MAGYAR KÖZTÁRSASÁG
KATONAI FELDERÍTŐ HIVATAL

VI. évfolyam Különszám **2007. február**

FELDERÍTŐ SZEMLE

BUDAPEST

A Magyar Köztársaság Katonai Felderítő Hivatal kiadványa

Felelős kiadó

Madarász Károly mk. vezérőrnagy,
megbízott főigazgató

Szerkesztőbizottság

Elnök: Tóth András mk. ezredes

Tagok: Gulyás József mk. ezredes
Keszmann Oszkár alezredes
Marton Csaba mk. ezredes
Svigruha Gyula mk. ezredes
Dr. Tömösváry Zsigmond nyá. dandártábornok
Vass Jenő nyá. ezredes

Lektorálták: Becski Géza nyá. mk. ezredes
Marton Csaba mk. ezredes
Pados László mk. ezredes
Svigruha Gyula mk. ezredes

A kötetet összeállította: Marton Csaba mk. ezredes
Olvasószerkesztő: Vass Jenő nyá. ezredes
Tördelőszerkesztő: Gerencsérné Tóth Krisztina főtörzsőrmester
Fotó: Székely Klára mk. őrnagy

Készült 200 példányban, az MK KFH nyomdájában
Felelős vezető: Juhász József mk. őrnagy
ISSN 1588-242X
Felelős szerkesztő: Vass Jenő nyá. ezredes

TARTALOM

A SIGINT
a XXI. század kihívásainak tükrében

Tudományos szakmai konferencia

BUDAPEST
2006. november 15.

A SIGINT a XXI. század kihívásainak tükrében című tudományos szakmai konferenciát a Magyar Köztársaság Katonai Felderítő Hivatal Tudományos Tanácsa égisze alatt a Rádióelektronikai Felderítő Igazgatóság szervezte és rendezte meg.

A konferencia célja a távközlési rendszerek fejlődési irányainak prognosztizálása, a rádióelektronikai felderítő rendszerre gyakorolt hatásainak elemzése, a korszerűsítést célzó közös gondolkodás elindítása volt. A konferencia törekszik az elmúlt években felhalmozódott nemzeti és nemzetközi tapasztalatok összegzésére, valamint az adatfeldolgozó tevékenység elvi, módszertani megújítására törekedett.

A konferencia elnöksége:

Madarász Károly mk. vezérőrnagy, az MK KFH TT elnöke
Tóth András mk. ezredes, az MK KFH TT tagja
Pászka Tibor mk. ezredes, az MK KFH TT tagja
Király Elemér mk. ezredes, gazdálkodási igazgató

A konferencia levezető elnöke:

Pászka Tibor mk. ezredes, rádióelektronikai felderítő igazgató

1. szekció
A SIGINT technikai kihívásai a XXI. században

Levezető elnök: Svigruha Gyula mk. alezredes

2. szekció
SIGINT műveletek a XXI. században

Levezető elnök: Pados László mk. ezredes

A Tudományos Tanács úgy határozott, hogy a konferencia szerkesztett anyagát az MK KFH periodikájában, a Felderítő Szemle 2007. évi Különszámában jelenteti meg.

*

A tudományos konferencia óta eltelt időszakban bekövetkezett főbb személyi változások:

Morber Ferenc altábornagy, az MK Katonai Felderítő Hivatal főigazgatója szolgálati nyugállományba vonult.

A Magyar Köztársaság honvédelmi minisztere **Madarász Károly mk. vezérőrnagyot**, a főigazgató műveleti helyettesét megbízta a főigazgatói teendők ellátásával, aki ezért felmentését kérte a Tudományos Tanács elnöke funkció ellátása alól.

A Tudományos Tanács kérésének eleget tett, és elnökének **dr. Tömösváry Zsigmond nyá. dandártábornokot, főtanácsost**, humán igazgatót választotta meg.

A Szerkesztőbizottság

MADARÁSZ KÁROLY MK. VEZÉRŐRNAGY
A FŐIGAZGATÓ MŰVELETI HELYETTESE,
A TUDOMÁNYOS TANÁCS ELNÖKE

KONFERENCIA-MEGNYITÓ

Tisztelt Tudományos Konferencia!
Tábornok és Tiszt Urak!
Kedves Vendégeink!

A Magyar Köztársaság Katonai Felderítő Hivatal vezetése és Tudományos Tanácsa nevében tisztelettel köszöntöm a konferencia valamennyi résztvevőjét.

A rendezvényre a Honvédelmi Minisztérium, a HM Honvéd Vezérkar, a Magyar Hadtudományi Társaság, a Zrínyi Miklós Nemzetvédelmi Egyetem, az MK Információs Hivatal, a MK Nemzetbiztonsági Szakszolgálat, a Budapesti Műszaki és Gazdaságtudományi Egyetem, a Nemzeti Hírközlési Hatóság, valamint a Rohde & Schwarz GmbH & Co. vezető képviselőit és tudományos szakértőit hívta meg a Hivatal Tudományos Tanácsa.

Külön köszöntöm azokat, akik felkérésünknek eleget téve vállalták, hogy előadás keretében osztják meg velünk tudásukat, személyes tapasztalataikat.

A Honvédelmi Miniszter Úr 74/2002. számú határozatával nyilvánította tudományos kutatóhellyé a Hivatalt, s azóta harmadik alkalommal kerül sor olyan tudományos rendezvényre, amely mind az adott témával kapcsolatos szakmai felelősséget, mind a résztvevők körét tekintve túlmutat a Hivatal keretein.

