

# HÍRVILLÁM

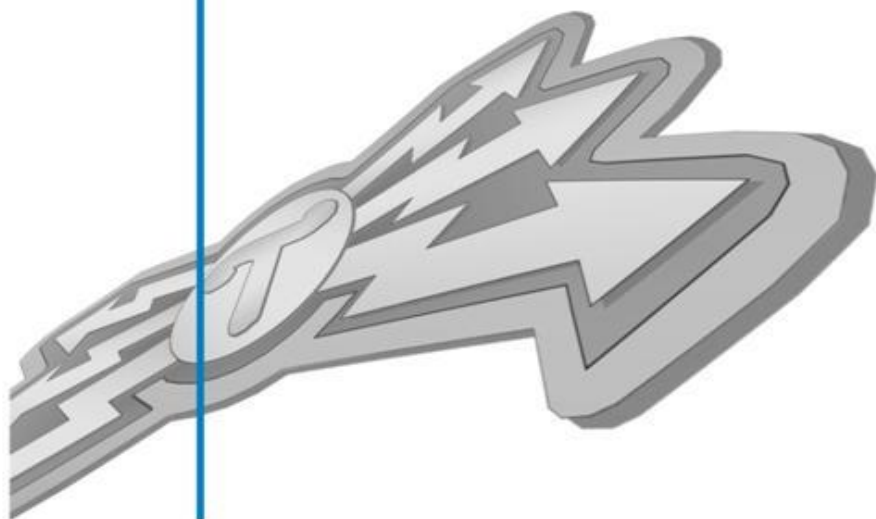
A Zrínyi Miklós Nemzetvédelmi Egyetem  
Híradó Tanszék szakmai tudományos kiadványa

## SIGNAL BADGE

Professional journal of Signal Department  
at the Zrínyi Miklós National Defence University

*2. évfolyam 1. szám*

**2011**





**A Zrínyi Miklós Nemzetvédelmi Egyetem Híradó Tanszék  
tudományos időszaki kiadványa**

***Professional journal of the Signal Department  
at the Zrínyi Miklós National Defence University***

Megjelenik évente két alkalommal

*Published twice a year*



2011. július 15.





*Felelős kiadó/Editor in Chief:*

Dr. Rajnai Zoltán mk. ezredes, egyetemi tanár

*Szerkesztőbizottság/Editorial Board:*

*Elnök/Chairman of the Board:*

Dr. Pándi Erik r. ezredes

*Elnökhelyettes/Depute Chairman:*

Dr. Farkas Tibor főhadnagy

*Tagok/Members:*

Czirok Ferenc nyá. r. ezredes

Dr. Fekete Károly mk. alezredes

Halmai Ottó mk. dandártábornok

Horváth Ferenc dandártábornok

Dr. Hóka Miklós nyá. mk. alezredes

Dr. Horváth Zoltán okl. mk. alezredes

Jobbágy Szabolcs főhadnagy

Dr. Kassai Károly mk. ezredes

Dr. Kerti András mk. alezredes

Dr. Lindner Miklós nyá. altábornagy

Mógor Tamásné százados

Dr. Osváth Zoltán nyá. mk. alezredes

Dr. Révész Gyula mk. ezredes

Dr. Sándor Miklós nyá. ezredes

Dr. Som Ferenc nyá. okl. mk. alezredes

Dr. Szöllösi Sándor nyá. okl. mk. őrnagy

Tóth András főhadnagy

Tőreki Ákos főhadnagy

*Technikai munkatársak/Technical Staff:*

Konta Sándorné

Molnárné Csősz Irma

*Szerkesztő és Webmester/Co-ordinating Editor and Web Manager:*

Dr. Pándi Erik r. ezredes

HU ISSN 2061-9499

\*\*\*

ZMNE BJKMK Híradó Tanszék  
1101 Budapest, Hungária krt. 9-11.  
1581 Budapest, Pf. 15.  
+36 1 432 9000 (29-356 mellék)  
hirado@zmne.hu

## Tartalomjegyzék

|                                                                                               |     |
|-----------------------------------------------------------------------------------------------|-----|
| Köszöntő                                                                                      | 9   |
| <b>Híradás, távközlés, kommunikáció, technika</b>                                             |     |
| <b>Józan Nándor</b><br>JAS 39 Gripen, mint „adoptált gyermek”                                 | 11  |
| <b>Dorkó Zsolt</b><br>A Heves Megyei Rendőr-főkapitányság térinformatikai fejlesztése         | 15  |
| <b>Bindis Bea Brigitta</b><br>A pilóta nélküli repülőgépek (PND) kommunikációs rendszere      | 27  |
| <b>Serege Gábor</b><br>A személyi informatikai eszközök és az IPv6                            | 31  |
| <b>Juhász Márta</b><br>Információcseré és adatátvitel a légi kutatás-mentésben                | 41  |
| <b>Horvayné Fehér Judit</b><br>Elektronikus ügyiratok továbbításának megoldása a Rendőrségnél | 47  |
| <b>Szalai Máté – Pándi Erik</b><br>Egy rendszergyakorlat tapasztalatai                        | 63  |
| <b>Bodnár István – Pándi Erik</b><br>A kommunikáció hajnalától napjainkig                     | 69  |
| <b>Tóth András</b><br>A felhőinformatika alapjai                                              | 85  |
| <b>Szalai Máté</b><br>ERASMUS                                                                 | 91  |
| <b>ifj. Veres György</b><br>Tűzvédelmi stratégia                                              | 95  |
| <b>Veres György</b><br>A katonai alkalmazású komplex villamos rendszerek oktatási kérdései    | 101 |
| <b>Tőreki Ákos</b><br>A C2 rendszer, mint a hálózatközpontú hadviselés eszköze                | 107 |





## **Köszöntő**

A **Hírvillám** második kiadványának megjelenése alkalmából tisztelettel köszöntjük Önt, Kedves Kolléga, Tisztelt Olvasó!

A Zrínyi Miklós Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Kar Híradó Tanszéke idén három ifjú hadnagy kollégával bővíti a Magyar Honvédség tiszti karát Államalapító Szent István királyunk ünnepének napján. Név szerint Bodnár István mk. hadnagy (MH 43. Nagysándor József Híradó és Vezetéstámogató Ezred, szakaszbparancsnok), Koncz Bencze mk. hadnagy (MH Támogató Dandár, szakaszbparancsnok), valamint Szalai Máté mk. hadnagy (MH 54. Veszprém Radarezred, szakaszbparancsnok) személyében, akik közül utolsó kettő hallgatónk kiválóan végzett.

Az elmúlt félév sikeres volt számunkra mind oktatási, mind kiképzési, mind tudományos szempontból, hiszen immáron négy negyedévesünkön túl hét haramadéves tisztjelölttel bővültünk, négynapos, összevont híradó szakharcászati zárógyakorlatot tartottunk, a HVK Híradó, Informatikai és Információvédelmi Csoportfőnökség védnökségével megszerveztük és lebonyolítottuk a második nemzetközi katonai információbiztonsági konferenciát, illetőleg ismét megjelentettük a Hírvillám kiadványunkat.

Reményeinknek adunk hangot, hogy az őszi félév sem alakul másképpen, amellyel egyidejűleg a kiadvány áttekintéséhez jó időtöltést kívánunk, egyúttal szemléljük bizakodva a jövőt, hogy a Hírvillám a szakmai-tudományos élet mérvadó fórumává válik.

**Budapest, 2011. július 15.**

**Pándi Erik**  
tanszékvezető



Józan Nándor

## JAS 39 GRIPEN, MINT „ADOPTÁLT GYERMEK”

### Absztrakt

*Jelen közlemény a Gripen JAS-39 típusú harci repülőgép hazai felhasználásának egyes kérdéseit tisztázza.*

*This article is about a combat aeroplane, called JAS-39 Gripen. We are entitled to state that this type of aircraft is the adopted child of the Hungarian Air Force by hiring from the Swedish Government. This publication provides the basic data of its armament and flying attributes. It also represents the ways of co-operation between the governments of Hungary and Sweden.*

**Kulcsszavak (key words):** *katonai műveletek, Magyar Honvédség, légierő ~ military operations, Hungarian Defence Forces, Air Force (Defence)*

### BEVEZETÉS

Svédország a XIX. század óta deklaráltan semleges állam. Ennek is köszönhető, hogy haderejét többségében saját fejlesztésű haditechnikai eszközökkel igyekszik ellátni. Vonatkozik ez a harcászati repülőkre is, ahol jelenleg már többnyire a Gripen többfeladatú harcászati repülőgépek védik az országot. Az önálló fejlesztésű, olcsón üzemben tartható, többfeladatú könnyű harci repülőgép, a legkisebb negyedik generációs vadászgép.

### 1. A FEJLESZTÉS KEZDETEI

A Saab, az Ericsson, a Volvo, a Saab Avionics és az FFV Aerotech fejlesztette. A gyártásban a BAe<sup>1</sup> is részt vett a futóművek és a szárnycsatolás gyártása révén (2003-ban kivonult). A JAS, a *Jakt, Attack och Spaning* hármas rövidítése, vagyis vadász, támadó és felderítő. 1988-ban repült először, a svéd légierő 1997-ben állította szolgálatba. Kis tömegéhez mérten óriási tömegű fegyvert lehet rá függeszteni: 5300 kg-ot. Ez éppen a duplája, mint elődjének, a JAS-37 Viggennek<sup>2</sup>. Kacsá előszárnyas, deltaszárnyú gép, mint a többi új fejlesztésű európai gép, a Eurofighter és a Rafale<sup>3</sup>, vagy elődei, a Viggen és a J-35 Draken (utóbbi előszárny nélkül). Ez kitűnő manőverező képességet ad neki. Alkalmas légvédelemre, amennyiben bevetethők repülőgépek, helikopterek és rakéták elfogására. Különösen rugalmas, Svédországban több száz ideiglenes támaszponton tölthetik és fegyverezhetik fel, országúton is fel és leszállhat (persze jó minőségű utakon).

---

<sup>1</sup> British Aerospace – Brit repülőgépgyártó cég.

<sup>2</sup> Szuperszonikus deltaszárnyú vadászbombázó repülőgép, melyet Svédországban fejlesztettek ki és gyártottak.

<sup>3</sup> Negyedik generációs, szuperszonikus, vadászbombázó repülőgép, melyet Franciaországban gyártanak a mai napig.

Ezen remek harcászati adatok miatt a Svéd Légierő 12 repülőszázad felállítását kezdeményezte, ám ez a bővítés a Hidegháború befejeződésével meghíúsult. A háború befejeződése a Svéd Légierőre is nagy kihatással volt, így döntés született, hogy az eredetileg tizenkettő Gripen századból csak nyolcat állítanak fel négy repülőezredbe szervezve. Így az addig már megrendelt 204 Gripen típusú repülőgép egy része feleslegessé vált a Svéd Légierő számára. Ez arra készítette a gyártót, hogy fokozza addig is aktív marketing tevékenységét, melynek keretében igen erősen kampányoltak hazánkban is már 1995-től. Az első külföldi megrendelő a Dél-Afrikai Köztársaság lett, mely egy csomag részeként 24 Hawk kiképző repülőgép mellett 28 darab (19+9) Gripent is rendelt. Emellett a Gripen ekkor még versenyben állt többek között Magyarországon, Csehországban, Lengyelországban, Ausztriában, Braziliában és Chilében is.

## 2. A HAZAI BESZERZÉS KÉRDÉSEI

Mivel hazánk anyagi helyzete nem tette lehetővé új gyártású repülőgépek beszerzését, ezért 2001. elején használt gépek bérletére kért ajánlatot, többek között a svéd kormánytól is, akik 24 (20+4) használt JAS 39 A/B változat 10 éves lízingjét ajánlották. Végül a magyar kormány 2001. szeptemberében - nagy meglepetést okozva - jelentette be, hogy Gripenekkel kívánja leváltani a rendszerben lévő MiG-29-eseket, és tárgyalásokat kezdenek a svéd kormánnyal 14 (12+2) használt Gripen 10 éves bérletéről. Az erről szóló szerződést 2001. novemberében írták alá, mely később módosításra került C/D típusú repülőgépek beszállítására.

Magyarország 2008. január 28-án vette át a 14 darab legmodernebb C és D verziójú JAS-39 harci gépet, amelyekből 12 együléses és 2 kétüléses. A változatok megkülönböztetése igen egyszerű: A: alaptípus; B: kétüléses gyakorlőváltozat; C: továbbfejlesztett változat fedélzeti oxigéngenerátorral, színes kijelzőkkel és légi utántöltési lehetőséggel; D: a „C” változat kétüléses változata. A repülőgépek fontos jellemzője a légi utántöltés lehetősége, ennek érdekében minden repülőgép visszahúzzható légi utántöltő csonkkal van felszerelve. A légi utántöltés megteremti a lehetőségét annak, hogy a magyar légierő gépei hazánktól távol, NATO bevetésekben vegyenek részt. A „C” és „D” Gripen változatok rendelkeznek mindazokkal a képességekkel, amelyek lehetővé teszik a NATO-n belüli hatékony együttműködést a kommunikáció, a navigáció, az azonosítás, a fegyverzet, a logisztikai támogatás, a feltöltés, a földi kiszolgálás és a kiképzés területén. A többi NATO-tagország légierőjével történő hatékony és zökkenőmentes együttműködést az azonos navigációs és műszeres leszálló rendszerek, az angol nyelvű kijelzők és jelzések, valamint a NATO szabványnak megfelelő fegyverzet és rakétatartók teszik lehetővé: beépített radarirányítású 27 mm-es Mauser gépágyú, Sidewinder, AMRAAM és a legújabb német fejlesztésű IRIS-T légiharc rakéta. Felszíni célok elleni irányított fegyverei között a Maverick mellett ott van a svéd fejlesztésű RBS-15F hajók elleni rakéta is. Bofors ARAK 70 mm-es nem irányított rakétakonténer. Felderítéshez külső konténerben magával vihet elektrooptikai eszközöket, amelyekkel és radarjával bármilyen látási viszonyok között képes az ellenséget felderíteni.

## 3. A SVÉD-MAGYAR EGYÜTTMŰKÖDÉS

A magyar-svéd együttműködés igen erős és összehangolt, mi sem bizonyítja ezt jobban, mint a pilótaképzések (Satena légibázis) Svédországban, vagy a „Satenas Exchange 2011” nevű közös repülőkiképzés, amely 2011. november 9-16. között zajlott le a Kecskeméten, a MH 59. Szentgyörgyi Dezső Repülőbázis Puma század és a Svéd Légierő F7-es század

pilótái részvételével. A közös kiképzési repülés a svédek ötlete volt, a *Satenas Exchange 2011* elnevezésű gyakorlat résztvevői „*Gripen Maffia 2011*” felirattal külön felvarrót is készítettek maguknak. Ez az első olyan közös kiképzési repülés, amelyen mindkét ország pilótái JAS 39-essel vettek részt. A svéd század három kétüléses és három együléses gépe, tizenkét pilótája, két tervező tisztje és huszonhárom technikus a részt a gyakorlaton.

„A magyar és a svéd pilóták gondolkodása hasonló, mindössze a repülőgépek működtetésében voltak különbségek a két nemzet pilótái között” - mondta Richard Carlqvist őrnagy, aki szerint a közös repülőképzés jó alkalom volt arra, hogy a kiképzők tapasztalatot szerezzenek arról, hogy a magyar pilóták a tanultakat hogyan adaptálták Kecskeméten.

## ÖSSZEGZÉS, KÖVETKEZTETÉSEK

A Magyar Honvédség eddigi tapasztalatai azt mutatják, hogy a svéd gyártmány katonai alkalmazása megfelel mind hazánk, mind a szövetség elvárásának.

## FELHASZNÁLT IRODALOM

- [1] [www.canit.se/~griffon/aviation/gripen](http://www.canit.se/~griffon/aviation/gripen)
- [2] [www.saabgroup.com](http://www.saabgroup.com)
- [3] [www.wikipedia.org](http://www.wikipedia.org)
- [4] Szabó József, Peták György: A Gripen, 2003.
- [5] Lőrinczy Szabolcs mk. alezredes: A magyar légierő fejlesztése a légi utántöltőképesség megvalósításával, 2009.
- [6] Szentesi György: Gripen-repülőgép a magyar légierőben, 2001.



**Dorkó Zsolt**  
dorkozs@emgei.hu

## **A HEVES MEGYEI RENDŐR-FŐKAPITÁNYSÁG TÉRINFORMATIKAI FEJLESZTÉSEI**

### ***Absztrakt***

*Jelen közlemény bemutatja a Heves Megyei Rendőr-főkapitányság helyzetismereti megoldásainak fejlesztési állomásait.*

*This announcement shows the situation solution development stages of Heves County Police headquarters*

**Kulcsszavak (key words):** GPS<sup>4</sup>, AVL<sup>5</sup>, rendőrség, térinformatikai rendszer ~ GPS, AVL, police, geographic information system

### **BEVEZETÉS**

A rendőrségi csapaterős tevékenységeinél különösen nagy hangsúlyt kapnak a térinformatikai, helyzetismereti alkalmazások. Bár ezek az alkalmazások a rendőrségen nem mondhatók újak és ismeretlennek mégis szinte újra felértékelődött, illetve átértékelődött a szerepük. A statikusnak mondható értelmezést villámcsapás szerűn váltotta fel a folyamatosan aktualizált dinamikus jellegű értelmezés.

A csapaterős tevékenységek alapvető jellemzője a térbeli jelleg. Ebből következően a helyzetismeret megjelenítésének alapvető formája a vizuális megjelenítés. A helyzetismeret vizuális megjelenítésének egyik legkézzelfoghatóbb és a rendőrség helyi és területi szerveinél is megtalálható megjelenési formája, a Jármű és Rádióterminál-követő szolgáltatás. (elterjedt angol rövidítése: AVL).

A rendszerben rejlő lehetőségeket a felhasználók köztük a rendőrség, jelenleg nem használja ki teljesen. A helyzetismeret megteremtésére irányuló képesség jelentheti azt is, hogy a felhasználási területet kitágítjuk és teljesen új funkciók integrálásával, fokozhatjuk ezt a képességet.

A közleményben szeretném bemutatni a Heves Megyei Rendőr-főkapitányságon megvalósult helyzetismereti alkalmazásokat, részleteiben is bemutatva az Integrált Járműkövető és Tevékenységirányító Minta-rendszert, az AVL rendszert, illetve az azt felváltó Pro-Mobil alkalmazást, valamint a helyzetismereti alkalmazások fontos szerepét a bevetés irányításban.

---

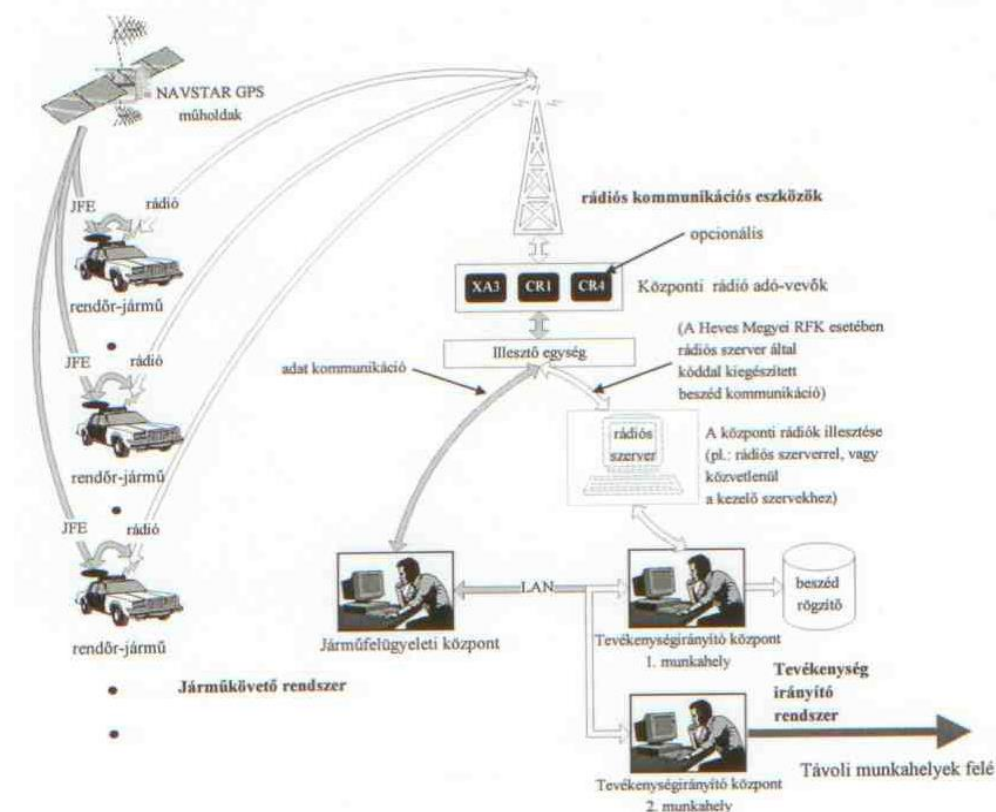
<sup>4</sup> Global Position System (Globális Helymeghatározó Rendszer)

<sup>5</sup> Automatic Vehicle Location

## 1. AZ INTEGRÁLT JÁRMŰKÖVETŐ ÉS TEVÉKENYSÉGIRÁNYÍTÓ MINTA-RENDSZER

Az Egységes Digitális Rádiórendszer bevezetése előtt a rendőrség különböző területi szerveinél több egymástól független próbálkozás, illetve kísérlet történt egy komplex, az ügyeleti, illetve közterületi feladatok támogatását segítő helyzetismeret alkalmazás, illetve rendszer kidolgozására.

A Heves Megyei Rendőr-főkapitányság a HM EI Rt.-vel együttműködve dolgozta ki saját rendszerét. A kifejlesztett járműkövető rendszer a NAVSTAR<sup>6</sup> GPS alapú helymeghatározó rendszer szolgáltatásait használta, integrálva a HRFK Tevékenységirányító rendszerével, az 1.sz. ábra szerinti rendszervázlat alapján. Az integrált rendszer képes volt a Járműfedélzeti egységekben (JFE) a műholdakról sugárzott jelek alapján 150 m pontosságú helymeghatározásra, a jármű útvonalával és állapotával kapcsolatos jelzések, ezáltal a szolgálatot teljesítő rendőrök tevékenységének naplózására, a pillanatnyi pozíciók, állapotok és a napló továbbítására a Járműfelügyeleti központ felé. Ennek segítségével lehetővé tette a járművek helyzetének meghatározását a bevetés irányítás támogatására, biztosította a rendőrijárművek útvonalának ábrázolását és utólagos kiértékelését a központi térképeken. Üzenetváltást tett lehetővé a jármű vezetője és a központi ügyelet között, továbbá lehetővé tette a vészjelzés esetén a központi riasztást, az erősítés hatékony megszervezését



1.sz. ábra [1]

<sup>6</sup> Navigation Satellites for Timing and Ranging (navigációs műholdak idő-, és távmérésre)

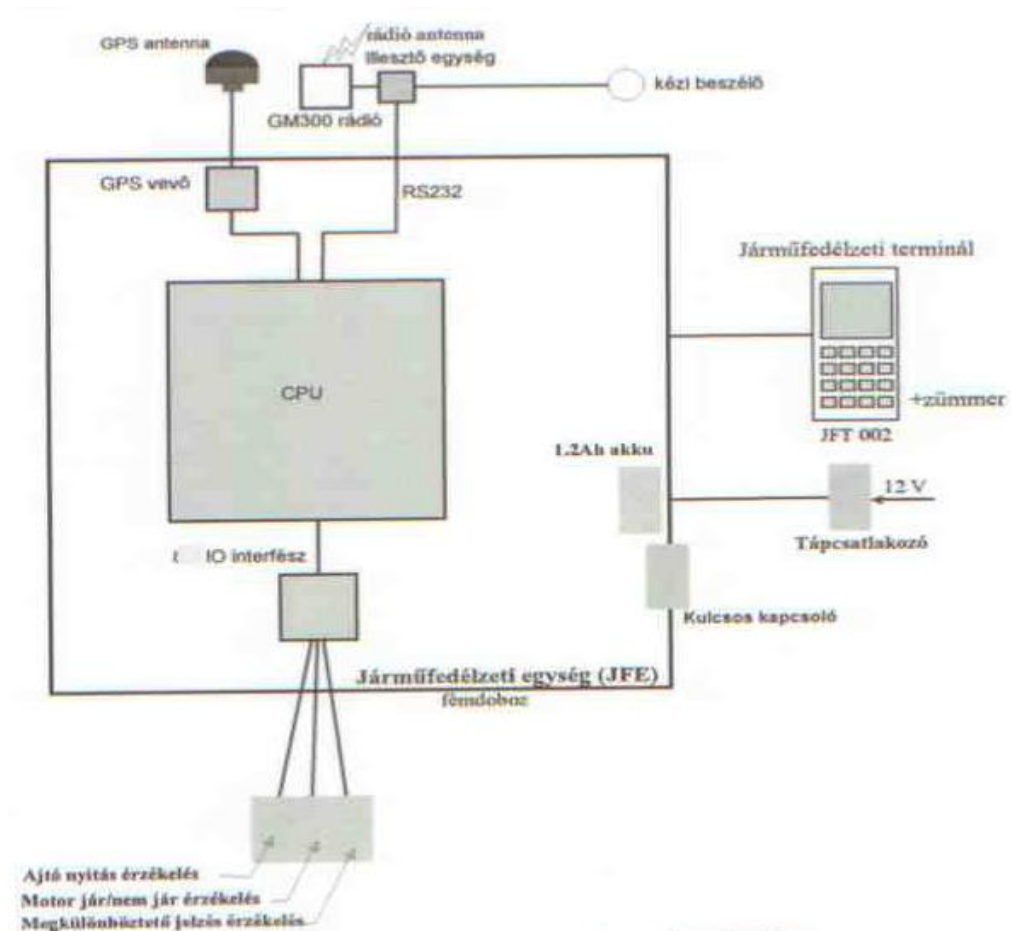


### 1.1. A rendszer felépítése

A rendszer járművekbe telepített egységekből, Járműfelügyeleti központból, Tevékenységirányító központi munkahelyekből és rádiós kommunikációs eszközökből állt. A központok és a járművek közötti kapcsolat beszéd és beszédmód alatti digitális adatátvitellel, analóg rádió csatornákon, analóg elven működő rádió adó-vevőkkel valósult meg. Az Integrált rendszer felhasznalta a tevékenység irányító- és rádiós kommunikációs eszközöket, programokat és rendszerben történő működésüket.

A rendőr-járműbe telepített egységek (2. sz. ábra )

- Jármű fedélzeti egység (JFE)
- GPS antenna
- Járműfedélzeti terminál
- Illesztő egység
- Jármű elektromos illesztő szerelvények, kábelezés



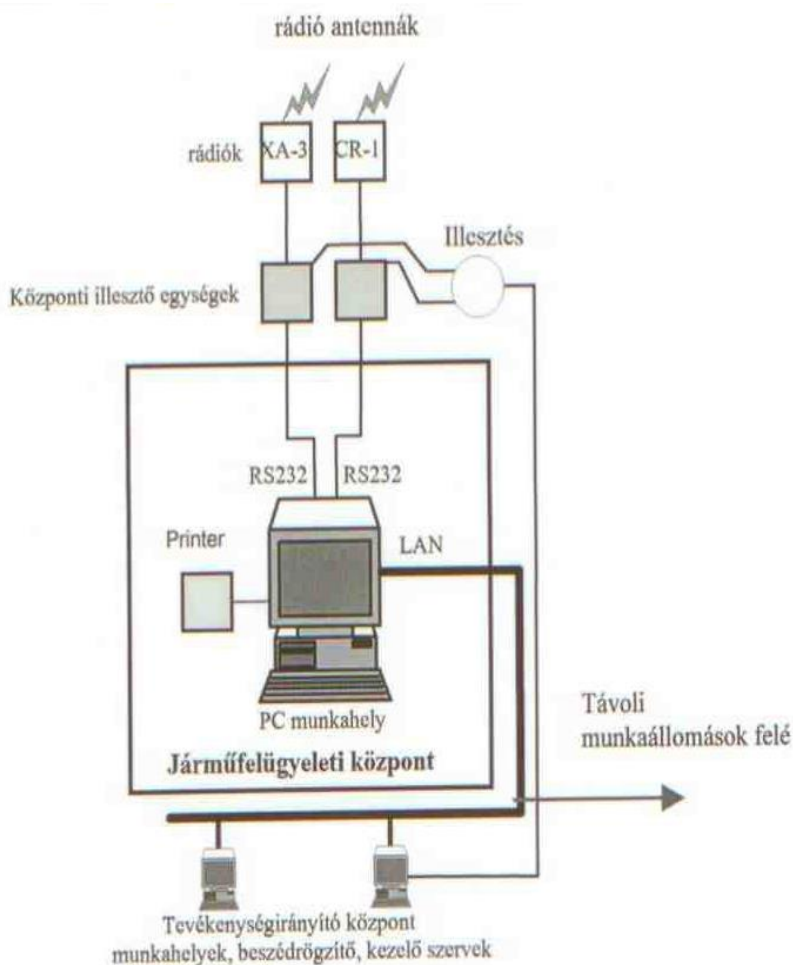
2.sz. ábra [2]

A GM300-as Motorola rádió, tartozékai és kézi-beszélője a járművek meglévő, korábban beépített kommunikációs eszközei. A beszéd kommunikáció változatlan működtetése mellett az illesztő egység segítségével a JFE kétirányú digitális adatkommunikációra képes.

A Járműfedélzeti egység egy processzor alapú intelligens eszköz, amely gyűjti és tárolja a térképészeti koordinátákat és a járművön kijelölt, illetve elhelyezett állapot figyelők jelzéseit. Vezérli és illeszti a kézi-beszélő és a rádió közé közbeiktatott Illesztő egység segítségével a központ felé az adatforgalmat. A JFE rövid idejű tápfeszültség-ellátás zavarainak kiküszöbölését belső akkumulátor biztosítja. A JFE tápellátásának bekapcsolása és programjának indítása kulcsos kapcsolóval történik.

A Járműfedélzeti terminál egy 4x20 karakteres háttér világításos kijelzőt és egy 16 gombos nyomógombsort tartalmaz. A Járműfedélzeti terminál a számozott üzenetek kiválasztását, (a JFE-en keresztül) központba küldését, valamint az onnan érkező üzenetek megjelenítését és nyugtázását végzi.

### 1.2. Az Integrált Járműkövető és Tevékenységirányító központ felépítése



3.sz. ábra [3]

### 1.3. Az Integrált Járműkövető és Tevékenységirányító Központ működése

Az Integrált Járműkövető és Tevékenységirányító központ a korábbi szolgáltatások megtartása mellett komplexebb szolgáltatások nyújtására alkalmas, mint pl.:

- a járművek tevékenységének ellenőrzése, dokumentálása,
- a járművek hatékonyabb bevetés irányítása, térképes követésük, üzenetek közvetítése útján,
- a bevetésben résztvevők biztonságának növelése.
- a rendszer adatvédelmének-, biztonságának növelése.

Az integrált rendszer komplex működését a Rádiós kommunikációs eszközök közös felhasználásával, valamint a két központ közötti hálózatos kommunikáció segítségével optimálisan oldotta meg.

A járművek és a központ közötti beszéd-kommunikáció elsődlegességét fenntartva, a beszéd-forgalom kismértékű zavarása mellett a Járműkövető központ (kommunikációs szoftverével) digitális adatkapcsolatot tartott fenn a járművekkel.

A Járműfelügyeleti központ a járműparaméterek beállítását, a pozíciók és állapotok megjelenítését, a naplórészletek elkérését, a naplók (útvonalak) visszajátszását és nyomtatását, valamint a riasztások lekezelését végezte el. A Járműfelügyeleti központban egy kommunikációs és egy térképes szoftver futott egy időben.

A kommunikációs és térképes szoftver egy WINDOWS NT operációs rendszer alatt futtatható integrált programcsomag, amely a járművek konfigurációját, kommunikáció vezérlését, a pozíciók és állapotok begyűjtését, a riasztások lekezelését, a napló adatbázisok összeállítását, ennek adatai alapján a térképes megjelenítést és a nyomtatást végezte.

A kommunikációs szoftver feladata volt, hogy a járművekkel a kommunikációt fenntartsa, a JFE pozíció adatai, állapota, naplórészleteinek kiolvasását vezérelje, a kiolvasott adatokat eltárolja, folyamatosan építve egy adatbázist (az adott naphoz egy fájlt rendelve, ebben gyűjtve a járművek pozíció és állapot jellemző adatait).

A térképes program feladata a járművek konfigurálása, a beérkezett jelentéseket az összeállított naplótartalom alapján, grafikus térképi háttérrel pozíció helyesen, és az egyéb állapotokat pedig táblázatosan ábrázolni, valamint kezelni a riasztási (vészhelyzet) és a nyomtatási feladatokat.

A tevékenységirányító munkahelyek, módosított tevékenységirányító programjukkal a korábbi szolgáltatásaikon felül az üzenetváltások lekezelését, ezáltal a bevetés-irányítás támogatását végezték.

A tevékenységirányító munkahelyeken a tevékenységirányító programmal párhuzamosan futtatható volt a térképes program, amely a járművek pillanatnyi pozícióit és állapotait jelezte a bevetés-irányítás további támogatására. A munkahelyeken lehetőség volt a naplók visszajátszására és nyomtatására, valamint a központi riasztás (vészhelyzet) lekezelésére is. A térképes programokhoz szükséges digitális térképeket a munkahelyek helyi adattároló eszközein kellett elhelyezni. A tevékenységirányító és a térképes programok működtetéséhez a járműkövető központ kommunikációs szoftvere egy kimeneti állományt generált. A tevékenységirányító szoftver üzeneteit és utasításait egy bemeneti állomány írása segítségével juttatta el a Járműfelügyeleti központra keresztül a járművekbe.

A rendszer teljes kiépítésében nem került a megyében rendszerezítésre, azonban a HM EI Rt. sikeresen alkalmazta az ugyanezen, elveken felépített járműkövető rendszerét a polgári biztonsági cégek, fuvarozó-, és a kommunális vállalatok körében úgy, hogy rendőrség URH mozgószolgálati rádió rendszere helyett az adatátvitelt a GSM szolgáltatók segítségével valósította meg. Ezt az adatátviteli közeget mi is teszteltük és használtuk, azonban a projekt egyik nem titkolt célja az volt, hogy a meglévő infrastruktúra lehetőségeit használjuk ki.

Amit maximálisan sikerült elérnünk, hiszen az adatátvitel ez esetben költségmentesen volt megoldható

Már e rendszer kidolgozásának a stádiumában is várható volt az EDR bevezetése azonban akkor még nem ismertük benne rejlő helyzetismeret lehetőségeket. Ezen lehetőségek mondhatni egy csapásra megoldották azokat a problémáinkat, amelyekre a fejlesztéseink irányultak azonban az itt megszerzett tapasztalatokat a TETRA<sup>7</sup> technológiára épülő rendszernél is hasznosítani tudtuk.

## 2. AZ AVL RENDSZER, MINT TERMINÁLKÖVETŐ SZOLGÁLTATÁS

A TETRA technológia megjelenésével okafogyottá váltak a megyei szintű térinformatikai fejlesztések, hiszen az EDR<sup>8</sup> rendszer azonnal kétféle megoldást kínált a rádiókészülékek, vagy másképpen terminálok ezzel együtt a felhasználók, vagy a rádiót hordozó gépjárművek helyzetének megállapítására.

Valamennyi diszpécser munkaállomás képes tájékoztatni a diszpécsert arról, hogy az ő felügyelete alatt álló felhasználók a hálózat melyik cellájában tartózkodnak. Azonban sokkal pontosabb pozíció meghatározást tesz lehetővé, ha a követendő jármű el van látva GPS vevőkészülékkel. A pozícióinformációt a GPS-hez csatlakoztatott EDR rádión és a hálózaton keresztül elküldi a diszpécser munkaállomásnak.

Az Egységes Digitális Rádiórendszer ezen szolgáltatása az ún. terminál-követés. Ezzel a technikai megoldással lehetővé válik, hogy a készülékek földrajzi helyzete ismertté váljon, amit a készülékek kijelzőjén szükség szerint meg is tudnak jeleníteni. A mért földrajzi pozíciót az EDR hálózatban elérhető terminálokra SDS<sup>9</sup> formájában továbbítani is lehet. A földrajzi koordinátákat és a tengerszint feletti magasságok, valamint a pont megnevezését, illetve, az ahhoz csatolt magyarázó szöveget, üzenet formájában továbbítjuk. Maga a terminál-követő rendszer a készülékek e technikai lehetőségére épül. A terminálkövető szolgáltatás egy szerver-kliens felépítésű rendszerből áll, amely meghatározott időnként lekérdezi a követésre kijelölt terminálok földrajzi koordinátáit. A beérkezett üzeneteket a szerver az EDR rendszerén keresztül megkapja, feldolgozza és a felhasználó képernyőjén grafikus és szöveges formában megjeleníti.

### 2.1. Az AVL rendszer felépítése

- Rádióterminálok
- Szerverek
- Adatkapcsolat a terminálok és a szerverek között.
- Adatkapcsolat a szerverek és a követő munkahelye között.
- A Jármű és Rádióterminál-követő munkahely

---

<sup>7</sup> Terrestrial Trunked Radio ( földi trónkölt rádió)

<sup>8</sup> Egységes Digitális Rádió Rendszer

<sup>9</sup> Short Data Service



4. sz. ábra [4]

A rádióterminálok:

A nyílt szabvány lehetővé teszi, hogy a TETRA hálózati infrastruktúrában, különböző szállítók által gyártott rádióterminálok működjenek. A Heves Megyei Rendőr-főkapitányság az 1. ellátási fázisban kapta meg a terminálokat, illetve kezdte el azok üzemeltetését. Az 1. ellátási fázisban valamennyi felhasználó EADS terminálokkal lett ellátva. A terminálok közül az AVL rendszerben az EADS THR 880i és az EADS TMR 880 rádióterminálok integrálhatók.

A terminálok helymeghatározó szolgáltatásai:

- A rádióterminálok GPS modulja 2D, vagy 3D típusú mérésre alkalmas.
- Meghatározható a terminál földrajzi koordinátája,
- a terminál mozgásának sebessége,
- a rádióterminálokon a mozgásának az iránya az északi földrajzi irányhoz képest jobbra forgó 360°-os rendszerben.
- Az AVL rendszer irányába továbbított időadat a műholdak atomórájától származik. A rendszer az egyértelmű időmérés miatt az UTC időt használja
- A dátumot szintén a GPS rendszer szolgáltatja, így az sem változtatható meg.

A terepen rögzíthetjük a készülék segítségével a pillanatnyi tartózkodási helyünk koordinátáit és a hozzá tartozó dátum és idő adatokat. Az így képződő pontot egyedi azonosítóval elláthatjuk, és elmenthetjük a terminál memóriájába illetve továbbítjuk az AVL rendszerhez.

A navigációs modul mindkét rádiótípusnál megfelelő jogosultság esetén ki- illetve bekapcsolható a készülék menüjéből azonban a HRFK-n szinten ezt a szolgáltatást a felhasználók nem kapcsolhatják ki.

A TMR 880-as készülék jellemzően jármű-fedélzeti használatra készült, azonban stabilan is telepíthető. A felhasználás jellegéből adódóan a THR 880i kézirádióhoz képest többszolgáltatásokat is nyújt.

Főbb jellegzetességeik:

- Külső kommunikációs- és GPS antennával rendelkezik

- A készülékhez önálló egységként csatlakozik a GPS vevő.
- Egyéb információkat is tud fogadni a járművön elhelyezett jeladóktól (motor kikapcsolt-bekapcsolt állapota, ajtónyitás, megkülönböztető jelzés használata, stb.) és azt továbbítani tudja az AVL rendszer segítségével a központba.

A szerverek valamint az adatkapcsolat a rádióterminálok, és a szerverek között:

A terminálok a GPS egységükkel meghatározzák a földrajzi helyzetüket, ezt követően üzenetet küldenek az AVL központba. A terminálokban programozott feltételek meghatározzák, mekkora megtett út után, vagy mennyi eltelt idő után küldjön üzenetet a központba, de az AVL munkahelyről is kezdeményezhető lekérdezés. Az üzenet tartalma a helymeghatározási adatok továbbítására alkotott kommunikációs szabványnak megfelelő, SDS formátumú üzent. A beérkező adatokat a kommunikációs szerver fogadja, és átadja a feldolgozó szervernek, amely SQL<sup>10</sup> adatbázisban tárolja az adatokat.

A terminálkövető szolgáltatást kiszolgáló szerver tulajdonképpen nem egy, hanem több együttműködő szerver. Területi elv szerint felosztották a szolgáltatást, megosztva az adatbázis-kezelés feladatát, amelyek az erőforrás megosztást és a működési biztonságot szolgálják. A szerverfarm, egy másik, a TCS<sup>11</sup> TETRA kapcsolattartó szerver segítségével kapcsolódik az EDR hálózathoz. A terminál-követő szolgáltatást megvalósító szerver logikailag is tagolt a következőkként:

- Kommunikációs szerver
- Elosztó szerver
- Feldolgozó szerver
- Publikációs szerver

Adatkapcsolat a szerverek és a követő munkahelye között:

A kliens, tehát az a számítógép, amelyen az operátor a szolgáltatást igénybe veszi, a kijelölt ügyleteken van elhelyezve. A kapcsolat TCP/IP protokollon, zárt hálózatban épül fel a kliens és a publikációs szerver között. A felhasználó számítógépén nem kíván a szolgáltatás speciális kliens oldali szoftvert, hanem Internet Explorer böngésző segítségével vehető igénybe a szolgáltatás.

A terminál - követő munkahely kialakítása:

A fő ablak: A leggyakrabban használt ablak felső ¾-ét, egy digitális térkép tölti be. Ezen a felületen jelenik meg Magyarország úthálózati térképe. A térkép vektoriális térkép, ezért minőség romlás nélkül nagyítható, illetve kicsinyíthető. A térkép léptéke változtatható. A szoftver automatikusan az optimális léptéket állítja be. Az ablak alsó részén a követésre felvett terminálok listája található. A táblázat első oszlopa tartalmazza a terminálok egyedi azonosítóit, amely lehet név, vagy gépjármű rendszám, stb. A második oszlopban az utolsó jelentés időpontja olvasható. Az előbbieken kívül megjeleníthető, a terminál mozgási sebessége, a GPS készülékének állapota, valamint a pánik-gomb esetleges használata. A táblázat oszlopai a felhasználó igénye szerint bővíthetők.

Térképen megjelenített adatok: A térkép olyan települések utca szintű térképét tartalmazza, amelyek lélekszáma meghaladja a 2000 főt, az annál kisebb települések csak a település határral kerültek ábrázolásra. Az utcák nevén kívül a sarkok házszámai láthatók. A sarkok közötti számok megállapítása, a térképi hely ismeretében, interpolálással történik. A terminál mozgását a jelentések beérkezésének helyszínét mutató pontokból álló pontsor ábrázolja, köztük a haladás irányát mutató nyilakkal. Abban az esetben, ha a terminál mozgását ábrázoló pont a térkép olyan részletén halad keresztül, amely nem közút ábrázolása, akkor a terminál olyan úton vagy egyéb területen halad, amely nincs a térképen ábrázolva.

---

<sup>10</sup> Structured Query Language ( struktúrált lekérdező nyelv)

<sup>11</sup> TETRA Connection Server

Megfigyelt körzetek megjelenítése és használata: A felhasználó a digitális térkép egy rétegén képes kijelölt területeket, (pl. elsődleges működési terület) bejelölni. Ezek a körzetek geometriai értelemben lehetnek körök, sokszögek, vagy vonalak. A kijelölés célja az, hogy a kiválasztott terminál mozgását ellenőrizze, adjon információt a terminálkövető rendszer felhasználójának arról, hogy a kijelölt területet a terminál elhagyta, vagy a kijelölt területre a terminál belépett.

