegészítve csoportos rejtjelző megoldásokkal megtörténik a hálózat csomópontjai közötti átviteli utak összefogott védelme, az előbbieken túlmenően akadályozva a különböző típusú forgalomanalízist. A vezeték nélküli átvitel útjait új, zavarás ellen védett, nehezen felderíthető üzemmódok védik.

Az eddigi védelmi mechanizmusokat további belső elemek egészíti ki. A hálózati hozzáférés, a távoli adatbázisok-, vagy alkalmazások elérése csak megfelelő logikai azonosítások alkalmazásával lehet biztonságos. Ez a követ-

kező védelmi lépcső a helyiségbe bejutók számára jelenti azt a válaszfalat, amely a „need to know” elv alkalmazásával eldönti, hogy az igényelt művelet elvégzése a személyi felhatalmazás keretein belüli-e.

A végberendezések *hardver* és *szoftver* védelme segít megvalósítani, hogy a biztonsági elemek ne legyenek kikerülhetők, a berendezések használata csak a meghatározott keretek között történjen. A különböző hardverkulcsok, az ellenőrzött egységek és alkatrészek alkalmazása biztosítja, hogy a rendszeresített berendezés valóban csak azokat a hardver elemeket tartalmazza, amelyek a rendszer kialakítójának szándékában voltak. A karbantartási és fenntartási műveletek kézbentartásának célja, hogy ezek során se változzanak a biztonsági elemek.

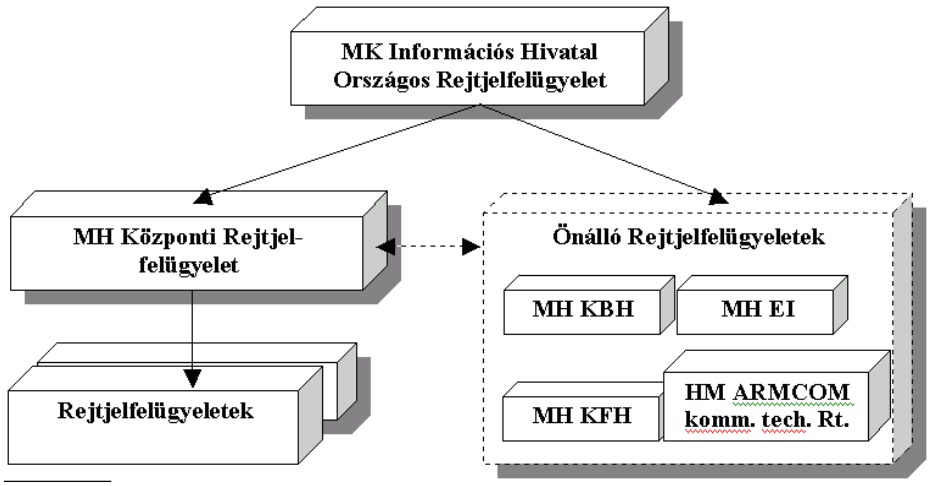
A szoftver védelem feladata, hogy szabályos installálás során, csak ellenőrzött programok kerülhessenek az alkalmazott berendezésekre, a működést védelmi szempontú memória rezidens programok felügyeljék, a vírusok és rosszindulatú programok ellen hatásos védelem legyen kialakítva, és a végzett műveletek naplózottak legyenek, a fontos adatok időszakos mentése megtörténjen.

A bonyolult védelmi megoldásokat néha megdöbbentően egyszerű megoldásokkal ki lehet cselezni. A hétfői kora reggel csendjét feldúló síró női hang a telefonban (például: „elromlott a Főnök gépe, mert a beütött jelszóra mindig az írja ki, hogy „érvénytelen jelszó” és nem tudom kinyomtatni számára a nyolckor kezdődő értekezletre a prezentációját!”) már több rendszerfelelős nyugalmát – és az informatikai biztonság rendjét – dúlta fel. A hasonló esetek szabályos megoldása elég sok konfliktust hordoz, de megfelelő képzéssel és türelemmel ezek a szituációk is feloldhatók.

Az említett néhány védelmi megoldás is mutatja, hogy a végberendezése és egyéb eszközök esetében gyakran nehéz a híradó-, informatikai (vagy egyéb) biztonság *elkülönítése* és önálló megjelenítése.

Manapság már harctéri körülmények között is lehetőség válik adatátvitelre, a grafikus megjelenítésre, a meghatározott szempontok szerint lekért információk letöltésére, képátvitelre is egyebekre. A korszerű rádióhoz kapcsolt számítógép (vagy speciálisan kialakított eszköz) esetében a veszélyeztetések sokasága miatt csak a *komplex biztonsági szempontok* képesek vezérelni az információ hatékony védelmét.

A dokumentum-, és az elektronikus információvédelem a szervezeti integrációt megelőzően 2000 őszétől a Honvédelmi Minisztériumnál, majd egy évvel későbbtől a Honvéd Vezérkarnál is közös szervezeti keretek között működik. A honvédség rejtjelző szervezetei még széttagoltak, ami mutatja a jövőben várható változások egyik feladatát.



2. sz. ábra: A Magyar Honvédség rejtjelfelügyeleti rendje[44]

A legnagyobb kihívást természetesen a Magyar Honvédség zártcélú hálózatának biztonsági feladatai adják.

Ennek egy érdekes területe a rendelkezésre álló védelmi rendszer karbantartása és az aktív és passzív védelmi műveletek vezérlése mellett az azonosított támadók ellen a megfelelő bizonyítékok biztosítása lesz. A valódi visszatartó erő egy információk elleni támadás ellen az, ha a megfelelő törvényi alapok rendelkezésre állnak és az események bizonyítottsága esetén megtörténik a cselekmény súlyával arányos felelősségre vonás. Így nem csak az a feladat, hogy passzívan védekezzünk, hanem e mellett a támadásra és károkozásra vonatkozó hiteles bizonyítékokat legyünk képesek felmutatni, amelyek bármelyik hazai és külföldi bíróságon bizonyító érvénnyel megállják helyüket.[45]

Ez a néhány gondolat is megmutatta, hogy információkat veszélyeztető fenyegetések hatásainak növekedése, bonyolultsága, a támadások érzékelési nehézségei, az információs műveletek felgyorsult tempója egyaránt megkövetelik az *összetett védelmi módszerek* alkalmazását. Elmondható, hogy a hagyományosan, vagy elektronikusan tárolt, feldolgozott, továbbított és megjelenített információk védelmét a korszerű támadó eszközök és módszerek technológiai színvonalára kell emelni. Ehhez szükség van az analóg híradó rendszerhez és hagyományos információs műveletekhez igazított módszerek és szervezetek átalakítására, az eddig elkülönült védelmi alrendszerek összefogására. Mivel már nem csak a nemzeti, hanem a ránk bízott NATO minősített anyagok biztonságát kell szavatolnunk, így logikus feladat, hogy a két alrendszert ne elkülönítve, hanem közös erőforrásokra támaszkodva kezeljük.

[44] 43/1994. (III. 29.) Kr. 4. és 6. §.
[45] Papp György: Doktori (PhD) értekezés p. 61.

Az elmondottak jól érzékeltetik, hogy a Magyar Honvédség információvédelmi feladatrendszerének működése számos nemzetbiztonsági-, jogszabályi-, iparbiztonsági-, gazdaságpolitikai tényező függvénye, nemzetközi megállapodás és egyeztetés eredménye, így fontosnak kell tekinteni az egyeztetési-, együttműködési feladatokat is.

Felhasznált irodalom

1) Papp György: Számítógép-hálózatok kommunikáció rendszerében történő illegális beavatkozás detektálása és nyilvántartása, doktori (PhD) értekezés, 1995, ZMNE
2) 43/1994. (III. 29.) Kormányrendelet a rejtjeltevékenységről
3) 94/1998 (XII. 29) OGY határozat a Magyar Köztársaság biztonság- és védelempolitikájának alapelveiről

Ökrös Tiborné

KONVERGÁLÓ MOBIL RENDSZEREK

Bevezetés

Európában az elmúlt két évtizedben a mobil távközlő rendszerek különféle kategóriáit és generációit fejlesztették ki. Megjelentek a cellás, a zsinórnélküli, a nyalábolt rádió, valamint a személyhívó rendszerek első és második generációs (1G, 2G) változatai, a harmadik generációs (3G) mobil rendszerek bevezetése pedig most van folyamatban. Napjainkban már a negyedik generációs (4G) fejlesztési tervek is körvonalazódtak. A mobil távközlésfejlődést a kategória határok fokozatos eltűnése és a fix-mobil konvergencia (FMC) koncepción alapuló fix-mobil integráció (FMI) jellemzi.

Ma a mobil technológiák fejlődése a 3G/4G rendszerek kialakulása felé mutat, melyet a 2G és a 2,5G megoldások alapoznak meg. A 3G UMTS kialakulásában kulcs szerepet játszanak a 2G/2,5G pre-UMTS rendszerek, a GSM és a TETRA. Ha pontosabban jelezni akarjuk a fejlődési fokozatokat is, akkor felsorolhatók a GSM mögött a HSCSD, a GPRS és az EDGE, a TETRA mögött pedig a TETRA (1) és a TETRA 2 fázisok. A fejlődéssel természetesen az UMTS koncepciója és megjelenési formája is állandóan változik, figyelembe véve a teljes fix-mobil konvergencia jelenséget, a fix és a mobil területek egymásra ható ill. egymás felé tartó fejlődését. A GSM és a TETRA azonos súlyú robusztus rendszerek, az előbbi homogén összetételű nyilvános előfizetői, az utóbbi inhomogén zárt- és különcélú felhasználói kör kiszolgálására optimalizált rendszer. Műszaki értelemben véve a TETRA a GSM rendszerhez viszonyítva egy nagyságrenddel bonyolultabb felépítésű, amely az eltérő rendeltetéseknek tudható be.

Az FMC folyamata és az UMTS kialakulása összefügg. A fix-mobil fejlesztések konvergens módon mennek végbe, melynek eredményei az UMTS különböző fázisú megjelenésével válnak mind inkább kézzelfoghatóvá. Az UMTS egy moduláris koncepció, amely teljes mértékben figyelembe veszi a meglévő és a jövő információs technológiák, rendszerek, hálózatok, eszközök és szolgáltatások konvergenciájának trendjét és az ilyen konvergenciából leszármaztatható lehetséges szinergiákat. A távközlés, az információs technológia (IT), valamint a média fejlesztésekkel összefüggésben - melyek összekapcsolódva közösen teremtik meg az információs társadalmat - az UMTS, mint globális mobil multimédia rendszer jön létre.

A mobil fejlődés nagy utat tett ill. tesz meg addig, amíg a szélessávú információátvitelt biztosító UMTS teljes mértékben rendelkezésre áll (10 év). A mobil hálózatokban ma a beszéd, a jövőben (2005) már az adatforgalom do-

minál. A mobil világban eddig a beszédközpontú környezet volt jellemző, míg a jövőben a 3G egy mindig elérhető (always-on) adatkörnyezetet valósít meg. 2010-ig várható a mobil multimédia szolgáltatások széleskörű megjelenése.

A 3G szolgáltatásokra 2004-re alakulnak ki a lényegesebb piacok (Finland, UK, Germany stb.). Az igazi nagy 3G piaci növekedés csak 2010 után várható, ekkorra a fejlődő országok is felzárkóznak nemzeti létesítéseikkel a fejlett világhoz.

A következő évtizedben még a 2, 5G – és nem a 3G – technológia dominál a vezetéknélküli adatpiacon (2010-ben globálisan kb. 1,3 – 1,5 Mrd vezetéknélküli adatfelhasználó közül még csak 24 % fog hozzáférni a 3G-hez). A valóság az, hogy a 3G hálózatok ekkor még nem szállítanak interaktív multimédiaszolgáltatásokat, de nem is lesz rá még kellő igény.

A fix-mobil konvergencia közelebbről

A fix-mobil konvergencia alapvető tulajdonságait az alábbiak szerint lehet megfogalmazni.

- *Az FMC fogalma:* A technológia és a szoftver felhasználható ill. hasznosítható alkalmazásokba történő transzparens integrációja.
- *Az FMC értelmezése:* A konvergencia nem szükségszerűen a hálózatban, hanem a felhasználói ponton történik.
- *Az FMC dinamikája:* 4 kulcs tényező függvénye. Serkentő tényező a felhasználói kényelem, lehetővé tevő tényezők a technológia, a verseny és az ár.

A konvergencia koncepció megvalósulásának sebességét befolyásolja még a szabványosítás és a szabályozás helyzete, alakulása pedig – mint írtuk - jelentősen függ a technológiától. Fő szerephez jut az internet és a mobil, melyek nagy fejlődésen mennek keresztül. Mobil és internet stratégiákra épülve a mobil terminálokon fokozatosan növekszik az adatszolgáltatások alkalmazása. Az internet és a mobil szolgáltatók integrációjával a portálok is mobilok lesznek (zsebportál). A zsebportál egy elektronikus eszköz, amely tartalmazza a PC-t, a mobilt, az Internetet és a portált, mindig együtt van a felhasználóval (személyi adatkísérő, elektronikus szolga).

A fix-mobil konvergenciáról elmondható, hogy a technológiai áttörés helyett inkább hangsúlyt kap a hozzáállásban ill. a magatartásban bekövetkező változás. A felhasználók az FMC révén többszörös útvonalon, többszörös szolgáltatásokhoz jutnak hozzá és megszokják, hogy már nem egyetlen rendszer modellben kell gondolkodniuk.

Az univerzális mobil távközlő rendszer

Az UMTS fő szerepet tölt be a jó minőségű vezeték nélküli multimédia kommunikációs tömegpiac kialakításában, amely 2010-re világszerte megközelíti majd a 2 milliárd felhasználói számot. (Megjegyezés: 2001-ben a világon

már kb. 600 millió a mobil készülékek száma.) Az UMTS rendszer a jövő tartalom gazdag szolgáltatások és alkalmazások számára preferált mobil szállító platformot képez.

Az UMTS evolúció útján, a GSM és a TETRA mobil fejlesztési platform rendszereken folyamatosan épül ki, a rendszerek együtt tudnak majd élni ill. összeférők (kompatibilisek) lesznek egymással. A 2G/2,5G infrastruktúrával rendelkező mobil üzemeltetőknek a fejlesztéseikkel nagy költségek nélkül, gyorsan lesz lehetőségük felzárkózni a 3G-hez.

A különálló mobil és fix távközlő hálózatok mai koncepciója már nem megfelelő a holnapi üzleti környezet elvárásainak kezelésére, ma tehát kellő megvilágításba kell helyezni az UMTS azon képességeit, hogy új technológiákat, koncepciókat és szolgáltatásokat foglal magában. A mobil, fix és műholdas hálózatokon keresztül az UMTS utat nyit az információs társadalomba, szélessávú információkat, kereskedelmi és szórakoztató szolgáltatásokat szállít a mobil felhasználónak. Felgyorsítja a távközlés, az információs technológia és a média közötti konvergencia folyamatokat, hogy új szolgáltatásokat szállítson és friss bevételeket generáló lehetőségeket teremtsen, felkínálva a nagysebességű adatszolgáltatásokat, továbbá a globális roaming és más korszerű képességeket.

Az UMTS látszólag a GSM lépéseket követi, de a kétféle piac nem lesz azonos. A GSM újszerű beszédalapú nagy piacot teremtett, míg az UMTS a személyivé formált, multimédia és internethez kapcsolódó adatszolgáltatások piacát hozza létre. Az UMTS több lesz, mint a 2,5G GSM.

Az FMC alapjában a fix és mobil üzemeltetőkhöz vezet el, UMTS szolgáltatásokat szállítva mindkét környezetben. A fix üzemeltetők támogatják, a mobil üzemeltetők ellenzik a konvergenciát. Kellő szabályozásra lesz majd szükség. Az EU is vizsgálja az FMC szabályozási hatásait.

A mobil szolgáltatásokat szállító 3G infrastruktúra kulcs elemei a mag és a hozzáférési hálózatok. Az utóbbi drága lehet, telepítése hosszú időt vehet igénybe. Az új belépőknek jórészt nincs kiépített 2G infrastruktúrájuk és szükségük lesz a meglévő mobil infrastruktúrák használatára (az összekapcsolásra ill. a roaming-ra). Várható, hogy a nemzeti szabályozó hatóságok kötelezővé teszik majd a roaming és a szolgáltatásnyújtás lehetőségek megengedését az idegen hálózatokban, amely hangsúlyt kap a licencek kiadásakor is.

A TETRA (1)

A GSM sikerét nehezen lehetne megismételni más mobil technikákkal, semmilyen mobil technológia nem léphet a nyomába, a GSM beágyazódott a 3G UMTS modellbe is. Másik ütőkártyának számít azonban a TETRA is, amely szintén fontos szerepet játszik a 3G UMTS kialakításában. Hol tart ma a TETRA és merre halad?

A TETRA (1) megfelel a legkorszerűbb professzionális mobil kommunikációs igényeknek és hatékony platform rendszer a jövő alkalmazásfejlesztések számára. Ma az 1. változatú TETRA (1) rendszerek működnek ill. kaphatók, melyek megfelelnek az ETSI 1. kibocsátású (Release 1) szabványoknak. A GSM rendszerhez hasonlóan a TETRA (1) is nagy belső fejlesztési tartalékokkal rendelkezik és folyamatos evolúción megy keresztül. A TETRA (1) új piacokat hódít (békefenntartó hadsereg, tengerhajózás) és globálisan terjed.

A TETRA (1) rendszerre is érvényesek a konvergens fejlődési trendek: globális szabványok, nagyobb adatátviteli sebességek, adatcentrikus szolgáltatások, iroda, otthon, félig fix helyszín, gyalogos, földi és légi gépjármű használati módok integrációja, kiterjedt Internet/Intranet alkalmazás stb. A TETRA (1) továbbfejlesztések irányait is az FMC koncepció szabja meg.

Két vonalon (EPT Release 2, PSPP-MESA) folynak már a következő generációs fejlesztések (TETRA 2, TETRA/DAWS). Ezek a fejlesztések a következő évtizeden túl is folyamatosan biztosítják a professzionális felhasználói igények korszerű kielégítését.

A TETRA 2

Az új TETRA 2 fejlesztések megőrzik a TETRA (1) egyedülálló és kivételes jellegzetességeit (gyors hívásfelépítés, csoport kommunikáció, DMO stb.), növekvő adatsebességeket, új multimédiaszolgáltatásokat, a 2G/2,5G/3G közcélú mobil technológiákkal kompatibilitást és roaming-ot biztosítanak.

Az ETSI Board 28. ülése 2000. szeptemberben hagyta jóvá a 3 éves TETRA 2 fejlesztések munkaprogramját: TETRA evolúció (nagysebességű csomag adatátvitel fejlesztés), járulékos beszéd kodek (készlet) fejlesztés, rádiós interfész fejlesztés, szabványfejlesztés a TETRA 2 és a közcélú mobil (GSM, HSCSD, GPRS, EDGE, UMTS és más 3G/IP) hálózatok együttműködésére (interoperability) és a barangolás (roaming) biztosítására, SIM evolúció (USIM), hatókörzet kiterjesztés, új ETSI dokumentumok elkészítése (a piaci ill. felhasználói követelmények feltárására és támogatására), teljes vissza irányú (TETRA 2 – TETRA 1) kompatibilitás biztosítása, dual-mode és quintuple-mode terminálok kifejlesztése.

TETRA vagy UMTS?

Egyes vélekedések szerint az UMTS már a küszöbön áll és mindent megold. Mondják, hogy már nem is érdemes a külön TETRA hálózat létesítésébe befektetni, amely igen költséges, kiépítése pedig hosszadalmas. Nincs azonban igazuk.

- Az UMTS kiépítése is hosszú időt (10 év) vesz igénybe, a 3G technológia előremozdítása az elvi szabványtól a teljes üzemelésig még hosszabb időbe telik.

- A közcélú cellás rendszer egyáltalán nem vagy csak részben helyettesítheti a professzionális TETRA rendszert. Nincs is más mai vagy jövő mobil technológia, amely a professzionális piac minden igényét kielégíti.
- A készenléti szervek szigorú követelményeinek teljesítésére fejlesztették ki a TETRA rendszert, jórészt ezekre (ellátottság, rendelkezésre állás, hálózat megbízhatóság) fordítódtak a költségek. Ezeket a paramétereket az UMTS nem teljesíti.

Fentiekből levonható a következtetés, hogy a felsorolt tulajdonságokat a kereskedelmi UMTS nem tudja felajánlani, tehát a konvergált 3G rendszerben is nélkülözhetetlen lesz a TETRA, különös tekintettel arra, hogy a TETRA rendszer az előfizetőinek szintén képes felajánlani a gyors, megbízható és biztonságos IP kapcsolhatóságot.

A TETRA/DAWS – MESA

Az ETSI és a TIA szervezetek új nemzetközi projektet indítottak el az Európában és USA-ban felmerülő speciális felhasználói (közbiztonsági, készenléti, törvény végrehajtási, katasztrófa elhárítási és mentési, békefenntartói, stb.) igények kielégítését szolgáló szabványok kifejlesztésére, a teljes mobilitás/roaming és a vezetéknélküli ATM bitsebességek (max. 155 Mb/s) megvalósításásra.

A TETRA/DAWS fejlesztések az ETSI-ben megszüntek és a PSPP - MESA hatáskörébe kerültek át. A továbbfejlesztések a TETRA PDO platformon történnek, melyek célja az IP protokollon alapuló mobil szélessávú rendszer kifejlesztése és szabványosítása egyelőre a 3 GHz-es frekvencia tartományban.

A TETRA/DAWS technológia lesz a 4G szélessávú mobil kommunikáció megvalósítója (2005). A 3G UMTS fejlesztéseken túl (2000 - 2005) ez az egyetlen 2G mobil technológia marad csak fenn a 4G mobil szélessávú rendszerben (MBS). A 4G fejlesztés által megcélzott vivő bitsebesség tartomány (2 - 200 Mbit/s) ma ismeretlen a nagyterületű mobil környezetben, ezek a bitsebességek emelik át a TETRA/DAWS technológiát a mobil szélessávú tartományba.

Az FMC és a TETRA

A fix-mobil (távközlés, IT és média) fejlesztések egymás felé tartanak, konvergálnak (FMC). Az FMC eredményei a 3G UMTS-ben hasznosulnak, melynek alapelemei a 2G/2,5G mobil rendszerek (GSM, HSCSD, GPRS, EDGE, TETRA 1, TETRA 2). Az UMTS üzemeltetése a meglévő 2G/2,5G mobil rendszereken indul, 2010-ben is még túlnyomóan a 2,5G rendszerek képezik működése alapját.

Az UMTS-ben (nem létezik más**)** csak a TETRA tudja majd megfelelően kielégíteni a professzionális igényeket, melyek a közcélú cellás rendszerekben

egyáltalán nem vagy csak részben teljesíthetők. A konvergens TETRA 2 fejlesztések lehetővé teszik az UMTS-be való teljes beilleszkedést (kompatibilitás, együttműködés, barangolás), az FMC koncepció szerinti integrálódást. A további konvergens fejlesztések következtében a TETRA a 3G fejlődési fázison túl is - mint 4G mobil szélessávú rendszer (MBS) - fennmarad.

Rövidítések listája

ATM	Asynchronous Transfer Mode
DAWS	Digital Advanced Wireless Services
DMO	Direct Mode Operation
EDGE	Enhanced Data rates for Global Evolution
EPT	ETSI Project TETRA
ETSI	European Telecommunications Standards Institute
EU	European Union
FMC	Fix-Mobile Convergence
FMI	Fix-Mobile Integration
GSM	Global System for Mobile communications
GPRS	General Pocket Radio Service
HSCSD	High Speed Circuit Switched Data
IP	Internet Protocol
IT	Information Technology
MBS	Mobile Broadband System
MESA	Mobility for Emergency and Safety Applications
PC	Personal Computer
PSPP	Public Safety Partnership Project
SIM	Subscriber Identification Modul
SMS	Short Message Service
TETRA	Terrestrial Trunked Radio
TIA	Telecommunications Industry Association
UMTS	Universal Mobile Telecommunications System
USIM	Universal Subscriber Identification Modul

Hóka Miklós

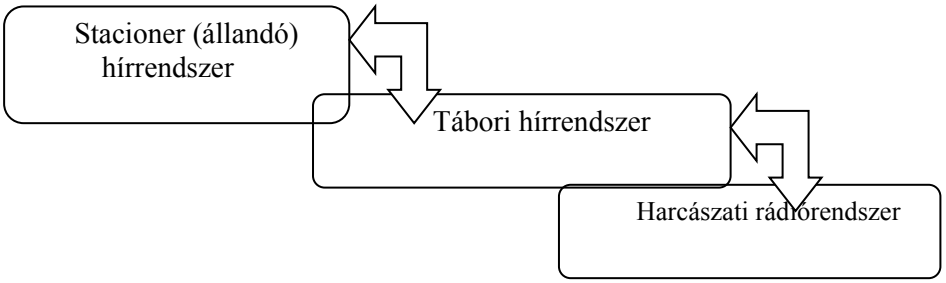
GONDOLATOK A HARCÁSZATI RÁDIÓRENDSZER KIALAKÍTÁSÁHOZ

A fejlesztés stratégiai koncepciója

„ A haditechnikai fejlesztés főbb irányait a NATO-val való együttműködés alapvető területeire a kompatibilitás és az interoperabilitás elérésének elengedhetetlenül szükséges szintje határozza meg, így prioritást élveznek a vezetési, irányítási és informatikai eszközökkel, az integrált légvédelmi rendszerrel, a logisztikai rendszerrel, a mobilitás technikai feltételeivel, a befogadó nemzeti támogatással, a csapatok és az infrastruktúra túlélőképességével kapcsolatos fejlesztések.”

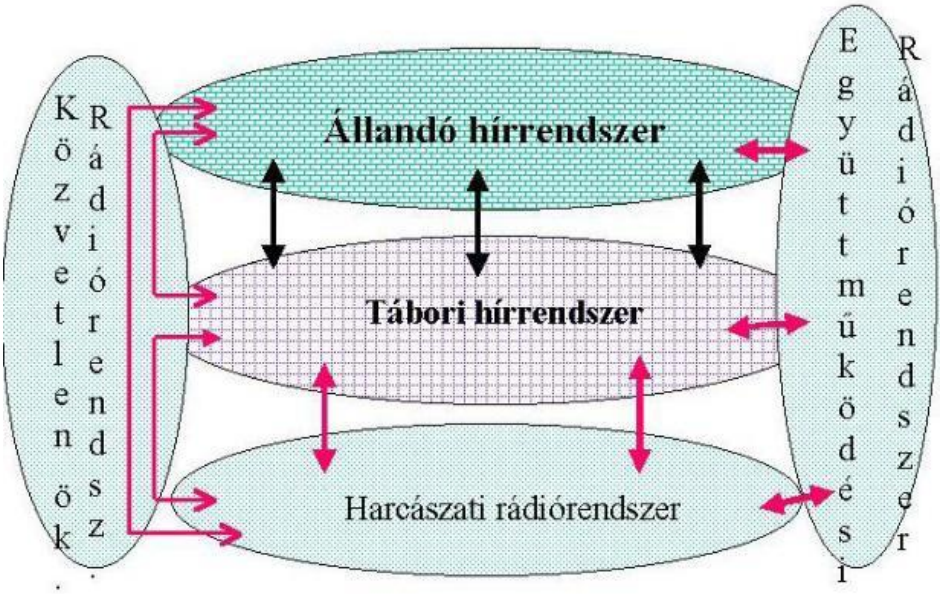
Az Országgyűlés 61/2000. (VI.21.) OGY határozata
a Magyar Honvédség hosszú távú átalakításának irányairól

A Magyar Honvédség Vezetési Csoportfőnökség koncepciója szorosan kapcsolódik az előbb vázolt elgondoláshoz, és felhasználói szempontból meghatározta a Katonai kommunikációs rendszer szintjeinek kialakítását, mely a következő ábrán látható:



1.ábra A katonai kommunikációs rendszer szintjei

Ahogy az ábrából is kiderül, jelen írás a harmadik szintre, a harcászati rádiórendszerek szintjére vonatkozik. Mivel a rádiók alkalmazása nem csak a legalsó, taktikai szinten történik, hanem része ugyanúgy a tábori rendszernek, mint a stratégiai szintnek is, így felállítottam egy kapcsolódási rendszert, nevezetesen, mely pontokat kell megvizsgálni a rádiórendszerek alkalmazásának szempontjából. Ezt mutatja be a következő ábra:



2. ábra. A rendszer felépítése és kapcsolódásai rádiós szempontból

A vizsgálati pontok kutatása fogja adni azokat az eredményeket, amelyek alapján meg lehet valósítani egy minden szempontból,- az általam vizsgált szempontokból elsődlegesen-, hatékonyan működő rádiórendszert, annak elvi kialakítási lehetőségét. Mivel jelenleg nem ismertek sem a rádiókészülékek típusai, sem a gyártó cég, egyáltalán az, hogy komplett rádiórendszer, vagy csak egyedi készülékek kerülnek rendszerbeállításra, (amelyekre a közbeszerzési törvény alapján pályázatot írnak ki,) így egyelőre csak elméleti síkon, mintegy általánosságban vizsgálhatom a problémát.

A továbbiakban tekintsük át azokat a károsan ható jelenségeket, amelyekkel a rádióhíradás során találkozhatunk:

- felharmonikusok megjelenése a spektrumban az adás során
- napszaki frekvenciaváltás szükségessége, a változó terjedési viszonyok miatt
- a többutas terjedés problémái (felületi és térhullám)
- a doppler effektus hatása az ionoszférában
- ön és kölcsönös zavarok a felhasználóknál

A gyakorlatban természetesen egyéb jelenségek is fellépnek, de úgy vélem a főbb zavarok e jelenségekhez kapcsolódóan hatnak, és ezek azok a jelenségek, amelyekre a modern rádiókészülékek tervezése során fő figyelmet fordítottak a fejlesztők és a gyártók.

Menedzselt rádiórendszerek

Az előző fejezetben felsorolt káros tényezők jelenléte arra inspirálta a fejlesztőket, hogy azokra megoldásokat keressenek a technikai fejlesztések során.

Az Automatikus Felcsatlakozás Létesítése, azaz az Automatic Link Establishment, (a továbbiakban ALE), valamint a hatékony frekvenciamenedzsment kezelni tudja ezeket a gondokat, és a rádiórendszerek rugalmas működését képesek biztosítani széles felhasználói körben.

A kulcsszerep a rádióhíradásban az, hogy támogatja az ionoszféra használatát a nagyobb távolságú összeköttetésekre. Így a rádióhíradás a következő főbb lehetőségeket biztosítja:

- relatív olcsóság a beszerzés és szállítás területén (főleg polgári alkalmazásokban)
- globális lefedettség érhető el, kontinensek közötti kapcsolatok lehetősége
- gyors telepíthetőség
- könnyen továbbfejleszthető (teljesítménynövelés, stb.)
- katonai vonatkozásban támogatja a vezetést, irányítást
- támogatja a mobilitást a műveletekben
- támogatja az együttműködést a készenléti és katonai műveletekben
- támogatja a különböző szállítási típusokat (földi, vízi, légi)
- interoperabilitást biztosít a nemzeti készenléti szolgálatok, de a multinacionális egységek között is.

A rádióhíradás fejlődésében központi tényezővé vált a lehetőség, - különösen a hidegháborút követő években -, hogy támogassa a nemzetközi békefenntartói műveleteket, és ezen túl interoperabilitást biztosítson a civil (rendvédelmi) és katonai felhasználók között.

Tekintsük át azokat a főbb irányvonalakat és trendeket, amelyek a 90-es években fejlődtek ki a rádióhíradás technikai megvalósításában.

Fejlesztések a rádiós technológiákban

Mielőtt rátérnénk a szorosan vett rádiós modemekre, tekintsük át röviden a modemek működésének az elvét, amely elemek alapvetően a számítógépes hálózatokhoz lettek kifejlesztve.

A *modem* szó a *mo*dulátor és a *dem*odulátor szavak kezdetének összevonásából jött létre. A modem lényegében egy olyan szerkezet, amelyet számítógépekhez csatlakoztatnak, hogy azok a telefonvonalakon keresztül is tudjanak egymással kommunikálni. A modem a számítógép digitális jeleit átalakítja a telefonvonalon továbbítható analóg jelekké (modulátor funkció), majd a vevő oldalon az analóg jelekből visszaállítja az eredeti digitális jeleket (demodulátor funkció). Tehát a modem egy modulátor és egy demodulátor együttesét képezi. A legtöbb modem aszinkron adatátvitelt valósít meg, de léteznek szinkron modemek is. A számítógéppel az RS-232C illesztőn (interface) keresztül kommunikálnak.

A kommunikáció megvalósításához persze egyedül a modem nem elegendő, szükség van még valamilyen kommunikációs programra is. Ezek a programok az adatokhoz általában hibaellenőrző kódot fűznek, amelynek segítségével felismerhető az átvitel során keletkezett esetleges adatveszteség. Idővel ez a

funkció a modemekbe került beépítésre, ugyanúgy, mint a hibajavító eljárás is, amely nem csak felismeri, de képes kijavítani is a kisebb hibákat. A következõ lépés az volt, hogy a modemekbe a tömörítés támogatását is beépítették, aminek révén ugyanazon a telefonvonalon nagyobb adatsebességet lehet elérni: kezdetben 1200, 2400, 9600 bit/s, a ma leginkább használt modemek esetében pedig 14400, 28800 és 33600 bit/s ez az érték. A kapcsolat felépítésekor a telefonvonal két végén lévő modemek egyeztetik a tudásukat, és mindig a kevesebbet tudó modemnek megfelelő értékekkel dolgoznak. Ma mindezeket szabványok írják le (V-szabványok[i]).

Rádiós modemek

A rádiórendszerek alkalmazásának sarkalatos pontja lett, a stacioner és tábori rendszereknél is jelentkező, megnövekedett adatátviteli kapacitás biztosításának szükséglete. Jóllehet a rádiók alkalmazása a köztudatban a beszédalapú információcserére korlátozódik, napjainkban új kihívásoknak kell megfelelni a korszerű rádióknak: az adatátviteli lehetőségek növelésének.

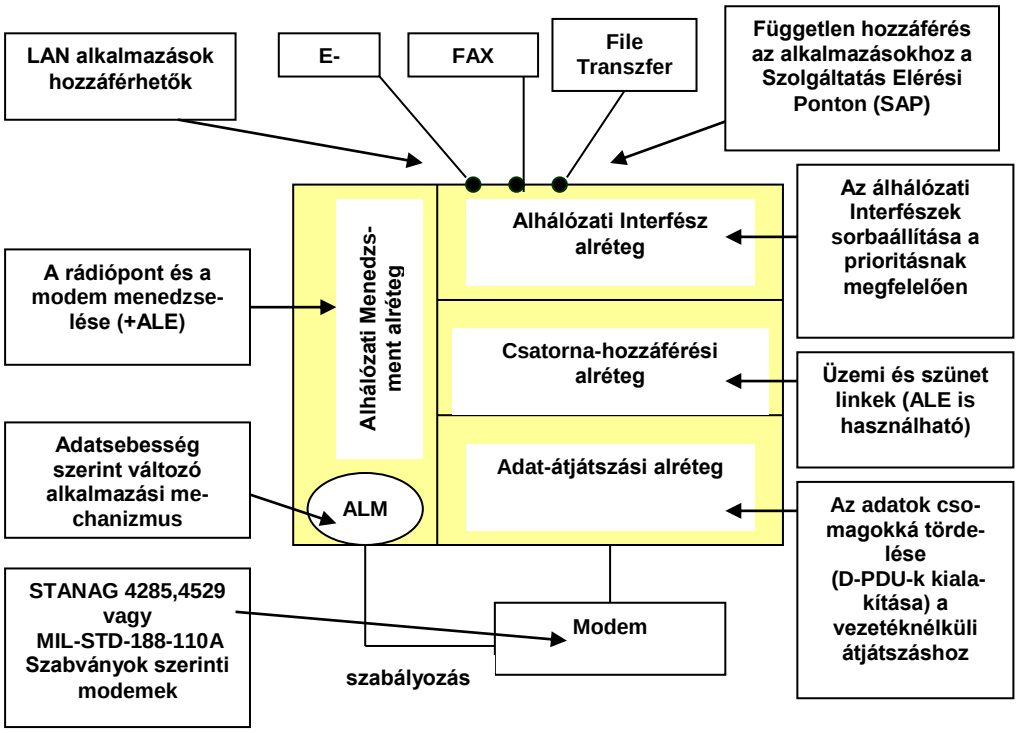
A gyors, Digitális Jel Processzorok (DSP) megjelenésével és alkalmazásával megnőtt a jelfeldolgozási sebesség, ami lehetővé tette a rádiós modemek egyszerű és rugalmas használatát. A rádiós modemek használata mára már meghatározó a rádiós rendszerekben. Ez a technológia az elmúlt években fejlődött ki és jelenleg a 9600 bit/s-os jelátviteli sebességet támogatja egy 3 (három!) KHz sávszélességű csatornán. (Vezeték nélküli jelátvitelről van szó!) Számos katonai szabvány van használatban, például a MIL-STD-188-110B, a STANAG 4285, a STANAG 4539, amelyek meghatározzák a hullámformát 75 bit/s és 9600 bit/s jelsebesség között. Ennél nagyobb jelátviteli sebesség is elérhető a független oldalsáv, az Independent Side Band (ISB) alkalmazásával, amely mintegy 19200 bit/s. A kutatások jelenleg is folynak a magasabb jelátviteli sebesség biztosításának lehetőségeire, különösen az Internet Protokoll (IP) szolgáltatás vonatkozásában. (Lásd az amerikai haderő Taktikai Internet kialakításának projektjét, vagy akár az angol hadsereg Bowman projektjét).

Adatkapcsolati Protokollok (Data Link Protocols)

A nagyobb teljesítményű modemek kifejlesztéséhez szükség volt bizonyos adatkapcsolati protokollok kifejlesztésére a rádiós adatkommunikációban. Számos adatkapcsolati protokollt szabványosítottak és használnak széles körben napjainkban. Példaként elevenítsük fel a több, mint 30 évvel ezelőtti, CCIR 476. számú Ajánlást, amely a telegráf kommunikációra mintegy 100 baud jelsebességet írt elő. Akkoriban még nem beszélhettünk számítógépes jelátviteli sebességekről, de mára ez már túl lassú lenne, ezért is vált szükségessé a modern felhasználók igényeihez igazítani a jelsebességek szabványait. Mai példát hozva, a STANAG 5066 szabvány, amely éppen a rádióadatkommunikációra vonatkozik, olyan funkciókat és interfészeket határoz meg, amelyek szükségesek a hálózati hibamentes kommunikációhoz a rádiócsatornákon.

Számos vezetési és irányítási (C2) rendszer fejlesztési tendenciája az IP alapú technológiák és a STANAG 5066 által meghatározott szerver-kliens alkalmazások felé mutat, amely lehetővé teszi e rendszereknek az olyan szolgáltatásokat, mint például e-mail küldése-fogadása rádiórendszeren keresztül. Mint látható, elmozdult az alkalmazások aránya a beszédhangú rádiókommunikáció irányából az adatátviteli rádiókommunikáció irányába.

3.ábra. Az adatkapcsolati réteg alhálózati felépítése a rádiós modemek alkalmazásánál



Visszatérve a STANAG 5066 szabványra, biztosít egy szabványos és nyílt rádiós átjátszási mechanizmust. A levegő interfész szabványosított, de nem szabadalmaztatott, (biztosítva a széleskörű gyárthatóságot), és egy további nyílt interfész biztosítja az alhálózati hozzáférést, amely lehetőség a független adatáramoltatást adja az adatkapcsolati réteg alatt és fölött (a fizikai rétegben és a hálózati rétegben - az OSI modell alapján). A protokollt úgy tervezték, hogy az interoperabilitás megoldott legyen a STANAG 4285, a STANAG 4529 és a MIL-STD-188-110B szabványok szerinti soros portú hangmodemekkel, de nem ad hozzáférési lehetőséget egyéb olyan modemeknek, amelyeket a nyitott achitektúrájú rendszereknek (OSI) terveztek. Tehát csak a ka-

tonai szabványok szerinti modemek csatlakoznak a protokollon keresztül, ezzel is egy biztonsági funkciót megvalósítva.

Az alhálózati hozzáférést biztosító nyílt interfész több kliens típust fog támogatni. Magában foglal egy ún. Automatikus Csatlakozás Fenntartási mechanizmust (ALM), amely az adatátvitel szerint változó algoritmussal biztosítja adott csatornán a legjobb átviteli minőséget. Egy kimondottan erre a célra tervezett keret-architektúra adja azt a maximális átviteli jelsebességet a keskeny sávú csatornákon, amely a NATO C3A kutatásai alapján alapul. A protokoll számos logikai alréteget ötvöz egybe az adatkapcsolati rétegben, többek között Alhálózati Interfészt, Csatorna-hozzáférési és Adatátjátszási alréteget. Az alrétegek saját interfészei mind csatlakoznak az Alhálózati Menedzsment alréteghez, ahogy a 3. ábrán is látható.

A STANAG 5066 szabvány alkalmazható mindazokon a helyeken, ahol az adatátvitel szükségessége felmerül a rádiózásban. (A katonai alkalmazásokon belül, természetesen.)