A SIGINT a XXI. század kihívásainak tükrében címmel szervezett konferencia a rádióelektronikai felderítés vizsgálatára és a korszerűsítés jövőbeni lehetséges irányaira koncentrál, lehetőséget biztosítva az alaprendeltetés teljesítése szempontjából nélkülözhetetlen szaktechnikai eszközöket fejlesztő, illetve az adatszerző és adatfeldolgozó szervezeti elemek tevékenységének bemutatására is.

A katonai rádióelektronikai felderítés a magyar haderőben meglévő más felderítési nemekkel együtt teszi lehetővé a többforrású adatszerzést, növelve a megszerzett adatokból kinyert információk magas fokú megalapozottságát és hitelességét, biztosítva ezzel párhuzamosan az információk megbízhatóságának kölcsönös ellenőrizhetőségét. Mindezt azáltal éri el, hogy specifikumainál fogva képes reálidőben adatokat szerezni olyan objektumokról is, amelyek más felderítési nemek alkalmazásával nem foghatók le.

A katonai rádióelektronikai felderítés olyan egyedülálló korai előrejelző, figyelmeztető funkciót lát el, amelyre más felderítési nem csak korlátozottan, vagy egyáltalán nem képes. Ezzel párhuzamosan kiszolgálja a HM HVK és a Magyar Honvédség hadműveleti tervezéshez és a csapatok felkészítéséhez, alkalmazásához kapcsolódó, csak ezzel a módszerrel megszerezhető információigényét.

A katonai rádióelektronikai felderítés nemcsak a katonai felhasználók, hanem az állami vezetés és a nemzetközi közösség információ igényének teljesítéséhez is hozzájárul.

Mint a közreadott programból és a már elmondottakból is kitűnik, a mai konferenciát azzal a határozott céllal szervezte meg a Tudományos Tanács, hogy a rádióelektronikai felderítés jelenlegi helyzetét és fejlesztésének lehetséges irányait tudományos igénnyel megvizsgáljuk, emellett bemutassuk a távközlési rendszerek fejlődésének tendenciáit. Célunk továbbá, hogy elemezzük a rádióelektronikai felderítés helyét, szerepét és lehetőségeit a felderítés rendszerében, megtárgyaljuk szakmai elméletét és gyakorlati módszereit. Megpróbáljuk összegezni az elmúlt években felhalmozódott nemzeti tapasztalatokat, és tudományosan megalapozni a szaktevékenység követendő irányait, továbbá törekszünk az adatszerző és az adatfeldolgozó tevékenység elvi, módszertani megújítására.

A globalizálódó világban a távközlési rendszerek is egyre inkább globalizálódnak. A rádióelektronikai felderítő adatszerzés önmagában is egy összetett tevékenység, amely csak a technikai eszközök folyamatos fejlesztése mellett biztosíthat információkat. Az adatszerző rendszerek fejlődésével párhuzamosan természetesen jelentősen növekszik a rögzített adatok mennyisége is. A nagy mennyiségű adat feldolgozását már csak egy új filozófia alapján felépített integrált feldolgozó rendszer képes ellátni.

Fontos, hogy megtaláljuk azokat a csomópontokat, amelyek érintésével a rádióelektronikai felderítés továbbfejlődhet. A mai konferencia elsősorban e téren adhat új gondolatokat és impulzusokat.

Tisztelt Konferencia!
Hölgyeim és Uraim!

A tanácskozást minden szempontból alkalmas fórumnak tartom arra, hogy közös gondolkodással, a különböző nézeteket feltárva és ütköztetve megvitassuk a szükséges elméleti kérdéseket, és felvázoljuk a cselekvési lánc elemeit a rádióelektronikai felderítés fejlesztéséhez.

Bízom abban, hogy az együttgondolkodás, a mai alkotó véleménycsere érdemben fog hozzájárulni az érintett szervek és szervezetek célirányos, tervszerű, eredményorientált tevékenységéhez.

E gondolatok jegyében a tudományos konferenciát megnyitom, a résztvevőknek eredményes munkát, sikeres tanácskozást kívánok!

JUHÁSZ ISTVÁN VEZÉRŐRNAGY

A MAGYAR KATONAI ERŐ ÚJSZERŰ ALKALMAZÁSA

Miért aktuális a kérdés?

Felgyorsult világunkban a technikai fejlődés hihetetlen méreteket öltött, s magával hozta az egyre pontosabb, és egyben egyre bonyolultabb fegyverek és fegyverrendszerek megjelenését, alkalmazását és azok folyamatos modernizációját. Ezek az új fegyverek új alkalmazási technikákat és harceljárásokat követelnek a katonáktól. Nekünk ehhez kell állandóan alkalmazkodnunk, s meg kell felelnünk a kor folyamatosan változó kihívásainak.

Emellett azonban figyelembe kell venni más befolyásoló tényezőket is, úgymint a haderőt fenntartó állam elvárásait és lehetőségeit, a nemzeti biztonságpolitikai érdekeket, a szövetségi együttműködés igényeit és hatásait, a haderő állapotát és fejlesztésének irányvonalait. Mindezek a tényezők együttesen befolyásolják az adott haderő felkészítését, fenntartását és alkalmazását. Amennyiben a funkciókban változás történik, akkor azok átrajzolhatják az addigi elveket és az alkalmazott gyakorlatot.