A terminálok adatainak elemzése: A követett terminál mozgásával kapcsolatos adatait folyamatosan adatbázisban tárolják, és a kiválasztott adatokat online megjelenítik. A tárolt adatok a későbbiek során külön elemzésre betölthetők. Az elemzés az adatok vizuális megjelenítésével vagy adatbázis-kezelő szoftverek terén ismert lekérdezésekkel történhet.

A vizuális megjelenítés: Egy ablakban megjelennek a kiválasztott terminál adatai. A vízszintes tengelyen az idő, a függőlegesen a pillanatnyi sebesség látható. A megjelenítés idő szerint nagyítható, és kicsinyíthető, vagyis a mozgás apró sebesség ingadozásai is láttathatók. A terminál által közölt adatok ezzel egy időben megjelennek, így adott időpontban láthatjuk, hogy a jármű milyen sebességgel haladt és a megkülönböztető jelzéseit használta-e. A terminál esetében a pánikgomb használatának megjelenítése lehet fontos.

### 3. A PRO-MOBIL JÁRMŰKÖVETŐ RENDSZER

Az AVL rendszer bebizonyította, hogy a hatékony tevékenységirányítás és flottamenedzsment alapja a jó minőségű, több funkciós járműkövető rendszer.

A szolgáltató a szolgáltatási szerződésének keretében, az EDR hálózat indulásakor meghatározott követelményeknek megfelelő az AVL rendszert fejlesztett ki és telepített a felhasználók részére. A rendszer használata során megfogalmazott javaslatok, kérések eredményeképpen megújult az AVL. A rendszer fejlesztésének eredményeként a szolgáltató üzembe helyezte a megújult az ún. Pro-Mobil Járműkövető rendszert.

2010. május 01-től, kizárólag a lényegesen több funkciót és adatot tartalmazó Pro- Mobil Járműkövető rendszer érhető el.

A technika nyújtotta lehetőségeket és a biztonság megtartásával, a szolgáltató kiterjesztette a Pro-Mobil terminálkövető szolgáltatás elérhetőségét:

- EDR hálózaton keresztül: AVL munkaállomás, illetve DWS<sup>12</sup> munkaállomásról
- HSDPA<sup>13</sup> kapcsolat, internetes technológia, de szeparált hálózat (külön APN)
- DSL kapcsolaton keresztül szeparált hálózat
- Tetra modemet tartalmazó tablet PC megoldás. EDR hálózat nyújtotta, szerényebb sávszélességű, de magas rendelkezésre állású, és minden készenléti szerv rendelkezésére álló meglévő átviteli kapacitás.
- Pro Mobil elérése a készenléti szervek saját hálózatából. Telepíthető a készenléti szervek saját hálózatában lévő gépekre.

Az üzembe helyezéssel egyidejűleg, a Heves megyei Rendőr-főkapitányság telepített DWS munkahelyeiről is elérhetővé vált az új járműkövető rendszert. A Pro-Mobil által jelentősen megnövekedett adatátviteli igényekhez igazodik a DWS munkahelyekhez rendelt átviteli utak sávszélessége is.

Az új járműkövető rendszer több adatot képes szolgáltatni, mint a korábbi, több térképművet használhatunk. A legújabb Pro- Mobil fejlesztés a legújabb térinformatikai

<sup>12</sup> TETRA Dispatcher Workstation (TETRA diszpécserállomás)

<sup>13</sup> High-Speed Downlink Packet Access (nagysebességű csomagletöltési hozzáférés)

szoftverek által nyújtott lehetőségek kihasználásával készült. Nagyobb adattartalommal rendelkező, így a több információt adó térképi adatbázis áll rendelkezésünkre.

Négy térképmű került leszállításra, melyekre a szolgáltató negyedévente tölt fel rész-frissítést.

- Simple: a régi rendszernél használt térképművel azonos tartalom (a három közül a legkevesebb adat, de leggyorsabb megjelenés)
- Vektor: nagy részletesség (fontosabb épület kontúrok), Magyarország és határon túli 50 km-es sáv
- Ortho: Magyarország teljes területére, légi-felvételek alapján készült orthofotók. Adatgazda: FÖMI (belterületen 50cm, külterületen 2 m pixelméret)
- Ortho-vektor: Magyarország teljes területére a vektor és az ortofotó kedvező tulajdonságait ötvöző térképmű POI adatbázis, és teljes országos címadatbázis áll rendelkezésre.

Lehetőség van a saját térképi rétegen saját objektumok felrajzolására (ikon, címke, négyszög, poligon, kör, vonal) Lehetőség van ugyanígy, meglévő saját térkép feltöltésére pl. KMB székhelyek stb.

A leggyorsabb működést a Szimpla térképmű használatával érhetjük el. Ezt és ennek a lokálisan is feltölthető változatát mobil eszközökön is lehet használni. A Vektor, Ortho és Ortho-Vektor térképeket az esetben használjuk, amennyiben több adatra van szükségünk.

A tájékozódást támogatja, hogy nagy nagyításban kiíródnak a térképen szereplő településnevek is. A keresési funkció is megújult, felgyorsult. Nem csak a települések, de a településrészek, Budapesten a kerületek is kereshetővé váltak. Az utólagos adatkinyerés is jelentősen felgyorsult.

A Helyszínvizsgálat perspektíván, körzetek meghatározására már nem csak kör, hanem négyszög, vonal, poligonon meghatározott szűréseket is lehetővé váltak. Szabályokat tudunk beállítani arra, hogy a meghatározott rádiókészülék körzetbe való belépésre és/vagy kilépésre riasztást kapjunk. Beállítható, hogy ezek a szabályok a hét mely napjain és milyen időpontok között lépjenek érvénybe. Így a szabályoknak megfelelő események megtörténte esetén dokumentáltan riasztás érkezik, a kezelőnek nem kell a követett járművet állandóan figyelnie.

A DWS munkaállomásról üzemeltetett Pro- Mobil alkalmazás a bevetés irányítás hatékony eszközévé válhat. Az EDR rádió által nyújtotta lehetőségeket kihasználva, a Pro-Mobil biztosítja annak lehetőségét, hogy a helyszínen lévő járőr előre meghatározott üzeneteket küldjön az irányítás részére, a helyszínen észlelt rendkívüli eseményről. A gyors észlelést hatásos intézkedés követheti, mivel a bevetés- vagy tevékenység irányító tiszt a rendelkezésre álló Pro-Mobil járőrkövető rendszerből nem csak a bejelentő helyét valamint az esemény fajtáját ismeri, hanem a rendelkezésre álló bevethető erővel is gazdálkodhat. Az ún. állapotüzenetek gombnyomásra beküldhetők a rendszerbe. A funkció használatára, valamennyi EDR rádió alkalmas, így nem csak a gépkocsik, de a gyalogos járőr is alkalmazhatja. A bevetés irányításhoz aktuális adatnyerést biztosít a fenti funkció. Így parancs kiadás ezen a módon is lehetséges.

A Pro-Mobil-ba beérkező információkat a rendszer visszakereshető módon tárolja, és megjeleníti a diszpécser számára. A felhasználói felületen lehetőség van szűrők és színezési szabályok definiálására, így akár az állapotüzenettel vezérelten tudjuk a felhasználói felületünkön megjelenő információtartalmat módosítani, ill. megfelelő módon színezni. Valamennyi a rendszerbe érkezett információ, tárolásra kerül, és elérhető. A Felhasználók számára egy évig online is biztosított a hozzáférést, ezentúl offline.

Útvonaladatok lekérdezése:

Útvonalvizsgálat: hívószám és időtartam alapján biztosított lekérdezés. Felhasználóbarát funkciók segítenek a dokumentáció készítésében pl. ügyészség részére, filmszerűen



lejátszható járműmozgás, naplók, grafikonok készíthetők

Helyszínvizsgálat: Több rádió, csoportok, vagy helyszín kijelölésével (térinformatikai lekérdezés) is lekérdezhetők adott időtartamra az adatbázisban lévő adatok. A rendszer tematikus térkép előállító funkciója, segít a járőrtevékenység tervezésében. Ki tudjuk mutatni segítségével, hogy mely településeken, mely helyszíneken, milyen gyakorisággal történt járőrtevékenység. Összekapcsolva ezt fertőzöttségi adatokkal a tervezés javítására ad lehetőséget.

## ÖSSZEGZÉS, KÖVETKEZTETÉSEK

A Heves Megyei Rendőr-főkapitányságon fejlesztett és alkalmazott, illetve az azt követő országosan, központilag rendszeresített helyzetismereti, térinformatikai megoldások az időben előre haladva és szinte egymásra épülve lehetővé tették és lehetővé teszik, hogy a készülékek földrajzi helyzete meghatározható legyen, az a rádióterminálok kijelzőjén, földrajzi koordinátákkal megjeleníthető legyen, ezzel párhuzamosan továbbítani lehet azokat egy munkahelyre, ahol megfelelő térinformatikai alkalmazás segítségével digitális térképen követhetjük a kiválasztott terminálokat. A követett rádióterminálokról a feladat jellegének megfelelő időközönként nyomvonal és egyéb, a bevetés jellegének megfelelő információkat kaphatunk. A jelenlegi megjeleníthető térképi információk, a dinamikus nyomvonal információk, és az egyéb leíró információk köre tovább bővíthető. Minden felhasználói körnek törekednie kell arra, hogy a rendszerben lévő lehetőségeket maximálisan kihasználja. Részletesen bemutattam az Pro-Mobil rendszer felépítését, elemeit és technikai adatait és szolgáltatásait azért, hogy láttassam a benne rejlő lehetőségeket, illetve azt hogy milyen szolgáltatások állnak még rendelkezésünkre ahhoz, hogy a bevetés-irányítás számára a döntéseit elősegítő és alátámasztó információt nyújtsunk.

## FELHASZNÁLT IRODALOM

- [1] Rendszerterv a Heves Megyei RFK Integrált Járműkövető és Tevékenységirányító mintarendszer kiépítéséhez – HM EI Rt. – Budapest, 1999
- [2] Automatikus Jármű és Rádióterminál-követő Rendszer (AVL) I. kötet, oktatási segédanyag - Pro-M ZRt.
- [3] Munk Sándor: Katonai Informatika II.; Katonai informatikai rendszerek, alkalmazások Egyetemi jegyzet; ZMNE, Budapest, 2006
- [4] Kimmo Heikkonen, Tero Pesonen, Tiina Saaristo: A TETRA rádió és ön
- [5] Az EDR, mint a készenléti szervek vezetésének hatékony eszköze, oktatási segédanyag Verzió: 1.0 - Pro-M ZRt.
- [6] Négyesi Imre: DIE VISION DER TRAGBAREN INFORMATIONS-TECHNOLOGIEGERÄTE (A viselhető számítástechnikai eszközök jövőképe) (Hadmérnök on-line, III. évfolyam (2008) 4. szám, 173-179. oldal, ISSN 1788-1919)
- [7] Dr. Négyesi Imre: TRAGBARE UND FELDINFORMATIK-GERÄTE I. (Tábori és hordozható informatikai eszközök I.) (Hadmérnök on-line, IV. évfolyam, (2009) 2. szám, 333-339. oldal, ISSN 1788-1919)
- [8] Dr. Négyesi Imre: TRAGBARE UND FELDINFORMATIK-GERÄTE II. (Tábori és hordozható informatikai eszközök II.) (Hadmérnök on-line, IV. évfolyam (2009) 3. szám, 355-362. oldal, ISSN 1788-1919)



**Bindis Bea Brigitta**  
brigittabindis@gmail.com

## **A PILÓTA NÉLKÜLI REPÜLŐGÉPEK (PNR) KOMMUNIKÁCIÓS RENDSZERE**

### **Absztrakt**

*Jelen cikk a Pilóta nélküli repülőgépek (PNR) kommunikációs rendszerével foglalkozik. Alkalmazásuk civil és katonai területen főként felderítő - és operatív egységként gyakori, békében és háborúban egyaránt. Manapság a katasztrófavédelem területén is igen elterjedtek, akár erdőtüzek, árvizek által veszélyeztetett területek monitorozása céljából. Szó esik majd az UAV-k rádiós hálózatról, amely rugalmas adatátviteli sebességgel működik.*

*This article is about the communication system of Unmanned Aerial Vehicles (UAV). These UAVs are usually used for civil but mainly for military purposes as a reconnaissance and operating units in peace and in war also. Nowadays it is common in disaster protection like in forest fires or in floods for monitoring the endangered areas. This item is also represents the UAV radio network, which works with flexible transmission data rate*

**Kulcsszavak (key words):** *valós idejű kommunikáció, légierő ~ real time communication, air force (defence)*

### **BEVEZETÉS**

Archibald Low angol fizikus, feltaláló, mérnök alkotta meg az első UAV-t 1916-ban, amely „Aerial Target” néven vonult be a történelembe. A katonai repülés területén a pilóta nélküli repülő eszközök az 1960-as évektől kezdve terjedtek el.

Amennyiben alkalmazásuk katonai célból történik, úgy harci robotnak minősülnek. Olyan feladatok ellátására használják elsősorban melyek túl veszélyesek és emberi élet kockáztatásával járna az elvégzésük - itt fontos megemlíteni, hogy az irányítás természetesen biztonságos távolságból történik. Abban az esetben is hasznos, ha hosszú ideig tartó bevetésről van szó, melyekhez több pilóta igénybevitelére lenne szükség.

Korlátot jelent azonban, hogy a repülés biztonsága a földi irányítópont és a repülőgép közötti kapcsolat folyamatosságától függ. Irányításuk történhet előre meghatározott útvonalon is, ezen útvonalak kidolgozása hagyományos térképen történik.

A bevetés hosszának akár korlátlan növelése érdekében a jövőben alkalmassá teszik ezeket az eszközöket légi utántöltésre is. Alkalmazásuk gazdaságos olyan szempontból, ha egy feladat annyira kevés eszközt igényel, hogy többszöröse lenne a hasznos tehernek a pilóta és a kezelőszemélyzet. A katonai célú feladatai között szerepet kap a rádiótechnikai átjátszás illetve rádióelektronikai zavarás. Léteznek kísérleti repülőgépek is, melyek a folyamatos korszerűsítést szolgálják.

## 1. AZ UAV-K ADATÁTVITELI RENDSZERE

A repülőeszközök a korábbi analóg adatátviteli rendszer helyett, mára már digitális rendszerrel működnek. A fedélzeti érzékelő eszközök közé tartozik a nappali- és infravörös-, valamint lehetőség szerint hő kamera is. Ezek megfelelő működéséhez azonban elengedhetetlen egy nagy sebességű adatátviteli rendszer, hogy "real-time" eseményközvetítés jöjjön létre a kezelő irányába. A felvétel minősége sem elhanyagolható tényező, melyet ugyancsak az átviteli rendszer sebessége befolyásol.

A rádiócsatornán történő adattovábbítás könnyen bemérhető és zavarható. Zavarvédett adatátvitelhez az adatkapcsolat el kell, hogy érje legalább az 1-10 Mbit/s sebességet. Képesek pillanatképek továbbítására is, valamint egyes típusok éjszaka is alkalmazhatóak.

Hatótávolságuk átlagosan 10 km körülire tehető. Fejlesztésük során mindig hangsúlyos szempont a nagy távolságú megbízható adatkapcsolat megléte, valamint a navigálás pontossága. Kis tömegű, illetve méretű eszközök használata szükséges, mivel a fedélzeten alkalmazott eszközök mennyisége limitált, össztömegükből adódóan.



1. sz. ábra: UAV adatátviteli rendszere és hasznos terhe [5]

## 2. AZ UAV-K IRÁNYÍTÁSA

A hajtómotor teljesítménye rádiócsatornán keresztül szabályozott a földi irányító pontról. A fedélzeti eszközök a kezelőnek szintén rádiócsatornán közlik a repülés sebességét, a magasságot és a pozíciót, a GPS koordinátákat, valamint a légtér képét, mely a repülőgép előtt van. A korszerű eszközök fedélzetén a GPS-en kívül interciális vagyis tehetetlenségi navigációs rendszer található, mely az autonóm irányítást teszi lehetővé. Jelen van még a TERCOM rendszer (Terrain Contour Matching – Terepkontúr egyeztetés).

Működését tekintve tulajdonképpen olyan, mintha a kezelő a repülőgép fedélzetén ülne. Amennyiben fedélzeti számítógép támogatásával történik az UAV irányítása, úgy inkább repülésirányító feladattal kell szembenézni, mintsem egy pilótáéval, tehát az irányító szerep nem szűnik meg, csak átalakul. Megkülönböztetjük az eszköz legyező, bólintó és orsózó mozgását.

Számos olyan tényező figyelembe vétele fontos a rádiókapcsolat létesítése során (a domborzat hatása, légköri hatások, a föld, a légkör törésmutatójának változása melyek igen számottevő mértékben befolyásolják a szakaszcillapítást. Szakaszcillapításnak azt a

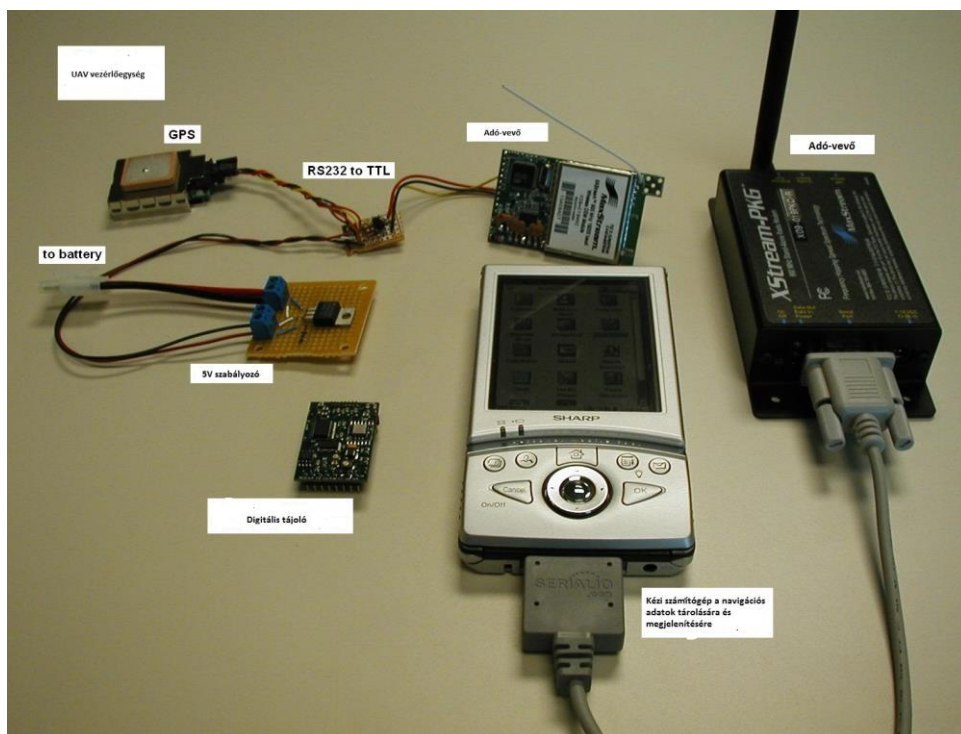
csillapítást nevezzük, amely csillapodást elszenved a jel a vevőantenna koaxcsatlakozójáig az adóantenna koaxcsatlakozójától.

Távírányítási módban a földön elhelyezett irányítóállomástól kapja a parancsjelet az UAV. Problémát jelent azonban sajnos, hogy egy UAV nem képes önállóan felvenni újra a kapcsolatot az irányítóval, ha az megszakadt. Nagy előrelépés lenne, ha a mért és tárolt adatok alapján kommunikáció kiesés alkalmával az eszköz képes lenne feladata folytatására a kapcsolat helyreállításáig.

### 3. ÚTVONALTERVEZÉS

Az útvonaltervezést több tényező befolyásolja. A feladat típusa elsődleges szempont, valamint számolni kell az időjárási viszonytagságokkal, az útvonal hosszával, és az időtartammal is. Az UAV technikai lehetőségét tekintve a számítógép minden megadott koordináta-hoz rendel magassági adatokat. Akadályok figyelembe vétele is fontos, ugyanis ilyen esetben meg kell adni az akadály átrepüléséhez szükséges minimális magasságot. A technikai előkészítést követően az indítás következik.

A repülés során eltérő módon irányíthatják az eszközt autonóm módon, illetve távirányítással, illetve a kombinált irányítás során programozzák be az útvonalat előre. A repülési pályaadatok rögzítése nem csak számítógéppel történhet. Itt azonban hátránként tűnik fel az, hogy a repülő indítása után útvonala nem változtatható. A GPS által meghatározott koordináták alapján és a repülési útvonaladatokat alapján a repülő számítógépe úgynevezett különbségjelet hoz létre, mely a repülő hajtóművét és kormány szerveit működtető elektromos jelekké alakítanak át.



2. sz. ábra: UAV vezérlőegység [6]

### 4. JÖVŐBENI ELKÉPZELÉSEK, FEJLESZTÉSEK

Fejlesztésük üteme olyan gyors, hogy nehéz egyes típusok és jellemzőik között eligazodni és nem utolsó sorban lépést tartani az újításokkal.

A Queensland University of Technology munkatársai a zöld Falcon programon dolgoznak, melynek célja egy olyan repülőeszköz kifejlesztése, amely napenergiával működik.

A Lasermotiv amerikai vállalat olyan módszer kifejlesztésén dolgozik, hogy az UAV-k a levegőben is képesek legyenek tankolni. A technika neve Laser Power Beam, melyben egy koncentrált lézersugár fénnyel tartósan a kisgéphez integrált napelemre irányul. Amikor energiáját elhasználta, visszatér automatikusan arra a helyre mely a lézersugár által megvilágított. Kísérletük során egy UAV 13 órán keresztül tartózkodott a levegőben, a robot tömege pedig mindösszesen 1 kg! .

A NASA is igen nagy összegű fejlesztéseket valósít meg, a Dryden Kutatóközpontban Kaliforniában található a Global Hawk óriásméretű repülő, melyet katonai célokra alkalmaztak, azonban felhasználási területe ennél jóval szélesebb, valamint repülési adatai sem az utolsók. Képes 30 órát a levegőben tölteni, akár 20 km-es magasságban.

Az USA a 2010-es évben 3,8 milliárd dollárt irányzott elő a PNR-ek fejlesztésére.

Az eszköz népszerűségét mutatja, hogy bevetésük száma évről évre növekszik és az USA légierijénél már az UAV fegyverrendszerére képezik ki a legtöbb kezelőt.

A jövőbeni elképzelések között a miniaturizálás is fontos szerepet kap.

### ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Az eszköz szerepe mára felértékelődött, ugyanis feladatköre egyre szélesedik, népszerűsége mindinkább növekszik. Magyarország számára az EU által az UAV-k fejlesztésére fordított összeg 0,1%-a került az elmúlt évben. A repülőgép irányítása leegyszerűsödhet a számítógép alkalmazásával, mert így elkerülhetővé válik a folyamatos összeköttetés hiánya.

Fejlesztésére nagy igény mutatkozik, egyre bővülő területen kísérleteznek felhasználásával, katonai és civil részről egyaránt. A fejlődés elsősorban a Chip technológia folyamatos újításának területén elért eredményeknek köszönhető. A kutatások összekapcsolódtak a térinformatikával, számítástechnikával.

Irányításuk GPS koordináták által lehetséges. Emberi felügyelettel üzemeltetik a repülőeszközöket, beavatkozásra, egy erre a célra kialakított rádiócsatornán lehetséges.

A terrorelhárítás területén is nő szerepük, földi célpontok megsemmisítésére is elterjedt használatuk. Mivel az USA-ban már rutinszerűen használják őket, a katonák lelkesedését az eddigi tapasztalatok táplálják.

### FELHASZNÁLT IRODALOM

- [1] Magyar UAV portál, <http://www.uav.hu>
- [2] HTKA – Haditechnikai Kerekasztal, <http://htka.hu/tag/uav/>
- [3] Art of War, <http://www.haborumuveszete.hu>
- [4] The UAV, <http://www.theuav.com/>
- [5] NASA Small Business Innovation Research, <http://sbir.nasa.gov/SBIR/successes/ss/5-056text.html>
- [6] Control Reset, [http://www.controlreset.com/projects/rc\\_uav/navunit/navunit.shtml](http://www.controlreset.com/projects/rc_uav/navunit/navunit.shtml)

**Serege Gábor**  
serege.gabor@zmne.hu

## A SZEMÉLYI INFORMATIKAI ESZKÖZÖK ÉS AZ IPV6

### Absztrakt

*Az Internet alapvető szabványa az internetprotokoll, amelynek feladata a csatlakoztatott hálózati eszközök egységes kommunikációjának a biztosítása. A legszélesebb körben alkalmazott négyes verzió (IPv4) hiányosságainak kiküszöbölése napjaink égető kérdése. A cikk egyrészt röviden összefoglalja a problémákra megoldást jelentő, azonban a mai napig az IPv4 egyeduralmát megtörni nem tudó hatos verzió (IPv6) legfőbb újonságait, másrészt bemutatja a hordozható és viselhető személyi informatikai eszközöket. A publikáció végére választ kaphatunk arra is, hogy az említett eszközök miként viszonyulnak az IPv6 használatához.*

*This article is about the IPv6 problems.*

**Kulcsszavak (key words):** internetprotokoll; IPv4, IPv6, személyi számítógép ~ internetprotocol, IPv4, IPv6, personal computer

### BEVEZETÉS

Az információs társadalom legfontosabb építőköve a XX. század utolsó évtizedeiben megjelenő információ-technológia, amelyet a nagy számítási kapacitással rendelkező személyi számítógépek egyre szélesebb körökben való elterjedése alapozott meg. [1] Az egyéni felhasználók számára is könnyen elérhető, egyre olcsóbbá váló informatikai eszközök csak a sikertörténet első, bevezető lépésének tekinthető, hiszen a továbbfejlődés kulcsát ezek világméretű hálózatba való kapcsolása jelentette, és jelenti a mai napig.

Az információ előállítása önmagában nem elégséges feltétele annak, hogy az értékke váljon, mivel annak a kívánt helyen és időben meg is kell jelennie. Az információ adott időn belüli szállítását az állomásokat összekötő kommunikációs csatornák végzik. A Földet, pontosabban az ember által meghódított geo-, és kozmoszférákat<sup>14</sup> összekapcsoló kommunikációs hálózat az Internet, amelyhez bárki szabadon csatlakozhat. A csatlakozás egyik legfontosabb alapkövetelménye az adatkommunikációt biztosító protokollkészletek szabványos alkalmazása.

Az informatikai hálózatokban szállított adatsomagok összeállításáért és vezérléséért a „kezdetektől” meglévő Internet Protokoll négyes (IPv4) és az ezredforduló első évtizedében megszülető hatos (IPv6) változatok a felelősek. Fontos kiemelni, hogy az IPv4 még mindig az a protokollkészlet, amelyet az Amerikai Egyesült Államok Védelmi Minisztériumának kutatásért felelős részlege kezdett kifejleszteni 1974-ben. Megalkotásának idejében a kitűzött cél a védelmi és oktatási intézményeket összekötő, lényegében néhány tucat számítógépet magába foglaló informatikai hálózat létrehozása volt. Ebből adódóan a tervezéskor még nem létező problémák napjainkra váltak égető fontosságuvá, ami azt bizonyítja, hogy az IPv4

<sup>14</sup> 2010 februárjában elsőként Timothy Creamer a Nemzetközi Űrállomás fedélzeti mérnöke létesített Internet kapcsolatot az úgynevezett Crew Support Lan hálózat segítségével.

felett vitathatatlanul eljárt az idő és megérett a lecserélésre. A nemzetek között szétszórt szűkös IPv4 címtartomány fejlődést visszafogó hatása elsőként a népes távol-keleti országokat érintette, ahol alapvető követelményként jelentkezett a kiosztható IP címek minél rövidebb időn belüli kibővítése. Az IPv6 egyéb újdonságai mellett ezt könnyen biztosítja, így ezeken a területeken már megtörtént az átállás. A világ többi részén, azonban továbbra is maradt az IPv4 egyeduralkodása, igaz a váltás, illetve a továbblépés szükségessége egyre jobban érzékelhető.

Az elmúlt 40 év során az Internet alapját jelentő IPv4 viszonylag csekély mértékű változása mellett a számítógépek teljesítménye milliós nagyságrenddel növekedett, a hardverelemek mérete pedig szinte minimálisra zsugorodott. Végigtekintve a fejlődést jól látható, hogy a teremméretűeket az asztali jóval kisebb, de még helyez kötött típus követte, amelyek egyeduralkodása napjainkban a hordozható, illetve a viselhető eszközök megjelenésével látszik véget érni.

A cikk megírásának kettős célja volt. Egyrészt fel kívánom hívni az olvasó figyelmét az IPv6 leglényegesebb újdonságaira. Másrészt a személyi számítógépek kategóriájából szeretném kiemelni az általános használatú hordozható- és a katonai alkalmazású viselhető informatikai eszközök jellemzőit, felhasználási területeit, azzal a kiegészítéssel, hogy közben vizsgálom azok IPv6 képességeit is. Meglátásom szerint az említett kategóriák IPv6 képességeinek vizsgálata napjaink egyik érdekes kérdése, hiszen az IPv6 elterjedtségének egyelőre csekély mértéke ellenére lehet, hogy a gyártók már alapkövetelményként kezelik annak támogatását.

### 1. AZ IPV6 KIALAKULÁSA ÉS LEGFONTOSABB ÚJDONSÁGAI

Az Internet az a kommunikációs csatorna, amely legszélesebb körben összeköti a csatlakoztatott eszközöket, és az eszközök „mögött” álló felhasználókat. Biztosítja az alapvető információcserét, és lehetőséget nyújt a legkülönbözőbb hálózati szolgáltatások elérésére. A csatlakozást megalapozó hardveres és szoftveres követelményeken túl, minden egyes állomásnak rendelkezni kell egy, a készülék fizikai címéhez rendelt úgynevezett logikai vagy más néven IP címmel is. Egy adott alhálózatot tekintve az egyedi azonosító használata elhagyhatatlan alapfeltétele a működőképességnek, ugyanis csak ezek által különböztethetőek meg egyértelműen a csatlakoztatott állomások.

Napjainkban a TCP/IP protokollcsaládban két IP generáció látja el ezt a feladatot. Az egyik az Internet korával egyidős, több mint 30 éve használt IPv4, és a következő generációként számon tartott IPv6. Minden kétséget kizáróan az IPv4 hosszú éveken keresztül bizonyította az alapkoncepció hibátlan voltát, azonban az információs társadalom rohamléptékű fejlődését már nem képes teljes mértékben támogatni, és így elérte az általa kiaknázható lehetőségek felső határát. Az alap protokollkészlet a különböző módosítások és pótfunkciók beépítése ellenére is már számottevő akadályokat képez a fellépő igények megvalósíthatósága útján.

Az infokommunikációs konvergencia<sup>15</sup> folyamatoként egyértelmű igények léptek fel a valósidejű IP hálózatok hálózati architektúrájának kialakításával szemben, valamint az olyan főbb szempontok kerültek reflektorfénybe, mint a megnövekedett sávszélesség, a szolgáltatás minőség valamint a mobil felhasználók részére nyújtott hálózati hozzáférés. A reformtörekvéseket sürgették az információtechnológiai eszközök tömegtermelése és

---

<sup>15</sup> A hagyományos értelemben vett kommunikációs szolgáltatások, illetve az adatközlő hálózatok által nyújtott szolgáltatások és ezek technikai határainak az összemosódása.



milliárdos számban való értékesítése is, amelyekre a hálózat szempontjából úgy kell tekinteni, mint hálózati erőforrást igénylő „hostok”<sup>16</sup> óriási halmaza.

Az IPv4 leendő utódjának a keresésékor a következő „Milyen legyen?” kérdések megválaszolása jelentette a kiindulási alapot:

- biztosítson „mindenki” számára elegendő IP címet<sup>17</sup>;
- oldja meg az óriásira duzzadt forgalomirányító táblák méretének csökkentését;
- gyorsítsa meg a protokollok feldolgozhatóságát;
- tartalmazzon beépített biztonsági megoldásokat;
- kiemelten támogassa a mobil hosztok címmenedzselését;
- legyen kellőképp rugalmas és bővíthető;
- legyen megfelelően strukturálható;
- működjön együtt a meglévő IPv4 hálózatokkal.

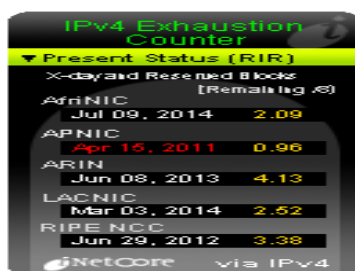
A problémák megoldására. 1992-ben hét különböző javaslat versengett, amelyek „összefésülése” eredményeként három évvel később megszületett az IPv6 végleges, az Internet Engineering Steering Group által is elfogadott (RFC 1883) verziója. [2][3]

Az IPv6 specifikációjában létrejött konszenzust egy olyan teszhálózatnak a kiépítése követetett, amely alkalmas volt a gyakorlati tapasztalatok megszerzésére. A projekt a világszerte önkéntes alapon csatlakozók<sup>18</sup> által mintegy ötven ország részvételével, és 1000 különböző helyszín sikeres kapcsolódásával 2008-ban, az utolsó fázis befejezésével zárult le.

A következőkben az IPv6 mélyre nyúló technikai részletezése helyett, a leglényegesebb újdonságait kívánom röviden összefoglalni.

### 1.1. IP címtér kiterjesztése

Az IPv4 által használt 32 bites címzés mintegy 4 milliárd egyedi logikai cím használatát biztosítja. Azok a vállalatok, amelyek az Internet elterjedésének kezdetén igényeltek címtartományokat, azok gyakran teljes A osztályokat<sup>19</sup> kaptak felhasználásra. Ez a gyakorlat abszolút nem valósította meg azt a napjainkban elképzelhetetlen szabályt, miszerint figyelembe kell venni a vállalat méretét és tilos pazarlóan bánni a szűkös készletekkel<sup>20</sup>.



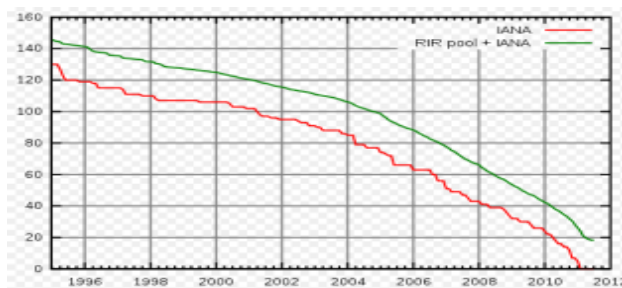
<sup>16</sup> Host: informatikai hálózatra csatlakoztatott berendezés. [4]

<sup>17</sup> A lényegesen nagyobb felhasználótáborral rendelkező távol-kelet az osztható IPv4 címek töredékével rendelkezett csak.

<sup>18</sup> Magyarország Budapest, Szekszárd, Szeged és Miskolc városok egyetemi csatlakoztatásával járult hozzá az önkéntes hálózat kiépítésében.

<sup>19</sup> Az „A” osztály használata esetén csak 8 bit áll rendelkezésre a hálózat azonosítására, amíg a fennmaradó 16 bit az egyéni állomások egyedi címzésére használható ( $2^{24}$ -2 host IP). Ez a gyakorlatban óriási címpazarlást jelent, ha indokolatlanul kisebb szervezetek kapnak ilyen.

<sup>20</sup> A problémát felismerve több millió IP címet juttattak vissza. Például: az USA Védelmi Minisztériuma, egyes amerikai egyetemek, és óriásvállalatok [5]



1. sz. ábra: IPv4 címek kimerülése [6][7]

A hálózati kapcsolatot igénylő eszközök terjedésének ütemét figyelembe véve előreláthatólag 2012 első felére végleg el fog fogyni az összes szabad osztható IPv4 cím. Az IT társadalom „felébresztése” érdekében több hazai és nemzetközi weboldalon találkozhatunk olyan vészharangként funkcionáló visszaszámlálókkal, mint az 1. ábrán is látható.

Véleményem szerint ennek pontos időpontja továbbra sem jósolható meg, hiszen nap, mint nap születnek olyan eljárások, amelyek még mindig ki tudják tolni az elfogyás végleges időpontját<sup>21</sup>.

Az IPv6 128 bites architektúrája  $3,4 \times 10^{38}$  egyedi IP címet jelent, amely egyrészt alkalmas a Föld összes lakójának fejenként több mint egy milliárd egyedi cím kiosztására, másrészt lehetőséget nyújt a címtér hierarchikus felosztására.

## 1.2. Beépített biztonsági elemek

Az IPv4 tervezésekor nem volt elvárás a biztonsági elemek beépítése, ezért az adatátvitel titkosításának kezelése áthárult a végponton futó alkalmazásokra. Példaként említhető az elektronikus levelezés, amely esetében az email kliens feladata a felhasználó által választott biztonsági szint megvalósítása. Általánosan kijelenthető, hogy ha az alkalmazás saját maga nem használ kriptográfiai eljárásokat, akkor az elküldött információ nyíltan „utazik” a címzett irányába<sup>22</sup>.

Az IPv6 tervezésekor egyik fő szempont volt az IPSec támogatása, amely három alapvető biztonsági szolgáltatást kínál:

- csak hitelesítés;
- kombinált hitelesítés és titkosítás;
- kulcskezelés.

Ezek a biztonság eljárások a hálózati rétegben találhatók, és fontos kiemelni, hogy használatuk nem zárja ki az alsóbb, illetve magasabb szinteken implementált biztonsági megoldások további alkalmazását sem.

## 1.3. Rugalmas keretszerkezet és gyorsabb hálózati útvonalválasztás

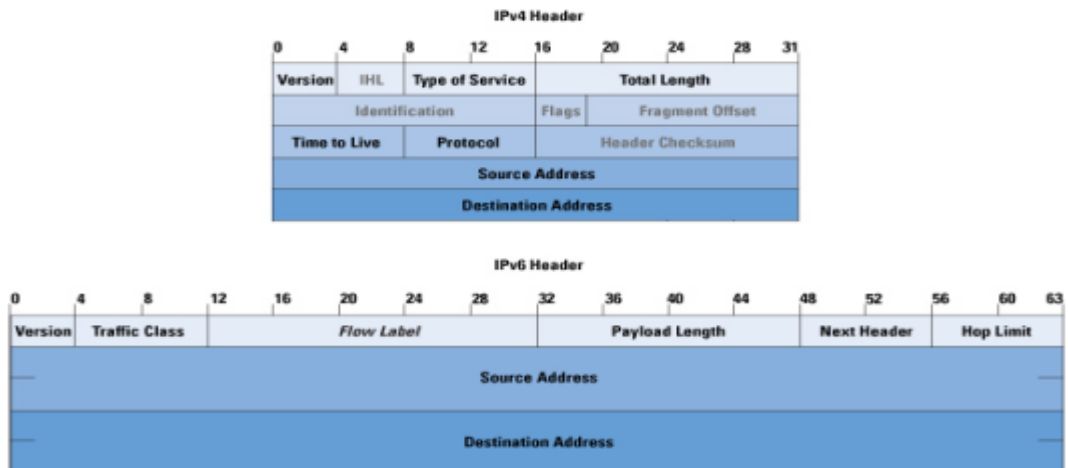
Az IPv4 architektúrában használt csomagok kezelése a rugalmatlan, kötött felépítésből adódóan gyakran okozhatja a forgalomirányító táblák hatalmas méretre való duzzadását. Ennek következményeként csak a megnövelt teljesítményű aktív eszközökkel lehetséges az IP csomagok elvárható időn belüli feldolgozása.

<sup>21</sup> hálózati címfordítás (NAT boks) és magánhálózati címzés használata, weboldalak név szerinti virtuális oldalakra való kihelyezése,

<sup>22</sup> A „man-in-the-middle”- típusú támadások esetén az elfogott csomagok minden nehézség nélkül olvashatók.

A két verzió IP keretképzését a 2. ábra szemlélteti, azokat összehasonlítva megállapítható, hogy egyes fejrészek maradtak, egyesek eltűntek, illetve születtek újjak és a fejléc mérete is megváltozott. Az IPv4 által alkalmazott tizennégy kötelező mező száma lecsökkent nyolc állandóra és az utána következő egy opcionálisan választhatóra.

Az opcionális mező rugalmas használatával csökkenthető az irányítótáblák mérete, illetve a működtetéshez szükséges hardverteljesítmény is.



2. sz. ábra: IPv4 és IPv6 fejlécek összehasonlítása [8]

#### 1.4. Mobilitás támogatása

Az elsődleges internetszolgáltató lefedettsége területét elhagyó egyedi IP címmel rendelkező mobil informatikai eszközök támogatása az IPv4 esetében csak számos technológiai hiányosság és inkompatibilitási probléma elhárítása után valósulhat meg. Ezzel szemben az IPv6 már magában hordozza az eszközök csatlakoztatásához szükséges alapfeltételeket, és képes a „mobil” eszközök számára transzparens hálózati környezetet biztosítani. A mobil IPv6 (MIPv6) olyan beépített funkcióinak az alkalmazása, mint a szomszéd felismerést szolgáló protokoll és az automatikus hálózati cím konfiguráció, lehetőséget nyújt az IPv4 esetén nélkülözhetetlen speciális routerek elhagyására.[9]

Összefoglalva megállapítható, hogy az IPv6 számos olyan beépített szolgáltatással rendelkezik, amelyek együttesen megoldást adnak az IPv4 hiányosságaira, illetve távlati perspektívát jelenthet az Internet jövőbeni üzemeltetésében.

A számos előny ellenére azonban teljes körű rendszerbe állítása csak azon távol-keleti országokban ment végbe, ahol az IPv6 bevezetése jelentette az egyetlen lehetőséget a piaci igények kiszolgálására.

A címtér kibővítése és a hálózati kapcsolatot igénylő mobil eszközök kiemelt támogatása joggal készíthet minket annak a kérdésnek a megfogalmazásához, hogy miként jelenik meg az IPv6 támogatása a modern hordozható és viselhető informatikai berendezésekben.

## 2. HORDOZHATÓ ÉS VISELHETŐ INFORMATIKAI ESZKÖZÖK

A harmadik fejezet első részében bemutatom a személyi informatikai eszközök kategóriájába sorolható hordozható informatikai eszközök egy lehetséges csoportosítását, összegyűjtöm a legjellemzőbb tulajdonságokat, illetve vizsgálom azok IPv6 képességeit. A

fejezet második felében keresem a viselhető informatikai eszközök behatárolásához szükséges ismérveket, és betekintést adok egy katonai alkalmazásra kifejlesztett rendszerről.

Az elmúlt negyven év sikere jól tükröződik az egyéni felhasználóknak értékesített számítógépek eladási mennyiségében, ami szám szerint 1981-ben 2,2 millió, a rákövetkező egy évre 5 millió, a 90'-es évek elejére pedig már több, mint 65 millió volt. [10] Jelenleg a Föld teljes lakosságát tekintve 4,5 számítógép jut 100 emberre.

A legszélesebb körben elterjedt számítógépek, a fejlettségi szint szerinti besorolás alapján a negyedik generációba tartoznak. A generáció alapja a méretek számottevő csökkentését biztosító VLSI technológiára támaszkodik, továbbá a fejlesztésnél a következő trendek érvényesültek:

- a méretek csökkentése;
- az informatikai eszközök univerzális alkalmazása;
- a minél egyszerű kezelőfelület biztosítása;
- a számítógép-hálózatokhoz való csatlakozás minél hangsúlyosabb támogatása.

A méretek számottevő minimalizálása eredményeként alakultak ki a személyi informatikai eszközök főbb típusai:

- asztali eszközök;
- szállítható eszközök;
- hordozható eszközök;
- viselhető eszközök.