Automatikus Csatlakozás Létesítése (Automatic Link Establishment-ALE)

A rádiófrekvenciák használatának jellemzője, hogy az összeköttetés lehetősége naponta, illetve napszakonként is változik. A múltban a rádiókezelők igen gyakran szembesültek azzal a problémával, hogy használható frekvenciát kellett találni az üzemeléshez. A forgalmi adatlapon meghatározott frekvenciák sokszor nem biztosították a minőségi összeköttetést, és lehetetlen volt egyáltalán az összeköttetés felvétele is. A rádiókezelő (távírász) egyik fő tevékenysége a használható frekvencia kiválasztása és az összeköttetés folyamatos fenntartása. Az ALE funkció éppen ezt a tevékenységet teszi automatikussá, így a távírász figyelme az információ-továbbításra koncentrálódhat.

Aszinkron ALE

Egy aszinkron ALE mechanizmust tartalmazó rádióadó-vevő végigpásztázza a rendelkezésre álló frekvenciasávot, és megáll minden időpillanatban, amikor elfogadhatónak ítélt frekvenciát talál. A különböző rádióknak nem közös az időalapjuk, így a frekvencia csoportok pásztázása csak aszinkron módon lehetséges. Mikor az ALE mechanizmus fel akarja venni a kapcsolatot egy másik felhasználóval, kiválaszt egy frekvenciát az előzetesen végigpásztázottak közül, és „ismertetőjelet kér-ad” a hitelesítéshez. Az ismertetőjel kérés-adás természetesen nem azonos az analóg rádiókon alkalmazott módszerrel, ne feledjük, itt digitális rádiókról beszélünk, amely digitális rádiók mindegyike tartalmaz egy azonosító kódszámot, hasonlóan a számítógépekhez. Ha a hívott állomás helyes válaszjelet ad, a kapcsolat felépül, ha nem, akkor az ALE tovább keres, a sikeres kapcsolódásig. Az aszinkronitás jellemzője a számottevő időtöbblet a kisugárzásban, hiszen a hívott állomásnak is végig kell pásztáznia minden frekvenciát adott sávban. A

hálón belüli rádióállomások címzésrendszerrel rendelkeznek, amely címzés a sikeres összeköttetés felépülése után beíródik a Csatlakozás Minőség Vizsgálati, Link Quality Analisis (LQA) táblázatba. Ez a táblázat minden frekvenciáról tartalmaz minősítést a végigpásztázott sávban.

Az előbb ismertetett változatot alkalmazzák a MIL-STD-188-141B és a FED STD 1045 szabványokban, amelyek jelenleg az egyedül elfogadottak az ALE rendszerekben. A MIL-STD-188-141B szabvány széleskörű elterjedése fogja biztosítani azt az interoperabilitást, amely meghatározó a többnemzetiségű katonai, de akár a készenléti szolgálatok műveleteiben is.

Szinkron ALE

Amennyiben a rádiórendszerünk azonos típusú, azonos paraméterű rádiókból áll, lehetőség van a szinkron ALE rendszer alkalmazására. Egy szinkron ALE rendszer ugyanúgy végigpásztázza a rendelkezésre álló sávot használható frekvencia után, mint az előző esetben, azzal a különbséggel, hogy a rádióhálón belül a rádióállomások ugyanazon idő alatt, ugyanazokat a frekvenciákat pásztázzák. Így csökken a kisugárzási idő és nő a felcsatlakozás gyorsasága. A szinkron ALE további előnyökkel is rendelkezik: minimális sávlefoglalás mellett megnő a forgalom kapacitása.

Ilyen technikai megoldással dolgozik jelenleg a svéd haderő koszovói kontingensénél telepített KV 90 típusú kapcsolóközpont rádió-felvevőpontja.

Frekvencia menedzsment

A kommunikációs rendszerek mind bonyolultabbá válásával, számos frekvencia-ellátási probléma merül fel a rádióhíradás területén, így sokkal precízebb frekvencia-felhasználási tervezést igényelnek, mint korábban. A vezeték nélküli összeköttetés tervezése során figyelembe kell venni a helyi interferenciaszintet, az antenna típusát, a rádióteljesítmény paramétereket, a földelés típusát, és megannyi egyéb faktort. A számos, egymástól független változó azonos szintre hozása, összehangolása ma már szerencsére szoftvertámogatást élvez. A vezető rádiógyártó cégek termékeik mellett opcióként biztosítanak hatékony összeköttetés tervező szoftvereket, amelyekkel, nagy biztonsággal megvalósítható a rádiókommunikáció.

Új irányvonalak a katonai rádiózásban

Kitekintve a jelentősebb rádióprojektek megvalósításának világába, általánosnak mondható a régi, analóg rádiórendszerek, rádiókészülékek kivonása a használatból, és digitális rádiórendszerek alkalmazásával lesz megoldva a csapatok vezeték nélküli eszközökön való vezetése. A két legjelentősebb digitalizációs projekt, ami napjainkban aktuális: az amerikai hadseregben a Taktikai Internet felépítése, illetve a brit hadsereg Bowman terve. A digitalizáció nem minden problémától mentes. Például az Egyesült Királyság hadseregében, ahol 1970 óta a Clansman megnevezésű rádiókat használták, az új típusú, multimédiás adatátvitelre is alkalmas digitális rádiók rendszerbeállítására mintegy kettőmilliárd angol fontot irányoztak elő

költségként. A megvalósítás során az ár közel a kétszeresére nőtt, de ennek ellenére a Bowman adatszolgáltató rendszere 2003-2004-re, míg a nem rejtjelző elemeket tartalmazó rádió elemek 2001 végére kerülnek a csapatokhoz.

Nem minden ország képes anyagilag finanszírozni a hadseregét, hogy ilyen mértékű technikai átalakítást legyen képes az végrehajtani. De talán nincs is rá szükség. A Magyar Honvédség vonatkozásában nem is gondolkodhatunk a katonai híradás új alapokra helyezésénél olyan hatalmas összegek rendelkezésre állásáról, de a digitális rádióhíradás vonatkozásában valószínűleg hasznosítható néhány új elgondolás, kísérleti eredmény, amelyet a nagy hadseregekben már sikerrel alkalmaznak, illetve a közeljövőben lesznek megvalósítva.

Az Egyesült Államok hadseregében jelenleg az Összhaderőnemi Harcászati Rádiórendszer, a Joint Tactical Radio System (JTRS) projekt koncepcióján dolgoznak. A kutatások 1999 elején indultak be, a Raytheon és a Motorola cégek közreműködésével. Közös nyilatkozatuk a tervről a következő: *A JTRS koncepció azon alapszik, hogy a 21.század harcosa a technológia fejlettségétől függetlenül használhassa a rádiót. Ugyanúgy dolgozhat vele, mint egy laptoppal: adatbázisból kijelöli és letölti az aktuálisan szükséges hullámformát (!). A „fekete doboznak" nevezett első generációs rádiók (értsd, hagyományos AM-FM) nem lehetnek többé korlátai a harctéri kommunikációnak.*

Az új irányvonal kijelölésének értelmében az ITT cég is egy olyan digitális rádiórendszer kifejlesztésébe kezdett, melynek fantázia neve „Mercury", és a következő főbb jellemzőkkel bír: A rendszer felépítése hasonló, mint egy mobil cellás rendszeré, de nem stabil bázisállomásokkal, hanem mobil, gépjárműbe épített, mozgó felvevőpontok fogják alkotni a digitális gerincet. A tervek szerint mintegy ezer különböző felhasználó csatlakozhat ehhez a mobil gerinchálózathoz, mely speciális antennáinak és egyáltalán az egész rendszernek a csapatpróbája már megtörtént, jó eredménnyel. A rádiórendszer fogja egyben a gerincét képezni az Egyesült Államok katonai felhasználású Taktikai Internetnek, amely mintegy Intranet hálózat, erőteljes mobil szolgáltatásokat fog biztosítani a harctéren.

Maguk a rádiók vonatkozásában a szoftverrádió megnevezés a helyes. Véleményem szerint a jövő egyértelműen ebben az irányban gondolkodva körvonalazható. A szoftverrel feltölthető digitális rendszerben lévő rádiók olyan új fejlett, kiterjesztett lehetőségeket támogató kreációk, amelyek lehetővé teszik a csatlakozást a még használatban lévő készülékekkel, de egyben lehetőséget adnak a jövő technológiái számára is.

Közép Európa vonatkozásában folytatva a vizsgálódást a három szóbajöhető ország, a friss NATO tag Lengyelország, Csehország és Magyarország katonai kommunikációs rendszereit tekintettem át. Az áttekintés szempontja ezúttal a fegyverzet eladási piacon való részvétel. Hazánkat – sajnos – itt nem jegyzik, viszont Lengyelország az ELINT/COMINT kompatíbilis

fegyverirányítási rendszerrel van jelen a piacon, míg Csehország ELINT rendszereket ad el nemzetközileg, illetve a DICOM cég a taktikai piacot célozta meg rádió termékeivel.

Következtetések

Az előző mondatokból is következik, hogy Magyarország nem rendelkezik számottevő hadiipari kapacitással, legalábbis olyannal, amely a nemzetközi kereskedelemben szerepet játszana.

A valamikor korszerűnek mondható R-142 rádiókomplexum (és a többi valamikor használt rádióállomás) felett eljárt az idő, mint ahogy a székesfehérvári Videoton cég sem foglalkozik a honvédség részére sem tervezéssel, sem gyártással. A katonai rádiózásban megjelent új elveket, és lehetőségeket ezekkel a régi eszközökkel már nem lehet megvalósítani, különösen az adatátvitel elvárásait. Megfontolandó az új rádióeszközök beszerzése során a szoftverrádió rendszeresítése, lévén ez a jövő várható fejlődési iránya.

A rádió felvevőpont kialakításánál olyan új NATO STANAG-ok figyelembevétele szükséges, mint az előzőekben már említett 5066, az adatátvitel biztosítására, valamint az automatikus felcsatlakozás elősegítésére. Kiemelt figyelmet kell fordítani a frekvenciamenedzsment területére, a modern, sok frekvenciát használó készülékek üzemeltetésének tervezésénél. Mindenképpen megfontolandó a kiírt pályázatot megnyerő cég rádióinak megvásárlásakor a frekvencia menedzsment hatékony kialakítását biztosító tervező szoftver megvásárlása. Ez a lehetőség messzemenően hasznos, mivel a jövő katonai kommunikációs rendszerszervezőinek hatékony segítséget és precizitást fog nyújtani a rádiórendszerek tervezése, de még az üzemeltetése területén is.

A rádióhálók számának meghatározásában, a szükséges és elégséges rádióhíradás biztosításában a STANAG 5048 szabvány az irányadó. Természetesen függ még a mindenkori szervezeti felépítéstől és a döntéshozók elvárásaitól, hogy milyen számú rádiócsatorna szükséges adott szituációban a vezetés hatékony támogatásához.

Jegyzetek:

A doktori értekezés tervezett címe:

Hadműveleti, harcászati rádiórendszerek alkalmazása békeműveletekben és hadműveletekben, valamint a harc támogatására a vezetés, irányítás, együttműködés és az interoperabilitás tükrében.

Aszinkron átvitel. Olyan adatátviteli mód, amikor a két kommunikáló fél nem használ külön idõzítõ jelet, ellentétben a szinkron átvitellel. Éppen ezért szükséges az átvitt adatok közé olyan információ elhelyezése, amely megmondja a vevõnek, hogy hol kezdõdnek az adatok (mikor küld adatot az adó fél). Ezt a problémát a stopbitekkel oldják meg: minden karakter (nyolc bit) elé és mögé egy-egy bitet ragasztanak, amelyek miatt egy karakter átviteléhez ezért nem 8, hanem 10 bit szükséges.

Szinkron átvitel. Szinkron átvitelrõl akkor beszélünk, ha az adatátvitel meghatározott ütemben történik. Ezt idõzítõ jel (szinkronjel) segítségével lehet elérni. Ilyenkor a kommunikáló gépek mindegyike az adott ritmusban adja, veszi, illetve értelmezi az adatokat. Ha a két gépnek nincs küldendõ adata, a byte-ok küldése akkor sem áll le: olyan adatot (szinkronkarakter) küldenek egymásnak, amellyel a szinkront tartják fent (ebben különbözik a szinkron az aszinkron átviteltõl). A vevõ oldal veszi a szinkronkaraktereket, de azokat nem továbbítja a processzorhoz, hanem mintegy lenyeli õket. A szinkronizáláshoz nyilván olyan byte-ot érdemes választani, amely az adatok közt nem fordulhat elõ. Éppen ezért nincs elõírás a szinkronkarakterre, az adó és a vevõ a kommunikáció kezdetén megegyeznek, hogy mit tekintenek szinkronkarakternek.

RS232. Az angol *Revised Standard 232* (232-es felülvizsgált szabvány) kifejezés rövidítése.
Az *RS232* megalkotója az *Electronic Industries Association* (*EIA*) elnevezésû, elektronikai gyártókat tömörítõ szakmai szervezet. A szabványt a létrehozása (1971) óta kétszer vizsgálták felül, ezért az *RS232C* elnevezést kapta. Az *RS232C* két számítógép közötti soros vonali kommunikációt támogat főleg aszinkron átvitellel, de vannak olyan elemei is, amelyek a szinkron átvitelt is támogatják.

V-szabványok. Az *ENSZ Nemzetközlési Távközlési Unió* nevû irodájának (*ITU*) *CCITT* (*Comité Consultatif International de Télégraphique et Téléphonique*) szerve által definiált, modemekre vonatkozó szabványok sorozata, amelyek a használt adattömörítési és hibajavító eljárásokat is leírják.

Protokoll. A hálózati kommunikációt leíró szabályok rendszere. Protokollokat használnak a hálózatokban egymással kommunikáló számítógépek és programok is. A protokollokat különböző testületek szabványosítják.

Interface. Angol szó, magyarul csatolófelület, csatlakozási felület, illetve illesztőfelület kifejezésekkel illetik. Az interface egy olyan eszköz, illetve illesztési felület, amelynek segítségével két különböző hardver- vagy szoftver-eszköz közötti kommunikációt valósíthatunk meg. A csatolófelület feladata például az összekapcsoláshoz felhasznált jelrendszer értelmezése is.

Felhasznált irodalom:

1. Az Országgyűlés 61/2000. (VI.21.) OGY határozata: A Magyar Honvédség hosszú távú átalakításának irányairól szóló dokumentum
2. NATO STANAG 5048 Minimum scale of communications for the NATO land forces (ed5)
3. MIL STD 188-141A Automatic Link Establishment (ALE)
4. Joint Tactical Radio System (JTRS). U.S. Army Signal Center and FORT GORDON.
5. RADIO COMMUNICATIONS IN THE DIGITAL AGE. VOLUME ONE: HF TECHNOLOGY
6. First Printing, May 1996. Copyright © 1996 by Harris Corporation
7. FM 24-2 Spectrum Management
8. Headquarters Department of the Army Washington, DC, 1991
9. AN/PRC-117F Special Operations Forces radio has applications for digital divisions and beyond *by David Fiedler* Army Communicator
10. US Land Warfare Systems - COMMUNICATIONS, COMMAND, CONTROL AND INTELLIGENCE www.fas.org/man/dod-101/sys/land/
11. Communicate by a Tactical Radio
12. 18 June 1998 U.S. Army Signal Center and School, Ft Gordon, GA

Hruska Éva

ANTENNA HUNGÁRIA RT. – EDUNIO KONZORCIUM – EDUWEB RT.

Az Antenna Hungária Rt. – kihasználva távközlési kapacitását – szerepet szeretne vállalni az elektronikus oktatás piacán. Ennek érdekében létrehozta az EDUNIO konzorciumot, melynek tagjai – az Antenna Hungária Rt., az Antenna Multimédia Rt., az OGYS Consulting Kft., valamint az Eduweb Rt. – rendelkeznek azokkal az ismeretekkel és kapacitásokkal, melyek segítségével a konzorcium meghatározó szereplője lehet a hazai elektronikus távoktatásnak.

Eduweb távoktatási rt.

Az Eduweb Távoktatási Rt. 2000 októberében kezdte meg hivatalosan működését, de ezt a lépést komoly piacelemző, és szoftverfejlesztési munka előzte meg.

Az Eduweb Rt. azzal a céllal jött létre, hogy – a hazai piacon egyedülállóan – minden anyagi és szellemi kapacitását arra használja fel, hogy megismertesse Magyarországon az e-learning (elektronikus oktatás) filozófiát, és a felmerülő internet/intranet alapú távoktatási igényeket kielégítse. Ehhez kifejlesztette, és folyamatosan továbbfejleszti a megfelelő technikai hátteret, kiépítette a hatékony kapcsolatrendszert, és megszerezte azokat a tapasztalatokat, amelyek a sikeres és hatékony e-learning-es képzés alapját adják

ELŐZMÉNYEK

Az e-learning térhódítása egyértelmű ma már Európában és Magyarországon is. A jelenleg elérhető külföldi keretrendszerek finanszírozásukban nem igazodnak a magyarországi lehetőségekhez, nehezen testre szabhatók (hiszen a forráskód külföldön van), és nehezen feleltethetők meg a magyar tanulási/tanítási igényeknek. Éppen ezért az Eduweb Rt. egy idegen rendszer disztribútori szerepe helyett egy teljesen új, magyar elektronikus oktatási környezet kialakítását választotta.

CÉLJAINK

Az Eduweb Rt.

- egy stabil és biztonságos technikai háttérrel rendelkező, valamint
- a felhasználók (diákok és tanárok) munkáját mindenben támogató oktatási környezetet akar létrehozni és működtetni. Ennek érdekében nemcsak a technikai, technológiai elemeket biztosítja az elektronikus oktatáshoz, hanem szakszerű és gyakorlati oktatásfejlesztési tanácsadást is nyújt partnereinek.

SIKERÜNK BIZTOSÍTÉKAI

- Rendelkezünk a szükséges anyagi és szakmai hátérrel.

- Az Európai Uniós ajánlások, illetve a hazai törekvések, célzott pályázati kiírások azt bizonyítják, hogy terveink és céljaink korszerűek, és előremutatóak.
- Az általunk kifejlesztett megoldás megfelel az iparági szabványoknak, ezáltal átjárhatóságot biztosít más e-learning rendszerek tartalmai felé.
- Az XML adattárolási technológia lehetővé teszi, hogy a tartalom megjelenítése igazodjon a felhasználói oldal adottságaihoz (sávszélesség, tanulási igények, szokások).

OKOK ÉS LEHETŐSÉGEK AZ E-LEARNING HAZAI ALKALMAZÁSÁHOZ

1. Ma már adottak, illetve kiépíthetőek azok a technikai és technológiai feltételek, amelyek a hálózati oktatáshoz szükségesek. Azaz szinte mindenhol van már számítógép, internet és/vagy intranet kapcsolat, nagysebességű adatátviteli hálózat.
2. A potenciális felhasználók közül egyre többen ismerik el azt, hogy az információk birtoklása előnyt jelent számukra a munkaerőpiacon, és ezekhez az információkhoz csak folyamatos tanulás útján lehet hozzájutni. A számítógép, az internet/intranet már nem számít „ellenségnek", vagyis a tanuláshoz való hozzáállás is megváltozott az e-learning javára.
3. Az információ birtoklása az egyének, ezek továbbítása és hozzáférhetővé tétele pedig a szervezet pozícióját, alkalmazkodó képességét javítja.
4. A földrajzi távolságok megszűnnek az elektronikus oktatásban. Az ország, a kontinens, vagy akár a Föld távoli pontjain is ugyanaz a követelményrendszer állítható fel a hallgatókkal szemben, hiszen képesek vagyunk standard oktatást (tananyagot és módszert) biztosítani számukra.
5. „E-világban" élünk, ahol az információk seregei támadnak bennünket, és csak folyamatos, és ugyanilyen gyors tanulással tudunk szelektálni ezek között, és alkalmazkodni az életünket befolyásoló újdonságokhoz.

AMI AZ EDUWEB KERETRENDSZER MELLETT SZÓL

- **Függetlenség helytől, időtől, tanulási szokásoktól, tanári attitűdtől:** A diák akkor, ott és olyan tempóban tanul, ami számára a legmegfelelőbb. Nem kell igazodni a többiekhez, és nem lényeges a tanár habitusa sem.
- **Frissíthetőség, naprakészség:** Az elektronikus formátumnak köszönhetően a tananyag mindig aktuális, és nem merülnek fel nyomdai költségek sem.
- **Fajlagosan alacsony üzemeltetési költség:** Bár a keretrendszer beüzemelése és tananyaggal történő feltöltése anyagi, idő, és munkaráfordítást igényel, működtetése olcsóbb, mint a hagyományos tantermi képzés, ahol egy adott kurzus lebonyolítása minden alkalommal ugyanakkora költséggel és

munkával jár. Az Eduweb Rt. oktatásfejlesztői csapata bármikor szívesen segít a tananyagfejlesztésben.

- **Rugalmas formátum:** Az elektronikus oktatás számos olyan prezentációs lehetőséget biztosít a tanár számára, amellyel érdekesebbé, szemléletesebbé, ezáltal hatékonyabbá teheti a virtuális tanórát (animációk, mozgóképek, hangok, szimulációk stb.)
- **Időtakarékosság, hatékonyság:** A keretrendszer sok adminisztrációs terhet levesz a tanár válláról (tesztek értékelése, statisztikák elkészítése). Az így felszabaduló idő mindenki számára kincs.
- **Automatizált ütemezés, mérés és dokumentálás:** A diák előrehaladása ütemezhető, s ezt a program folyamatosan „észben tartja" és kontrollálja. Az eredményeket, statisztikai adatokat nem kell rendszerezni, hiszen ezt a keretrendszer önmaga megteszi.

FELHASZNÁLÁSI TERÜLETEK

Az Eduweb keretrendszere az ismeretátadás több területén is alkalmazható. Ezek egy részében önállóan is megállja a helyét, máshol célszerű a hagyományos oktatási módszerekkel együtt alkalmazni. Példaként álljon itt néhány ötlet:

- Informatikai képzés
- Általános ismeretek átadása:
  - eszközhasználati leírások
  - eljárásrendek
  - minőségbiztosítási leírás
  - belső szabályozások, utasítások
- Elméleti oktatások törzsanyaga és segédanyagai
- Nyelvoktatás
- Számonkérés

Az eduweb keretrendszer elemei

EDU.WEB vagy EDU.SITE

A megcélzott hallgatói tábor összetételétől, illetve a tananyag elérhetőségének módjától függően lehetőség van internetes (EDU.WEB), vagy intranetes (EDU.SITE) technikai megoldás kiépítésére. Ezáltal kialakítható egy nyitott, vagy egy zárt oktatási környezet.

TARTALOM

A tartalom alapvetően három, oktatási szempontból eltérő funkciót szolgáló részből áll(hat).

1. A tananyag képezi az oktatás központi magját, ezt nevezhetnénk törzsanyagnak is. Ennek ismerete alapvető fontosságú a diák továbbhaladása és értékelése szempontjából.
2. A segédanyagok a tananyag jobb megértését szolgálhatják, illetve kiegészítő információkat nyújthatnak a hallgató számára. A segédanyagok típusa nagyon sokféle lehet: definíciótár, szószedet, képgyűjtemény, irodalomgyűjtemény, internet-hivatkozás, térképtár, nyomtatványtár, kapcsolódó szabálygyűjtemény stb.
3. A feladatok segíthetik a hallgató előrehaladását (próbatesztek), illetve a megszerzett tudás színvonalát is mérik.

FELADATOK

A feladatok beiktatásával szabályozható a hallgató előrehaladása, hiszen ezek teljesítéséhez köthető a továbblépés. A feladatok paraméterei oly módon állíthatók be, hogy a szoftver automatikusan értékelje a megoldásokat, de természetesen adott az esszékérdés lehetősége is. A feladatlapok összetétele lehet állandó (azaz az adott feladatsor kérdései mindig változatlanok), változó (vagyis egy kérdéshalmazból a rendszer a megadott paraméterek alapján osztja ki az egyes diákoknak a feladatlapokat), illetve adaptív (a hallgató felkészültségi szintjéhez igazodó nehézségű feladatsort generál a szoftver).

STATISZTIKÁK

A keretrendszer a hallgatók és a diákok minden egyes mozdulatát naplózza. Ezek az adatok előre gyártott vagy tetszőleges tartalmú jelentéseken tanulmányozhatók

ADMINISZTRÁCIÓ

Az adminisztráció elsősorban a jogosultságok beállítását és karbantartását jelenti. Ezek a paraméterek határozzák meg, hogy az egyes felhasználók milyen minőségben léphetnek be a rendszerbe, és ott milyen jogosultságokkal rendelkeznek.

KOMMUNIKÁCIÓ

A keretrendszer felhasználói közötti információáramlást az on-line és off-line kommunikációs csatornák biztosítják. A levelezés és a fórum segítségével üzenhetnek egymásnak a hallgatók és a tanárok, a társalgóban pedig valós idejű megbeszélhetik egymással ügyes-bajos dolgaikat.

TANÁCSADÁS ÉS TÁMOGATÁS

Az Eduweb Rt. szolgáltatási körébe az oktatásfejlesztési tanácsadás és a technikai segítségnyújtás egyaránt beletartozik. Ez a biztosíték arra, hogy a keretrendszer funkcióit teljes mértékben kihasználhassák a felhasználók.

ÖSSZEFOGLALÁS

Az Eduweb Távoktatási Rt. komplex e-learning megoldást biztosít partnerei számára, amely magába foglalja

- a technikai feltételek biztosítását,
- a szükséges szoftverek folyamatos fejlesztését és a rendszer karbantartását,
- az oktatásfejlesztési tanácsadást, illetve aktív részvételt a tananyagok kidolgozásában,
- a kommunikációs lehetőségeket
- és az interaktív tartalom elhelyezésének és megjelenítésének lehetőségét.

Szöllősi Sándor

A MAGYAR HONVÉDSÉG ÁLLANDÓ ÉS TÁBORI HÍRHÁLÓZATÁNAK ÁTALAKÍTÁSÁVAL KAPCSOLATOS PROBLÉMÁK

Bevezetés

A vizsgálat során *kiindulópontnak* kell tekinteni azt a tényt, hogy a Magyar Honvédség állandó hírhálózata pillanatnyilag átalakítás alatt áll. Ez az átalakítás az analóg rendszerek irányából a PCM alapú, ISDN szolgáltatású digitális rendszerek felé történik. A *másik alapvető szempont* az, hogy a tábori hírhálózat pillanatnyilag csak papíron, elvekben kerül(t) digitalizálásra és elsősorban a ma még rendszerben lévő néhány analóg elem biztosítaná a csapatok vezetésének elemi feltételeit (Bár ezzel kapcsolatosan erős kételyeim vannak, ha egy valódi konfliktushelyzetet tételezek fel.).

A fentiek mellett *szervezeti átalakulások* következtek be az ésszerű ***szükséges és elégséges védelem*** feltételeinek biztosítása érdekében, valamint az analógból a majdani digitális eszközökre épülő rendszerbe való minél zökkenőmentesebb átmenet érdekében. A pillanatnyi gazdasági helyzetet és lehetőségeket figyelembe véve ez az út meglehetősen ésszerűnek tűnik. Ennek ellenére, véleményem szerint, sajnos újfent abba a hibába készülünk beleesni, hogy a rövid (esetleg közép-) távú célokat próbálunk hosszú távra elnyújtani A ***túl hosszú megvalósítási, megvalósulási intervallum*** magában hordozza a ma még viszonylag korszerűnek mondható technológia elavulásának lehetőségét, a technikai lemaradásunk permanenssé válását, valamint azt, hogy esetleg a rengeteg erőfeszítés ellenére sem leszünk képesek a kor által megkövetelt és a NATO tagságunkból is adódó elvárásoknak megfelelni.

Az átalakulás problematikája

Az eddigi analóg rendszerek cseréjét több dolog is kiköveteli. A valóságos helyzetet tekintve, a kozmetikázás és a nosztalgiázás mellőzésével megállapíthatjuk, hogy a korábbi technika napjainkra erkölcsileg 100%-osan elavult, technikailag – a civil szférával összehasonlítva – majdnem minden területen több generációval lemaradt. Ez a lehetetlen műszaki állapot és utánpótlási problémák mellett egyéb súlyos gondokat is magában hordoz. Nézzük sorban ezeket.

Technikai és szervezési oldalát tekintve azon szervezeteink, melyek egy adott körletbe való kivonulás esetén szükségszerűen fel kellene, hogy csatlakozzanak valamely területileg közeli polgári szolgáltatón keresztül az Országos Távbeszélő Hálózat (OTH) rendszerébe, pillanatnyilag – a törvényi szabályozás ellenére – majdhogynem lehetetlen feladat elé lennének állítva. Eltekintve attól, hogy egyes szolgáltatók sok esetben egymással sem hajlandóak

együttműködni (lásd: Puskás-emléknapok), nézzük meg a mi technikai lehetőségeinket.

A kezdetek kezdetén a légvezetékes korszakban egyszerű eszközök segítségével lehetőség volt a postai vonalakra rácsatlakozni, majd a postai központon át az OTH-t elérni. A technikai fejlődés adta lehetőségek és a megnövekedett igények miatt ezen vonalak vivőzésre kerültek, több eres földkábelek váltották ki a korábbiakat. A különböző csoportképzési eljárások fejlődésével, az előfizetők számának jelentős növekedésével a jobb szolgáltatási minőség elérése érdekében sok területen koax-kábeles rendszerek is alkalmazásra kerültek. A honvédség részéről egyre szűkült a közvetlen rácsatlakozás lehetősége. Egyre inkább láthatóvá vált, hogy a postai rendszerekhez való felcsatlakozás során külön a honvédség becsatlakozását lehetővé tevő, külön nekünk fenntartott, fixen kiépített „bálványrendszer" szűk keresztmetszetet biztosít, a szolgáltatónak csak nyűg, melyet előbb-utóbb megpróbál ledobni magáról. Ez a Magyar Posta szétdarabolásával, majd a területi koncessziók létrejöttével közel egyidőben a civil szférában szinte robbanásszerű technikai fejlődés-fejlesztés során be is következett. A lakott területek közötti trönkvonalak ma már döntően optikai kábeles rendszereken alapulnak, digitális központokon keresztül kapcsolódnak egymáshoz, nem egy esetben SDH rendszerben struktúrálva.

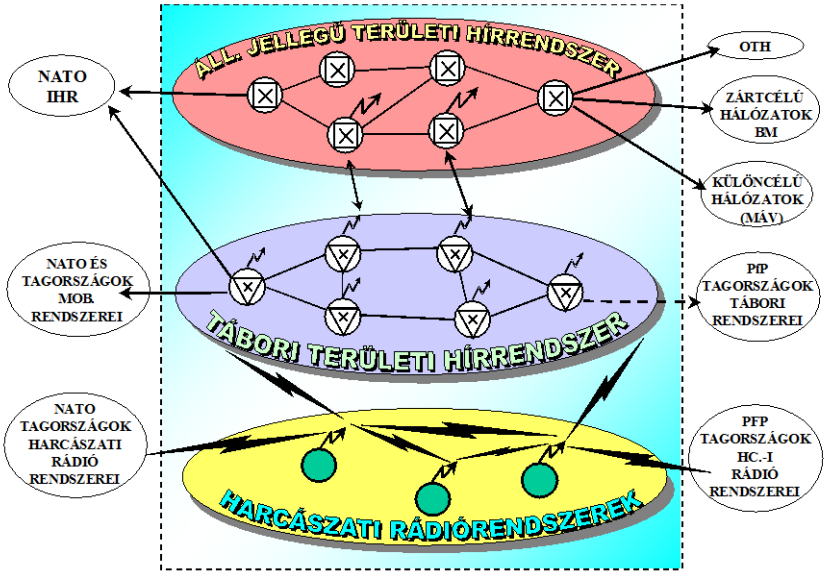
Gyakorlatilag nincs semmilyen lehetőségünk ezen rendszerekhez való direkt felcsatlakozásra,

hiszen az optikai kábelt nem igazán lehet a hagyományos értelemben „megcsapolni". Sokan úgy gondolják, hogy semmi baj, hiszen nekünk is lesz digitális eszközrendszerünk, majd azzal valahogy meg lehet oldani. Sajnálatos módon ez nem igaz. Vizsgáljuk meg, hogy miért.

A technikai oldalát tekintve tudni lehet, hogy ebbe a fent említett optikai gerinchálózatba tábori eszközökkel csak *a szolgáltató által kitelepített digitális koncentrátorokon* (digitális kisközpontokon) át lehet felcsatlakozni, ha azt a saját központjában az igények szerint felprogramozta, szoftveresen „berendezte", a viszonylatokat beállította. Kérdéses az, hogy ezeket az eszközöket ki felügyeli, ki őrzi, ha felügyeletmentes akkor hogyan lehet hozzáférni, stb... Az 50/1998. sz. „ ...a zárt célú hálózatokról és azok igénybevételéről ..." szóló kormányrendelet , a 175. sz. „Végrehajtási kormányrendelet ..." , valamint az új Egységes Hírközlési Törvény megfogalmazza mind a Magyar Honvédség, mind a nyílt-, a külön- és a zárt célú rendszerek közötti összekapcsolás jogi és alkalmasint gazdasági feltételeit. Többek között – a polgári szolgáltató vonakodó, ill. az ország biztonsági érdekeit sértő magatartása esetén lehetőség van a szolgáltató rendszerének, annak beleegyezése nélküli, utólagos kártalanítás mellett történő felhasználására. A gond csak az, hogy hogyan. Hiszen megint csak ott tartunk, hogy kivettük a szolgáltató kezéből a rendszerének irányítását, nem ismerjük annak struktúráját, nem tudunk arra a mi eszközeinkkel az ő együttműködése nélkül felcsatlakozni. Különösen akkor nem, ha a szolgáltató

valamely egészen más, nem ISDN alapú szolgáltatást alkalmaz. (pld. IP alapú technológiát alkalmaz, melyhez nekünk – tervezetten - nincsenek eszközeink) Márpedig az idő tényező döntő fontosságúvá válik a Magyar Honvédség várható feladatainak függvényében. Marad tehát az együttműködés. A „gond" csak az, hogy a Magyar Köztársaság biztonságpolitikai alapelveit tekintve védelmi jellegű struktúra kialakítására törekszik a katonapolitika oldaláról is, mely többek között magába foglalja azt is, hogy nincs ellenségképünk sem.

MAGYAR VÉDELMI DIGITÁLIS HÍRADÓ RENDSZER
SEMATIKUS VÁZLATA



1. számú vázlat (HVK. VCSF. Hír. Osztály előadás)

Gazdaságpolitikai oldalát tekintve nem engedhetjük meg magunknak, hogy az országot „körkörös-védelemre" rendezzük be, különös tekintettel arra, hogy a hidegháborús korszak lezárásának egyik hatása a nemzetközi egyezményekben vállalt, két és többoldalú szerződéseinkben is rögzített fegyverzet- és létszámcsökkentés, mely a haderőreform kapcsán is testet öltött. Ezzel a létszámmal nem vagyunk képesek körkörös védelmet biztosítani, erődrendszer kiépítésére a magyar katonaföldrajzi viszonyokat figyelembe véve nincs reális, gazdaságos lehetőség.

A szolgáltató oldalát tekintve azt mondhatjuk, hogy - ***nem elhanyagolva a nemzetbiztonsági szempontokat*** - nem tudjuk, ill. nem mondhatjuk meg a szolgáltatónak azt, hogy hol, mikorra, milyen csatornaszámmal, kivel, esetleg

milyen szolgáltatón keresztül akarunk minősített esetben az OTH-n keresztül összeköttetést teremteni.

Ha viszont nem mondhatjuk meg, a szolgáltató nem tud előre elkészített tervekkel (programokkal) igen gyorsan csatlakozásokat létrehozni és számunkra biztosítani, tehát csak *a fejlesztési koncepcióban* is látható három rétegű hírközlő rendszer alkalmazható.

A fejlesztési koncepció főbb irányelveit tekintve, a tábori digitális híradórendszer **csak az állandó híradórendszerünkön** *keresztül* válhat alkalmassá ezen problémák megoldására, különös tekintettel arra, hogy a haderőreform előbb-utóbb szükségszerűen a hivatásos, kis létszámú, jól felkészült, jól felszerelt, gyorsan mobilizálható, ütőképes hadsereg és a vele együttműködésre képes területi milícia (vagy Nemzetőrség) koncepciójára fog vezetni, ahol a *digitalizált laktanyahírközpontok* képesek lesznek a visszamaradó állomány kiszolgálása mellett ezen feladat ellátására is.

(Ezzel viszont elveszítjük azt a lehetőséget, hogy esetleges komoly rendszerkiesés esetén is tudjunk tábori eszközökkel ***az OTH-ra is*** támaszkodva összeköttetést teremteni – másképpen fogalmazva: ***időt nyerni***.)

Joggal vetődhet fel a kérdés, hogy miért gondolom azt, hogy csak ***rövid idő*** áll rendelkezésre a fenti probléma megoldására. Az okok a következők. A nemzetközi helyzet változásait és a hidegháborús időszak lezáródását figyelembe véve megállapítható – és ez a Magyar Köztársaság Biztonságpolitikai Irányelveiben is jól megfogalmazott -, hogy nem kell számítanunk szomszédos országból érkező, ellenünk irányuló támadó hadműveletekre.

A veszély ***elsősorban*** egyéni-, csoportos terrorista ill. diverziós, szomszédos országon keresztül érkező, vegyi-, biológiai-, stb. agressziót elkövető kisebb-nagyobb fegyveres csoportok irányából fenyegethet, akár provokációs céllal egy konfliktus kirobbantása érdekében, melynek nagy eséllyel vallási háttere is lehet. Ezen eseményeket lassú reagálás esetén nem lehet megfelelően lekezelni. Amennyiben a felderítési adatok alapján ezen csoportok helye és tevékenysége behatárolható, mindenképpen szükség van a minél szélesebb körű együttműködésre, gyors információcserére. Ehhez

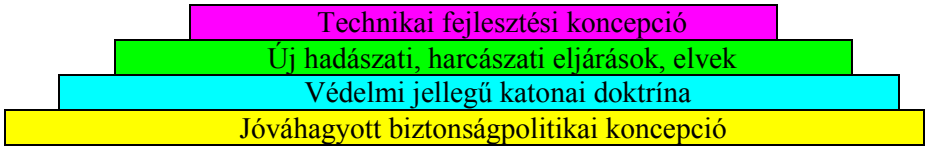
- ***azonnal*** használható,
- tetszőleges technikai megoldású és ***képességű***
- nagy állóképességű rendszert kell alkalmazni, melyet
- nem lehet sem zavarni,
- sem lehallgatni és
- képes ***bármely*** nyílt-, zárt- ill. különcélú rendszerbe való belépésre,
- annak használatára

a különféle együttműködő szervezetekkel való kommunikáció érdekében.

Véleményem szerint a fentiekből következően hadszíntér híradó előkészítéséről nem beszélhetünk.

A másik alapvető problémakör a következő. A jelenlegi fejlesztési koncepció – előremutató jellege mellett is – nem áll szilárd alapokon, meglehetősen öncélúnak tűnik, nem látszik, hogy mit miért kell fejlesztenünk, ill. miért pont úgy, ahogy az tervezve van. A véleményem a következők miatt alakult így ki.

Egy haderőfejlesztés sarkalatos kérdésének kellene lennie egy az Országgyűlés által elfogadott biztonságpolitikai koncepciónak. Jelenleg ilyen hivatalos dokumentumról nem tudok. Egy meglévő biztonságpolitikai koncepció lehetne az alapja a Magyar Honvédség védelmi katonai doktrínájának. A doktrínára alapozva lehetne egyértelműen, világosan kidolgozni a különböző új hadműveleti, harcászati elveket, eljárásokat. Ezen eljárásoknak kellene determinálniuk a szükséges technikai fejlesztés alapvető irányait, a technikai, szervezeti, személyi szükségleteket. Lehetővé válna a fejlesztés hosszú távú, korrekt, gazdaságos tervezése.



2. sz. ábra

Jelenleg a tendencia az, hogy más országok rendszereit tekintve mintának, a magyar viszonyokra próbáljuk kissé ráerőszakolni, „barkács módszerekkel”. Le kell szögeznem, hogy nem vagyok a reform ellen, de

a nemzeti sajátosságaink, katonaföldrajzi helyzetünk vizsgálata alapján elsősorban

- a *gyors reagálású,*
- *nagy tűzerejű,*
- *kis létszámú,*
- *hivatásos katonákra épülő,*
- *hatékony együttműködésre képes* alakulatok kialakítását tartanám célszerűnek,
- *figyelembe véve azt, **hogy önálló, nagymérvű technikai fejlesztésre** nincs hadiiparunk, nincs pénzünk, nincs időnk*

Véleményem szerint a *tábori hírhálózat* rácspontokon alapuló ***tervezett rendszere*** a fenti szempontoknak és követelményeknek sem lesz képes megfelelni. Kiemelten kell ezek mellett kezelni az ***átcsoportosításokkal kapcsolatos technikai és szervezési problémákat,*** mely jelenleg - az időtényezőt is figyelembe véve - a hálózat- és frekvenciamenedzsmentet szinte megoldhatatlan problémák elé állítja, ill. állítaná.