A magyar haderő folyamatos modernizációja és átalakítása elengedhetetlen, hiszen a kihívásokra reagálni képes hadsereg fenntartása minden ország alapvető érdeke. Ezt a tényt az támasztja alá leginkább, hogy a nemzetközi terrorizmus elleni világméretű küzdelemben, a Szövetségre és tagországaira veszélyt jelentő globális válságok kezelésében, valamint a súlyos természeti katasztrófák megelőzésében, azok következményeinek felszámolásában felértékelődött a katonai erő alkalmazása. A Magyar Honvédségnek ebben a dinamikusan változó biztonságpolitikai környezetben – a vonatkozó törvények és országgyűlési határozatok alapján, a haderő szervezeteinek és létszámának, valamint a védelem területén korábban szükségesnek ítélt források folyamatos csökkentése közepette kell végrehajtania a feladatait.

Azokra a témákra szeretnék kitérni, amelyek a Magyar Honvédség átalakításával, valamint a transzformációs igényeknek és a tudatos képességfejlesztési követelményeknek történő megfeleléssel kapcsolatosak. Megállapíthatjuk, hogy az újszerű alkalmazás generáló tényezői nem a haditechnikai fejlődés következményei, hanem az egyéb tényezők voltak.

A kiindulópontok és a háttér

A Magyar Köztársaságot jelenleg nem fenyegeti hagyományos jellegű katonai agresszió, és ez hosszú távon sem prognosztizálható. Ugyanakkor olyan fenyegetések jelentek meg, melyek új típusú, részben vagy egészben katonai eszközökkel kezelendő kihívást is jelentenek. Ilyenek a nemzetközi terrorizmus és az etnikai–vallási jellegű konfliktusok. További potenciális veszélyt jelent a tömegpusztító (vegyi, biológiai, radiológiai, nukleáris) fegyverek, valamint az előállításukhoz és célba juttatásukhoz szükséges eszközök és technológiák további elterjedése.

Fennáll a lehetősége annak, hogy ezek a fegyverek a nemzetközi békét és biztonságot veszélyeztető államok, szervezetek, vagy terrorista csoportok kezébe kerülhetnek.

Hazánk 1999. március 12-én csatlakozott a NATO-hoz, így az ország védelme a szövetségi védelem feladatrendszerében valósul meg, s ez 2004-ben az Európai Unióhoz történt csatlakozással egy újabb elemmel bővült.

Feladataink teljesítéséhez a törvényi hátteret az alkotmány, a Honvédelmi törvény, a biztonság- és védelempolitikai alapelvek, a 2004-ben elfogadott Nemzeti Biztonsági Stratégia, valamint a kormányprogram védelempolitikája biztosítja. A Nemzeti Katonai Stratégia tervezete a Nemzeti Biztonsági Stratégia alapján készült el 2005 őszére, és azokkal a kérdésekkel foglalkozik, amelyek kezelése katonai eszközöket igényel. Ugyanakkor ez a dokumentum tartalmazza a haderővel szemben támasztott elvárásokat, a szervezeti kereteket, valamint a fejlesztés főbb irányait. A politikai elvárásokat rögzítő jogszabályi hátterek és a rendelkezésre bocsátott erőforrások alapján módosulhatnak a képességigények. Felül kell vizsgálni, hogy mi maradjon meg a régiből, s hogy milyen újakat kell létrehozni, hogy teljesíteni tudjuk a követelményeket. Az erőforrások viszonylatában látni kell, hogy az ország teherbíró képességéhez igazítva, a felhasználható költségek évről-évre csökkennek. Nekünk, katonáknak ezen igények figyelembevételével, ilyen körülmények között, a lehetőségekhez igazítva kell a haderő képességeit kialakítani.

A biztonságpolitika

A magyar védelempolitika célja a Magyar Köztársaság stabilitásának, állampolgárai jólétének, biztonságának, a demokrácia, a jogállamiság és az emberi jogok érvényesülése feltételeinek biztosítása. E célok megvalósítása jelenleg kedvező nemzetközi körülmények között mehet végbe.

A biztonságpolitikai alapelvek értelmében hazánknak nincs ellenségképe. Szomszédainkkal kölcsönös előnyökön nyugvó kapcsolatokat tartunk fenn. Azt valljuk, hogy a katonai erő a konfliktusok kezelésének végső eszköze, továbbá hazánk védelmét a NATO szövetségi kereteken belül hajtjuk végre úgy, hogy aktívan hozzájárulunk a közös védelmi képességekhez.

Ki kell emelni, hogy a Magyar Köztársaság biztonsági környezete stabil, a haderő – két- és többoldalú nemzetközi kapcsolatainak alakításával – aktív részvevője a régió stabilitásának megőrzésére irányuló válságmegelőző, válságkezelő műveleteknek, a katonai bizalom- és biztonságerősítő programoknak.

A képességek kialakítása

Az adott háttérrel és a haderővel szemben támasztott követelményekkel együtt kialakításra került az új, vagy a módosult feladatrendszer, szervezeti felépítés, a felkészítés és kiképzés rendszere, és azok a projektek, amelyek megvalósulásával a haderő készen áll az újszerű alkalmazásra.