Az utóbbi évek kereskedelmi eredményeit megvizsgálva megállapítható, hogy az első két kategória visszaesésével fordított arányban növekedett a hordozható és viselhető informatikai eszközök térnyerése.[11] A fokozódó népszerűségükből adódóan publikációm további részében ezeket kívánom bemutatni.

### 2.1. Hordozható informatikai eszközök

Az alfejezetben ismertetem a hordozható informatikai eszközök általános kategorizálását, illetve kitérek ezen eszközök IPv6 képességeire is.

A hordozható informatikai eszközök értelmezésénél a Dr. Munk Sándor által megfogalmazott leírásból indultam ki:

„A hordozható (portable) számítógép a mikroszámítógép kategóriából elsőként vált ki, kiterjesztve az alkalmazás lehetőségét az irodák határain kívülre, változó helyszíneken lehetővé téve a megszokott szolgáltatások igénybevételét, az összegyűjtött adatok felhasználását”[12 pp.23]

Az informatikai eszközök használata, pontosabban az általuk biztosított szolgáltatások a mindennapi életünk szinte nélkülözhetetlen részévé vált, amelyek elérése helytől és időponttól függetlenül egyre fontosabb.

Felosztásuk alapján szolgáló de jure, illetve de facto szabványok csak egyes esetekben alakultak ki, hiszen dinamikus fejlesztésük során a legfontosabb szempont mindig fellépő legnépszerűbb alkalmazási módok és programok minél gyorsabb támogatása volt. A viszonylag nagy teljesítmény melletti kis tömeg és alacsony energiafogyasztás mind a hordozható informatikai eszközök közös jellemvonása.

Csoportosításuk a képzeletbeli határvonalak gyakori összemosódása miatt nehézkes. A leggyakoribb felosztás szerint az alábbi „változatok” különíthetők el:

- laptop;
- notebook;

- netbook;
- táblaszámítógép;
- kézi számítógép.

A *laptop* és *notebook* elnevezéseket napjainkban már egymás szinonimájaként használjuk. A legnagyobb különbség a kettő közötti méretbeli eltérés, azonban érdemes megjegyezni, hogy a kereskedelmi forgalomban a laptop igazi ritkaságnak számít. Ezek az eszközök az asztali változatokhoz képest lényegében csak a kompakt méretekből, illetve a hordozhatóságot elősegítő kivitelezésben különböznek, ugyanis a futtatott operációs rendszerek, illetve felhasználói programok általánosságban megegyeznek, vagy nagy hasonlóságot mutatnak. Áttekintve a piacon található termékek széles skáláját megállapítható, hogy ugyanazokat a Microsoft, Linux és Macintosh rendszereket futtatják, mint asztali társaik. Természetesen ezeknél az eszközöknél a hálózati energiaellátás nélküli üzemmód támogatása kiemelt figyelmet kapott. Ennek biztosítása egyrészt a legnagyobb energiaszükségletű hardverelemek optimalizálásával, másrészt az operációs rendszerekbe beépített energiagazdálkodási profilok használatával történik.

Az IPv6 támogatottsága elsősorban a telepített rendszerprogramtól függ. Az IPv6 specifikációt tartalmazó RFC kidolgozásával párhuzamosan az olyan szoftvergyártó óriások, mint például a Microsoft és az Apple is megkezdtek saját kutatásaikat az új protokollkészlet implementálásához. A Microsoft már 1998-ban elindította ilyen irányú fejlesztéseit, így a Windows 2000-es rendszer már lehetővé tette az IPv6 tesztelését. A teljes körű támogatás azonban csak a Vista megjelenésétől valósult meg. Az OS X operációs rendszerek 2004-től támogatják az IPv6 használatát. A Linux disztribúciók esetében a 2.6.x kernelváltozatok rendelkeznek IPv6 támogatással, igaz számos kiadás alap installációja nem telepíti a szükséges kiegészítéseket.[13]

A *netbook* olyan kicsi, általában 9-10 inch képernyő átmérővel rendelkező számítógép, amely teljesítménye az *internet használatára van optimalizálva*. A futtatott operációs rendszerek lehetnek „hagyományosak”, vagy célirányosan csökkentett erőforrás igényűek. Az alább felsorolt legnépszerűbb netbook operációs rendszerek teljes támogatással, alapértelmezett telepítés mellett is már alkalmasak az IPv6 alapon nyugvó hálózatok használatára:

- Windows 7;
- Ubuntu;
- Joli OS;
- OS X;
- Linux Mint.[14]

A *táblaszámítógép* a hordozható informatikai eszközök speciális változata. Nem rendelkezik hagyományos billentyűzettel, ezért a legfőbb különbséget a beviteli interfészként használt érintőképernyő jelenti. A legújabb változatok képesek IPv6 alapú csatlakozások létesítésére.

A *kézi számítógépek* kategóriáját további alcsoportok alkotják (palmtop, PDA, okostelefon), amelyek közös tulajdonsága a kézben elférő méret. Olyan IPv6 képes speciális operációs rendszereket futtatnak, mint például: Symbian, Android, Blackberry, iOS, Windows Mobile.

Összegezve megállapítható, hogy a hordozható számítógépek csoportosítása az összegyűjtött jellemzők ellenére sem mindig egyértelmű. Véleményem szerint a besorolás elvégzése az egyes kategóriák határainak definiálása helyett inkább az adott csoportra legjellemzőbb tulajdonságok összegyűjtése és számbavétele alapján lehetséges. A hordozható számítógépek „változatainak” jellemzéséből egyértelműen kitűnik, hogy ezek az

eszközök a telepített felhasználói programok futtatása mellett kiemelt figyelmet fordítanak a világháló elérésére. Az IPv6 csekély mértékű elterjedése ellenére kimondható, hogy a gyártók számolnak vele, ezért ezek a berendezések már mind hardver mind pedig szoftver szinten támogatják annak használatát.

### 2.2. Viselhető informatikai eszközök

Az információs társadalom egyik jellemző folyamata az ember és gép kapcsolatának folyamatos mélyülése. Ez a kapcsolat napjainkban is tovább erősödik a bárhol „elővehető” hordozható informatikai berendezések robbanásszerű elterjedésével.

A méretek csökkenését és a hordozhatóság egyre tökéletesebbé válását továbbgondolva előreláthatólag a következő lépcsőfok a viselhető eszközök elterjedése lesz. Az ilyen jellegű kutatások erősödését mutatja, hogy 2005-ben az ISWC<sup>23</sup> témacsoportjai közé bekerült a viselhető eszköz technológia.[15]

A viselhető informatikai eszközök meghatározásánál a Steve Mann által megfogalmazott jellemzőkkel értek egyet, amelyek alapján:

- olyan informatikai eszköz, amelyet az ember testére, ruházatára rögzítve lehet viselni;
- folyamatosan hozzáférhető;
- közvetlen kapcsolat mind az utasítások bevitele, mind az eszköz által adott „válaszok” esetén;
- teljes értékű számítógép, amely specializálódott az adott tevékenység támogatására.[16]

Az emberre telepített eszközök célja mindig valamilyen hiányosság pótlása, vagy valamiféle plusz képesség megszerzése volt.

A született képességek kiterjesztésének lehetősége felkeltette a katonai vezetők érdeklődését is, ezért a viselhető informatikai eszközök harctéri alkalmazásának szándéka számos ország fejlesztési stratégiájában jelen van. A legkiterjedtebb kutatási projekttel, illetve a legtöbb harctéri tapasztalattal az Amerikai Egyesült Államok rendelkezik.

Az I. Öböl-háborúban szerzett tapasztalatok alapján elsőként az Amerikai Egyesült Államok hadseregében jelentkezett a digitális egyéni képességnövelő felszerelésrendszerek használatának az igénye. A hálózat alapú hadviselésben rejlő lehetőségek kiterjesztése érdekében 1994-ben kezdődtek meg azok a kutatások, amelyek a kisebb alegységek, illetve az egyes katonák rendszerbe integrálását kívánták megoldani. Az 1999-ben megjelenő legelső felszerelésrendszer a Land Warrior nevet kapta, amely azóta mind a felépítésben, mind az elnevezésében megváltozott. A fejlettségi szint alapján három kategória alakult ki: a digitális katona, a hálózatos katona és a jövő katonája.[17]

A Land Warrior általános rendszerelemei:

- Fegyver alrendszer
- Harctéri ruházat és védőmellény alrendszer
- Integrált sisak alrendszer
- Vezérlőegység
- Központi számítógép
- Energiaforrás alrendszer
- Rádió alrendszer

---

<sup>23</sup> International Semantic Web Conference

- Navigációs alrendszer [18]

A központi számítógép alrendszer esetében szükséges megjegyezni, hogy a felszerelések Windows 2000 és Linux alapú operációsrendszerrel kerültek rendszerezítésre. A Windows 2000 operációs rendszer nem támogatja az IPv6 kommunikációt.

Éles harci körülmények közötti használatára 2006-ban került sor, amikor az iraki műveletekben 230 darab Land Warrior Stryker készletet vetettek be. A tapasztalatok közül két fontos következtetés a legszembetűnőbb:

- az alapkoncepció az egyéni képességnövelő felszerelésrendszerek alkalmazására előremutató;
- a felszerelésrendszer számos eleme fölösleges és a plusz súlyból adódóan csak a katona nehezkesebb mozgását eredményezi.

A projekt 2008-as befagyasztása ellenére 2009-ben egy komplett harcoló egységnél<sup>24</sup> került rendszerezítésre, amely azt bizonyítja, hogy a hadserege bízik az ilyen irányú fejlesztések jövőbeni sikerében. A jelenlegi kutatások célja a súly csökkentése, az alkalmazási mód optimalizálása és a hálózati kapcsolatok megbízhatóságának és áteresztőképességének a növelése.

Az amerikai hadsereg modernizálásának középpontjában a hálózat alapú hadviselés minél szélesebb körű támogatása áll.[19] A stratégiai tervekben már szerepel az IPv6 alapú gerinchálózat kiépítése, amely előre láthatólag maga után fogja vonni a rendszer összes elemének a modernizálását. Ez alapján várható a hálózatba integrált egyéni felszerelések IPv6 kompatibilissé tétele is.

## ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Jelen korunk információs társadalmában a hordozható informatikai eszközök kiemelt fontossággal bírnak a kommunikációs csatornák elérésében. A polgári, illetve katonai tevékenységek során a megfelelő információ, minél rövidebb időbeni elérése nélkülözhetetlen alapfeltétele a feladatok sikeres végrehajtásának.

A világháló jellemző Internet Protokollja a több mint negyven évvel ezelőtt kifejlesztett IPv4, amely megalkotásakor nem láthatták előre az internet mérhetetlen sikerét. Napjainkra azonban világosan kitűnnek a hiányosságok, amelyek kiküszöbölése érdekében megalkották az Internet Protokoll hatos verzióját. Az új protokollkészlet számos olyan újdonsággal rendelkezik, amelyek egyrészt támogatják a felhasználók népszerű alkalmazásait, másrészt egyszerűsítik és gyorsítják a hálózat működését. Teljes körű alkalmazása a Távol-Keleten már megtörtént és számolni kell bevezetésével a világ többi országában is.

Az IPv6 világméretű hódítása még várat magára, azonban a hardvergyártók látva a fejlődési tendenciákat már éveken ezelőtt kompatibilissé tették eszközeiket. Jelenleg az IPv6 támogatottsága egy adott eszköz esetén leginkább az alkalmazott operációs rendszer függvénye.

Áttekintve az amerikai Land Warrior rendszer családot a katonai viselhető informatikai eszközök tekintetében nem az IPv6 támogatásának biztosítása jelenti a legfőbb megoldandó problémát. A hadsereg hálózatfejlesztési stratégiájában kiemelt helyen szerepel az IPv6 képesség elérése, ezért valószínű, hogy a katonai viselhető informatikai eszközök ilyen irányú modernizálása is rövidesen be fog következni.

<sup>24</sup> Az 5th Striker Brigade Combat Team teljes állománya felszerelésre került a csökkentett súlyú (10 lb) verzióval.

## FELHASZNÁLT IRODALOM

- [1] Karvalics László; Információs társadalom történelem; 2003  
<http://mek.niif.hu/04400/04469/04469.pdf>, letöltve: 2010-12-10
- [2] The Source for IPv6 Information, Training, Consulting & Hardware  
<http://ipv6.com/>, letöltve: 2010-11-28
- [3] Magyar Telekom Nyrt.; Miért jobb az IPv6?  
[http://www.telekom.hu/ipv6/miert\\_jobb\\_az\\_ipv6](http://www.telekom.hu/ipv6/miert_jobb_az_ipv6), letöltve: 2010-12-10
- [4] Denis Howe; Free On-Line Dictionary of Computing; 2010  
<http://foldoc.org/host>, letöltve: 2011-11-10
- [5] American Registry for Internet Numbers; ARIN recognizes interop for returning IPv4 address space; 2010  
<https://www.arin.net/announcements/2010/20101020.html>, letöltve 2011-10-30
- [6] IPv4 exhaustion; 2010  
<http://hu.wikipedia.org/w/index.php?title=F%C3%A1jl:Ipv4-exhaust.svg&filetimestamp=20110701064328>
- [7] INTEC Inc.; IPv4 Exhaustion Counter (English)  
[http://inetcore.com/project/ipv4ec/index\\_en.html](http://inetcore.com/project/ipv4ec/index_en.html)
- [8] IPv6 vs IPv4  
[http://hu.wikipedia.org/w/index.php?title=F%C3%A1jl:IPv6\\_vs\\_IPv4.jpg&filetimestamp=20080506215822](http://hu.wikipedia.org/w/index.php?title=F%C3%A1jl:IPv6_vs_IPv4.jpg&filetimestamp=20080506215822), letöltve: 2011-10-30
- [9] T. Naren – E. Nordmark – W. Simpson: Neighbor Discovery for IP Version 6 (IPv6); 1998  
<http://www.faqs.org/rfcs/rfc2461.html>, letöltve 2011-10-20
- [10] Computer Industry Almanac Inc.: Market Research Reports  
<http://www.c-i-a.com>, letöltve: 2011-09-10
- [11] Microsoft Kisvállalati Információs Központ  
[http://www.microsoft.com/hun/kisvallalat/themes/practical/get\\_most.mspix](http://www.microsoft.com/hun/kisvallalat/themes/practical/get_most.mspix), letöltve: 2010-12-30
- [12] Munk Sándor: Katonai informatika III. egyetemi jegyzet, 2003, Zrínyi Miklós Nemzetvédelmi Egyetem
- [13] Peter Bieringer: Linux IPv6 HOWTO (en); 2010  
<http://tldp.org/HOWTO/Linux+IPv6-HOWTO/systemcheck-kernel.html>, letöltve: 2010-12-13
- [14] Five Best Netbook Operating System  
<http://lifehacker.com/5471394/five-best-netbook-operating-systems>, letöltve: 2011-11-01
- [15] Fodor Dezső: Egy adalék a viselhető eszközök tervezéséhez; Informatika a felsőoktatásban; Debrecen; 2005  
<http://agrinf.agr.unideb.hu/if2005/kiadvany/papers/C44.pdf>, letöltve: 2011-11-01
- [16] Steve Mann: Definition of „Wearable Computer”; Toronto; 1998  
<http://wearcam.org/wearcompdef.html>, letöltve: 2011-11-01
- [17] Noah Shachtman: The Army’s New Land Warrior Gear: Why Soldiers Don’t like It; Popular Mechanics; 2009  
<http://www.popularmechanics.com/technology/military/4215715>, letöltve: 2010-12-15
- [18] General Dynamics: The Land Warrior system puts the Soldier into the network; 2007  
[http://www.gdc4s.com/documents/landwarrior\\_web010.pdf](http://www.gdc4s.com/documents/landwarrior_web010.pdf), letöltve: 2010-12-15
- [19] Land Warrior; 2003  
[http://www.army-technology.com/projects/land\\_warrior/land\\_warrior2.html](http://www.army-technology.com/projects/land_warrior/land_warrior2.html), letöltve: 2010-12-16
- [20] Négyesi Imre: DIE VISION DER TRAGBAREN INFORMATIONSTECHNOLOGIEGERÄTE (A viselhető számítástechnikai eszközök jövőképe) (Hadmérnök on-line, III. évfolyam (2008) 4. szám, 173-179. oldal, ISSN 1788-1919)
- [21] Dr. Négyesi Imre: TRAGBARE UND FELDINFORMATIK-GERÄTE I. (Tábori és hordozható informatikai eszközök I.) (Hadmérnök on-line, IV. évfolyam, (2009) 2. szám, 333-339. oldal, ISSN 1788-1919);
- [22] Dr. Négyesi Imre: TRAGBARE UND FELDINFORMATIK-GERÄTE II. (Tábori és hordozható informatikai eszközök II.) (Hadmérnök on-line, IV. évfolyam (2009) 3. szám, 355-362. oldal, ISSN 1788-1919);



**Juhász Márta**  
marti.juhasz@hotmail.com

## INFORMÁCIÓCSERE ÉS ADATÁTVITEL A LÉGI KUTATÁS-MENTÉSBEN

### Absztrakt

*Napjainkban a valós idejű információcsere és adatátvitel kiemelten fontos szerepet kap a mindennapi életünkben, főleg a légi segítségnyújtás területén. Jelen cikk bemutatja a légi kutató-mentő szolgálat információs rendszerét, alkalmazott kommunikációs csatornáit, hiányosságait, illetve fejlesztési lehetőségeit.*

*In these days the real-time exchange of information and data transmission plays an important role in our daily life, especially in air assistance. This publication represents the information system of the air search and rescue service, the used communication channels, the deficiencies and the possibilities of development.*

**Kulcsszavak (key words):** kutatás-mentés, kommunikáció, adatátvitel ~ search and rescue, communication, data transfer

### BEVEZETÉS

A kommunikáció a mai modern világban észrevétlenül behálózza életünket, és alapvető szükségletté vált. Komfortérzetünkhöz hozzátartozik, az azonnali információszerzés és kapcsolatfelvétel lehetősége, de vannak területek, ahol ez életbevágóan fontos lehet. Ilyenek a készenléti szervek, ahol az emberi életet percek múlhatnak. A információáramlás hitelessége, és minél szélesebb körű megvalósítása növelheti a segítségnyújtás hatékonyságát.

A repülésben, ahol az események gyorsan történnek, és nagy veszélyekkel járhatnak, így fontos az azonnali hatékony beavatkozás. Ezt a munkát végzi Magyarország légi kutató-mentő szolgálat. A készenlétet egy-egy erre a célra átalakított, mentőeszközökkel felszerelt MI-8-as típusú helikopter adja 24 órában, két állomáshelyen, Pápan és Szolnokon.

Cikkemben bemutatom a szolgálat információs rendszerét, a tevékenység során használt fontosabb kommunikációs csatornákat, eszközöket. Ezen kívül bemutatásra kerülnek a rendszer hiányosságai, illetve további lehetőségek a hatékonyság növelésére.

### 1. A KUTATÓ-MENTŐ SZOLGÁLAT SZERVEZETÉNEK INFORMÁCIÓS RENDSZERE

A kutató-mentő szolgálat információs rendszerének fő elemei között elsőként az irányító szervezeteket kell megemlíteni. Ezek a 267/2011. (XII. 13.) Kormányrendelet alapján a Kutatás-Mentés Koordináló Központ (KMKK), a Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság (BM OKF) és a Magyar Honvédség Összhaderőnemi Parancsnokság (MH ÖHP) bázisán 24 órás szolgálati rendben működő ügyeleti szolgálat. Az információáramlásban részt vesz még a Nemzeti Közlekedési Hatóság repülőbaleseti készenléti szolgálat, a rádióiránymérő (helymeghatározó) szolgálat, a Kormányzati

Távközlési Rendszer, illetőleg annak útján elérhető - kutatási-mentési feladatokhoz kapcsolódó - adatbázis elérési lehetősége. Fontos továbbá a mindenkor meteorológiai szolgálat, illetve a meghatározott légi kutató-mentő körzetek működési rádiófrekvenciáin, valamint a légiközlekedés vészfrekvenciáin történő forgalmazás.

## 2. KOMMUNIKÁCIÓ A LÉGI KUTATÁS-MENTÉSBEN

A kutató- mentő helikopterek, feladatukból adódóan széles körű hírforgalmazási tevékenységet folytatnak. Egyrészt kapcsolatot kell tartaniuk a mentés helyszínén lévő erőkkel (ha már kiérkeztek), a mentést összehangoló szervezettel, és a saját személyzetükkel, illetve a kutatás-mentést elrendelő szervvel, továbbá a kutatás- mentés területén és a megközelítő útvonalon a légtérért felelős légiforgalmi egységgel.

A kárhelyszínhez történő repülés során a helikopter személyzete elsőként az illetékes légiforgalmi irányító egységekkel veszi fel a kapcsolatot. Minden légiforgalmi légtérhez egy kijelölt frekvencia tartozik, melyen az adott légiforgalmi irányító a légtérben tartózkodó összes járművel kommunikál. Ezek emellett meghatározásra került egy nemzetközi vészfrekvencia (121,5 MHz), melyet a bajba jutott légi járművek használnak segítségkérésre, illetve a mentő egységek segítségnyújtásra.

### 2.1. Kommunikációs eszközök

Az irányító egységekkel és más légi járművekkel történő kapcsolatfelvétel eszköze az R-842 illetve R-860 típusú fedélzeti rádió berendezés. Jellemzői:

- URH hullámsáv,
- Frekvenciatartomány: 118,25-136,5 MHz,
- Adóteljesítmény: 3W, 180 csatorna.
- Amplitúdómoduláció, modulációs mélység 40-90%,
- Vevő érzékenység nem rosszabb, mint 7 mikrovolt,
- Tápfeszültség: 22-29V,
- Teljesítményfelvétel vételen max. 32 W, adásban max. 85W,
- Kétoldalú összeköttetés hatótávolsága RASZ-UKV ellenállomással 1000 m-es magasságból nem kevesebb, mint 100 km,
- A rádió 50 Ohm-os koax-al csatlakozik az erre a sávra méretezett „kés” antennára.



1. sz. ábra: R-860 rádió [3]

Annak érdekében, hogy a rádióforgalmazás a légi jármű vezetését ne korlátozza, a kommunikáció jellemzően sisakba épített hangrendszer segítségével történik. A MI-8-as típusú helikopterhez az amerikai SPH-4AF típusú helikoptervezető sisak van rendszeresítve.

Jellemzői:

- Integrált fülhallgatót és mikrofon,
- Négy részre tagolt U- 174/U típusú csatlakozó (melyről meg kell említeni, hogy nem kompatibilis a fent említett rádió hangrendszer-csatlakozójával valamint a fülhallgató és mikrofon impedanciája is eltér a szükségesétől),
- Átalakító az előbbi problémák megoldására,
- EV986 típusú, 19 Ohm impedanciájú fülhallgató,
- Több részből álló külső zajokat hangszigetelő, biztonságos fülhallgató-foglalat,
- M-87A/AIC típusú, 6 Ohm impedanciájú dinamikus mikrofon (a sisak bal külső oldalán rögzített állítható rudazaton).



2. sz. ábra: SPH-4AF helikoptervezető sisak, és U-174/U csatlakozó [4]

## 2.2. Belső kommunikáció

Természetesen nagyon fontos a légi jármű fedélzeti belső kommunikáció is. Belső kommunikációs rendszer alatt a személyzet a fedélzeten belüli folyamatos beszéd alapú összeköttetését értjük. A helikoptereken jellemzően legalább három szolgálati személy tartózkodik: légi jármű parancsnok, másodpilóta, és a fedélzeti technikus. Közöttük az összeköttetés a fent említett helikoptervezető sisak és belső kommunikációs rendszer (INTERCOM) segítségével történik.

A kutató-mentő küldetések végrehajtása közben jellemző a feladatorientált munkamegosztás, mely kiemelt szerepet kap, csökkentve az információs csatornák leterheltségét. Vannak azonban feladatkörök, ahol a közvetlen összeköttetés szintén elengedhetetlen, a kommunikáció még sincs teljesen megoldva. A legnagyobb hiányossága a sisakrádió, amely lehetővé tenné a területen dolgozó kutató-mentő személyek (ejtőernyős

gyorsbeavatkozó, felcser) közötti folyamatos kapcsolattartást, és biztosítja a gépszeméllyel történő rádió- összeköttetést. Ez a hiány akkor tűnik fel a legjobban, ha a feladatot korlátozott látási körülmények mellett (például: köd, füst, por), esetleg nehezen átlátható terepen (ártéri, vagy hegyes- völgyes erdő) vagy éjszaka kell végrehajtani és itt már nem nyújt kellő segítséget a hagyományos beszéd, illetve látjelek útján történő információcsere. Jelenleg EDR rendszerű kézi rádiókkal történik a kapcsolatfenntartás, amelynek nagy problémája, hogy a beavatkozó személy egyik kezét teljesen lefoglalja, miközben a segítségnyújtás érdekében mindkét kezére szüksége lenne. A helyzet javítása érdekében felmerült headset-ek beszerzésének lehetősége a jelenlegi rádióeszközökhöz. A sisakrádiók használatával azonban közvetlen összeköttetés lenne létesíthető a területen dolgozó személyek, a helikopter és a mentés-összehangoló szervezet között. Az első kézből érkezett információk jelentősen segítenék a további munkálatok megtervezését, illetve biztos alapot nyújtanának a kiegészítő erők időbeni kirendeléséhez.

### 3. EGYÉB FEDÉLZETI ADATÁTVITELI ESZKÖZÖK

Kijelenthetjük, hogy hiányosság továbbá az is, hogy a Magyar Honvédség kutató-mentő helikopterei nem rendelkeznek fedélzeti hangrögzítő készülékkel. A helyszínen rögzített felvételek, amik a későbbiekben feldolgozhatóak jelentősen megkönnyítenék és gyorsítanák a munkát. Ezek alapján készíthetők el a jegyzőkönyvek, melyek egyszerűen a feladat végrehajtás során tapasztaltakat rögzítik. Segítségével elkerülhetők az esetleges félreértések, információ-torzulások.

Ugyanígy kialakíthatók képrögzítő berendezések is a járművek fedélzetén. A katasztrófa területén készült felvételekkel azonnali segítséget tudnak nyújtani a mentésben részt vevő szervezetek számára, mivel lehetőség nyílik az eszközök készenlébbe helyezésére, a terület vezénylésére, és a várható helyzetre való felkészítésre. Tehát feladatuk igen széles körű. Az általuk nyújtott adatok a több szempontból történő feldolgozást; többirányú felhasználást teszik lehetővé.

A katasztrófavédelemben és a kutatás-mentésben részt vevő erők alkalmazását tehát minden esetben meggyorsítják a real-time információk mivel csökkentik a károkat, a beavatkozó egységek tevékenysége pedig hatékonyabbá válik. Mindent összevetve kijelenthetjük, hogy a korszerű kommunikációs eszközök használata lényegesen mérsékli az egyéb (anyagi vonatkozású, technikai, szervezeti) hátrányokat a katasztrófahelyzetekben.

### ÖSSZEGZÉS,KÖVETKEZTETÉSEK

A kutatás-mentésben részt vevő helikopterek kommunikációs rendszere sajnos nem tökéletes. A szükséges rádióeszközökben is hiányt szenved, ugyanakkor kommunikáció címszó alatt manapság már nem csak a rádióösszeköttetést biztosító berendezéseket értjük, hanem az adatátvitelt, mint a rádió alapú hangos összeköttetést. Különböző csatornákon keresztül, írásos vagy képi formában el lehet juttatni a fedélzetre/fedélzetről a friss információkat (például: légtérfoglaltság, légtérstátus, meteorológiai adatok stb.) Ez a fajta kommunikáció sokkal szélesebb körű információcserét tesz lehetővé a fedélzeten tartózkodók és a földi irányító (mentéskoordináló) között. Ez az adatcsatorna a földön tartózkodó személyeknek lehetőséget ad pl. real-time videofelvételek vételére, közvetítésére, légköri adatok továbbítására (szennyezettség, láthatóság stb.). Ennek segítségével a mentés folyamata sokkal hatékonyabban tervezhető meg, valamint a szükséges kiegészítő erők a helyszínre irányításuk alatt kaphatnak aktuális helyzetet, tükröző tájékozódást a rájuk váró

feladatról. Az adatátviteli csatornák ezen kívül biztosíthatják a kommunikáció teljes körű archiválhatóságát a későbbi feldolgozás, elemzés céljára.

Publikációból kiderül, hogy a légi kutató- mentő szolgálat információs rendszere igen összetett. Bár csak egy kisebb területet érintve elemeztem, mégis megmutatkoztak olyan hibák, melyek nehezítik a munkát. Emellett lehetőség nyílhat a fejlesztések megvalósítására több irányban és más kommunikációs csatornákon is, mely véleményem szerint szükséges is.

### FELHASZNÁLT IRODALOM

- [1] 267/2011. (XII. 13.) Korm. rendelet a bajba jutott légi járművek megsegítését, valamint a katasztrófák elleni védekezéssel és a mentéssel összefüggő tevékenységet ellátó légi kutató-mentő szolgálat szervezetéről, működésének, fenntartásának, riasztásának és a mentéssel járó költségek viselésének rendjéről, e tevékenységek engedélyezésére vonatkozó szabályokról.
- [2] Airplane radio R-860 „Pero” {P-860} I  
[http://www.radiomuseum.org/r/unknown\\_airplane\\_radioper\\_r\\_860p\\_2.html](http://www.radiomuseum.org/r/unknown_airplane_radioper_r_860p_2.html) (2011-01-06)
- [3] R-860-II, Repülő fedélzeti rádió adó-vevő  
<http://www.radiohistoria.sk/Oldradio/mainhu.nsf/wcatalid/0002279> (2011-01-05)
- [4] Az SPH-4AF helikoptervezető sisak  
<http://lhsn.hu/az-sph-4af-helikoptervezeto-sisak/> (2011-01-06)
- [5] Jeremy Warriner: Real-time two way time transfer to aircraft  
<http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA474550> (2011-01-04)



**Horvayné Fehér Judit**  
feherjenator@gmail.com

## **ELEKTRONIKUS ÜGYIRATOK TOVÁBBÍTÁSÁNAK MEGOLDÁSAI A RENDŐRSÉGNÉL**

### **Absztrakt**

*„Az elektronikus kormányzat az információs technológia használatával kívánja támogatni a kormányzat működését, ezen a platformon is megvalósítani az állampolgárok kiszolgálását és kormányzati szolgáltatások biztosítását.”[1] A kormányzat struktúrájának elektronizáltságát tekintve az uniós tagállamok legnagyobb része az egyoldalú interaktív szolgáltatások kiépítésénél tart. A magyar kormányzat célja, hogy az elektronikus ügyintézés mellett megvalósítsa az elektronikus aláírás alkalmazását is. A rendőrség célja, hogy ne csak a szervezetek közötti kommunikáció kapcsán kerüljön alkalmazásra az elektronikus aláírás, hanem a „külső”, kormányzati szervezetek között is megvalósuljon ez ügyvitel. Tekintettel arra, hogy már 10 éve van lehetőség elektronikus aláírásra. A Belügyminisztériumi (a továbbiakban: BM) szervezetek további célként fogalmazták meg, hogy az elektronikus aláírásról szóló 2001. évi XXXV. törvény (a továbbiakban: Eat.) szerinti tanúsító szervezatként kívánnak megjelenni a megvalósulás során. Az egyik legnagyobb belső aláírásra alkalmas terület a kormányzaton belül a BM. Az iratforgalom mennyisége, a továbbítás gyorsítása is indokolja a bevezetését elsődlegesen a rendőrségen.*

*This article is about a security services of MoI.*

**Kulcsszavak (key words):** biztonság, IT rendszerek ~ security, IT systems

### **BEVEZETÉS**

Az elektronikus ügyintézés megvalósítása kormányzati szinten sok évre visszanyúló történet. Az információ áramlás első állomása az elektronikus ügyintézésben, az e-kormányzat. Ahhoz hogy átlássuk az elektronikus ügymenetet, el kell különíteni az e-kormányzati modelleket, melyek az e-kormányzati működésekről készült tervezések során felhasználtak a magyar kormányzati szervek, és amelyek Európai Unió országokban megjelenőket. Magyarországi e-kormányzás modelljét megismerve, teljesen új megvilágításba kerül az intézményrendszeri együttműködést, ahol a rendőrség szervesen csatlakozik az e-kormányzathoz. Az Európai Unióbeli környezetek és elvárások ebben a tekintetben rendkívül széles spektrumon sorakoznak fel.

Az Eat. már tíz éve megteremtette az elektronikus aláírás lehetőségét Magyarországon. A kormányzat célja, hogy a ne csak a szervezetek közötti kommunikáció kapcsán kerüljön alkalmazásra az elektronikus aláírás, hanem a „külső” szervezeten kívüli aláírás is megvalósuljon. Tekintettel arra, hogy már 10 éve van lehetőség elektronikus aláírásra, a szervezetek további célként fogalmazták meg, hogy az Eat. szerinti tanúsító szervezatként jelenjenek meg a megvalósulás során. Az iratforgalom mennyisége, a továbbítás gyorsítása is indokolja a bevezetését. Ezek alapján azt gondolom, hogy kormányzati szinten már időszerű az elektronikus aláírás bevezetése. A BM-on belüli és az ágazati szervekkel történő

iratforgalom tetemes mennyiségére is tekintettel időszerű az elektronikus aláírás feltételrendszerének kialakítása, mely szerves része az elektronikus ügyintézésnek.

Elemzéseim részleteiben nem térnek ki az egész e-kormányzat magyarországi megvalósítási lehetőségeinek vizsgálatára, korlátozódik a BM és ágazati szervezeteinél történő alkalmazhatóság eseteinek vizsgálatára, és kiemelten kezeli a rendőrséget a bevezetés eredményeinek megismerésére.

Jelen publikációm célja az elektronikus aláírás rendőrségi területen való alkalmazhatóság követelményrendszerét, azok akadályait felfedni, továbbá meghatározni, hogy a „belső” anyagok aláírásához milyen feltételrendszert alkalmazunk. Ténykérdésként megvizsgálom, hogy a rendőrség maga auditáltat-e, vagy elegendőnek bizonyul a rendszer belső mechanizmusa által garantált a hitelesség.

## **1. AZ E-KORMÁNYZAT MAGYARORSZÁGON**

### **1.1. Az E-kormányzat kialakulása Magyarországon**

Magyarország az elektronizálódás korát éli. Megfigyelhető ez a tendencia a legmagasabbtól a legalacsonyabb szintekig. Kimutatható ez a trend az Európai Unió hazánkkal szemben támasztott elvárásaiban, a kormányzat rövid és hosszú távú stratégiai terveiben.

Az Európai Unió kidolgozott stratégiai elképzelésekkel, tervekkel rendelkezik az informatika és a közigazgatás témakörében is (eEurope). Ezzel összhangban kormányzati szinten kialakításra került az Európa-terv, illetve annak kisebb időszakokra lebontott ütemei, melyek a kormányzat hosszú távú fejlesztési célkitűzéseit tartalmazzák. Az Európa-terv híd az Európai Unió céljai, illetve támogatásai, és a Magyar Köztársaság kormányának szándékai között. Összehangolja az állam, a gazdaság és a civil társadalom törekvéseit. Egyesíti a központi (állami, önkormányzati) és a gazdasági, pénzügyi forrásokat. Hatékony eszköze a modernizációnak.

Az Európai Unió a csatlakozó államokkal folytatott közös tervezés támogatására Strukturális és Kohéziós Alapokat hozott létre, melyeknek hazai szintén való forrásként történő felhasználására kialakításra került a Nemzeti Fejlesztési Terv (a továbbiakban: NFT), ami a különböző célkitűzések megvalósításának támogatására operatív programokat hoz létre folyamatosan.

A célkitűzések megvalósítására 2002 elején megalakult Magyarországon a Kormányzati Informatika és Társadalmi Kapcsolatok Hivatala (a továbbiakban: KITKH) a kormányzati informatikai feladatok ellátására. 2002 végén a kormány elfogadta a Magyar Információs Társadalom Stratégia (a továbbiakban: MITS) elkészítésének rendjét. Az egyes minisztériumok részstratégiái az IHM ajánlái alapján készültek el. A MITS fejlesztése az eEurope programmal és a NFT összhangban történik, ezáltal biztosított Magyarország számára, hogy az Európai Unió támogatási alapjaiból részesülhessen.

A kormányzati informatika és az elektronikus kormányzás feladatait a Miniszterelnöki Hivatalról szóló 148/2002 (VII.1.) Korm. rendelet (statútum) határozza meg. E feladatokat 2002-2003-ban a KITKH végezte, ezt követően az Elektronikus-kormányzat-központ (a továbbiakban EKK) látja el. A Miniszterelnöki Hivatal vezető miniszter hatáskörébe utalt feladatokat a kormányzati informatikáért felelős kormány megbízott irányítja.

A statútumban meghatározott feladatok alapján - figyelembe véve a kapcsolódó EU-dokumentumokat, irányelveket, ajánlásokat, a legjobb nemzetközi tapasztalatokat és az informatikai fejlesztések terén jelentkező trendeket - készült el az Elektronikus Kormányzat Stratégia és Programterv (E-kormányzati stratégia), amelyet a Kormány 2003. decemberben fogadott el [1].



Az E-kormányzat stratégia megvalósítása érdekében a KITKH, majd az EKK összkormányzati koordinációs tevékenységét a Kormányzati Informatikai Egyeztető Tárcaközi Bizottság (a továbbiakban : KIETB) segíti. A KIETB az 1991-ben létrehozott Informatikai Tárcaközi Bizottság ( a továbbiakban ITB) jogutódja. Tagjai a fejezeti jogkörű költségvetési szerveknek az informatika ágazati stratégiájának kidolgozásáért és végrehajtásáért felelős vezetői. A KIETB működését a 1054/2004 (VI. 3.) Korm. határozat szabályozza.

Az elektronikus kormányzás feladatainak fontos részét képezi az EU által az eEurope 2005 akciótervben meghatározott 20 alapvető szolgáltatás megvalósításának koordinálása. E területen az EKK tevékenységét segíti a szolgáltató állam létrehozásához kapcsolódó reformfolyamatok felgyorsítása érdekében a közigazgatási szolgáltatások korszerűsítésével kapcsolatos feladatokat összehangoló Koordinációs Bizottság irányítása alatt működő, a 1126/2003. (XII. 12.) Korm. határozattal létrehozott E-Kormányzat Operatív Bizottság (a továbbiakban EKOB). Az EKOB összetételét és feladatait a 1054/2004 (VI. 3.) Korm. határozat szabályozza.

Az elektronikus kormányzás alapinfrastruktúráját a 1122/2001 (XI. 22.) Korm. határozatban megfogalmazottaknak megfelelően létrehozott Elektronikus Kormányzati Gerinchálózat (a továbbiakban EKG) képezi. Az EKG a 18 megyeszékhelyet és Budapestet összekötő szélessávú, nagysebességű hálózat, amely biztosítja a központi közigazgatás és a területi intézmények adatkommunikációs kapcsolatát, internet-elérését és elektronikus levelezését.[2]

Az EKG biztosítja a kapcsolatot az EU TESTA[3] hálózatán keresztül az EU intézményrendszeréhez. Az EKG szerves részét képező H-SecNet [4] titkosított hálózat, szolgál az EU döntéshozatali tevékenységéhez kapcsolódó kormányzati koordináció informatikai hátterét. E rendszer kialakítását a 2329/2003. (XII. 16.) Korm. határozat írja elő.

Az 1995/468/EK határozat alapján beindított IDA [5] Program alapvető feladata az EU-tagországok közigazgatásai közötti elektronikus információcsere támogatása az egységes piac szabályozásának és a közösségi politikák megvalósításának elősegítésére. Az IDA szolgáltatásai elérésének telekommunikációs infrastrukturális eszköze a TESTA hálózat. Az IDA Program magyarországi koordinálását a KIETB keretén belül 2004-ben létrehozott KIETB IDA szakmai bizottság végzi. Az IDA program továbbfejlesztéseként a 2004/387/EK határozattal indult el az IDABC program.

A 2002-es Kormányprogramban meghirdetett "szolgáltató állam" elektronikus információs kapuja a Kormányzati Portál, amely a magyarorszag.hu internetes honlapon keresztül érhető el. A Kormányzati Portál látja el a közigazgatási ügyek intézéséhez szükséges "ügyfélkapu" szerepét, ugyanakkor információs-tájékoztatási szolgáltatásai a kormányzati kommunikáció; speciális (azonosított személyek részvételével zajló) fórumszolgáltatása, pedig a felelős állampolgári véleménynyilvánítás szempontjából nagy jelentőségű.

„Az elektronikus kormányzás magyarországi tevékenysége összhangban áll a 2004-ben, Athénban rendezett XIV. Információtechnológiai Világkongresszuson (a továbbiakban WCIT 2004) az e-kormányzati tevékenységgel kapcsolatosan elfogadott nyilatkozat alapelveivel.”[6]

## 1.2. E-kormányzati szcenáriók Magyarországon

Az elektronikus kormányzati fejlesztések tágabb környezetének fél tucat olyan, meghatározó elemét különítettük el, amelyek alakulása döntő mértékben határozhatja meg a

mindenkori állapotokat, illetve forgatókönyveket. Három-három komponens egymás mellé rendezésével két tengely jött létre, amely a problémateret négy részre osztja. A két tengely:

1. Belső (politikai) feltételekre.
2. Külső (gazdasági-technológiai) változásokra.

### **1.3. A Belső feltételek három komponense**

1. A politikai porond, fokozódó párt-megosztottsága, éleződő ellentétek, erősödő konfliktusok, a politikai közélet kriminalizálódása con kooperatívabb, európaibb együttműködés a rivális erők között.
2. Lassú, nehézkes, az ellenérdekek oldaláról állandó fékezőerőt jelentő kormányzati modernizáció, stagnáló (vagy rosszabbodó) korrupciós háttérrel con dinamikus és sikeres modernizáció, amely fokozatosan a szakmaiság, a professzionális államigazgatás mintáit erősíti.
3. Nyögvenyelős, elhúzódnó EU-integráció, elvesztett esélyekkel, sértődésekkel, politikai „büntetésekkel” con hatékony alkalmazkodás, felkészült fogadó oldal, sikeres és innovatív adaptáció.

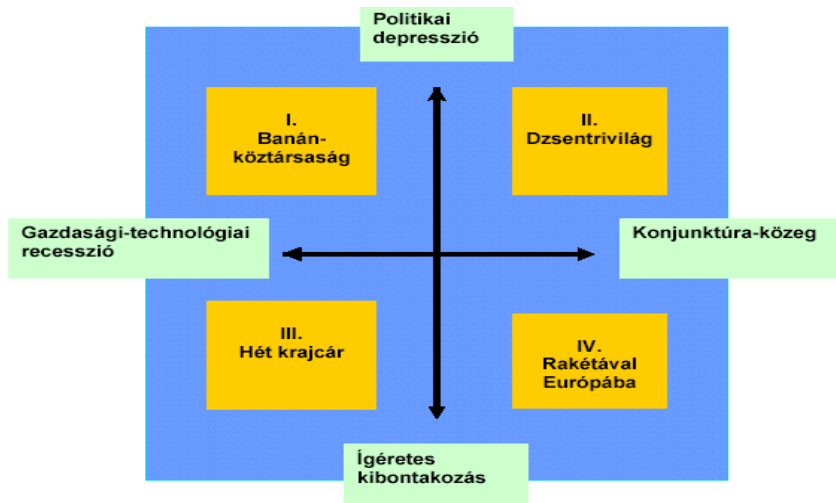
A három komponens egymást feltételezi, egymást erősíti akár a pozitív, akár a negatív irányba – a különböző komponensek ellentétes irányba történő mozgása nagyon nehezen elképzelhető. Véleményem szerint az integráció esetében inkábbba gazdasággal való együttmozgás esélye nő meg, ott egy recesszió növeli meg a nyögvenyelős integrálódás valószínűségét.