Mindezeken felül fellép az a probléma is, hogy a tábori rendszerfelügyeletet ellátó munkahelyek ***kiemelten fontos célobjektumokká válnak*** diverziós-

vagy szabotázscselekmények szempontjából, akár számítógépes vírusokkal való „megfertőzést” is értve ezalatt.. Ezen eszközeinkben okozott károk nagy valószínűséggel képesek a rácsponti rendszerünket - különösen egy nagy dinamikát követelő átcsoportosítás esetére időzítve – összeomlasztani.

A további problémát az okozza, hogy akár az állandó, akár a tábori rendszerünk felől bekövetkezhet egy ilyen jellegű támadás. Az egymásra való kölcsönös ráhatás miatt pedig katasztrofális következményeket is okozhat. Mivel a teljes rendszer digitalizálásra kerül (előbb-utóbb a rádiók is), fokozott figyelmet kell fordítani az ilyen jellegű rendszerösszeomlások megakadályozására. Ez jelentheti adminisztrációs, szervezési valamint nem utolsósorban személyi jellegű biztonsági intézkedések alkalmazását.

A következő problémacsoport a szervezeti változásokkal összefüggő. Az új technikai rendszer kialakítása során a híradó személyi állománnyal szembeni szakmai követelmények és elvárások jelentős mértékben átstrukturálódásra kerülnek. A mai, alapvetően gyengén kiképzett híradó szakállomány csak az analóg technikát ismeri, (kivétel a HiCom rendszer üzemeltetésével foglalkozó központkezelői állomány), alkalmatlan továbbképzés nélkül az új technikai eszközök kezelésére, alkalmazására. A technikaváltás esetén gyakorlatilag jelentős tartalékos utánképzés letöltésére lenne szükség, mely meglehetősen drága és nem eléggé hatékony. A tervezett hathónapos sorkatonai szolgálat ezt a tendenciát csak tovább erősíti, a kiképzettség fokát tovább gyengíti. Nem elhanyagolható az ezen kiképzési feladatokkal járó, várhatóan igen magas számú technikai meghibásodások aránya sem.

Ezen okok is indokolják azon álláspontomat, hogy az új rendszer alkalmazására, kezelésére csak hivatásos hadsereg keretein belül kerülhet sor. A jelenleg meglévő híradó szakember gárda könnyen átképezhető, lényegesen kevesebb ráfordítással. A meglevő tiszti (tiszthelyettesi) állomány jelentős része alkalmas az új technikák, eljárások megtanulására, elsajátítására. Meglátásom szerint igénylik is a hadsereg megújhodását és képesek a megújulásra.

Véleményem szerint ezzel szemben a szerződéses katonák híradó szakfeladat végrehajtására továbbra is alkalmatlanok, mert a régi technikát már nem képesek kezelni, az újat pedig még nem tanulták meg. A szerződéses katonák rendszerét elsősorban előzetes alkalmassági vizsgálatok után néhány hónapos tanfolyamok elvégzése és eredményes vizsgaletétel után lehetne csak fenntartani. Ez természetesen plusz költséget jelent. A kiképzett állomány megtartására csak megfelelő versenyképes fizetések mellett van lehetőség, mert nem cél az, hogy a szerződéses katonák „téli átvonulási szállásnak” tekintsék a Magyar Honvédséget.

Összességében megállapítható, hogy a tervezett tábori híradórendszer kialakítása

- túl hosszú időre van tervezve,
- nincsenek meg hozzá a személyi feltételek,

- közel sem biztos, hogy ezt a típusú rácsponti rendszert kell megvalósítani, (szükség lenne hatástanulmányok elkészítésére a más rendszerekkel való összehasonlításra)
- a tervezett rendszerrel kapcsolatos ***alkalmazási-eljárási módok*** nincsenek kimunkálva (fejreállított piramis, lásd 2. sz. ábra), nem látszanak ***a felhasználói oldalról felmerülő igények***
- figyelembe kell venni a nemzeti sajátosságokat,
- lehetőség szerint egységes technikai eszközparkot kell kialakítani, mely lehetőséget nyújt adott illesztőegységek segítségével bármely más rendszerre való felcsatlakozásra, melyet a szolgáltató rendelkezésünkre tud bocsátani,
- megfontolandó, hogy hosszabb távon nem olcsóbb-e egy konkrét rendszert beszerezni és nem több rendszerből összerakott többékevésbé együttműködésre hajlandó heterogén rendszerrel küszködnünk.

Ezen problémák felvetése azon késztetésből fakad, hogy a Magyar Honvédség hosszú évtizedek után most kapott (ill. kap) esélyt arra, hogy korszerű, ütőképes haderővé váljon, hiszen a „haderőreformnak" nevezett haderőleépítés gyakorlatilag a többszöri szervezeti átstruktúráláson kívül más eredményt nem hozott. Most kell kihasználnunk a felkínált lehetőséget, mely úgy tűnik, hogy politikai akarat és politikai kényszer által született és megfelelő indíttatást adhat a hadsereg jövőjét tekintve. Nem szabad elvétenünk a kezdeti lépést (mely már így is nagyon hosszúra nyúlt), hiszen bármit teszünk, bármilyen döntés is születik, az több generációra meghatározhatja a hadsereg állapotát, lehetőségeit, döntően befolyásolva az ország önvédelmi képességeit.

Ennek a képességnek egyik döntő záloga a felhasználói igényekhez rugalmasan alkalmazkodni képes, széleskörű szolgáltatási lehetőségekkel rendelkező, gazdaságosan üzemeltethető, nagy állóképességű katonai info-kommunikációs rendszer.

Mottó:

Murphy után szabadon: Ami elromolhat, az el is romlik. Na de muszáj pont nekünk siettetni?!

Irodalomjegyzék

- 1992. évi LXXII. törvény a távközlésről
- Melléklet a távközlésről szól 1992. évi LXXII. törvényhez
- 50/1998. (III. 27.) Kormány rendelet a zártcéú távközlő hálózatokról
  1. számú melléklet az 50/1998. (III. 27.) Kormány rendelethez
  2. számú melléklet az 50/1998. (III. 27.) Kormány rendelethez
  3. számú melléklet az 50/1998. (III. 27.) Kormány rendelethez
  4. számú melléklet az 50/1998. (III. 27.) Kormány rendelethez
- 1991. évi XVI. törvény a koncesszióról
- 158/1993. (XI. 11.) Kormány rendelet a távközlő hálózatok összekapcsolásáról, együttműködésének engedélyezéséről, valamint a hálózati szerződésekről.
- Hamar Sándor mk. ezds. (HVK Vezetési Csoportfőnökség Híradó osztály): A Magyar Honvédség híradása és híradó szolgálata
  Előadás, Budapest, 2001. március 22.
- Fekete Károly mk. alez.: A Magyar Honvédség kommunikációs infrastruktúráját érintő szabályzók
  http://www.zmne.hu/tanszekek/vegyi/indexlogo.htm
- Rajnai Zoltán mk. őrgy.: A tábori alaphírhálózat (szárazföldi) vizsgálata egyes NATO országok kommunikációs rendszereinek tükrében
  ZMNE Budapest 2001.
- Végh Ferenc: A Magyar Honvédség feladatai és struktúrája az ezredforduló után, a biztonság alakulásának függvényében
  ZMNE Budapest 1999.
- Dr. Széplaki János: A magyar fegyveres erőkkel szemben támasztott követelmények és feladatok
  ZMNE Budapest 1999.
- Dr. Simon Sándor: Az ország honvédelmi felkészítésének főbb területei és feladatai
  ZMNE Budapest 1999.
- Dr. Kőszegvári Tibor: A biztonságpolitika alapjai
  ZMNE Budapest 1999.
- Kiss Jenő, Horváth István: A Magyar Köztársaságot fenyegető kihívások és veszélyek kezelésének katonai eszközei és feladatai
  ZMNE Budapest 1999.
- Dr. Kőszegvári Tibor: A nemzetközi biztonságot fenyegető új kihívások és kockázatok
  ZMNE Budapest 1999.
- Dr. Kőszegvári Tibor, Dr. Szternák György ezds., Magyar István alez.: A XXI. századi hadviselés
  ZMNE Budapest 2000.
- A Magyar Köztársaság biztonság és védelempolitikai alapelvei (kézirati munkapéldány)
  Budapest 1999.

Vörös Miklós

AZ INFORMÁCIÓS ÉS KOMMUNIKÁCIÓS TECHNOLÓGIAI FORRADALOM ÉS A KATONAI FELSŐOKTATÁS

BEVEZETÉS

Az utóbbi években a szellemi erőforrások váltak a régiók, nemzetgazdaságok és a vállalkozások gazdagságát, sikerességét és versenyképességét leginkább befolyásoló erőforrásokká. Általánosan elfogadottá vált az a nézet, hogy az egyén boldogulásának, szakmai előmenetelének, társadalmi hasznosságának és beilleszkedésének legfontosabb feltétele a tanulás. A tudás felértékelődése a minőségi és a piaci igényeknek megfelelő oktatás, a rugalmas képzési rendszer iránti igény növekedését eredményezte. Az ismeretek mennyiségének növekedése, a munkaerőpiac gyors változása, a gyakorlatban azonnal alkalmazható tudás megszerzése szükségessé teszi a teljes életen át tartó tanulást. Ez a folyamat gyökeresen megváltoztatja az oktatási rendszert. A felsőoktatásnak nem lehet többé alapfeladata egy terület teljes ismeretanyagának átadása. A diplomával záruló képzés fő feladata a hallgatók tudásának megalapozása és felkészítésük a teljes életpályára kiterjedő tanulásra, ezért a felsőoktatási intézmények tevékenysége fokozatosan diverzifikálódik: hagyományos feladataikkal egyenértékűen fontos lesz a felnőttek munka melletti képzése.

A Magyar Honvédség korszerűsítése során a technikai és szervezeti fejlődés gyors üteme miatt jelentős a tudás amortizációja, ezért megnő a rendszeres, azonnal alkalmazható és számon kérhető ismereteket nyújtó (tovább)képzések szerepe. A képzési költségek és az oktatói terhelhetőség korlátjai, valamint a személyek helyettesítési nehézségei miatt az önképzés és a távoktatás szerepének rohamos növekedése várható.

A TÁVOKTATÁS JELENTŐSÉGE ÉS LEHETŐSÉGEI

Az információs és kommunikációs technológia (IKT) robbanásszerű fejlődése által kínált új lehetőségek, valamint a távoktatás módszertani fejlődése következtében a távoktatás elfogadottsága az elmúlt néhány év alatt gyökeresen megváltozott. A távoktatás az Európai Unió szellemi erőforrás politikája központi komponenseinek egyike lett (pl. a távoktatás, a korszerű informatikai technológia oktatási alkalmazása a SOCRATES és LEONARDO programok központi része).

A szellemi erőforrás-fejlesztés iránt a gazdaság és az állampolgárok oldaláról egyaránt megnyilvánuló, rohamosan növekvő igényt a hagyományos módon nem lehet kielégíteni. A megoldást a távoktatás kínálja.

A teljes életpályára kiterjedő tanulás során az oktatás és képzés egyre nagyobb részét képezik azok a feladatok (pl. munka melletti továbbképzés), ame-

lyek nem, vagy racionálisan nem végezhetők el a hagyományos oktatási módszerek alkalmazásával. Megoldást itt is a tanuló önálló munkájára építő, igen hatékony távoktatási módszerek alkalmazása jelentheti.

Az európai integrációs folyamatokra való felkészülésnek az oktatás az egyik legfontosabb eleme. A hallgatók döntő többsége azonban -alapvetően finanszírozási okok miatt- nem tud részt venni külföldi részképzésben: a tananyagok határokon keresztül történő áramlásával lehet biztosítani az oktatás egész Európára történő terjesztését. A rohamosan fejlődő IKT az oktatás és képzés számára szinte beláthatatlan lehetőséget nyitott, melyeket csak a távoktatás képes kiaknázni.

Az elmúlt időszakban a távoktatás oktatatási, tanulási és képzési módszerei diverzifikációjának lehettünk tanúi. E módszerek legfontosabb közös sajátossága, hogy az elsajátítandó tananyagot, ismereteket valamint az elsajátításra vonatkozó útmutatást és a megszerzett tudás ellenőrzését különböző információhordozók tartalmazzák: nyomtatott anyagok, audio- és videokazetták, mágnes és CD lemezek. Egyre több tananyag érhető el hálózatokon keresztül. E médiumok lehetővé teszik az önálló, tanár jelenléte nélküli tanulást.

A tanár szerepe nélkülözhetetlen, de a hagyományostól eltérő e folyamatban. Nem ő a tananyag fő közvetítője, hiszen az a más tanárok és szakemberek feldolgozásában áll rendelkezésre különböző médiumokon. A tanár fő feladata a tanulók kérdéseinek megválaszolása, motivációjuk, tanulmányaik elősegítése, szükség szerint szabályozása, a diákok közötti együttműködés létrehozása, az ismeretek elsajátításának értékelése. Különválik tehát a tananyagok elkészítése, amely szakértői csoportok tevékenysége és az oktatás folyamata, amely tutorok, szervezők feladata.

Az önálló tanulást biztosító, különböző médiumokon rögzített tananyagok alkalmazása, a tanár megváltozott szerepe, az önálló tanulás a hagyományos oktatásban elképzelhetetlen szabadságot és rugalmasságot biztosít a tanuló számára a tananyag tartalma, a tanulás üteme, időbeosztása és helye tekintetében. Ez a rugalmasság nemcsak azt teszi lehetővé, hogy a diák tanárjától ill. az iskolától földrajzilag távol végezhesse tanulmányait, hanem a szellemi erőforrás-fejlesztés hatékony módszerévé teszik a távoktatást.

A távoktatásban az akadémiai elemek (tudományos és gyakorlati ismeretek és alkalmazásuk, pedagógiai értékek, kulturális tartalom és háttér) és a társadalmi tevékenység (igényfelmérés, tervszerűség, gazdaságosság, csoportmunka, szervezettség, minőségellenőrzés, marketing, menedzsment, hatásvizsgálat) kölcsönhatásban vannak egymással - a társadalmi elem az, amely megnehezíti ennek az oktatási-tanulási kultúrának a meghonosítását hagyományos akadémiai környezetben, amely jórészt a tanárok egyéni teljesítményére és kompetenciájára épít. Jelentős különbség van a költségek nagysága, megjelenésük időpontja és módja tekintetében is. A gondosan szervezett távoktatás összköltsége általában lényegesen kisebb a hagyományos képzésénél, de költ-

ségek nagy része a tananyagok elkészítésével van összefüggésben, ezért a képzés elkezdése előtt koncentráltan jelentkezik. A hagyományos képzés általában nagyobb költségei időben széthúzva (részben a meglévő infrastruktúra költségeiben és a munkatársak fizetésében, részben pedig a diákok kiadásaiban és kiesett munkaidejében) jelentkeznek.

A távoktatás a felsőoktatási intézményektől távoli területeken, határokon keresztül történő alkalmazása jelentős többletbefektetés nélkül és a résztvevők számára is sokkal olcsóbban teremti meg a felsőoktatási intézmények képzésébe való bekapcsolódás, színvonalas tanulmányok folytatásának lehetőségét. E tanulmányok egy része folyhat hagyományos módon a felsőoktatási intézményben, de a képzés nagyobb részére a tanulók lakóhelyén, tutori segítséggel, laboratóriumok, konzultációs központok és szakmai gyakorlati lehetőségek igénybevételével kerül sor.

A távoktatás módszertanának fejlődése, a képzési költségek csökkenése, a korszerű informatikai technológia oktatási alkalmazásának és a felsőoktatás nemzetközivé válásának egyidejű fennállása a szellemi erőforrás-fejlesztés történetében először teremti meg a tananyagok és oktatási rendszerek globális versenyét. A hagyományos keretek között vagy azokon kívül folytatott tanulmányok részeként a diák felveheti a világ más részén kifejlesztett és oktatott, általa legszínvonalasabbnak ítélt tananyagot és az informatika korszerű eszközeinek felhasználásával igénybe veheti az adott intézmény távoktatási rendszerének szolgáltatásait.

A távoktatás mellet az egész életpályára kiterjedő tanulás megvalósítása jelentheti a legnagyobb kihívást a felsőoktatási rendszerek számára. Az a körülmény, hogy az egyén szakmai előrehaladása tekintetében a kezdeti képzéssel összemérhető jelentősége van a folyamatos továbbképzésnek, alapvetően megváltoztatja a hagyományos oktatási rendszerek működését: a tanterveket, az elméleti és a gyakorlati képzés kapcsolatát, a kezdeti felsőfokú képzés időbeni ütemezését. Az egyetemek fontos feladata lesz a felnőttek munka mellett folyó továbbképzése is.

A távoktatás jelentősen eltér a tradicionális egyetemi képzéstől: az elméleti megalapozás rovására nő a gyakorlati ismeretek, az általános ismeretek rovására pedig a speciálisak szerepe. A tananyag szorosan kapcsolódik a tanulók korábbi napi feladataihoz. Az oktatásnak figyelemmel kell lennie a résztvevők munkájára és családi életére. Ellentétben a hagyományos képzéssel, itt a hallgatók kiesett munkaidejét és az emiatt elmaradt hasznot is figyelembe kell venni a gazdaságosság megítélésénél: a képzés hatékonysága elsőrendű követelmény.

OKTATÁS AZ ELEKTRONIKUS EURÓPÁBAN

Az Európa Tanács 2000. márciusában Lisszabonban tartott ülésén azt a célt tűzte ki Európa elé, hogy legyen a világ legversenyképesebb és legdinamikusabb gazdasága. Az elképzelések megvalósítását célzó eEurope akciótervet a

portugáliai Feirában tartott tanácskozáson fogadták el. Az akcióterv alapján kidolgozott eLearning kezdeményezés együtt kezeli az eEurope intézkedéseinek különböző oktatási elemeit, arra törekszik, hogy mozgósítsa az oktatásban és a kultúrában résztvevő közösségeket, továbbá az európai gazdaság és társadalom szereplőit azért, hogy felgyorsítsa a képzési és oktatási rendszerek átalakulását és Európa mielőbb tudáson alapuló társadalommá váljék.

Mivel a kommunikáció fejlődésének minden új lépcsőfoka (beszéd, írás, könyvnyomtatás, elektronikus sajtó, számítógépes hálózatok, információs szupersztráda) egy időben hatott az oktatási-tanulási folyamat mindegyik elemére, ezért a tudáson alapuló társadalom kialakításának első, megkerülhetetlen szakasza az, hogy a társadalom tagjai magabiztosan használják a tudáshoz való hozzáférésre szolgáló eszközöket, és széles körben elterjedjen a számítógépismeret.

Az eEUROPE akcióterv

A jövőben a társadalom teljesítménye egyre nagyobb mértékben függ majd attól, hogy polgárai mennyire tudják kiaknázni az új technológiák lehetőségeit, milyen hatékonyan építik be a gazdaságba és építik fel a tudáson alapuló társadalmat. Ebben a folyamatban döntő az oktatás és képzés szerepének növelése (az Európai Unió 25 évesnél fiatalabb 117 millió lakosa közül 81 milliónyi jár iskolába, ahol 5 millió tanár tanít, a különböző képzési formákban több millió ember vesz részt).

Az eEurope akcióterv együtt kezel több stratégiai területet, meghatározza a kihívásokat, és válaszlépéseket javasol. „A digitális korszak európai fiatalsága” és a „Gyorsabb Internet a kutatóknak és a diákoknak” az oktatásról szól, három másik pedig szorosan összefügg a szakmát adó képzéssel és az egész életen át tartó tanulással. Az új technológiák alkalmazásával az önállóságnak és a rugalmasságnak kedvező tanulási környezet hozható létre.

Az eEurope akcióterv kulcsterületei:

- olcsóbb, gyorsabb, biztonságos Internet:
  - olcsóbb és gyorsabb Internet hozzáférés,
  - gyorsabb Internet a kutatóknak és a diákoknak,
  - biztonságos hálózatok és intelligens kártyák.
- befektetés az emberi képességek javítására:
  - a digitális korszak európai fiatalsága,
  - munkavállalás a tudáson alapuló gazdaságban,
  - részvétel a tudáson alapuló gazdaságban.
- az Internet használatának ösztönzése:
  - az elektronikus kereskedelem elterjesztése,
  - on-line közigazgatás,
  - on-line egészségügy,
  - euópai digitális tartalom a globális hálózatokban,
  - intelligens közlekedési rendszerek.

Az Európa Tanács elvárásai alapján:

- minden európai polgárnak rendelkeznie kell az információs társadalomban való élethez és munkához szükséges készségekkel (az iskolaköteles kor végéig minden egyes tanuló tudjon bánni a számítógéppel),
- 2001 végére az Unió minden iskolájában legyen elérhető az Internet és álljanak rendelkezésre multimédiás eszközök,
- 2002 végére fejeződjön be azon tanárok képzése, akikre szükség van az Internet és a multimédiás eszközök használatának oktatásához,
- az iskolák folyamatosan kapcsolódjanak rá a 2001 végéig létrehozandó elektronikus tudományos kommunikációt szolgáló nagysebességű európai hálózatra,
- az európai oktatási és képzési rendszer feleljen meg a tudáson alapuló társadalom követelményeinek.

Az európai társadalmi modellen belül prioritást kell kapnia az élethosszig tartó tanulásnak: meg kell határozni az ennek során elsajátítandó új alapkészségeket, be kell vezetni számítógépes alapismereteket igazoló európai diplomát. A számítógépes műveltség szerves része lesz a munkaerő alkalmazkodóképességének és minden polgár elhelyezkedési lehetőségének: a cégek munkahelyi képzési formái kulcsfontosságúak lesznek az élethosszig tartó tanulásban.

Az akcióterv célkitűzéseit 2002. végére kell megvalósítani.

Az eLEARNING kezdeményezés

Az Európa Tanács prioritásként kezeli az új technológiák sikeres beépítését az oktatási és képzési rendszerekbe. Az európai polgárok a világon a legiskolázottabbak között vannak, az európai oktatási rendszerek a világ legjobbjai sorába tartoznak, Európa mégis súlyos hiányosságokkal küzd és lemaradt az új információs és kommunikációs technológiák használatában, az alábbi okok miatt:

- hardver- és szoftverhiány (az általános iskolákban az egy számítógépre jutó tanulók száma 400 és 25 között változik),
- aggasztó szakemberhiány, különösen az IKT-ban otthonosan mozgó tanárokból és oktatókból,
- Európa túl kevés oktatási multimédiás szoftvert, terméket és szolgáltatást kínál a képzés és az oktatás céljaira,
- komoly kihívást jelent az európai társadalom igényeinek megfelelő szoftverek, tartalmak és szolgáltatások megfelelő kínálatának kialakítása,
- a távközlés magas költsége Európában akadályozza az intenzív Internet-használatot és a számítógépes ismeretek elterjedését.

Az eLearning kezdeményezés alapját négy fő területen tett intézkedések jelentik.

- Gépek és berendezések:
  - kulcskérdés a multimédiás számítógépek számának növelése a különböző tanulási, képzési és tudásfórumok összekapcsolása és a digitális hálózatokhoz való hozzáférés javítása érdekében (2004-re egy multimédiás számítógépre 5—15 felhasználó juthat),
  - szükség van olyan tanulási környezetek kialakítására, amelyek megfelelnek az egész életen át tartó tanulás különböző szintjei sajátos igényeinek,
  - a hardverre fordított kiadások kalkulálásához hasonlóan gondoskodni kell szoftverekre, multimédiás termékekre és szolgáltatásokra fordított költségek kalkulálásáról is.
- Képzés minden szinten:
  - a technológia hatással van a szervezetekre és a módszerekre, az oktatási és képzési programok szerkezetére és tartalmára, továbbá új tanulási környezetet és új tanár-diák kapcsolatot alakít ki. Így az új technológiák használatát a tanulási módszerek összefüggésében kell szemlélni.
  - a képzés irányításában is az új technológiákhoz szükséges készségek fejleszté-sére kell összpontosítani.
- Multimédiás szolgáltatás és tartalomfejlesztés:
  - az információ-technológiáknak az oktatásba és a képzésbe történő sikeres beépítésének feltétele a szükséges jó minőségű szolgáltatások és tartalmak megléte,
  - a tanárok és tanulók irányításához az új tanulási környezetben meg kell teremteni a minőségi kritériumok, a tudományos és szakmai értékek hivatalos elismerésének rendszerét.2002 végére jelentősen meg kell erősíteni a szakmai tanácsadó szolgáltatásokat annak érdekében, hogy az új technológiák révén mindenki hozzáférhessen az alapképzésre és a szakmai továbbképzésekre, illetve felnőttoktatásra vonatkozó információkhoz.
- A tudás megszerzését szolgáló központok fejlesztése és hálózatba kapcsolása:
  - A tanítási és képzési központokat sokoldalú, mindenki számára hozzáférhető tudásszerző központokká kell átalakítani, biztosítani kell a szükséges berendezéseket és a tanárok felkészítését.
  - A virtuális fórumok és kampuszok egyre több tanár, tanuló és témavezető hálózatba kapcsolását teszik lehetővé. Az

eLearning ösztönözni fogja a virtuális terek és kampuszok összekapcsolását, az egyetemek, iskolák, képzési központok, valamint a kulturális centrumok hálózatának kialakítását.

A katonai felsőoktatás és a Magyar Honvédség korszerűsítése

A jövő honvédségében a tisztek és a tiszthelyettesek létszámarányának változása jelentősen átalakítja tevékenységük tartalmát:

- a tisztek esetében nő az irányító, vezető szerepük és csökken az általuk végzett fizikai tevékenységek mennyisége,
- a tiszthelyettesek végzik az operatív tevékenységek zömét,
- a technikai színvonal növekedésével változik a csapatjavítás, ezért a tisztek esetében a képzés és felkészítés iránya, tartalma a gyakorlati tevékenységek oldaláról eltolódik az elméleti és a magatartástudományi - vezetői területek irányába,
- tekintettel a fejlődés ütemére, jelentős mértékben nő a tudás amortizációja és nő a rendszeres, számon kérhető és azonnal alkalmazható ismeretek szerepe. Az állandósult és nagy ütemű fejlődés folyamatosan erodálja a megszerzett ismereteket, ezért megnő a rendszeres továbbképzések és az önképzés szerepe.

Az egyén versenyképessége közvetlenül kapcsolódik a teljes életpályára kiterjedő tanuláshoz, mely alapvető célja a kreativitás, a rugalmasság, az adaptációs, a problémamegoldó és a tanulási készségek folyamatos fejlesztése. Az egyén szempontjából:

- a tanulás és önképzés a pályán maradás és előrejutás feltételévé válik, ezért az egyénnek motiválttá kell válnia a folyamatos tanulásra,
- az önképzés és tanulás befektetéssé válik, amelyre áldozni kell, és nem várható el, hogy teljes egészében a honvédség erőforrásaira épüljön,
- a tanulás versenyhelyzetet teremt, amelynek révén - különösen a pályázati rendszer elterjedésével és szélesedésével - gyorsan változhatnak a függőségi viszonyok,
- a tanulás nem csak önmegvalósítás, hanem a szervezettel történő azonosulás is,
- a katonai, szakmai és nyelvi ismeretek mellett nő az általános műveltség szerepe a társadalom- és magatartástudományok területén. Utóbbiak hozzájárulnak az egyének rangsorolásához is, mert a katonai hierarchiában történő előrejutásban szerepük folyamatosan növekszik.

A professzionális hadsereg kialakítása során a szervezeti hatékonyság fokozása megköveteli a tartalékok feltárását és szelekcióját. Szervezeti oldalról:

- a professzionális értékek irányába fejlődő honvédségben a szakmai képességek gondozása, fejlesztése stratégia feladattá válik. A szakmai hozzáértés és felkészültség, valamint a hozzájuk kötődő képes-

ségek lesznek azok, amelyek az előrejutás és az ezzel párhuzamosan zajló szelekció alapját biztosítják;

- a honvédség szociális okok alapján nem folytathatja az intellektuálisan vagy képességeikben lemaradók foglalkoztatását, ugyanis ezzel növeli mások terhelését, csökkentve így fejlődésük esélyét, illetve rontva az alkalmazás feltételeit. A munkaerő szelekciója kiterjed az ismeretek, képességek, készségek területére;
- a kiválás szelekció útján történő biztosítása szervezeti kényszer lesz;
- az állománytáblák és munkaköri jegyzékek „zártsága", a helyettesíthetőség csökkenése, az ehhez alkalmazkodó munkarend megnehezíti a tartós vezénylést, ezért a továbbképzések tekintetében megnő a távoktatás, az önképzés és a folyamatos tanulás szerepe;
- a katonai szakmai specifikáció és a honvédség több területre kiterjedő munkaerő szükséglete a legtöbb területen nem teszi lehetővé alapképzés szervezését, ezeken a területeken a pályázati vagy más úton megvalósuló átképzés szerepe nő meg;
- a hadsereg átalakulása felveti új „szakmák" feltárását, leírását és az ezekre történő felkészítés megszervezését, ugyanis a gyorsan változó területekre az Országos Képzési Jegyzékben elfogadott szakmák nem adnak releváns ismereteket;
- a megrendelői igények gyors változása megnöveli az alkalmazók és a képzést végzők együttműködésének szerepét és jelentőségét;
- a technikai eszközök erkölcsi kopását és amortizációját a jövőben sem fogja automatikusan követni a hadrendből történő tömeges kivonásuk, ezért az új helyzethez történő alkalmazkodás, a jövőre történő felkészülés érdekében a honvédség hadrafoghatóságát növelő tényező lesz az állomány intellektusának, felkészültségének növelése, különös tekintettel arra, hogy a koalíciós együttműködés keretei között az új eszközökhöz szükségszerűen közel kerül az állomány egy része;
- a felkészítés és átképzés igénye ma a vezetés, az együttműködés, a szervezeti kommunikáció és az ezt biztosító informatikai és nyelvi területeken a legnagyobb.

A katonai hivatás gyakorlása oldaláról:

- előtérbe kerül a „tudásmenedzsment" speciális katonai formációja, mint a várható átalakulásra történő felkészítés teoretikus bázisa azért is, mert a hadseregek közvetlen alkalmazása helyébe egyre inkább új szervezeti funkciók kerülnek, és ezen ismereteket előre tekintve, jövőorientáltan kell fejleszteni;
- megjelenik az a kulturális dimenzió, amely egyrészt más nemzetiségűekkel történő együttműködésben, másrészt idegen (külföldi) kö-

zegben végzett munkában jelenik meg - az új szituáció új magatartásformákat vár el;

- előtérbe kerülnek az együttműködésre, a csoportos feladatmegoldásra és a kommunikációs képességekre épülő, a szervezeti magatartás területéhez tartozó viselkedésmódok, amelyek a katonai szakma új erőforrásait tárják fel.

A szervezeti változások és az IKT rohamos fejlődése következtében átalakul a képzés eszközrendszere, módszertana és didaktikája:

- a képzésre fordítható költségek és az oktatók terhelhetőségének korlátjai, a helyettesítés nehézségei miatt csökken az összevonások, a hosszú idejű beiskolázások aránya, megnő a távoktatás, a konzultációk, az önképzés szerepe;
- a távoktatás és az önképzés megkövetelik a korszerű információhordozók és oktatástechnikai eszközök kidolgozását és alkalmazását, a multimédia szakmódszertanba illesztését, és a tananyagok hálózaton keresztül a felhasználók igényei szerinti hozzáférhetőségének biztosítását;
- megnő a „csapatelőadók" szerepe, különösen a gyakorlati foglalkozások szervezésében és vezetésében. Mindenképpen célszerűnek látszik egy tutori/mentori hálózat kiépítése;
- felmerül - különösen vezetői és kis létszámú szakmai beosztások esetében - a személyes, egyéni felkészítés igénye;
- a rövid időigényű és széles körre kiterjedő továbbképzések megkövetelik egy mobil és rugalmas továbbképzési rendszer személyi és technikai kialakítását, melyben vagy az oktatókat kell mozgatni meghatározott feladatok érdekében, vagy virtuális képzési központokon keresztül kell biztosítani a(z) (ön)képzést. Ez feltételezi az alakulatok tantermi/informatikai ellátottságának biztosítását és fejlesztését;
- az IKT eredményeképpen kialakul és rohamosan fejlődik a virtuális tanulási környezet. Az oktatás új paradigmája a hatékonyság: kit, mennyi idő alatt, mennyiért juttatott adott ismerethez, mely azonnal alkalmazható a munkahelyen;
- a haditechnikai eszközök ára és a legtöbb eszköz mennyisége kizárja, hogy a tanintézetek oktatási célra kapjanak belőlük, ezért az elméleti és a gyakorlati képzésben megnő a külföldi és a csapatfelkészítés szerepe. Ennek hatékonyságát és az ismeretek szinten tartását segíti a hazai tanintézetek és csapatok közötti együttműködés fejlesztése, az elméleti és a gyakorlati képzés összehangolása;

Az oktatás (felsőoktatás) átalakulásának nemzetközi tendenciája, működési feltételeinek alapvető módosulása várhatóan hatással lesz a hazai viszonyokra is. A változások iránya:

- strukturális területen:
  - módosul a termelői és a szolgáltatói szféra aránya,
  - növekszik a szolgáltatás és a kis szervezetek jelentősége,
  - terjednek a környezet-, energia- és anyagkímélő technológiák,
  - az államé mellett jelentősen nő a piac szerepe,
  - verseny alakul ki az oktatásban.
- tartalmi kérdésekben:
  - változnak a szakemberekkel kapcsolatos igények,
  - nő a gazdasági, gazdálkodási, menedzseri ismeretek iránti igény,
  - felértékelődik a kommunikációs készség (idegen nyelven is),
  - nemzetközi szereplésre kell szakembereket képezni,
  - fel kell készülni az egész életen keresztül tartó tanulásra.

Ezek a társadalmi hatások teljes terjedelmükben és hatásukban felerősödve jelennek meg a katonai felsőoktatásban. Már ma is jelentős lemaradásunk van ezeken a „relatíve" új területeken. A civil egyetemek létrehozták továbbképző központjaikat, ezek intenzíven dolgoznak az új módszerek elterjesztésén. A külföldi tőke is megjelent az oktatási piacon (OMEGAGLEN; EUROCONTACT, EDE Hungary, …). A versenyt a társadalmi-gazdasági változások várhatóan tovább fogják élezni.

ÖSSZEFOGLALÁS

A Magyar Honvédség korszerűsítése, a professzionális hadsereg kialakítása az állomány ismereteinek folyamatos frissítését követeli meg. A rendelkezésre álló pénz- és anyagi eszközök mennyisége, az oktatás személyi feltételeinek és infrastruktúrájának koncentráltsága, a speciális katonai-szakmai ismeretek iránti követelmények és az alacsonyabb létszámból eredő nehéz helyettesíthetőség miatt a hagyományos, tanfolyamrendszerű, 'bentlakásos' képzési formák aránya várhatóan jelentősen csökkeni fog akkor, amikor a szervezett át- és továbbképzések iránti igény erőteljesen megnő. A hagyományos képzés ennek a kihívásnak nem tud megfelelni, ezért a Magyar Honvédség részére szükségszerű az új tanítási/tanulási módszerek, eszközök és médiumok bevezetése és elterjesztése. A korszerű információs és kommunikációs rendszerekre épülő távoktatási rendszer nemzetközi és hazai téren egyaránt bizonyította, hogy az általa adott relevancia, minőség, kiegyenlített tartalom és színvonal, magas költséghatékonyság és az otthoni, rugalmas tanulás lehetősége biztosítja a szükséges ismeretek megszerzését és folyamatos frissítését, a tanulást a kényszerből az emberek mindennapos tevékenységévé, az életforma szerves részévé alakítja át.

FELHASZNÁLT IRODALOM

1. Lajos Tamás: Informatika a nyitott és távoktatásban. Informatika a felsőoktatásban konferencia, 1996.
2. Műegyetem 2000 konferencia 1999.január 20-21, BKE Digitális Gyorsnyomda, Budapest, 1999.
3. Informatika a felsőoktatásban ’99**,** Debrecen, 1999. augusztus 27-29. konferencia előadásai:
4. Kis-Tóth Lajos: Az információrendszerek (IS)/információtechnológiák (IT) fejlődési korszakainak tükröződése a tantervekben
5. Nagy Ádám: Információs írástudás és informatikai intelligencia – az informatika-oktatás para-digmaváltásai Magyarországon
6. Dr. Magyar Gábor: Plug&Play? Paradigmaváltás az informatika oktatásában
7. Dr. Kormos János – Dr. Juhász István: Informatika= …? Tudjuk vagy oktatjuk?
8. Csibor Zoltán: Klasszikus oktatás, kontra eredményesség, hatékonyság, gyakorlatiasság
9. Havass Miklós: Paradigmaváltás a felsőoktatásban
10. Online irodalom:
11. Nyíri Kristóf: Globális tanulás és helyi közösségek
12. www.mtsystem.hu/uniworld2/course/unit1
13. Nyíri Kristóf: Nyitott és távoktatás – történeti nézőpontból
14. www.mtsystem.hu/uniworld2/course/unit2
15. Frank Tibor: Az egyetemi hagyomány védelmében: ellenérvek és ellenérzések
16. www.bme-tk.bme.hu:
17. Quentin Whitlock-Zarka Dénes: Kötetlen és önálló tanulás a szakképzésben
18. Claudio Dondi: Az ODL fő európai trendjeinek alkalmazása a képzési szektorban.
19. Janet Jenkins: Megjegyzések A nyitott szakképzés lehetőségei Magyarországon című jelentéshez

Egri Gábor

PROJEKTEK A BELÜGYMINISZTÉRIUMBAN

1. A projekt fogalom értelmezése:

Mielőtt összeütközésbe kerülnék különféle diszciplínák (közgazdaságtan, vezetéselmélet stb.) projekt definícióival, elöljáróban a projekt fogalmát csupán értelmezem, valószínűleg jelentősen egyszerűsítem és szűkítem. A jelen tanulmány szemszögéből a projektet természetesen **távközlési, informatikai** (vagy mai terminológiával élve **telematikai**) tárgyúnak tekintem, amely a Belügyminisztérium alárendeltségében valamilyen **folyamat** eredményeképpen valósult meg.

Ezek a folyamatok valamilyen stratégiai célkitűzés megvalósítására irányultak, amely célokat a dolgozat további részében mutatom be. Ezeket a folyamatokat időben is korlátozva tekintem át. A gyökereket ugyan a ’60-as, ’70-es évekre vezetem vissza, azonban az elemzés a rendszerváltás utáni évekre fókuszál.

2. A BM távközlő rendszerének múltbeli gyökerei, kialakulása

A BM távközlő rendszerének kialakulását nem lehet az ország távközlési infrastruktúrájától elválasztva értelmezni. Mivel a nemzetgazdaság távközlési szektora a ’60-as évekre az európai átlagtól jelentősen (becslések szerint cca. 20 évvel) lemaradt, a belügyi ágazat ilyen irányú igényeit fokozott fejlesztésekkel kellett kielégíteni. Ezek eredményeképpen az akkori BM távközlési infrastruktúra a ’70-es, ’80-as évek fordulójára az ország színvonalát jelentősen meghaladta. (Ez a megállapítás egyébként többé-kevésbé a honvédelmi ágazat területére is igaz.)

Ekkor jött létre a BM országos távbeszélő távhívó hálózata, amely az akkori európai átlagtól abban az időben alig tért el. Ebben az időszakban épült ki az országos rádió hálózat, a budapesti és vidéki felügyeletes és felügyelet nélküli objektumok rendszere.

Ez az infrastruktúra a ’90-es évekig (egyes elemei még napjainkban is) megbízhatóan üzemelt, azonban a rekonstrukció igénye elengedhetetlenül megjelent.

A rendszerváltást közvetlenül megelőző időszaktól kezdődve az ország távközlése ugrásszerű fejlődésnek indult. Ennek eredményeképpen a ’90-es évek közepére e téren kínálati piac alakult ki, sőt Magyarország a mobil távközlés (GSM) valamint a piac-konform hírközlési szabályozás terén semmiképpen sem szégyenkezhet.

Ezek az okok vezettek alapvetően ahhoz, hogy a belügyi távközlési infrastruktúra rekonstrukciója elinduljon.

3. Projektek a Belügyminisztériumban

A BM és a felügyelete alá tartozó szervezetek projektjei közül (valószínűleg önkényesen) csupán az általam jobban ismerteket és jelentősebbnek gondoltakat sorolom fel. Ezeket is elsősorban a megvalósításhoz szükséges források biztosítása, valamint a legfőbb felhasználók szerint csoportosítom.

Ezek szerint távközlési projektek valósultak meg a

a. BM központi
b. rendőrségi
c. határőrségi kereteken belül.

(A Tűzoltóság és Polgári Védelem - jelenleg összevontan Katasztrófavédelem - ilyen célú, elsősorban rádiós projektjei a tanulmány keretei miatt maradtak ki.)

a. BM központi projektek:
   - távbeszélő hálózat kapcsolástechnikai rekonstrukció főgyűjtő gócközponti sík; gyűjtő-gócközponti, valamint gócközponti sík, közösen a rendőrséggel;
   - gerinchálózati rekonstrukció részben közösen a rendőrséggel;
   - digitális rádiórendszer rekonstrukció előkészületek, közösen a BM alárendelt , valamint a potenciális társ-felhasználó szervekkel;
   - okmányirodai hálózat távközlő rendszere;
   - ATM kísérlet.

b. Rendőrségi projektek:
   - RIK székház létesítéséhez kapcsolódó távközlési rendszer;
   - távbeszélő hálózat digitalizálása: a.) rendőrkapitányságí szint; b.) góc- és gyűjtőgóc központi szint, közösen a BM központi igazgatással;
   - budapesti és megyei rádiórendszerek korszerűsítése (EDACS és szinkron rendszerek);
   - országos adatátviteli hálózat kiépítése.

c. Határőrségi projektek
   - távbeszélő hálózat és kapcsolástechnikai rekonstrukció;
   - határőrizeti rádió rekonstrukció;
   - határregisztrációs rendszerhez kapcsolódó adatátviteli és infrastruktúra rekonstrukció.