A magyar haderő vonatkozásában ez az újszerű alkalmazás egy önkéntes alapon álló, expedíciós jellegű, professzionális haderő kialakítását követeli meg, amely alkalmas a szövetségi együttműködésre, képesség-alapú, korszerű fegyverzettel és felszereléssel rendelkezik, gyorsan bevethető és manőverezésre képes, modul

rendszerű, és a költségvetés szempontjából finanszírozható. Egy ilyen haderő valóban képes arra, hogy területvédelem helyett az érdekek védelmére helyezze a hangsúlyt. Ehhez olyan kis létszámú alegységeket kell kialakítani és fenntartani, amelyek széles skálán képesek feladatot végrehajtani, logisztikailag támogatottak, és képesek együttműködni a szövetséges erőkkel.

A NATO-műveletek súlypontja folyamatosan Európán kívülre helyeződött át. A területvédelem elve helyett itt is egyre inkább előtérbe került az érdekek védelmének hangsúlyozása. Megnő a jelentősége a katonai konfliktusokat lezáró, stabilizációs műveleteknek. Előtérbe kerül a polgári–katonai együttműködés (CIMIC) és más, a stabilizációt elősegítő képesség, például az újjáépítési csoportok (PRT-k) alkalmazása. Emelkednek a követelmények a vezetés–irányítási, az erők megóvását biztosító (Force Protection) és a különleges műveleti képességgel (SOF) rendelkező erők telepíthetőségének területén.

A fentieknek megfelelően a haderővel szembeni alapvető követelmény a professzionális és expedíciós képességekkel bíró szervezet kialakítása, megteremtése.

A szervezeti átalakítások

A Honvédelmi Minisztériumban a létszámcsökkentést és az átszervezést követően a tervezett MH Összhaderőnemi Parancsnokság (MH ÖHP) Székesfehérváron kerül megalakításra. Az átalakítás megtervezésére 2005 végén került sor, és a parancsnokság tervezett létszáma mintegy 500 fő, az alárendelt katonai szervezetek létszáma pedig mintegy 18 000 fő körül alakul. Néhány szervezet továbbra is a HM Honvéd Vezérkar főnök közvetlen alárendeltségébe tartozik majd, kb. 4000 főnyi létszámmal. Ezáltal a Magyar Honvédség összlétszáma 2007 végére mintegy 22 000 fő lesz.

Az alkalmazási sajátosságok

A magyar haderő alkalmazásának sajátosságai, hogy a szövetséges erők beérkezéséig, az MH ÖHP vezetésével mintegy két dandár – légi harccsoport megerősítéssel –, manőverező tevékenység alkalmazásával határbiztosítást folytat, majd a szövetséges erők beérkezése után önálló műveleti körletben tevékenykedik, szövetségesi megerősítéssel, illetve a szövetségi erők alárendeltségében. Más tagország megsegítése esetén a szövetségesi erők alárendeltségében veszünk részt megerősített zászlóalj-harccsoport alkalmazásával, valamint kisebb méretű kötelékekkel a NATO Reagáló Erőibe (RF) és az EU Harccsoportba (EU BG) felajánlott harcoló, harctámogató, és harcbiztosító-támogató erőkkel, illetve a felajánlott légierő-komponenssel.

A magyar katonai erő alkalmazása terén jelentős változás figyelhető meg a korábbi időkhöz viszonyítva. Napjainkban ugyanis már valós feladatokban vesznek részt katonáink. A végrehajtás során összehangoltan vizsgáljuk a nemzeti és a szövetségesi igényeket. Már nemcsak harcoló alegységekben gondolkodunk, hanem a teljes harcbiztosítás és harctámogató biztosítás feladatait is el kell látnunk. Az országvédelmi feladatainkat is átdolgoztuk és hozzáigazítottuk a szövetségben jelentkező feladatokhoz.

A napi feladatok végzése közben előre is tekintünk: megvizsgáljuk a jövő igényeit, figyelemmel kísérjük a NATO transzformációs elképzeléseit. Technikai fejlesztéseinket is úgy próbáljuk megvalósítani, hogy azok maximálisan szolgálják a meg-megújuló nemzeti és szövetségesi igényeket.

Hazánk nemzetközi szerepvállalása

Az Országgyűlés felhatalmazása alapján a Magyar Honvédség katonái jelenleg különféle nemzetközi missziókban teljesítenek szolgálatot. Az ENSZ és az EBESZ mandátuma alapján Cipruson, Nyugat-Szaharában, Grúziában, továbbá az MFO kötelékében a Sínai-félszigeten békefenntartó műveletben hajtják végre feladataikat. A NATO által vezetett műveletek közül a KFOR-erők részeként a Balkánon, Koszovóban, illetve ISAF-erőként Afganisztánban, valamint Irakban – kiképzőként – járulnak hozzá a nemzetközi béke és biztonság fenntartásához. Ezen túlmenően fontosnak tartom megemlíteni az EU keretében az ALTHEA misszióban való részvételünket Bosznia-Hercegovinában.

A békeműveletekben való részvételünk az utóbbi időben nagymértékben nőtt. Míg a kontingensek összlétszáma a délszláv válság rendezését követően 700–800 főben stabilizálódott, addig napjainkban az afganisztáni újjáépítési csoport (PRT) működtetésével már megközelíti az 1000 főt.

Amennyiben a NATO Reagáló Erőkhöz kijelölt készenléti erők lehívása megtörténik, a külföldön állomásozó magyar csoportosítások létszáma – országgyűlési felhatalmazás megadását követően – meghaladhatja az 1200 főt is. A fentieken túl a HM és az MH állományából közel 200 fő teljesít külszolgálatot különböző nemzeti és NATO-beosztásokban.