A tengelycsúcsok neve: Politikai Depresszió (PD) con Ígéretes Kibontakozás (IK), a Valóság e két szélsőérték között, de vélhetően valamelyikhez közelebb helyezkedik majd el, de 5-10 év távlatában akár változó irányú mozgás is elképzelhető. Hosszú távon szocio-kulturális okok miatt mindhárom elem esetében a javulás prognosztizálható, de a következő 2-3 évben a változás iránya teljesen nyitott.

### **1.4. A Külső változások három komponense**

1. Gazdasági recesszió con gazdasági konjunktúra (a világban és Európában – azt nem vizsgáljuk, hogy mi van, ha regionálisan eltér a trend).
2. Az e-kormányzatra fordítható források csökkennek, visszaesik a fejlesztés lendülete con bővülnek a források.
3. A technológia (elsősorban a költség szerkezete és upgrade-kényszere ) miatt anyagi és emberi erőforrás-oldalról nehezíti a szinten tartást vagy a fejlesztést con a technológia változása az egyre olcsóbb és egyre nagyobb tudású rendszerekkel fokozatosan, megkönnyíti az implementációt, a re-engineeringet. A tengelycsúcsok neve: Gazdasági-technológiai Recesszió(GR) con Konjunktúraközeg (KK).

A két tengely (Belső- Külső) által kialakított négy cellára készített a kormány forgatókönyvet, végiggondolva, hogy mi is lehet akkor, ha ezek így találkoznak. A külső változások komponenseit az alábbiakban mutatom be:



1. sz. ábra [2]

Az e-kormányzás stratégiai kérdései jó ideig az átfogó, de kormányzati szintre soha nem emelkedő, információs társadalom-fejlesztési szakanyagokban jelentek meg, élükön az 1995-re elkészült Nemzeti Informatikai Stratégiával (a továbbiakban NIS), majd az 1999-es Tézisek az információs társadalomról és a Magyar Válasz az Információs Társadalom kihívására című dokumentumokkal. A stratégiák elemzése, értékelése a végleges Magyar Információs Társadalom Stratégia kidolgozásának hangsúlyos eleme.

Az első e-kormányzati programként hivatkozható mű – az Informatikai Kormánybiztosság Elektronikus Kormányzat Főcsoportja által kidolgozott Nemzeti Információs Társadalom Stratégia (a továbbiakban NITS) elektronikus kormányzat alprogramja – a kormányzati ügyvitel elektronizálását és a szolgáltató kormányzat létrehozását jelölte ki célként. Az alprogram a demokratizálódás előfeltételeként tekintett az elektronikus kormányzat megteremtésére, az állam szolgáltató jellegének erősítésére.

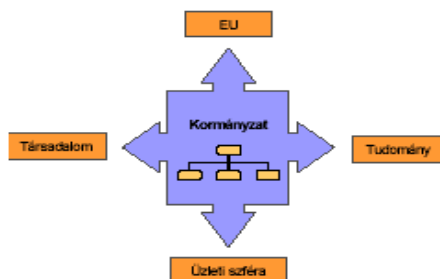
Kiemelt feladatként jelölte meg „az egységes kormányzati háló és az elektronikus közbeszerzési rendszer kialakítását, a jogszabályi környezet megváltoztatását, az elektronikus aláírás feltételeinek megteremtését és az egységes hírközlési törvény megalkotását.”[7]

### 1.5. Intézményrendszer és együttműködés

A magyar állam- és közigazgatás felépítése hierarchikus, piramis típusú. A merev, lassan változó struktúrában működő közigazgatási egységek a saját, jogszabályokban előírt feladataik ellátására koncentrálnak, nem a társadalom vagy a gazdaság felől érkező igényeknek való megfelelésre. Az ügyfélközpontú szolgáltató állam koncepció előretörése és az információs és kommunikációs technológiák (a továbbiakban: IKT) térnyerése az állam működésében a horizontális, az intézményi kereteket és határokat átlépő együttműködési formák irányába mutat. Ezek a horizontális folyamatok szükségessé teszik a jelenlegi intézményi feladatok átalakítását.

Az e-kormányzat kialakításának alap feltétele a jól szervezett és átlátható kormányzati szervezeti működés. Informális kapcsolatrendszeren nyugvó államigazgatási intézményrendszer esetén az e-kormányzat csupán a felszínen tud megvalósulni, és a várt szolgáltatás minőség javulás és működési hatékonyság növekedés elmarad. A kormányzat

egy összefüggő társadalmi rendszerben működik. Az innen érkező, dinamikus elvárások folyamatosan változási „kényszert” generálnak a kormányzatban. Az elektronikus ügyintézés iránti igény az informatikai erőforrás kihelyezés – outsourcing, 2004-ben Magyarország az Európai Unió tagjává vált. Ez az EU intézmények és a tagállamok közötti elektronikus kapcsolatot biztosító infrastrukturális fejlesztéseken túl a szervezeti együttműködési képesség kialakítását is igényli. Az e-kormányzat kapcsolatrendszerét az alábbiakban ábrázolom:



2. sz. ábra [7]

## 1.6. Az e-kormányzás jövőképe

Az elektronikus kormányzat magyar stratégiája közép- és hosszú távon a következő fő értékek, megvalósulását kívánja szolgálni:

- Az elektronikus kormányzat fejlesztésével hatékonyabbá, átláthatóbbá és hosszabb távon olcsóbbá válhat a közigazgatás, az állam működése;
- A hatékonyabban működő, jobb szolgáltatásokat nyújtó közigazgatás révén válhat lehetségessé a részvételi demokrácia kiszélesítése, az állampolgárok, az üzleti szereplők bizalmának növelése, az emberek nagyobb mértékű részvétele a politikai életben. Minden korábbinál nyitottabb és valódi, kétoldali kapcsolatok, kiépülését kell elősegíteni a közhatalom képviselői és az állampolgárok között;
- A nyilvánosság új fórumaival, az állampolgár-központú közszolgáltatásokhoz való könnyebb hozzáféréssel olyan környezet alakítható ki, amelyben a közigazgatási szervek és a közösségek folyamatosan megoszthatják tapasztalataikat, befolyásolhatják a helyi és országos e-kormányzati programok megvalósítását, és ezzel új, az állampolgári és vállalkozói igényeket kielégítő alapokra helyeződik az állam és a polgárok, valamint azok közösségeinek kapcsolata.
- Egy szolgáltató és esélyteremtő állam egyre inkább az információ szabad áramlásának biztosításával lehet képes csak feladatait betölteni. A közigazgatásnak tudatosan kell a konzultációs folyamatokat, lehetőségeket kialakító folyamatok élére állnia, és minden vonatkozásban, kezdeményező szerepben kell tudni fellépnie.
- A szolgáltató állam és a szolgáltató kormányzat kiépítésének egyik legfontosabb (de nem kizárólagos) eszközét az elektronikus kormányzat lehetőségei alkotják, amelyet a jövőben kihasználva Magyarország felzárkózhat az elektronikus kormányzati szolgáltatások fejlettségében és használatában élenjáró országokhoz (legyenek azok közvetlen környezetünkben, az EU-ban vagy másutt).
- Ha az IKT modern eszközeinek alkalmazása, használata és elterjesztése terén az állam vezető szerepet tud betölteni, a kormányzati munka sikerén túlmutató módon lesz képes támogatni a tudástársadalom kiépítésének folyamatát, fejlődését, a társadalmi-gazdasági versenyképesség fokozását.

A meghatározó elemek egymást feltételezik, egymást erősítik. „A stratégia szemléletében azonosul az európai elvárásokkal, de a hazai kiindulási feltételekre épít és megvalósítása során alkalmazni kívánja a hazai tudományos, szakmai és szervezési eredményeket.” [7]

## 2. AZ ELEKTRONIKUS ÜGYIRATOK KEZELÉSE

### 2.1. Mit értünk ügyiratok alatt?

Jelen elemzésemben az elektronikus ügyiratkezelés témakörében a vizsgálatot a kormányzaton belül a BM két ágazati területére szűkítettem: a rendvédelmi szervekre és a nemzetbiztonsági szolgálatokra. Ezeknél a szervezeteknél az ügyirat szó értelmezése a jogszabályban előírtaknak megfelelő, tartalmi követelmények alapján kerül meghatározásra. Az ügyiratok kezelése, a 12/2010. (XI.16.) BM utasítás, a 14/2010. (XI.12.) BM utasítása alapján történik. Főbb feladatok között szerepel az érkeztetés, iktatás, nyilvántartás.

Jelenleg a rendvédelmi szférában az ügyiratok kezelése papír alapon történik. A szervezetek közötti dokumentumok átadása általában az állami futárszolgálattal valósul meg. Az átfutási idő akár több napi is lehet. Ezért rendszereztem a papír alapú ügymenet, ügyiratok hátrányai:

- lassú ügymenet, romlik a reakció idő,
- rengeteg papír, nyomtató patron kerül felhasználásra, mely nem környezetbarát megoldás (papír felhasználás, nyomtató patronok felhasználása, futárszolgálat által használt gépjárművek környezetszennyezése, stb.),
- a számítógép által adta lehetőség nem kerül kihasználásra (az ügyirat elkészítésre kerül a számítógépen, majd a nyomtatásra kerül, és a papír dokumentummal dolgoznak tovább /tekintettel arra, hogy az a hiteles dokumentum/),
- a papírok tárolása sok helyet igényel, azok védelme igen sokba kerül (több tároló helyszín, biztonság megteremtése magasabb költségeket eredményeznek).

### 2.1. Az elektronikus ügyiratok kezelése ma Magyarországon

A közigazgatásban a jogszabálynak megfelelően csak az elektronikus cégeljáráásban van elektronikus ügymenet. A BM és ágazatainak ügyiratkezeléséről 12/2010. (XI.16.) BM utasítás IX. fejezet 5. pontja rendelkezik. Elektronikus ügyiratnak nevezzük azt az ügyiratot, melynek a papíralapú háttere nem létezik, csak elektronikusan fellelhető maga az egész irat. Ma Magyarországon nem valósult meg az elektronikus ügyirat kezelése, mert minden elektronikus formában megjelent iratnak a papíralapú valósága létezik. A kormány elsődleges célja ezt az állapotot megszüntetni, és legalább a papíralapú iktatást 2012.december 31-ig megszüntetni. A feltétel rendszere viszont az elektronikus hitelesség és bizalmasság megteremtése. Melynek egyik alapfeltétele az elektronikus aláírás és az időpecsét alkalmazása.

### 2.2. Nehézségek és megoldandó problémák

Az elektronikus aláírásra vonatkozó szabályozás nagy volumenű, rendkívül szigorú szabályozást tartalmaz. A szükséges feltételek megteremtése és biztosítása mind humán erőforrásban, mind pénzügyi forrás tekintetében folyamatosan jelentős háttérigényt jelent. Az elektronikus aláírás bevezetésével kapcsolatban létrehozott projekthez szükséges

pénzügyi forrást több százmillió forint összegben tervezi a kormányzat. A költségek tekintetében az összeg nagysága mértékadó, tekintettel arra, hogy az elektronikus aláírást támogató informatikai megoldások folyamatos auditálása komoly pénzügyi forrásokat igényel. Így költségként jelentkezik – többek között – a rendszeres auditálás a Nemzeti Média- és Hírközlési Hatóság által, az éves üzemeltetési költség, mint a szoftver licenz, karbantartás, szervezet fenntartása.

### **2.3. Az elektronikus ügyiratok biztonságos Továbbításához Szükséges feltételek**

A rendőrség az elektronikus ügyvitelben a BM célját követve, elsődlegesnek tekinti, hogy az elektronikus formában történjen a társszervek, gazdálkodó szervezetek szintjén folytatott kimenő és bejövő iratok forgalmazása. Ehhez meg kell teremteni a megfelelő infrastruktúrát és hálózati infrastruktúrát az EKG, Rendészeti Hálózat felhasználásával. Ennek a tervnek a megvalósításához a 24/2006. Kormányrendelet által előírt iratkezelő rendszer nyújt segítséget. Minden szervezet tekintetében kell alkalmazni, viszont azokon a helyeken, ahol minősített adatkezelés történik, ott a 2009. évi 155. törvény és annak végrehajtási rendeletei által előírt feltételeket kell teljesíteni.

Minden esetben biztosítani kell a hitelességet és bizalmasságot, továbbá meg kell valósítani a maximális biztonságot. Azt a célt kell megvalósítani, hogy a papír alapú ügymeneteket elektronikus ügymenetekre alakítsuk át.

### **2.4. Hitelesség és bizalmasság biztosításának szükségessége**

Ahhoz, hogy a hitelességet biztosítsuk egy hitelesítési szolgáltatás felállításához mindenképpen megfelelő jogi háttér szükséges, melyet jelenleg a 2001. évi XXXV. törvény biztosít. Továbbá a hitelesség megvalósítható az elektronikus aláírás használatával (melynek felhasználása elsősorban személyhez kötött). Az elektronikus aláírás használata egyben a bizalmasság megteremtésére is (amennyiben a dokumentum tartalma változik a továbbítás közben, akkor az érzékelhető). Ugyanis az aláírás dátumának megállapítása esetében hitelesített időbélyeg használata lehetővé teszi az elektronikus aláírások ellenőrzését. De itt feltétlenül pontosítani szükséges azt, hogy mit jelent a tanúsított elektronikus aláírás (azaz kik milyen formában fogadják el annak hitelességét).

### **2.5. Az elektronikus ügyiratok biztonságával kapcsolat általános követelmények**

Az elektronikus ügyiratok kezelése során elsősorban a biztonságra kell törekedni. Az alábbi általános követelményeket határoztam meg a biztonság elérése érdekében a nyíltan kezelt elektronikus iratokra:

- Az adatbiztonság megteremtése adatvesztés elkerülése érdekében. Olyan megfelelő technológiát kell alkalmazni, mely a legkisebb százaléku adatvesztést okozza egy esetleges támadás vagy meghibásodás esetén. Ilyen lehet például a Storage, RAID5 tömbök alkalmazása;
- Az adathozzáférés szabályozása a szándékos károkozás, a megsemmisítés vagy az adatmódosítás elkerülése érdekében. Olyan jogosultsági rendszereket kell kiépíteni, amelyek a rendszer által adta lehetőségeket használják ki nagyobb anyagi ráfordítás nélkül;
- A rendszerbiztonság megteremtése riasztó rendszerek, tűzjelző rendszerek, és szünetmentes tápellátó rendszerek kiépítésével;

- A számítógépes hálózatok teljes körű védelmének megvalósítása, a DMZ kialakítással, tűzfalak alkalmazásával és a hálózatokhoz való hozzáférések szabályozásával;
- Magasabb biztonsági igények támasztása adatlopás esetén. Olyan, az adatok megismerését akadályozó védelmi megoldásokat kell alkalmazni, amelyek fizikailag meggátolják az adatlopást. Például: az adott adathordozó csak az adott gépben olvasható, vagy az eszköz maga titkosít, vagy manuális titkosítást kell alkalmazni az adatokra;
- Új védelmi megoldásokat kell bevezetni a távközlési hálózatok védelmének érdekében. Ilyen a különböző titkosítási eljárások alkalmazása, mint például a MPLS VPN, IPSEC. További megoldást jelentene a végpontok hitelesítése és a tanúsítványok alkalmazása;

## 2.6. Minősített, elektronikus adatkezeléssel kapcsolatos problémák

Az elektronikus ügyiratkezelés témakörében rövid elemzéseket folytattam le az alkalmazhatóság területén. A szervezetek ügyiratainak adattartalmi minősítésének tekintetében, igen nagy az igény elektronikusan továbbított és kezelt ügyiratokra. Három területen alkalmazható az elektronikus ügyintézés és adatkezelés:

- a nyílt adatok
- a nem nyilvános, szenzitív adatok
- a minősített adatok (az államtitokról és a szolgálati titokról szóló 1995. évi LXV. törvény alapján)

Jelenleg is létezik az elektronikus továbbítása a minősített iratoknak, viszont a mai napig nem valósult meg az elektronikus ügyiratkezelése. Összegyűjtöttem néhány, a megvalósulást akadályoztató tényezőt:

- a minősített adatkezelést a Nemzetbiztonsági Felügyelet (a továbbiakban: NBF), hatóságilag szabályozza a tevékenységet a 161/2010. (V. 6.) Korm. rendeletben, a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól. A szabályozás alapjait az Európai Unió és NATO-s szabványok alkotják;
- a távközlési hálózatok védelmére csak speciális eszköz alkalmazható melyet a 161/2010. (V. 6.) Korm. rendelete a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól és a 2009. évi CLV. törvény a minősített adat védelméről, 90/2010. (III. 26.) Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének (jogszabályi hivatkozás) jogszabályok írják elő;
- az iratkezelő szoftvernek a 24/2006. Kormányrendeleten túlmenően a hatósági követelményeknek is meg kell felelnie;
- kiemelt fontosságot kapott az adatok áramlási szabályozása, mely szerint a különböző minősítésű rendszerek összekapcsolása rendkívül erős szabályozás alá esik;
- az adatmegismerés szabályozását a nemzetbiztonsági ellenőrzések és betekintői engedélyek határozzák meg;
- adatok fizikai védelmét a 2009. évi CLV. törvény a minősített adat védelméről írja elő, amely nagy pénzügyi terhet ró a felhasználó szervezetekre a fizikai elhelyezésekkel és az adatok tárolásával kapcsolatos követelmények miatt;
- a legnagyobb probléma az elektronikus kisugárzás elleni védelem érdekében hozott TEMPEST követelmények teljesítése.

## **2.7. A távközlő hálózatok védelmére alkalmazott eszközök bemutatása, nyílt hálózaton történő minősített adat továbbítása esetén**

Ma kormányzati szinten és szűkítve a BM és ágazati szerveire, a távközlési hálózatok védelmére, nyílt hálózaton történő minősített adat továbbítása esetén, rejtjelezni kell az adatot. „A rejtjelzés minden olyan tevékenység, eljárás, amelynek során valamely minősített adatot abból a célból alakítanak át, hogy annak eredeti állapota a megismerésére illetéktelenek számára rejtve maradjon és ennek következtében a minősített adat minősítés nélkülként kezelhető legyen, valamint a rejtjelzett adat eredeti állapotba történő visszaállítása.”[8] Ez egy kulcspár alapon működő eszköz, melyet utoljára 2004-ben fejlesztettek tovább. Egy új eszköz gyártásához és forgalmazásához speciális rendszer engedély szükséges (NBF), melynek eredményeképpen az eszköz jelen igen drága. A jelenlegi technológiai feltételek korlátozzák a tömeges gyártást, mint például a laboratóriumi körülmények, manufaktúráis előállítási lehetőség, korlátozott darabszám, nagy hibaszám a gyártás során az egyedi alkatrészek miatt. A jelenleg fejlesztett prototípust az NBF még csak ideiglenesen engedélyezte, ezért rendszerbe még csak ideiglenesen állítható.

A jelenleg rendszeresített eszköz hálózati szempontból nehezen illeszthető a 21. századi számítógépes hálózatokba, elmaradott technológiával és technikával, rendszerelemekkel működik. Kulcsanyagait az Információs Hivatal generálja minden egyes alkalmazó szervezetnek. Az eszköz a tűzfal tekintetében kiválóan alkalmazható, mert igen szigorú informatikai biztonsági követelményeknek felel meg.

Összefoglalóan elmondhatom, hogy jelenleg Magyarországon nem létezik, a felhasználói igényeket teljes mértékben kielégítő, biztonságosan működő és engedélyezett rejtjelző eszköz.

## **2.8. TEMPEST-ről és a követelményeinek teljesítése**

„A TEMPEST követelmények: a „Bizalmas!” vagy magasabb minősítési szintű adat bizalmasságának védelme érdekében kialakított biztonsági intézkedések – amelyek kiterjednek az elektromos és adatkábelek vonalvezetésére, a rendszer környezetében alkalmazható berendezésekre, árnyékolástechnikai megoldásokra, valamint csökkentett kisugárzású eszközökre – együttese, amelyet a rendszer valamennyi eleme vezetett és elektromágneses kompromittáló kisugárzásának csökkentése érdekében alakítottak ki.” [8]

Ez gyakorlatban azt jelenti, hogy a TEMPEST követelmények kiterjednek a rendszer környezetében alkalmazható berendezésekre, elektromos árnyékolástechnikai megoldásokra, csökkentett kisugárzású hardver eszközök alkalmazására, az építészeti, épületgépészeti, épületvillamossági, valamint a rendszerhez tartozó vagy a rendszer környezetében található fém berendezések földelésére. A NATO- és EU által meghatározott paraméterek szerint zónákban sorolják az eszköz elhelyezési körletét, és az ott meghatározottak szerint védelmi intézkedéseket kell tenni. Például be kell tartani a megfelelő védőtávolságot, a minősített adatkezelésre kijelölt helyiségek elektro-mágneses árnyékolását kell elvégezni rézháló, vagy speciális festék, vagy védőfólia alkalmazásával a falakon és az ablakokon.

További védelmi intézkedésként alkalmazható a TEMPEST eszközök beszerzése (NATO SDIP 27 előírásai alapján Level A, B, C szabványoknak megfelelő eszközök). A legtöbb esetben viszont a fentebb említettek kombinációs megoldások a legcélravezetőbbek.

## **2.9. Akadályozó tényezők az elektronikus minősített ügyiratok küldésével kapcsolatban**

Mint már említettem a legnagyobb gondot az elektronikus ügyintézés során a minősített ügyiratok küldése okozza. Alapvető problémát jelent, hogy jelenleg nem rendelkezünk



online IP rejtjelező eszközzel, mely az NBF rendszeresítési engedélyével és megfelelő sávszélességgel rendelkezne. Tovább vizsgálva az informatikai feltételrendszert megállapítottam, hogy olyan elektronikus iratkezelő rendszer, mely jelenleg minősített elektronikus ügyiratokat kezelne (azaz NBF rendszerengedéllyel rendelkező szoftver) nem rendelkezik a BM és ágazati szervezetei. Rendszerengedéllyel rendelkező szoftvert találtam, az RZS NEO személyében, amely iktatásra alkalmas az engedély szerint, de ügyiratkezelésre (irat elektronikus tárolásra) nem. További problémát okozott a hitelesítés és az elektronikus aláírás problémája. Ugyanis a Biztonsági Hitelesítési Szolgáltató hiányzik. Kormányzati szinten működő, bizalmas pozíciót betöltő személyek részére kibocsátható elektronikus aláírás, mely hiteles, harmadik féltől származik, és nem a versenyszféra valamelyik szolgáltatója által kerül kiadásra jelenleg hivatalosan nem létezik.

Ennek megoldására, véleményem szerint olyan egységes, díjmentesen (minden tekintetben, beleértve az eszközök bérleti díját is) használható kormányzati infrastruktúrára lenne szükség, mely a felhasználási végpontokig kiépítésre kerülnének.

Ennek érdekében megvizsgáltam az EKG alapszolgáltatásai között szereplő időbélyeges szolgáltatást, és azt tapasztaltam, hogy alkalmazása nehézkes vagy lehetetlen felhasználása elektronikus minősített adat tekintetében.

Mindezeket összefoglalva, ha a rendőrség által fejlesztett RZS NEO-t alkalmassá is tesszük minősített adatok elektronikus ügyiratkezelésére, és engedélyt is kap a megfelelő felügyelő szervezettől, még mindig problémát jelent a megfelelő rejtjelező eszköz végleges engedélyezése (akár külföldi is) a nemzeti minősített adatok rejtjelezésére. Megoldási lehetőségként számba vettem a jogszabály módosítást is a minősített adatkezelés tekintetében, a TEMPEST követelmények alkalmazására. De ez csak úgy lehetséges, ha az adatok minősítése során átminősítést alkalmazunk, amely már veszélyeztetheti is az adat tényleges kezelését, ezért ezt a lehetőséget elvettem.

### **3. AZ ELEKTRONIKUS ALÁÍRÁS ALAKALMAZÁSÁNAK LEHETŐSÉGEI A RENDŐRSÉGNÉL**

#### **3.1. Normatív megoldási javaslat**

Az elektronikus aláírásról szóló 2001. évi XXXV. törvény (a továbbiakban: Eat.) már tíz éve megteremtette az elektronikus aláírás lehetőségét. Az elektronikus aláírás elsősorban dokumentumkezelési, ügyviteli, nem pedig informatikai kérdés, ugyanakkor nagy lépés, tekintettel arra, hogy az elektronikus aláírással kiválthatja a papírt.

A BM-on belüli és az ágazati szervekkel történő iratforgalom tetemes mennyiségére is tekintettel időszerű az elektronikus aláírás feltételrendszerének kialakítása. Ezen indokok figyelembe vételével a KIM és az NFM munkatársaival való egyeztetést követően a BM-on belüli elektronikus aláírás feltételrendszerének kialakítását kezdte meg a BM. Miután a rendőrségen keletkezik a legtöbb irat arányaiban véve a BM ügyiratforgalmát, ezen a területen kezdtem meg az elektronikus aláírás alkalmazásának lehetőségének vizsgálatát.

Az alábbi vizsgálat pontokat vettem alapul:

1. Elsődleges pont elektronikus aláírásra vonatkozó jogszabályok körének meghatározása:
  - 93/1999. EU Irányelv,
  - az elektronikus aláírásról szóló 2001. évi XXXV. tv. (Eat.),
  - az elektronikus aláírás közigazgatási használatához kapcsolódó követelményekről és az elektronikus kapcsolattartás egyes szabályairól szóló 78/2010. (III.25.) Kormányrendelet,

- az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes körülményekről szóló 3/2005. (III.18.) IHM-rendelet,
  - a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről szóló 2/2002. (IV.26.) MeHVM irányelv.
2. Második pont a minősített elektronikus aláíró biztonsági tanúsítványt kibocsátó cég megléte. Magyarországon jelenleg három olyan szakértő működik, aki a gyakorlatban elektronikus aláírással kapcsolatos szakvéleményeket készített, és egyetlen olyan szakértő van, aki több mint 10 magyar szakvélemény referenciával rendelkezik. A kérdést megvizsgálva, azt tapasztaltam, hogy két tanúsítványt kibocsátó szervezet áll jelenleg rendelkezésre az államigazgatásban. Az egyik a MÁV Informatikai INFORMATIKA Zrt.-n (a továbbiakban: MÁVI), a másik, amely tanúsítványokat ugyan adhat ki, azonban ez nem a szervezet jelenleg nem működik. A Kopint-Datorg Zrt. (jelenleg NIS), mint a kormányzat teljes értékű informatikai üzemeltetője – figyelemmel arra, hogy érdekelt ebben a tárgykörben – felmérte a lehetőségeket, az idő- és pénzigényt, és ezért felötlött benne a gondolattal, hogy saját minősített kormányzati szolgáltatót állítson fel, akár egy létező szolgáltató (MÁVI) átvételével, miután a MÁVI már megvalósított a rendszert működtet. Tanulmányoztam a MÁVI működését, és a jelenlegi feltételek, a jelenlegi szakmai működési színvonala szakmaiság megteremtése a MÁVI-nál kb. 7 évet vett igénybe. Ez a tevékenység, melyet a MÁVI folytat, folyamatos, állandóan végzendő tevékenység. Így meg kellett állapítanom, hogy a MÁVI-n kívül jelenleg nincs reális lehetőség az államigazgatásban új független, költséghatékony minősített tanúsító szervezet létrehozására.
3. Harmadik pont az iratok minősítési szintjének kérdésköre. Megállapítottam, hogy a fokozott minősítési szintnek nincs értelme a rendőrség tekintetében, mivel a rendőrség a teljes bizonyító erőt alapértelmezettnek tekinti a maga számára használható dokumentumok esetében, amit csak a minősítettnek rendkívül szigorúak a követelményeknek megfelelő minősített aláírás teljesíti. Véleményem szerint, az adatok támadási célértéke magasabb, mint egy bank esetén, ezért a fokozott minősítési szint – a tanúsítványok szoftveres jelenlétének lehetősége miatt – erősen ellenjavalltnak tartom.
4. Negyedik pont az ellenőrzés. A MÁVI-t elemezve azt tapasztaltam, hogy a minősített elektronikus aláíró szervezetnél négy-szintű az ellenőrzés, belső és külső oldalon.
- A két belső ellenőrzés:
- a vezetői kontrollt jelenti,
  - az évenkénti minőségirányítási és informatikai ellenőrzést, amely belső minőségügyi és IT biztonsági auditálást jelent. A rendszer megteremtése erre a szintre (folyamatosan ellenőrzött minőségirányítási és információbiztonság rendszer) meglehetősen nehéz, és a szint fenntartása is folyamatos munkát igényel.
- A két külső ellenőrzés:
- évente szakvélemény készítése, amelyhez a szakértő begyűjti az evidenciákat (az előző évi auditálás, a pénzügyi garanciák, az ügyfelekkel való bánásmód, a jogszabályoknak való megfelelés, a megvalósulás mélysége, stb.). elkészíti szakvéleményét és megküldi az NMHH részére,
  - az NMHH a szakvélemény figyelembe vételével vizsgálja a jogszabályoknak való megfelelést, és évente helyszíni szemlén győződik meg a szolgáltató működéséről.

Egy ötödik szint is megemlítenék, mivel a jogszabályok szerint az NMHH felett EU-s ellenőrzés is megjelenhet.

5. Ötödik pont az egységesítés. Ahhoz, hogy a rendőrségen megvalósuljon az elektronikus aláírása, ahhoz az egységes kormányzati információ-rendszerbe tartozó alegységként, tanúsítvány-kibocsátói szinten logikai, regisztrációs szinten pedig fizikai elkülönüléssel kell a BM-nek a minősített elektronikus aláírás készítésére feljogosító tanúsítványok kibocsátását, használatát végrehajtania. Jelenleg is működnek elkülönült alegységeket működtető minősített elektronikus aláírás szolgáltatók. Ennek a kormányzatban kihasználható előnye, hogy egy új szerv csatlakozása némi hardver-bővítéssel és üzemeltetési oktatással megoldható. Ugyanakkor a tanúsítványok menedzselése ebben az esetben is komoly humán-erőforrás menedzsmenetet igényel a kibocsátó szerv részéről, hiszen nem megengedhető az, hogy egy megszűnt munkaviszonnyal rendelkező dolgozó az aláírást használva megtéveszthesse az aláírását fogadókat, amennyiben a fogadói oldal nem készült volna még fel kellő módon az aláírások ellenőrzésére.
6. Hatodik pont az oktatás. Rendkívül nagy hangsúlyt kell a bevezetés során az oktatásra fektetni. Az oktatás keretében az European Computer Driving Licence (ECDL) operációs rendszer és az internet ismeretét kell előtérbe helyezni. Az ismeretek körét úgy kell kialakítani, hogy bármely elektronikus aláírást használó informatikai rendszerben alkalmazhatók legyenek a jövőben is, úgy hogy a hiteles digitális kommunikációjának megteremtésén kívül a magyar és európai információs társadalomban a szükséges informatikai írástudás szintjének erőteljes növekedését is biztosítja.

Összefoglalva a célokat egységesíteni kell, célirányosan kell az anyagi források csoportosítani. Az elektronikus aláírásról szóló törvény alapján saját elektronikus aláírás szolgáltatót kell üzemeltetni és állami hitelesítési szolgáltatót kell felállítani.

Nem egyedi fejlesztés keretében kerüljön a rendszer kialakításra, hanem már működő megoldás kerüljön megvásárlásra, beszerzésre. Feleslegesnek egy olyan rendszer kifejlesztése, mely már létezik, és valószínűleg olcsóbban megvásárolható.

### **3.2. Az elektronikus ügykezelés megvalósításának lehetőségei a rendőrségnél**

Három területen alkalmazható az elektronikus ügyintézés és egyben az elektronikus aláírás a rendőrségnél.

- a) a nyílt adatok feldolgozása és továbbítása;
- b) a nem nyilvános, szenzitív adatok továbbítása és feldolgozása;
- c) a minősített adatok feldolgozása és továbbítása (az államtitokról és a szolgálati titokról szóló 1995. évi LXV. törvény alapján).

Magyary Zoltán Közigazgatás-fejlesztési Programban meghatározottak szerint az elérendő célként határozta meg a rendőrség, hogy

- a) a nyílt adatok feldolgozza és továbbítása, a kormányzat elektronikus ügyintézés vérkeringésében részt vállalva, megvalósítja az elektronikus úton tehető bejelentést, és az elektronikus tájékoztatását a közvéleménynek;
- b) a nem nyilvános, szenzitív adatok továbbítása és feldolgozása, ügyiratkezelés a rendőrség szervezetei között, a rendőrség hálózatán, elektronikus aláírás és hiteles időpecsét alkalmazása, a papírmentes iroda megalkotása;
- c) a minősített adatok feldolgozása és továbbítása (az államtitokról és a szolgálati titokról szóló 1995. évi LXV. törvény alapján) a rendőrség és a BM ágazati szervezetei között, az e-szolgálati jegy projekt megvalósítása, elektronikus ügyintézés, és a szervezetek egymás közötti aláírásának elfogadása.

A felhasználó szervezetek tekintetében keletkező feladatok nagysága és mértéke erősen függ a választott műszaki megvalósítástól, így centralizált vagy decentralizált rendszerről beszélhetünk. A centralizált rendszer esetén meg kell vizsgálni, hogy van-e lehetőség távolról elektronikus aláírás igénylésére és kiállítására, a decentralizált rendszer esetében ez evidens, hogy rendelkezésre áll.

A rendőrség esetében egyértelműen a centralizált rendszerről beszélhetünk csak. Miután a szervezeti felépítés tekintetében és a hierarchiája miatt központosított az informatikai hálózat, így egyetlen megoldás jöhet csak szóba az elektronikus ügykezelés és az elektronikus aláírás szempontjából, az RZS NEO rendszer. Ezt a rendszert alkalmazza a rendőrségnek minden szervezete nyílt ügyiratkezelésre, és a hálózat minden szegmenség megtalálható. Ahhoz, hogy az elektronikus ügykezelés megvalósuljon, teljes egészében az ügyiratokat hitelesíteni kell, aláírással kell ellátni, és időpecsétet kell hozzá generálni. Melyre jelenleg is képes rendszer, de nem rendelkezik NBF általi engedéllyel. Ehhez egy központosított hitelesítés szolgáltatót kell létre hozni a rendőrségen belül.

A hitelesítési szolgáltatónak kell végrehajtania az egységes jogszabályi feltételek biztosítása, egységes eljárások kialakítása (pl.: eljárási rend, hitelesítési rend, általános szerződési feltételek, stb.) és egy helyre koncentrált humán- és anyagi források koncentrállása céljából. Az aláírás tekintetében az alábbi tevékenységeket (vagy azok valamelyikét) hajthatják végre a rendszerben:

- a) minősítésre javasoltak;
- b) minősítettek;
- c) kiadmányoztak.

Megvizsgáltam a megvalósíthatóság érdekében a küldő auditálló, hitelesítő alkalmazásának lehetőségét is. A „külső” auditálásnak - figyelemmel a jelentős pénzügyi és humán erőforrás szükségletére is - akkor van értelme, ha minden szervezet azonos szinten elfogadja, ha minden szervezetnek azonos szinten és területen van rá igénye, ha megtérül, és ha felkészül minden szervezet bevezetésére és fenntartására.

Véleményem szerint a belső auditálást kell alkalmazni, melyre a rendszer lehetőséget ad. A törvények által előírt iratkezelési feltételek jelenleg is adottak az elektronikus ügykezelés során. A bevezetés tekintetében viszont több lépcsőben határoznám meg alkalmazását a rendszer által generált tanúsított elektronikus aláírásnak:

- 1) elsődleges célterületként a belső levelezés szintjén elfogadható megvalósítást kell tekinteni;
- 2) második célnak kell tekinteni a RZS belül a teljes ügyiratkezelést a szervezetek között;
- 3) harmadik célként kell megfogalmazni a BM ágazati szervezetei közötti elektronikus ügykezelést. Melynek teljes értékű feltétele egymás között azonos szinten értelmezett és elfogadott elektronikus hiteles aláírás és időpecsét.

Felméréseket folytattam le a rendőrségnél az érintett területek személyvonzatainak tekintetében és megállapítottam, hogy kb. kétezer főt érint a kiadmányozás, az elektronikus belső aláírás kb. negyvenezer főt.

### 3.3. A megvalósítás akadályai

Az alkalmazható UNIX, NETLOCK, ORACLE szoftverek rendkívül költségesek. Költségkímélőbb megoldásnak tartom a Microsoft licenz vásárlását, azonban ez ennek alkalmazása nem problémamentes. Viszont ennek a köztes állapotot jelentő „belső” auditálás megoldás mellett az elektronikus aláírásra feltétlenül szükség van.

Megvizsgáltam néhány műszaki követelményt. Különösen az alábbiakat emelném ki az elektronikus aláírás alkalmazhatóságánál:

- a) az időbélyegnél, egy másodpercnél nagyobb eltérés nem megengedett;
- b) ehhez kapcsolódik egy naponta többszöri ellenőrzés, amely azt is jelenti, hogy amennyiben helyesbítésre van szükség, azt is naplózzák;
- c) a szakértő szűrőpróba-szerűen ellenőrzi ezt a többszörösen biztosított folyamatot;
- d) 25 napról, az eszköz 1 mp-nél nagyobb eltérés esetén automatikusan leállítja az időbélyegeg kiállítását – ezt a rendszer szintén naplózza, ami ellenőrizhető.

### 3.4. Hibrid rendszerek alkalmazásának lehetőségei

A belügyi szerveket összekötő egyik alkalmazási terület az NBSZ-től mint szolgáltatótól megkért (titkosszolgálati) szolgáltatások témaköre. Az NBSZ az Új Magyarország Fejlesztési Terv keretében megvalósítás alatt álló „Biztonságos elektronikus összeköttetés kiépítése” című projektjében (a továbbiakban: eSzolgálati Jegy Rendszer /eSZJR/) egy zárt hitelesítési szolgáltatást állít fel, melynek a jogi háttérét a 2001. évi XXXV. törvény 1§ (2) bekezdése és a 78/2010. (III. 25) Kormányrendelet 6§ (1)-es és (2)-es bekezdései biztosítják. Ennek eredményeképpen az alkalmazott elektronikus aláírás a zárt felhasználói csoport tekintetében hitelesnek tekintendő. Az elektronikus aláírások használata az elektronikus minősített adatok tekintetében is felhasználhatóak, ezzel kihasználva a 2009. évi CLV. törvény – és annak végrehajtási rendeletei – által biztosított lehetőségeket, továbbá teljesítve annak követelményeit.

De ennek a hibrid alkalmazásnak egyik gátja a 161/2010. (V. 6.) kormányrendelet 22-es § II. bekezdése mely szerint „a rendszer védelmét a rendszeren a rendszerengedélyben meghatározott legmagasabb minősítési szintnek megfelelő fizikai biztonság kialakításával kell biztosítani.” Ez komoly problémát jelent a különböző szintű szervezetek között. Egy adott helyszínen belül eltérő minősítésű adatok kezelése a rendszere különböző elemei oly módon kerülnek megvalósításra, hogy a rendszerelemek vonatkozásában az azokon kezelt legmagasabb minősítésű adatoknak megfelelően fizikai és informatikai továbbá tempert követelmények megvalósíthatóak legyenek. Erre két megoldási javaslat van:

- a) jogszabály módosítás,
- b) nagyobb rendszerek kisebbekre való feldarabolása, jogszabálynak megfelelően történő összekapcsolása (pl. munkaállomásonként szét kell választani: 160 db külön rendszer, külön rendszerengedély, a központra és minden egyes munkaállomásra.).

## ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Elemzéseim során bemutattam a magyarországi e-kormányzatot és rámutattam, hogy a rendőrség egyik legfontosabb célja szervesen kapcsolódni az e-kormányzat tevékenységeihez. Amint láttuk az elektronikus ügyintézés már meg is tette az első lépéseket ez irányba. Az elektronikus ügyintézés alapja a biztonságos rendszerek környezet és a védett hálózat. Az elektronikus ügyintézés és ügykezelés alapvető feltétele a hitelesített elektronikus aláírás és az időpecsét. Az elektronikus aláírás alkalmazása a rendőrségnél a felelősségi rendszer nagyon erőteljes. Az ellenőrzés szintjeinek megsokszorozítása azt is eredményezik, hogy olyan működési zavart okozó szabálytalanság nem történhet, amelyekre nem tud reagálni az előírt 3 órán belül egy minősített hitelesítés szolgáltató, jelent esetünkben a rendőrség. Amennyiben egy nagyobb incidens feltételezésem szerint bekövetkezne, a felelősség nyilvánvaló módon megállapítható lenne, amely egyben bizalomvesztést is eredményezhet az egész világon a magyar PKI-rendszerek iránt. Három területen alkalmazható az elektronikus ügyintézés és egyben az elektronikus aláírás, mint feltétel a rendőrségnél.

- a) a nyílt adatok feldolgozása és továbbítása;

- b) a nem nyilvános, szenzitív adatok továbbítása és feldolgozása,
- c) a minősített adatok feldolgozása és továbbítása (az államtitokról és a szolgálati titokról szóló 1995. évi LXV. törvény alapján).

Azt a célt kell megvalósítani, hogy a papír alapú ügymeneteket elektronikus ügymenetekre alakítsuk át mind három területen, ennek egyik pillére a hiteles elektronikus aláírás és az időpecsét együttes alkalmazása, melyet a RZS NEO rendszerrel kell alátámasztani.

### FELHASZNÁLT IRODALOM

- [1] 1126/2003. (XII. 12.) Korm. határozat
- [2] 1188/2002. (XI. 7.) Korm. határozat
- [3] Trans European Services for Telematics between Administrations
- [4] Hungarian Security Network
- [5] Interchange of Data between Administrations, Közigazgatási szervezetek közötti adatcsere
- [6] <http://www.meh.hu/szervezet/hivatalok/ekk/ekk/alap.html> 2004. október 8.,
- [7] E-KORMÁNYZAT 2005 - E-KORMÁNYZAT STRATÉGIA ÉS PROGRAMTERV  
<http://www.meh.hu/szervezet> 2005.11.20.
- [8] A Kormány 161/2010. (V. 6.) Korm. rendelete a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól
- [9] Négyesi Imre: Az elektronikus aláírás lehetőségei a Magyar Honvédségben I. (Nemzetvédelmi Egyetemi Közlemények, 11. évfolyam/3. szám (2007), 110-121. oldal, ISSN 1417-7323);
- [10] Négyesi Imre: Az elektronikus aláírás lehetőségei a Magyar Honvédségben II. (Nemzetvédelmi Egyetemi Közlemények, 11. évfolyam/3. szám (2007), 122-137. oldal, ISSN 1417-7323);

**Szalai Máté – Pándi Erik**  
szalai.mate@zmne.hu, pandi.erik@zmne.hu

## EGY RENDSZERGYAKORLAT TAPASZTALATAI

### *Absztrakt*

*2011. április 26-29. között a Híradó Tanszék szervezésében híradó és informatikai rendszergyakorlat került lebonyolításra a harmad- és negyedéves híradó specializációjú tisztjelöltek,<sup>25</sup> a tanszék oktatói állományának, valamint az MH Támogató Dandár személyi állományának bevonásával. A rendszergyakorlat alapvetően nem háborús katonai művelet híradó és informatikai támogatását tűzte ki célul, így e peremfeltétel mellett került kiépítésre a vezetés-irányítást támogató technikai (kommunikációs) rendszer. Mindezek figyelembevételével jelen publikációban röviden összefoglalásra kerülnek a megszerzett tapasztalatok és megállapítások.*

*This article shows experience of signal training in ZMNDU.*

**Kulcsszavak (key words):** *híradó és informatikai rendszer, gyakorlat Híradó Tanszék ~ CIS, training, Signal Department*

### BEVEZETÉS

A Híradó Tanszék nem rendelkezik mobil tábori híradó és informatikai rendszerelemekkel, azok csak beépített formában találhatók meg szakkabineti rendszerben. Ilyen szakkabinetek az R-142, kisztrádiós, Hicom (Hipath), mikrohullámú tantermek, amelyek természetesen párosával találhatók meg az oktatási egységnél. Ebből kifolyólag gyakorlati képzésre tábori körülmények között nincs lehetőség.