4. Távlati célkitűzések

Az előzőekben felsorolt és megvalósított projektek a rendszerváltozást követő évtizedben jelentősen átalakították a belügyi távközlési infrastruktúrát. Ennek során a demokratikus intézményrendszernek megfelelően a távközlést, mint szolgáltatást igénybevevők köre decentralizálódott, jelentős önállósággal bíró rendvédelmi szervezetek épültek fel. Ehhez igazodóan alakultak ki a belügyi távközlési rendszert üzemeltető szervezetek, ugyanakkor a műszaki sajátosságoknak megfelelően egységes rendszer jött létre. E folyamatnak olyan jellemzői is dominálnak, mint a digitális jelleg uralkodóvá válása, valamint a konvergencia különböző aspektusai (lásd a 2000. évi "A kommunikáció (híradás) helye és szerepe a vezetés rendszerében" című országos tudományos konferencián elhangzottak.)

Ezeknek megfelelően a BM telematikával foglalkozó szervezetei a BM informatikai stratégiájának megfelelően folytatják tovább az egységes belügyi digitális hálózat (EBDH) kiépítésére irányuló munkájukat. Ennek nagy forgalmat lebonyolító szegmenseiben távlatilag az ATM technológia alkalmazását tűztük ki célul. Az EBDH-t, mint hordozó hálózatot figyelembe véve olyan komplex alkalmazásokat kívánunk teljes körűen bevezetni, mint a Robotzsaru információs rendszer, továbbá az okmányirodák országos hálózatának kiszolgálása. A készenléti illetve rendvédelmi szervek sajátos mobil távközlési igényeinek kiszolgálására egységes digitális trönkölt rádió rendszer (EDTR) kiépítését illetve alkalmazását tűztük ki célul. Ennek elérésére műszaki, alkalmazási kísérleti rendszert építettünk ki, digitális rádiós technológiákat vontunk elemzés alá, továbbá a politikai döntéshozók számára megfelelő információt biztosító előterjesztéseket dolgoztunk ki a kormányzat egyéb illetékes szerveivel együttműködve.

5. Következtetések

A belügyi távközlési infrastruktúra elmúlt évtizedes rekonstrukciós tevékenységei következtében a folyamatosan bővülő igényeket mind magasabb színvonalon kielégítő országos rendszer épült ki. Ez a rendszer érvényesíti a szervek önállósságára épülő műszaki- tartalmi egységesség szempontjait a hatékony forrás-felhasználás érdekében.

Ezen infrastruktúrán alapulva a belügyi ágazat szakmai szervezetei munkavégzésük során mind jobban tudják érvényesíteni a demokratikus társadalmi berendezkedés által elvárt **szolgáltató állam** funkció maradéktalan kibontakozását.

Dr. Töltési Imre

NEM BESZÉD ALAPÚ SZOLGÁLTATÁSOK A KÉSZENLÉTI TETRA RENDSZERBEN

A készenléti TETRA rendszer beszédalapú szolgáltatásai ma már széles körben ismertek a potenciális felhasználó körében. Talán kevesebb nyilvánosságot kaptak eddig a TETRA rendszer más, elsősorban adatátviteli szolgáltatásai. Ezek nagymértékben képesek megkönnyíteni a felhasználók munkáját, gyorsabb, pontosabb információátvitelt tesznek lehetővé. Előadásomban ezek a lehetséges alkalmazásokat kívánom ismertetni.

1. Műszaki megvalósítás

1.1 Átviteli rendszer

A szolgáltatások a TETRA rádióállomásokhoz csatlakoztatott intelligens végberendezések és egy vagy több központi diszpécser állomás közötti, kliens-szerver rendszerű adatcserén alapulnak. Az adatok továbbítási módja szerint kétféle megvalósítás lehetséges.

Általános esetben jól alkalmazhatóak a tárol és továbbít elven működő, GSM hálózatokban elterjedten használt SMS üzenetekhez hasonló rendszerek. Az adattovábbítás a jelzésátviteli csatornán zajlik, külön időrést nem igényel. Ez az átviteli mód az adatátviteli csatorna felépítéséhez képest több szempontból előnyös:

- Gyorsabb, nem szükséges minden egyes adat továbbításához (akár percenként) a teljes hívásfelépülést kivárni.
- Sávtakarékos. A jelzésátviteli csatorna átviteli kapacitása nagyszámú kapcsolat kiépítését teszi lehetővé, az adatforgalom miatt nincs szükség a bázisállomások kapacitásának növelésére.
- Ha a diszpécser központ éppen nem tudja fogadni az üzenetet, a rendszer tárolja azt. A központokban ezért nincs szükség nagyszámú fogadó vonal kiépítésére, hiszen a foglaltság és ütközések problémáját a TETRA rendszer kezeli.
- A GSM rendszerben szerzett tapasztalatok alapján, az így felépülő rendszer üzemeltetése olcsóbb.

Egyes kritikus, adatgyűjtési és vezérlési alkalmazásoknál azonban nem engedhető meg az üzenetek késése, valós idejű kapcsolat és azonnali beavatkozási lehetőség szükséges. Ezekben az esetekben az információ továbbítása valósidejű adatátviteli csatornán valósítható meg. Ilyenkor a diszpécser központ kapacitását is e követelményeknek megfelelően kell kialakítani.

1.2 A végberendezések

A Tetra rádiókhoz csatlakoztatható ipari kivitelű számítógépet tartalmazó egység. Általában többfeladatos, feladatorientált operációs rendszerrel rendelkezik, programozható. A terminálhoz sokféle adat be- és kiviteli eszköz csatlakoztatható:

- képernyő,
- GPS vevő,
- billentyűzet,
- mérőegységek (hőmérséklet, sebesség, feszültség, áram, stb.),
- nyomtató,
- érintkezők állapotának beolvasása, ezek vezérlése,
- vonalkód olvasó,
- RS-232 csatlakozó felülettel rendelkező bővítő eszközök
- tároló egység
- mikrofon.

1.3 A központ

Egy kommunikációs és alkalmazás szerverként működő számítógép. Hálózatba köthető, az adatok és a kommunikációs kapcsolat megoszthatók.

Az alkalmazás szerver főbb funkciói:

- a kliensektől érkező kérések végrehajtása, illetve továbbítása a diszpécser felé, és viszont;
- kapcsolat teremtése az intézmény máshol tárolt adataihoz, bennük adatbázis műveletek elvégzése, a végberendezések vagy a diszpécsertől jövő igények alapján;
- térképkezelés;
- a végberendezések technikai jellegű adatainak kezelése, működésük ellenőrzése, vezérlése;
- hozzáférési jogosultságok kezelése, adminisztráció, naplózás.

Az alkalmazásszerver szolgáltatásai többféle távközlési rendszeren válhatnak elérhetővé. A végberendezések felé a TETRA mellett, egyidejűleg működhetnek más elérési utak is (GSM, rádió modemek, vezetékes távbeszélő vonalak, stb.). Egyszerűbb alkalmazásoknál a diszpécser dolgozhat magán a szerver feladatokat ellátó számítógépen, de gyakrabban szükség van önálló munkaállomás(ok) használatára. A szerver elérése ilyenkor helyi számítógép hálózat segítségével valósul meg, de az adatok megoszthatók akár az Interneten is.

Ezeknek a távközlési kapcsolatoknak a kezelése a kommunikációs szerver feladata. A rendszer akkor tekinthető kellően rugalmasnak, ha a mennyiségi bővíthetőségen túl moduláris felépítésű, így szükség esetén egy-egy új távközlési móddal (pl. GSM után TETRA-val) való bővítése is megoldható, ehhez az alkalmazás szerverben és a diszpécser programban csak minimális kiegészítések válnak szükségessé.

1.4 Diszpécser munkaállomás

A futtatott alkalmazások függvényében sokféle kialakítású lehet. Fő feladata a szöveges vagy grafikus adatok megjelenítése, hatékony és felhasználóbarát munkakörnyezet teremtése a diszpécser számára. Lényeges, hogy az adatbevitel rendje és a kimeneti dokumentum formátumok megfeleljenek az intézmény meglévő ügyviteli rendjének.

2. Alkalmazások

A rendszer által nyújtott szolgáltatások az alábbi alapvető csoportokba oszthatók:

2.1 Formalizált vagy szabadon összeállított üzenetek küldése.

A diszpécser központ és a tagállomások közti üzenetek jelentős része gyakran ismétlődő, szabvány üzenet. Ezek továbbítása feleslegesen növeli a forgalmat és megakadályozhatja esetleg fontosabb beszédkapcsolat felépülését. A gyakran ismétlődő üzenetek kód formájában egy gombnyomásra továbbíthatók. A képernyőn ebben az esetben is természetesen az üzenet szövege jelenik meg.

A szabad szövegezésű üzeneteknél pedig lényeges, hogy ezek írásos formában jelennek meg a képernyőn, később is visszakereshetőek, többször elolvashatóak, kizárva ezzel a félreértést. Hosszabb, bonyolultabb adatok (név, lakcím, rendszám, stb.) továbbításakor a szöveges továbbítás jelentősen csökkenti a diszpécser és a vonal foglaltságát.

Az üzeneteket a rendszer napló állományban rögzíti. A napló tartalmazza a küldés és a vétel időpontját, mobil állomásnál a földrajzi pozíciót is.

Lehetséges felhasználás:

- bevetés irányítás, diszpécser szolgálat;
- kapcsolattartás;
- flottavezérlés.

2.2 Térinformatikai alkalmazások

A térinformatikai alkalmazások lehetővé teszik a grafikus információk és szöveges adatbázisok egységes rendszerben való kezelését. Az állandó adatok megjelenítése mellett műholdas navigációs vevő használata esetén lehetséges a tagállomások helyzetének akár valósidejű megjelenítése. A pozíció küldése történhet automatikusan, beállított időközönként vagy riasztási jelként feltételhez kötötten, valamilyen esemény bekövetkeztekor (adott körzet, útvonal elhagyása, ajtónyitás, megállás, megindulás, stb.). A pozíció tetszés szerinti időben lekérhető a központból is.

A térképen megjelenő grafikus objektumok közvetlenül kapcsolódnak a szöveges adatbázishoz, és viszont. Az objektumra kattintva például azonnal megkaphatjuk a járőrkocsi személyzetének nevét, jelenlegi feladatát, a nekik küldött üzeneteket, egy mozgó csoport felszereltségét, a mentőautó által szállított beteg nevét, úti célját, a kórházak szabad ágykapacitását, egy

szállítmány összetételét, baleset esetén az adott szállítmány mentéséhez szükséges anyagokat és eszközöket, valamint ezek telepítési helyét a térképen.

Lehetséges felhasználás:

- bevetés irányítás;
- jármű követés;
- veszélyes szállítmányok ellenőrzése;
- betegszállítás;
- erőforrás, készlet nyilvántartás és optimalizálás, logisztikai feladatok.

2.3 Hozzáférés központi adatbázisokhoz.

A rendszer lehetővé teszi, hogy a felhasználók a terepről, jogosultságuknak megfelelően elérjék a szolgálatok központi adatbázisait, lekérdezéseket, adatmódosításokat hajtsanak végre. Egyes esetekben szükség lehet egyéb elektronikus információforrások elérésére is, például javítási, szerelési utasítások, műveleti, intézkedési sorrendek, stb.

Lehetséges felhasználás:

- okmányellenőrzés (szig., vezetői engedély, útlevél, forgalmi engedély, stb.),
- gépjármű ellenőrzés,
- körözési listák,
- ujjlenyomat azonosítás,
- veszélyes anyagok kezelésére vonatkozó biztonsági, mentesítési szabályok,
- közmű adatok,
- szakértői címjegyzék,
- riasztási, ügyeleti listák.

2.4 Mérési adatgyűjtés, érzékelés, távvezérlés.

A végberendezések képesek különböző érzékelők, mérőegységek adatainak továbbítására, technikai eszközök, gépek ki/be kapcsolására, távvezérlésére, működési paramétereik továbbítására.

Lehetséges felhasználás:

- mérő, észlelő hálózatok adat és vezérlő jeleinek továbbítása (sugárszint ellenőrzés, meteorológiai adatok, stb.),
- bonyolult vezérlőrendszerek átkonfigurálása (pl. közlekedési lámpák),
- őrzés-védelmi rendszerek, behatolás jelzők riasztási jelzéseinek továbbítása,
- tartalék berendezések, rendszerek aktivizálása (áramfejlesztők, szivattyúk, távközlési berendezések, stb.).

2.5 Elektronikus okmánykezelés.

Az informatika fejlődésével a papír alapú okmánykezelést egyre inkább kiszorítja az elektronikus továbbítás és feldolgozás. A rendszer lehetőséget ad arra, hogy az elektronikus okmánykezelés határai kiterjeszthetőek legyenek

akár a Tetra végberendezésekig is. Nagyon lényeges, hogy az adatokat keletkezésük helyén, azonnal digitálisan rögzítsük. Ezzel elkerülhető a felesleges és drága ismételt adatbevitel és az ezzel járó hibalehetőség is.

Csomagok, okmányok, egyéb tárgyak azonosítása, mozgásuk nyomon követése a vonalkód olvasóval kiegészített terminálról könnyen megvalósítható.

Lehetséges felhasználás:

- jegyzőkönyv felvétel, elektronikus űrlapok kitöltése (baleseti helyszínelés, betörés egyéb események helyszínen történő rögzítése, elektronikus menetlevél kezelés stb.);
- szállítmányok, tárgyak azonosítása;
- fuvar és vámokmányok kezelése;
- értékes, nyilvántartott küldemények követése átadás- átvételének elektronikus bizonylatolása (futárszolgálat).

3. A fejlesztés jelenlegi helyzete

Cégünk a Carinex Kft., mint alkalmazásfejlesztő, és az i-Cell Kft., mint rendszerintegrátor, a Belügyminisztérium támogatásával és koordinálásával, a NOKIA és az Antenna Hungária Rt. részvételével, 1999. tavaszán azzal a céllal kapcsolódott be a TETRA rendszer és eszközök magyarországi tesztjébe, hogy a hangátvitel mellett, a szükséges magyar fejlesztések integrálásával bemutassák a TETRA rendszer és eszközök újabb alkalmazási lehetőségeit. A pilot projekt során sikerrel mutattunk be az érdekelt készenléti szolgálatok képviselői részére távoli adatbázisok elérését, térinformatikai feladatok megoldását és mérési feladatok elvégzését TETRA hálózaton keresztül. A kialakított rendszer előnye, hogy felhasználói felülete teljes egészében magyar fejlesztés, illeszkedik a felhasználó igényeihez, jelenlegi ügyviteli előírásaihoz és okmányaihoz, valamint az alkalmazás eltérő, egyidejűleg akár többféle távközlési hálózaton is megvalósítható.

A szolgáltatás lehetőséget teremt arra, hogy mind a szöveges, mind az írott vagy elektronikus formában jelen lévő információt ugyanazon a robosztus felépítésű távközlési rendszeren ellenőrzött, naplózott módon továbbítsuk, és adatok bevitelét (digitalizálását) az informatikai rendszerbe közvetlenül azok keletkezési helyén végezzük el. Az információk bináris formában történő továbbításával jelentősen csökkenthető a beszédcsatornák terheltsége, elkerülhető a szóbeli közlemények félreérthetősége és ismétlése. E megoldás természetesen lehetővé teszi az adatok megosztását a belső számítógép-hálózaton vagy akár az Interneten keresztül is.

Pándi Erik

KORMÁNYZATI TÖREKVÉSEK VÁRHATÓ HATÁSA A VÉDELMI JELLEGŰ KOMMUNIKÁCIÓS RENDSZEREK FEJLESZTÉSÉRE

I. Az információs társadalom államigazgatási kihívásaival összefüggő kormányzati és ágazati szerepvállalás alakulása

A XX. század utolsó harmadának globalizációs folyamatai, a távközlés területén végbemenő és prognosztizálható fejlődés, a szolgáltatások és technológiák integrációja, az informatika, a távközlés egyre szorosabb összekapcsolódása hazánk kormányai számára is egyértelművé tették, hogy a hírközlési infrastruktúra nemzetgazdasági és társadalmi jelentősége egyre meghatározóbb lesz a XXI. században. Ma már az oktatás, a kereskedelem, az ipar, az államigazgatás és a háztartások működésének nélkülözhetetlen része a telekommunikáció és annak bázisán megvalósuló integrált információs infrastruktúra. Felmérések alapján a hazai távközlési piac teljes liberalizációja további befektetéseket eredményez a hírközlés, ezen belül főleg a távközlés területén.

Jelen kormányzati ciklus kezdetén a Miniszterelnöki Hivatal által tanulmány került publikálásra az információs társadalom problematikájával kapcsolatban. A kidolgozásban részt vállaló szakértői csoport a *„szolgáltató állam és közigazgatás”* megteremtése érdekében történő **informatizálás** jelentőségét az alábbiakban fogalmazta meg:

- az állam, mint a társadalom aktív szereplője – *végrehajtva és biztosítva közigazgatási funkcióit* – saját hatékonysága érdekében **alkalmazza** az informatikát;
- az állam, mint a demokrácia és az alkotmányos állampolgári jogok fenntartója igyekszik **létrehozni** az állampolgári és regionális esélyegyenlőséget;
- az állam, mint a jövőt meghatározó információk birtokosa és mint aki a stratégiai elemzésekre képes intézményrendszerrel rendelkezik irányítólag **befolyásolja** az információs társadalom kialakulásának feltételeit.

Ahhoz, hogy a közigazgatás elősegítse a jobb társadalmi integrációt, szolgáltatásaival, illetve az általa gyűjtött és prezentált adatokkal egyenlő esélyeket biztosítson állampolgárai számára magának is változónak kell lennie, melyhez többek között:

- hatékonyan kell működnie, azaz szervezetében és eljárásaiban átlátható kell lennie, gyorsabban és olcsóbban kell megbízható adatokat és szolgáltatásokat nyújtania;

- tevékenységét úgy kell végeznie, hogy nyilvános szolgáltatásai széles körben és univerzálisan hozzáférhetők legyenek miközben biztosítja a megfelelő jogi biztonságot és garanciákat.

Fenti gondolatokból kiindulva a kormányzat stratégiai célként tűzte ki a ***papír nélküli közigazgatás***, az ***egy ablakos ügyintézés***, a ***közösségi építkezés*** és az ***elektronikus állampolgári konzultáció*** megteremtését.

A papír nélküli államigazgatás kapcsán elérendő célként fogalmazódik meg a kormányzat és a közigazgatás információs munkájának digitális alapon történő megszervezése, mely során a minisztériumok, hivatalok, valamint azok adatbázisai – *elsődlegesen az alapadatbázisok* – összekapcsolásra kerülnek. Az így kialakított integrált adatbázisokkal megoldhatóvá válik a kormányzati és önkormányzati információk egymáshoz kötése. Az egy ablakos ügyintézés műszaki koncepciója szerint az alapadatbázisok felhasználásával az állampolgár és az államigazgatás közötti kapcsolat interaktívvá tehető, így oldva meg a komplex ügyintézéssel kapcsolatos elvárásokat. A tanulmányban a közösségépítés tartalmazza mindazon elképzeléseket és gondolatokat melyek felhasználásával a jövő állampolgári- és önkormányzati információs hálózatainak kialakítása megkezdhető.

A MEH-tanulmány kiemelkedő fontosságúnak értékeli a hozzáférés és zavarérzékenység minimalizálásának kérdését. Elgondolás szerint a jelen évszázadra tervezett szolgáltató-típusú kormányzati munka egyre inkább függeni fog a felhasznált információs rendszerek mennyiségi és minőségi mutatóitól, melyek sérülékenységének mérséklésére teendő intézkedések a jövőben várhatóan összemérhetők lesznek a **honvédelmi, nemzet- és közbiztonsági** erőfeszítések jelentőségével és – *azok financiális* – nagyságával.

A technológiai fejlődés folyamán az elektronikus adatbázisok, az informatikai rendszerek közti kapcsolódási felületként – *magától értetődően* – jöttek számításba a meglevő, hagyományos távközlési infrastruktúrák, mivel azok elterjedtsége, illetve műszaki paraméterei felhasználhatónak bizonyultak az integrációs folyamatok megvalósítására. Természetesen ehhez nagymértékben járult hozzá a korszerű programvezérlési eljárások és technikák meghonosodása a távközlés területén.

A XX. század utolsó évtizedében, a megnyíló piacok hatására hazánkban is megfigyelhető volt a távközlés egészében végbemenő, viszonylag gyors technológiai ugrás. Miután, azonban Magyarország 1990. előtti távközlési infrastruktúrájában jelentős technológiai színvonalat képviseltek az államigazgatási igényeket kiszolgáló (zártcélú) hálózatok (közigazgatási „K” távbeszélő-, ALTÁJ rádiótelefon-, BM és HM állandó hírrendszer, K-600, stb.), így azok többsége a ’90-es évek jogszabályi felhatalmazása révén jelenleg is funkcionál, bár a mindenkor rendelkezésre álló beruházási keretek csak viszonylag lassabb fejlesztési ütemet engednek meg e rendszerek átalakítása tekintetében. A meglevő zártcélú kommunikációs infrastruktúrák továbbfejlesztésére, fenn-

tartására és üzemeltetésére több elgondolás született, illetve ezzel kapcsolatosan vagy ezt érintően az elmúlt tíz esztendőben egy sor jogszabály került megalkotásra. Ezek közül a legjelentősebbek az 1992. évi LXXII., 1993. évi LXII., 1999. LXVI., 2001. évi XL., 2001. évi XXXV. törvények, a 17/1994., 50/1998., 75/1998., 95/1999., 100/2000., 122/2001., 131/2001., 151/2001. számú kormányrendeletek, a 1026/1992., 1039/1993., 1033/1994., 1071/1998., 1066/1999., 2146/1999., 2350/1999., 1075/2000., 1071/2001., 2050/2001. kormányhatározatok.

A problémák mellett azonban elmondható, hogy a védelmi jellegű távközlő rendszerekben az alapvető rekonstrukciós beruházások – *ágazatonként, elszigetelten* – végbementek, tehát a különböző távbeszélő központi síkok, illetve átviteli utak digitalizálása megtörtént, illetve újabb átviteli technológiák és szabványok kerültek rendszeresítésre, illetve állnak a bevezetés stádiumában (pl.: ISDN, valamint ATM és IP szabványok).

Összességében véve a kormányzati munkát elősegítő kommunikációs hálózatok száma jelenleg is magas szinten konzerválódott, és azok elsősorban a védelmi jellegű szervezetek (fegyveres erők, rendvédelmi szervek) fenntartásában vannak. A kilencvenes évek közepén már megfogalmazódott, hogy *„hosszútávon csak egy összevont, a kormányzat kommunikációs igényeit kiszolgálni képes, korszerű technológiai eljáráson alapuló, szintenként differenciált és védett rendszerrel”* kell számolni, melynek integrálnia kell a jelenlegi zártcélú hálózatok több alrendszerét is.

Ezen elvek alapján létesülő rendszer elsődleges minőségi követelményeként került megfogalmazásra, hogy minden időben és mindenhol biztosítania kell mind az országirányítás távközlési feltételeit, mind az Európai Unió, illetve NATO kormányzati és védelmi szervezeteivel történő kapcsolattartást.

Elmondható, hogy az államigazgatási igényeket kiszolgáló zártcélú távközlő hálózatok, illetve informatikai rendszerek fejlesztésével kapcsolatos elvi kormányzati akarat az elmúlt időkben mindig is támogatta a technológiai és szervezeti korszerűsítés megindítását e területen. A technológiai képességek változása azonban az elgondolásokat némileg módosították, így a két évvel ezelőtt napvilágot látott kormányhatározat (1066/1999.) az egységes kommunikációs rendszerek megszervezésének újszerű koncepcióját vázolta fel.

A határozat rögzíti a kormányzati szervek hálózati struktúrájának alapelvét, mely szerint az nem része a nyilvános rendszereknek, illetve a nyílt szabványú hálózati protokollok és alkalmazások segítségével lehetővé válik a belső virtuális hálózatok képzése is oly módon, hogy az átjárókon keresztül csak az engedélyezett kommunikáció valósul meg.

Összességében érzékelhető, hogy a zártcélú hálózatok alkalmazásával kapcsolatos nézetek elméleti síkon egy egységes, integrált rendszer irányába mutatnak, ugyanakkor a gyakorlati megvalósulást a különböző ágazati érdekek és lehetőségek – *úgy tűnik, hogy* – nem segítik kellőképpen, így az információs

társadalom államigazgatási kihívásaival kapcsolatos informatikai fejlesztések sem haladhattak megfelelően.

II. A kormányzati kommunikációs alaphálózat

Az 50/1998. számú kormányrendelet az X.400 kormányzati levelezőrendszer tekintetében – *az akkori* – Miniszterelnöki Hivatalt vezető államtitkárt nevezte meg hálózatgazdaként. E hálózat eredendő céljaként fogalmazódott meg, hogy gyors, elektronikusan feldolgozott adatok áramlásával segítse elő a végrehajtó hatalom különböző szintjei közötti munkafolyamatok hatékonyságának növekedését.

Az Internet térhódításával a fejlett országok közszférájában is egyre nagyobb ütemben terjed a munkafolyamatok gépesítése. Olybá tűnik, hogy az árban elérhető számítástechnikai eszközök kínálta lehetőségek terjedésével ma már a kormányzati munka sem képzelhető el elektronikus levelezés, internetes tájékoztatás nélkül. A gyors fejlődést mi sem bizonyítja, hogy ezen igények kielégítésére létrehozott budapesti hálózat napjainkra már képtelen a megfelelő átviteli kapacitásokat biztosítani.

Problémát jelent többek közt azon tény is, hogy a jelenlegi hálózati erőforrások nem biztosítják a több tárca munkáját érintő, jogszabályokban lefektetett határidejű alkalmazás-fejlesztési beruházások sikeres végrehajtását sem.

Az első fejezetben már említett szétaprózottság és nehézségek miatt az ágazati zártcélú hálózatgazdák számos, egymástól független, csak az adott igényeket kielégítő hálózatokat létesítették többnyire saját erőforrásaik terhére. Jelenleg hozzávetőlegesen 20 különféle, topológiáját tekintve hasonló információátviteli hálózat jött létre, melyek fajlagos fenntartási költségei magasabbak, mint egy önálló, jóideje áhított kormányzati rendszernek.

Hazánkban fenti célból, külön ágazati érdekek kiszolgálására létrejött rendszerek fejlesztésében és fenntartásában egyrészt a Belügyminisztérium, másrészt a Honvédelmi Minisztérium, valamint a K-600-as rendszert fenntartó KHVM (2000-től: MeH) jár élen.

Az egységes kommunikációs rendszer kialakításának sikertelensége a következő kettő lehetséges megvalósítási eljárások nem megfelelő végrehajtására vezethetők vissza:

a., az egyes tárcák által összeadható financiális és technikai erőforrásokat a különböző pénzügyi, szakmai, üzemeltetési érdekek miatt nem lehetett egyesíteni;

b., az országos államigazgatási magánhálózat kialakítása mögött nem sikerült megfelelő pénzügyi erőforrásokat felsorakoztatni.

Az elmúlt évtized sikertelen folyamatainak, valamint a távközlési szolgáltatói piac trendjeinek elemzését követően, a jogi-szabályozási oldalt módosításával a KHVM egyes feladatköreit átvevő MeH Informatikai Kormánybiztos-

ság központi finanszírozás mellett, előre deklarált célokkal meghirdette az Elektronikus Kormányzati Gerinchálózat (EKG) kialakítását.

III. Az EKG koncepció lényege és megvalósítása

A megépítendő országos rendszer nagysebességű kapcsolatot valósít meg a Budapesten található intézmények között, illetve a vidéki és budapesti közigazgatási szervekkel. A MeH elképzelése alapján a létesítés két fázisban, összesen fél éven belül megvalósulhat. A feszített ütem egyik oka, hogy a 2003. évre esedékes költségvetési tervezés megkezdése előtt világosan kell látniuk az érdekelt kormányzati szerveknek az EKG-be való becsatlakozásból megtakarítható beruházási keretek nagyságát. Másik ok lehet, hogy az országos alkalmazások fejlesztésénél már figyelembe vehető a központi adatbázisok felhasználásának gyakorlati lehetősége a megyei szinteken elosztottakkal szemben.

A terv megvalósításának érdekessége abban áll, hogy a budapesti és megyei végpontok tekintetében nagysebességű **bérelt vonali** összeköttetések épülnek ki, de néhány viszonylaton ezt a megoldást ki lehet váltani kormányzati tulajdonú és üzemeltetésű megoldásokkal.

A budapesti hálózat saját, illetve bérelt, optikai végződtető egységek nélküli átviteli utakból állna. Optimális esetben a hálózat saját tulajdonú, saját alépítményben levő optikai szálakkal valósul meg.

Az országos hálózat bérelt, nagysebességű SDH, ATM kapcsolatokból, illetve szintén optikai végződtető egységek nélküli optikai szálakból épülne fel.

Az EKG által felhasználható, illetve nyújtott szolgáltatások:

a., intézményi hálózatok logikai elkülöníthetősége;
b., szabályozott kommunikáció az egyes intézményi hálózatok között;
c., központilag biztosított biztonsági eljárások;
d., központilag biztosított, mérhető Internet hozzáférés;
e., szolgáltatásosztályok definiálása;
f, garantált sávszélesség egyes kiemelt alkalmazások felhasználásakor;
g., VoIP képesség kialakítása, többek közt a távbeszélő forgalom berendezésére;
h., multimédia jellegű szolgáltatások kialakítása

Az EKG összetevői:

a., saját tulajdonú aktív eszközök;
b., budapesti gerinchálózat;
c., országos gerinchálózat;
d., megyei üzemeltetési központok;
e., Internet kapcsolat;
f., üzemeltetési szervezet;
g., MeH központi felügyelet

Az EKG koncepciójának egyik célkitűzése, hogy a jelenlegi széttagolt, az egyes minisztériumok által üzemeltett eltérő minőségi paraméterekkel bíró hálózatok helyébe egy országos elérhetőséget biztosító, egységes gerinchálózat jöjjön létre. Az elgondolás megvalósítása során azonban figyelembe kell venni, hogy e struktúrába a közigazgatás legszélesebb körű szervezeti egységeit kell tudni bekapcsolni, illetve megfelelő szolgáltatási nívón kiszolgálni.

A MeH által készített előzetes felmérések szerint az egyes minisztériumi hálózatok sem technológiai, sem biztonsági, sem rendelkezésre állási tulajdonságaikat tekintve nem felelnek meg az egységes elektronikus kormányzat megvalósítását szolgáló kormányzati hálózattal kapcsolatban megfogalmazott követelményeknek, ezért az egységes gerinchálózat melletti fenntartásuk sem hatékonysági, sem gazdaságossági megfontolásokból nem indokolt. Tehát a központi akarat egyértelműen kinyilvánítja a különböző szervek **csatlakozási kötelezettségét**.

Természetesen kezdeti lépésben az 50/1998. kormányrendeletben meghatározott, védelmi, bűnüldözési, nemzet- és közbiztonsági érdekeket szolgáló szervezeteknek a csatlakozási kötelezettséget csak kinyilvánított szándék esetén lehet érvényesíteni.

Az EKG **üzemeltetését** a MeH elsődleges fontosságúnak tartja az elektronikus kormányzat megvalósítása kapcsán. A jövőbeni hálózat üzemeltetésével kapcsolatosan az alapvető követelmények az alábbiak:

a., biztosítani szükséges a rendszerben üzemelő eszközök megfelelő üzemeltetéséhez szükséges fizikai infrastruktúrát;

b., szaktudásban és létszámban megfelelő humán erőforrást kell koncentrálni

Miután a gerinchálózat összkormányzati érdekeket szolgál, ezért azt központi felügyelet és irányítás alatt (MeH, mint hálózatgazda) kell üzemeltetni. Elképzelések szerint egy kormányzati többségi tulajdonú gazdálkodási szervezet (kht., kft., rt.) megfelelően rugalmas és képes gyorsan reagálni a piaci változásokra. Természetesen ez a megoldás hosszútávon magában hordozza az államigazgatási informatikai tevékenységgel kapcsolatos feladatok ellátásának átadását is.

Az EKG kulcskérdése a vidéki központok kialakítása. A megyei központok a következő főbb feladatcsoportokat látnák el:

a., megyei hálózati eszközök üzemeltetése;
b., megyén belüli csatlakozási lehetőségek biztosítása;
c., távbeszélő útján történő behívási rendszer menedzselése;
d., folyamatos támogatás nyújtása a megyei felhasználók részére

Az utóbbi feladat kiemelt fontosságú a szolgáltatások minőségbiztosítása érdekében. A MeH egyértelműen a megyei Területi Államháztartási Hivatal (TÁH) szakembergárdájának segítségét kívánja igénybe venni, aki valószínűsíthetően már rendelkeznek megfelelő informatikai- és közigazgatási gyakorlattal, illetve helyi kapcsolatrendszerrel.

A megvalósítás konkrét költségei központi becslés alapján folyó évre **765 millió** Ft, 2002-re **695 millió** Ft körüli összeg, melyből összesen **400-500** millió Ft-ot tesz ki a MeH többségi tulajdonában levő gazdasági társaság üzemeltetése, valamint **245** millió Ft-ot a kétirányú Internet kapcsolatot biztosító, központilag kiválasztott szolgáltató bevétele.

IV. A rendvédelmi szervek és a fegyveres erők zártcélú hálózatait üzemeltetők és az EKG

Az előző fejezetekben elhangzott, hogy mind a katonai-, mind a rendvédelmi szervezetek kezelésében levő zártcélú hálózatok fordíthattak viszonylag nagyobb mértékű fejlesztési előirányzatokat rendszereik modernizálására. Talán ismeretes a távbeszélő technika alrendszerein kifejlődött számítástechnika egyre nagyobb mértékű térnyerése, így talán érthető, hogy a nagyobb, összetettebb távbeszélő struktúrákkal rendelkező szervezetek kezdték meg elsőként adathálózataik kiépítését.

A Belügyminisztérium (BM) középtávú informatikai és távközlési programja (1999-2002.) célul tűzi ki többek közt az Egységes Belügyi Digitális Hálózat végleges kialakítását. E koncepció keretén belül nemcsak a rendőri, hanem a határőr, a katasztrófavédelmi, valamint a belügyi szervek (pl.: Bevándorlási és Állampolgársági Hivatal, Központi Adatfeldolgozó, Nyilvántartó és Választási Hivatal) központi és területi szervei kerültek volna csatlakoztatásra a tervezett hálózathoz. Ezen elképzelés tartalmazza mind az adat, mind a hagyományos távbeszélő kapcsolatok biztosítását, mely alapvetően ATM alapú átviteli megoldásokat tartalmaz.

Jelenleg a BM a főváros viszonylatában jelentősnek mondható, saját optikai kábeles infrastruktúrával, illetőleg a megyei székhelyek irányába ugyancsak saját mikrohullámú átviteli utakkal rendelkezik. Mindkét esetben az üzemviteli feladatokat és a financiális kötelezettségek rendezését a BM szervek látják el. Természetesen a TÁH-k (korábban: TÁKISZ) BM alárendeltségből a Pénzügyminisztérium alárendeltségébe való, rövid idővel ezelőtti átadás-átvétele csökkentette a belügyi ágazat ellátásra kötelezetteinek létszámát, azonban nem oldódott meg a létező erőforrások egységesítésének problematikája, melyre a MeH valószínűsíthetően előre is számított. A BM mellett a Honvédelmi Minisztérium (HM) alárendeltségében működő szervezeteknél is jelentkezett mind a távbeszélő, mind az ezekhez csatlakozó átviteli technológiák korszerűsítésének szükségszerűsége, illetve a problémakör lezárásához vezető modernizálási folyamatok végrehajtása.

Visszatekintve a kormányzati (állami) érdekeket kiszolgáló kommunikációs rendszerek elmúlt évtizedben kiéleződött, azonban permanensen előtérbe kerülő – *együttműködés-, alkalmazás- és fejlesztésbeli* – problematikájára úgy tűnik, hogy a MeH magához ragadva a kezdeményezést idén hozzálát egy egységes hálózat azonnali kialakításához. Az alapot ehhez az elektronikus kormányzás mielőbbi bevezetésének időszerűsége (sürgető volta) adja, azonban úgy tűnik, hogy a kormányzat kevéssé kíván támaszkodni a védelmi jellegű kommunikációs hálózatokat fenntartó szervezetek meglevő infrastruktúráira és humán erőforrásaira, pedig elsősorban a BM által üzemben tartott kommunikációs rendszerek elhelyezkedése nagyjából fedi a közigazgatási egységek diszlokációját. Lévén, hogy bizonyos szempontból a belügyi szervek a közigazgatás részének tekinthetők így a becsatlakoztatás műszaki megvalósítása sem lehetne különösebben problematikus.

E mellőzöttség magyarázható azzal, hogy hazánkban – *általában* – a központi kormányzati gondolkodásban elsőrangú problémaként merül fel egy olyan szervezet kiszolgáló szerepének megítélése, amelynek bármilyen kapcsolódási pontja lehet a nem-civil szférához, de azzal is, hogy az egységesítés irányába mutató törekvések rendre meghiúsultak a minisztériumi szervek útvesztőiben. Ezekből kiindulva talán érthetővé válik az is, hogy egy elsősorban biztonsági ismérveket magán viselő technikai rendszer felügyelete miért is kft. vagy rt. társasági formában kerülhet majd megszervezésre.

Összességében véve elmondható, hogy a környezetünkben lezajló fejlődési trendek kényszerítő hatása miatt a MeH kezdeményezésére megindított folyamat kilendítette a holtpontjáról a kormányzati érdekeket kiszolgáló kommunikációs rendszerekkel kapcsolatosan fennálló problémakört. Az elmozdulással párhuzamosan azonban még nem látható világosan, hogy a kormányzati EKG létesítése milyen módon befolyásolja a védelmi jellegű kommunikációs rendszerek megszervezésének és jövőbeni alkalmazásának kérdéseit, ugyanis azon kívül, hogy az 50/1998. számú kormányrendeletben meghatározott, védelmi, bűnüldözési, nemzet- és közbiztonsági érdekeket szolgáló szervezetek csak kinyilvánított csatlakozási szándék esetén kötelesek belépni, nem került deklarálásra semmilyen egyéb szervezési vagy együttműködési koncepció.

Valószínű, hogy az EKG-val megindított fejlesztés hosszútávon jótékony hatással lesz az összkormányzati tevékenységre és a kifejtett munka hatékonyságára, azonban szükségesnek mutatkozik a védelmi ágazatok közötti, távközlési és informatikai szakmai konzultáció elmélyítése, mivel koordináció híján, a működési kényszerből adódóan a jövőben is tovább folytatódhatnak a párhuzamos technikai fejlesztések, így dekoncentrálva a pénzügyi erőforrásokat. A konzultációs folyamatok során:

- célszerű pontosítani mindazon technológiai, illetve szervezéstechnikai alapkövetelményeket és feltételeket, melyek figyelembevétele

mellett eldönthető, hogy az egyes, állami feladatokat ellátó szervezetek EKG-hoz való csatlakoztatása mikor szükségszerű;
- felhasználva a védelmi ágazatban összpontosuló szakismeretet és gyakorlatot meg kell kezdeni az EKG honvédelmi jellegű felkészítése alapelveinek kidolgozását;
- meg kell határozni a biztonsági, illetve nemzetbiztonsági követelményeket.

V. Összegzés

Az EKG megvalósításával talán elmozdulás történik az állami érdekeket szolgáló kommunikációs rendszerekkel összefüggésben évek óta folyó szakmai vitáknak. A döntés ugyan sajátos módon, a központi kormányzat legfelsőbb szintjén centralizáltan született meg, ezért némileg mellőzi is az államigazgatás alsóbb szintjeinek álláspontját. Ettől eltekintve valószínűsíthető, hogy hosszútávon képes lesz kooperatív módon kiszolgálni a jelenlegi zártcélú távközlő hálózatok rendelkező szervezetek kommunikációs igényeit akár úgy is, hogy magába integrálja azok rendszereit.

Jelenleg azonban elmondható, hogy a rendvédelmi szervek és a fegyveres erők zártcélú hálózatait üzemeltetők körében az EKG tervezett kiépítése egyenlőre több bizonytalansági pontot vet fel az együttműködés, illetve a saját rendszerek további alkalmazásával összefüggő kérdésekben, melyek mielőbbi tisztázása egyik alapfeltétele a hosszútávú tervezésnek és a védelmi jellegű kommunikációs rendszerek fejlődési irányainak meghatározásának.