A két- és többnemzetiségű regionális szerepvállalásokat is a kollektív biztonság erősítése érdekében hívták életre. A „Szövetséget a szövetségben" elv alapján, a kis országok műveleti hatékonyságának fokozása érdekében, a szövetségi érdekeket szem előtt tartva folyik a regionális együttműködés.

A nemzetközi felajánlásaink területén jól látható, hogy vannak konkrét, aktív részvételek (például Balkán, Afganisztán) és vannak készenléti feladatok, ahol bizonyos képességeket ajánlunk fel (például NRF).

A NATO Reagáló Erők (NATO Reaction Forces – NRF)

Az NRF célja, hogy a NATO számára egy hiteles, magas készenlétű erőt biztosítson, amely teljesen kiképzett összhaderőnemi haderő, és amely gyorsan bevethető annak érdekében, hogy szükség esetén részese legyen a NATO-missziónak.

Az NRF ugyanakkor erődemonstráció is, amely megmutatja a NATO határozottságát és együttérzését a válságok megakadályozásában és megoldásában (a diplomáciát támogató gyors reagálású műveletek).

Magyarország teljes mértékben támogatja a NRF-koncepciót, és egyre növekvő mértékű erővel járul hozzá a működtetéséhez. Mivel az NRF a fejlesztések területén a transzformáció hajtómotorja a NATO-ban – és bátran kijelenthetjük, hogy a Magyar Honvédségben is –, ezért elengedhetetlenül fontos az NRF-be felajánlott

erőink további folyamatos fejlesztése, kiképzettségük és hadrafoghatóságuk biztosítása. A mintegy 26 ezer főre tervezett NATO Reagáló Erők az alábbi feladatok és műveletek végrehajtásához szükséges képességekkel rendelkezik:

- válságkezelés (beleértve a békefenntartást);
- a terrorizmus elleni műveletek támogatása;
- következménykezelés (ABV-események és humanitárius katasztrófák);
- békekikényszerítés;
- embargó-műveletek (tengerészeti, szárazföldi, repülésmentes övezet);
- elsődleges beérkező erő, vagy támogató erő;
- erődemonstráció (gyors reagálású műveletek);
- civilek evakuációja.

Az Európai Unió Harccsoport (EU Battle Group – EU BG)

Az EU BG koncepciója szintén a közösségi szerepvállalás és az összhaderőnemi szintű szemlélet kialakításának fontosságára fókuszál már a haderőnemek, sőt a végrehajtásban érintett csapatok szintjén is.

Az NRF-képességekhez történő hozzájáruláson túl, immáron az Unió keretein belül is konkrétan jelentkeznek a minőségi mutatókkal rendelkező csapatok kialakítására és alkalmazására vonatkozó igények.

A folyamatos mennyiségi csökkenéssel egyidejűleg, a védelem területén korábban szükségesnek ítélt források nélkül kell a NATO- és az EU-környezetben minőséget nyújtani. Ennek a minőségnek egyik alapvető letéteményese lehet a Többnemzetű Szárazföldi Kötelék, a közös olasz–magyar–szlovén (ITA–HUN–SLO) EU Harccsoport kialakításának alapja.

A magyar hozzájárulás mintegy 230 fős. Az egység egy BTR-ekkel, vagy személyszállító terepjáró gépjárművekkel felszerelt könnyű lövészszázad, amelyhez nemzeti támogató elem, egy víztisztító alegység és törzsállomány tartozik.

A felkészítés és a kiképzés

A Magyar Honvédségben a kiképzést és felkészítést a 2006-ban kiadott **Miniszteri Irányelvek a Magyar Honvédség kiképzéséhez és felkészítéséhez** és a **HM HVKF intézkedése a Magyar Honvédség 2007. (2008-2009.) évi felkészítési és kiképzési feladatairól** szóló dokumentumok alapján hajtjuk végre. A fő irányelv a professzionális és az expedíciós jelleg kidomborítása.

A csapatok kiképzése eltérő a szárazföldi alakulatoknál és a légierőnél, de mindkettőnél megfigyelhető, hogy a blokkok egymásra épülő rendszert alkotnak. A feladatokra történő felkészítés is szorosan kapcsolódik a kiképzési rendszerhez.

A tiszti és a tiszthelyettesi képzés keretén belül egy rövidebb idejű, tanfolyam rendszerű (különböző szak-, előmeneteli és továbbképzés), valamint a hosszabb időt igénybe vevő tanintézeti képzés (főiskolai és egyetemi) folyik.

A kiképzés során az alsóbb szinteken működő parancsnokok döntései felértékelődnek. Maximális információ biztosítás mellett egyes esetekben a tiszthelyettesek mint műveleti vezetők tevékenykednek. A feladatokra történő felkészítés során komplex, akár haderő szintű együttműködési képesség kialakítása valósul meg a szövetséges erőkkel.

A speciális képességek

A „kisebb" tagállamok – köztük hazánk is –, speciális módon járulhatnak hozzá a NATO kollektív védelméhez, illetve a nemzetközi biztonság és az érdekeink védelme érdekében folytatott műveletekhez. Olyan hozzáadott értékekkel, amelyek minőségi képességeket jelentenek, és pótolhatják azokat a hiányosságokat, amelyekkel a Szövetség jelenleg csak korlátozottan, vagy egyáltalán nem rendelkezik. Itt szeretném kiemelni, hogy a 21. század elején nincs szükség arra, hogy minden tagország a képességek teljes spektrumával rendelkezzen. Ma már az egyes államok által biztosított speciális képességek eredője alkotja a Szövetség erejét. A hazánkhoz hasonló adottságokkal rendelkező NATO-tagállamokban – a nagyméretű csoportosítások helyett – egyre inkább a kisebb, de mobilizálható, speciális feladatok ellátására képes kötelékek kialakításában és fenntartásában gondolkodnak. A szakosodás, specializálódás kérdése az utóbbi időben még hangsúlyosabbá vált.