A távközlés és informatika területének konvergenciája teljesen nyilvánvaló tény napjainkra, amely megmutatkozik az általam vizsgált ázsiai és balkáni hadműveleti területeken is, hiszen a magyar kontingensek mindkét helyszínen alkalmaznak integrált híradó és informatikai központokat (HIK) konténeres kivitelben. A konvergencia hatása a tanszéki tananyagban is megjelent, hiszen a 2010/11. tanévtől kezdődött meg a CISCO Hálózati Akadémia CCNA Discovery D1-D4 programjának fakultatív oktatása, amely korszerű IP alapú hálózati ismereteket kínál a hallgatóknak. A program a 2011/12. tanévtől már részét képezi a katonai távközlés, valamint a katonai információbiztonság specializáció tanmenetének.

Hazánk szerepvállalása elsősorban a nem háborús katonai műveletek irányába tolódik el, elsősorban zászlóalj, esetlegesen dandár erejű kötelékek igénybevételével. Ez a tendencia megmutatkozott a híradó szakharcászati ismeretek harmad- és negyedéves tananyagában is, hiszen a szervezési elveket elsősorban dandár szintig sajátítottuk el, többségében védelmi jellegű műveletek keretében.

---

<sup>25</sup> Harmadévesek: Gömör Marianna, Kátai Dániel, Lukács Kornél, Nagy Balázs. Negyedévesek: Bodnár István, Koncz Bence, Szalai Máté.

Tekintettel a megváltozó a katona-politikai és technológiai környezetre, valamint arra a tényre, hogy több éve nem volt lehetőség a hallgatói állomány elméleti szakmai tudását próbára tevő rendszergyakorlat lebonyolítására, ezért az oktatási egység elhatározta – *alapvetően* – saját intellektuális és technikai kapacitásainak igénybevételeivel megvalósuló gyakorlás végrehajtásának megszervezését. Tekintettel a hallgatói létszámok adottságaira, a gyakorlaton három fő negyedéves és négy fő harmadéves tisztjelölt vett részt.

### 1. A FELADAT

A feladat megfogalmazására a *Híradásszervezés* tantárgy keretében került sor több mint egy hónappal a gyakorlat megkezdése előtt. Az elméleti harcászati feladat egy lövészdandár békeműveletét irányozta elő, szervezetében három alárendelt lövésszázlóaljjal. A gyakorlati végrehajtás során tervezni dandár fő- és mögöttes harcálláspont, valamint egy zászlóalj figyelő-harcálláspont híradó és informatikai központtal kellett. Ezek mellett a zászlóalj alárendeltségében egy-egy ellenőrző-áteresztő pont (EÁP) létesült.

A híradás és informatika rendszerét úgy kellett megtervezni, hogy a vezetés-irányítást a híradó és informatikai rendszer minden hagyományos és korszerű szolgáltatása kiszolgálja az alábbiak szerint:

- Távbeszélő szolgáltatás (ISDN, IP, analóg [CB, LB]);
- Telefax szolgáltatás (analóg);
- Videokonferencia szolgáltatás;
- Elektronikus levelező (adatátviteli) szolgáltatás;
- Internet szolgáltatás;
- Intranet szolgáltatás;
- Harcászati URH és RH rádiókommunikációs szolgáltatások;
- Harcászati adatátviteli szolgáltatás;
- EDR rádiókommunikációs szolgáltatás;
- URH belső rádiókommunikációs szolgáltatás;
- Videó (térfelügyelő) szolgáltatás.

A vezetési pontokat oly módon kellett megtervezni, hogy a dandár főharcálláspont híradó és informatikai központ tantermekben települjön, a mögöttes harcállásponté az MH Támogató Dandár által biztosított HIK/G központban, valamint a zászlóalj figyelő-harcállásponté sátrakban. Az EÁP-ok szintén sátrakban települtek.

A fő- és mögöttes harcálláspontok VSAT műholdas átviteli úton csatlakoztak egymáshoz közvetlenül, mivel a mögöttes vezetési pont alapvetően az MH stacioner hálózatába került integrálásra. A főharcálláspont az egyetemi állandó kommunikációs rendszeren keresztül került kapcsolatba a stacioner hálózattal. A távbeszélő és fax szolgáltatások HM mellékek révén testesültek meg. E-mail szerver hiányában az egyetem infrastruktúrája biztosította az elektronikus fiókokat, amelyeket webes (Internetes) felületen keresztül lehetett alkalmazás alá vetni.

A főharcálláspont, valamint a zászlóalj vezetési pont egy TDR-15/2 Mbps mikrohullámú berendezéssel, valamint egy WiFi vezeték nélküli eszközzel került összekapcsolásra. Az első biztosította a dandár vezetési ponton települt Hicom távbeszélő alközpont, valamint a zászlóalj vezetési ponton települt CISCO VoIP távbeszélő alközpont közti kapcsolatot, amíg az utóbbi a VLAN-ok és a HM mellékek (VoIP) kialakítására szolgáltak. A videokonferencia szolgáltatás igénybevétele VSAT műholdas átviteli út állt rendelkezésre.





1. sz. ábra: VSAT műholdas parabola antenna [1]

A főharcálláspont, valamint a zászlóalj vezetési pont egy TDR-15/2 Mbps mikrohullámú berendezéssel, valamint egy WiFi vezeték nélküli eszközzel került összekapcsolásra. Az első biztosította a dandár vezetési ponton települt Hicom távbeszélő alközpont, valamint a zászlóalj vezetési ponton települt CISCO VoIP távbeszélő alközpont közti kapcsolatot, amíg az utóbbi a VLAN-ok és a HM mellékek (VoIP) kialakítására szolgáltak. A videokonferencia szolgáltatás igénybevételére VSAT műholdas átviteli út állt rendelkezésre.

A zászlóalj híradó és informatikai központban a CISCO VoIP távbeszélő alközpont mellett egy analóg K-12 alközpont is települt, amely a CB melléke révén átjárást biztosított az analóg és digitális technológia között. A K-12 alközpont biztosította a távbeszélő szolgáltatást az EÁP-ok számára. A dandár vezetési pont a K-12 alközponton keresztül kapcsolatba léphetett az EÁP személyi állományával és viszont. A dandár mögöttes vezetési pontja HM mellékek útján tudott kapcsolatba lépni a zászlóalj vezetési pontjával. A mikrohullámú és műholdas kapcsolatokon keresztül tehát a zászlóalj vezetési pontján biztosítottá váltak a különféle távbeszélő, fax, Internet és Intranet, e-mail és videokonferencia szolgáltatások.

A harcászati rádiórendszerek irányokban és hálóban kerültek megszervezésre. Ezekben felhasználásra kerültek a korszerű MRR és HARRIS rádiók, valamint az R-111 és R-130-as rádiókészülékek. Az analóg rádióeszközök alapvetően távvezérléssel kerültek alkalmazásra, mind a dandárnál, mind a zászlóaljnál. Az EÁP-okon MRR rádiók kerültek telepítésre, annak érdekében, hogy ki lehessen használni adatátviteli képességeiket egy migrációs feladat végrehajtása során, amikor az ellenőrzött adatokat, illetve digitális fényképeket kell a zászlóalj vezetési pontra megküldeni további feldolgozásra.

Az őrzés-védelmi, valamint felderítő feladatok hatékonyabb ellátása érdekében telepített IP kamera a zászlóalj vezetési ponton került bekötésre, amelynek videó jelfolyama az Internet, illetve Intranet szolgáltatásokon keresztül megosztható volt a dandár fő- és mögöttes harcállásponton is.



A harmadik napon a rendszergyakorlat különböző manőverek végrehajtásával folytatódott, amelynek keretében – *többek között* – frekvenciaváltásra, összeköttetések és szolgáltatások megszakadásának modellezésére, majd hibaelhárításra, valamint különböző bemutatók megtartására került sor.

A negyedik napon megtörtént a híradó és informatikai rendszer bontása, majd a kommandáns tevékenységek végrehajtása és lezárása. A gyakorlat utóélete során anyagkarbantartásra is sor került.

A rendszergyakorlat során a dandár főharcálláspontján, valamint a zászlóalj figyelő-harcálláspontján mindvégig híradó és informatikai ügyeletes tevékenykedett, végezve szak- és adminisztratív feladatát.

## ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Megítélésünk szerint a tanszék által megtervezett és lebonyolított gyakorlat jól modellezte a nem háborús szárazföldi katonai műveletek során a híradás és informatika témakörében alkalmazandó eljárásokat és módszereket.

A rendelkezésre álló technikai erőforrások tükrében lényegében sikerült minden olyan szolgáltatást biztosítani a vezetés-irányítási tevékenységek támogatása céljából, amely napjainkban korszerűnek tekinthetők. A szolgáltatásokhoz kötődő infrastruktúra, vagyis a híradó és informatikai rendszer a lehetőségekhez képest célszerűen épült ki.

A gyakorlat egyik előnyeként lehet értékelni, hogy a hallgatók számára komplex problémákat kellett megoldani, ugyanakkor megítélésünk szerint egy ilyen összetett feladat eredménye lebonyolításának előfeltétele az egyes részfeladatok (pl.: rádiókommunikáció szervezése, vagy VLAN kialakítása) előzetes gyakoroltatása. Második előnynek tekinthető, hogy elősegíti a rendszerszemlélet erősítését az összefüggések megvilágításával és megértésével. Harmadikként elmondható, hogy napjaink kommunikációs rendszereinek megtervezése, megszervezése és üzemeltetése nem képzelhető el korszerű hálózati ismeretek nélkül.

Hátrányként lehet viszont értékelni, hogy a felhasznált modern eszközpark mindegyike kevésbé alkalmas tábori körülmények közötti igénybevételre, amely megnyilvánul többek között az RJ-45 típusú csatlakozók szerszám és viszonylag bonyolult szerelési igényében, vagy a távközlő és informatikai, illetőleg irodatechnikai eszközök porral szembeni csekély ellenálló képességében. További hátránynak tartjuk, hogy a rendszer információbiztonsági kérdéseivel – *vélhetően az adottságok miatt* – csak érintőlegesen tudtak a hallgatók foglalkozni.

## FELHASZNÁLT IRODALOM

- [1] Szalai Máté által a helyszínen készített fotó
- [2] A Híradó Tanszék oktatói által összeállított és Dr. Rajnai Zoltán mk. ezds. által szerkesztett ábra
- [3] Dr. Négyesi Imre: TRAGBARE UND FELDINFORMATIK-GERÄTE I. (Tábori és hordozható informatikai eszközök I.) (Hadmérnök on-line, IV. évfolyam, (2009) 2. szám, 333-339. oldal, ISSN 1788-1919);
- [4] Dr. Négyesi Imre: TRAGBARE UND FELDINFORMATIK-GERÄTE II. (Tábori és hordozható informatikai eszközök II.) (Hadmérnök on-line, IV. évfolyam (2009) 3. szám, 355-362. oldal, ISSN 1788-1919);



bodisz@gmail.com, pandi.erik@zmne.hu

## A KOMMUNIKÁCIÓ HAJNALÁTÓL NAPJAINKIG

## Absztrakt

*Jelen közlemény szakszerűen összefoglalva betekintést ad a kommunikációs technikai világába.*

*This article shows development of world of communication.*

**Kulcsszavak (key words):** *kommunikáció, protokollok ~ communications, protocols*

## BEVEZETÉS

Az ember még a beszéd kialakulása előtt kézjelekkel, hangutánzó szavakkal próbált kommunikálni társaival. A kezdeti nem-verbális kommunikációs formák majd később a verbális beszéd és írás kialakulása segítette azt is, hogy a vadászó törzsek barlangjaitól eljussunk a mai nagyvárosi dzsungelig. Ahogy fejlődött a világ és az emberek egyre több tapasztalatra és tudásra tettek szert, úgy egyre nagyobb kommunikáló csoportok is jöttek létre. Ezen csoportok kommunikációja helyhez volt kötve, ez magyarázatul szolgál arra, hogy miért is van ma a világon olyan sok nyelv. A fejlődés első szakaszaiban törzsekről beszélhetünk később városállamokról majd országokról, birodalmakról és napjainkban földrészekről.

Ma már az egész világot behálózzák a kommunikációs csatornák, melyek a világ több milliárd emberét kötik össze egészen a föl északi részén fekvő Európától a föld déli részén fekvő Ausztráliáig vagy a jeges Antarktiszról Afrikának tűzforró egyenlítői részéig. Vagyis ma már nem jelent akadályt az, hogy a világon bármely egyén kommunikálhasson egy másik egyénnel, aki a föld ellentétes végén él, feltéve, ha adott a közös csatorna és közös jelrendszert használnak az információ cserére.

Hogyan is jutottunk el ide és milyen megoldások tették lehetővé azt, hogy elérjük ezt a fejlettséget? Először is úgy gondoljuk nem szükséges taglalni a beszéd kialakulásától az első elektromos jelátvivő készülék megjelenéséig a történéseket. Maximum egy-egy mondat erejéig annyit elmondhatunk, hogy az információ átvitelére egyre nagyobb és nagyobb távolságokat próbáltak őseink áthidalni. Ha a távolság-idő dimenzióról a fejlődés függvényében készítenénk egy grafikont, annak exponenciális alakja lenne. Kezdve a kiabáló ősembertől a füstjeleket használó indiánokon át egészen a postagalambokig.

A robbanásszerű változás az elektromosság megjelenésével kezdődött, amit a XVIII-XIX század környékére lehet tenni. Megjelenik Marconi találmánya a távíró készülék, majd Bell készüléke a telefon, mely már hang átvitelére volt képes. A fejlődési vonalban fontos megemlítenünk Puskás Tivadar telefonközpontját, mely kiküszöbölte az összekötések problémáit, mivel addig a telefonhálózatok teljes hálózati struktúrát követtek, vagyis minden telefon minden telefontalálattal közvetlenül volt összekötve (full meshed). Ezt követően inkább csak technológiai fejlődésről beszélhetünk, mely folytán megjelenik a rádió és a televízió is, közben lefolyik az I. és II. világháború és következik a hidegháború időszaka, ahol a két szemben álló fél Amerika és a Szovjetunió hatalmas technikai fejlesztésekbe kezd.

Amerikában Neumann feltalálja a számítógépet, Gróf András és csapata a mikroprocesszort és megalkotják a ARPANET-ben a számítógépek hálózatát is, melynek későbbi eredménye az Internet létrejötte. Kezdetben főleg kormányzati és katonai célokra használták az újonnan kifejlesztett dolgokat, majd jóval később a civil lakosság is beszerezhetette neki kialakított szolgáltatásokkal.

Végigtekintve az eddig említett mérföldköveket láthatjuk, hogy elég rögzített út vezetett a ma ismert digitális adatátvitelig. Ebben nagy szerepe volt az informatika fejlődésének, mivel olyan mértékű lépéseket tett, hogy húsz-harminc éve nem is gondolhattuk volna, hogy az addig ismert kommunikációs csatornáinkat felváltják a számítógépes hálózatok. Kezdvén az egyszerű szöveges adatátviteltől a hangátvitelen keresztül egészen a kép, mozgókép átviteléig.

### 1. AZ ANALÓG TELEFONTÓL A VOIP-IG

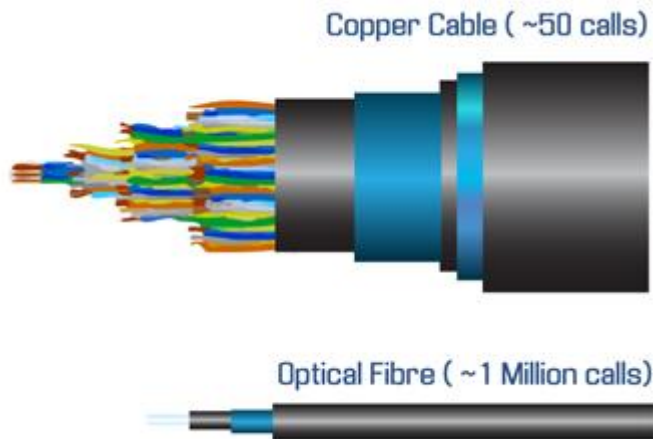
Az előzőekben említettük, hogy a feltalálók közül kinek milyen felfedező szerepe volt abban, hogy eljutottunk a ma ismert legmagasabb adatátviteli hegy csúcsára, de ne rohanjunk annyira előre, ereszkedjünk kicsit vissza arra a magaslatra, ahol a számítógépes hálózatok és a telefonos hálózatok elkezdtek egymásba fonódni. Ma már azt láthatjuk, hogy telefonálhatunk az interneten és internetezhetünk a telefonon. Még a kezdeteknél, mind a telefonos (crossbar), mind pedig a számítógépes (modemes) hálózatok kifejlesztésekor volt egy alapkoncepció, mégpedig az, hogy kapcsoljunk össze az eszközöket, eszközcsoportokat és így természetesen az embereket, embercsoportokat.

A telefonos hálózat és a hálózat részek majd kétszáz évvel korábbi találmányok, mint az internetes hálózat eszközei. Mivel az internetes hálózat a kezdetektől fogva digitális adatátvitel céljából volt kialakítva, már a fizikai rétegben eltért a telefonos hálózattól, mely analóg megoldásokra hagyatkozott és nem felelt meg az adatátviteli elvárásainak. Joggal feltehetjük azt a kérdést, hogy ma miért olvad szinte egybe a telefonos és internetes hálózat. A telefonos hálózat alapkoncepciója szinte nem változott a feltalálása óta, de jelentek meg technológiai, technikai újítások. Főleg a központoknál figyelhető meg nagy fejlődés. A manuálisan emberek által kapcsolt vonalakat később elektronikus kapcsolóközpontok vették át (Crossbar, Rotary), majd a 80-as évek hoztak egy nagy méretcsökkentést és technikai újítást a digitális telefonközpontok megjelenésével, bár a tervek megvoltak az internet világméretűvé tételére.

Az internetes hálózatok megjelenése magával hozta az IP (Internet Protokoll) fogalmát, amivel a digitális eszközök címezését oldják meg. Az IP lehetővé tette a világ több millió internetes eszközének összekapcsolását, bár napjainkban kiderült, hogy az akkor megalkotott IPv4-es szabványnak korlátai vannak a ma megjelenő IP alapú eszközök mennyisége miatt, ezért kidolgoztak több címezési megoldást, melyből a legjobbat az IPv6 jelentette. Az internetes címezés e verziójának bevezetésének folyamata jelenleg aktuális.

A legnagyobb problémát a fizikai kiépítést szerencsére még az internet nagymértékű kiépülése előtt sikerült megoldani, mivel elég költséges munka lett volna behálózni a világot az internet kedvéért, éppen kapóra jött, hogy rendelkezésre állt már a telefonhálózat, csak egy híd kellett volna, ami összekösse a két hálózatot. Az első igazi hidat az ISDN megjelenése jelentette, amely egy olyan megoldás, ami integrálja magába az analóg és digitális adatátvitelt. Lényege, hogy különböző csatornákat tartalmaz, melyből az analóg hangátvitelt, míg a digitális adatátvitelt tesz lehetővé. Ezen a digitális sávon működik a telefonvonalon keresztüli internet is, de a telefonösszeköttetések megteremtéséhez szükséges jelzések is ebben a sávban közlekednek.

A távközlési hálózatok fejlődése, vagyis inkább a felhasználói igények és az egyre bővülő szolgáltatások, magyarul a hálózatipar diktálta, hogy nagyobb és nagyobb sáv szélességet használjanak a kommunikációra. Eljutottunk odáig, hogy a hangot már digitális csatornán továbbítják, ennek az előnyéről a későbbiekben még ejtek néhány szót. Egyre-másra jelentek meg újabbnál-újabb fejlesztések egyik ilyen jelentős újítás, hogy az



1. sz. ábra: A réz kábel és az optikai kábel méret és kapacitásbeli összehasonlítása. A rézkábelben egy időben körülbelül 50 vonalat vihetünk át, míg az optikai szálon 1 millió vonalat [1]

előnyben. Az ISDN után a csomag alapú hang és adatátvitel szolgáltatások legjövedelmezőbb érdekházassága a VoIP (Voice over Internet Protokoll) lett, mely magyarul azt jelenti, hogy az eddigi internetalapú adatátviteli hálózatainkon beszédalapú szolgáltatásokat is használunk.

átviteltechnikai rendszereket lecserélték optikai adatátviteli rendszerekre, azaz a réz kábelek helyére üvegszálat húztak, mellyel együtt természetesen a hozzájuk tartozó átviteltechnikai egységeket is lecserélték. Ez mindenképp óriási mérföldkőnek számít, hiszem az üvegszálnak akkora a sáv szélessége, hogy a mai adatátviteli megoldásokkal is csak töredékét tudjuk kihasználni. Ilyen technikai háttérrel adott, hogy mind a felhasználók, mind pedig a szolgáltatók a digitális átvitelt részesítik

## 2. A CSOMAG ALAPÚ HANGTOVÁBBÍTÁSI RENDSZEREK ALAPJAI

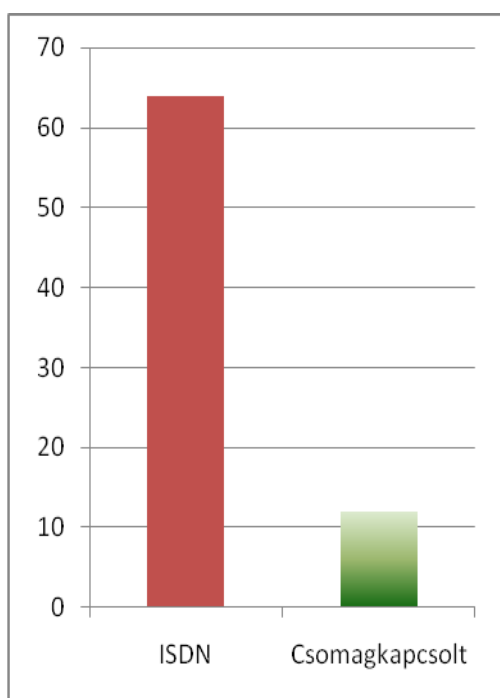
### 2.1. Csomag alapon működő hangtovábbításról általában

Egyre-másra születtek olyan digitális megoldások, melyek az analóg hálózatokat próbálták a legeredményesebben kihasználni adat, majd hangátvitel tekintetében. Közülük is a mai napig három kiemelkedő megoldást érdemes tárgyalni, ezek egyben, ahogyan nevük is mutatja a legelterjedtebb csomag alapú transzport hálózatokon valósulnak meg, mely hálózatok az OSI modell szerinti adatkapcsolati és hálózati rétegek részei:

- FR: adatkapcsolati réteg adatátviteli protokollja, adatkapcsolati kereteket továbbít, használatához be kell állítani mind a fogadó mind pedig a küldő oldalon azonos átviteli sebességet.
- ATM: adatkapcsolati réteg adatátviteli protokollja, időosztásos multiplex átvitelt biztosít, minden időrésnek fix sáv szélessége van.
- IP: hálózati réteg adatátviteli összeköttetés mentes protokollja, az adatokat apró csomagokra vágja a forráshelyen, a célhelyen pedig összeilleszti.

A nem laikusok közül joggal kérdezheti bárki, hogy az ismert transzport hálózatok, melyeknél léteznek gyorsabb átviteli biztosító megoldások is, miért nem kerültek a felsorolásba. Ésszerű magyarázatként az szolgálhat, hogy az olyan hálózatok, mint T1/J1/E1 általában bérelt vonali fizikai rétegbeli hálózati megoldások. Ezekhez a megoldásokhoz tartozhatnak vezeték nélküli megoldások, melyek között lehet akár WLAN vagy műholdas adatátvitel. Az X.25 és VBR alapú átvitelek pedig az ATM-mel szoros kapcsolatban álló adatkapcsolati réteg átviteli formái. Az IP pedig a hálózati rétegében bármelyik alacsonyabb rétegbeli hálózatnak életképes hálózati protokollja. A három, általam kiemelt transzport-hálózat mindenképp vegyíthető, és a valóságban vegyül is az utóbb említett transzport-hálózatokkal. Így természetesen, azok alkalmasak hangátvitelre is. Egyébként általánosságban megfigyelhető, hogy egy vállalati vagy legyen az akár kormányzati szint, mindig költséghatékony megoldásokat próbálnak alkalmazni a hálózatok kiépítésénél.

A fent felsorolt transzport-hálózatok mindegyikére igaz, hogy a hangadatot ugyanabban a sávban továbbítják, mint a normál adatsomagokat. Mivel egy analóg csomag 64 kbit-es állandóan fenntartott másodpercenkénti sáv szélességet igényel, addig a digitális adatsomag ennek töredékével is beéri, mely átlagosan 8-12 kbit másodpercenként és az analóggal ellentétben a csatornán hívás közben csak akkor küld adatot, ha van is információ tartalma. Mivel mindenképp teljes duplex kapcsolatról beszélünk és a szokványos kommunikációban egyszerre csak az egyik fél beszél, ezért az egyik csatornát már meg is spóroljuk. Így utánaszámolva egy csomag alapú átviteli rendszer, ha még nagyon szigorúak is vagyunk 12-



2. sz. ábra: sáv szélesség igények [2]

16-szor hatékonyabb hangátvitel szempontjából, mint a hagyományos analóg rendszer, de lazábban fogva ez a hatékonyság elérheti akár a 25-szörös értéket is. Gondoljunk csak bele mennyire is fontos ez olyan szervezeteknél, vagy vállalatoknál, ahol a kiadások nagy része telefonköltség és a telekommunikáció miatt nagyban függenek a telefonszolgáltatóktól, főleg olyan esetekben, amikor a telephelyek földrajzilag messze esnek egymástól. Számolhatunk olyan esetekkel is, amikor az analóg csatornák számánál többre van szükség, mint amennyit képes biztosítani a rendszer két végpont között.

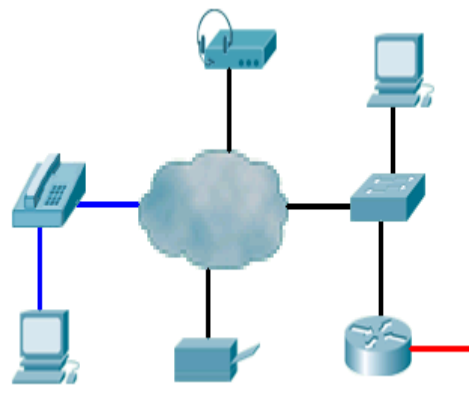
Természetesen a digitális rendszerekhez megfelelő infrastrukturális háttérre van szükség, ami egy elavult vagy alacsony fejlettségű telefonrendszereknél komoly fejlesztési költségeket jelent, mivel egy modern digitális hangátviteli rendszer csak megfelelő követelmények, előírások teljesítése mellett képes működni (QoS). Ezek hiányában romlik a felhasználói élmény és rossz hangminőséggel valamint állandóan megszakadó és zajos összeköttetéssel találkozhatunk. A csomag alapú átviteli rendszerek megfelelő technikai háttérrel rendelkeznek és képesek kielégíteni a hangátvitelhez szükséges igényeket.



## 2.2. A csomag alapú hangtovábbítási rendszerek felépítése

Egy rendszert elsőként mindig az határoz meg, hogy milyen technikai eszközökből épül fel, milyen paraméterekkel rendelkezik. A csomag alapú átviteli rendszerek felépítése hasonló a hálózatba szerveződő rendszerekhez, mint ahogyan arról már szó esett a meglévő hálózatokra épültek rá, ezért ezekhez a hálózatokhoz hasonló a hierarchiájuk. Nem célszerű visszamenni egészen az alap kommunikációs séma vázlatáig a csomag alapú hálózatok ismertetéséhez, ahol egy adóból egy vevőből és egy csatornából építkezünk, mivel ezek a rendszerek sokadik generációt képzik vagy sokkal magasabb fejlettségi szinten állnak azokhoz képest.

Azokat a hálózatokat, melyek a végpontok között helyezkednek el és transzferként működnek általában egy kommunikációs felhőként jelenítjük meg. Ebben a felhőben különböző fejlettségű, kiterjedésű és felépítésű, hierarchiájú hálózatok lehetnek. Ennek megfelelően beszélhetnénk ATM, FR és IP alapú hálózatokról. A hálózatok szélein pedig Voice Agent-eket találunk, melyek küldik és fogadják a hálózat csomagjait. A felhőből a Voice Agent-eken keresztül érkeznek a végberendezésekhez a csomagok. A végberendezés, mivel hangkommunikációról beszélünk főként telefon vagy faxkészülék, de lehet bármilyen a hálózatra csatlakoztatható eszköz a hálózat szolgáltatásainak megfelelően.



3. sz. ábra: A hálózati felhő és a hozzá kapcsolódó végberendezések [2]

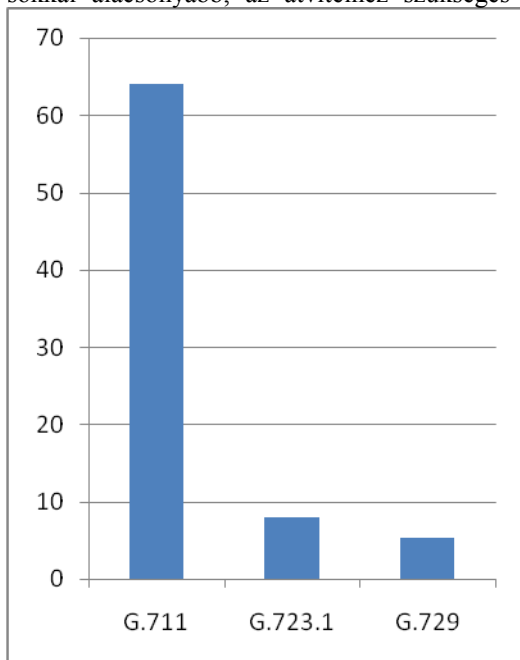
A hálózat hardveres felépítése után második rendszer meghatározó forma a rendszert vezérlő szoftverek. Fejlesztői berkekből kiindulva jól tudjuk, hogy a hardvert mindig egyszerű létrehozni főként azért, mert legtöbbször a rendszereken belül drasztikus mértékben csak egy-egy hardverelem fejlődik, de minden egyes hardverelemhez új szoftvert kell írni és ezen a szoftvereknek rengeteg funkcióját kell leprogramozni. Itt főleg azokra a szoftverekre, programokra, algoritmusokra gondolok, melyeket a hardverek chipjei tartalmaznak, de természetesen idetartoznak a hardverek háttértárain található vezérlő szoftverek, operációs rendszerek. A csomag alapú hálózatok szoftverei látják el a hangok kódolását, tömörítését, biztosítanak kényelmi funkciókat és a QoS előírásait.

## 2.3. A csomagkapcsolt hálózatokon megvalósuló kommunikáció

Egy digitális hálózaton, ahol csomag küldésére és fogadásra vannak felkészítve a rendszerek, nem tudunk analóg hangot átvinni. A digitális rendszerekben és ez már igaz volt az ISDN hálózatoknál is a végberendezések által vett hangot átalakítják digitális jelekké és természetesen az adó oldalon pedig visszaalakítják analóg jelekké. Ahhoz, hogy analóg hangból digitális jeleket tudjunk létrehozni természetesen a hangot másodpercenként több ezer részre kell osztanunk, majd ezen osztásokat leírni különböző digitális jelekkel pillanatnyi amplitúdójuk nagysága szerint. Ezt az eljárást nevezzük mintavételezésnek. A mintavett jel digitalizálásának több szabványa is van, természetesen ezek nemzetközi szinten léteznek. Digitális jelről lévén szó a bit sorok mindössze két jelből épülnek fel, melyek az áramkörben általában feszültségváltozással fognak megjelenni, a számítás-technikában ezt a két értéket „0” és „1” számjegyekkel különböztetjük meg egymástól.

Egyik nemzetközi kódolási szabvány a PCM kódolás, melynek szabvány neve a G.711, egy fix mintavételezési eljárás, amit az ISDN is használ. Itt 8000 jelet mintáznak másodpercenként és 8 bites kódot használ. Ha az értékeket összeszorozzuk, megkapjuk, hogy másodpercenként 64 kb-es sávszélességre van szükség az átviteléhez. Léteznek olyan szabványok is, amelyek alacsonyabb sávszélességet kívánnak, de ezeknél - mivel kevesebb bittel írják le a hangokat vagy kevesebb mintát vesznek másodpercenként - sokszor kapunk torzabb, nem valóság-hű hangot. Gondoljunk csak arra, hogy egy 8 bites jellel 256 féle amplitúdó nagyságot tudunk leírni, míg egy 4 bitessel már csak 16 félé, de az átvitelhez szükséges sávszélesség csak felére 32 kb/s-ra csökken.

A G.711 egy tömörítetlen hangátviteli forma, ami kis sávszélességnél sok problémát okoz akkor, ha több csatornát szeretnénk egyszerre átvinni. Ennek orvoslására létrehoztak olyan szabványokat, amelyek a már mintavett és kvantált jelsorozatokat tömörítik így érve el sokkal alacsonyabb, az átvitelhez szükséges sávszélességet. A tömörítéssel akár 10-ed



4. sz. ábra: Néhány hangtömörítő kodek összehasonlítása hatásfokuk alapján [1]

részére is tömöríthetjük a hangot a PCM kódoláshoz képest. Természetesen a mércét mindig az jelenti, hogy két ember között mennyire érthető az átvitel. A hangminőség mérésére létrehoztak egy mérési rendszert (MOS), mely 5-ös skálán értékeli az átalakított hangot. Ezen a skálán például a PCM 4.5-ös értéket ér el. Említésre méltó, hogy ugyanebben a rendszerben a G.723.1 vagy a G.729 másnéven ACELP kimondottan beszéd tömörítésére használt kódolás 3.5-öt ért el és ez a szabvány a PCM-nél 16-szor kisebb sávszélesség mellett is érthető hangot képes átvinni.

A rendszer egyébként az értékeléseket a tömörítésből adódó hangminőség romlason kívül a szabványok késleltetését is kiértékeli. A késleltetés nagyon fontos egy hangátviteli kapcsolatnál, mivel az összeköttetés minőségét és a felhasználói

élményt nagymértékben befolyásolja. A késleltetés nagyságát főként két érték határozza meg, melyek ugyanúgy igazak a hagyományos telefonhálózatokra, mint a

digitálisakra:

- **jelterjedési késleltetés:** a fentiekben említettem, hogy a hálózatokat felhőként képzelhetjük el, ebben a felhőben többféle hálózati megoldást találhatunk, így az átvitel során a hang többféle szerkezetű (optikai, réz), felépítésű és nagyságú, akár világ kiterjedésű hálózaton keresztül halad. Ezek a tényezők mind-mind késleltetik a jelterjedést.

- **jelfeldolgozási késleltetés:** Az egyes, főleg digitálishálózatok határán többször AD/DA átalakításra és ki-betömörítésre kerül a hangunk, melyek időigényes feladatok, főleg azokon a hálózati elemeken jelentkezik kritikus mértékben, melyek nem csak hang, hanem egyéb adatforgalommal is meg kell, hogy birkózzanak. Az OSI modell rétegeinek megfelelően több protokoll is lehet egymásba ágyazva, a hálózati eszközöknek ezen protokollok kibontása, kiolvasása valamint a hálózati eszközökön folytatott kommunikáció során a szétdarabolt részek összerakása is időigényes feladat.

Főként pszichológiai hatása van az emberekre telefonbeszélgetés közben a csatornából visszaérkező visszhangoknak, mivel ezek alapján bizonyosodhatnak meg arról, hogy vonalban vannak és nem szakadt meg a kapcsolat. Analóg rendszerekben a visszhang az alkatrészek analóg mivolta lévén kialakul, de az ott megszokott visszhang egy olyan digitális rendszernél, ami nagyban védett a zajok ellen már nem hallható. Ezért ezeknek a visszhangoknak a létezéséért külön áramkörök felelősek, melyek vigyáznak arra is, hogy a visszhangot ne 25 ms-nál később halljuk, mert akkor átesünk a ló másik oldalára és az fog zavaróan hatni, hogy később halljuk vissza magunkat. Ezek az áramkörök alkalmasak arra is, hogy a kapcsolat számára valóban zavaró a vonal túlsó végéről többszörösen visszaverődő visszhangokat kiszűrjék.

Úgy véljük sikerült teljes képet adni a hangátvitel transzport megoldásairól, illetve arról, hogy hogyan lesz a hangból tömörített digitális jel, de bizonytalanság lehet sokak számára az, és felmerülhet az a kérdés, hogy egy hálózat sokadik végpontja hogyan talál meg egy másik, általa célnak megjelölt végpontot? Végiggondolva a rendszert, rögtön arra a megoldásra juthatunk, hogy a végpontok közötti kommunikációhoz valamilyen jelzésrendszer használhatnak a rendszerek.

A jelzésrendszerek tisztázása előtt a transzport modellek ismertetése elengedhetetlen. Azon transzportmegoldásokról beszélünk, melyeket a hangátviteli rendszerek alkalmazhatnak. Az első és legegyszerűbb és a számítástechnikai vagy híradási modellekhez hasonló pont-pont közötti összeköttetés, melyet transzport modellnek nevezünk. A pontok alatt telefonközpontokat kell értenünk, mely telefonközpontok természetesen ismerik a hozzájuk kapcsolódó készülékeket. A telefonközpontok között csak kimondottan egymás felé kerülnek küldésre azok a hívások, melyek nem a telefonközponton belül valósulnak meg. A másik megoldásra szolgál - melyet szintén az informatikából vagy híradásból ismerhetünk - a translációs modell, ahol egy pont több ponthoz kapcsolódik. Ennél a megoldásnál fontos szerepet kapnak a Voice Agentek, ahogy arról már szó volt az ő feladatuk fogadni a hozzájuk tartozó csomagokat, illetve kiválogatni a hozzájuk tartozókat a felhőkből. A küldést végző Voice Agent egy 'telefonkönyv'-ből dolgozik, mely ismeri a hívandó számhoz tartozó útvonalat. A csomagokat úgy ismerik fel, hogy a hozzájuk érkező hangcsomagon kívül egy jelzés is érkezik, mely információt tartalmaz a fogadott hangadattal kapcsolatban. Ez az információ tartalmazza küldő és fogadó azonosítóit. A jelzéseknek két főcsoportját különböztetjük meg:

- külső jelzésrendszer: A végberendezés és a Voice Agent közötti kommunikációt valósítják meg. Mivel a végberendezések eltérőek lehetnek, gondolok itt LB, CB, Automata, Digitális és Analóg rendszerűekre is valamint a digitális rendszereknél az alkalmazásbeli protokolljaik jelzésrendszereire, ezért a Voice Agentek-től a végberendezésekig menő jelzések is mások. A jelzéseket a központokban lévő trónkkártyák valósítják meg, azoknak megfelelően tudjuk csatlakoztatni a központokhoz a fent felsorolt különböző technikai felépítésű végberendezéseket. Ha nincs olyan trónkkártya a központban, amilyen fejlettségű készüléket szeretnénk használni, akkor csak abban az esetben kapcsolhatjuk hozzá, ha a végberendezés tudja az alacsonyabb fejlettségű szolgáltatás jelzésrendszerét és természetesen a fejlettebb készüléket alacsonyabb szolgáltatáscsomagokkal tudjuk használni. A trónkkártyák szolgáltatásai is eltérőek lehetnek, ezért nem minden extra szolgáltatás vehető igénybe a végponti készülékeken.

- belső jelzésrendszer: A Voice Agent-ek egymás közötti kommunikációjában játszik fontos szerepet. Kiemelten fontos, hogy a Voice Agent-ek ugyanolyan szabványt használjanak a kommunikációban való részvételhez. Minden transzferhálózatnak megvan a saját jelzésrendszere, de mindegyik jelzésrendszer alapfunkcióban kell, hogy támogassa az összeköttetés vezérlést illetve folyamatosan információval rendelkezzen a hívás állapotával és folyamatával kapcsolatban. Egy hívás alkalmával nincs folyamatos összeköttetés, mivel a

hálózatok csak csomagokat küldenek egymásnak, de amennyiben nincs átvendő információ, - amikor egyik fél részéről sem kerül hang a csatornába - akkor is érkezik bizonyos időközönként állapot információ, nehogy a vonal megszakadjon. A jelzésrendszerek az egyes transzportálózatokon az alap funkciójukon kívül rendelkezhetnek plusz funkciókkal.

### **3. INTERNET PROTOKOLL FELETTI HANGÁTVITEL ALAPJAI**

#### **3.1. Miért a VoIP?**

A csomag alapú hálózatokon való hangátvitel a számítástechnika gyorsan fejlődő világában és rövidnek mondható történelmében viszonylag régi technikának számít. Elterjedése lassúnak mondható - bár ez igaz nagyon sok új hálózati megoldásra is - mivel az internetes hálózatok kiépítettségének foka és velük együtt az új fejlesztések térnyerése legtöbbször nem igény, hanem pénz kérdése. Manapság legtöbb kormány, kormányzati egység, vállalat és ami nagyon fontos, a legtöbb internetszolgáltató IP alapú rendszereket használ, így leggyakrabban a beszéd átvivő rendszerek is a már kiépített hálózatokra települnek, arról nem is beszélve, hogy a piaci kínálatban szétnézve szinte csak IP alapú eszközökkel találkozunk. Ez azért nem szokatlan, mivel a hardvergyártó cégek is ezen eszközöket gyártják olcsón, nagy tömegekben. Az otthoni felhasználók pénztárcakímélésének tekintetében még olyan megoldások is születnek, melyek számítógépes program segítségével egyfajta telefonklienssé alakítják a PC-t és így azok képesek hangátvitelt szolgáltatni, egyik legelterjedtebb ilyen alkalmazás a Skype nevet viseli, de a legtöbb nagy szoftvergyártó cégnek is van saját szoftvere erre a célra. Sőt olyan megoldások is születtek, melyek egy számítógépből képesek telefonközpontot varázsolni Linux alapú operációs rendszer formában, erre egyik nagyon jó példa az AsteriskNow rendszer. Pénztárcakímélő megoldást nyújt a kisköltségvetés cégeknek, vállalkozásoknak. A Linux alapú rendszerek nagy előnye, hogy ingyenesek, továbbá az AsteriskNow egy böngészőben megnyitható GUI felületet is rendelkezésünkre bocsát, melyen keresztül egyszerűen és gyorsan beállíthatjuk a telefonközpontunkat.

Mindezeket összevetve úgy gondoljuk célszerű a VoFR és a VoATM hangátviteli rendszerek mellett a legelterjedtebb és legnépszerűbb, bár néhány paraméterében és néhány megoldásában gyengébb, egyes megoldásaiban viszont markánsan kitűnő hangátviteli rendszerről a VoIP-ről beszélni.

#### **3.2. A bemutatandó technikáról**

A VoIP-ről kommunikációjának mélyebb megismerése előtt fontos megemlíteni a jelenleg tárgyalandó rétegek átviteli protokolljait, ez esetben az OSI modellnek megfelelően lentől felfelé haladva ETHERNET keretet, IP-t, UDP-t és a TCP-t. Majd ezek megismerése után a VoIP alkalmazásrétegbeli H.323-as, SIP, SCCP és CorNet-IP belső jelzésrendszer protokolljait, melyek a kompatibilis rendszerek alapjain túlmenve nyújtanak interoperabilitási megoldásokat nem csak audio, hanem ahogyan majd látjuk adat és video átvitelre is. Szükséges tárgyalni a szolgáltatásminőségről valamint a routolási hibákról.