Magyar Sándor

HÁLÓZATFELÜGYELET KATONAI KOMMUNIKÁCIÓS OLDALRÓL TÖRTÉNŐ MEGKÖZELÍTÉSE

Minden ország, katonai szervezete számára fontos a távközlés megfelelő színtű biztosítása és annak a felügyelhetősége. Felhasználó oldalról vizsgálva minél nagyobb a szervezet és annak kommunikációs igénye, a távközlés kiesése annál nagyobb problémát jelent, okoz számára. Üzemeltetési oldalról megközelítve pedig minél nagyobb a távközlési rendszerünk, azon belül minél többfelé elemből épül fel és többféle átviteli utat használ, annál több lehet a meghibásodás valószínűsége és annál nehezebb biztonságosan üzemeltetni azt.

Jelen előadásban a hálózatok felügyeletével, azon belül is a katonai kommunikációs hálózatok felügyeletével kívánok foglalkozni.

A hálózatok fogalmát rendkívül sok féle módon értelmezhetjük: érhálózat, úthálózat, közüzemi hálózat, stb. Elfogadható azonban, hogy a hálózat: „ Tágabb értelemben térben elosztott azonos jellegű tárgyak illetve létesítmények rendszere”. (1)

Kommunikációs oldalról megközelítve a „Hálózat: Csomópontok és átviteli utak olyan rendszere, amelyen összeköttetések létesíthetők információátvitel céljára, két vagy több meghatározott pont között.” (2)

A fogalmat távközlési oldalról értelmezve megállapíthatjuk, hogy a mi esetünkben nem csak az átviteli utak, hanem a távközlést kiszolgáló eszközök, berendezések is létfontosságúak számunkra.

A kiépített hálózatok felépítésük szerint igen sokszínűek lehetnek: fa-, csillag-, gyűrű-, busz-, teljes-, szövevényes topológiájúak, vagy ezek tetszés szerinti kombinációi. Az előbb felsorolt topológiák mindegyikének vannak előnyei és hátrányai, de megbízhatóság szempontjából a katonai felhasználóknál cél egy olyan hálózat kiépítése, ahol minden hálózati elemnek legalább két másik elemmel van kapcsolata. Ahol a hálózati elemünknek legalább két másik elemmel van összeköttetése, ott a kerülőirány biztosított, az egyik átviteli út kiesése esetén az elem nem szakad el a „külvilágtól”, hálózattól, a hálózat üzemelése folyamatos lesz. A hálózati elem a hálózattól történő leszakadása ellen még jó megoldás, ha a két elemünk közötti átviteli utat fizikailag is más útvonalon megkétszerezzük, vagy megtöbbszörözzük, ezáltal is biztosítva a folyamatosságot.

Hálózatfelügyelet alatt egy hálózatot alkotó több autonóm elem felügyeletének rendszerét értjük. Egy hálózati elem felügyelete történhet: helyi beavatkozással, illetve távfelügyelettel.

A távfelügyeletnek törekednie kell egy a használt átviteli úttól független útvonal biztosítására is a kapcsolástechnikai, illetve felügyelt eszköz felé. A

Magyar Honvédség átviteli útjainak keresztmetszetei többnyire szűkek. Az átviteli utak megszakadásával a felügyeleteknek mindig kell rendelkezniük tartalék útvonallal. Értem ezalatt például ha megszakad egy 2 Mbps-os trönk áramkör amely a fő felügyeleti útvonalat szolgáltatja, akkor a felügyelt eszközhöz kell rendelkeznünk még egy másik tartalék útvonallal is (ha kell analóg vonalon keresztül történő csatlakozással). Ezekben az esetekben a tartalék útvonalon biztosítja a folyamatos felügyeletet és konfigurálhatóságot.

A hálózatfelügyeleti rendszerünk a folyamatos kapcsolaton keresztül gyűjtheti a hálózati eszközökről és a hálózat forgalmáról az adatokat ezért az útvonal kiesése a rendszerünk részleges sérülését okozhatja.

Az, hogy melyik szervezet milyen hálózatot épít ki kommunikációs igényei kiszolgálására, azt nagymértékben befolyásolják pénzügyi erőforrásai.

A hálózatokat azonban csoportosíthatjuk más oldalról megközelítve is, így ezek lehetnek: - analóg hálózatok (analóg - átviteli utak, - eszközök, - berendezések)

- digitális hálózatok (digitális - átviteli utak, - eszközök, - berendezések)

- vegyes hálózatok (az előző kettő elemeit együtt tartalmazza)

A Magyar Honvédségen belül vegyes hálózat található, ez adódik egyrészt a még rendszerben lévő analóg hálózati elemekből, másrészt a megkezdett digitális fejlesztés előrehaladásából.

A hálózatfelügyeletek tekintetében cél a rendszer teljes digitalizálása mivel az analóg eszközök, berendezések nem támogatják a távfelügyeleti lehetőséget. Az analóg átviteli utak esetében ugyan alkalmazhatóak bizonyos technikai megoldások, de ezek a riasztások is csak a helyben lévő szakemberek részére nyújtanak információt.

A hálózati elemek alkotta rendszer összetettsége bonyolítja a hálózatfelügyeleti, hibabehatárolási és javítási feladatait is. Ugyancsak nehezíti a felügyeletet, ha többféle technikát és távközlési szolgáltatót magába foglaló átviteli szakasszal van a probléma. A Magyar Honvédség és más országos hálózattal rendelkező szervezet tekintetében nehéz a külső cégeket, szolgáltatókat egy esetleges közös méréshez időben és helyben egyszerre a feladatmegoldáshoz koordinálni.

Eddig a hálózatfelügyelet, távfelügyelet szűken vett értelmezéséve került szóba. Azonban a felügyeleti rendszereknek az átviteli utak, eszközök, berendezések fizikális felügyelete mellet még számos funkciót kell kielégíteni. A hálózatfelügyeleteknek feladatai lehetnek a következők:

- forgalom és teljesítmény túlcsordulás figyelése,
- hibaelemzések készítése a szükséges beavatkozásokkal,
- a távközlési eszközök hozzáférésének és biztonságfigyelésének kérdései,
- az adott eszköz, berendezés konfiguráció felügyelete.

A hálózatfelügyelet tehát nemcsak olyan monitorozó tevékenységet takar, ami a hálózati elemünk közvetlen, aktuális állapotát tükrözi vissza, hanem olyan tevékenységeket is magába foglal, amely lehetővé teszi a rendszerünk átláthatóságát és a központi menedzselését. A hálózatfelügyelet által gyűjtött adatokból előre prognosztizálható a rendszerünk várható meghibásodása is.

A távfelügyelet során a szakember közvetlenül a felügyelt rendszerrel kerül kapcsolatba. Az összeköttetés segítségével pontos képet kap a rendszer állapotáról. Az ilyen kapcsolatban a hibaelhárítás lehetősége a lehető leggyorsabb, mivel az estetek döntő többségében nem kell a helyszínre utazni, és az intézkedés azonnal megtehető.

Az automatikus rendszer tovább növeli a megbízhatóságot, ráadásul a humán erőforrások hatékonyabb kihasználását teszi lehetővé. A felhasználó üzemeltetési ráfordításai jelentősen csökkennek, a megelőzés lehetőségével az üzemeltetési és karbantartási folyamat alacsonyabb költségekkel előre tervezhetővé, jól kézben tarthatóvá válik. A távfelügyeletek gazdaságosságát támasztja alá az is, hogy riasztások köthetők be más területekről az adott felügyeleti helyekre.

A modern telekommunikációs hálózatok egyre bonyolultabbá válása megkívánja az üzemeltetés központosítását, ezzel együtt pedig olyan rendszerek beszerzését, amelyek megvalósítják ezt a központosított felügyeletet és vezérlést, az egész országot lefedő telekommunikációs hálózatra – kapcsolástechnikai és átviteltechnikai eszközökre. Ezen rendszer elősegíti a jobb minőség és szolgáltatásnyújtást a felhasználók felé, költségmegtakarítást és hatékonyságot eredményez az üzemeltetés terén és egységesítést a hálózaton belül.

A katonai szervezetek tevékenysége folyhat nemzeti területen, illetve idegen ország területén. Már országon belüli együttműködést vizsgálva, előjön a különböző béke (stacioner) és háborús (mobil) kommunikációs rendszerek összekapcsolhatóságának, közös felügyeletének kérdésköre. Lényeges szempont a kommunikációs rendszer tervezésénél, szervezésénél az, hogy a szervezet milyen feladatot hajt végre, milyen az alá-, fölérendeltségi viszonya, a szervezeten belül hogyan alakítható ki a hálózatfelügyelet szervezeti, technikai támogatása.

Hálózatfelügyelet alatt Magyar Honvédség viszonylatában folyamatos felügyeletet értünk gyors beavatkozással, olyan rendszereken, amelyeknek működésében nem engedhetők meg hosszabb ideig tartó zavarok.

A folyamatos felügyelet és a rendszer rendeltetéséből adódó potenciális célponttá válása miatt, mindenképpen kell tartalék hálózatfelügyeleti lehetőséggel rendelkezni.

Az új katonai terminológiák alapján a katonai tevékenységek osztályozását az alábbiak szerint tehetjük meg:

- Béketevékenységek;
- Nem háborús katonai műveletek:

- Katonai műveletek békében
- Katonai műveletek konfliktushelyzetben

♦ Háborús katonai műveletek.

Tevékenységi terület elhelyezkedése, terep, évszak, napszak, időjárás mind-mind hatással vannak a katonai művelet végrehajtásának híradó biztosítására. Ezért szükséges olyan kommunikációs rendszerek kutatása, tanulmányozása, amelyek képesek a fent említett körülmények között is kielégítő, a megváltozott igényeknek megfelelő szolgáltatás biztosítására, a helyi beavatkozás lehetősége mellett a távfelügyeleti problémák kielégítésére. Ezen rendszereknek ki kell elégíteni az újszerű követelményeket, melyek a mobilitás, rugalmasság, reagáló képesség, biztonság és a szabványosság fogalmait foglalják magukba.

A harc eredményes megvívását jelentősen befolyásolja a vezetés-irányítás támogatási rendszere. A megfelelő szintű kommunikáció biztosítása nélkül az egységek, alegységek nem képesek feladataik maradéktalan végrehajtására, a harc sikeres megvívására. Minden vezetési szinten egyre nagyobb igény jelentkezik arra, hogy minél több információ álljon a döntések körültekintő előkészítéséhez és meghozatalához. Nekünk híradóknak egyre inkább feladatunk lesz a távbeszélő összeköttetések mellett, az adat és képi (kép, mozgókép) információk hiteles, rejtett, időbeni továbbítása. A technika fejlődésével a berendezéseink központjaink, is egyre könnyebben kezelhetőek, méretüket tekintve kisebbek, tudásukat napról napra felülmúlók és nem utolsó sorban távfelügyelhetőségüket tekintve biztonságosabbá válnak.

A tábori híradásnak a kor követelményei szerint nem csak a távbeszélő híradást kell magas színvonalon kielégítenie, hanem a telekommunikációval mind jobban összefonódó informatika igényeit is. Mindemellett a tábori híradás rendszerének tökéletesen illeszkednie kell az állandó híradást biztosító távközlő hálózattal, beleértve a műholdas távközlést is, továbbá tökéletesen illeszkednie kell a NATO rendszeréhez.

A szervezeti felépítését, feladatát tekintve rendelkeznie kell (és rendelkezik is) egy olyan szervezeti elemmel, amely a katonai kommunikációs igényeit kielégíti.

A Magyar Honvédség katonai kommunikációs hálózatfelügyeleti szervezetének (mivel hatalmas felhasználói és technikai bázist felügyel) a feladatai támogatására szükségesek az alárendeltségébe tartozó regionális hálózatfelügyeleti elemek. Ezek az országot régiókra bontva a saját központjaikban, eszközeikben felmerült kisebb - semmiképp sem hálózati szintű- konfigurálásait végzik. Ilyen regionális hálózati elemként lehet beilleszteni a béke hálózatfelügyeleti rendszerbe a háborús hálózatfelügyeleti rendszert.

Felhasznált irodalom

- Magyarné Kucsera Erika: A hálózatfelügyelet és lehetőségei a Magyar Honvédség híradó szolgálatánál, ZMNE Tudományos Diákköri Konferencia 2000
- Mindenki lexikona, Akadémiai kiadó Budapest 1974.
- A távközlési szolgálatok fogalmai és meghatározásai, D. Távközlő hálózatok, Távközlési könyvkiadó 1995.
- Tannenbaum-Andrew S.: Számítógép hálózatok BP.-Novotrade kiadó Kft.-1992.
- 158/1993. (XI.11.) Kormányrendelet a távközlő hálózatok összekapcsolásáról, együttműködésüknek engedélyezéséről, valamint a hálózati szerződésekről.
- 1992. évi LXXII. törvény a távközlésről
- 3. számú melléklet az 50/1998. (III.27.) Kormányrendelethez: A távközlés felkészítésének rendje, az átállítás és a minősített időszaki alkalmazás szempontjából
- 50/1998. (III.27.) Kormányrendelet a zártcélú távközlő hálózatokról
- Internet: http://www.scinetwork.hu/services

Dobos Attila

ELLENŐRZÖTT KISUGÁRZÁSÚ SZÁMÍTÓGÉPEK

Az információ technológiai biztonság kihívásai
TEMPEST megoldások a Siemenstől

Már napjaink információs társadalmát megelőzően is értéket és sokszor hatalmat jelentett, ha valaki a megfelelő időben a megfelelő információhoz hozzájutott. Emberek, csoportok, országok, nemzetek és rendszerek sorsa múlott azon az adathalmazon, amit információnak nevezünk. Időt, energiát és pénzt nem kímélve fejlődött önálló mesterséggé és tudománnyá a szükséges információk felderítése, az információgyűjtés, valamint azok feldolgozása és eljuttatása a megfelelő személyekhez. Természetesen ezalatt a folyamat alatt mindet el kell követni annak érdekében, hogy a vadászból nehogy áldozat legyen, a megszerzett információt mások ne birtokolhassák.

Ezen ördögi körforgás problémáinak megoldására örökös versenyfutás van információ védelemével és megszerzésével foglalkozó szakemberek és szervezetek között. Azt, hogy éppen ki jár elől és mekkora előnyre tett szert, igen nehéz megítélni és megállapítani, mivel ez a versenyfutás a nagy nyilvánosság teljes mellőzése mellett folyik. Egyre bonyolultabb megoldások kerülnek napvilágra a védelem piacán, de az ellentábor – nagyobb hírverés nélkül – folyamatosan követi az eseményeket.

Az elektronikai világpiac egyik meghatározó tagjaként a Siemens is kínál megoldásokat mindkét oldal részére. Az elkövetkezőkben az információ technológiai biztonság területen kínált megoldásainkat szeretnénk ismertetni.

A veszélyforrás a mérhető sugárzás

A Maxwell egyenletek megalkotása óta immár tudományosan is bizonyítottá vált a kapcsolat az elektromos és a mágnese tér között. Az elektromos berendezések működését kísérő elektromágneses sugárzás napjaink már természetessé vált jelensége, amely spektrumszennyező és egészségkárosító – vagy gyógyító - hatása mellett alkalmas az áhított információk megszerzésének médiumaként és viselkedni.

Ez a sugárzás, annak időbeni változása képes az információk hordozására, olykor olyanokéra is, amelyeket nem szeretnénk a nagyvilágba szétszórni. Ezek a különböző forrásból származó sugárzások a szó szoros és fizikai értelmében is hordozóként képesek a nem kívánt információkat is továbbítani.

Az így kisugárzott információk antennákkal történő detektálás után a sugárzásból visszanyerhető – gyakran elég a szuperponálódott komponenseket szétválasztani – ezzel gyengítve biztonsági rendszerünket.

Különösen nagy veszélyforrást jelentenek azok eszközök, amelyeken elektronikus módon nagy mennyiségű információ feldolgozása folyik.

Különösen a könnyen detektálhatóak azok a jelek, amelyek a monitorok állandó magas energiaszintű sugárzására ülnek rá. Ezáltal egy adott helyiség a benne működő – sugárzó – monitor révén nyitott rendszerként, valamennyi védettségét elveszítve számítható.

A sugárzó eszköz környezetében lévő fémes berendezések nagy részében áram indukálódik, melyet elemezve, hasznos információkat lehet összegyűjteni. Nem szükséges komoly berendezésekre gondolni, hiszen egy egyszerű fűtéscső is viselkedhet antennaként és alkalmas lehet egy adott helyiség felderítési eszközeként működni.

Természetesen a professzionális információszerzők nagy érzékenységű vevőkkel, nagy nyereségű és irányított antennákkal és nagy teljesítményű jelfeldolgozó berendezésekkel rendelkeznek.

A megoldás a TEMPEST technológia

Az elektronikus információk is lehet védeni az ilyen jellegű felderítés ellen. A TEMPEST jelölésű berendezések elektromágneses sugárzása jelentős mértékben redukált, megakadályozva ezzel a korábbiakban leírt felderítést.

Természetesen jól előkészített módszerekkel (tárolók beépítése elektromos alkatrészekbe, rejtett szoftvermodulok) a kézben tartott sugárzás ellenére is megtámadhatók az elektronikus adatfeldolgozó rendszerek.

Az elektronikus adatfeldolgozó rendszerek elleni támadásokban az utóbbi években jelentős változás történt. A korábban nagy számban elkövetett ipari jellegű – nagyvállalatok rendszerei ellen elkövetett – támadások száma jelentősen csökkent, ezzel szemben ugrásszerűen megemelkedett a kormányzati és védelmi szervezetek elektronikus rendszerei ellen elkövetett támadások száma.

A TEMPEST előírások nemzetközi szinten, a NATO-ban is honosításra kerültek és a „Zóna elv” alkalmazásával nagymértékben hozzájárultak a biztonságos elektronikus adatfeldolgozó rendszerek kialakításához. A környezeti és elektromos biztonság összehangolásával és kombinálásával olyan körülmények alakíthatók ki, amelyek a legszigorúbb biztonsági elvárásoknak is megfelelnek.

A TEMPEST előírásoknak való megfelelést szigorú szabályok szerint működő mérőlaborban kell bizonyítani. A Siemens a NATO SECAN által akkreditált saját TEMPEST bevizsgáló laborral rendelkezik és az itt vizsgált és megfelelt berendezések megfelelőségét a német BSI tanúsítványai bizonyítják.

Természetes, hogy az ilyen berendezések nem követik az informatikai piac száguldását, hiszen az adott berendezéstípusra egyedileg kell a benne

lévő sugárzó elemek szerinti védelmet tervezni és bevizsgálni. Teljesítményükben azonban nem maradnak el a hagyományos piaci berendezésektől.

A biztonságos hálózat

Az elektronikus információfeldolgozás az információ jellegétől és mennyiségétől függően hálózatokba kötött berendezéseken is folyhat. Ebben az esetben nem elegendő a hálózati elemek kisugárzás védelmére figyelni, hanem a hálózatban alkalmazott kábeleket is nagy körültekintéssel kell megválasztani.

Természetesen a legbiztonságosabb megoldásnak az optikai kábelek alkalmazása tűnik. Elektromágneses kisugárzása valóban elhanyagolható, azonban léteik olyan technológia, amely képes a kábeleket „megcsapolni" és a felhasználók tudta nélkül valamennyi információt a kábelből kinyerni. Mindezek mellet az optikai kábelek még igen drágák és telepítésük (hajlításuk, csiszolásuk) technológiai korlátokba ütközhet.

A strukturált kábelezési rendszerekben alkalmazott kábelek típustól függően előnyökkel és hátrányokkal rendelkeznek.

Az STP kábel kellőképpen védett, de az érpárankénti árnyékolás a szerelési technológiát megnehezíti, mivel merevvé és nehezen kezelhetővé teszi a kábelt. Az FTP kábelezés szerelési könnyebb, azonban védettsége jelentősen rosszabb. A legrosszabbak az UTP kábelek, hiszen semmilyen védelemmel nem rendelkeznek.

A Siemens FUTUREWay kábelezési rendszere a fentiekben felsorolt kábeleken túl tartalmaz egy speciálisan kifejlesztett típust, amely már jelzésével is – S-FTP – sejteti jellemzőit. Az FTP kábel könnyű szerelése került ötvözésre az STP kábelezés védettségével. Amellett, hogy a kábel anyagában szilárd, az égés akadályozza, kettős árnyékoló fóliával és földelő harisnyával került megtervezésre és gyártásra. Az így kapott kábel sugárzása minimális, zavarállósága és zavarás elleni védettsége igen magas.

Az árnyékolás a kábelezési rendszer valamennyi elemén kialakításra került a szerelt csatlakozóktól megkezdve a rendező panelekig.

A biztonságos hálózat

Napjaink elektronikus adatfeldolgozáson alapuló világában a **Siemens** a frissen kifejlesztett megoldásaival nem csak termékek és szolgáltatások szállítására képes, hanem olyan védett és nagy biztonságú – igény esetén nagy kiterjedésű – adatfeldolgozó berendezések és hálózatok tervezésére és telepítésére, amelyek minden biztonsági szempontból megfelelnek napjaink információvédelmi elvárásainak

Szűcs Endre

KOMMUNIKÁCIÓ A XXI. SZÁZADI HELYSÉGHARCBAN[46].

A XXI. században a fegyveres küzdelem az információs társadalom vívmányainak eszközeivel kerül megvívásra. Az emberiség nagy léptékű fejlődése az információs társadalom kialakulását eredményezi. Az információs társadalom kialakulásával egy időben a Föld népessége is gyors ütemben gyarapszik. A népesség gyarapodás a helységek (városok, falvak, stb.) területének növekedését eredményezi, ezáltal a jelentőségük is növekedni fog. A fegyveres küzdelem során az elérendő célok megvalósításához szükséges lesz a helységek védelme, illetve elfoglalása (birtokbavétele). A helységekért folytatott harctevékenységekben is fontos tényező lesz a kommunikáció.

A Magyar Köztársaság védelmére történő felkészülés során béke időszakban a helységharcra ki kell képezni, illetve a harctevékenységek folyamán a helységharcot is alkalmazni kell a Magyar Honvédségnek. A Magyar Honvédség erői közül a gépesített lövész csapatok azok, amelyek a helységharc megvívására a legalkalmasabbak.

A munkámban azt vizsgálom, hogy a XXI. században a helységharcot a gépesített lövészek milyen körülmények között fogják – várhatóan - megvívni. A körülmények hogyan befolyásolják a kommunikációt. Melyek azok az eszközök, amelyek biztosítani tudják a korszerűséget.

1. A helység, mint harcmező[47]

A XXI. században a helységek területe egyre inkább a harcmező részét fogja képezni. A városiasodás (urbanizáció)[48] jelentősen meg fogja változtatni a harcmezőt. A XXI. században a fegyveres küzdelem az információs hadvise-

[46] A harcnak sajátos viszonyok közötti megvívása, amikor is a magasabbegység (egység, alegység) a harcát a település (város, község) különböző építményei, létesítményei (épületek, épületcsoportok, utcák, terek stb.) figyelembevételével, sajátos módon, sajátos eljárással és csoportosításban folytatja. Damó László: Katonai Lexikon. Zrínyi Katonai Kiadó, Budapest, 1985. 269. o.

[47] Annak a területnek (terepnek) a megnevezése, amelyen a csapatok harcukat (hadműveleteiket, ütközeteiket) közvetlenül megvívják. Uo. 258. O.

[48] „Az urbanizáció gyors növekedése egyszerűen azt jelenti, hogy kevesebb lesz az olyan nyílt terep, amelyen harcolhatnak. Az urbanizáció elnyeli a kulcsfontosságú kommunikációs vonalakat, szállítási gócokat, út-és vasútcsatlakozásokat és hagyományos hadviselésben megnehezíti a szárazföldi csapatok számára a városok megkerülését, vagy azok környezetében a manőverezést oly módon, ahogyan hagyományosan megkísérelték, és ahogyan a hadviselési doktrína többnyire hangsúlyozza.” Rosenau, W G. Minden helység új csata: A korszerű városi hadviselés tapasztalatai. In Studies in Conflikct and Terorism, 1997. 4. szám. Fordítás: Szabó Ferenc: p. 6.

lés jelentős hatása alatt és nagy valószínűséggel a helységek (városok, stb.) területén illetve azok közelében fog történni. Ez a harcmező már digitális harcmező lesz.

A digitális harcmező *olyan terület, ahol a harcoló erők a harcaikat digitális eszközök nagy arányú alkalmazásával fogják megvívni. Ezen a harcmezőn a harcos és a parancsnoka részére a harc megvívásához illetve a harc megtervezéséhez, megszervezéséhez és a vezetéséhez szinte minden információ rendelkezésre fog állni a terepről, az időjárásról, az ellenségről és annak tevékenységéről, a saját csapatokról, az egyes harcosról (helyzetéről, testi-fizikai állapotáról stb.). A digitális harcmező nem csak azért lesz digitális, mert az ott folyó harcok digitális eszközökkel történnek, hanem azért, mert az információs társadalom információs rendszerei is jelen lesznek*

A digitális harcmező tehát hatással lesz a helységharcra, melyeket az alábbiak tartalmaznak.

1.1 A helységharcot befolyásoló körülmények

Nézzük meg azokat a körülményeket, amelyek a helységharcot befolyásolják.

A befolyásoló körülmények a következők:

— a szemben álló ellenség helyzete, ereje, jelenlegi és várható tevékenysége;
— az elöljáró kötelék tevékenysége;
— az adott kötelék helye, szerepe az elöljáró kötelék harcrendjében, hadműveleti felépítésében;
— a csapatok tevékenysége a helységharc előtt;
— az adott kötelék jellege és harcértéke;
— a szomszédok helyzete és tevékenysége;
— a helységharcba való átmenetre rendelkezésre álló idő;
— a felek által alkalmazott pusztító eszközök minősége, mennyisége;
— a háború időszaka;
— a terep;
— a kialakult vagy várható vegyi-, sugárhelyzet;
— az év- és napszak, valamint az időjárási viszonyok.

A körülmények komplex módon fejtik ki hatásukat a helységharcra.

A befolyásoló körülmények közül csak néhányat mutatok be részletesebben.

Elsőként a terepet vizsgálom, amely a helységet is magába foglalja.

1. 1. 1. A terep.

A helységharcot (az általánoson kívül) az alábbi sajátos körülmények is befolyásolhatják. A sajátos körülmények:

- a helység lélekszáma;
- a helység nagysága;
- a helység alakja és szerkezete;

- a lakónegyedek elhelyezkedése és felépítése;
- az épületek mennyisége és minősége;
- a földalatti létesítmények;
- a helység terepviszonyai;
- a helységhez vezető utak (száma, minősége);
- a helység jelentősége (politikai, gazdasági, társadalmi stb.);
- a helység információs (kommunikációs) infrastruktúrájának helyzete.

A felsorolt sajátos tényezők közül is csak azokat részletezem, amelyek a kommunikációt befolyásolják

A helység szerkezete.

A helység részei lehetnek:

- közigazgatási rész;
- lakórész (kertvárosi, lakótelepi);
- ipari rész (gép, vegyi, elektronikai, stb.);
- szállítási objektumok (szárazföldi, vízi, légi);
- raktárak (üzemanyag, vegyi anyag, élelmiszer, építőanyag, stb.);
- be nem épített részek (parkok, terek, tavak);
- egészségügyi részek (kórházak, klinikák, szanatóriumok stb.);
- történelmi rész (várak, kastélyok, stb.);
- katonai objektumok;
- oktatási részek.

A különböző részeken belül más és más az utcák, terek, épületek száma, minősége. A részek hatással vannak a védő és a támadó harcrendre, az alkalmazandó eszközökre, a harcvezetésre, azon belül a kommunikáció kiépítésére, fenntartására.

A közigazgatási, egészségügyi, oktatási és az ipari rész részben, valamint a raktárak területén, *az egyes épületeken belül is vannak kiépített kommunikációs rendszerek, illetve más épületek felé is, melyek felhasználásával a kommunikáció feltételei részben már adottak*.

A lakórészben a lakásokban *meglévő vonalas telefonokat lehet a kommunikáció céljaira hasznosítani.*

A katonai objektumokban *a meglévő kommunikációs lehetőségeket a település kommunikációs lehetőségeivel összekötve hatékony rendszert lehet kialakítani főként, ha helységben védelem előkészítésére van idő.*

A be nem épített részekben *a rádióforgalmazás feltételei könnyebben biztosíthatók*.

Az épületek mennyisége és minősége.

A több száz éve meglévő helységekben az épületek anyagaik és az építési módjuk miatt szilárdabbak és közel vannak egymáshoz. Az utcák szűkek, kanyargósak kisebb távolságra vannak egymástól, mint a modern városrészek-

ben. *A rádióforgalmazást kismértékben befolyásolják. A vezetékes összeköttetést jobban lehet rejteni.*

A modern városrészekben széles sugárutak vannak, amelyek kedvezőek a körültekintően előkészített támadás esetén. A széles sugárutak lehetővé teszik a fegyverek közel maximális lőtávolságának kihasználását, illetve manőverezési lehetőségeket biztosít. *A modern épületekben a belső telefonhálózat felhasználása megkönnyíti a védő fél kommunikációjának kiépítését és fenntartását a harctevékenység alatt. A modern városrészek kommunikációs hálózata nagy segítséget jelenthet a védő részére az összeköttetés fenntartásában.*

A XX. század második felében épült helységek, helység részek épületei nem elég szilárdak sok bennük az üveg és a gyúlékony anyag. Az épületek távolabb épültek egymástól, az utcák szélesebbek. *Az épületek sok esetben tíz emeletesek vagy annál is magasabbak az építési anyagaik között sok a vasbeton, ezáltal a rádióforgalmazást sok esetben teljesen lehetetlenné teszik.*

A helység terepviszonyai.

A harctevékenységekre nagy hatással vannak, mert a helységek szerkezete, alakja követi a terepviszonyokat. A terepviszonyok (domborzat, talajviszonyok) segíthetik vagy gátolhatják a fegyverek használatát, *az összeköttetés kiépítését és fenntartását*, a műszaki munkák végzését stb.

A helység információs (kommunikációs) infrastruktúrájának helyzete.

A helységen belül van-e telefonközpont, halad-e át rajta nemzetközi, országos, regionális közszolgálati – közüzemi – közellátási - közrendvédelmi érdekű távközlési és informatikai vonal. Működik-e a helységben olyan vállalat vagy egyéb szervezet, amely a központjával kisméretű földi antennával rendelkező műholdon keresztül tartja a kapcsolatot. A helységben lévő rendőrséghez vannak-e közintézmények, vállalkozások, lakások védelmét biztosító riasztó rendszerek végpontjai bekötve. A helységben található-e olyan jelzőrendszer, amelyet távolról működtetnek, vagy olyan rendszer szenzorai, amelyek országos, regionális központba továbbítják mérési adataikat.

Az információs infrastruktúra jelentős hatást fejt ki a harctevékenységekre. Az infrastruktúra fejlettségének színvonala segíteni fogja a harctevékenységek során a kommunikációt.

A bemutatott tényezőkön keresztül látható, hogy a helység segíti és gátolja a kommunikáció kiépítését és fenntartását. Megállapítható, hogy a védelmet előkészítő előnyösebb helyzetben van – főként, ha saját hazája területén tevékenykedik -, mert a helyi kommunikáció lehetőségei teljes mértékben a rendelkezésére állnak.

A következőkben az adott kötelék jellege körülményt elemzem.

1. 1. 2. Az adott kötelék jellege.

A haderő átalakítás során a gépesített lövész fegyvernem is változott. A gépesített lövész fegyvernemen belül az alegységek szervezeti felépítésében

jelentkezik a változás. Az alegységek szervezeti felépítése annyiban változott, hogy a szakaszokon belül négy raj van szervezve. A szakaszok száma is változott, mert egy páncéltörő szakaszok is lettek szervezve a századokban.

A gépesített lövész fegyvernem alegységei (zászlóaljtól rajig) folytathatnak harctevékenységet helységben, mert a harc megvívására a fegyverzetük és a szervezetük alkalmassá teszi őket.

A gépesített lövész alegységek rendelkeznek híradó eszközökkel, de azok nem korszerűek[49] és így nem biztosítják a zavarmentes összeköttetést a helységharc megvívása során.

A rendszeresített eszközök alkalmazására a személyi állomány (parancsnokoktól a beosztottakig) felkészítése, kiképzése megtörténik. Az eszközök kezelését a kiképzést követően az állománytáblában meghatározott híradó beosztásúakon kívül más beosztású katonák csak kismértékben gyakorolják, végzik.

Megállapítható, hogy a gépesített lövész alegységek kommunikációs lehetőségeit radikálisan meg kell változtatni.

A következő részben azokat a lehetőségeket, azokat az elképzeléseimet foglalom össze, amelyek szerintem szükségesek ahhoz, hogy a gépesített lövész alegységek kommunikációja korszerű legyen és a helységben vívandó harctevékenységük sikeréhez hozzájáruljon. .

2. A korszerű kommunikáció eszközei a helységharcban.

A korszerű kommunikációról csak abban az esetben beszélhetünk, ha az elektronikai ipar legújabb eredményeit magukban hordozó eszközöket alkalmazunk. A helységharc sikeres megvívása érdekében az alábbi lehetőségeket és eszközöket tartom célszerűnek vizsgálat alá vonni.

A gépesített lövészkatona számára olyan kommunikációs eszközt célszerű beszerezni, amellyel könnyen tud kapcsolatot tartani társaival és parancsnokaival, illetve ami nem akadályozza sem a védelmi, sem a támadó tevékenysége során. A megvalósítást kétféle képen tudom elképzelni.

Az egyik változatban megoldás lehet a cellarendszerű rádiótelefonok[50] alkalmazása, melyhez a készülékek már rendelkezésre állnak. Átalakítással ezek a telefonok katonai alkalmazása is biztos megoldható. A cellarendszerű rádió-

[49] „Az MH jelenlegi állandó telepítésű és tábori híradásának rendszerei és eszközei nem alkotnak egységes rendszert. Szolgáltatásaikban, műszaki színvonalukban elmaradnak a kor követelményétől, az országos távközlési rendszerek, szolgáltatások színvonalától, valamint a NATO-rendszerektől. Mráz István: A katonai felső szintű vezetés információs rendszerének korszerűsítése I. Új Honvédségi Szemle, Budapest, 2001, 55. évfolyam 7. szám, 45. o.

[50] A Csecsenek az oroszok elleni harcaik során a cellarendszerű rádiótelefonokat alkalmazták egymás közötti kommunikációra. Mr. Lester W. Grau: Urban Warfare Communications: A Contemporary Russian View, Red Thurst Star, July, 1996,call.army.mil/fmsopubs/issues/urbanwar/urbanwar.htm

telefonok kezelésére a katonák kiképzése könnyen megvalósítható lenne. Egyre több ember rendelkezik rádiótelefonnal és a kezelését, lehetőségeit ismeri. A másik megoldás az olyan rendszerű sisak[51] lenne, amelyben rádió adóvevő van beépítve. A sisak alkalmazása esetén a használatára történő kiképzés a hírváltás szabályainak megtanításából állna.

Az alegységeknek olyan a korszínvonalán álló kommunikációs berendezéseket kellene rendszeresíteni, amelyek az interoperabilítás eléréséhez, illetve a helységharc sikeres megvívásához is hozzájárulnak. Ezek az eszközök az alábbiak lehetnének:

— „új működési elvű (SQID), kisméretű antennák;
— kis zajú, gyors hangolású rádiófrekvenciás erősítők (FH/SSM);
— speciális átviteli karakterisztikájú erősítők;
— magas hatásfokú, gyors hangolású adóberendezések;
— kiterjesztett spektrumú (LPI/LPD) adó-vevők;
— digitális titkosító (COMSEC) berendezések;
— kódosztásos (CDMA), ATM-képességű rádiók .."52

Ezek az eszközök a NATO vezető katonai országaiban már részben rendelkezésre állnak, valamint kifejlesztésük folyamatban van.

A harcvezetés korszerűsítése megköveteli, hogy az alegységek vezetését is lássák el korszerű számítástechnikai berendezésekkel.

A technikai eszközök, valamint a korszerű számítástechnikai berendezések kezelésére a személyi állományt ki kell képezni, illetve fel kell készíteni, mert az eszköz magától nem működik. A felkészítés és a kiképzés alapjai tulajdonképpen adottak lesznek, mert a bevonuló fiatalok közül a többség rendelkezni fog bizonyos fokú előképzettséggel. Az előképzettséget úgy értem, hogy a bevonuló fiatalok számára a számítástechnika nem ismeretlen, tehát a felkészítést és a kiképzést nem nulláról kell kezdeni. A kiképzés és felkészítés az alábbiak szerint valósítható meg:

– a kiválasztott eszközök kezelését oktató tanárok részére a külföldi felkészítést biztosítani kell, hogy a szakszerű felkészülésük biztosított lenne;

[51] A sisak rendszere rendkívül összetett. Egyszerre bonyolult kommunikációs és érzékelő rendszer, amely azt a célt szolgálja, hogy a harcos kezelhesse a rendelkezésére álló intelligens rendszereket, mikrorobotokat. Ez a rendszer felügyeli a lézervezérlést, számolja a ballisztikai adatokat, tájékoztat a környezet állapotáról, méri a vegyi és bakteriológiai szennyezést. A külső szenzorok tájékoztatnak mindenről, esetleges ellenséges járművekről, kapcsolatot tartanak a műholdakkal. A sisak belső kijelzőjén minden adat megjeleníthető, amely éppen szükséges a katona számára. Tóth Csaba: Lethal Weapon „X". Fordítás a Defence News Vol. 15. No. 6 alapján. Új Honvédségi Szemle, Budapest, 2000, 54. évfolyam, 5. szám , 146-147. o.

[52] Dr. Makkay Imre: Az elektronika, távközlés és az elektronikai hadviselés a XXI. században. Nemzetvédelmi Egyetemi Közlemények, Budapest, 1997, 1. évfolyam, 2. szám, 271. o.

– a katonai vezetői szak gépesített lövész szakirányán tanuló hallgatók (leendő tisztek), illetve a tiszthelyettes hallgatók felkészítése során az új eszközök alkalmazásának elsajátítását oktatni kell;

– a gépesített lövészkatonák kiképzése során a rádió kiképzést meg kell változtatni és helyette kommunikációs kiképzéssé szükséges átalakítani. A módosítás azért szükséges, mert a helységharcban nem csak rádió híradással tartható fenn a kommunikáció.

Befejezés

A munkám célja az volt, hogy bemutassam, hogy a gépesített lövészek milyen körülmények között fogják – várhatóan – megvívni a XXI. században a helységharcot, illetve a körülmények ilyen hatással vannak a kommunikációra.

A vizsgálatommal bizonyítom, hogy a XXI. századi helységharcot befolyásoló körülmények már az információs társadalom viszonyait is magukban fogják hordozni. A változó körülmények a helységharc kommunikációjára is hatást fognak gyakorolni, melyet nem szabad figyelmen kívül hagyni. A hatások bizonyítják, hogy a helységharcban a kommunikáció milyen fontos. A bemutatott eszközökön kívül biztosan vannak még mások is, amelyek biztosíthatják korszerűséget.

A kommunikáció a XXI. században igen fontos eszköze lesz a harctevékenységeknek és a kimenetelüket is lényegesen befolyásolhatja.

FELHASZNÁLT IRODALOM

1. Damó László: Katonai Lexikon. Zrínyi Katonai Kiadó, Budapest, 1985.
2. Rosenau, W G. Minden helység új csata: A korszerű városi hadviselés tapasztalatai. In Studies in Conflikct and Terorism, Új Honvédségi Szemle, Budapest, 1997. 51. évfolyam 4. szám. Fordítás: Szabó Ferenc
3. Mráz István: A katonai felső szintű vezetés információs rendszerének korszerűsítése I. Új Honvédségi Szemle, Budapest, 2001, 55. évfolyam 7. szám.
4. Mr. Lester W. Grau: Urban Warfare Communictions. A Contemporary Russian View, Thurts Red July, 1996. call. Army. Mil/fmsopubs/issues/urbanwar/urbanwar.htm
5. Tóth Csaba: Lethal Weapon „X”. Fordítás a Defence News Vol. 15. No. 6 alapján. Új Honvédségi Szemle, Budapest, 2000, 54. évfolyam, 5. szám.
6. Dr. Makkay Imre: Az elektronika, távközlés és az elektronikai hadviselés a XXI. században. Nemzetvédelmi Egyetemi Közlemények, Budapest, 1997, 1. évfolyam, 2. szám.

Tatárka István

A BM OK FŐIGAZGATÓSÁG ÉS TERÜLETI SZERVEI HÍRADÓ ÉS INFORMATIKAI RENDSZEREI

A Katasztrófavédelem feladatrendszerét az alábbi törvények, kormányrendeletek határozzák meg:

-A katasztrófavédelem (polgári védelem) számára a lakossági riasztással kapcsolatos feladatokat az 1993. évi CX. törvény és az alapján kiadott 133/1994. (X.21.) sz. kormányrendelet, a Kormány 60/1997.(IV.18.) Korm. rendelete valamint a polgári védelemről szóló 1996. évi XXXVII törvény szabályozza.

-1996. évi XXXI. törvény a tűz elleni védekezésről, a műszaki mentésről és a tűzoltóságról

-A katasztrófák elleni védekezés irányításáról és a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről szóló 1999. évi LXXIV törvény.