Emiatt hazánkban is nagy hangsúlyt kapott a NATO-ban folyó, és a Szövetséges Átalakítási Parancsnokság (ACT) által irányított átalakítási folyamat nyomon követése, mert ennek során olyan tapasztalatokra tehetünk szert, amelyek felhasználásával lehetőségünk nyílik azon képességeink tökéletesítésére, amelyeket a kollektív szerepvállalás és a minőségi haderő kialakítása érdekében vállaltunk fel.

A fejlesztési programok

Az önkéntes professzionális haderőre történő áttérés fontos aspektusa a haditechnikai eszközök fejlesztése. A haditechnikai fejlesztések nagyban hozzájárulnak a kor kihívásaihoz jobban alkalmazkodó haderő létrehozásához. Ennek megvalósítása nemcsak nemzeti érdek, de a NATO tagjaként hozzájárulás a Szövetség védelmi képességeihez is. A haditechnikai eszközök interoperabilitása igen jelentős tényező egy külföldi művelet során, legyen szó akár béketámogató, válságkezelő műveletről is.

Már a korábbi átalakításoknak is fontos aspektusa volt a technikai modernizáció megvalósítása, ugyanakkor a szűkös gazdasági és költségvetési lehetőségek miatt nem könnyű megtalálni a rendelkezésre álló erőforrások és az elképzelések közötti egyensúlyt.

Tervezzük a főbb technikai eszközök viszonylag rövid idő alatti modernizációját, cseréjét, nem elfelejtve, hogy a jelenleg rendelkezésre álló technikai park mind mennyiségi, mind minőségi szempontból a „hidegháború terméke". Ezen a területen nagy kreativitásra, a gondolkodásmód megváltoztatására van szükség, de ez még nem elég. Ami ezen túl szükséges: a pénz.

Ezért a modernizáció végrehajtása nagy kihívás számunkra, de létfontosságú. Meg kell találnunk a rendelkezésre álló technikai lehetőségeket is, nem csak új eszközök beszerzésében kell gondolkodnunk. Ennek megfelelően kerül sor egyes haditechnikai felújítására, modernizációjára, mint például a BTR-ek éjjellátó berendezéssel, korszerű kommunikációs eszközökkel történő felszerelése.

Összegzés

Összességében kijelenthetjük, hogy a képességek nemzeti szempontok szerinti alakításánál prioritást kell biztosítanunk a hazánkat érintő globális veszélyforrások kezeléséhez szükséges feltételek megteremtésének, illetve fejlesztésének.

A hagyományos értelemben vett háborús konfliktus valós bekövetkeztével továbbra sem kell számolnunk, de egyre nagyobb jelentőséget kapnak a határainktól távol végrehajtandó béke-, illetve stabilizációs műveletek, valamint a nemzetközi terrorizmus elleni harc katonai lépései. A képességeink fejlesztését ebbe az irányba kell folytatnunk a Szövetség azon államainak egyikeként, amely kisebb méretű haderővel rendelkezik. A NATO transzformációjának folyamatos nyomon követésével és az abból levonható következtetésekkel, elemzésekkel, és ajánlásokkal összhangban a specializált képességekre célszerű a nagyobb hangsúlyt fektetnünk.

Ezeknek a képességeknek a kialakítása, a küldetésorientált katonai erő megteremtése érdekében a törvényhozóknak, a szakértőknek, a katonai vezetőknek, a tervezőknek és a végrehajtó állománynak egyaránt igen komoly munkát kell végezniük, most és a jövőben egyaránt.

A tudományos konferencia elnöksége

MARTON CSABA MK. EZREDES

A SIGINT FELADATAINAK ÉS VEZETÉSI RENDSZERÉNEK VÁLTOZÁSA

Minden korban megvásárolhatjuk a katonáknak a legmodernebb felszereléseket (például fegyverzet, páncél stb.), de ezzel még nem garantálhatjuk a biztonságukat és a hatékony feladat-végrehajtást. Az eredményes tevékenységhez a harcosnak a fegyverzeten kívül megfelelő minőségű és mennyiségű felderítési információra van szüksége.

A katonai felderítési nemek, mint például a humán erővel folytatott, a képi, a műszeres és a rádióelektronikai felderítés képes információt szolgáltatni a vezető részére. Maga a több forrásból megerősített információ biztosítja, hogy hatékonyan lehessen felhasználni a döntés-előkészítésben.

A katonai rádióelektronikai felderítés más felderítési nemekkel együtt teszi lehetővé a többforrású adatszerzést, növelve a megszerzett adatokból kinyert információk megalapozottságát és hitelességét. A rádióelektronikai felderítés sajátosságánál fogva képes reálidőben adatokat szerezni olyan objektumokról is, amelyek más felderítési nemek alkalmazásával nem foghatók le**.**

A rádióelektronikai felderítés specifikus eszközrendszerével az elektromágneses kisugárzások összegyűjtéséből, összevetéséből, feldolgozásából és értékeléséből szerez információkat. A rádióelektronikai felderítés előnye, hogy az elektromágneses kisugárzások széles skáláját képes megfigyelni, nagy földrajzi mélységben tevékenykedhet, reálidejű információt szolgáltat és passzív eszközöket használ. Hátrányos oldala, hogy függ az adatforrások aktivitásától, a hullámterjedést befolyásoló fizikai tényezőktől, illetve folyamatosan fejleszteni kell a szaktechnikai eszközöket, eljárásai bonyolultak, sokoldalú támogatást, valamint speciális képzettségű és szaktudású munkatársakat igényel.