#### **3.3. Internet Protokoll**

Valójában az IP nem más, mint egy csomag, melyet az internet különböző szolgáltatásainál megvalósuló adatforgalomhoz használnak. Tudni kell, hogy az IP csomagot egy ETHERNET keret fogja közre, mely keretet az adatkapcsolati rétegben használnak az internetes eszközök. Minden ETHERNET eszköz rendelkezik egy MAC címmel, ami egy 12

hexadecimális számból álló egyedi azonosítója az eszköznek. A keret fejlécében található a küldő és a célállomás MAC címe. A láblécében pedig egy ellenőrző bejegyzést találunk, mely segítségével a fogadó oldal el tudja dönteni, hogy a kapott adat sérült vagy sem. A hálózatok eszközei különböző módon navigálják a csomagokat. Van, amelyik a MAC cím-et, van, amelyik az IP címet használja az irányításhoz, de ez természetesen a rétegektől is függ. A MAC cím a 2. rétegben, míg az IP a 3. rétegben látja el a navigációt.

Minden egyes hálózatban résztvevő önálló IP végberendezésnek rendelkeznie kell egy IP címmel ahhoz, hogy a kommunikációban részt vegyen. Magyarul az IP felelős azért, hogy a küldött adat célba érjen. Az IP cím, bár ez ránézésre nem derül ki, de két részből áll. Egyik része azonosítja a hálózatot, másik része pedig a hosztot. Egy IP csomag több részből áll, ezek a részek különböző információkat tartalmaznak. Az IP tartalmaz egy fejléct, amiben küldő és fogadó címét találjuk. Jelenleg a legelterjedtebb cím egy 32 bites számsor és IPv4-nek nevezzük, a címek 8 bitenként vannak felosztva és decimális számként vannak kifejezve. Ebben a fejlécben találunk információt többek között a csomag méretére illetve azzal kapcsolatban is, hogy a csomag maximálisan hány routeren mehet keresztül. Ezt TTL-nek vagy hop-nak nevezzük, legkisebb értéke 255 lehet. Minden egyes routeren való keresztülhaladáskor az eszköz elvesz egyet az értékéből és annál a routernél, ahol ez a szám 0 a csomag nem kerül továbbküldésre, hanem az eszköz eldobja azt. Erre azért van szükség, hogy ha egy csomag nem ér célba egy redundáns hálózaton, akkor ne keringjen örökre a hálózaton. Mivel a forgalomirányítás hibája miatt végtelen ciklusba kerülhet. Az IP csomag a fejléce után az OSI modell soron következő szintjeinek protokolljait tartalmazza, egészen eljutva alkalmazási szintig, ami után már csak a ténylegesen küldésre szánt adatok helyezkednek el. Az IP-nél fontos tudni, hogy nem végez sem hibajavítást sem pedig hibakeresést, ezeket a folyamatokat a felsőbb rétegbeli protokollokra bízta. Minden információval a fejrésztől az adatrészig egy IP csomag 512 kb nagyságú is lehet.

Az IPv4-et, amikor megalkotta az ARPANET az 1970-es években, még azt gondolták, hogy az a mennyiségű IP cím, melyet az biztosít bőven elég lesz arra, hogy akik a világon az internetet fogják használni, biztosítsa a hálózaton való részvételt. Azonban a rohamosan terjeszkedő és fejlődő internethálózat már nem képes boldogulni ilyen kevés címmel, ezért ahogy az a bevezetőben említettem a címrendszert jelenleg az IPv6 váltja, melynek a címezése már egy négyszer hosszabb 128 bites számsor, a címek 16 bitenként vannak felosztva és hexadecimális számként vannak kifejezve. Míg 4-es verzió  $2^{32}$ -en számú címet képes szolgáltatni addig a 6-os verzió már  $2^{128}$ -ont. Természetesen ezekből levonásra kerülnek a magán, a szórás, és a tesztelésre szánt IP címek csak úgy, mint elődjénél, de így is közel  $10^{36}$ -on címet szolgáltat ellentétben a 4-es verzió a  $4 \cdot 10^9$ -en címkészletével szemben. Újdonság, hogy a címből nem derül ki melyik hálózat részei vagyunk, hanem a cím egy konkrét végpontra vonatkozik aminek egyszerre több IP címe is lehet. Nem csak a címezésben van változás az új verziónál, hanem a protokoll szerkezet fejlécében lévő információkra vonatkozó leírások is megváltoztak, mivel a címelfogyás által életre hívott új protokoll lehetőséget adott nagyon sok fejlesztésre elődjéhez képest. Például, ha a jövőben olyan új szolgáltatás kerül kifejlesztésre, melyhez a harmadig réteg protokolljában van szükség információ átvitelére, egyszerűen csak hozzáadjuk a fejlécéhez, mivel az abban lévő információknak nincs meghatározott állandó helye és szabadon bővíthető, így természetesen alkalmazkodni tud bármilyen változáshoz is, ezzel biztosítva nagyobb flexibilitást. A lényeg az, hogy a fogadó oldal értse az üzenetet. Ezzel egyúttal az IPv6 fejléce kisebb is, mint az IPv4-é mivel nem tartalmazza azokat az információkat, melyekre az adott átvitelhez nincs szükség. Egy IPv6 csomag akár 4 GB nagyságú is lehet, de természetesen az alsóbb rétegekben lévő protokollok szét darabolhatják kisebb méretekre a saját átviteli kapacitásuknak megfelelően. Találunk benne egy új szolgáltatást is, mely segítségével sávzélességet tudunk előre lefoglalni épp a real-time alkalmazások szolgáltatásainak

akadálymentes átvitele miatt. Az IPv4 nem teljes egészében volt alkalmas multimédiás alkalmazások adatátvitelére, ezt az IPv6 teljes egészében kiküszöböli.

### 3.4. Szállítási protokollok

Az IP csomag felbontásakor találjuk az OSI modell szerinti következő, átviteli szinten az UDP protokollt a TCP, ICMP, SCTP, RTCP és az RTP protokollok mellett. A szállítási protokollokat tekinthetjük egyfajta szolgáltatónak is, mivel ezek biztosítják az alkalmazások számára a megfelelő átviteli lehetőségeket, illetve nyújtanak többlépcsős szolgáltatásokat az IP-nek, valamint az alsóbb rétegbeli protokollok számára vagy, ha úgy tetszik azokat kiegészítve. Ahogy ismertettem az ETHERNET keret MAC címmel dolgozik, az IP csomag IP címmel a szállítási protokollok és a föllette lévő protokollok mind-mind port címmel kommunikálnak.

Kezdjük a legegyszerűbb viszonylag ritkábban használt mégis sok segítség nyújtó protokollal az ICMP-vel. Ez a protokoll főleg a hálózaton végzett diagnosztikában, tesztelésen van segítségünkre, de a végpontok is küldenek ICMP üzeneteket információszerezés céljából. Az egyik legkorábbi protokoll ezért már parancssori szinten is a legtöbb operációsrendszerben megtaláljuk. Szolgáltatásai között találjuk a csomagok útvonal listázását (traceroute), vagy annak ellenőrzését, hogy a csomag célba ér-e vagy sem (ping).

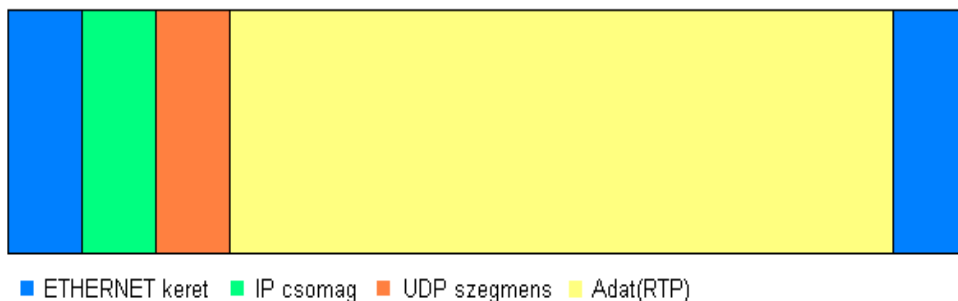
A TCP protokollról sokat hallhatunk internetezéssel kapcsolatban. Felelős azért, hogy a küldendő adatokat szétdarabolja, IP csomagba tegye majd a fogadó részen kicsomagolja, összeilleszti. Természetesen a kiküldött csomagok különböző útvonalakon juthatnak el a célig, ezért a protokoll feladata a datagrammok sorszámozása, sorba rendezése is. Mivel a TCP protokoll folyam alapú, így a hálózaton elveszett vagy megsérült csomagokat a fogadó oldalon újrakéri ezután a küldő oldalon újraküldi. Valójában ez úgy működik, hogy a csomagküldés után egy nyugtázást tartalmazó üzenetet vár a küldő oldalon, amennyiben egy bizonyos idő eltelté után nem érkezik meg ez az üzenet a csomagot újraküldi. Képzeljük el, hogy egy honlapot töltünk le és a csomagok fele elveszne letöltés közben, csonka információkból elég nehéz lenne tájékozódni. Igaz az is, hogy a TCP jelentősége a mai korszerű nagy megbízhatóságú hálózatokon egyre kisebb, de nem szabad arról sem megfeledkezni, hogy összeköttetési hibák kialakulhatnak, a lassabb átvitelt biztosító vagy túlterhelt eszközökön torlódhatnak, eldobásra kerülhetnek vagy a vezeték nélküli hálózatokon az összeköttetés megszakadása miatt nem érnek célba az egyes csomagok, melyek pótlására a megoldás csakis a TCP lehet.

Az UDP nem sorszámozza a csomagokat, így a fogadó helyen nem is állítja őket sorba. Az UDP protokoll jellegéből adódóan nem folyamat alapú, hanem burst jellegű, ezért a fogadó oldal nem nyugtázza a fogadást, így az elveszett csomagok újraküldése sem valósul meg. A TCP protokoll ismertetése után könnyebb beszélni az UDP protokollról, mivel nagyon sok tekintetben szöges ellentéte a két protokoll egymásnak. Míg a TCP kiválóan alkalmas szolgáltatásai lévén nem valós idejű alkalmazások adatátvitelére, addig az UDP szöges ellentétben vele teljesen alkalmatlan erre, viszont ő pont a valós idejű alkalmazások adatátvitelében jeleskedik.

Általában azok az alkalmazások részesítik előnyben, ahol apró részletekben elégséges az adatokat átküldeni, nem probléma, ha elveszik a csomagok egy része, de a megmaradó csomagok is gyorsan a célhoz érnek. Erre a legjobb példa a valós idejű hanghívás – telefonhívás. Egy másodperc alatt a rendszer átküldhet több tíz csomagot és az egyik valamilyen úton-módon nem érkezik célba, akkor is a hanghívásunkból kevesebb, mint egy tizedmásodperc fog kiesni. Vagy épp két csomag felcserélődik és nem sorrendben egymás után fog megérkezni. Ezekben az esetekben a visszahallott hang nem sokat torzul az eredeti hanghoz képest is jó hangminőségben lesz hallható.

Újabb fejlesztések, a rohamosan fejlődő valós idejű és jó minőségű adatok átvitele céljából hívták életre az SCTP és az RTP protokollokat. Legtöbb esetben az UDP hiányosságainak kiküszöbölésére használják. Természetesen a legújabb rendszerekbe ezek a protokollok is be vannak építve és a Voice Agentek tudják őket alkalmazni. De nem csak egycélú forgalmat tudunk bonyolítani a segítségükkel, hanem az egyszerre több IP címre küldés lehetőségét is támogatják a protokollok, ami alatt a klasszikus csoportos címzéshez hasonló valós idejű műsorszórást kell értenünk. Ahol csak az lesz a csoporttagja, aki kéri.

Az SCTP egyesíti az TCP és UDP protokollokat. Főleg azokban a multimédiás szórakoztató rendszerekben alkalmazzák, melyek kifejezetten multimédiás anyagok szórására vannak kihegyezve. A küldő oldal sorszámozza a csomagokat a fogadó oldal pedig eldönti, hogy sorba rendezi azokat vagy sem, természetesen ez alkalmazás függő. Kimondottan telefon-szerű adatátvitel miatt lett kifejlesztve. Egyszerre több digitális csatornát használ az adatok átvitelére. Egyik csatornáján történik a hangátvitel a többit pedig a jelzések átvitelére használja.



5. sz. ábra: A csomagalapú adatátvitel felépítése a protokollok tükrében RTP segítségével [1]

Az RTP-t kimondottan az audio és video átvitel miatt alkották meg. A hálózatokon az RTCP-vel együtt lett kifejlesztve. Az RTP a hang és video adatokat szállítja, míg az RTCP a csatorna jelzéseit, de az RTCP nem lehet nagyobb a csatorna forgalmának 5%-ánál. Egyik nagy előnye, hogy a többi protokollnál fellépő késleltetéseket lecsökkenti, amit a csomagok küldése közötti idő lefaragásával ér el. Főleg videokonferencia-beszélgetések lebonyolításához használják. Az RTCP kiválóan alkalmas egy időben több résztvevős kommunikáció létrehozására.

### 3.5. Alkalmazásrétegbeli protokollok

A VoIP technológia egy eléggé szerteágazó főleg jelzésrendszereiben változatos hangátviteli megoldás lett. A változatossága azzal magyarázható, hogy a különböző gyártók közel egy időben fejlesztettek, alakítottak át IP alapú rendszereket hangátviteli céllal. Így mai napig nagyon sok megoldás létezik, ezek közül a legelterjedtebbekkel célszerű megismerkedni. Közülük is a H.323-as és SIP nemzetközi protokollokkal, melyeket a VoIP rendszerek egységesítéséért születtek vagy a Cisco saját SCCP és a Siemens saját CorNet-IP protokolljaikkal. Ezek a protokollok természetesen életképesek minden az eddig általunk ismertetett fizikai rétegbeli protokolltól egészen a szállítási protokollokig azok tetszőleges vegyítése esetén. Azt mindenképp látnunk kell, hogy ezek a protokollok jelzéseket szállítanak egyik végponttól a másikig, így a központok szolgáltatásait ők fogják ellátni.

Elsőként ismerkedjünk meg a H.323-as protokollal. Illetve nem is egészen csak egy protokollról van szó, mivel a H.323 név nem csak egy protokollt, hanem a hálózati

eszközöktől megkezdve alkalmazási protokollokig egy teljes multimédiás rendszer nevét jelenti, mely lehetővé teszi a különböző gyártók eszközeinek interoperabilis együttműködését. (H.323 umbrella recommendation). Továbbá megfelelő minőségi paraméterekkel látja el azokat a hálózatokat, melyek nem képesek hang és video átvitelére így támogatva az internetes telefonálást és konferenciabeszélgetést, videokonferenciát. A protokoll lehetővé teszi a pont-pont közötti és a pont-többpont közötti kommunikációt. Önmagában az alkalmazásrétegbeli protokoll jelzésátvitelre szolgál, kommunikációs feladatokat lát el. Több alösszetevője van, melyek a különböző médiaformátumok átvitelét kezelik, illetve a tömörítésért felelnek. Magát a teljes H.323 rendszert és annak eszközeit egy későbbi fejezet részben ismertetem részletesen.

Másodikként pedig ismerkedjünk a SIP-pel, mely kimondottan egy kommunikációs protokoll és nagyon hasonlít a web böngészők HTTP protokoll kérdés-válasz modelljéhez, mivel ez is egyszerűszöveg alapú illetve kimondottan UTF-8 kódolást használ. A főerőkifejtése pedig a pont-pont kapcsolatok létesítésére összpontosul. A protokollt természetesen így magában nem is lehet telefonálásra használni a hangátvitelét az RTP protokoll biztosítja. Sokkal egyszerűbb és 'butább' protokoll, mint a H.323, mégis egyre népszerűbbé kezd válni, mivel a VoIP rendszerek jelentős napjainkban gyártott része ezt használja, talán pont túlzott egyszerűsége miatt.

A nagy gyártók legtöbb esetben próbálják hadititokként kezelni protokolljaik működését, így van ezzel a Cisco és a Siemens is. Kevés nyilvános információt lehet megtalálni protokolljaikról az interneten, a szakkönyvekben pedig általános leírásokat találunk az eszközeik működéséről. Ezért felhasználtam a Wireshark nevű számítógépes hálózatmonitorozó programot és a Cisco valamint a Siemens központokból rögzítettem adatfolyamokat, melyekből világosan kiderül, hogy a cégek bármennyire is rejtegetik, vagy illetik más néven protokolljaikat azok mögött, bár kicsi finomításokkal a már jól bevált H.323 és SIP protokollok dolgoznak. Sikert a gyártók honlapjain található leírásokból megtudnom, hogy a Siemens CorNet-IP protokollját HFA fantáziánéven is megtaláljuk. ISDN vonalon, annak a D csatornáin viszi át a jelzésinformációit és teljes mértékben kompatibilis a SIP rendszerekkel. A Cisco tekintetében pedig ugyanez a kompatibilitási mérték elmondható a H.323-as protokollal. Megfigyelhető egyébként, hogy azok a részek, amelyek nem mutatnak kompatibilitást, a gyártó specifikus többlétszolgáltatások körében mutatkoznak meg.

### 3.6. H.323 rendszer

A H.323 protokoll specifikációját a Nemzetközi Telekommunikációs Szervezet (International Telecommunication Union) a digitális telekommunikációs rendszerek egységesítésért hozta létre. A protokoll a kommunikációs réteg része és a belső jelzésrendszer megvalósításáért felel. A belső jelzésrendszer önmagában nem tudna különböző telefonrendszerbeli szolgáltatás megvalósítani, ezért több olyan eszközt tartozik hozzá, melyekkel egységes rendszert alkot. Vigyázni kell viszont, mert nem feltétlenül lesz minden H.323-at használó rendszer minden szolgáltatásában interoperabilis, mivel a H.323 protokoll tartalmaz egyéni bővítési lehetőséget, melyet a gyártók általában ki is használnak. Így előfordulhat az, hogy két különböző gyártótól származó eszköz nem fog ugyanazzal a szolgáltatáscsomaggal rendelkezni. A hálózatokon jelent megoldást, melyek nem rendelkeznek megfelelő minőségi paraméterekkel. Mivel nem foglalkozik más alsóbb rétegbeli protokollokkal, így a hálózati architektúrájába bármilyen olyan eszköz beilleszthető, melynek alkalmazásrétegbeli protokollja a H.323 lehet. Ilyen módon bármely csomagalapú adattovábbítási rendszerben használható.

A H.323 rendszernek egész architektúrája van, melyhez nem csak az alkalmazásbeli protokoll tartozik, hanem hardverelemek is. A protokollhoz tartozó hálózati eszközök között



található terminál, gateway, gatekeeper és a pont-többpont kapcsolat létrehozását lehetővé tevő egységek. Ezek a rendszerelemek vesznek részt a kommunikációban és a vezérlésben. Illetve egy H.323 rendszerben a H.323 protokoll mellett dolgozik még a H.245 és a H.225.0 protokollok is. Ezek lehetővé teszik a pont-multipont kapcsolatokat is a pont-pont kapcsolatok mellett illetve alkalmasak arra, hogy a konferenciabeszélgetéseket ne egy végberendezés vezérelje, hanem osztozzanak az erőforrásokon.

Ismertetteük a csomagkapcsolt hálózatoknál a Voice Agentek szerepét a H.323 rendszerben ezeket termináloknak nevezik, nevük változása ellenére feladatuk nem változik, vagy csak annyiban, hogy a neki megfelelő végponton átjárókkal és többponti összeköttetésért felelős eszközökkel kommunikálhat. A terminálok képesek hang, hang-adat, hang-videó kommunikációkra. A következő elemekkel mindenképp rendelkeznie kell egy terminálnak:

- H.245 protokoll, mely ellátja a hívás közbeni teendőket állandó sávszélesség lefoglalás, csomagkezelés, tulajdonképpen a csatorna minőségi paramétereikért felelős.
- Q.931 hívásfelépítésért és vezérléséért felelős jelzésprotokoll.
- RAS protokoll, mely a gatekeeperrel való kommunikációt valósítja meg.
- RTP/RTCP protokollok, ahogy már szó volt róluk adat és video szállításért felelnek, illetve azok átviteléhez szükséges jelzéseket szállítják.

Vannak olyan szolgáltatások is, melyeket nem feltétlenül tartalmaz egy H.323-as rendszer csak opcionálisan beépíthető, ahogy említettem, ezek miatt lehet szolgáltatásaiban eltérő két H.323 eszköz:

- Video kodekek: Segítségükkel a video átvitel sávszélesség-igényét tudjuk lecsökkenteni, többféle kódoló eljárást használhat a videók méretének csökkentése céljából.
- T.120 adatkonferencia protokoll: a multimédiás tartalmak valós idejű átvitelét biztosítja, főleg itt a video és hang együttes szinkronban való átvitelére gondolok.
- MCU-val való kommunikációs képesség: Több résztvevős központosított konferenciabeszélgetések céljából.
- Gateway: más hálózatokba való átjárást illetve a különböző protokollok, kommunikációs eljárások és kodekek közötti átalakítást, átjárást teszi lehetővé.

Az IP rendszereknél általában a végberendezést kell felkonfigurálni ahhoz, hogy részt vegyen a kommunikációban, nem pedig a központról fogja betölteni a kommunikációban való részvételhez a paramétereket, viszont a szolgáltatásokat a központtól fogja kapni, ezeket pedig egy H.323-as rendszerben a gatekeeper fogja szolgáltatni, abban az esetben, ha a rendszer tartalmazza, mivel nem kötelező eleme egy H.323 rendszernek. A gatekeeper más eszközről, esetleg szoftveresen is megvalósítható. Bármilyen megoldás is legyen a szolgáltatások, melyeket biztosan megtalálunk egy ilyen eszközben a következők:

- Címfordítás: Egy egyszerűbb, vagy egységesített fix hívószámra fordítja IP címünket, mely fordításokat adatbázisában tárolja és egy összeköttetés felvétele esetén onnan olvassa ki.
- Kérések vezérlése: A hálózaton lévő VoIP eszközök kéréseit azonosítja és eljuttatja a kérésnek megfelelő eszközhöz.
- Sávszélesség vezérlés: a minőségi hangátvitelhez szükséges sávszélesség lefoglalását vezérli.
- Területkezelés: Az eddig említett szolgáltatások érvényesítésére szolgál a hálózat többi elemén.

Ahogy a termináloknál ugyanúgy a gatekeeper funkciót betöltő eszköznél is igaz, hogy a szolgáltatásokban lehet eltérés, mivel itt is vannak opcionálisan beépíthető funkciók:

- Hívásirányítás-jelzés: Főleg egy bonyolultabb hálózaton általában eleme szokott lenni a H.323-as rendszernek. Feladata a jelzésrendszer biztosítása.
- Jogosultság kezelés: Segítségével többféle jogosultsági tényezőt beállíthatunk, így érvénybe léptethetünk, mind összeköttetésbeli, mind időbeni és mind prioritásbeli korlátozásokat.
- Sáv szélesség kezelés: Több összeköttetés esetén, ahol lecsökken a szabad sáv szélesség vagy eleve alacsony sáv szélességű hálózaton a nagyobb prioritású hívásoknak ad megfelelő minőségű vonalat vagy ennek megfelelően korlátozza az alacsonyabb prioritású összeköttetések létrejöttét.
- Híváskezelés: Egy adatbázist hoz létre, mely a folyamatban lévő hívásokat tartalmazza, ez alapján tud a hálózat foglalat jelzést adni, vagy hívásban lévő csatornabeli funkciókat kezelni.

A felsorolt szolgáltatásokon kívül természetesen léteznek még szolgáltatások, de ezek gyártó specifikusak vagy csak ritkábban használjuk őket.

A H.323 rendszer fontos része a konferenciahívást biztosító egység (MCU), melyre igazából csak akkor van szükség, ha a konferenciabeszélgetést központilag szeretnénk vezérelni, mivel más a H.323-al együttműködő protokollok képesek az osztott konferenciabeszélgetés létrehozására.

Az MCU-nak két része van az MC és az MP. Az MC feladata a 3 vagy annál több résztvevő hívások irányítása, de feladata nem csak a hangátvitelre, hanem a konferencia-videó átvitelére is kiterjedhet. Valójában ő azt a folyamatot irányítja, amit az MP feldolgoz számára. Az MP nemcsak központilag feldolgozza a konferencia adatait, hanem párosítja az audio, adat és video csomagokat, illetve információt szolgáltat a csatornák kiépülésével kapcsolatban.

Arról szó volt, hogy a video átvitel opcionális része a rendszernek röviden csak annyit szeretnénk bemutatni, hogy milyen minőségű video átvitelre alkalmasak az egyes kodekek. A legalacsonyabb felbontás, amivel rendelkeznie kell egy video átvitelre alkalmas H.323 rendszernek az 128x96 pixel és 30 képet kell tartalmaznia másodpercenként, ezt nevezzük SQCIF-nek. A videó átvitelét a H.261 és H.263 nevű kodek végzi. A kodekek egyébként nem teljes képet vizsik át, mindig csak annyit belőlük, ami az előző mintához képest különbség. A legnagyobb átvihető kodekek által biztosított formátum a 16CIF, melynek felbontás 1408x1153 pixel, ez méreteiből is látszik, hogy elég robosztus és nagy sáv szélesség kell az átviteléhez. Az alap video formátumot CIF-nek nevezzük, ezt mindkét kódolás ismeri, felbontása 352x288 pixel.

A H.323 protokoll tanulmányozása után annyit sikerült megállapítanom, hogy bár sokkal összetettebb és kevésbé népszerű, mint a SIP, de valójában egy egész rendszert alkot, mely nemzetközileg egységes és nagyon jól ráépíthető a már meglévő számítógépes hálózatok rendszerekre is akár. Kiválóan alkalmas különböző képességű készülékek közötti konferenciabeszélgetések létrehozására és megfelelő telefonrendszerbeli szolgáltatások biztosítására.

### 3.7. Szolgáltatásminőség

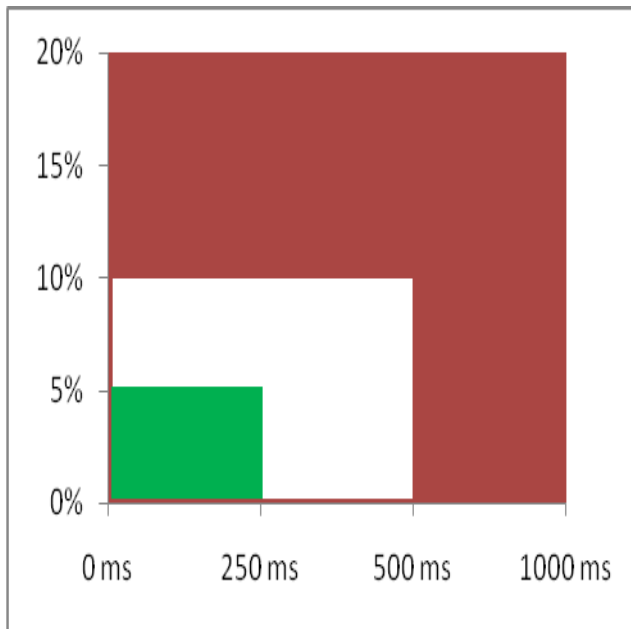
Hivatkoztunk már több ízben arra, hogy a protokolloknak képesnek kell lenniük egy megfelelő szintű minőséget nyújtani az alkalmazások zavartalan működéséhez, mely nem csak az IP hálózatokon igaz, hanem az összes csomagkapcsolt átvitelt megvalósító hálózaton. A megfelelő szintű minőség pedig nem jelent mást, mint a megfelelő sáv szélesség biztosítást, mely csatornánként minimálisan 7-8 kbit/s-ot jelent, de az ajánlott 15 kbit/s. Természetesen a késleltetés mérete is egy minőségi követelmény, melynek a mértéke két végpont között nem szabad, hogy meghaladja a negyed vagy maximálisan fél másodperces

időt. Nagyon fontos még az is, hogy a valamilyen úton-módon elvesző csomagok mértéke az összesen elküldött csomagok mértékének 10%-a alatt maradjon.

Van egy bizonyos jitter érték, amiről még nem esett szó. A jitter magyarul késleltetés-ingadozást jelent. Az apró mintákat a hálózati eszköz egy mesterségesen késleltetett mechanizmussal fogja csomagokba szervezni. Több mintát puffereel egymás után és megadott időközönként a mintákat egy csomagba rendezve küldi tovább. A megfelelő szolgáltatásminőség eléréséhez ennek az időköznek a nagysága 30 ms körül kell, hogy mozogjon. A nagyon nagy eltérés mind negatív, mind pozitív irányban akadozást okozhat a csatornában.

A felsorolt tényezők természetesen konstans berendezéstől függő tényezők, de a szolgáltatás minőséget befolyásolja nagyban a hálózatok aktuális állapota, pillanatnyi hálózati forgalom nagysága és a csomagok torlódása, valamint nagyon fontos, hogy lehetnek routelési hibák is.

A QoS (RFC 3714) előírásainak megfelelően összességében arra következtethetünk, hogy egy adott szolgáltatásnak megfelelő sávszélesség és jitter érték mellett akkor mondható egy csatorna jó minőségűnek, ha abban a csomagvesztés mértéke 5% alatt és a késleltetés



6. sz. ábra: A QoS minőségi határai a késleltetés és a csomagvesztés arányában [2]

mérete 250 ms alatt van. Az ilyen minőségű csatornák kiválóan alkalmasak kormányzati és vállalati és így a Magyar Honvédség telekommunikációs igényeik megvalósítására, melyek a laktanyákon, hivatalokon belüli és azok közötti hívások kiszolgálását tennék lehetővé. A következő határvonalat a minőségbiztosításban a 10% csomagvesztés és az 500 ms-os késleltetés adja. Az ilyen minőségű csatornák megfelelőek a hétköznapi magánbeszéd lebonyolítására. Az e fölötti értékekkel rendelkező csomagalapú átvitelt biztosító

rendszerek csatornái nem alkalmasak beszéd átvitelre.

A QoS rendelkezik egy RSVP nevű saját szállítási rétegbeli protokollal, mely a többi azonos rétegszinten lévő protokollal ellentétben nem tartalmaz felsőbb rétegbeli protollokat, így természetesen adatokat sem küldhetünk segítségével. Ez a protokoll egy jelzésprotokoll, mely a végpontok között sávszélesség és puffer foglalat végez a routereken és a switcheken. A protokoll az erőforrás lefoglalások állapotüzeneteit - amennyiben az összeköttetés él - meghatározott időnként, periodikusan küldi. Az eszköz amin a foglalás történt ugyanilyen időközönként törli a foglalást. Ezért nem fordulhat elő az, hogy ha már megszakították a hívást, akkor is megmarad a lefoglalás. Természetesen a protokoll lehetővé teszi azt is, hogy azok az eszközök, melyeken a lefoglalás megtörténik, ellenőrizzék a jogosultságot.

### 3.8. Útvonal választási hibák

A QoS nem tudja kezelni a routereken, azok feldolgozási képességeikből fakadó késleltetést, de mindenképp figyelembe kell vennünk, mivel a szemléltetett hálózati felhőben nagyon sok olyan eszköz lehet, mely a csomagokat irányítja és ezek a berendezések többféle struktúrában kapcsolódhatnak egymáshoz, vagy többféle módon lehetnek felkonfigurálva, így nem tudjuk előre meg, hogy egy-egy általunk küldött csomag milyen útvonalon fog eljutni a célig. Nagyon sok esetben történik olyan, hogy nem a legrövidebb utat használja.

Előfordulhat olyan hiba, hogy egy virtuális hurok képződik és az általunk küldött csomag nem jut el a célig, hanem valamilyen úton visszakerül a saját helyi hálózatunkba. Esetleg a virtuális hurok routerről-routerre küldi körbe-körbe a csomagunkat egészen addig, míg az IP csomag ugrási értéke 0 nem lesz és eldobásra kerül a csomag.

Mivel a különböző rétegekben a különböző protokollok más-más csomagmérettel dolgoznak, így előfordulhat, hogy a megfelelő csomag összeállítása után a router az IP csomagunk egyik felét A irányba másik felét pedig B irányba küldi ki. Általában ezt azért teszi, mert nem feladata a csomagok helyes sorrendben való elküldése, annál inkább feladta a hálózat terhelésének a csökkentése. Így ezzel a módszerrel osztja meg pártjain a terhelést. A nem valósidejű alkalmazásoknál ez észrevehetetlen, viszont a valósidejű alkalmazásoknál növeli a késleltetést.

Gyakran olyan hiba is előfordul, hogy a routerek a két végpont felől nem azonos útvonalakon küldik a csomagokat, így aszimmetriát okozva a hálózatokon. Ez azért lehet problémás, mert míg az egyik oldalon normális minőséget tud produkálni a hálózat, addig a másik oldalon a csomagok nagyobb késleltetéssel fognak megérkezni. Ilyenkor a két beszélő fél nem egyforma minőségben fogja egymást hallani.

Még hibát okozhat a routerek szempontjából az, amikor a routerek nem állandó útvonalon küldik a csomagokat, hanem azokat változtatják saját routing protokoll értékeiknek megfelelően, arra vonatkozóan, hogy mikor melyik hálózat melyik porton érhető el hamarabb. Nagy általánosságban egy hívás alkalmával a csomagok kevés kivétellel, de ugyanazon az útvonalon „közlekednek”.

### ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Jelen publikációnk összeállításával megpróbáltunk betekintést nyújtani a kommunikációs hálózatok múltjába és jelenébe annak érdekében, hogy segítséget nyújthassunk az IP feletti hangátvitel megvalósításához, vagyis a VoIP rendszerek tervezéséhez.

### FELHASZNÁLT IRODALOM

- [1] Dárdai Árpád: Mobil Távközlés, Mobil Internet (A mindennapok kommunikációs technikája) - ISBN: 9789634409960 - 2003 - Computerbooks
- [2] VoIP-info.org anyagainak felhasználása /Többek között: H.323; SIP; QoS; Asterisk címszavak alatt található anyagok/ - Letöltve: 2011.02. 10. - 2011.04.26. - <http://www.voip-info.org/>
- [3] Wireshark Wiki anyagainak felhasználása - Letöltve: 2011.02. 10. - 2011.04.26. - <http://wiki.wireshark.org/>

**Tóth András**  
toth.hir.andras@zmne.hu

## **A FELHŐINFORMATIKA ALAPJAI**

### ***Absztrakt***

*A felhőinformatika egy mostanában előtérbe került informatikai fogalom, amely azt hivatott szolgálni, hogy a felhasználó által használt adatok, alkalmazások egy távoli szerveren kerül tárolásra, illetve ott van futtatva. A cikk ennek az új típusú rendszernek az alapjaival foglalkozik, annak lehetőségeivel.*

*The cloud computing has recently come to the front as an IT concept, which provides the users a remote server, where the user's data and applications are stored and run. The article deals with the basics and possibilities of this new system.*

**Kulcsszavak (keywords):** *felhőinformatika, IT ~ cloud informatics, IT*

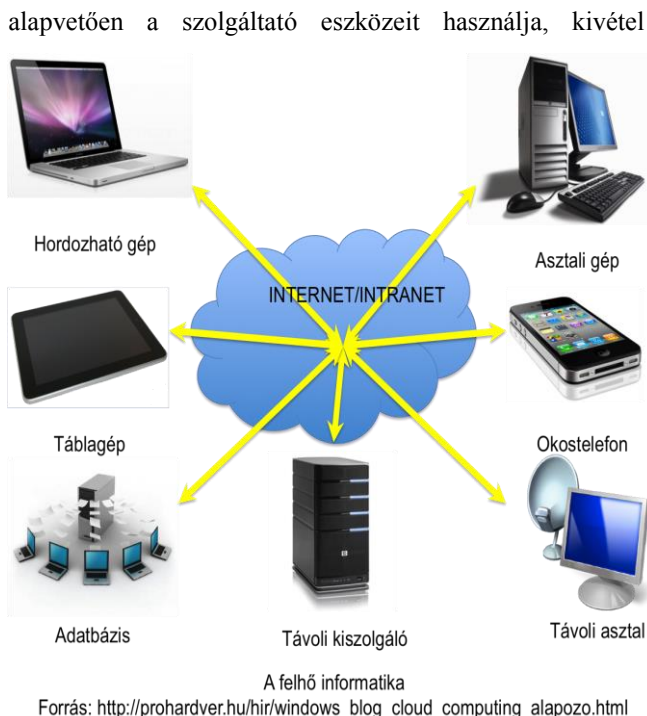
### **BEVEZETÉS**

A felhőinformatika leginkább az elektromos áram szolgáltatáshoz hasonlítható. Körülbelül egy évszázaddal ezelőtt mindenki saját magának termelte meg a szükséges energiát különböző módszerek alkalmazásával, míg napjainkban mindenki egy központi szervezettől kaja, és senki sem tartja fontosnak, hogy az az energia milyen módon kerül előállításra, hol van tárolva, hogyan jut el hozzánk. Ez az informatikára is ugyanúgy jellemző volt a múltban, és most a felhő informatikával a jelenben is. Régebben mindenki saját maga tárolta az adatait, ő vásárolta meg a szükséges hardvereket, szoftvereket, licenzeket. Napjainkban viszont több szolgáltató nyújt számunkra olyan lehetőségeket, hogy adatainkat, alkalmazásainkat egy távoli szerveren tárolhatjuk, aminek a pontos helyét nem tudjuk, és nem is kell tudnunk, mert azt teljes mértékben a szolgáltató üzemelteti.

### **1. MI IS AZ A FELHŐINFORMATIKA?**

Az elmúlt hosszú éveknek megfelelően a „felhő”, mint informatikai fogalom magát az Internetet jelenti. Abban az esetben viszont, ha úgy alkalmazzuk, mint „informatikai felhő” akkor Interneten/Intraneten keresztül elérhető virtuális szerverekről, és azon telepített és futtatott alkalmazásokról beszélhetünk. Egy szervezetnek, cégnek abban az esetben lehet szüksége az informatikai felhőre, ha számítástechnikai értelemben vett méreteit, képességeit szeretné fejleszteni, anélkül, hogy új eszközöket, rendszereket vásárolna; különböző szakembereket alkalmazna, képezne; valamint a szoftveres háttérhez szükséges, sok esetben nagyon drága licenzeket be kellene szereznie. Amikor egy felhasználó az informatikai felhő

segítségével dolgozik, akkor természetesen az adott végberendezést, amely segítségével képes elérni a felhőt, és a részére szükséges adatok mindegyike, vagy csak egy adott része távoli szervereken van tárolva. Tehát az informatikai felhő lehetővé teszi a vállalatok, közigazgatási, közszolgálati szervezetek, valamint egyének számára valamilyen hálózat (Intranet, Internet, valamilyen helyi hálózat) használatát, vagy az adatokhoz, alkalmazásokhoz történő hozzáférést, hogy azok valamilyen máshol található számítógépen helyezkednek el. Igazából ez azt jelenti, hogy a számítási erőforrások egy hálózaton keresztül valós időben használhatók, és a szolgáltatás díjazása a felhasználás alapján történik.



*"A számítási felhő (cloud computing) modell révén a felhasználók kényelmesen és igény szerint férhetnek hozzá a megosztott, beállítható informatikai erőforrásokhoz (például nyomtatókhoz, kiszolgálókhoz, tárolókapacitáshoz, alkalmazásokhoz és szolgáltatásokhoz), amelyeket gyorsan és minimális adminisztrációs megterhelés vagy szolgáltatói beavatkozás mellett rendelkezésre lehet bocsátani és fel lehet szabadítani."*<sup>27</sup>

Jelenleg még sokan úgy gondolják, hogy a felhőben történő adattárolás nem biztonságos, de gondoljunk csak bele, hogy egy cég, amely teljes mértékben arra koncentrál, hogy egy olyan környezetet biztosítson az adataink számára, amely amelelt, hogy a lehető legmagasabb rendelkezésre állást biztosítja, még a legújabb, leghatékonyabb biztonsági eszközökkel, szoftverekkel van ellátva, sokkal magasabb szintű biztonságot nyújthat az adatainknak, mint a mi általunk kiépített, és a saját költségvetésünktől és képességeinktől nagyban függő rendszer képes.

A szolgáltatóknak alapvetően egy olyan biztonságos rendszert kell kiépíteniük, amely alkalmas arra, hogy bármilyen céget, aki hozzájuk kapcsolódik, annak auditálási és megfelelőségi követelményeinek megfelelően képesek legyen kiszolgálni. Fontos szempont a szabványosság is, amely azért elengedhetetlen, mert egy olyan szabványt használó szolgáltatót kell választanom, amelynek a futtatott szolgáltatása képes csatlakozni a felhasználó vállalat biztonsági rendszeréhez. Ahhoz azonban, hogy ezek az információk

<sup>27</sup>National Institute of Standards and Technology (NIST) –Nemzeti Szabványügyi és Technológiai Intézet

minden szinten és minden egyes helyen biztonságban legyenek a cégeknek is rendelkezni kell a legjobb megfelelőségi infrastruktúrákkal. A biztonsági rendszabályoknál fontos, hogy mind a szolgáltató, mind a megrendelő felhasználók azonosítására, a jelszókezelésre, a jogosultságokra és az auditra vonatkozó intézkedéseket.

A felhőinformatika több különböző formában létezik:

- Nyilvános felhők
- Magán felhők
- Hibrid felhők, ami kombinálja a nyilvános és magán felhőket
- Közösségi felhők.

A nyilvános felhő számítástechnikai erőforrásait külső fél üzemelteti, bárki által hozzáférhető, azaz több szervezet megosztva használja, akár egy időben is. Előnye, hogy a felhasználó jelentős összegeket képes megspórolni az alkalmazásával, mivel nem szükséges beszereznie a szolgáltatások futtatásához szükséges hardver és szoftverelemeket. Ezzel szemben azonban kockázatot jelenthet, hogy nem tudja befolyásolni sem a rendszer, sem a használt alkalmazások működését.

A magán felhők jellemzője, hogy csak egy vállalat használja, és az a saját rendszerén belül helyezkedik el, vagyis a tűzfalain belül. Ez a típus sok vállalat esetében az első lépés a felhőinformatika területén. Ez is egy jól méretezhető, hatékony környezet, amely lehetőséget nyújt a többi felhő típushoz hasonlóan a rendelkezésre álló erőforrások megosztására.

A hibrid felhők jellemzője, hogy az alapvető alkalmazások a saját rendszeren belül futnak, viszont a szükséges információt szolgáltató adatok, alkalmazások és rendszerek a vállalaton kívül, valahol a felhőben elhelyezett külső szerveren vannak tárolva, illetve futnak.

A közösségi felhő, egy olyan formája a felhő informatikának, amelyet több ember, vagy szervezet használ egy bizonyos közös érdekből.

## 2. AZ INFORMATIKAI FELHŐ ELŐNYEI

Amennyiben felhő alapú hálózat kiépítésén, üzemeltetésén gondolkozunk az első dolog, ami előnyként merülhet fel, hogy nincs szükségünk akkora erőforrás mennyiségre a rendszerünk üzemeltetéséhez, nem kell befektetnünk új eszközökbe, és nem kell azon gondolkozunk, hogy mit fogunk kezdeni a jövőben azokkal a berendezésekkel, különböző rendszerelemekkel, amelyekre már nincs szükségünk. Különböző vizsgálatok is bizonyítják, hogy napjainkban egy szervezetnél működő szerver állomás (például fájlserver) körülbelül 15%-os kihasználtsággal működik. Miért fektetnénk komoly összegeket egy olyan eszközbe, amely ekkora kihasználtsággal működik? Nem is beszélve arról, hogy abban az esetben, ha például megnövekszik az adataink forgalma, nekünk kell ezeket az adatközpontokat bővítenünk, míg a felhő alkalmazása esetén csak kérünk egy nagyobb tároló kapacitást, és nem kell azzal foglalkoznunk, hogy új háttértárolókat szerezzünk be, és alakítsunk ki egy nagyobb adattárolásra alkalmas szervert.