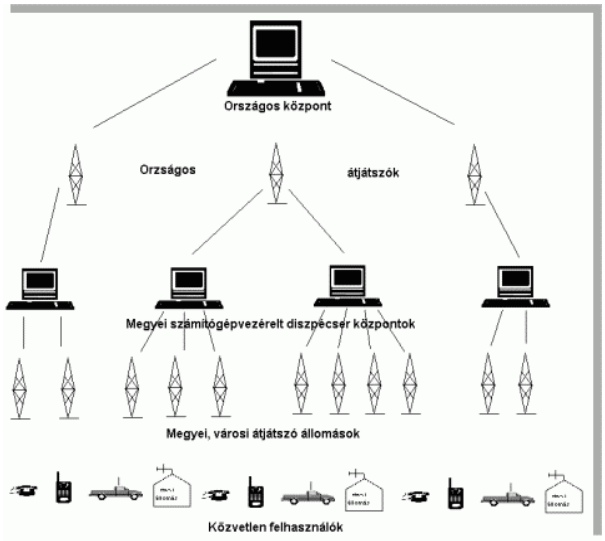
A Katasztrófavédelem híradó és informatikai rendszerei

- Katasztrófavédelmi URH, RH rádió rendszer
- Duna-Majna-Rajna Információs Segélyhívó Rendszer
- Tiszai Információs Segélyhívó Rendszer
- Balatoni és Velence-tavi Viharjelző Rendszer
- Lakossági riasztó és tájékoztató rendszerek
- Informatikai stratégia (BM OKF és területi szervei informatikai hálózatai, levelező rendszer, SEVESO II, GIS, SIS, RODOS, Adatcsere központ, Amar)

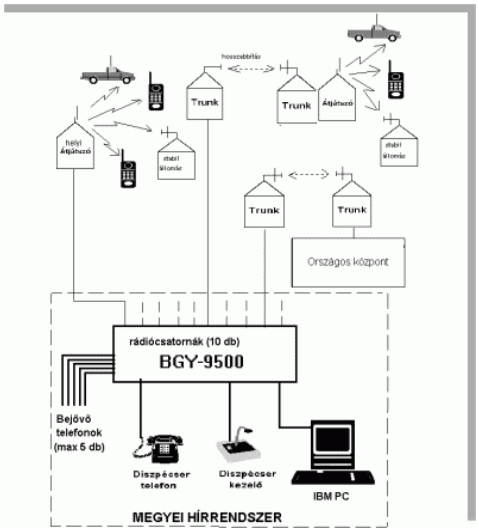
Katasztrófavédelmi URH, RH rádió rendszer

A BM Országos Katasztrófavédelmi Főigazgatóság országos gerinchálózata

Az országos URH rádiórendszer elvi vázlata



A megyei Katasztrófavédelmi Igazgatóságok rádiórendszere



Duna-Majna-Rajna Információs Segélyhívó Rendszer (DISR)

A rendszer feladata és szolgáltatásai:

A Duna hazai szakaszán a rádiós rendszer a vízi balesetek elkerülésének, illetve baleseti helyzetben a mentés szervezésének alapvető hírközlési eszköze.

A veszélyes áruk szállításával kapcsolatos feladatok tekintetében (ADR-hajók) a hajózási hatóság által előírt bejelentkezési közlemények vétele, rögzítése a hajózási és rendőrhatóság részére *a szükséges adatok továbbítása.*

A hajók műszaki meghibásodása, a veszélyes rakományokkal összefüggő esetleges havariák esetén több szervezet összehangolt munkájának koordinálása.

Vízállások közlése a vízügyi szervektől kapott adatok alapján.

A parti létesítményekben és hajózási műtárgyakban keletkezett károkról több szervezet kap gyors és azonos tartalmú információt, amely lehetővé teszi a hatékony szabályozási, illetve javítási munkákat.

A hajózási útvonalakon előforduló bűncselekményekről, gyanút ébresztő hajózási manőverekről a teljes dunai szakaszt átfogó monitoring rendszer tájékoztatást ad a hatóságok felé.

A hajózási hatóság által kibocsátott átmeneti rendelkezések /hajózási információk/ hatósági közlemények előre meghirdetett időpontban és csatornán való közzététele.

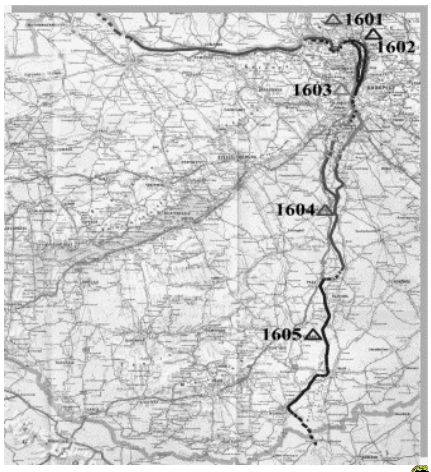
A kárelhárítás szervezésében, irányításában a nagy kiterjedésű kommunikációs rendszer biztosította lehetőségek kihasználása.

Elemi csapások, természeti katasztrófák esetén a veszélyeztetett területek lakosságának gyors és közvetlen tájékoztatása.

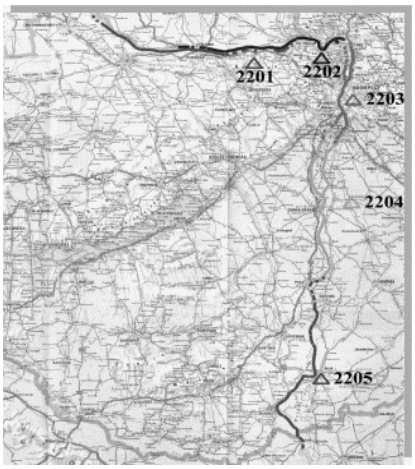
A dunai környezeti szennyezésekkel kapcsolatos információk gyűjtése (a Duna-völgyi regionális vízminőségi riasztórendszerhez való csatlakozás).

A Duna magyarországi szakaszán telepített átjátszó állomások

16. Segélyhívó csatorna



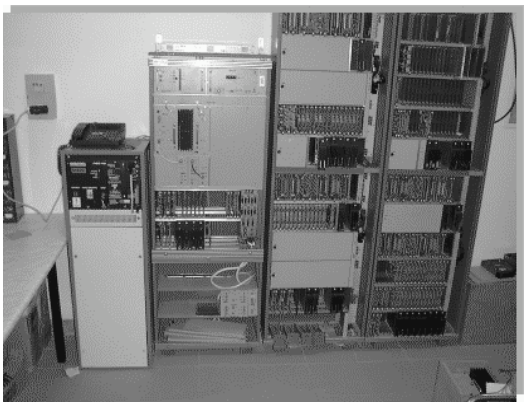
20. Információs csatorna



A rendszerben telepített átjátszó és mikroállomások

Motorola ájá.

mikroállomás



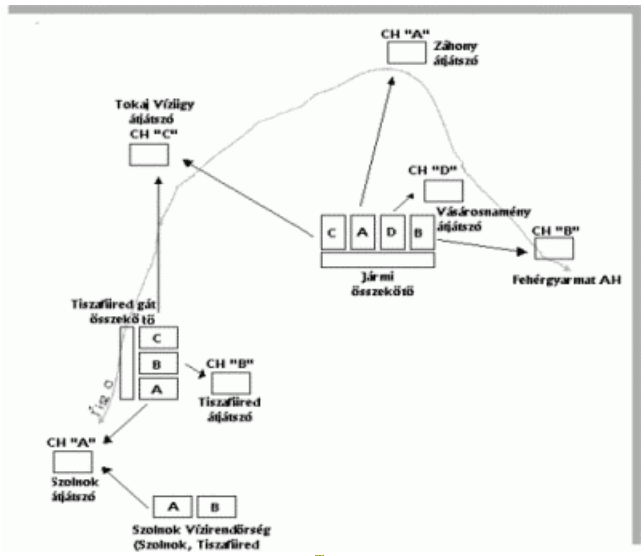
Tiszai Információs és Segélyhívó Rendszer (TISR)

Tiszai Információs és Segélyhívó Rendszer

Célja:
A Tisza mentén megvalósítsa a hajózásban, vízi turizmusban egyaránt használható rádióhálózatot, melyet árvizek és más környezeti katasztrófák idején mind a hivatalos szervek, mind a polgári lakosság igénybe tud venni.

A Rendszer (TISR) „békeidőszakban" a folyón közlekedő hajókról, kompokról és a víziturizmusban résztvevőktől beérkező hívásokat, segélykéréseket fogadja, illetve továbbítja az illetékes szervek felé.

A rendszer felépítése, működése:



A rendszer alkalmazási lehetőségei

- vízminőség figyelő monitoring rendszer adatainak fogadása, illetve továbbítása
- árvízelőjelzés a Kárpátalján kialakított rendszerhez való kapcsolódás révén.
- a hajózási 16-os nemzetközi segélykérő rádiócsatornán érkező segélyhívások fogadása és figyelemmel kísérése
- az információs 22 (28) -as csatornán a biztonságot meghatározó információk közzététele (vízállás, időjárás, korlátozások, folyami munkák, vízi rendezvények stb.)
- az Információs Központban a bejelentések naplózása, továbbítása az érintett hatóságok felé, valamint a közérdekű adatok tárolása, frissítése, és adatátviteli csatornákon történő elérésének biztosítása.

Balatoni Információs Segélyhívó Rendszer (BISR)

Balatoni Viharjelző Rendszer (BVR)

Balatoni Információs Segélyhívó Rendszer

Közösségi célokat szolgáló trönkölt rádiórendszer.

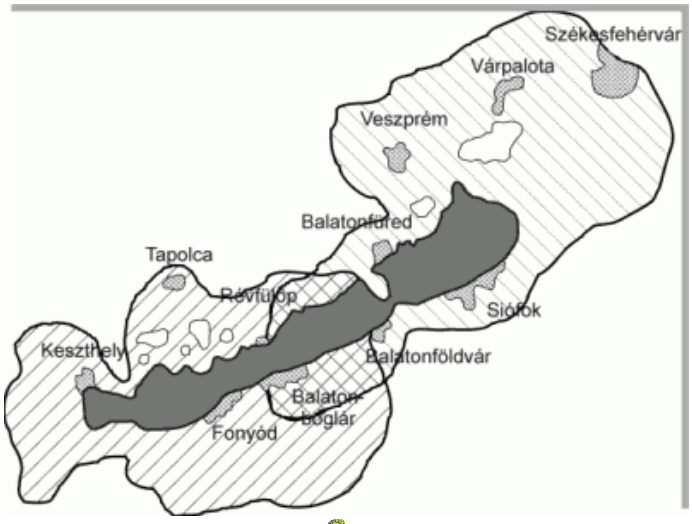
Elsősorban viharok, közlekedési és vízi balesetek, egyéb rendkívüli események kapcsán keletkező kommunikációs igényeket hivatott kielégíteni.

A rendszernél a segélyhívás lehetősége mellett a megelőzés és a tájékoztatás biztosítása volt a cél.

Vízimentés koordinációja a Vízirendészet, a Katasztrófavédelem, Karitatív Mentőszolgálatok és más szervezetek közreműködésével.

A felújított Viharjelző Rendszer távvezérlése

A Balatrönk Rendszer működési területe a régióban



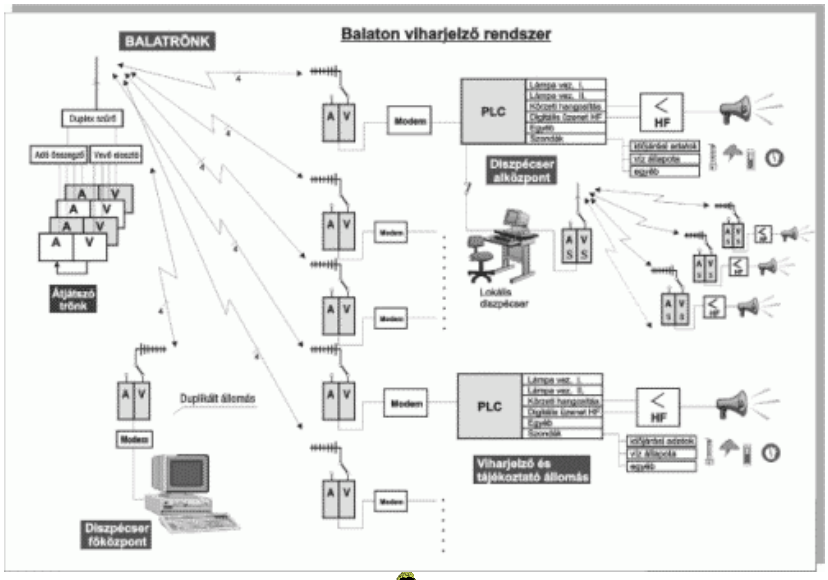
A BISR funkciói a BVR működésében

- Meteorológiai adatok küldése
- Vezérlési parancsok továbbítása, visszaigazolások küldése
- Diagnosztikai adatok továbbítása
- A rádiós adatátvitel biztosítása a központ és alállomások között

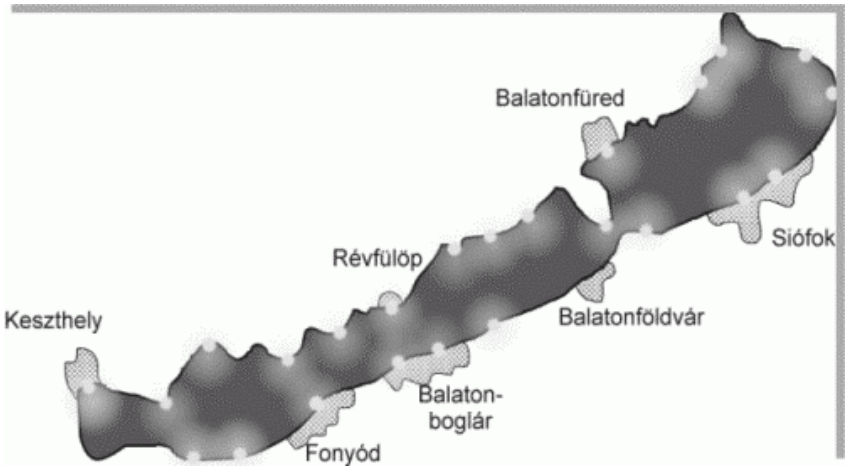
A fényjelző funkciói

- alapszintű állapot (nincs villogás)
- első fokozat, 30 villogás/perc
- második fokozat 60 villogás/perc

A BVR sematikus vázlata



A viharjelzőrendszer jelenleg látható területe



A parton található viharjelző egységek elhelyezkedése

Velence tavi Viharjelző Rendszer (VVR)

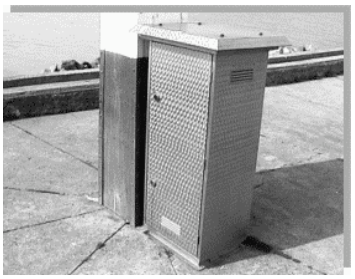
Velence tavi Viharjelző Rendszer

Az új Balatoni és Velence tavi Viharjelző Rendszer

Előnyei:

- *Közös vezérlőközpont, önálló balatoni és Velence tavi indítással*
- *Korszerű felépítés*
- *Mozgó alkatrészek nélküli működés*
- *Speciális, időjárásálló védelemmel ellátott egységek*
- *Magas megbízhatóságú kódolt adatátvitel*
- *Többfunkciós felhasználás*
- *Alacsony üzemeltetési költségek*

A letelepített új rendszer részei



Lakossági riasztó és tájékoztató rendszerek

A katasztrófavédelem (polgári védelem) számára a lakossági riasztással kapcsolatos feladatokat az 1993. évi CX. törvény és az alapján kiadott 133/1994. (X.21.) sz. kormányrendelet, a Kormány 60/1997.(IV.18.) Korm. rendelete valamint a polgári védelemről szóló 1996. évi XXXVII törvény szabályozza.

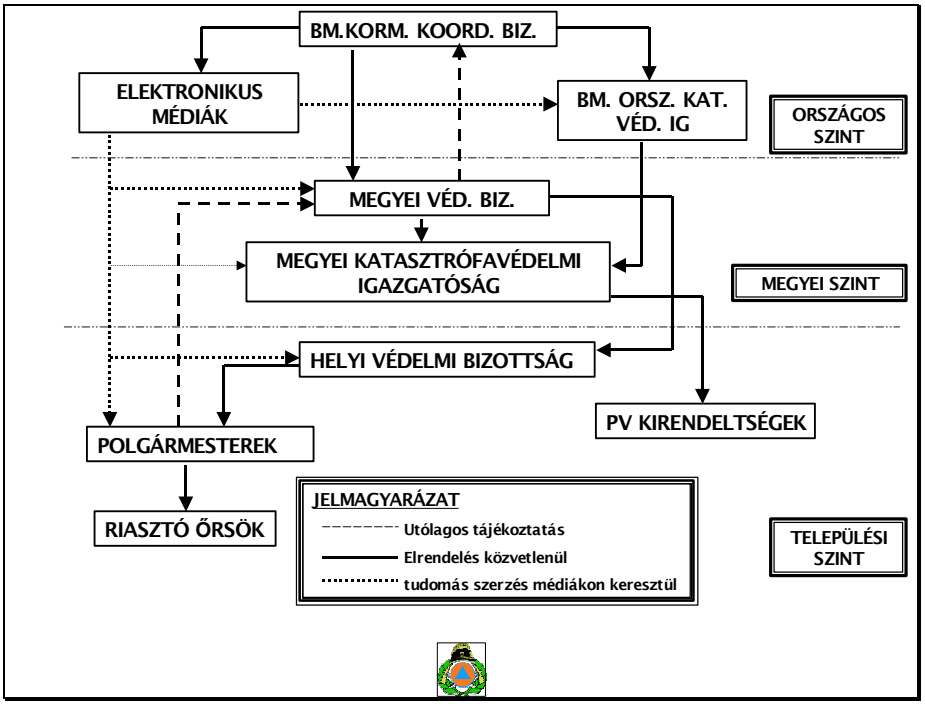
Lakossági riasztás-tájékoztatás megoldásának lehetőségei

A katasztrófavédelem riasztási rendszerén, motorszirénákkal.

Lakossági riasztó-tájékoztató lokális rendszereken, elektronikus eszközökkel.

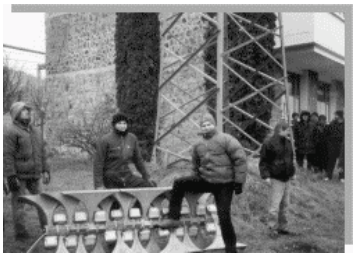
Az önkormányzatok által a helyi lehetőségek felhasználásával, illetve szükség riasztó eszközökkel.

Közszolgálati műsorszóró rádió- és televízió stúdiókból és a nem közszolgálati műsort sugárzó rádió- és televízió adó állomások bevonásával.

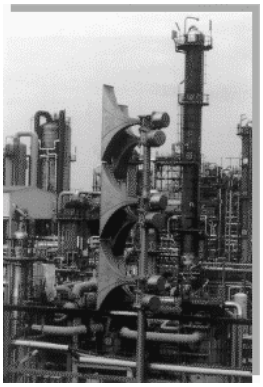


Lakossági riasztó és tájékoztató eszközök

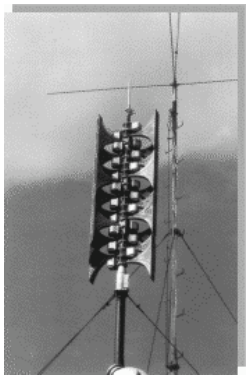
Elektronikus riasztó-tájékoztató eszközök



Telepítés előkészítése



Termelő cégnél telepítve



Lakossági riasztás céljából háztetőre telepítve

Motoros szirénák

(csak riasztásra alkalmas)

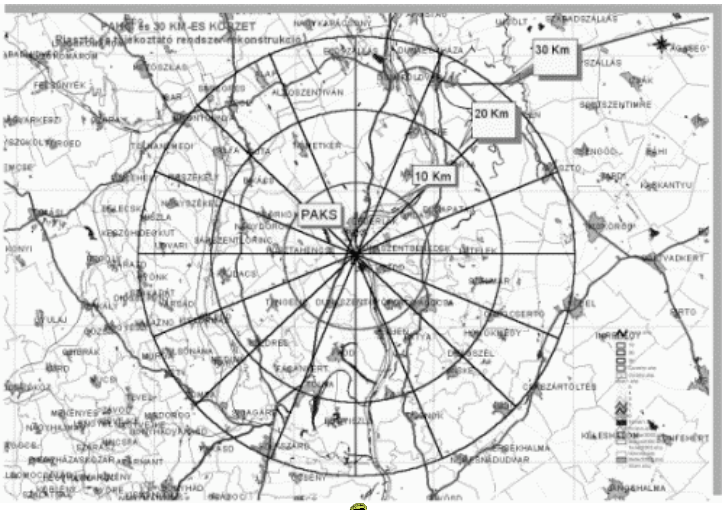
Vasbeton oszlopra telepítve

Háztetőre telepítve

Mobil kivitelû tájékoztató-riasztó eszköz

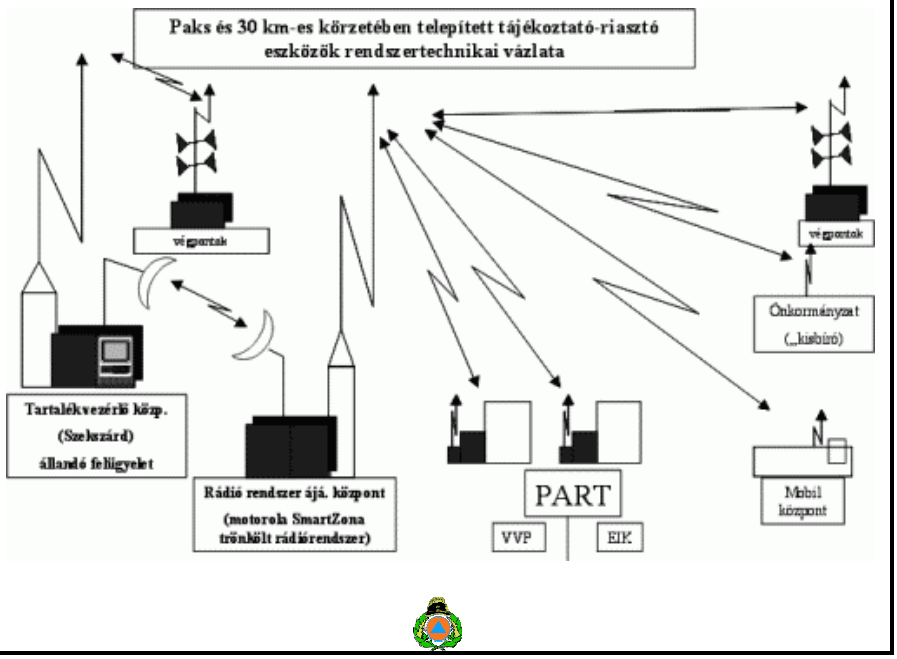
Szükség riasztó eszköz

Paks és 30 km-es körzetében a riasztó-tájékoztató rendszer felújítása



A projekt ütemterve

Év	sugár (km)	darab	ár USD	ár HUF	terület (km2)	lakos	település
2000	r = 10	66	854 110	298 938 500	452	58 663	13
2001	r = 20	78	857 430	300 846 000	804	84 200	20
2002	r = 30	83	914 660	320 131 000	1 570	82 187	39
összesen	30	227	2 626 200	919 915 500	2 826	225 050	72



Informatikai stratégia

BM OKF és területi szervei informatikai hálózatai, levelező rendszer, SEVESO II, GIS, SIS, RODOS, Adatcsere központ, Amar

Az információtechnológia rohamos fejlődése új távlatokat nyitott a közigazgatáson belül a katasztrófavédelmi szervezetek előtt.

A már hagyományosnak nevezhető irodai alkalmazásokról (szövegszerkesztés, táblázatszerkesztés, személyzeti és gazdálkodási modulok) el kell mozdulni az aktív döntéstámogató rendszerek irányába.

A katasztrófák elleni védekezés irányításáról és a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről szóló 1999. évi LXXIV törvény 14. paragrafusa határozza meg a katasztrófavédelmi célú távközlési és informatikai rendszerek egységes irányítási rendszerbe történő kialakítását és működtetését.
Ebből, illetve a Belügyminisztérium 1999-2002-re szóló ágazati szintű informatikai stratégiájából kiindulva határozzuk meg a katasztrófavédelem informatikai stratégiáját.

Általánosságban az informatikai rendszerekkel szemben felmerülő alapvető követelmények az alábbiakban foglalhatók össze:

- Pontos információk az adott problémáról
- Gyors hozzáférés az adatokhoz
- Döntés előkészítés -segítés
- „Automatizált" működés, minimális emberi felügyelettel
- Ok-okozati összefüggések prognosztizálása
- Maximális megbízhatóság, akár szélsőséges körülmények között is

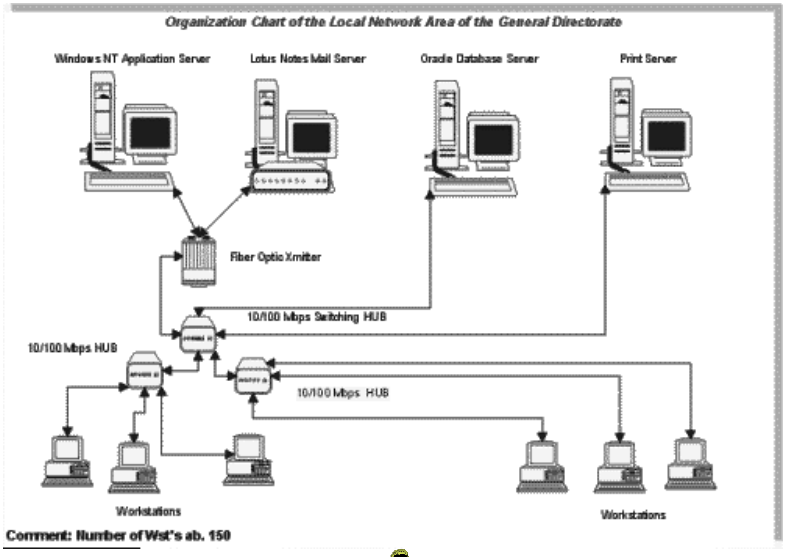
A katasztrófavédelem esetében speciálisan felmerülő „extra" igények:

- A szabványosnál magasabb százalékú rendelkezésre állás
- Hibatűrő rendszer kialakítása
- Adat replikálás
- Szélsőséges körülmények között a működőképesség és funkcionalitás megőrzése
- Folyamatos adatgyűjtés és kiértékelés a távoli érzékelők által szolgáltatott adatok alapján

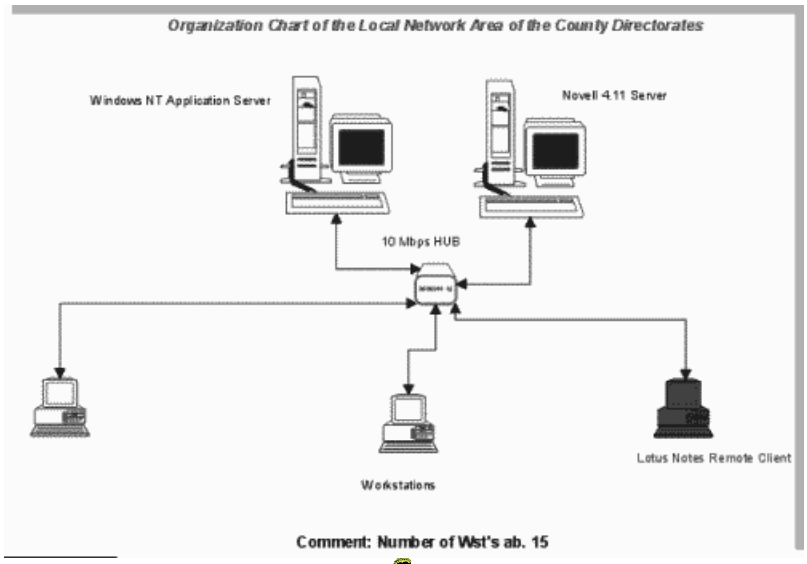
Célunk egy egységes, integrált, jól menedzselhető, redundáns kommunikációs infrastruktúra kialakítása.

- Az IP alapú hálózatok jól mendzselhetőek és felügyelhetőek.
- Napjainkban a legtöbb eszköz (számítógéphálózati eszközök, telefonközpontok, mobiltelefonok, mérőrendszerek, jeladók, stb) rendelkezik IP csatoló felülettel
- Az IP technológia a számítástechnikai eszközök közötti kommunikáció legelterjedtebb közege
- Az IP protocoll távoli adatkommunikáció számára az egyik legmegbízhatóbb protokoll (hiszen kifejlesztésekor ez volt az egyik szempont)
- Az IP hálózat nem csak adatkommunikációt tesz lehetővé, hanem hang és videó jel is átvihető vele
- Az IP az internet alap protokollja, könnyű csatlakozást tesz lehetővé a világháló felé

BM OKF belső informatikai hálózata

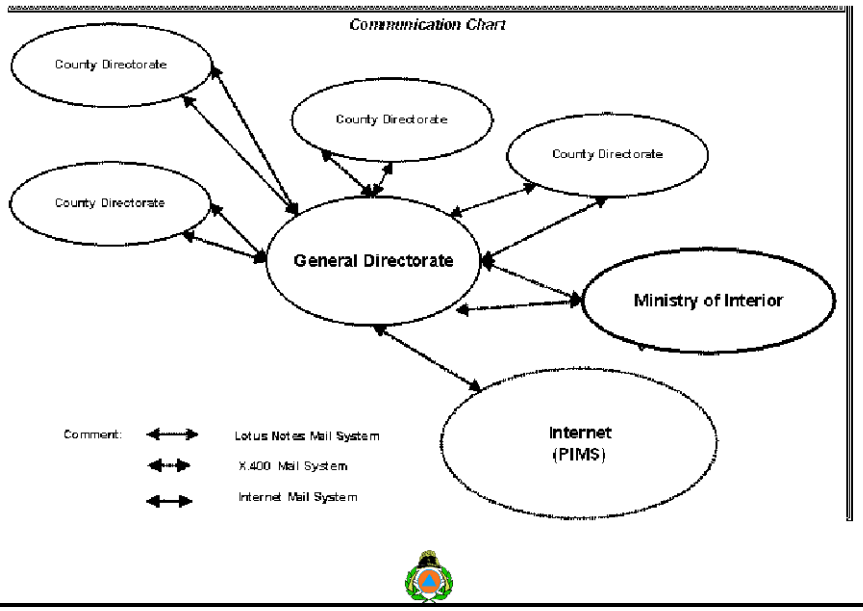


Megyei Katasztrófavédelmi Igazgatóságok belső hálózata

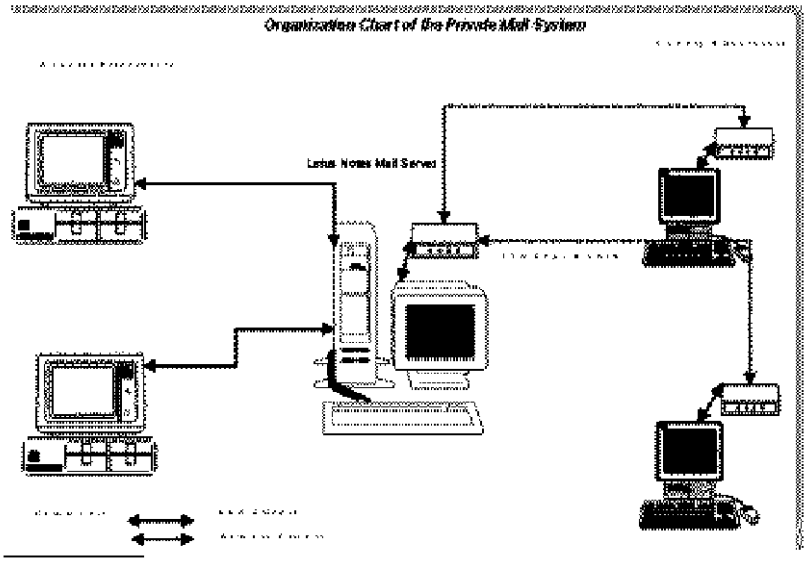


A Belügyminisztérium levelező rendszerei

(a katasztrófavédelem viszonylatában)



A Katasztrófavédelem belső levelező rendszere



Az 1999. évi LXXIV törvény IV. fejezetében előírt feladatok (SEVESO II) informatikai biztosításának rendszerterve

Adatbázis struktúrák koncepciója

* Külső védelmi tervek adatbázisa a BM Országos Katasztrófavédelmi Főigazgatóság területi szerveinek és az érintett települések polgármestereinek közreműködésével.

* Belső védelmi tervek adatbázisa a veszélyes üzemek létesítmény üzemeltetőinek közreműködésével (az üzemeltető köteles adatokat szolgáltatni a hatóság megyei, illetve körzeti szerve számára a külső védelmi terv kidolgozásához.

* Veszélyes anyagok katalógusai (a veszélyes anyagok jelenlétében történő elhárítási és felszámolási feladatok adatbázisa (HOMMEL, SIX, VAKOND, VESVE)

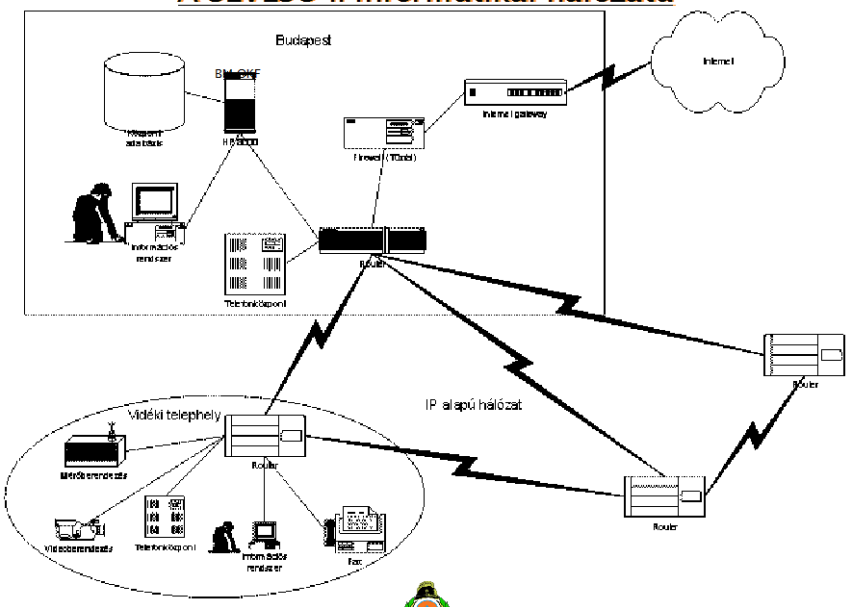
* Katasztrófavédelmi monitoring rendszer által biztosított mérési eredmények adatbázisa

* Térinformatikai adatbázis (vizek, vízfolyások, elöntési modellek, kitelepítési objektumok, nemzeti és nemzetközi erőforrás analízis)

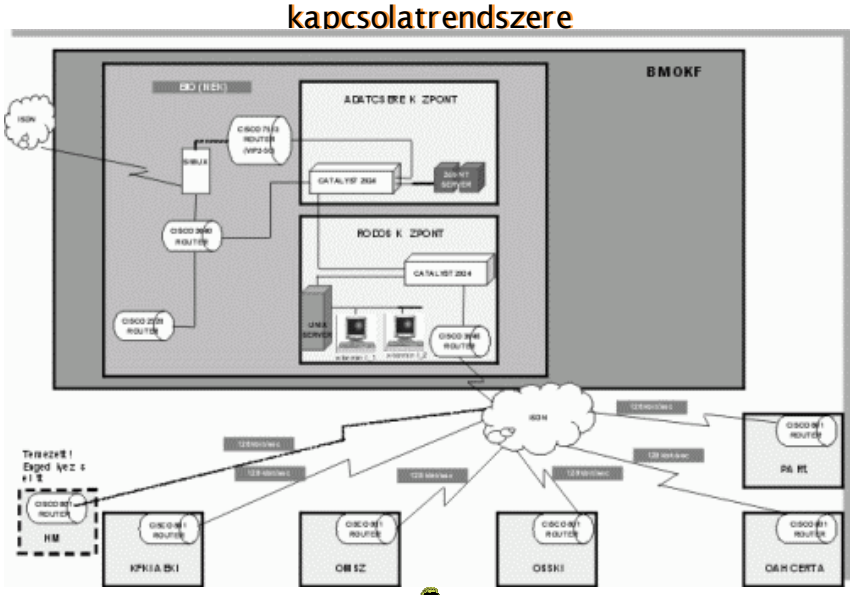
A Katasztrófavédelmi Tv. a IV. fejezetében igen széleskörűen határozza meg a veszélyes anyagokkal és technológiákkal üzemelő létesítmények nyilvántartásainak, biztonsági jelentéseinek, védelmi terveinek, felülvizsgálatainak stb. hatósági követelményeit.

A **Katasztrófa kockázati adatbázis** létrehozásának célja az, hogy a Tv. által jól meghatározott kritériumok alapján besorolja a létesítményeket, egyben gyors és pontos adatokat szolgáltasson a megelőzés, védekezés, kitelepítés feladatának ellátásához.

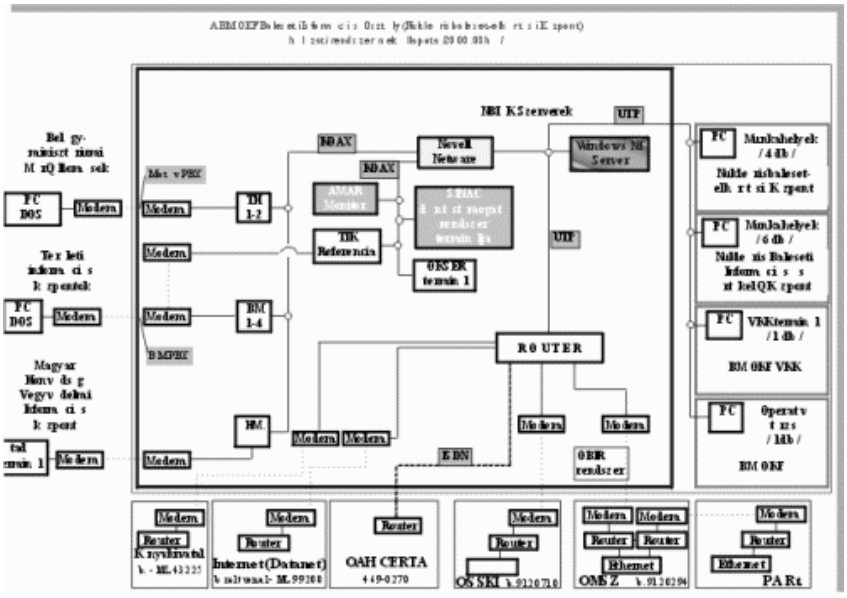
A SEVESO II informatikai hálózata



A RODOS, valamint az ADATCSERE Központ kapcsolatrendszere

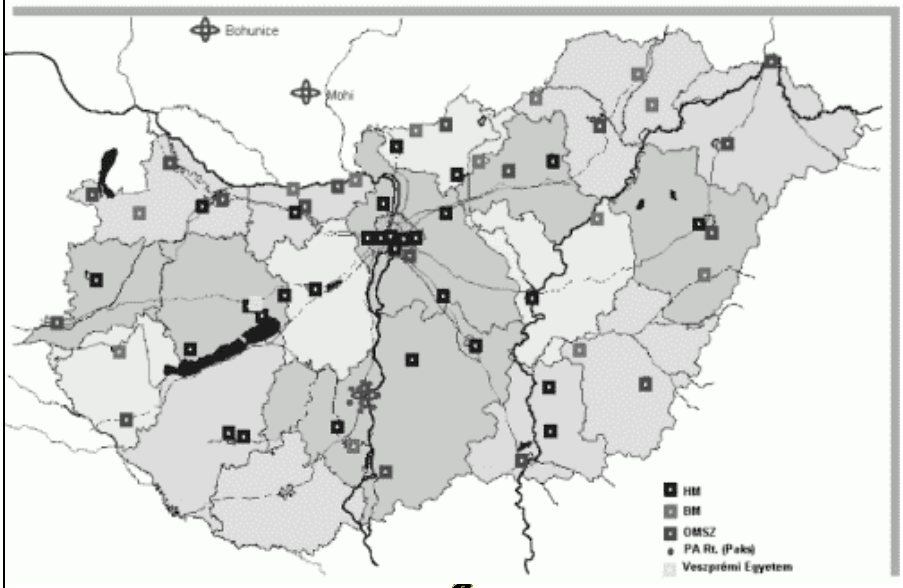


A BM OKF BIO hálózati rendszere



A Nemzeti RODOS Központ

Az AMAR Rendszer mérõállomásai



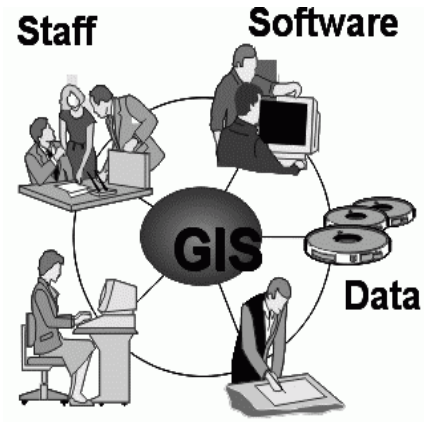
GIS térinformatikai rendszer

A legnagyobb mértékű katasztrófaveszélyt természetes vízfolyásaink okozzák. A veszélyeztetettség mértékének minél pontosabb előrejelzéséhez, az elöntések topológiájához, a védekezés, a kitelepítések, a kitelepítettek elhelyezése stb. gyors, pontos és szervezett végrehajtásához van szükség **Árvíz és belvíz védekezési adatbázisra** .