A rádióelektronikai felderítés képes adatokat és információkat szerezni:

- a biztonságpolitika katonai elemét érintő katonapolitikai, katonai hadiipari témákról;
- a Magyar Köztársaság biztonságát közvetlenül veszélyeztető katonai és nem hagyományos fenyegetésekről, azok előre jelzése érdekében;
- a hazánk környezetében elhelyezkedő fegyveres erők készültségéről, állapotáról, fegyverrendszereiről;
- a közeli és távolabbi instabil régiókban, válságkörzetekben zajló eseményekről, változásokról;
- a transznacionális fenyegetésekről és kockázatokról;
- a kormányzatok, a nemzetközi szervezetek és a nem kormányzati szervezetek állásfoglalásairól, reagálásairól.

A politikai–társadalmi rendszerváltozás előtt a rádióelektronikai felderítés viszonylag könnyű helyzetben volt, mivel a célországok katonai szervezetinek felépítése, harceljárásai megismerhetők voltak. A hadászati, hadműveleti és harcászati tagolódáshoz pontosan kapcsolódtak a híradó rendszer elemei. Abban az időszakban a felhasználói igények beérkezését követően a vezetők – rövid feladattisztázás után – már feladatot tudtak szabni az adatszerző erők részére.

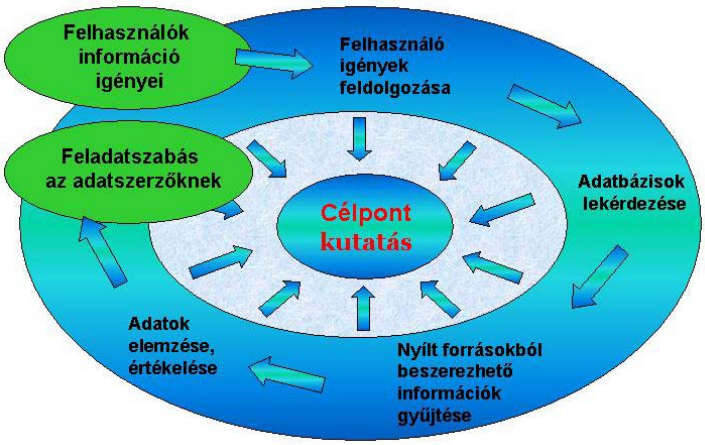
A **hadászati** szinthez az állami és katonai felső vezetés vezetési rendszerei, valamint a légierő és a légvédelmi rakétacsapatok rövidhullámú, rádiórelé és műholdas rendszerei tartoztak. A **hadműveleti** kategóriához a magasabbegységek rövidhullámú és rádiórelé rendszerei, valamint harcászati légierő irányítására szolgáló rendszerek voltak köthetők. A **harcászati** szinten a zászlóalj és század híradását biztosító, súllyal az URH és VHF tartományban üzemelő rendszerek elemeit találhattuk.

Rádióelektronikai felderítési szempontból napjainkban nehezebb pontosan kategorizálni célobjektumokat, mivel nagyon ritka a reguláris csapatok egymással szemben állása, valamint nehéz meghatározni, hogy egyes fegyveres csoportok milyen kommunikációs eszközöket alkalmaznak.

A helyzet jelentősen megváltozott, mivel a felhasználók a távközlési eszközök széles skáláját használhatják az információk átadására. Már nem a katonai távközlés dominanciája jellemző, hanem alternatív polgári hírközlő eszközök vették át a szerepüket. Egy terrorista csoport azt a híradó eszközt használja, amellyel az adott térségben legjobban tud kommunikálni, és általában komplex szolgáltatást biztosító eszközöket részesítenek előnyben: zsebben hordozható számítógépet, mobiltelefont, műholdas kép- és hangtovábbító eszközöket. A fentiekből is következik, hogy nehéz az általános összeköttetés-szervező elveket ráhúzni erre a helyzetre, valamint a hadműveleti és harcászati kategóriák közötti különbség napjainkban egyre jobban elmosódik.

A rádióelektronikai felderítő erők feladatainak pontosabb meghatározása érdekében, illetve az optimális adatszerző eszközök kiválasztása céljából a felderítő tevékenység megkezdése előtt a „célpont jellemzőit” kell meghatározni, úgynevezett „célpontkutatást” kell végezni (1. ábra).