Az informatikai felhő esetében az alkalmazások nagy része webes alapon érhető el, amely a hardver elemek terhelését csökkenti, így azok felhasználhatók, más a szervezet számára hasznos feladatok végrehajtására. A hardverek tehermentesítése mellett egy másik nagyon fontos terület is felszabadul, mégpedig az emberi erőforrás. Mivel az adataink,

leveleink, alkalmazásaink egy távoli szerveren futnak, így nem a mi IT szakemberünknek kell azokkal foglalkoznia, nem ők fogják menedzselni az elektronikus levelező rendszerünket, nem ők változtatják a jelszavakat, ehelyett a cég működését sokkal inkább befolyásoló fejlesztésekre és alkalmazásokra tudnak koncentrálni. Az emberi erőforrás tekintetében a másik nagy előny, hogy a felhőszolgáltatás esetén nem a mi embereinknek kell foglalkoznia egy esetleges meghibásodott szerver újra üzembe helyezésével, az a szolgáltató erre szakosodott embereinek feladata. A legtöbb olyan cég, amely felhőszolgáltatást biztosít a világ különböző pontjain elhelyezett hatalmas méretű adatközpontokkal rendelkezik, amelyek nagy, 99,9%-os rendelkezésre állást biztosítanak. Amennyiben valamilyen probléma mégis fellépne a szolgáltatók egy 24/7-es támogatási központot üzemeltetnek, ahol a felhasználók segítséget kérhetnek a probléma mihamarabbi megszüntetésére.

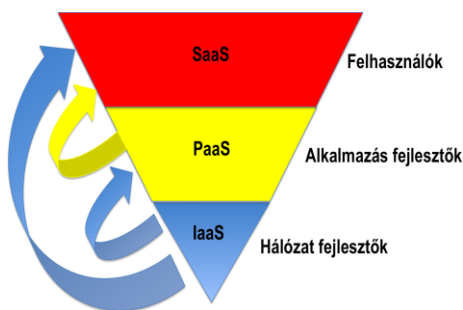
### 3. A FELHŐINFORMATIKA SZOLGÁLTATÁSAI

Attól függően, hogy egy vállalat mit tervez szervezetén kívül helyezni a felhőinformatika különböző szolgáltatásokat képes nyújtani számára. Ez jelentheti azt, hogy egy megrendelő tárolókapacitás hiányában csak egy bizonyos méretű tárhelyet igényel a felhőben, de lehetséges az is, hogy néhány alkalmazást, szolgáltatást helyez ki. Célszerű a választás előtt figyelembe venni azt, hogy melyik lehetőségnél mik azok a szoftver és hardver elemek, amelyekkel a rendszernek minimálisan rendelkeznie kell. A különböző szolgáltatásoknál ezek a következők:

- Amennyiben valamilyen folyamatot vizsgálunk a szükséges szolgáltatás-komponensek: alkalmazások, platformok, az infrastruktúra, a folyamatok és az integráció.
- Amennyiben valamilyen adatot vizsgálunk a szükséges szolgáltatás-komponensek: alkalmazások, platformok, az infrastruktúra, a tárolóhely, adatbázis és az információ.
- Amennyiben valamilyen szolgáltatást vizsgálunk a szükséges szolgáltatás-komponensek: alkalmazások, platformok, az infrastruktúra és az információ.

A felhő informatikában három fő szolgáltatást különböztetünk meg:

- Szolgáltatásként kínált infrastruktúra<sup>28</sup>  
Nincs szüksége a felhasználónak helyi szerverekre, tárolóhelyekre,



Informatikai felhő szolgáltatási modellek

Forrás: <http://lepenyet.wordpress.com/2011/06/16/szmts-i-felho-egyszeruen-2-rsz/>

<sup>28</sup>Infrastructure as a Service – IaaS



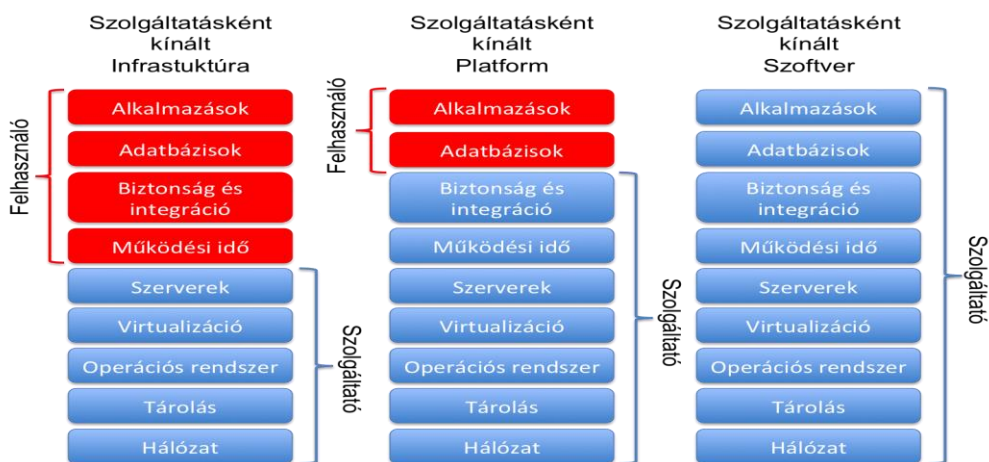
hálózatokra, valamint egyéb a hálózat üzemeltetéséhez szükséges eszközökre. A szolgáltató a szervereket, tároló- és munkahelyek összességét, valamint a hozzájuk tartozó szoftvereket, mint szolgáltatás nyújtja (például operációs rendszer), amelyek egy hálózaton keresztül érhetők el a felhasználók számára. A hálózati eszközök általában olyan virtuális berendezések, amelyeken futó alkalmazások üzemeltetéséért és karbantartásáért a felhasználó felelős ugyanúgy, mint a saját környezetében futtatott szerverekért, tárolókért. Ez a legalacsonyabb szintű szolgáltatás a felhő informatikában.

- Szolgáltatásként kínált platform<sup>29</sup>

A szolgáltató az IaaS-hez hasonlóan egy virtuális környezetben biztosít a felhasználó számára szervereket, tárolóhelyeket, szoftvereket, de rendelkezésre bocsát egy programkörnyezetet (platform) is. A környezet lehetővé teszi a felhasználók számára, hogy alkalmazásokat hozzanak létre, kövessék annak teljes életciklusát a tervezéstől a megvalósulásig, a menedzselésig, valamint biztosítja a már működő alkalmazás személyre szabását. Előnye, hogy minden mögöttes berendezés a felhőben kerül elhelyezésre, így az informatikai szakembernek lehetősége van csak az alkalmazásfejlesztésre összpontosítani.

- Szolgáltatásként kínált szoftver<sup>30</sup>

A végfelhasználó részére nyújtott kész alkalmazás, amely egy hálózati kapcsolattal érhető el, a felhasználó azon keresztül használja. Az alkalmazás megtervezéséért, menedzseléséért a szolgáltató felelős. Hátránya lehet, hogy a hálózat megszakadása esetén, vagy a sávszélesség lecsökkenését követően az alkalmazás nem érhető el, ezért az nem is használható.



A felhőszolgáltatások menedzselése  
 Forrás: <http://www.silverlighthack.com/post/2011/02/27/IaaS-PaaS-and-SaaS-Terms-Explained-and-Defined.aspx>

<sup>29</sup>Platform as a Service – PaaS

<sup>30</sup>Software as a Service – SaaS

#### **4. A FELHŐINFORMATIKA ALKALMAZÁSI LEHETŐSÉGEI HÁBORÚS, ÉS NEM HÁBORÚS MŰVELETEKBEN**

A felhőinformatika egy olyan új típusú informatikai lehetőség, amely alkalmazásával az egyes szervezetek, vállalatok képesek lesznek adataik, alkalmazásaik tárolására, megfelelő időben történő rendelkezésre bocsátására, mind a szervezeten belül, mind azon kívül, a világ bármely pontján, a megfelelő jogosultságok alkalmazásával. Ennek megfelelően a katonai alkalmazás során, amely jelen esetben lehet háborús és nem háborús egyaránt, ez egy nagyon jól alkalmazható rendszer lehet bázis objektumon belül, és kívül egyaránt. Amikor egy adott alegység, egység békehelyőrségben tartózkodik a saját rendszeresített, telepített informatikai eszközeivel képes egy általa nem ismert helyen elhelyezett szerverhez csatlakozni, és azon tárolt, illetve futtatott adatokhoz, alkalmazásokhoz hozzáférni, azokat alkalmazni. Ez a jelenleg kiépített Intranet hálózat alkalmazásával megvalósítható. Amennyiben egy szervezet valamilyen katonai tevékenységet hajt végre ugyanúgy alkalmas lesz ehhez a szerverhez csatlakozni egy kiépített mikrohullámú, műholdas, esetleg rádiós kapcsolat segítségével, és a saját mobil informatikai eszközök segítségével képes lesz a szükséges feladatok ellátására.

#### **ÖSSZEGZÉS, KÖVETKEZTETÉSEK**

A fentiek figyelembe vételével a felhőinformatika alkalmas lehet egy szerver központú vezetés- irányítási rendszer kiszolgálására, amely összekötheti a tűzvezetési, fegyverirányítási, híradó és informatikai rendszereket, illetve minden olyan hálózatot, amely a harc sikeres megvívásához szükségesek. Előnye, hogy a szükséges jogosultságokkal felruházott felhasználók könnyedén hozzáférhetnek a számukra szükséges információhoz, helytől, időtől függetlenül.

#### **FELHASZNÁLT IRODALOM**

- [1] Cloud computing, avagy a felhő-informatika az IT jövője - [http://infovilag.hu/hir-17875-cloud\\_computing\\_avagy.html](http://infovilag.hu/hir-17875-cloud_computing_avagy.html)
- [2] Windows blog: cloud computing alapozó  
[http://prohardver.hu/hir/windows\\_blog\\_cloud\\_computing\\_alapozo.html](http://prohardver.hu/hir/windows_blog_cloud_computing_alapozo.html)
- IaaS - Cloud Computing
- [3] What is Infrastructure as a Service (IaaS)?  
<http://deletemalware.blogspot.com/2011/07/iaas-cloud-computing.html>
- [4] Sinclair Schuller: Demystifying The Cloud: Where Do SaaS, PaaS and Other Acronyms Fit In? - <http://www.saasblogs.com/tag/iaas/>
- [5] The Future of Cloud Computing - <http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf>
- [6] Cloud Computing: Silver Lining or Storm Ahead?  
[http://iac.dtic.mil/iatac/download/Vol13\\_No2.pdf](http://iac.dtic.mil/iatac/download/Vol13_No2.pdf)
- [7] Négyesi Imre: CHANGING ROLE OF THE INTERNET IN THE LIGHT OF AN INTERNATIONAL CONFERENCE (Az internet szerepének változása egy nemzetközi értekezlet tükrében) (Hadmérnök on-line, III. évfolyam (2008) 3. szám, 147-153. oldal, ISSN 1788-1919);

**Szalai Máté**  
szalai.mate@zmne.hu

## ERASMUS

### *Absztrakt*

*Jelen közlemény a Híradó Tanszék hallgatója beszámolójának rövidített változatát adja közre varsói résztanulmányai kapcsán.*

*This publication shows the final report of the cadet of Signal Department.*

**Kulcsszavak (keywords):** ERASMUS, WAT ~ ERASMUS, Military University of Technology (in Warsaw)

## BEVEZETÉS

A 2010/11. tanév őszi szemeszterében öt hóapot töltöttem el a Varsói Katonai Műszaki Egyetemen, a WAT-on. „Polak, Wegier, dwa bratanki, i do szabli, i do szklanki, oba zuchy, oba zwawi, niech im pan bóg blogoslawi!” „Lengyel, magyar két jó barát, együtt harcol, s issza borát, vitéz, s bátor mindkettője, áldás szálljon mindkettőre!” Ezzel a rímbe szedett közmondással, melyet a mai nappal már biztosan állíthatok, hogy Lengyelország és Magyarország minden állampolgára jól ismer, indultam el Varsó felé 2010. szeptember 28-án este 20:00-kor a budapesti Keleti pályaudvar vasútállomásáról.

### 1. A KEZDETEK

A pályaudvarra egyik barátom és az egyetemi tanárom kísért ki, akik elől igyekeztem elrejtetni a félelmemet, ami azonban izgalommal, kíváncsisággal és természetesen kalandvágygal keveredett a közel 12 órás vonatút során. Amint már a beszámolóim elején említettem a jól ismert közmondást, mely tartalmának érvényessége gyorsan megállapításra jutott azzal a kedves ténnyel, hogy a kabinban velem utazó lengyel lány 2 órányi beszélgetés után felajánlotta, hogy ha bármilyen problémám lenne a szállásom elfoglalásával illetve felkutatásával, készséggel áll rendelkezésemre.

A kollégiumi szállásom ismét magyar szálakhoz fűződtek, ugyanis Varsó „Bemowo” negyedében található, ami Bem József lengyel és magyar honvéd altábornagy után kapta nevét. Miután a szállást a szokásos bürokratikus és egyéb adminisztrációs ügyek után elfoglaltam, megérkeztek a szobatársaim Olaszországból és Törökországból. Őszintén szólva a lengyelországi tanulmányaim előtt kissé kíváncsisággal töltöttem el az általános érzés, mely az első alkalommal az anyaországuktól távolra kerülő embereket megérint a kommunikáció terén, vagyis hogy, hogy fogjuk megérteni egymást, és hogy fogunk egymással kijönni.

Azonban az első 5 percnél beszélgetés után rájöttem, hogy nem lesz semmi efféle problémánk egymással az elkövetkezendő fél év során.

Sajnos az Erasmus diákoknak szervezett „welcome week”-ről lemaradtunk, de ennek ellenére is nagyon gyorsan baráti szálak szövődtek. Az első hét az adminisztrációs ügyek intézésére volt szánva (amire szükség is volt).

## 2. ISMERKEDÉS A VÁROSSAL

Az ország fővárosa Varsó, ami mondhatni az ország közepén található, a maga 1,8 millió lakosával. A vasútállomás a város központjában található, szemben a Kulturális Palotával, amit még 1955-ben Sztálin építtetett a lengyel „barátaiknak” (a 231 méteres Kulturális Palota Lengyelország legmagasabb épülete). Egy régi varsói vicc szerint a város látképe innen a legszebb, mivel ez az egyetlen pont, ahonnan a torony nem látható. A város talán kicsit a szocialista időket idézi, ugyanis a 2. világháború után porig bombázták Varsó legnagyobb részét, és mivel tudjuk, hogy a világháború után Lengyelországban is a kommunista rendszer következett, így akaratlanul is, de szocialista stílusjegyek ragadtak az országra. Személy szerint építészeti szempontból a legnagyobb benyomást az Old Town (Óváros) hatotta rám, melyet nem véletlenül az UNESCO is a világörökség részévé nyilvánított. Ami még igen tetszett a lengyel fővárosban, hogy igen sok a zöld terület, a parkos rész. Ősszel, de szerintem a tavaszi időszakban a Łazienki Park csodálatos, tele állatokkal, virágzó növényekkel, fákkal, valamint itt a található az utolsó lengyel király nyári rezidenciája is.

## 3. TANULMÁNYOK

Az Erasmus tanulmányaimat a Wojskowa Akademia Techniczna Elektronika karán (Military University of Technology – Katonai Műszaki Egyetem) folytattam. Az egyetemet 1951-ben alapították és a mai napra Lengyelország TOP 10-es műszaki képzést folytató egyetemei közé sorolják. Az egyetem 2002-ben csatlakozott az Erasmus programhoz, és mára már 27 országból fogadnak hallgatókat. Azonban itt meg kell jegyeznem, hogy a többi varsói egyetemhez képest véleményem szerint le vannak maradva Erasmusos hallgatóik koordinálásában, programok szervezésében, ugyanis a félév során egyszer szerveztek hallgatóiknak egy városnézést, míg a többi egyetem a városban napról napra bulikkal, koncertekkel, kirándulásokkal igyekeztek programokat kínálni szabadidőnk kellemes eltöltéséhez.

Az egyetem műszaki képzése viszont kiemelkedő. Az 1970-es évektől egészen a rendszerváltásig minden évben 20-30 fő magyar katonatiszti hallgató tanult az egyetemen. A jelenlegi varsói magyar katonai attasé 1980-ba kiváló minősítéssel végzett az egyetemen. Ami a magyar oktatástól véleményem szerint eltér, és megkockáztatom jobb is, hogy az egyetem hallgatói több gyakorlati foglalkozáson vesznek részt az egyes tanórák keretében. Még egy pozitívum, hogy az iskola tanárai, munkatársai nagyon kedvesen, pozitívan és segítőkészen álltak hozzánk, tanulmányilag a maximumot nyújtották. A félév során 5 tantárgyat hallgattam:

- Satellite systems,
- Antennas and waves propagation,
- Remote sensing principles,
- Circuits and signlas,
- Signal processing fundamentals.

Ezek közül az Anennas and waves propagation illetve a Remote sensing principles volt a kedvencem, mert viszonylag sok (az otthonihoz képest több) gyakorlati foglalkozás volt. A tantárgyaim írásos zárthelyi dolgozatokkal zárultak.

#### 4. ÉLET A VÁROSBAN

A varsói tömegközlekedés egy rémálom. Az első napomon a kollégium felé tartva a buszon állva körülbelül 5 perc alatt sikerült megállapítanom, hogy a buszsofőrök nem tudnak vezetni, ugyanis egy vidámparkban egy hullámvasúton képzeltem magam, aminek pedig én nem vagyok a szerelmese (vagy csak az első 2 percig igen). Nagyon sok dugó van a belvárosban, nagyon kevés a buszsáv illetve, hogy csak egy metró vonaluk van. Mindezek ellenére azonban azt kell mondanom, hogy a tömegközlekedés jól szervezett, gyakran járnak a buszok, pontosak és szinte egész Varsót behálózzák. És plusz egy jó pont, hogy sokkal olcsóbb a tömegközlekedés, mint Budapesten, illetve a buszok, metrószerelvények állapota kifejezetten jónak mondható.

Az Erasmus pályázattal egy időben kellett leadni a jelentkezést a kollégiumi szállásért is. Szerencsésnek mondhatom magamat, hogy a kollégium az iskolától 5 perc séta távolságra van, nem úgy, mint a más egyetemeken tanuló ismerőseimnek, akik közül sokaknak 1 órást volt bejutni az iskolába. Az egyetemen tanuló többi lengyel hallgatóval közös szálláson voltunk elhelyezve. A szobák 3 fősek voltak, én 2 olasz sráccal laktam együtt, és minden 2 szobára volt WC és zuhanyzó. Minden szinten, a folyosó végén konyha található, 3 főzőlappal. A kollégiumban lakó többi lengyel diákkal nagyon jó kapcsolatban voltunk, esténként együtt buliztunk, főztünk vagy akár kártyáztunk. A földszinten mosoda is működött, ahova 1-2 nappal korábban kellett bejelentkezni. Pozitívum, hogy a Varsóban tanuló Erasmus hallgatók közül talán mi fizettük a legkevesebbet a szállásért (havi 300 zloty, ami kb. 22000 forintnak felel meg), de negatívum, hogy a portások, recepcióskok nem beszéltek angolul, így ennek köszönhetően szerintem az „Activity” nevű játékban is sokat fejlődtem. Ha a megélhetési árakat az itthoniakkal akarnám összehasonlítani, akkor azt mondhatom, hogy egy kicsit drágábbak (max. 10-20%). Nézzük például a szállást. Ez a 22000 forintos kollégium itthon drágának mondható, de kint, mint már említettem talán ez volt a legjobb ár (bár azt most megjegyzem, hogy a kollégium a külvárosba volt, 45-50 perc busszal bejutni a központba). Lengyelország szerte is ugyanúgy találni Tesco és Auchan áruházakat, McDonald's-ot, KFC-t és Burger Kinget, amelyek az itthoni árakhoz hasonló árakkal kínálják termékeiket. Amit talán egy kicsit drágábbnak találtam a félév során, az az éjszakai élet. Egy klubba átlagosan a belépő 10-12 zloty, sör, vodka 6-7-8 zloty, kóla 8-9 zloty. Nagyon élvezetes, kellemes társasági életet éltünk. Varsóban nagyon sok külföldi diák tanul minden szemeszterben, így könnyű volt barátokat szerezni a világ szinte minden pontjáról. Ha őszintén betartanám mindenkinek a szavamat, hogy az elkövetkező 1-2 évben meglátogatom, akkor eljutnék: (kezdem Magyarországhoz közelebbivel):

- Szlovákiába,
- Szlovéniába,
- Romániába,
- Csehországba,
- Olaszországba,
- Bulgáriába,
- Törökországba,
- Iránba,
- Indiába,
- Kínába,

- Indonéziába is.

Jól hangzik, ugye? ☺ Gyakran szerveztünk illetve kaptam meghívást nemzetközi vacsorákra, ahol Magyarország részéről paprikás krumpli, palacsinta, és csirkepörkölt volt az asztalon (persze mindez nem egy estén ☺), de megkóstoltam a kínai, indonéz, olasz és török konyha jellegzetességeit is. A félév során más varsói egyetemek szervezésében kirándulni voltam Krakóban, Auschwitzban és Prágában is. 2011 februárjában a Északi- tenger partvidékére (Gdansk, Sopot, Gdynia) is sikerült ellátogatnom szlovák és román barátaimmal. Bár igaz nem a legmegfelelőbb időben látogattuk meg az Északi- tengert, mert egyrészt nagyon hideg volt, másrészt elég kihaltak voltak a városok, de mindezek ellenére is megérte elmenni, hiszen csodálatosan szép városokról van szó.

### ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Tehát összességében egy remek féléven vagyok túl, talán az egyetemi tanulmányaim félévei közül a legjobban. Varsó egy nagyszerű város, tele szórakozással, kalanddal, nyüzsgő éjszakai élettel, kulturális látnivalókkal, múzeumokkal, rengeteg kedves emberrel és gyönyörű lengyel lányokkal. Az Erasmus program nem csak arra adott lehetőséget, hogy az angol nyelvtudásomat fejlesszem, hanem arra is, hogy új kultúrákat, embereket ismerjek meg, valamint hogy nagyon fontos élettapasztalatot tudtam szerezni. Személy szerint, 2010. szeptember 28-a este 20:00-ra tekerném vissza az idő kerekét, ha tudnám, és újra átélhetném azokat az élményeket, amelyeket már senki sem tud tőlem elvenni. Remélem a lengyelországi tapasztalataimat a további életem, munkám során kamatoztatni tudom. Én csak ajánlani tudom, hogy minél többen vegyetek részt az Erasmus programban, hiszen külföldön élhettek, tanulhattok, ismerkedhettek, új baráti kapcsolatokat alakíthattok ki a világ minden pontjáról érkezőkkel, és mint már említettem nagyon hasznos élettapasztalatokat szerezhettek.

### FELHASZNÁLT IRODALOM

[1] Szalai Máté: Kari beszámoló - ZMNE

**Ifj. Veres György**  
veresgy@tuzoltosagbp.hu

## TÜZVÉDELMI STRATÉGIA

### Absztrakt

*A szerző ebben a tanulmányban definiálja a tűzvédelmi stratégia fogalmát, megfogalmazza a tűzvédelmi stratégia célját és elemzi a tűzvédelmi stratégia elemeit.*

*The author defines the concept of fire protection strategy, formulates the aim of fire protection strategy, and analyzes the components of fire protection strategy in this study.*

**Kulcszavak (key words):** tűzvédelem, tűzbiztonság, stratégia ~ fireprotection, fire safety, strategy,

### BEVEZETÉS

A magyar tűzvédelmi szabályozásban nem jelenik meg a tűzvédelmi stratégia fogalma. Azonban a tűzvédelmi törvény<sup>31</sup> 18. § (1) bekezdése értelmében értékelni kell a veszélyeket, illetve azt, hogy a körülmények megfelelnek-e a jogszabályi előírásoknak, különben nem hozhatók meg a tűzbiztonságot biztosító pozitív intézkedések. Át kell tekinteni, milyen veszélyek fenyegethetik a személyeket, mennyire súlyosak a veszélylehetőségek és hány személyt fenyegethetnek.

### 1. A TÜZVÉDELMI STRATÉGIA MEGHATÁROZÁSA

Általában a stratégia meghatározható, mint cselekvések hosszabb távú terve egy bizonyos cél elérése érdekében. Megkülönböztetjük a taktikától és az azonnali akcióktól, mivel a stratégia a cselekvések és azok végrehajtásához szükséges erőforrások biztosítását időben kiterjedten gondolkodva tervezi meg. Stratégián célok, valamint a célok eléréséhez szükséges eszközök és módszerek együttesét értjük.

A tűzvédelmi stratégiát úgy definiálhatjuk, hogy miként használjunk vagy kombináljunk a tűzvédelmi mérési eredményeket, adatokat, hogy a kitűzött tűzbiztonsági célokat elérjük. Egy adott létesítménynél egy, de akár több tűzbiztonsági cél is felmerülhet.

### 2. A TÜZVÉDELMI STRATÉGIA CÉLJA

A tűzvédelmi célok az alábbiak szerint foglalhatók össze:

- épületben benn tartózkodó személyek védelme,
- a beavatkozó tűzoltók védelme,
- vagyoni védelem,

---

<sup>31</sup> 1996. évi XXXI. törvény a tűz elleni védekezésről, a műszaki mentésről és a tűzoltóságról

- szomszédos tulajdonosok vagyonának védelme,
- üzleti folytonosság biztosítása,
- megakadályozni egy teljes gazdasági tönkremenetelt,
- környezetvédelem.

Amikor a tűzvédelmi célok megváltoznak a tűzvédelmi stratégiát is változtatni szükséges. A rendeltetés megváltoztatási építés hatósági engedélyeztetési eljárás megszüntetésével ez még inkább előtérbe kerül, hiszen sok olyan épület funkcióváltás történik, amely feltételezi a jogkövető állampolgári magatartást.

Az általános irányvonal lefektetése a legfontosabb feladat, hogy megértsük a lehetséges utakat a tűzbiztonsági célok elérése érdekében. A kvalitatív megközelítése a tűzbiztonság bemutatására, magába foglalja a fő elemeket úgy, mint tüzmegeelőzést és a szervezeti irányítást logikai formában. Amennyiben a tüzek megelőzésére tett rendszabályok, intézkedések 100 %-ot biztosítanak minden időben, akkor nem lenne szükség tűzoltóságokra. Nincs olyan rendszer vagy szabályzó, amely 100 %-os biztonságot nyújtana, lehetetlen az épített környezetben a tűzkeletkezést teljesen megelőzni.

A vizsgálatok szükségesek – mérések, valószínűség számítás, valamint modellezések - a tüzek keletkezésének elemzéséhez.

A tűz hatásának kezelése megvalósítható, illetve a veszélynek kitettek kezelhetőek úgymint személyek, épületszerkezetek, tevékenységek, környezet stb. A tűzbiztonság függ a megfontolt céloktól vagy a tüznek kitett hatásoktól. A veszélynek kitetteket teljes mértékig nem tudjuk lecsökkenteni. A veszélyek elleni védelem épületek esetében a tűzvédelmi előírásokban realizálódik. Ez két fő biztonsági veszély elleni védelmet tartalmaz:

a.) veszélytől való eltávolodás biztosítás:

- ideiglenes védett hely: lépcső, közlekedő,
- biztonságos tér: utca, nyitott tér.

b.) védett tér biztosítása: a tűz keletkezésének utáni elégséges időig fenntartható épületen belüli védett tér

### 3. A TŰZVÉDELMI STRATÉGIA ELEMEI

A tűzvédelem aktív elemei tűz, égéstermékek jellemzőinek detektálása alapján beépített vezérlő elem vagy külső vezérlés által avatkoznak be, vagy jelzést adnak felügyeleti rendszerek felé. A passzív elemek a tűz tovább terjedését akadályozzák, amelyek épületbe, építménybe beépített építési termékek csoportja megfelelő tűzvédelmi osztállyal, tűzállósági teljesítmény jellemzővel és tűzállósági határértékkel.

A passzív és aktív tűzvédelmi potenciális stratégiai elemek az alábbiak:

- beépített tűzjelző berendezés,
- beépített tűzoltó berendezés,
- menekülési utak kijelölése,
- tartalékvilágítás<sup>32</sup>,
- kiürítési útvonalak védelme,
- tűzálló épületszerkezetek, tűzszakaszolás,
- hő- és füstelvezető rendszerek,
- vészhelyzeti szervezet felállítása,
- kiürítési tervek elkészítése,

---

<sup>32</sup> Emergency lighting: olyan világítás, amely akkor lép működésbe, amikor a normál világítás tápellátása meghibásodik

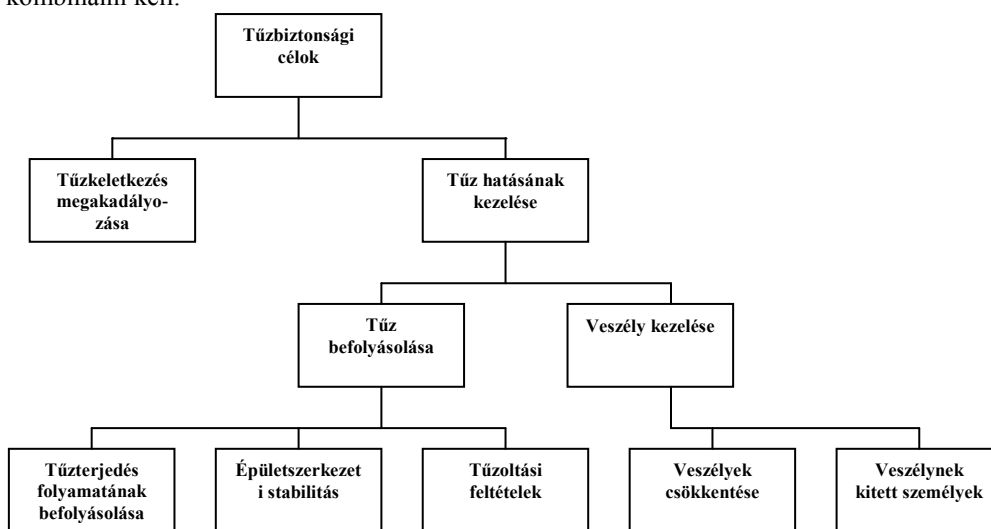


- kommunikáció biztosítása épületen belül és kívül.

#### 4. A TŰZVÉDELMI STRATÉGIA KIVÁLASZTÁSA

A fő kérdés a tűzvédelem során meghatározni melyik stratégia működik a legjobban az épület és a bent tartózkodó személyek védelmében, valamint meg kell meghatározni azokat a tűzvédelmi célokat, amelyek biztosítják a kiválasztott stratégiát. A népi bölcsesség ismeri azt a mondást, mely szerint jobb megelőzni, elébe menni a dolgoknak, mint utánuk kullogni. A kutatások kimutatták, hogy a fejlődő tűzvédelem csökkentette a tüzesetek számát, de azt nem szüntette meg.

A minőségi stratégia szinten egyszerűen meg lehet ítélni, hogy a veszélytől való eltávolítás, eltávolodás pl. kórházak intenzív részlegéből vagy ápolóintézetekből nem biztosítható teljes mértékben vagy lehetetlen. Sok esetben a tűzvédelmi stratégiát - 4. ábra - kombinálni kell.



1. sz. ábra: A tűzbiztonság stratégiája[1]

Az első szint meghatározza az alapvető elveket, amelyek az épületben benn tartózkodók, beavatkozó tűzoltók, szomszédos épületekbe tartózkodók személyek védelme, valamint ingó és ingatlan vagyonkárosodásnak megakadályozását. A tűzvédelmi stratégiának biztosítania kell az üzleti folytonosság biztosítását, megakadályozni egy teljes gazdasági tönkremenetelt, valamint környezet védelemét.

##### 4.1. A tűzvédelmi stratégia második szintje

A tűzvédelmi stratégia második szintje két stratégiát tartalmaz:

- a tűzkeletkezés megakadályozását, ami feltételezi a 100 %-os tűzbiztonságot,
- valamint a tűzterjedés irányítását, hatásának kezelését.

Az emberek döntő többsége úgy gondolja, hogy az előírások betartásával ez kielégíthető, ami természetesen legtöbbször elegendő is. Azonban belátható, az ábra logikáját követve

meghatározható, hogy melyik tűzvédelmi stratégia használható és a jogszabályi előírásoknak melyik felel meg jobban.

### 4.2. A tűzvédelmi stratégia harmadik szintje

A tűz keletkezésének, hatásának befolyásolásának célja minimalizálni a sérüléseket, halálhoz vezető okokat. Két csoportra osztjuk: a tűz keletkezése vállalására és a veszélyek vállalására. A veszély vagyona és emberekre utal. Mint utaltam rá, 100 %-os tűzbiztonság nincs a jogszabályok, elfogadnak egy sokrétű stratégiát remélve, hogy a tűz és a veszély csökken és irányítható.

### 4.3. A tűzvédelmi stratégia negyedik szintje

A negyedik szint jelenik meg normatívákban, szabványokban és jogszabályokban. Ezen szabályozókban foglaltak az alábbiak szerint csoportosíthatók:

- tűzterjedés folyamatának ellenőrzése: az éghető anyag és a környezet ellenőrzését, befolyásolását jelenti. „Nem éghető” A1 és A2 tűzosztályú épületszerkezetek, tűzszakaszolás (tűzgátló falak, tűzgátló födémek, tűzgátak), az épületben tartózkodók mozgásának, menekülésének védelmének érdekében. A stratégiának nagy tűzvédelmi hatása van, de önmagában nem elégíti ki teljesen a célokat, mivel az épületben éghető anyagok tárolása is történhet.
- épületszerkezet stabilitás: a tűz fejlődés és füst keletkezés csökkentése érdekében beépített épületelemek tűz ellenállása, a kiürítés és a beavatkozás, az omlások, tűzterjedés megakadályozása érdekében,
- tűzoltás feltételek: automatikus és kézi tűzoltási rendszerek. A tűz eloltásának ideje nagy hatással van a kiürítési időre. A beépített automatikus tűzoltó berendezések (pl. sprinkler rendszer) magas megbízhatósági mutatóval rendelkeznek és hatásosak, de egyes tanulmányok rámutatnak, [2] hogy nem vehető 100%-os megbízhatóságú tűzvédelemi rendszereknek. A stratégia a tűzvédelmi célokat önmagában nem elégíti ki.
- veszélyek kezelése: mivel a stratégiában kikerülhetetlen, a személyek ki lesznek téve a tűz által okozható veszélynek.
- veszélyek mennyiségének csökkentése: a veszélyeknek kitett személyek számát és tűz keletkezési kockázatokat<sup>33</sup> [3] csökkenteni szükséges.

## ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Tűzvédelmi stratégiának tekinthetünk, tehát minden olyan intézkedést, amelynek célja a tűzveszélyforrások, illetve hatásaik csökkentése, vagy megszüntetése. A tűzvédelmi tevékenységnek mindig is a prevenció volt az egyik legfontosabb eleme. A tűzmegelőzés legfőbb feladata a létesítés és a használat során a megfelelő tűzvédelmi stratégiai elemek használata a kötelező jogszabályi előírásokon túl vagy a jogszabályi eltérés során az ésszerű ellensúlyozó alkalmazása a megfelelő tűzbiztonsági szint fenntartása érdekében.

---

<sup>33</sup> kockázat: egy nemkívánatos esemény előfordulási valószínűségének és súlyosságának együttes hatása

### FELHASZNÁLT IRODALOM

- [1] Veres György: A tűzbiztonság stratégiaja - saját
- [2] Richardson, J.K.: An Assessment of the Performance of Automatic Sprinkler Systems, Fire Technology, Vol. 19, No. 4, National Fire Protection Association, Quincy, MA, 1983.
- [3] Dr. Balogh Albert – Földesi Tamás: A minőségügy nemzetközi értelmező szótár. Kiadó: EOQ MNB 2003



**Veres György**  
veres.gyorgy@zmne.hu

## **A KATONAI ALKALMAZÁSÚ KOMPLEX VILLAMOS RENDSZEREK ÜZEMELTETÉSÉVEL KAPCSOLATOS OKTATÁSI KÉRDÉSEK**

### **Absztrakt**

*A szerző összefoglalja a katonai alkalmazású komplex villamos rendszerek sajátosságait és ezek üzemeltetésére, üzembenntartására alkalmas mérnök tisztekkel szemben támasztott fontosabb követelményeket, valamint ebből a fejlődésből a katonai felsőoktatásra háruló megújult feladatokat.*

*The author summarizes the specifics of complex electrical systems in military use, the relevant requirements to their operation and the maintenance demanded to the officer engineers, and the new tasks deriving from their development to the higher military educational system.*

**Kulcsszavak (key words):** mérnök-képzés, hadmérnök, komplex rendszer, elektrotechnika, analóg elektronika, digitális elektronika ~ engineer education, military engineer, complex system, electrical engineering, analog electronics, digital design

### **BEVEZETÉS**

Az elmúlt évtizedekben tapasztalt rendkívül dinamikus fejlődés alaposan megváltoztatta mindazokat a technikai eszközöket és berendezéseket, amelyekkel a mindennapi élet során naponta találkozunk. Természetesen e fejlődés hatással volt a katonai technikai rendszerekre is. A rendszerbe állított új és a jövőben is várhatóan még újabb eszközök üzemeltetése szükségessé teszi, hogy a jövő mérnök-tisztjeit az általánosan szükséges mérnöki alapismereteken túl a legmodernebb műszaki ismeretek elsajátításával készítsük fel jövőbeli feladataik sikeres teljesítésére.

Ez a cikk a hadmérnökképzésen belül csak a katonai elektronika szakirányon tanuló hallgatók képzésével foglalkozik, hangsúlyozottan csak a szakmai törzsanyag villamos jellegű tananyagrésze oldaláról közelítve.

## **1. A KATONAI ALKALMAZÁSÚ KOMPLEX VILLAMOS RENDSZEREK ÜZEMELTETÉSÉRE ALKALMAS HADMÉRNÖKÖK RENDELTETÉSE**

A tudományos-technikai forradalom felgyorsulásából és a NATO-hoz való csatlakozásból következő feladatok minél jobb megoldásában jelentős szerepe van és lesz a Magyar Honvédség hadmérnök tisztjeinek. A katonai elektronika szakirányon végzett tisztek elsősorban a honvédség elektronikai és elektrotechnikai rendszerein belül látnak el feladatokat, és alapvető szerepük van azok optimális működtetésében. A mérnöktisztek döntő többsége a ZMNE Bolyai János Katonai Műszaki Karán szerzi meg diplomáját.

A mérnöktisztek katonai szakmai képzésének célja az, hogy a szak gyakorlati műveléséhez szükséges általános műveltségi, műszaki tudományi, biztonság-technikai,

minőségbiztosítási, környezetvédelmi társadalomtudományi alapok, általános és speciális katonai, katonai-vezetői ismeretek, konkrét gyakorlati módszerek és reprodukció mérnöktisztai alkalmazás birtokában megfelelő gyakorlat után az MH-nál rendszeresített elektronikai és elektrotechnikai rendszerek üzemeltetési, üzembenntartási és irányítási feladatait, a tervezés és a katonai műszaki fejlesztési részfeladatokat, valamint az első tiszti beosztásukkal járó szakmai feladatukat önállóan meg tudják oldani az egyes szakirányoknak megfelelően.

A Karon hallgatóink mérnöki tudásszintjét a szakmai törzsanyag és a differenciált (katonai) szakmai ismeretek tanulmányi területekhez tartozó tantárgyai együttesen biztosítják. Az így megszerezhető mérnöki szakmai ismeretanyag legalább egyenértékűnek tekinthető a jelenlegi polgári felsőoktatásban végzett mérnökökével. Van azonban egy alapvető különbség: a karon végzett mérnökök szélesebb spektrumú képzést kapnak, a hasonló képzési profilú polgári főiskolákon végzettekhez képest. A legtöbb polgári főiskolán – különböző tradíciók és az utóbbi időben a piaci viszonyok miatt – a képzés specializáltabb, azaz keskeny spektrumú. Mindkét fajta képzési struktúrának megvannak az előnyei. A ZMNE Bolyai János Katonai Műszaki Kar rendeltetését, céljait és a képzésben résztvevő hallgatók érdekeit figyelembe véve, a mérnök-képzésben az egyes szakirányok igényeit figyelembe vevő, széles spektrumú képzés a célravezetőbb. A végzett mérnökhallgatók olyan jól megalapozott szakmai szemléletmóddal és széleskörű, BSc szintű tudással rendelkeznek, amely alkalmassá teszi őket a későbbiek során felmerülő gyakorlati problémák megoldásához szükséges speciális elméleti ismeretek elsajátítására.

A széles spektrumú képzésnek a hallgatók, az oktatók és az egész képzési rendszer szempontjából megvannak a nehézségei, hiszen – a polgári felsőoktatásban elképzelhetetlen módon – egyidejűleg, egymástól távoli mérnöki szakterületek ismeretanyagát kell megfelelő módon elsajátítani és ezeket az ismereteket a Villamosmérnöki és Természettudományi Intézet Elektronika Tanszéke által a szakmailag elvárt igényeknek megfelelően kell a szakmai törzsanyag oktatása során megalapozni.

## 2. A SZAKMAI TÖRZSANYAG

Az ehhez a tanulmányi területhez tartozó tantárgyak oktatásának fő célja – az általános mérnöki ismeretek elsajátíttatása és a korszerű mérnöki szemléletmód megalapozása mellett – az egyes szakirányok szakmai alapozásának biztosítása. A szakmai törzsanyag tantárgyainak tananyaga és oktatásuk szintje nagymértékben meghatározza a Kar mérnök-képzésének színvonalát. Amellett, hogy az ehhez a tanulmányi területhez tartozó tantárgyak oktatásánál biztosítani kell a szakmai közvélemény által elvárt mérnöki alaptudás elsajátítását (a polgári főiskolákon oktatott tananyaggal, illetve ismeretszinttel a mérnök-képzésen belül itt van lehetőség az egyértelmű összehasonlításra), a mérnökhallgatók ezen a tanulmányi területen belül találkoznak először a mérnöki gondolkodás alapjaival. Ezért rendkívül fontos a tanulmányi terület tantárgyai tananyagának és a tantárgyak egymás közötti kapcsolatának szakmailag és pedagógiai tudományos alapokon nyugvó felépítése, a tananyag-kiválasztás korszerű elveinek alkalmazása, **a tananyagszerkezet és a tantárgyak közötti kapcsolatrendszer egzakt matematikai alapokon nyugvó megtervezése.**

## 3. A KATONAI ALKALMAZÁSÚ KOMPLEX VILLAMOS RENDSZER NÉHÁNY SAJÁTOSSÁGA

A közelmúltig érvényben volt egyik alapvető villamos szabvány (MSZ 1600) a komplex villamos berendezés fogalmát a következőképpen definiálja: „komplex az a villamos

berendezés, amely nem sorolható sem a gyengeáramú, sem az erősáramú berendezések közé”. A mérnökök – így a Karon végzett mérnök-hallgatók – döntő többsége **komplex berendezések (rendszerek)** üzemeltetésével, tervezésével foglalkozik. Az ilyen rendszereknél – a műszaki-gazdasági szempontokból optimális megoldások keresése mellett – főleg a várható hiba jellegét, romboló hatását, a különböző villamos, elektronikai, irányítástechnikai, hírközlési paraméterek megváltozásait figyelembe vevő, egyedi mérlegelésekkel kell eldönteni, hogy az erősáramú, a gyengeáramú, vagy mindkét fajta **alrendszerre** vonatkozó előírásokat kell-e teljesíteni.

Az erősáramú berendezésekre vonatkozó előírások általában a nagyobb zárlati teljesítmény, a beálló hibákkal kapcsolatos energia, a közvetlenebb életveszély miatt szigorúbbak. A gyengeáramú berendezésekre vonatkozó előírások elsősorban a különböző jeltorzító hatásokat igyekeznek kiküszöbölni (az érintésvédelemre vonatkozóan természetesen itt is be kell tartani az ilyen berendezésekre vonatkozó speciális előírásokat).