Az adatbázishoz a térképészeti alapadatok alapján csatolt grafikus, táblázatos és szöveges állomány fűzhető, amelyek megmutatják a helyzethez tartozó veszélyeztetettség mértékét, a védekezéshez, felszámoláshoz szükséges és rendelkezésre álló humán és anyagi erőforrásokat.

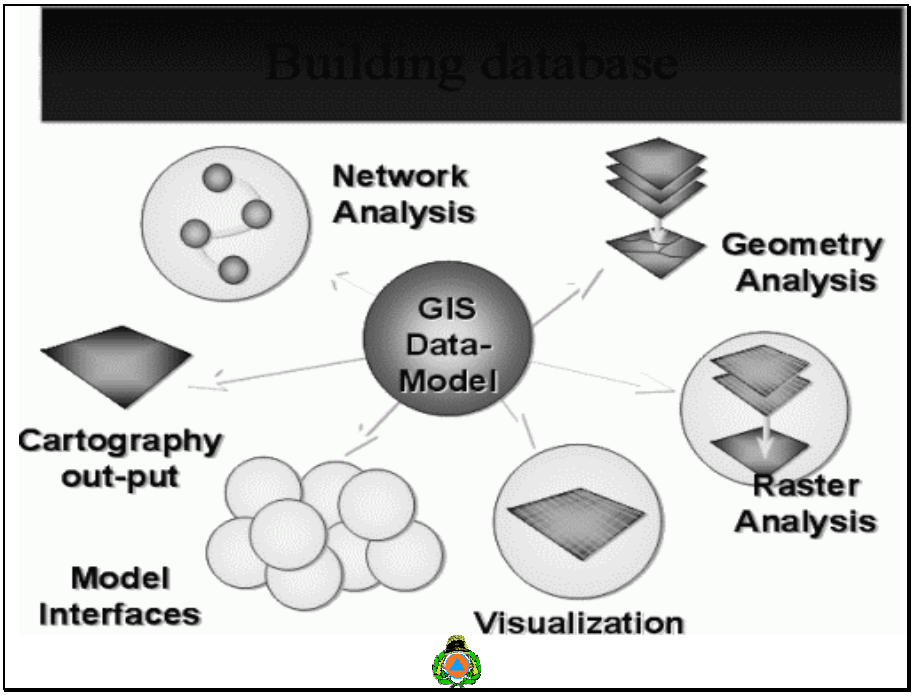
Ez az adatbázis természetesen nem szorítkozhat a határokon belüli területekre, hanem – mint azt a TISZA 2000 és a TRANSCARPATIA munkaműhelyek és gyakorlatok is bizonyítják – a vízfolyások mentén szomszédos országokra is ki kell terjeszteni.

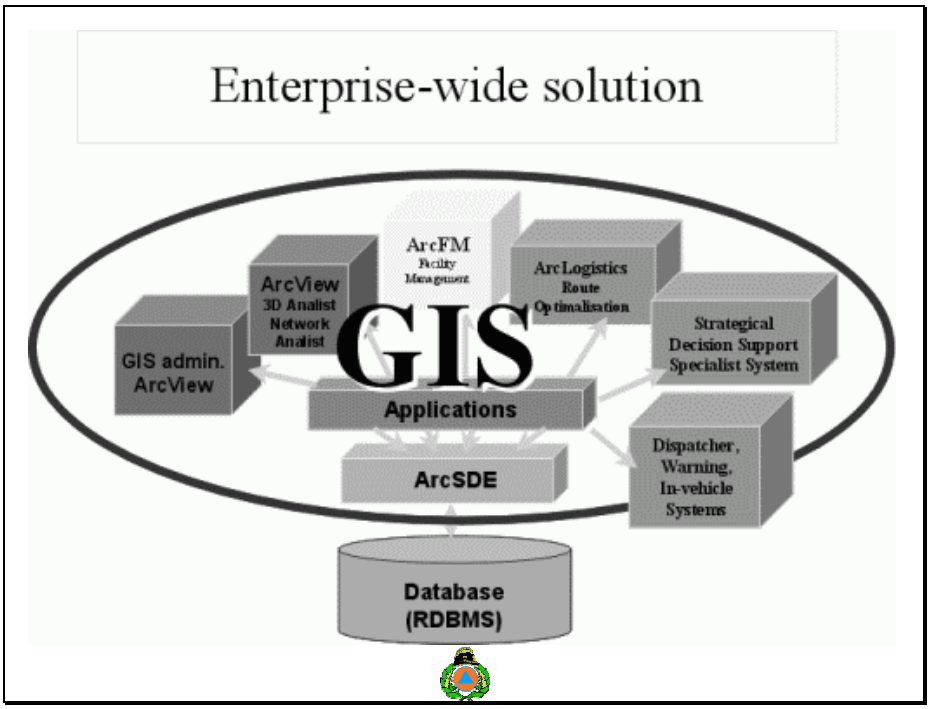
Az adatközpont létrehozására, az adatbázisok feltöltésére és karbantartására megoldást biztosít a GIS.



- An Information Technology
- a Data Management Method
- an aspect
- „Our common language”

» (Jack Dangermond)





Humán informatikai stratégia

Az informatika emberi oldaláról általában kevés szó esik, holott mint az információtechnológia (IT), mind az adatbázisok és más alrendszerek működtetése elképzelhetetlen a géppel, rendszerrel kommunikálni tudó, az IT - t mesterien felhasználó ember nélkül.

Tervezzük, hogy 2001-2002 években a hatósági megelőzési és a veszélyhelyzet kezelési területen dolgozók részére adatbázis kezelői, az ügyintézői állomány részére hálózati (LOTUS NOTES, E-mail, Internet, Intranet) alapképzést indítunk.

Köszönöm megtisztelő figyelmüket!

Révész Gyula

A HÍRADÓ KIKÉPZÉS AKTUÁLIS JELLEMZŐI

Bevezető

A Magyar Honvédség stratégiai felülvizsgálatának és átszervezésének célja, a korábbinál kisebb létszámú, korszerű technikai eszközökkel felszerelt, felkészített katonákból álló ütőképes hadsereg létrehozása.

A Magyar Honvédség kiképzési rendszerére döntő befolyást gyakorol a Magyar Köztársaság védelmi politikája, mely deklarálja, hogy az ország megvédésére készül, így a védelmi elképzelések kerülnek előtérbe.

Az előadásomban a híradó kiképzés jelenével és a jövőjével foglalkozom, a XXI. század kihívásának tükrében.

A fegyveres erők felkészítésének alapjai

A Magyar Köztársaságban a parlamenti demokrácia kialakulásával a Biztonságpolitikai Alapelveket a Külügyminisztérium, a Honvédelmi Alapelveket pedig a Honvédelmi Minisztérium terjeszti a parlament elé, mint döntéshozó elé.

Az Alapelvek elfogadása után kerülnek kidolgozásra az ország védelmével kapcsolatos törvények, melyek alapjai a Magyar Honvédség szabályzatainak, utasításainak, intézkedéseinek és doktrínáinak.

Jól látható tehát, hogy a fegyveres erők felkészítése, a kiképzés célja, tartalma, követelménye úgy követi a változásokat, ahogy a politikai érdekek megkívánják.

A Magyar Honvédség legfontosabb békefeladatai:

- a csapatok folyamatos felkészítése és kiképzése,
- válságkezelés katonai feladatainak ellátása,
- nemzetközi kötelezettségek teljesítése.

A továbbiakban a felkészítéssel és kiképzéssel foglalkozom, hármas tagolás szerint:

- a sorozott állomány,
- a szerződéses állomány
- a hívatásos állomány képzésével.

A sorozott állomány képzése

Jelenleg a Magyar Honvédség átmeneti időszakot él meg a sorköteles katonák kiképzésével kapcsolatban, hiszen köztudott, hogy a 9 hónapos sorkötelezettségről 2002. évben áttérünk a 6 hónapos sorkatonai szolgálati időre.

A kilenc hónapos sorkatonai szolgálat váltási rendje (háromhavonta) biztosítja az alegységek folyamatos kiegészítését.

Alapkiképzés:

Az alapkiképzések tervezését, szervezését, végrehajtását az érvényben lévő utasítások, szakutasítások, kiképzési programok alapján hajtják végre a Magyar Honvédség kiképző központjaiban. Az alapkiképzés időtartama 180 óra.

Szakbeosztásra történő felkészítés:

A híradó-szakkiképzésre Szombathelyen kerül sor, két híradókiképző zászlóaljban. A zászlóaljak 13 szakcsoportnak megfelelő felépítésűek. 19 híradó szaktanterem és 39 híradókiképző technika áll rendelkezésükre. A szakkiképzés időtartama 120 óra, melyből aránytalanul magas 36 óra a távírász (Morse), és gépelési gyakorlat.

Híradó-szakkiképzést folytatnak még a csapatok híradó szakalegységei is, valamint a parancsnokságom alatt álló híradózászlóalj is.

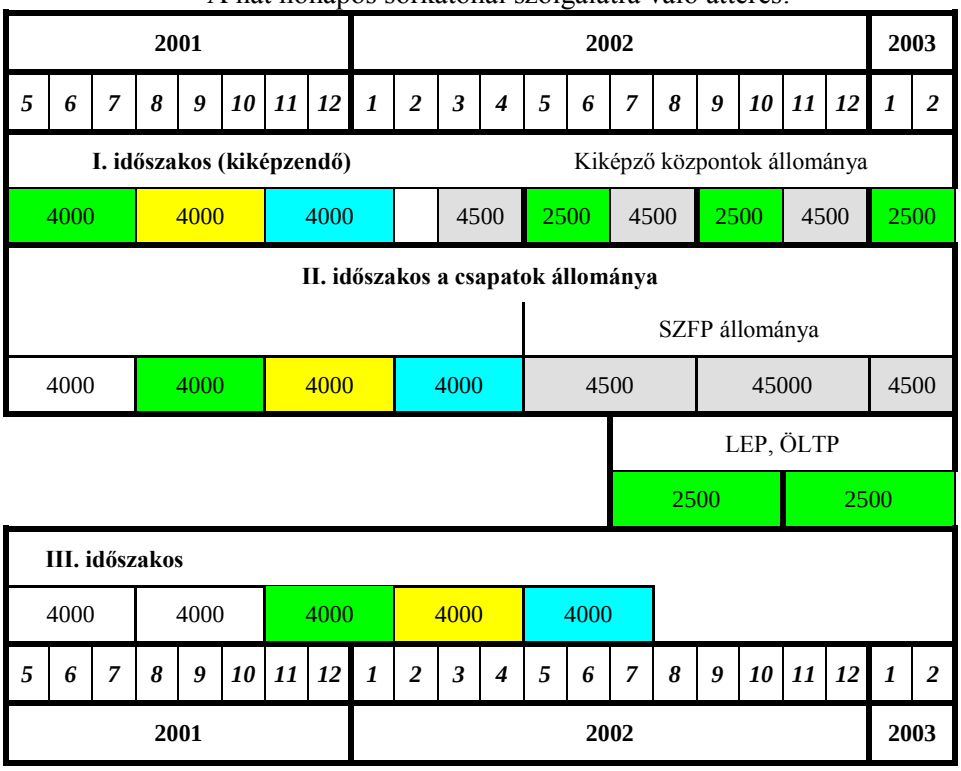
A 43. Nagysándor József Híradózászlóalj az alapkiképzést követően kapja meg a szakkiképzésre kijelölt állományt. A szakkiképzés időtartama 120 óra.

Kiképzési rendszer (9 hónapos)

<table>
<tr><th>1. hó</th><th>2. hó</th><th>3. hó</th><th>4. hó</th><th>5. hó</th><th>6. hó</th><th>7. hó</th><th>8. hó</th><th>9. hó</th></tr>
<tr><td colspan="3">első harmad</td><td colspan="3">második harmad</td><td colspan="3">harmadik harmad</td></tr>
<tr><td colspan="3" rowspan="2">alapkiképzés
(180 óra)
szakkiképzés
(120 óra)</td><td colspan="3">alegység szakkiképzése</td><td colspan="3">szintentartó
foglalkozások</td></tr>
<tr><td colspan="6">480 óra</td></tr>
</table>

Sorállományú rajparancsnok jelöltek, vagy más fontos beosztásba tervezet katonák a saját szakalegységüknél kerülnek kiválasztásra és felkészítésre.

A hat hónapos sorkatonai szolgálatra való áttérés:



A hat hónapos sorkatonai szolgálat:

A bevonulás rendje meghatározó a kiképzés rendjére is. A hat hónapos sorkatonai szolgálat bevezetésével kéthavonta kerül sor bevonulásra.

Négyhavonta a Szárazföldi Parancsnokság állományába, négyhavonta a Légierő Parancsnokság, ill. az Összhaderőnemi Logisztikai Támogató Parancsnokság állományába kerül sor a bevonulásra.

A sorkatona az első időszakban, a kiképzőközpontban alap- és szakbeosztásra történő felkészítést, a második (esetleg harmadik) időszakban a csapatoknál kötelékkiképzést hajt végre.

Előnye az előző rendszerhez képest, az alapkiképzés egységes követelmény szerint kerül végrehajtásra a kiképző központban, a szakfelkészítés kötelékkiképzés keretében az alakulatnál kerül végrehajtásra.

Hat hónapos sorkatonai szolgálat

Hó-nap	Bevo-nulás	2002										2003	
		3	4	5	6	7	8	9	10	11	12	1	2
SZFP	II	I. id.		II. id.									
	IV.					I. id.		II. id.					
	VI.									I. id.		II. id.	
LEP, ÖL TP	III.			I. id.		II. id.							
	V.							I. id.		II. id.			
	I.											I. id.	

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 híradózászlóaljnál jelenleg gép- és harcjármű-vezetői, híradó berendezés kezelői (R-142, R-145, R-1406, V-36) helyek kerültek rendszeresítésre.

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 hívatásos állomány képzése

A tiszthelyettes és zászlósképzés

Jelenleg még meglévő tiszthelyettes képzés az alapképzésre korlátozódik.

Érettségi vizsgával rendelkező fiatalokat képeznek át híradó tiszthelyettessé, de nem készítik fel a vezetési-irányítási, parancsnoklási feladatokra.

A jelenlegi állománytáblák nem biztosítják az előmenetelt a szakbeosztású, így a híradó beosztású tiszthelyettesek részére. A legmagasabb elérhető rendfokozat törzsőrmester.

Híradószázad tiszthelyettesi előmenetel

Rf.	zászlós	főtörzsőrmester	törzsőrmester	őrmester
Beosztás	századvezénylő tts.	szakaszvezénylő tts.	állománysparancsnok	híradó beosztás

A tiszthelyettes és zászlósképzés jövője:

- ⌦ ki kell jelölni a tiszthelyettesi és zászlósi feladat és munkaköröket,
- ⌦ kellő motiváló erő a pályaképre, kiszámítható előmenetel és járandósági rendszer,
- ⌦ a beosztásokhoz tartozó képesítési, alkalmassági követelmények kidolgozása,
- ⌦ alap-, át-, és továbbképzési rendszer, nyelvképzés lehetősége,
- ⌦ külszolgálat lehetősége.

A tisztképzés

A jelenlegi tisztképzés alap- és továbbképzésre épül.

A jelenlegi állománytáblák csak korlátozottan biztosítják az előmenetelt a szakbeosztású, így a híradó beosztású tisztek részére.

Híradózászlóalj tiszti előmenetel

	Főtiszt	Tiszt		
Rf.	alezredes, őrnagy	százados	főhadnagy	hadnagy
Beosztás	parancsnok és helyettesei	részlegvezetők, szd. parancsnokok	szd. pk. helyettesek, szaktisztek	szakaszparancsnokok

A tisztképzés jövője:

- ⌦ ki kell jelölni a tiszti és főtiszti feladat és munkaköröket,

- kellő motiváló erő a pályaképre, kiszámítható előmenetel és járandósági rendszer,
- a beosztásokhoz tartozó képesítési, alkalmassági követelmények kidolgozása,
- alap-, át-, és továbbképzési rendszer, nyelvképzés lehetősége,
- rendszeres időszakonkénti szakmai felkészítés
- külszolgálat lehetősége.

XXI. század kihívása a híradó kiképzésben

A XXI. század katonai műveleteinek hatékonyságát és eredményességét az ellenséggel szembeni információs fölény fogja meghatározni. Ehhez szükséges az új technológiák beszerzése és alkalmazási feltételeinek megteremtése a Magyar Honvédségben is.

A technológiai fejlődés lehetőségei:

- számítógépes támogatottság,
- adatbázisok osztott használata,
- elektronikus levelezés,
- elektronikus harctér megjelenítés,
- videokonferencia alkalmazások,
- fegyverirányítási rendszerek,
- szélessávú adatátvitel,
- korszerű adattovábbítási eljárások alkalmazása.

Az előbbi felsorolásból is következik, hogy a XXI. század hadseregének széles látókörű, magasan kvalifikált, korszerű ismeretekkel rendelkező katonákra van szüksége.

A jövő feladatai közé tartozik a felkészítés és kiképzés terén:

- a békefenntartói kiképzés,
- a tiszti, tiszthelyettesi, és szerződéses állomány át- és továbbképzésének kiszélesítése, tanfolyam rendszerek kidolgozása és meghonosítása,
- fokozott odafigyeléssel tervezni, szervezni és végrehajtani a tanintézeti hallgatók csapatgyakorlatát,
- a sorállomány kiképzésének korszerűsítése,
- új oktatási lehetőségek (távoktatás), valamint az új oktatási segédeszközök alkalmazási lehetőségének megteremtése.

A híradó szakkiképzés célja és követelményei

Célja:

- megtanítani és képessé tenni a katonákat szakbeosztásuk teljes értékű ellátására, kialakítani és megszilárdítani együttműködési készségüket az alegység előtt álló feladatok megoldásában;
- felkészíteni a katonákat a híradó és FRISZ eszközök (állomások) telepítésénél és bontásánál egy kezelői feladat irányítás

mellett történő ellátására, megtanítani őket az ehhez szükséges alapvető szabályokra, valamint a tevékenységek során betartandó biztonsági rendszabályokra. Felkészíteni a katonákat az eszközök szabályos üzemeltetésére és forgalmazási szakfeladataik ellátására.

A sorállományú katonák:

Ismerjék meg:

- a tervezett beosztásuk ellátásához szükséges szakmai, elméleti alapokat, gyakorlati tevékenységeket és a beosztásuk ellátásának feladat-rendszerét, normatív követelményeit;
- az élet és baleset elleni védelem rendszabályait;
- a híradó eszközökön folytatott - szakágnak megfelelő - hírváltás szabályait.

Legyenek képesek:

- a beosztásuknak megfelelő híradó eszköz, berendezés, állomás üzembe helyezésére, (telepítésére) hangolására, beszabályozására, üzemeltetésére;
- a komplexumokhoz beosztottak egy kezelői feladat irányítás melletti, szükségszerű ellátására;
- egyszerűbb forgalmazási feladatok ellátására távbeszélő, távíró és géptávíró üzemmódokban;
- a gyakorlati tevékenységek során az élet- és baleset elleni védelem előírásainak, rendszabályainak betartására.

A szerződéses katonák:

Ismerjék meg:

- a beosztásuk ellátásához nélkülözhetetlen szakmai elméleti és gyakorlati feladatrendszert, normatív követelményeket ;
- az élet és baleset elleni védelem rendszabályait;
- a híradó eszközökön folytatott - szakágnak megfelelő - hírváltás szabályait.

Legyenek képesek:

- a beosztásuknak megfelelő híradó eszköz üzembe helyezésére, üzemeltetésére;
- a komplexumokhoz beosztott állomány feladat meghatározására, szakmai irányítására, ellenőrzésére;
- a beosztott állomány szakmai felkészítésének végrehajtására.

Szakkiképzési ágak

A híradócsapatoknál a szakkiképzési ágak a következők:

- Híradó technikai kiképzés;
- Híradó gyakorlati kiképzés;
- Híradó szakharcászati kiképzés.

Híradó technikai kiképzés

A híradó technikai kiképzés célja:

A technikai kiképzés tárgyköreinek oktatása során a katonákkal meg kell ismertetni a rendszeresített eszközeik főbb műszaki - technikai jellemzőit, alkalmazásuk lehetőségeit és körülményeit, az állomások (eszközök, berendezések) által biztosított szolgáltatások, üzemmódok és vezérlési változatok kialakításának szükségességét, módozatait.

A híradó állomások ismertetése, magába foglalja:

- az adott híradó állomás, komplexum (eszköz, berendezés) legfontosabb jellemzőit, műszaki - technikai adatait, belső és külső rendszertechnikai felépítését;
- az áramellátás rendszerét;
- a vezérlési és távvezérlési lehetőségeket;
- a rendszeresített antennák típusait, jellemzőit és azok alkalmazását;
- a különböző rádiókészülékek, eszközök, kisegítő- és végberendezések funkcionális feladatait, egymással való kapcsolatukat;
- a kezelő-, jelző- és csatlakozószervek megnevezését, és azok funkcionális feladatát;
- az üzemeltetés biztonsági - és a környezetvédelem rendszabályait.

Kiképzési követelmények

A kezelőszemélyzet tagjai ismerjék meg a rendszeresített állomások, eszközök rendszertechnikai alkalmazásával összefüggő feladatokat, a fő- és segédberendezések technikai adatait, jellemzőit, az állomások táplálási, kommunikációs és antennarendszerét. Ismerjék meg a hangolás, a távíró és távbeszélő üzemmódok létesítésének szabályait nyílt és titkosított üzemben helyi-, illetve távvezérléssel. Ismerjék a rendszeresített eszközeik kezelői szintű bevizsgálásának, önellenőrzésének szabályait. Az alkalmazás szintjén ismerjék az életvédelmi és balesetelhárítási rendszabályokat.

Az állomás-, és rajparancsnokok teljes terjedelemben ismerjék az állomások, berendezések szakszerű üzembe helyezésének és üzemeltetésének, a lehetséges üzem- és vezérlési módok kialakításának szabályait, az alkalmazási lehetőségeket, módozatait, a bevizsgálás és önellenőrzés, továbbá az egyszerűbb hibák felismerésének és elhárításának módjait, fogásait. Legyenek képesek a katonák kiképzésében oktatóként tevékenykedni.

Az alegységparancsnokok (szakasz, század és ezekkel azonos szintűek) fejlesszék ismereteiket és jártasságukat az alegységeiknél rendszeresített híradó technikai eszközök kiszolgálásában; szervezzék, vezessék, irányítsák és ellenőrizzék a kiképzési foglalkozásokat. Folyamatosan kísérjék figyelemmel és értékeljék a katonák teljesítményét. A tárgykörzáró foglalkozásokig alegységeikkel maradéktalanul érjék el a kiképzési követelményekben meghatározott célkitűzéseket.

Híradó gyakorlati kiképzés

A híradó gyakorlati kiképzés célja:

A híradó technikai kiképzés és a híradó gyakorlati kiképzés közötti megfelelő logikai összhang biztosításával felkészíteni a különböző híradó szakbeosztású katonákat a rendszeresített eszközeik biztonságos és megbízható üzemeltetésére, a kezelői feladatok szakszerű ellátására, az állomások, eszközök és berendezések telepítésének, építésének, üzembe helyezésének és működtetésének, a hírrendszer elemeihez történő csatlakoztatásának rendjére, fogadásaira, gyakorlati végrehajtására a biztonsági előírások betartásával.

A gyakorlati kiképzés tárgyköreinek oktatása során a kezelőkkel meg kell tanítani az állomások, eszközök, berendezések által biztosított szolgáltatások teljes körű kihasználását a lehetséges üzem- és vezérlési módokban, változatokban, továbbá az információk gyors, pontos és megbízható továbbítását, az ehhez szükséges nyílt és titkosított csatornák paramétereknek megfelelő létrehozását, beszabályozását.

A gyakorlati kiképzés folyamatában a katonákat, rajokat, állomásokat fel kell készíteni a kötelmeik szerinti feladatok gyors és összehangolt végrehajtására, a megszerzett ismeretek, jártasságok állandó fejlesztésére.

Magába foglalja:

- a híradó állomás és forgalmi szolgálati ismereteket,
- a hangolvasást (mely a közeljövőben nem kerül oktatásra),
- a gépírás elsajátítását,
- a telepítést és üzemeltetést,
- a forgalmazási feladatok begyakorlását.

Kiképzési követelmények

Híradó állomás és forgalmi szolgálati ismeretekből a kezelők, távbeszélők, géptávírászok, rádió-géptávírászok, rádiótávírászok sajátítsák el a saját beosztásukhoz kapcsolódó forgalmi és szolgálati utasítások szabályait; a kezelők általános és konkrét kötelmeit; a különböző híradó eszközökön az összeköttetések felvételével és fenntartásával kapcsolatos előírásokat, tevékenységeket a berendezések, eszközök által biztosított üzemmódokban. Váljanak képessé a megismert előírások, szabályok gyakorlatban történő alkalmazására, a szolgálati és üzemi csatornákon való hírváltás végrehajtására, a közlemények, küldemények továbbítására és kezelésére. Ismerjék meg a természetes és szándékos zavarok elleni védekezés módozatait, a REH alapjait és összetevőit. Sajátítsák el a szolgálati közlések táblázatának alkalmazását, a különböző kódokat és rövidítéseket, valamint a forgalmazásban megengedett egyszerűsítéseket. Ismerjék meg az adatlapok, vázlatparancsok, eseménynaplók és más, az állomásokon rendszeresített egyéb okmányok kezelésével és vezetésével kapcsolatos teendőket.

A kezelőszemélyzet (raj) tagjai az egyéni felkészítés időszaka végére ismerjék meg a beosztásuknak megfelelő híradó technikai eszközök, komple-

xumok, állomások, stb. alkalmazásának alapelveit; gyakorolják be a kezelői tevékenységeket és fogásokat, amelyek funkcionális kötelmeikhez kapcsolódnak. Legyenek képesek irányítás mellett (kezdeti jártassági szinten) a telepítési, építési, üzembe helyezési, üzemeltetési és bontási folyamatokban a szaktevékenységek végrehajtására.

A rajok, állomások a kötelékkiképzés végére érjék el az összekovácsolás olyan szintjét, hogy képesek legyenek az építési, telepítési, üzembe helyezési, üzemeltetési és bontási feladatok összehangolt végrehajtására egyszerű és bonyolult viszonyok között a meghatározott normatívák szerint. Legyenek felkészülve a híradórendszerben kijelölt helyüknek és szerepüknek megfelelő összeköttetések létesítésére, a rájuk háruló híradás biztosítási feladatok ellátására.

A szakasz és század (zászlóalj) személyi állománya a kötelékkiképzés végére gyakorolja be a vezetési pontok szerinti funkcionális feladatait. Legyenek gyakorlottak a hírközpontok, illetve azok részeinek, csoportjainak, telepítésében és üzemeltetésében, az előírt mennyiségű és minőségű csatornák létesítésében.

Az állomás- és rajparancsnokok teljes mélységben ismerjék meg az állomások, berendezések szakszerű telepítésének, üzembe helyezésének, üzemeltetésének és bontásának, az információk adás-vételének gyakorlati fogásait, végrehajtását, a lehetséges - és a szakáguknak megfelelő - üzemmódokban, vezérlési változatokban. Legyenek képesek az üzemeltetési folyamatok kialakításán túlmenően azok ellenőrzésére, az egyszerűbb hibák felismerésére és elhárítására. Legyenek képesek az üzemeltetés, karbantartás szakszerű irányítására, továbbá a katonák kiképzésében oktatóként tevékenykedni.

Az alegységparancsnokok (szakasz, század és ezekkel azonos szintűek) állandóan fejlesszék ismereteiket és gyakorlati jártasságukat az alegységeiknél rendszeresített híradó technikai eszközök kiszolgálásában; szervezzék, vezessék és irányítsák a híradó gyakorlati kiképzés foglalkozásait. Kísérjék figyelemmel és értékeljék a katonák teljesítményét. A tárgykörzáró foglalkozásokig alegységeikkel maradéktalanul érjék el a kiképzési követelményekben meghatározott célkitűzéseket.

Híradó szakharcászati kiképzés

A híradó szakharcászati kiképzés célja:

A kiképzés folyamatában oktatott valamennyi kiképzési ág ismeretanyagát logikailag integrálva felkészíteni a katonákat és alegységeket a korszerű harc követelményeiből adódó - a vezetés igényeit kielégítő - híradás létesítési és biztosítási feladatok ellátására egyszerű és bonyolult viszonyok között.

Felkészíteni a különböző híradó szakbeosztású katonákat kezelőszemélyzetet a híradó állomások komplexumok, eszközök telepítésében, üzembe helyezésében és üzemeltetésében szerzett ismereteik, jártasságaik alkalmazására.

Begyakoroltatni a raj, állomás, kezelőszemélyzet összehangolt tevékenységét, a különböző szintű vezetési pontok hírközpontjainak és azok elemeinek szakszerű telepítését, az egynemű és a különböző típusú - vezetékes és vezeték nélküli - eszközök együttes üzemét, az információk gyors, pontos és megbízható továbbítását a lehetséges üzemmódokban és vezérlési változatokban.

Magába foglalja:

- a harckészültségi híradó szakfeladatok begyakorlását,
- a híradó szakharcászati gyakorlatoknak és komplex foglalkozásoknak azt a rendjét, amely biztosítja a kezelőszemélyzet, raj (állomás, részleg, stb.), szakasz, század (zászlóalj) összehangolt tevékenységének, a vezetési pontok, illetve az elöljáró és alárendeltek közötti összeköttetések létesítésének és fenntartásának begyakorlását, az alegységek alkalmazásra való felkészítését;
- a gyakorlatok híradásának biztosítását.

Kiképzési követelmények

A kezelőszemélyzet tagjai ismerjék meg saját alegységük (raj, állomás, stb.) rendeltetését, helyét és szerepét a hírrendszerben, alkalmazásuk alapelveit, sajátítsák el a kezelői kötelmeket és az abból adódó feladatokat, gyakorlati fogásokat, az információk gyors, pontos és megbízható továbbítását valamennyi lehetséges üzemmódban és vezérlési változatban.

A rajok, állomások gyakorolják be a harckészültség híradó szakfeladataikat, továbbá a hírrendszerben elfoglalt helyüknek és szerepüknek megfelelő tevékenységeket.

A szakasz és század (zászlóalj) személyi állománya legyen képes:

- a különböző szintű vezetési pontok hírközpontjainak normaidőre történő telepítésére, bontására és áttelepítésére;
- az összekovácsolt tevékenységre;
- az összeköttetések létesítésére és fenntartására vezetékes és vezeték nélküli eszközökkel az elöljáróval és az alárendeltekkel (együttműködőkkel, szomszédokkal) bármilyen üzemmódban és vezérlési változatban;
- a szolgálati összeköttetések létesítésére és folyamatos fenntartására;
- a megszakadt összeköttetések gyors helyreállítására, kerülő irányok létesítésére, illetve átjátszó vagy közvetítő állomásokon keresztül történő hírváltás, információ-továbbítás végrehajtására;
- mozgó (légi) állomásokkal való összeköttetés létesítésére és fenntartására;

- a hírközpont elemek egymáshoz történő csatlakoztatására és azok együttes üzemét biztosító beszabályozások, ellenőrzések szakszerű végrehajtására;
- a tömegpusztító és gyújtófegyverek hatása elleni védelemre, valamint az ilyen fegyverekkel mért csapások következményeinek részleges felszámolására, mentesítésre;
- különleges viszonyok (erdős-hegyes terep, zord időjárási viszonyok, ellenséges zavarás, stb.) között a szaktevékenységek megszakítás nélküli végzésére.

A kiképzés tervezése, okmányai

A kiképzés tervezésének alapját a szakkiképzési programban meghatározott feladatok, az elöljáró parancsnokok (főnökök) intézkedései és utasításai, valamint az adott kiképzési időszakra tervezett kiemelt kiképzési feladatok képezik.

A kiképzés tervezése során figyelembe kell venni a harckészültségi követelmények teljesítését, a katonák időszakosságát, az alegységek személyi állományának összetételét (sor, szerződéses állomány), feltöltöttség szintjét, a kiképzésre rendelkezésre álló időmennyiséget, a parancsnok elgondolását a meghatározott kiképzési célok és követelmények teljesítésére, a katonák és alegységek komplex felkészítésének lehetőségeit, valamint tartalék idő képzésének lehetőségét.

A kiképzés tervezése és a tervokmányok kidolgozása során az alábbi rendező elveket célszerű figyelembe venni:

- Kiképzési tervet a kiképző zászlóaljnál 3 hónapra, a kiképző századnál egy-egy tervet az alapkiképzés, valamint a bázis, illetve szakalapozó kiképzések teljes időtartamára kell készíteni.
- A kötelékben lévő zászlóaljak 3 hónaptól a kötelékkiképzés teljes időszakára (6 hónap), a századok két héttől egy hónapig terjedő időszakra készíthetnek - a parancsnok döntésétől függően - kiképzési terveket.

A zászlóalj kiképzési terve tartalmazza:

- a kiképzési feladatokat,
- a kiképzési ágakat és tárgyköröket (ha szükséges azok foglalkozásait),
- alegységszintű technikai kiszolgálási feladatokat és az azokra fordítandó időt alegységenkénti és napi bontásban,
- az egység terveiből a zászlóaljra (századra) vonatkozó adatokat,
- a zászlóalj (század) által tervezett normagyakorlásokat,
- az alegységek, katonák őr- és ügyeleti szolgálat adásának rendjét,

- a szolgálatok ellátásáért, valamint egyes kiképzési feladatok végrehajtása után biztosított kiképzésmentes időt,
- az alegységek kiképzésére biztosított bázisok, gyakorlóterek, szaktantermek napra - órára történő elosztását,
- a kiképzők, az oktatók és a rajparancsnokok oktató-módszertani továbbképzésének témáit és időpontjait,
- a felhasználható technikai eszközök típusát és számát, valamint a felhasználható kilométer (üzemóra) mennyiségét.

A zászlóalj kiképzési tervét a kiképző Központ, illetve az egységparancsnok legkésőbb a kiképzés megkezdése előtt 2 héttel hagyja jóvá.

A század részletes kiképzési terve tartalmazza:

- naponként a kiképzési feladatokat tárgykörökre és foglalkozásokra való bontásban, és az azokra fordítandó kiképzési időt,
- a foglalkozások helyét, vezetőjét, a technikai eszközök típusát és számát, valamint a felhasználható kilométer és üzemóra mennyiséget,
- a kiképzés anyagi és egyéb szükségletét,
- vegyvédelmi normagyakorlásokat,
- a különböző gyakorlások idejét, rendjét, tartalmát,
- a kulturális és sportrendezvények idejét, rövid tartalmát,
- századgyűlés, fegyelmi értekezlet időpontját,
- a szolgálatok ellátásáért, a kiképzési feladatokért biztosított pihenő időt.

A foglalkozási jegy (foglalkozási terv, vázlat)

A kiképzési tervet a zászlóaljparancsnok a kiképzés megkezdése előtt egy héttel hagyja jóvá.

Az alegységszintű gyakorlatok terveit legalább egy héttel, a foglalkozási jegyeket azok megkezdése előtt legalább 2 nappal a közvetlen elöljáró hagyja jóvá.

A szakalapozó kiképzés

1. Rádió -, rádiórelé és troposzféra híradáshoz beosztottak

- A kis- és közepes teljesítményű állomások, komplexumok távírászai és kezelői
- A nagyteljesítményű állomások és vezérlőközpontok távírászai, géptávírászai és kezelői
- A távírászok, rádió-géptávírászok
- A rádiórelé kezelők
- A troposzféra állomások kezelői

2. Központ- és vezetékes híradáshoz beosztottak

- A távbeszélő központok kezelői
- A géptávíró központok kezelői
- A vivő-, vivőrendező központok kezelői

- A vezetékes- és több erű kábelt építő rajok beosztottai
- Az expedíció-, futár és tábori posta állomások, a híradó irányító központok kezelői

Fő kiképzési ágak a szárazföldi híradó csapatok részére:

- híradó technikai kiképzés,
- híradó gyakorlati kiképzés,
- lőkiképzés,
- testnevelés,
- híradó szakharcászati képzés (amikor gyakorlat nem kerül levezetésre).

Híradó szakharcászati képzés és komplex gyakorlások

A kiképzés célja:

A kiképzés folyamatában oktatott valamennyi kiképzési ág ismeretanyagát logikailag integrálva felkészíteni a katonákat és alegységeket a korszerű harc követelményeiből adódó - a vezetés igényeit kielégítő - híradás létesítési és biztosítási feladatok ellátására egyszerű és bonyolult viszonyok között.

Felkészíteni a különböző híradó szakbeosztású katonákat, kezelőszemélyzetet a híradó állomások, komplexumok, eszközök telepítésében, üzembe helyezésében és üzemeltetésében szerzett ismereteik, jártasságaik alkalmazására.

Begyakoroltatni a raj, állomás, kezelőszemélyzet összehangolt tevékenységét, a különböző szintű vezetési pontok hírközpontjainak és azok elemeinek telepítését.

Magába foglalja:

- a **harckészültségi híradó szakfeladatok** begyakorlását nappal és éjszaka a harckészültségi tervekben meghatározottak szerint;
- a **híradó szakharcászati gyakorlatoknak és komplex foglalkozásoknak** azt a rendjét, amely biztosítja a kezelőszemélyzet, raj (állomás, részleg, stb.), szakasz, század (zászlóalj) összehangolt tevékenységének, a vezetési pontok, illetve az elöljáró és alárendeltek közötti összeköttetések létesítésének és fenntartásának begyakorlását, az alegységeknek **alkalmazásra való felkészítését;**
- a **gyakorlatok híradásának biztosítását** a különböző szintű parancsnokságok igénye és a híradófőnök terve szerint.

Kiképzési követelmények

Valamennyi szakág alegységei, katonái részére

A kezelőszemélyzet tagjai ismerjék meg saját alegységük (raj, állomás, stb.) rendeltetését, helyét, szerepét a hírrendszerben, alkalmazásuk alapelveit, sajátítsák el a kezelői kötelmeket, és az abból adódó feladatokat, gyakorlati fogásokat.

Legyenek képesek a korszerű harc jellegéből adódó fokozott fizikai, pszichikai megterhelés elviselésére, az összeköttetések létesítésére és folyamatos fenntartására bonyolult rádióelektronikai viszonyok között is.

A rajok, állomások gyakorolják be a harckészültség híradó szakfeladatait, továbbá a hírrendszerben elfoglalt helyüknek és szerepüknek megfelelő tevékenységeket.

A szakasz és század (zászlóalj) személyi állománya legyen képes:

- a különböző szintű vezetési pontok hírközpontjainak normaidőre történő telepítésére, bontására és áttelepítésére,
- az összeköttetések létesítésére és fenntartására vezetékes és vezeték nélküli eszközökkel, az elöljáróval és az alárendeltekkel, együttműködőkkel,
- a szolgálati összeköttetések létesítésére és folyamatos fenntartására,
- a megszakadt összeköttetések gyors helyreállítására, kerülő irányok létesítésére, illetve átjátszó vagy közvetítő állomásokon keresztül történő hírváltás, információ-továbbítás végrehajtására,
- mozgó (légi) állomásokkal való összeköttetés létesítésére és fenntartására,
- a hírközpont elemek egymáshoz történő csatlakoztatására és azok együttes üzemét biztosító beszabályozások, ellenőrzések szakszerű végrehajtására,
- a különböző típusú és eredetű zavarok melletti hírváltásra,
- a tömegpusztító és gyújtófegyverek hatása elleni védelemre, valamint az ilyen fegyverekkel mért csapások következményeinek részleges felszámolására, mentesítésére,
- az állomások, hírközpont elemek, illetve a hírközpontok őrzésvédelmére,
- különleges viszonyok (erdős-hegyes terep, zord időjárási viszonyok, ellenséges zavarás, stb.) között a szaktevékenységek megszakítás nélküli végzésére.

Általános módszertani követelmények

A különböző szakbeosztású híradó katonák, a kezelőszemélyzetek, részlegek és az alegységek híradó szakharcászati kiképzése a komplex foglalkozásokon, a harckészültségi szakharcászati, a híradó szakharcászati és a különböző szintű harcászati gyakorlatokon történik.

A híradó-alegységek szakharcászati felkészítését, összekovácsolását kezelőszemélyzet kötelékben kell végrehajtani.

A híradó szakharcászati kiképzés egyes tárgyköreinek végrehajtását meg kell hogy előzze más kiképzési ágak azon tárgyköreinek - elsősorban a híradó technikai és a híradó gyakorlati kiképzés - ‚foglalkozásainak eredmé-

nyes végrehajtása, amelyek feltételei a híradó szakharcászati kiképzéssel szemben támasztott kiképzési követelmények elérésének, a híradó-alegységek komplex gyakoroltatásának.