[1]

A villamos és mágneses fizikai jelenségek elméleti törvényszerűségeivel és azok gyakorlati felhasználásával az elektrotechnika foglalkozik. Ennek tárgykörébe tartozik a különböző villamos, mágneses és elektromágneses eszközök készülékek, gépek, berendezések tervezése, fejlesztése, gyártása, ellenőrzése, üzemeltetése. Az elektrotechnika két nagy területre, az energetikára és az elektronikára bontható. Az energetika a fémekben és az elektrolitokban lejátszódó fizikai folyamatokat és ezek áramköröit tárgyalja. Az elektronika olyan eszközökkel és alkatrészekkel foglalkozik, amelyekben az áramvezetés vákuumban, gázokban vagy félvezetőkben valósul meg. Az elektronikát az alkalmazási terület szerint tovább oszthatjuk híradástechnikára, ipari elektronikára és számítógép technikára. A feldolgozott jel fizikai jellemzői alapján az elektronika lehet analóg- és digitális elektronika.

A különböző **elektronikai alrendszerek** (analóg és digitális áramkörök) fejlődése miatt egyre modernebb eszközök kerülnek rendszeresítésre az MH-ban is, ezért e rendszerek elméleti és gyakorlati kérdéseinek oktatása a Karon folyó mérnök-képzésben egyre nagyobb szerepet játszik. Különösen a digitális rendszerek elméleti alapjainak tisztázása, a gyakorlati alkalmazások számára rendkívül fontos üzemi paraméterek értékelése sok tekintetben alapvetően eltérő szemléletmódot kíván a még mindig lényeges szerepet játszó analóg rendszereknél megszokotthoz képest. Ennek egyik fontos következménye, hogy a tananyagban néhány fontos változtatást mindenképpen végre kell hajtani.

Az elektronikai alrendszert illetően, az elmúlt évtizedekben minden korábbit felülmúló, elképesztően dinamikus növekedés volt tapasztalható az analóg elektronika, és különösen a digitális elektronika területén. Az elektronikus adatfeldolgozás, folyamatszabályozás, a számítógépek, az összetett funkciókat végző berendezések elterjedése és továbbfejlesztése alapjaiban változtatja meg a hadseregek stratégiai és taktikai lehetőségeinek eszközeit. A számítógépek alkalmazása a társadalmi-gazdasági jelenségek és a hadügy területén új vizsgálati lehetőségeket tár fel.

Az MH-ban rendszeresített technikai eszközszínvonalra jellemző példa, hogy 1990. elején a rendszerben lévő, erkölcsileg és technikailag is elavult lokátorok 95 %-a még analóg működésű (40 – 42 %-a az 1950-es évek, további 42 %-a az 1960-as évek ipari bázisára épülő) elektroncsöves berendezés volt, amelyek átlagos meghibásodás mentes működési időtartama 10 – 20 óra. A radartechnika közben tovább fejlődött és mai legfontosabb jellemzője a digitális jelfeldolgozás és a mikrohullámú félvezetők alkalmazása. [2]

Az elektronika, ezen belül mindenekelőtt a digitális technika dinamikus fejlődése új, minden eddiginél hatékonyabb, nagy találati pontosságú, precíziós fegyverek kifejlesztését eredményezte.

A számítógépek szerepe jelentős a felgyorsult információ-áramlásban, az ismeretanyag feldolgozásában, mert ez által az ember fejlődésének új korszaka bontakozik

ki. Ahhoz a minőségi ugráshoz, ami a természet és a társadalom mozgástörvényeinek megismerésében bekövetkezett, az informatika adja a lehetőséget. Ennek következtében a klasszikus gépi nagyiparra alapozott civilizációt felváltja egy újabb és fejlettebb műszaki civilizáció, amelynek a fejlett tudomány intenzív és széleskörű alkalmazása lesz az alapja. Egy új típusú társadalmi-termelési korszak van kialakulóban, amelyet egyes szakirodalmakban információs korszaknak, illetve információs társadalomnak neveznek [3].

A védelmi szférában – a technológiai fejlődésre alapozva – új, komplex, a katonai gondolkodásmódot gyökeresen megváltoztató fogalmak és tevékenységek jelentek meg. Ezek között is meghatározó jelentőségű az 1995-től alkalmazott információs műveletek (Information Operations), amely nem más, mint valamennyi katonai képesség (közte a műveleti biztonság, a katonai megtestesítés, a pszichológiai hadviselés **az elektronikai hadviselés** és a fizikai megsemmisítés, illetve a számítógép-hálózati hadviselés) integrált alkalmazása, a felderítés valamennyi formájával, továbbá híradó és informatikai rendszerrel támogatva.

Az információs fölény elérésére az információs műveletek mellett olyan új koncepciók jelentek meg, mint a **Hálózatközpontú Hadviselés** (NCW –Network Centric Warfare), melynek lényege a földrajzilag elkülönült harctéri entitások hatékony összekapcsolása, vagy hálózatba kapcsolása. A hadműveletek vezetése számára rendelkezésre álló sáv szélesség fokozatosan nőtt és továbbra is nőni fog.

Egyre dinamikusabban fejlődik a Magyar Honvédség infokommunikációs rendszere, amely szorosan együttműködik a NATO híradó és informatikai rendszerével. A hatékony működtetés biztosításához elengedhetetlenül szükséges az állomány magas szintű felkészítése a korszerű infokommunikációs eszközök alkalmazására. A XXI. század hadserege a legmodernebb digitális elektronikus eszközökkel jól ellátott digitális hadsereg lesz, amely a tevékenységét – szükség esetén – a digitális hadszíntéren fejti ki, Hálózatközpontú Hadviselést alkalmazva. [4]

A csapathíradás területén felkészülnek a mobil számítógéphálózat-alapú harcvezetésre (NCW/NC2-Net Control Warfare/Net Command and Control) és a szoftvervezérlésű frekvenciaugratásos URH csapatrádiók bevezetésére így a Magyar Honvédségben rendszerítésre kerültek a norvég fejlesztésű multifunkciós harcászati rádió-berendezések: a Kongsberg által kifejlesztett MH 300-as kézi, az MP 300-as hordozható és az MV 300-as járműbe építhető változatok.

A XXI. század hadseregére a magas fokú elektronizáltság lesz a jellemző, ahol alkalmazzák a modern elektronika legújabb vívmányait. Mindegyik haderőnem valamennyi fegyverneme alkalmaz olyan technikai eszközöket, amelyek a villamosság és a mágnesség alkalmazásán alapul. Vannak olyanok, amelyek (pl. a radarok, a híradó berendezések, a rádióelektronikai felderítő és zavaró berendezések, stb.) működése kizárólag az elektromágnességen alapszik. Ezeknek a berendezéseknek a gyártásához, fejlesztéséhez, kutatásához és üzemeltetéséhez alapos felkészültségű, magas szakmai intelligenciájú szakemberekre van szükség.

## ÖSSZEGEZÉS, KÖVETKEZTETÉSEK

A mérnöktisztek képzésének szakmai-műszaki tartalmát, a végzett hallgatók ez irányú tudásszintjének kialakítását a szakmai törzsanyag és a differenciált (katonai) szakmai ismeretek tanulmányi területekhez tartozó tantárgyainak a kor igényeihez igazodó színvonalas oktatása együttesen biztosítja.

A végzett mérnökhallgatók olyan jól megalapozott szakmai szemléletmóddal és széleskörű, BSC szintű tudással rendelkeznek, amely alkalmassá teszi őket a műszaki-szakmai feladataik színvonalas ellátására és a későbbiek során felmerülő gyakorlati



problémák megoldásához szükséges speciális elméleti ismeretek elsajátítására. Az ilyen színvonalú képzési eredmény biztosítása szükségessé teszi az oktatott tananyag folyamatos felülvizsgálatát és mindenkor technikai színvonalhoz történő, tudományos kiigazítását, továbbfejlesztését.

### **FELHASZNÁLT IRODALOM**

- [1] Rádli Tibor – Zsigmond Gyula: Villamosmérnök-képzés a Bolyai János Katonai Műszaki Főiskolán. Hadtudomány 1998. 4. sz.
- [2] Fekete László mérnök alezredes: Új forma és tartalom a katonai villamos üzemmérnök képzésben, Egyetemi doktori értekezés, 1992. 53. p.
- [3] Dr. Haig Zsolt–Dr. Várhegyi István: Hadviselés az információs hadszíntéren, Zrínyi Kiadó, Budapest, 2005. 53- 55.p.
- [4] Mikita János mk. ezredes: A katonai infokommunikációs rendszerek fejlődésének főbb irányai. Bolyai Szemle 2001. X. évf. 1sz



**Tőreki Ákos**  
akos.toreki@gmail.com

## **A C2 RENDSZER, MINT A HÁLÓZATKÖZPONTÚ HADVISELÉS ESZKÖZE**

### **Absztrakt**

*A közlemény betekintést nyújt napjaink katonai műveleteinek jellemzőiből, valamint a szövetségi tagságból adódó technikai, technológiai követelmények egyik élenjáró ágának, a vezetés-irányítási rendszerek rendeltetésének, funkcióinak alapjaiba és a Magyar Honvédség e téren történő fejlesztési koncepciójába.*

*This publication shows the development of the Hungarian C2 system.*

**Kulcsszavak (keywords):** *hálózatközpontú hadviselés, vezetés-irányítás, tábori C2 rendszer ~ NCW, Command-Control, field C2 system*

### **BEVEZETÉS**

A modern fegyveres erők a napjainkban végrehajtott hadműveletek során nagymértékben támaszkodnak az információs társadalom technikai, technológiai vívmányaira. Főként a vezetés és irányítás területén van szükség olyan rendszerek alkalmazására, melyek révén lehetővé válik a csapatok hatékonyabb vezetése. Persze a technikai fejlődés vívmányainak alkalmazása a hadműveletek elméletére is hatással bír, így a kor stratégiai gondolkodói új hadviselési formát határoztak meg, amely az információk hatékony feldolgozását szolgáló információs, kommunikációs hálóra támaszkodva a katona hadműveletek teljes dimenziójának „modellezésén” alapul.

A hálózatközpontú műveletek sikere – a kiválóan felkészült, kiképzett állományon, a kezdeményező-képesség meglétén, valamint a katonai műveletek megvívása módszerének megértésén túl – függ a technikai-technológiai felszereltségen is. Ezért többek között a szövetségi tagság követelményeként megjelenő együttműködési képesség biztosítása, valamint a jelen és a jövő katonai műveletei által megkövetelt gondolati beállítottság kialakítása érdekében lépést kell tartani a modern eszközök és eljárások alkalmazása, azon belül a vezetés és irányítás eszközrendszerének fejlesztése terén.

### **1. A HÁLÓZATKÖZPONTÚ HADVISELÉSRŐL**

*„A hálózatközpontú katonai művelet lényege, hogy egy rendszert alkot a felderítés, a döntés és a cél pusztítása a katonai műveletek végrehajtása teljes időtartamában.”*<sup>0</sup> Ami alapjául szolgált a hálózatközpontú hadviselés kialakulásához, az a technikai eszközök gyors fejlődése volt. Bár napjaink katonai műveleteinek sikere továbbra is a jól felkészült katonákon, első sorban a parancsnokokon áll vagy bukik, a modern technikai eszközök és új technológiák alkalmazása megváltoztatta a műveletek végrehajtásának módját és formáját.

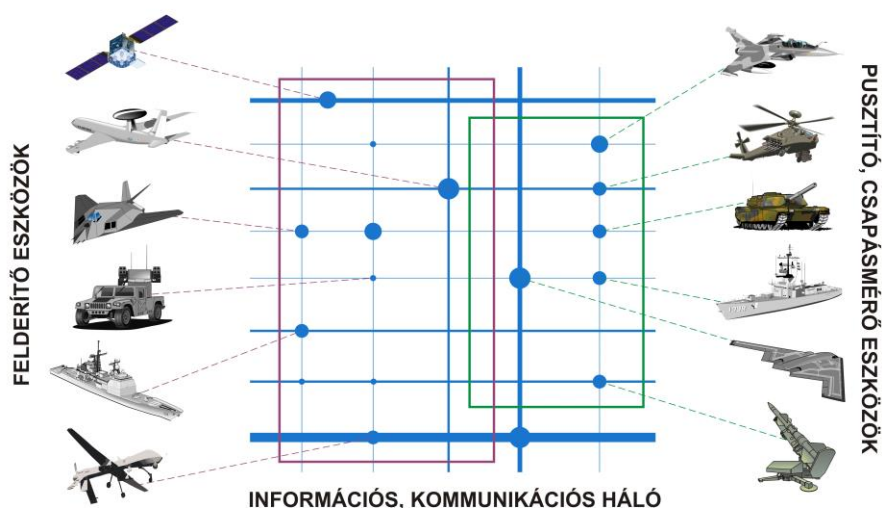
Visszatérve a hálózatközpontú katonai műveletek lényegének megfogalmazásához a felderítés, a döntés és a fegyverzet egy rendszerbe történő integrálásával lerövidült az információ megszerzése, a döntés meghozatala és a csapás kiváltása közötti idő, így a

katonai műveletek üteme is felgyorsult. Ezen műveletek alappillére a hadszíntér szereplői közötti folyamatos információáramlás biztosítása a teljes időtartam alatt, amely által a fegyveres erő különböző haderőneveinek, fegyvernemeinek és szakcsapatainak rugalmas együttműködése érhető el.

A folyamatos és gyors információáramlásnak köszönhetően a műveleti parancsnok állandóan valós helyzetképet kap a hadszíntéri tevékenységről (saját csapatok helyzete, ellenséges erők elhelyezkedése, terepi adottságok, időjárási viszonyok stb.) és a rendelkezésre álló – valós idejű – információk birtokában hozza meg döntését. A döntéshozatal felgyorsítása mellett lehetővé teszi, hogy a megfelelő időben a megfelelő katonai eszköz kerüljön bevetésre.

A hálózatközpontú módszer az információk megszerzésének és felhasználásának új módját jelenti, amely lehetővé teszi, hogy minden információ a vezetés minden szintjén egy időben álljon rendelkezésre, és ennek megfelelően a döntések mindig a lehető leggyorsabban és a megfelelő szinten szülessenek. Az új módszer gyökeresen átalakítja a haderő vezetési rendszerét is.

A rendszer a különböző szinteken résztvevő elemeket hálózati rétegekbe osztja és a közöttük lévő kapcsolatot az információs, kommunikációs háló biztosítja.



1. sz. ábra: Az eszközök, rendszerek alkalmazása 0

A hálózatközpontú katonai művelet lényege tehát, hogy egyetlen integrált rendszerbe foglalja az érzékelőket, a döntéshozókat és a fegyverrendszereket. Eredményessége a döntési fölény kialakításának függvénye. A döntési fölény eléréséhez a hadszíntéren működő katonai vezetés minden szintjén képesnek kell lenni a pontos információk valós idejű megszerzésére, azok biztonságos továbbítására, valamint azonos elvek és eljárások szerinti értelmezésére. Mindehhez nyújt alapot a hadszíntéren kialakított információs és kommunikációs háló, azon belül az információ gyűjtésére és feldolgozására, majd a felhasználók által érhető formában történő megjelenítésére használt vezetés-irányítási rendszer.

## 2. A VEZETÉS ÉS AZ IRÁNYÍTÁS ELMÉLETE

Mielőtt rátérnénk a vezetés-irányítási rendszerek ismertetésére, vizsgáljuk meg a vezetés és az irányítás tartalmát, valamint a C2<sup>34</sup> jelentését:

A vezetés olyan tevékenység, amely során a vezető a vezetett szervezet tagjaként meghatározó befolyást gyakorol a szervezet tevékenységére az irányító által meghatározott feladatok végrehajtása érdekében, azonban a szervezet tevékenységének célját és rendeltetését nem változtathatja meg.

Katonai terminológiában a vezetés az alárendeltek befolyásolásának folyamata a parancsnoki szándék közvetlen megvalósítása érdekében. A vezetés a szervezet(ek) hatékony működtetésére, a csapatok vezetésére, tevékenységeik koordinálására irányul, amelyet az egyszemélyi katonai vezető végez. A vezetés megvalósulhat békeidőben, válságreagáló és katasztrófavédelmi műveletek során, háborús vezetésre történő átállás alkalmával, és háborús katonai tevékenységek végrehajtása közben.

Az irányítás pedig olyan tevékenység, amelynek eredményeként beavatkozás történik egy rendszer működésébe, annak érdekében, hogy egy ott értelmezett folyamat révén az irányító az irányított szervezeten kívülről meghatározó befolyást gyakoroljon az irányított szervezet tevékenységének minden területére. Egy adott rendszer (szervezet) tevékenységének a tervek (kitűzött célok) követelményeivel összhangban történő végrehajtására irányuló törekvés.

Az irányítás tehát olyan tevékenységi folyamat, mely során az irányítás jogkörével felruházott személy tervezi, szervezi, vezeti, és koordinálja a felelősségi körébe tartozó szervezet(ek)et.

A C2, vagyis a vezetés és irányítás pedig az előző két fogalom ötvözetéből áll, azaz a parancsnok(ok) jog- és felelősségi köre, illetve tevékenysége az erők irányítása és koordinálása, a műveletek végrehajtásához kapcsolódó parancsok megvalósítása érdekében.

A vezetés és irányítás kulcsfontosságú eleme maga a parancsnok. A vezetés művészetének és az irányítás tudományának kombinálása során a parancsnok vizualizálja a harcteret és az így kapott „képet” megosztja az alárendeltjeivel, vezeti alegységét és irányítja annak tevékenységét a küldetés sikeres teljesítése érdekében, mialatt folyamatosan értékeli a kialakult helyzetet.

## 3. C2 VEZETÉSI ÉS IRÁNYÍTÁSI RENDSZEREK

Műveleti területen a csapatok vezetéséhez elengedhetetlenül szükséges egy modern, megbízható szélsőséges körülmények között is megfelelően működő vezetési és irányítási rendszer. A hadseregekben egyre nagyobb tér nyer a vezetési és irányítási rendszerek digitalizálása, így az információs rendszerek legfontosabb tényezőivé is a digitalizált képességekkel rendelkező központok válnak. A vezetési és irányítási infrastruktúra a felderítés, hírszerzés, a műszeres megfigyelés, a doktrína, az eljárások, a szervezeti struktúrák, a személyi állomány, a felszerelés, a létesítmények, a híradó berendezések és a számítógépek rendszere.

A C2 rendszer (C2S<sup>35</sup>) egy harcvezetési rendszer, amely segítségével a parancsnok automatizált híradó és informatikai rendszerek nyújtotta „szolgáltatások” felhasználásával irányítja és koordinálja az alárendelt katonai szervezeteket. A rendszerben folyamatosan rendelkezésre állnak azok az információk, amelyekre a parancsnoknak (és törzsének) szüksége van a döntés meghozatalához (előkészítéséhez). Az információk feldolgozott és szűrt megjelenítésével a parancsnok sokkal gyorsabban képes meghozni a döntéseket,

<sup>34</sup> C2 – Command and Control (vezetés és irányítás)

<sup>35</sup> C2S – Command and Control System (vezetési és irányítási rendszer)

valamint az állandóan frissített, valós helyzetnek megfelelő információk birtokában a hibalehetőség is csökkenthető.

A C2 rendszerrel kapcsolatban érdemes kiemelni még két fogalmat, a *vezetés és irányítás információs rendszerét* (C2IS<sup>36</sup>) és a *vezetés és irányítás híradó rendszerét* (C2CS<sup>37</sup>). Az előbbi azt az informatikai rendszert takarja, amely a vezetés és irányítás informatikai támogatása érdekében kerül kialakításra, míg az utóbbi nem más, mint a katonai szervezetek között a vezetéshez és irányításhoz szükséges információkat továbbító hírendszer.

A vezetési és irányítási rendszerek számos szegmensből állnak, példaként egy tábori C2 rendszer a vezető szervezet, a vezetési pontokat, a hírendszert, az informatikai rendszert, továbbá a csapatok automatizált vezetési eszközeit foglalja magába.



2. sz. ábra: Egy C2 rendszer kezelői felülete [9]

A C2 rendszer különböző szervezeti elemekből (harcjárművek, vezetési komplexumok) és hardver elemekből (számítógépek, rádiók, szerverek) áll, alapját pedig egy rendszerszoftver alkotja.

A C2 vezetés-irányítási rendszerek komplex vezetési rendszerek, melyek rendeltetése, hogy egységbe foglalják a különböző forrásokból származó információk gyűjtését, tárolását, feldolgozását, címzettek felé történő továbbítását, a parancsnoki döntéshozatal folyamatának megkönnyítését, meggyorsítását, a vezetéssel és irányítással kapcsolatos feladatok támogatása érdekében. Tágabb értelemben feladatuk a parancsnoki tervezés, a döntéshozatal, a jelentések készítésének támogatása, csapatvezetési, fegyverirányítási, logisztikai, térképészeti, ABV, meteorológiai (stb.) támogatás biztosításával a közös és objektív helyzetkép megalakítása. Mindez által támogatja a szervezet és az alárendelt alegységek harctevékenységet, csökkenti a parancsnoki döntéshozatali, vezetési, irányítási folyamat idejét, továbbá biztosítja az együttműködési képesség kialakítását a műveleti terület más szereplőinek (például idegen országok hadseregeinek) rendszereivel.

A C2 rendszer főbb funkciói:

- törzstámogatás;
- katonai üzenetközlő rendszer;
- csapatvezetés;
- fegyverirányítás;
- tűzérségi támogatás;
- logisztika;

<sup>36</sup> C2IS – Command and Control Information System (vezetés és irányítás információs rendszere)

<sup>37</sup> C2CS – Command and Control Communication System (vezetés és irányítás híradó rendszere)

- hírszerzés, felderítés;
- ABV<sup>38</sup> funkció;
- idegen-barát felismerő rendszer;
- humán erőforrás menedzsment;
- térképészeti és navigációs képességek;
- meteorológiai funkció;
- oktatási és kiképzési funkció.

A rendszer funkcióinak összessége által egy közös helyzetkép alakítható ki, ami magába foglalja a valós idejű, teljes hadműveleti, harcszintéri képet az összes résztvevő egység (saját és ellenséges) és folyó tevékenység megjelenítésével. Tehát tudjuk, hogy hol vagyunk, mi zajlik körülöttünk, merre vannak a saját csapatok, merre van, és mit csinál az ellenség. Az automatizált folyamatok révén az információ minden egység részére rendelkezésre áll, ezáltal megelőzhető baráti tűz kiváltása, felgyorsulhat a műveleti terület kiértékelése, továbbá leegyszerűsíthető az ellenséges erők felderítése és nyilvántartása.

Megállapítható, hogy a C2 vezetés-irányítási rendszerek által nyújtott képességek – összevetve korunk katonai műveleteivel, melyek főbb jellemzői a többnemzetiség, az összhaderőnemi jelleg, a hálózatközpontú és hatásalapú megközelítés – jelentik azt az eszközrendszert, amely napjaink és a jövő fegyveres konfliktusai során biztosítja a döntési főlény kialakítását, elősegíti a katonai művelet sikeres végrehajtását.

#### 4. C2 KÉPESSÉG A MAGYAR HONVÉDSÉGBEN

A fejlett hadsereggel rendelkező NATO tagok már rendelkeznek C2 vezetés-irányítási rendszerrel, így felmerült az igény a Magyar Honvédség C2 rendszerének megvalósítására is.

A tervezési munkák 2006. körül kezdődtek és a fő koncepciót – az anyagi források rendelkezésre állása tekintetében – a már meglévő technikai eszközökre épülő átalakítás, korszerűsítés jelentette. Mindenek előtt tehát el kellett dönteni, hogy a C2 rendszer alkotó elemei közül (harcjárművek, vezetési komplexumok, híradó és informatikai rendszerek, szoftverek, külső érzékelők) melyek kerülnek újonnan beszerzésre és mely meglévő eszközök integrálhatók a rendszerbe.

A rendszer legköltségesebb részeit jelentő különböző gépjárművek, harcjárművek, valamint híradó és informatikai komplexumok így a már rendszerben álló technikai eszközök átalakításával, korszerűsítésével valósulnak/valósultak meg. Az újonnan beszerzésre tervezett elemekre és a C2 rendszerszoftverre közbeszerzési pályázat került kiírásra.

Az anyagi források korlátai meghatározták a rendszer többlepcsős bevezetését is, miszerint az első ütemben egyetlen zászlóalj szintű szervezet kerül felszerelésre a modern harcvezetési rendszerrel, majd a későbbiekben a projekt sikerétől, valamint a NATO szövetségi rendszer jövőbeni fejlesztési irányaitól függően adott lesz a lehetőség további szervezetek felszerelésére is. Jelenleg a bevezetésre váró vezetés-irányítási rendszer teljes összeállításának végső munkálatai folynak, tervezetten a 2010. évben kezdi meg a Magyar Honvédség C2 rendszere a teljes funkcionalitással rendelkező működését.

A C2 rendszer alkotóelemeit tekintve három fő részre osztható: gépjárművekre, hardver eszközökre és a szoftver(ek)re.

<sup>38</sup> Atom-, vegyi-, biológiai-



3. sz. ábra: A C2 rendszer elemei 0

A gépjárművek csoportjába beletartoznak a különböző parancsnoki komplexumok, a harcjárművek, a híradó és informatikai központok, valamint megtalálhatók egyedi rendeltetésű komplexumok is. Kiemelendő, hogy minden egyes komplexum azonos adatbázissal van ellátva, így képes önállóan funkcionálni, vagyis a működéshez nincs szükség a C2 rendszer teljes infrastruktúrájára.

A C2 rendszer hardver eszközei fokozott katonai igénybevételre alkalmas híradó és informatikai eszközökből (rádiók, számítógépek, egyéb kommunikációs és informatikai eszközök, szenzorok) tevődnek össze.

A hardver eszközök főbb típusai:

- számítógépek;
- szerverek;
- rádiók;
- belső kommunikációs rendszer;
- GPS;
- opcionális szenzorok és kiértékelő modulok.

A C2 vezetés-irányítási rendszer rendeltetését a szoftverek valósítják meg. Végzik a beépített eszközök vezérlését, biztosítják a funkcionális modulok szolgáltatásait, egységes rendszerbe szervezik a számítógépeket, híradó és informatikai eszközöket, felelősek az információ biztonságáért és a hálózat menedzseléséért.

Fő szoftvertípusok a funkciójuk alapján:

- rendszerszoftver;
- információbiztonságot, titkosítást és rejtjelezést végző szoftver;
- digitális terepmodell, térképészeti adatbázis.

A Magyar Honvédség tábori C2 szoftverére kiírt beszerzési eljárás győztese a vezetés-irányítási rendszerek fejlesztésével foglalkozó – németországi központú – Rheinmetall Defence GmbH. lett. A C2 szoftver fejlesztése teljes mértékben NATO szabványokon, ajánlásokon, protokollokon, interfészeken és jelzéseken alapszik, így a rendszer képes együttműködni a szövetséges országok hadseregeinek hasonló rendszereivel.



## ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Összefoglalva tehát a hálózatközpontú megközelítés az érzékelők, a döntéshozók és a fegyverrendszerek egyetlen rendszerbe történő integrálását jelenti. Lényege, hogy a hadszíntéren kialakított információs és kommunikációs háló segítségével a katonai vezetés minden szintjén biztosítja a pontos információk valósidejű megszerzését, azok biztonságos továbbítását, valamint azonos elvek és eljárások szerinti értelmezését.

Az információ gyűjtésére és feldolgozására, majd a felhasználók által érthető formában történő megjelenítésére a vezetés-irányítási rendszerek szolgálnak, melyek műveleti területen elengedhetetlenül szükségesek a csapatok vezetéséhez, legyen szó háborús feladatról, missziós műveletről, katasztrófa elhárításáról, vagy békeidejű gyakorlatról.

Az erők irányítása és koordinálása, a műveletek végrehajtásához kapcsolódó parancsok megvalósítása érdekében rendszeresített C2 vezetés-irányítási rendszerek által nyújtott képességek jelentik tehát napjaink többnemzeti, összhaderőnemi katonai műveleteiben azt az eszközrendszert, amely biztosítja a döntési fölény kialakítását, elősegíti a katonai művelet sikeres végrehajtását.

Mindezek tükrében merült fel az igény a Magyar Honvédség C2 rendszerének megvalósítására is, melynek keretében a tervek szerint 2010-re egy zászlóalj szintű szervezet kerül felszerelésre modern harcvezetési rendszerrel. De remélhetőleg ez csak az első lépés a Magyar Honvédség egyik fő fejlesztési irányán, melynek célja a vezetés és irányítás modernizálása, valamint a NATO szövetségi rendszerben történő együttműködés megkönnyítése.

## FELHASZNÁLT IRODALOM

- [1] Koós Gábor – Szternák György: Gondolatok a hatásalapú- és a hálózatközpontú katonai műveletekről, Sereg Szemle, VII. évfolyam 3. szám, Budapest, 2009, pp93-114 (ISSN 2060-3924)
- [2] Lédeczi Zoltán: A C2 vezetés-irányítási rendszerek felépítése, alkalmazhatósági lehetőségei a vezetésben, Diplomamunka, ZMNE, Budapest, 2010, p61
- [3] Hóka Miklós: Szenzorok háborúja: A hálózatközpontú hadviselés, Új Honvédségi Szemle, LVI. évfolyam 2. szám, Budapest, 2002, pp129-140 (ISSN 1216-7436)
- [4] Dr. Várhegyi István – Dr. Ványa László: Hadviselés az információs hadszíntéren: Trendek, új eljárások és eszközök, Bolyai Szemle, XV. évfolyam 1. szám, Budapest, 2006, pp9-20 (ISSN 1416-1443)
- [5] Dr. Haig Zsolt: Számítógép-hálózati hadviselés rendszere az információs műveletekben, Bolyai Szemle, XV. évfolyam 1. szám, Budapest, 2006, pp54-73 (ISSN 1416-1443)
- [6] Tóth András: A tábori C2 automatizált vezetési és irányítási rendszer alkalmazhatósága a Magyar Honvédség csapatvezetési rendszerében, Kommunikáció 2009 Nemzetközi Szakmai Tudományos Konferencia Kiadvány kötet, ZMNE, Budapest, 2009, pp185-192 (ISBN 9789637060700)
- [7] Tóth András: Az Automatizált Harcvezetési és Információs Rendszer modell, Kommunikáció 2009 Nemzetközi Szakmai Tudományos Konferencia Kiadvány kötet, ZMNE, Budapest, 2009, pp199-206 (ISBN 9789637060700)
- [8] Tóth András: A vezetés-irányítási rendszerek alkalmazásával szemben támasztott követelmények a csapatvezetésben, gyakorlati használata során felmerült észrevételek, tapasztalatok, Hadmérnök on-line, IV. évfolyam 1. szám, 2009, pp276-283 [http://www.hadmernok.hu/2009\\_1\\_toth.pdf](http://www.hadmernok.hu/2009_1_toth.pdf) (letöltve: 2010.06.21.)(ISSN 1788-1919)
- [9] <http://defense-update.com/images/SIT.jpg>

[10] Négyesi Imre: Az Információ szerepe a Katonai-Vezetői Információs Rendszerekben (Hadtudományi Szemle on-line, II. évfolyam (2009) 1. szám, 119-125. oldal, HU ISSN 2060-0437);





## Jelen számunk szerzői

|                                      |                                                                           |
|--------------------------------------|---------------------------------------------------------------------------|
| <b>Bindis Bea Brigitta htj.</b>      | ZMNE Had- és Biztonságtechnikai Mérnök Alapképzési Szak II. éves hallgató |
| <b>Bodnár István htj.</b>            | ZMNE Had- és Biztonságtechnikai Mérnök Alapképzési Szak IV. éves hallgató |
| <b>Dorkó Zsolt r. alez.</b>          | ORFK GF ÉMGEI, osztályvezető-helyettes                                    |
| <b>Horvayné Fehér Judit r. örgy.</b> | ORFK GF Informatikai Főosztály                                            |
| <b>Józan Nándor htj.</b>             | ZMNE Had- és Biztonságtechnikai Mérnök Alapképzési Szak II. éves hallgató |
| <b>Juhász Márta htj.</b>             | ZMNE Had- és Biztonságtechnikai Mérnök Alapképzési Szak II. éves hallgató |
| <b>Dr. Pándi Erik r. ezds.</b>       | ZMNE Híradó Tanszék, főiskolai tanár                                      |
| <b>Serege Gábor fhdgy.</b>           | ZMNE Informatikai Tanszék, tanársegéd                                     |
| <b>Szalai Máté htj.</b>              | ZMNE Had- és Biztonságtechnikai Mérnök Alapképzési Szak IV. éves hallgató |
| <b>Tóth András fhdgy.</b>            | ZMNE Híradó Tanszék, tanársegéd                                           |
| <b>Tőreki Ákos fhdgy.</b>            | ZMNE Híradó Tanszék, tanársegéd                                           |
| <b>ifj. Veres György tű. örgy.</b>   | Fővárosi Tűzoltóparancsnokság                                             |
| <b>Dr. Veres György</b>              | ZMNE, egyetemi docens                                                     |

## Szerzőink figyelmébe

A kiadvány lehetőséget biztosít max. 40 ezer leütés (egy szerzői ív) terjedelemben – elsősorban: távközlés, híradás, informatika és információvédelem témakörökben – tanulmányok, szakcikkek megjelentetésére.

A cikknek tartalmaznia kell:

- egy 2-5 soros absztraktot magyar és angol nyelven;
- 2-5 magyar és angol kulcsszót;
- a cím angol nyelvű fordítását.

A cikkek beküldése e-mailen a [hirado@zmne.hu](mailto:hirado@zmne.hu) címre lehetséges.

A cikkek leadási határideje: folyamatos (megjelenés évente kétszer)

A megjelentetésre szánt cikkek csak a szerző(k) eddig máshol még meg nem jelent, saját önálló (társszerzők esetében közös) írásműve(i) lehetnek. Az írásművekben lévő idézeteknek meg kell felelniük a szerzői jogról szóló hatályos jogszabályoknak. A megjelentetésre szánt írásművek csak nyílt (nem minősített) információkat és adatokat tartalmazhatnak. Ezek minősített voltát a szerkesztőbizottság nem vizsgálja, ennek felelőssége a cikk szerzőjét terheli.

A szerkesztőbizottság a megjelentetésre szánt írásműveket lektoráltatja. A szerkesztőbizottság fenntartja a jogot, hogy a megjelentetésre szánt írásművet - külön indoklás nélkül - megjelenésre alkalmatlannak ítélje. Az ilyen cikkeket nem küldi vissza, és nem őrzi meg.

A kiadványban lehetőség van idegen nyelvű cikkek megjelentetésére. Az idegen nyelven megjelentetésre szánt írásművek nyelvi lektorálása a szerzőt terheli.

Minden kéziratához elektronikusan is mellékelni kell egy kitöltött "Kéziratbeküldési űrlap"-ot, és egy "Copyright átruházási űrlap"-ot. Mindkét űrlapot ki kell nyomtatni és alá kell írni (tőbbszerzős cikk esetében minden szerzőnek!), majd a kinyomtatott és aláírt űrlapokat faxon (fax szám: +36-1-432-9025), vagy postai úton levélben (levélcím: Hírvillám Szerkesztőség, 1581. Budapest Pf.: 15.) is meg kell küldeni a szerkesztőségnek. Ezek hiányában a cikkeket a szerkesztőség nem lektoráltatja és nem jelenteti meg!

A cikkekkel szemben támasztott formai követelmények:

Szerző(k):

**Tóth András - Kovács Péter**

(12 pontos ARIAL félkövér, kisbetűkkel, középre zárt)

A szerző(k) intézménye

(12 pontos ARIAL, kisbetűkkel, középre zárt)

A szerző(k) e-mail címe

(10 pontos ARIAL, kisbetűkkel, középre zárt)

**CIKK CÍME**

(14 pontos ARIAL, félkövér, nagybetű, középre zárt)

*Absztrakt*

(12 pontos Times New Roman, szimpla sorköz, dőlt, kisbetűkkel, sorkizárt)

2-5 soros magyar és angol nyelvű absztrakt. Idegen nyelvű cikk esetében is szükséges a magyar absztrakt

Kulcsszavak: 2-5 magyar és angol nyelvű kulcsszó

**FEJEZETCÍM**

(12 pontos ARIAL, félkövér, nagybetű, középre zárt, bekezdések előtt és után nincs beállított sorköz érték, számozás kézzel!)

A szövegtörzset Times New Roman 12 pontos betűből kell kialakítani. Sorkizárt. Sorköz szimpla. A második és minden további új bekezdés első sorát 0,5 cm-rel kell behúzni. A szövegben történő kiemelés (ha elengedhetetlenül szükséges) dőlt betűkkel, nincs félkövér kiemelés a szövegben. Lábjegyzet: Times New Roman 10 pontos betű, szimpla sorköz, sorkizárt, sem előtte, sem utána nincs beállított térköz! Ne használjunk stílusokat!

Ábrákat, képeket, valamint a táblázatokat középre rendezve, a képaláírást vagy a táblázat nevét a kép/ábra illetve a táblázat alá középre Times New Roman 12 pontos betűből kell elkészíteni. Minden képnél, ábránál és táblázatnál meg kell adni a forrást is!

Nincs oldalszámozás. Élőfej és élőláb területe üres.

**Alfejezetcím**

(12 pontos ARIAL, félkövér, kisbetű, középre zárt, bekezdések előtt és után nincs beállított sorköz érték! Az alfejezetek számozása kézzel történik.)

A szövegtörzset Times New Roman 12 pontos betűből kell kialakítani. Sorkizárt. Sorköz szimpla. A második és minden további új bekezdés első sorát 0,5 cm-rel kell behúzni. A szövegben történő kiemelés (ha elengedhetetlenül szükséges) dőlt betűkkel, nincs félkövér kiemelés a szövegben. Lábjegyzet: Times New Roman 10 pontos betű, szimpla sorköz, sorkizárt, sem előtte, sem utána nincs beállított térköz! Ne használjunk stílusokat!

Ábrákat, képeket, valamint a táblázatokat középre rendezve, a képaláírást vagy a táblázat nevét a kép/ábra illetve a táblázat alá középre Times New Roman 12 pontos betűből kell elkészíteni. Minden képnél, ábránál és táblázatnál meg kell adni a forrást is!

Nincs oldalszámozás. Élőfej és élőláb területe üres.

Irodalmi hivatkozás (Times New Roman, 12 pontos betűk, balra rendezve, bekezdés után 6 pont). A szerzők a cikk témájától függetlenül szabadon választhatnak a számozott, vagy a névszerinti módszer között.

### *Számozott hivatkozások:*

A hivatkozásokat a szövegben való előfordulásuk sorrendjében számozzuk, a szövegben a hivatkozási számot szögletes zárójelben tüntetjük fel, pl. [1]. Az irodalomjegyzékben a számozott hivatkozások bibliográfiai elemeit az alábbi minták szerint adjuk meg:

#### FOLYÓIRATCIKKRE

[1] P. Smith, E. McGregor: Effect Based Operations in Afghanistan. *Military Journal*, 62 (2007) 482-490.

#### KÖNYVRE

[2] R. Cook, P. R. Hammer: *Military Inventions in the World War II*. United Press, 1990.

#### KÖNYV VAGY MONOGRÁFIA FEJEZETÉRE

[3] K. Wells: The reasons of the terrorist attacks. In: K. Wells, R. Pupil (Eds), *2006 Islam in the 21th Century*. United Press, 2006.

### *Névszerinti hivatkozások:*

Az irodalomjegyzékben a hivatkozásokat számozás nélkül, abc-rendben soroljuk fel. A szövegbeli hivatkozás a szerző nevével és a megjelenés évszámával történik, pl. "Kovács (1990) szerint" vagy "egy korábbi tanulmány (Kovács, 1990) szerint". Ha ugyanattól a szerzőtől és ugyanabból az évből több munkára hivatkozunk, azokat lássuk el megkülönböztető jelzéssel (pl. a,b,c). Az irodalomjegyzékben a névszerinti hivatkozások bibliográfiai elemeit az alábbi minták szerint adjuk meg:

#### FOLYÓIRATCIKKRE

Smith, P., McGregor, E. (2007): Effect Based Operations in Afghanistan. *Military Journal*, 62:482-490.

#### KÖNYVRE

Cook,R., Hammer, P. R. (1990): *Military Inventions in the World War II*. United Press.

#### KÖNYV VAGY MONOGRÁFIA FEJEZETÉRE

Wells, K. (2006): The reasons of the terrorist attacks. In: K. Wells, R. Pupil (Eds), *2006 Islam in the 21th Century*. United Press.



## Kézirat publikációs céllal történő benyújtása



HÍR  
VIL  
LÁ  
M

Az alábbi cikket a *HírVillám* című folyóiratban kívánom megjelentetni:

A kézirat címe: .....

.....  
.....

A szerző\*

neve: .....

munkahelye: .....

levelezési címe: .....

telefonszáma: .....

FAX száma: .....

e-mail címe: .....

Aláírással igazolom, hogy a publikációs céllal benyújtott kézirat eredeti, saját munkám, amely még nem jelent meg máshol, és eddig nem is nyújtottam be ilyen céllal máshová.

A kézirat minősített anyagot, vagy minősített információt nem tartalmaz.

A kéziratban a szerzői jogoknak megfelelő módon vannak jelezve a hivatkozások, idézések, azok jelen írás szerzői jogainak átruházását nem érinti.

Kelt: .....

.....  
a szerző aláírása

\* több szerző esetén minden személynek külön kitöltött „Kézirat beküldési űrlap”-ot kell mellékelni a kézirathoz



## Copyright átruházási nyilatkozat



ZRÍNYI MIKLÓS  
NEMZETVÉDELMI  
EGYETEM  
HÍRADÓ  
TANSZÉK

Az alább megjelölt cikk copyright jogait az alább megnevezett szerző vagy szerzői kollektíva átruházza a Zrínyi Miklós Nemzetvédelmi Egyetem Híradó Tanszékére, ha és amikor a cikket közlésre elfogadják. A copyright jogok magukban foglalják a cikk sokszorosításának és terjesztésének jogait beleértve a fotografikus, elektronikus vagy bármely más hasonló technikával történő másolás, ill. a fordítás jogát is.

A nyilatkozatot aláíró szerző aláírásával tanúsítja, hogy a cikk eredeti és hogy birtokában van az átruházandó jogoknak, valamint hogy felelősséget vállal az összes társalkotó nevében is a copyright jogok átruházásának jogosságát illetően.

A szerzők a publikált cikket saját honlapjukon hozzáférhetővé tehetik az Interneten, feltéve, hogy feltüntetik a megjelenés pontos bibliográfiai adatait, az elérhetőség címét (URL), és a copyright tulajdonosaként a Zrínyi Miklós Nemzetvédelmi Egyetem Híradó Tanszék nevét.

A cikk címe: .....

.....  
.....

Szerző(k)

neve:

aláírása:

|       |       |
|-------|-------|
| ..... | ..... |
| ..... | ..... |
| ..... | ..... |
| ..... | ..... |

Kelt: .....



Felelős kiadó: Prof. Dr. Rajnai Zoltán mk. ezredes  
Megjelent a ZMNE BJKMK Híradó Tanszék gondozásában, 10 példányban, illetve elektronikusan:

[www.puskashirbaje.hu](http://www.puskashirbaje.hu)

HU ISSN 2061-9499

\*\*\*

ZMNE BJKMK Híradó Tanszék  
1101 Budapest, Hungária krt. 9-11.  
1581 Budapest, Pf. 15.  
+36 1 432 9000 (29-358 mellék)  
[hirado@zmne.hu](mailto:hirado@zmne.hu)