A foglalkozásokat a híradó technikai eszközök igénybevételével kell megtartani. A gyakorlások első fázisaiban először az egyes eszközök, berendezések önálló telepítését és üzembe helyezését kell gyakoroltatni, majd fokozatosan bővítve a tevékenységeket az egyszerű, illetve az eltérő típusú (vezetékes és vezeték nélküli) eszközök, hírközpont elemek együttes üzemére célszerű helyezni a hangsúlyt.

Fokozott gondossággal kell a kezelőszemélyzetben tudatosítani, hogy a híradó eszközökkel, berendezésekkel létesítendő összeköttetések megvalósításának alapvető feltétele a hangolások, beszabályozások szakszerű végrehajtása, az üzemi folyamatok állandó ellenőrzése, figyelemmel kisérése.

A komplex foglalkozásokat úgy kell megtervezni és levezetni, hogy a kezelői kötelmek gyakorlása mellett biztosított legyen a híradó végrehajtó közegek feladatainak gyakoroltatása is.

A feladatokat nappal és éjszaka is végre kell hajtani.

A híradó szakharcászati kiképzés és komplex foglalkozásaihoz levezetési tervet kell készíteni, amely tartalmazza naponként és óránkénti bontásban a feladatokat és azokra fordítható időt, a végrehajtás helyét, az anyagi biztosítást, az igénybevett híradó technikai eszközöket, a gyakorlók létszámát, a szolgálati beosztást, az őrzés-védelem rendjét.

Abban a kiképzési időszakban, amikor az összfegyvernemi vagy fegyvernemi csapat, amelyiknek kötelékébe az adott híradó alegység tartozik, nem hajt végre harcászati gyakorlatot, akkor a **„Gyakorlatok híradásának biztosítása”** tárgykörre tervezett időt komplex gyakorlásokra kell fordítani.

Tárgykörök és foglalkozások tartalma

1. Tárgykör: Harckészültségi híradó szakharcászati gyakorlat

Kiképzési cél:

- A kezelőkkel megismertetni és megtanítani a harckészültség különböző időszakaiban elvégzendő feladataikat és azok végrehajtásának módját.
- A híradó-alegységek szakfeladatai együttes végrehajtásának begyakorlása, az elöljáró és az alárendeltek felé az összeköttetések biztosítása.

A HKSZ-i feladatok begyakorlása nappal és éjszaka.

- Ténykedés a harckészültségi feladat elrendelésekor.
- A besorolás és menet végrehajtása.
- A kijelölt települési hely elfoglalása, az állomás, komplexum telepítése.

- A berendezések üzembe helyezése, hangolások, beszabályozások végrehajtása. az összeköttetés felvétele és hírváltás a HKSZ terv szerint.
- A vezérlő és távvezérlő vonalak kiépítése.
- A veszélyjelzések vételekor végrehajtandó tevékenységek, valamint az őrzés-védelmi feladatok gyakorlása.
- Műszaki, álcázási munkák, részleges mentesítés végrehajtása a technikán.
- Kezelői, állomásparancsnoki, illetve híradó végrehajtó közegek kötelmei végrehajtásának gyakorlása.

2. Tárgykör: Komplex gyakorlások

A kiképzés célja:

- Az alegységekkel begyakoroltatni a híradó technikai eszközök együttes, komplex, hírrendszerben történő üzemeltetését.
- Felkészíteni az állományt a vezetési pontok hírközpontjainak normaidőre történő telepítésére, áttelepítésére és a bontás végrehajtására nappal és éjszaka, egyszerű és bonyolult viszonyok között.

Szakasz komplex gyakorlás.

- A hírközpont elemek telepítése, vezetéképítés.
- A vezérlő és távvezérlő vonalak, a hírközpont elemek közötti (belső) vezetékes összeköttetés kiépítése, létesítése.
- Az állomások, komplexumok, eszközök, berendezések üzem előtti bevizsgálása, üzembe helyezése.
- Az egymáshoz kapcsolódó hírközpont elemek csatlakoztatása.
- Hangolások, be- és összeszabályozások végrehajtása, szintek beállítása.
- Szolgálati összeköttetések létesítése a szolgálati csatornákon.
- Összeköttetések felvételének gyakorlása a lehetséges üzemmódokban és vezérlési változatokban.
- Közlemények adás-vételének, a hírváltási feladatok végrehajtásának gyakorlása.
- Üzemmódokkal, antennákkal, teljesítménnyel, csatornákkal stb. való manőverek gyakorlása.
- A hírközpont elemek bontása, áttelepülés végrehajtása.
- A híradó végrehajtó közegek kötelmeinek gyakorlása.
- Karbantartás.

Század (zászlóalj) komplex gyakorlás.

- A hírközpont elemek, csoportok (központok), a vezetési pont hírközpontjának (hírközpontjainak) telepítése, vezetéképítés.
- A vezérlő és távvezérlő vonalak, a hírközpont elemek, csoportok, központok stb. közötti összeköttetések kiépítése, létesítése.

- ⌦ Az állomások, komplexumok, eszközök, berendezések üzem előtti bevizsgálása, üzembe helyezése.
- ⌦ Csatlakoztatások, be- és összeszabályozások végrehajtása, szintek beállítása. Szolgálati összeköttetések létesítése a szolgálati csatornákon.
- ⌦ Összeköttetések felvétele különböző üzemmódokban.
- ⌦ Közlemények adás-vétele, hírváltási és forgalmazási feladatok végrehajtásának gyakorlása a különböző helyeken telepített végberendezésekről, központokból. Az üzemmódokkal, frekvenciákkal, antennákkal, vezérlési módokkal, teljesítménnyel és csatornákkal történő manőverezés gyakorlása.
- ⌦ A vezetési pont (pontok) hírközpontjainak bontása, áttelepítése.
- ⌦ A híradó végrehajtó közegek kötelmeinek gyakorlása.
- ⌦ Karbantartás.

Ellenőrző komplex gyakorlás

- ⌦ Az összfegyvernemi, fegyvernemi és szakcsapatok kötelékébe tartozó szakaszok ellenőrző komplex gyakorlását a híradó századparancsnokok, a századokét az érintett híradófőnökök, a híradó zászlóaljak kötelékében lévő szakaszokét a századparancsnokok, önálló szakaszokét és a századokét a zászlóaljparancsnokok vezessék.
- ⌦ A kötelékben lévő zászlóaljak komplex gyakorlását az egységparancsnokok, illetve a híradófőnökök tervezzék és vezessék le.

3. Tárgykör: Gyakorlatok híradásának biztosítása

A kiképzés célja:

Az általános katonai, a híradó technikai és a híradó gyakorlati, továbbá a híradó szakharcászati kiképzés oktatása során elsajátított ismeretekre, a gyakorlati jártasságokra alapozva a különböző szakbeosztású híradó végrehajtó közegek, illetve alegységek váljanak képessé a különböző szintű és fokozatú harcászati gyakorlatok híradás biztosítási feladatainak ellátására a vezetés igényeinek megfelelően.

Szervezetszerű kötelékben, illetve eltérő csoportosításban legyenek képesek a vezetési pontok hírközpontjainak szakszerű és gyors telepítésére, áttelepítésére, valamint az előírt összeköttetések létesítésére, folyamatos fenntartására, egyszerű és bonyolult viszonyok között.

Tartalma:

- ⌦ A híradó technikai eszközök és a személyi állomány felkészítése a gyakorlat jellegéből adódó követelményeknek és igényeknek megfelelően.
- ⌦ Besorolás, menet (vasúti szállítás) végrehajtása a kijelölt körletbe.

- Menet közbeni összeköttetések biztosítása.
- A kijelölt (előzetesen szemrevételezett) települési helyek elfoglalása.
- A vezetési pontok hírközpontjainak telepítése, a meghatározott összeköttetések létesítése és fenntartása az elöljáróval és alárendeltekkel, együttműködőkkel.
- A hírközpontok bontása, áttelepítése.
- Menet végrehajtása a béke elhelyezési körletbe.
- Karbantartás.

Összefoglalás

Összefoglalva az eddig elhangzottakat, a jövőben nagy hangsúlyt kell fektetni a szervezeti és technikai fejlesztés mellett, a sorozott állomány (megszüntetéséig), a szerződéses és hívatásos állomány kiképzésére.

Ki kell dolgozni a jövő kiképzési rendszerét az átmeneti, valamint a „digitális hírrendszer” időszakára.

Ehhez alapvetően néhány kérdésre kell választ adni, melyeket gondolat ébresztőként és zárásként tennék fel.

Milyen feladatra, milyen technikai eszközre, kit, mikor, milyen időtartamban, hogyan, hol, és milyen körülmények között képezzünk, ahhoz, hogy a stratégiai felülvizsgálat és átszervezés céljait, a korábbinál kisebb létszámú, korszerű technikai eszközökkel felszerelt, felkészített katonákból álló ütőképes hadsereg hozhassunk létre.

Pascal ROUCH

LES SYSTEMES D'INFORMATION ET DE COMMUNICATION (SIC)

et les transmissions de l'armée de terre

Je suis le LCL ROUCH, officier des transmissions de l'armée de terre. J'ai le plaisir de vous présenter maintenant les SIC[53] et l'arme des transmissions .

La généralisation de l'emploi de l'électronique et de l'informatique dans tous les systèmes d'armes comme dans le cycle décisionnel est une évolution majeure qui est reconnue comme un multiplicateur de force.

Le monde militaire vit comme le monde civil qui l'entoure la révolution de l'information. Les besoins militaires sont identiques aux besoins civils avec des conditions d'emploi différentes.

Le premier enjeu est le passage du monde simple des télécommunications (domination de la téléphonie et de la télégraphie) au monde complexe de l'information avec l'accélération très forte de la vitesse et du volume de transmissions des informations.

Le deuxième est l'évolution du cadre d'engagement des armées qui se traduit par :

des engagements presque systématiquement dans un cadre multinational ;

engagements systématiquement interarmées.

Il s'agit pour l'arme des transmissions de :

- traiter et transmettre l'information amie ;
- intercepter et, si besoin est, neutraliser l'information ennemie.

A cet effet, l'arme des transmissions met en œuvre un système unique, cohérent, global et sécurisé, qui s'articule principalement en trois composantes complémentaires:

- la composante stratégique ;
- la composante tactique ;

[53] L'appellation SIC est désormais la seule qui soit officiellement reconnue dans nos armées et pour clarifier au mieux les esprits dans ce domaine sensible, un décret paru au journal officiel le 30 décembre 1998 a donné au général CEMA la responsabilité d 'assurer la coordination des systèmes d 'information opérationnels et de communication. Au niveau du ministre, un directoire des SIC est chargé de définir la politique générale et de veiller à la cohérence d 'ensemble des SIC.

Nos alliés parlent communément de CIS pour Communications and Information System.

- la guerre électronique.

LA COMPOSANTE STRATEGIQUE

Missions de la composante stratégique

Assurer la permanence du commandement de l'armée de Terre malgré la neutralisation des autres circuits civils ou militaires.

Véritable système nerveux de l'armée de terre et vitale pour son fonctionnement, la chaîne des télécommunications et de l'informatique est implantée sur environ 250 sites en métropole et outre-mer. Elle assure l'interconnexion aux différents réseaux nationaux militaires et civils, et aux divers réseaux alliés des forces projetées dans un cadre national ou multinational. De plus, elle fournit un service fiable, sécurisé et de qualité dans le domaine des télécommunications et de l'informatique à tous les organismes de l'armée de terre ainsi qu'à certains organismes de la Défense ou d'autres ministères. Et enfin, elle participe à la conception, elle réalise ou participe à la réalisation, elle met en oeuvre et maintient les systèmes d'informatique et de communication qui lui sont confiés

La permanence du commandement impose des réseaux :

- denses (desserte de sites importants au plan opérationnel),
- diversifiés (autonomie opérationnelle et couverture globale),
- protégés (sécurité des communications et durcissement à l'IEM).

Réseau métropolitain interarmées et unifié des télécommunications d'infrastructure , le réseau de transit SOCRATE doit assurer la satisfaction des besoins opérationnels des armées et de la gendarmerie en temps de paix , de crise ou de guerre . Il consiste à substituer une action interarmées à des actions jusqu'alors menées séparément dans chaque armée .

C'est un réseau numérique destiné à véhiculer des informations de toute nature (voix , données , texte, image, vidéoconférence) . Il assure un haut niveau de protection .

LA COMPOSANTE TACTIQUE

Le système de transmissions, nécessaire à l'entraînement et l'engagement des grandes unités terrestres, est constitué pour l'essentiel par le réseau intégré des transmissions automatiques mobile RITA (réseau fédérateur).

Ce système associé à des supports satellitaires, radio et (ou) liens TELECOM civiles loués, déploie sur le terrain un filet (maillage) qui évolue au rythme de la manœuvre interarmes.

La composante tactique de l'arme est organisée en régiments dans une brigade d'appui spécialisé ainsi qu'une compagnie par brigade interarmes.

La Brigade d'Appui spécialisée Transmissions est subordonnée au Commandement des forces de l'armée de terre (CFAT), elle dispose de 5 régiments.

Sur le maillage constitué de centre nodaux viennent se raccorder les centres brigades.

Les moyens satellitaires

La projection d'une force se caractérise par l'importance de certains facteurs dont:

- distances et délais ;
- importance des débits requis ;
- capacité d'évolution d'une force et du réseau qui lui est associé ;
- notion de zones différenciées.

Le système intégré de communications pour intervention légère SICILE est parfaitement adapté pour une mission de type humanitaire avec projection de moyens légers.

LA GUERRE ELECTRONIQUE

La conduite et le succès des opérations dépend de la maîtrise de l'espace électromagnétique, pour connaître les intentions adverses, pour contraindre l'adversaire à des retards critiques dans la transmission des ordres, pour le leurrer sur nos propres intentions et pour permettre un bon déroulement de nos propres opérations.

Dans un conflit moderne. La guerre électronique, dans le cadre de la maîtrise de cette quatrième dimension, assure deux grandes fonctions:

- le ROEM (renseignement d'origine électromagnétique)
- l'intervention de la guerre électronique.

Gyurics Attila

ANTENNA HUNGÁRIA RT., TÁVKÖZLÉSI ÁGAZAT


Stratégiaváltás az AH-nál
Tradicionális műsorszóró vállalatból
komplex távközlési vállalat
A fejlődés irányai:
DIGITÁLIS
FÖLDFELSZÍNI
MŰSORSZÓRÁS
MULTIMÉDIA
TELEKOMMUNIKÁCIÓ
www.ahrt.hu
antenna hungária
Teret adunk gondolatainak


A Távközlési Ágazat felépítése
Távközlési tevékenység 1998 óta.
Távközlési üzletág
Távközlési termékmenedzsment
Távközlés fejlesztés
Távközlés értékesítés
Távközlés üzemeltetés
Távközlés telepítés
www.ahrt.hu
antenna hungária
Teret adunk gondolatainak

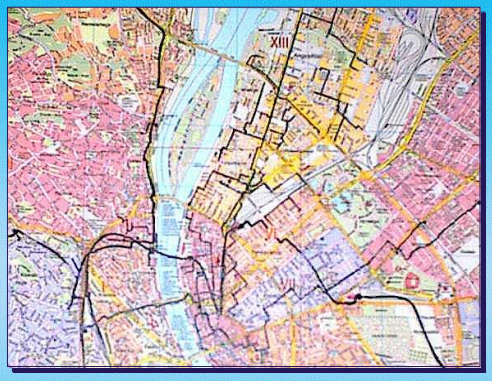
Az Antenna Hungária cégcsoport távközlési érdekeltségei

- Eurotel Rt.
- HungaroDigiTel Kft.
- AnteCom Rt.
- TeleDataCast Kft.
- Antetra Kft.

www.ahrt.hu

antenna hungária
Teret adunk gondolatainak

City Network



•Az optimális gerinchálózati topológia miatt minimális építések szükségesek

•Az Antenna Hungária Rt. és az Eurotel Rt. budapesti optikai hálózata

•Budapest legfontosabb üzleti negyedeit (Belváros, XIII. kerület) fedi le

•Eléri a nagyobb bankokat és pénzintézeteket, vállalati központokat, kormányzati épületeket, intézményeket.

www.ahrt.hu

antenna hungária
Teret adunk gondolatainak

Országos Transzport Hálózat (OTH)

•mikrohullámú gerinchálózat

•51 kicsatlakozási ponttal

•országos kiterjedés

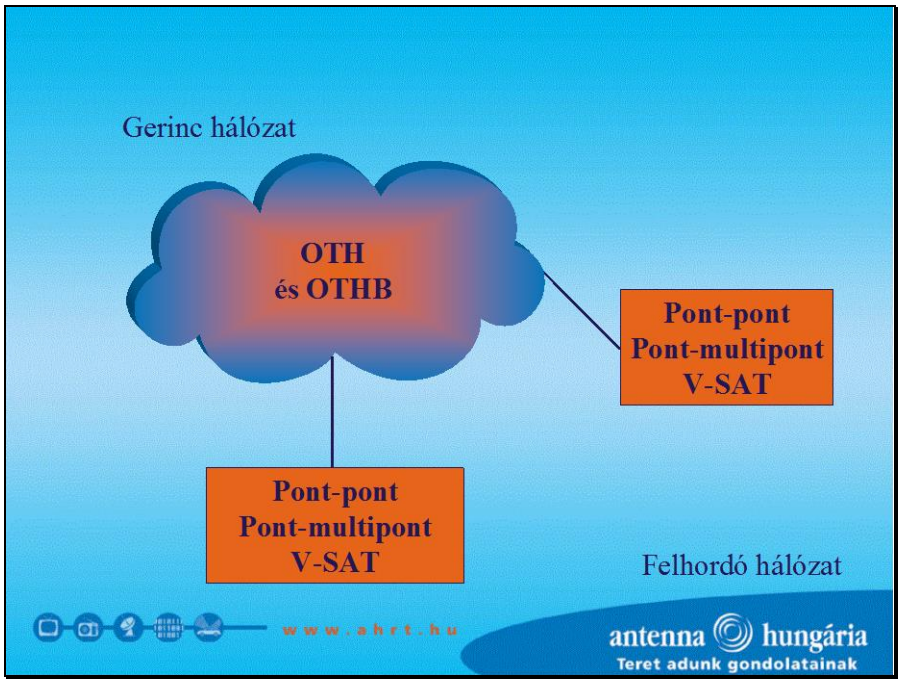
•nagy sebesség

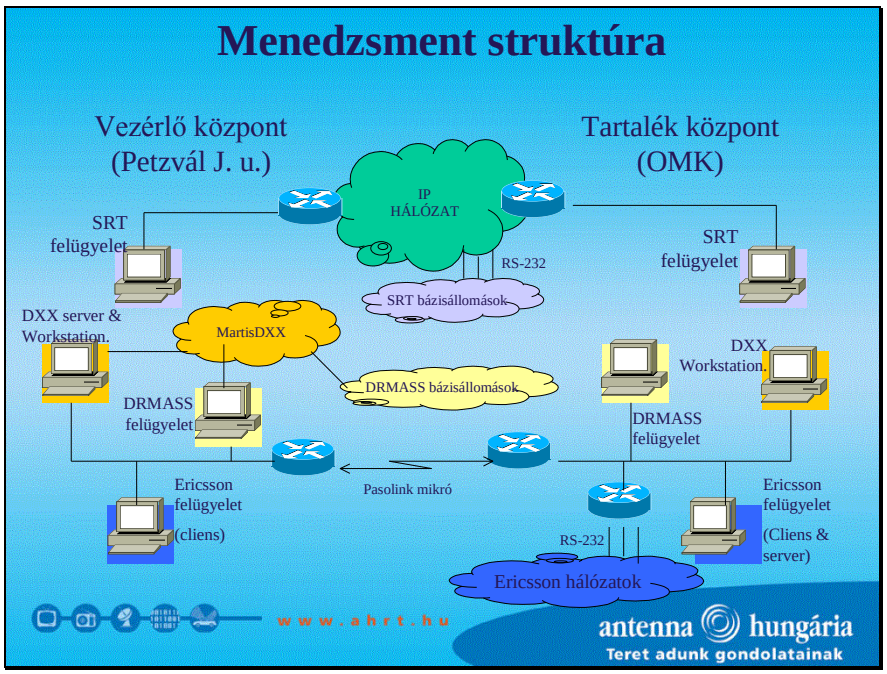
•forgalmi konfigurálhatóság

•SDH rendszerű, topológiája 9 gyűrűből áll

Kapacitások

- 9 db STM-1 gyűrű
- 2 db átkötés
- 2 Mbps, 34 Mbps tributary ki/be csatlakozás


Gerinc hálózat
OTH
és OTHB
Pont-pont
Pont-multipont
V-SAT
Pont-pont
Pont-multipont
V-SAT
Felhordó hálózat
www.ahrt.hu
antenna hungária
Teret adunk gondolatainak


Menedzsment struktúra
Vezérlő központ
(Petzvál J. u.)
Tartalék központ
(OMK)
IP
HÁLÓZAT
SRT
felügyelet
RS-232
SRT bázisállomások
SRT
felügyelet
DXX server &
Workstation
MartisDXX
DXX
Workstation
DRMASS bázisállomások
DRMASS
felügyelet
DRMASS
felügyelet
Ericsson
felügyelet
(cliens)
Pasolink mikró
Ericsson
felügyelet
(Cliens &
server)
RS-232
Ericsson hálózatok
www.ahrt.hu
antenna hungária
Teret adunk gondolatainak


Hálózati réteg struktúra
Szolgáltatások
Bérelt vonalak
Internet
VoIP
VPN
FR
VoFR
Euteltracs
Pandant
Hálózati- és szolgáltatás menedzsment
Carrier szolgál-tatás
IP
Frame Relay
Egyéb
SDH
Optikai kábel
Mikrohullám
www.ahrt.hu
antenna hungária
Teret adunk gondolatainak


Szolgáltatás portfoliónk
• Adatátviteli szolgáltatások
Bérelt vonal
• IP alapú szolgáltatások
Internet gerinc
VoIP
VPN
• Pandant - GPS alapú járműkövetéses vagyonvédelmi rendszer
• Euteltracs - Műholdas kommunikációs és jármű-helymeghatározó rendszer
www.ahrt.hu
antenna hungária
Teret adunk gondolatainak

Távközlési üzembehelyezési szolgáltatás

- Az Antenna Hungária Rt. vállalja optikai és pont-pont vagy pont-multipont mikrohullámú berendezések telepítési folyamatának teljes vagy részleges lebonyolítását, a megvalósíthatósági terv készítésétől, az eszközrendelésen, az engedélyezési eljárás lefolytatásán, a frekvenciakijelölés kérelmezésén, a kiviteli terv készítésén, a kiépítésen és frekvenciaellenőrzésen át az üzembe helyezési eljárás lefolytatásáig.
- Optikai és mikrohullámú eszközök telepítése mellett szolgáltatásunkat televízió és rádió stúdiók modulációs vonalainak kiépítésére, áthelyezésére és korszerűsítésére is ajánljuk.

Hálózatmenedzsment

- Társaságunk vállalja működő mikrohullámú összeköttetések és hálózatok karbantartását, üzemeltetését, egyben állandó felügyeletét is.
- Önálló hálózatmenedzsment központtal nem rendelkező ügyfeleink részére az Antenna Hungária Rt. nagy kapacitású hálózatmenedzsment rendszerébe történő bekapcsolást ajánljuk, mellyel mikrohullámú hálózatuk folyamatos rendelkezésre állását biztosítjuk.


Ügyfeleink
Távközlési szolgáltatók
Vodafone
MATÁV
Pannon GSM
Vivendi
GTS
Pantel
Pénzintézetek
Takarékbank
Konzumbank
Postabank
GIRO
OTP
Budapest Bank
Euronet
Kormányzati szektor
MH Országos Mikrohullámú Rendszer
LRI
BM HÖR
Vállalati szektor
Dunapack, KITE, ESSO,
BAT, METRO, ARAL,
TOTAL, OMV
www.ahrt.hu
antenna hungária
Teret adunk gondolatainak

Bemutatkoznak a nemzetközi szakmai tudományos konferencia szponzorai

CeoTronics® AG Rödermark Németország
Hans Helmut PEER

Egy hatékony hadseregnek tökéletes kommunikációs eszközökre van szüksége.

Jó tíz évvel a berlini fal lebontása után, amikor a volt Varsói Szerződés országai közül egyre több lesz a NATO tagja, egyúttal a fegyveres erők reformja is a küszöbön áll.

Az „élesben„ harcoló hadseregeknek, ahhoz hogy az új, komplex követelmények között is megállják a helyüket, nagyhatékonyságú egységekre van szükségük.

Ezek a „kicsiny de ütőképes" egységek nem minősíthetők csupán a kiképzés minőségével, a gyakorlatok mennyiségével, vagy a rendelkezésre álló tűzfegyverek színvonalával. Professzionális híradó eszközök nélkül a még harcoló aktív csoportnak megmarad ugyan a támaszpontja, de a biztonsági, békefenntartó vagy harci műveletek bevetéseiben végveszély fenyegeti.

Csak a tökéletes kommunikáció szavatolja a legnagyobb biztonságot.

A rosszminőségű kommunikációs eszköz gyakran félreértésekhez, információtorzuláshoz vezet, a többszöri visszakérdezés időveszteség és bizonytalanság forrása, rossz esetben az egység felszámolásához vezethet.

Ezek a veszélyek állnak fenn bármely összeköttetési szinten, akár a rohamsisak beszélőkészletéről. a helikopter pilóta kommunikációs rendszeréről, vagy egy beavatkozó alegység mesterlövészének összeköttetéséről legyen szó.

A jövőben a nemzetvédelem minden területén a NATO és EU bevetésekben, akciókban résztvevő országoknak elsőrendű kötelességük a kato-

nák személyes biztonságára gondolni a kommunikációs eszközök beszerzésénél is.

Az olcsó eszköz ritkán előnyös.

Egy kommunikációs eszköz beszerzésénél az ár csak alárendelt szerepet játszik. Sokkal fontosabb szempont hogy az olcsó eszközök beszerzésével elért megtakarításokat vajon nem emésztik-e fel a negatív következmények költségei és más kihatásai. A javítási, és más pótlólagos beruházások gyakran többe kerülnek, nem beszélve a biztonságról. az időveszteségről.

A **CeoTronics**® és a katonák „egy hajóban „vannak.

A fegyveres erőknél nagyon fontos a legjobb kommunikációs eszközökkel való felszerelés. Éppen ezért vette célba a **CeoTronics**® a fegyveres erők különleges egységeinek és a bűnüldöző hatóságok termékmenedzsereit. Ők ugyanis a legfontosabb tanácsadói, és szakértői a döntéshozó parancsnokoknak az egyedi kivitelű hang, kép és adatátviteli eszközök beszerzésénél.

Ugyancsak ők a közvetlen partnereink az új fejlesztések ösztönzésénél és a termékszinvonal, a minőség javítása érdekében.

Csak a többszintű követelmények figyelembevételével hozott beruházási döntésekkel sikerülhet a fegyveres erők felszereltségének szintjét a kívánt színvonalra emelni.

Számunkra, a **CeoTronics**® cég számára nagyon fontosak azok a döntések, amelyek hosszabb távú katonai szempontokat vesznek célba, és ezek biztonságát szolgálják.

UNITRONEX Corporation

Company overview

Unitronex Corporation is a leading provider of international trade services that support the introduction of Central European and Polish products, technologies, and services to the United States and the marketing of American products, technologies, and services to Central Europe and Asia.

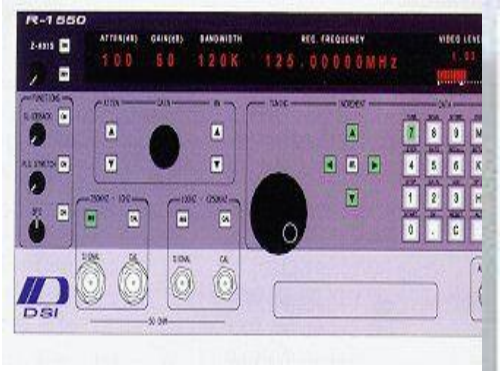
Unitronex Corporation is an international trading company incorporated in the U.S.A. in 1974. For over 27 years Unitronex Corporation has been a leading provider of international trade services that support the introduction and sale of products, technologies and services to Central Europe as well as the export of European products to the U.S.A. With our knowledge and extensive experience we have been able to provide our customers with a long list of successful contracts and orders. Our list of industrial customers includes manufacturing companies, scientific research institutions, industrial distributors. We supply them with industrial machines and equipment, control and measuring instruments, spare parts, electronic and electric subassemblies, as well as technological lines of well known North American manufacturers.

Since Poland, Hungary and the Czech Republic joined NATO, Unitronex Corporation has emerged as a leading supplier of defense related products. Together with the U.S. companies, which Unitronex represents, Unitronex is able to provide a full range of defense and electronics warfare products, including reconnaissance, signal intelligence, communication and information security and protection. We offer products such as Tempest and EMC testing antennas from Antenna Research Associates, shielded and NENP enclosure systems featuring products from Braden Shielding Systems, Corcom Inc. and Laird Technologies. Tempest and EMC testing equipment, high sensitivity up to 40 GHz receivers from Dynamic Sciences, Tempest computers and peripherals from Hetra Secure Solutions, rugged computers, laptops and disk drives from Miltope Corporation, MSTAR ultra quiet battlefield radars from Systems & Electronics Inc.We feature Bren-Tronics batteries and chargers for all military applications and all military radios. Among our products offering we also have RF power amplifiers, microwave components and preamplifiers manufactured by IFI as well as the OSCOR and ORION linear and junction detectors for counter surveillance applications manufactured by Research Electronics Inc. We also supply other products and services from leading manufacturers specified on the NATO Recommended Products List.

Pictures

ANTENNA RESEARCH - RF antennas and antenna systems, GTEM, EMC

BRADEN SHIELDING SYS. - shielded enclosures, components, RF, MRI

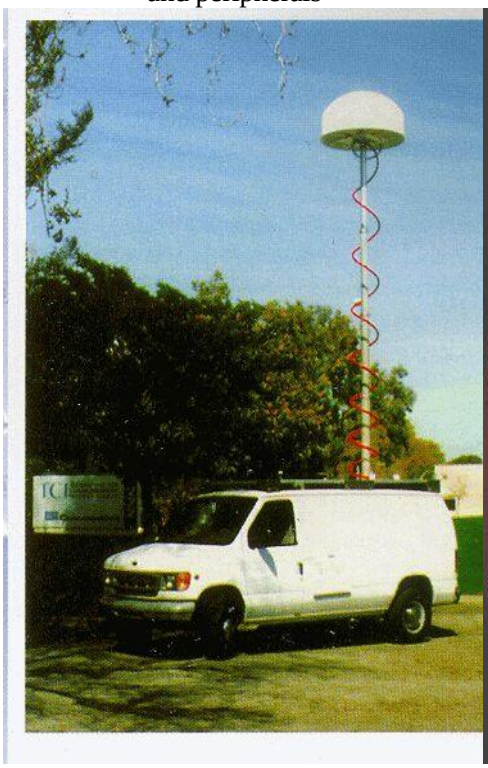


DYNAMIC SCIENCES - TEMPEST test systems, radio system engineering, EMC/EMI

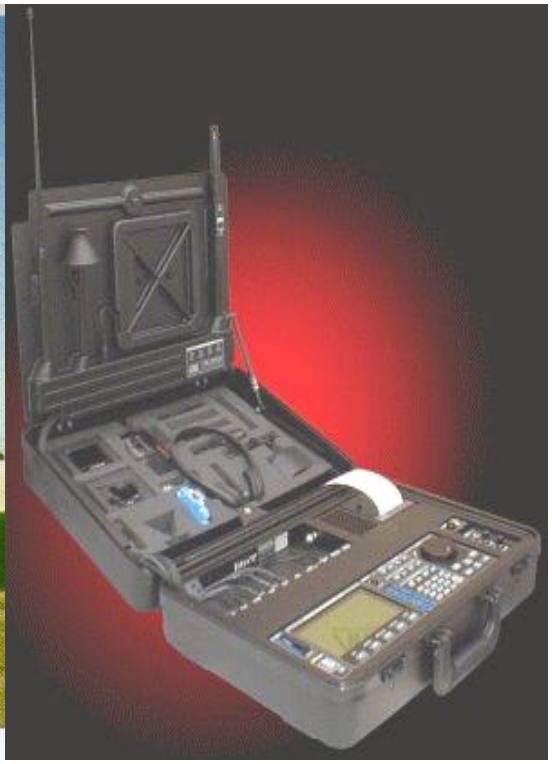
FERRISHIELD - interference control components

HETRA SECURE SOLUTIONS - TEMPEST, EMI and rugged computers and peripherals

MILTOPE CORPORATION - rugged mass storage units, disk drive cartridges



TCI/BR - DF, communications and surveillance systems

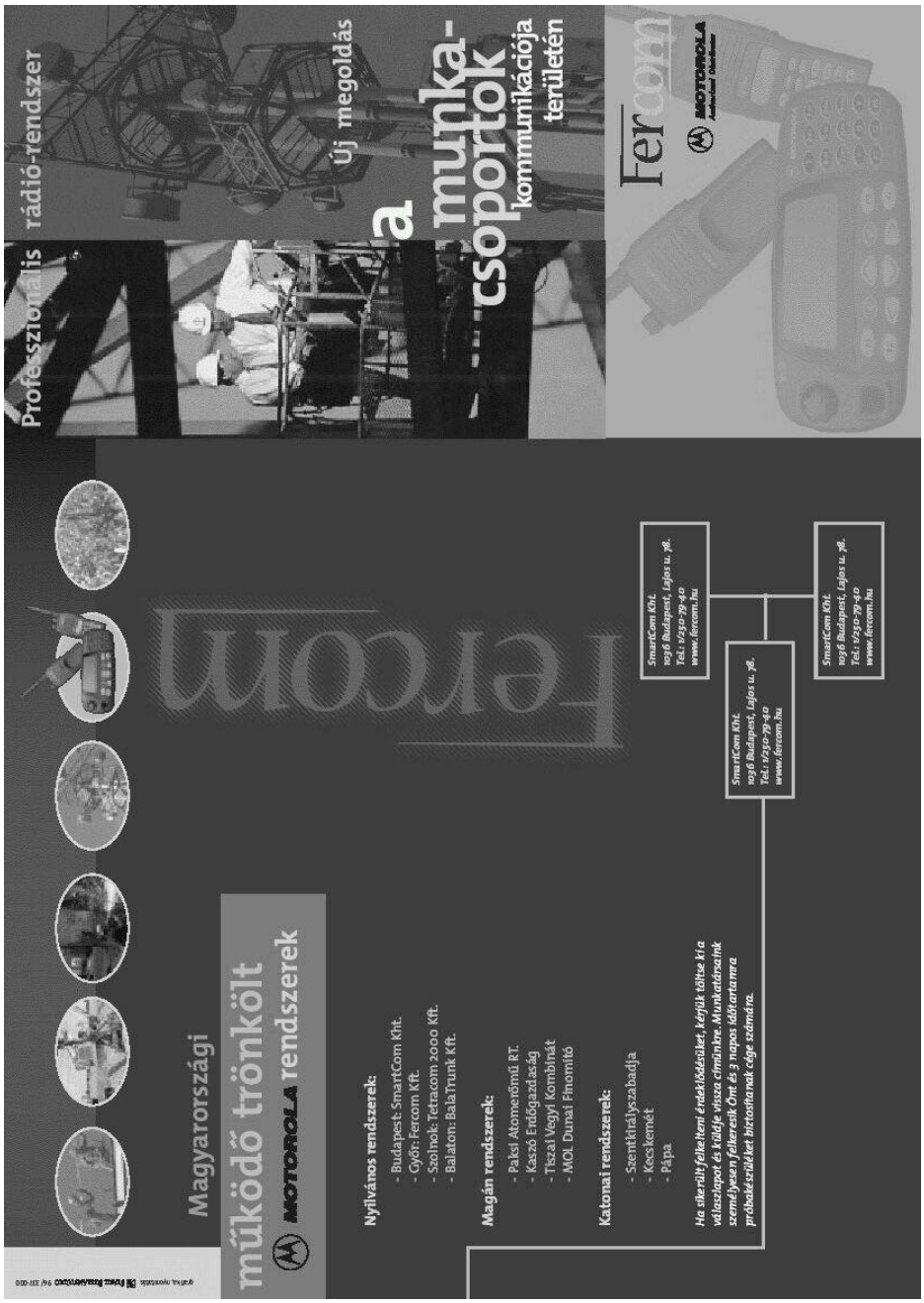


RESEARCH ELECTRONICS INC. - OSCOR, counter surveillance detection systems

SEI - MSTAR battlefield radar, WARLORD system

RESEARCH ELECTRONICS INC. - ORION counter surveillance detection systems

Fercom Kft


Professzionális rádió-rendszer
Új megoldás a munkacsoportok kommunikációja területén
Fercom
működő trönkölt
MOTOROLA rendszerek
Magyarországi
Nyilvános rendszerek:
- Budapest: SmartCom Kft.
- Győr: Fercom Kft.
- Szolnok: Tetracom 2000 Kft.
- Balaton: Bala Trunk Kft.
Magán rendszerek:
- Paksi Atomerőmű RT.
- Kaszó Erdőgazdaság
- Tiszai Vegyi Kombinát
- MOL Dunai Finomító
Katonai rendszerek:
- Szentkirályszabadja
- Kecskemét
- Pápa
Ha sikerült felkelteni érdeklődését, kérjük töltse ki a válaszlapot és küldje vissza címünkre. Munkatársaink személyesen felkeresik Önt és 3 napos időtartamra próbakészüléket biztosítanak cége számára.
SmartCom Kft.
1036 Budapest, Lajos u. 78.
Tel.: 1/250-79-40
www.fercom.hu
SmartCom Kft.
1036 Budapest, Lajos u. 78.
Tel.: 1/250-79-40
www.fercom.hu
SmartCom Kft.
1036 Budapest, Lajos u. 78.
Tel.: 1/250-79-40
www.fercom.hu
Fercom
MOTOROLA


MOTOROLA
SmartNet
URH Rádió Rendszer
Ingyenes
tesztelési
lehetőség
A MOTOROLA SmartNet rádiórendszer
lehetővé teszi, hogy Ön és munkatársai tárcsázás nélkül, egyetlen gombnyomással kapcsolatba kerülhessenek egymással. Ezáltal a cég központjából egyidejűleg, egyszerűen és időveszteség nélkül elérhetők és irányíthatók a város bármely pontján dolgozó munkatársak, valamint biztosított az egyes rádiók közötti közvetlen beszéd-összeköttetés is.
-ben az átjátszókat használó hagyományos URH rádiórendszerekkel ellentétben, a kommunikációban kizárólag csak az Ön cégének tagjai vesznek részt, nem hallanak másokat, nem kell várakozni más beszélgetése végére és Önök sem zavarnak másokat.
egyik fontos szolgáltatása lehetővé teszi, hogy - amennyiben erre igény van - cégén belül több, egymástól független beszédcsoport is létrehozható. A különböző beszédcsoportok akár egyidejűleg is kommunikálhatnak, nem zavarva egymás munkáját. Igény esetén egy vagy több rádiókészülék (pl. az irodában telepített rádiókészülékek) egyszerre több beszédcsoporttal is kapcsolatban lehet.
egyik legnagyobb előnye az, hogy Önöknek már nem kell egy költséges infrastruktúrába beruházniuk. A rendszer használatához csak a rádiókészülékekre van szükség.
rádiórendszer használatáért fixösszegű havidíjat kell fizetni a használt rádiók darabszáma alapján, a beszélgetéssel töltött időtől függetlenül, így Ön költségeit előre kalkulálhatja.
által le nem fedett területeken is használhatók a rádiók, mind szimplex, mind félduplex üzemmódban, amennyiben a felhasználó rendelkezik rádióengedéllyel.
Fercom
MOTOROLA
Authorized Distributor
Budapesten a SmartCom Kht. üzemelteti a Motorola SmartNet nyilvános rendszerét, melynek működési területe Budapest és vonzáskörzete. A jelenleg működő két átjátszó állomás s Főváros és 30 km-es körzetében működik, mintegy 90%-os lefedettséget biztosítva a felhasználók számára.
SmartCom Kht.
1036 Budapest, Lajos u. 78.
Tel.: 1/250-79-40
www.fercom.hu
Győrben a Fercom Kft. üzemelteti a Motorola SmartNet nyilvános rendszerét, teljes lefedettséget biztosítva a felhasználók számára Győr város területén és 30 km-es vonzáskörzetében.
Fercom Kft.
9021 Győr, Aradi Vt. útja 16.
Tel.: 96/525-555
www.fercom.hu
Lehetőséget teremtve rádiórendszerünk gyakorlati kipróbálására cégünk felajánlja, hogy 1 hetes próbaidőre ingyenesen rendelkezésükre bocsát 3 db kézi rádiókészüléket.
A MOTOROLA SmartNet rendszerben a cégünk által forgalmazott szintén MOTOROLA gyártmányú trönkölt URH rádiókészülékek alkalmazhatóak. Ezek a rádiókészülékek rendkívül magas műszaki színvonalúak, és megfelelnek az ipari célú felhasználáson túl a katonai szabványok követelményeinek is. Az igényeknek megfelelően használhatóak
- hordozható, kézi rádiókészülékek
- mobil, autóba telepített rádiókészülékek
- fixen (pl. irodában) telepített asztali rádiókészülékek
A most belépő tagok számára a rádiórendszer használatához szükséges készülékeket kedvező fizetési lehetőségek mellett tudjuk rendelkezésre bocsátani.