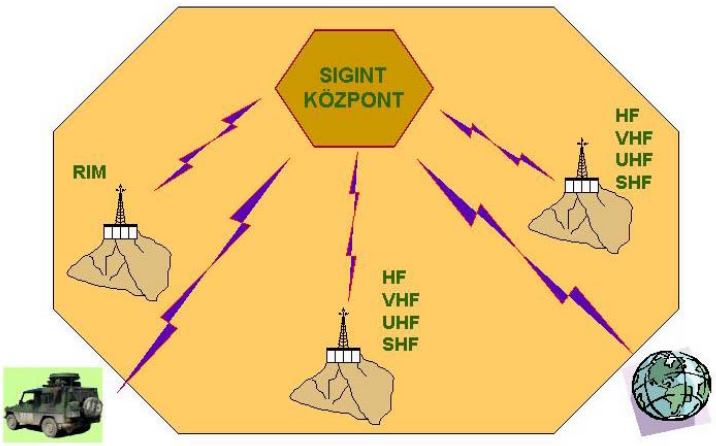
A **célpontkutatás** első lépése a beérkezett információigények feldolgozása, osztályozása. Ezt követően meg kell vizsgálni, hogy az információigényre vonatkozó adatok az adatbázisokban rendelkezésre állnak-e, vagy sem. Ha nem rendelkezünk az igény kielégítéséhez elegendő információval, akkor elemezni kell, hogy milyen távközlési eszközöket, illetve rendszereket alkalmazhat a célobjektum az adott térségben. Az elemzéshez minden rendelkezésre álló forrást igénybe kell venni, például a nyílt forrásból hozzáférhető adatokat is (internetcímek, telefonkönyvek adatai, a távközlési rendszer felépítése stb.). Az adatok elemezését, értékelését követően alkothatjuk meg a célpont profilját. A célpont profiljából kiindulva választható ki a leghatékonyabban alkalmazható rádióelektronikai felderítő erő, illetve szaktechnikai eszköz. A **célpont** több forrásból történő megközelítésével jelentősen növelhető az adatszerzés hatékonysága.



1. ábra. A célpontkutatás elvi folyamata

Milyen adatszerző rendszert alakítsunk ki?

Egy komplex rádióelektronikai felderítő rendszer honi területen települt központi egységből, kihelyezett stabil telepítésű automatizált állomásokból és a rendszer rugalmasságát biztosító mobil állomásokból, valamint a szövetségi rendszerből adódóan missziós területen alkalmazott rádióelektronikai felderítő erőkből célszerű felépíteni (2. ábra).



2. ábra. Adatszerző rendszer elvi felépítése

A honi területen üzemelő **központi egység** supervisor munkahelyeiről – megfelelő kapacitású és átviteli sebességű informatikai rendszeren keresztül – történik a kihelyezett stabil állomások vevő-alrendszereinek vezérlése.

Az adatok rögzítése történhet közvetlenül a központ szerverén, ez esetben a távvezérelt állomások által felfedett információt reálidőben továbbítják. Ez a módszer nagy adatátviteli és rögzítő kapacitást igényel.

Ha az adatok rögzítése a kihelyezett állomás adattároló rendszerében történik, akkor a supervisor szerepe csak a vevők lehangolására és ellenőrzésére korlátozódik. A rögzített adatokat csak előzetes szelektálás, előértékelés után továbbítják a központnak. Ez a megoldás kisebb kapacitású adatátviteli sebességet igényel, viszont csorbát szenved az információ reálidejűsége.

Az állandó telepítésű rádióelektronikai felderítő rendszert célszerű **mobil elemekkel** kiegészíteni, amely egy adott feladat-végrehajtás esetén képes az erőkifejtés meghatározott irányokba történő, rövid időn belüli áthelyezésére. A mobil állomásnak gyorsan alkalmazhatónak, rugalmasan felkészíthetőnek, különböző szaktechnikai eszközökkel és megfelelő terepjáró képességgel kell rendelkeznie.

Az állomást az adott feladatok figyelembevételével készítik fel, de az alábbi alapkövetelményeknek mindig meg kell felelnie:

- rendelkezzen forgatható antennarendszerrel és iránymérési képességgel;
- biztosítson vételi lehetőséget minél szélesebb frekvenciatartományban;
- rendelkezzen hagyományos és digitális jelanalizálás-képességgel;
- rendelkezzen digitális adatrögzítési képességgel;
- a híradó rendszere biztosítson közvetlen, védett összeköttetést a központi állománnyal.

Az adatszerző rendszernek egyik fontos eleme a **missziós területen alkalmazott rádióelektronikai felderítőerő**, amely képes folyamatosan adatokat szolgáltatni a szemben álló félről az elöljáró szövetséges parancsnokságnak, illetve a koalícióban részt vevő nemzetek honi felderítőerőinek.

A műveleti területen alkalmazott rádióelektronikai felderítőerők feladata az elektromágneses energiát kisugárzó aktív elektronikai eszközök felderítése, ezáltal adatok szerzése a szemben álló felek állapotáról, helyzetéről, csoportosításáról, tevékenységéről és szándékáról.

A válságreagáló műveletekben részt vevő erők felderítő biztosításának körülményeit alapvetően meghatározza, hogy a feladatot végrehajtó kontingens rendelkezik-e saját felelősségi körzettel. Az önálló felelősségi körzettel rendelkező békefenntartó kontingens alkalmazásakor indokolt a felderítőerőket rádióelektronikai felderítő-alegységgel is kiegészíteni.

Az alegység elsődleges feladata a kontingens napi tevékenységéhez szükséges rádióelektronikai felderítőadatok biztosítása (Force Protection), illetve a J–2 törzsének információkkal történő ellátása.

A **rádióelektronikai felderítő-alegységek** szervezetébe az alábbi elemek tartozhatnak:

- stabil, állandó telepítésű rádióelektronikai felderítőállomás;
- mobil rádióelektronikai felderítőállomás;
- értékelő csoport.

A válságreagáló erők állományából indokolt egy stabil rádióelektronikai felderítőcsoport létrehozása. A csoport létszáma 6–10 fő.

A rádióelektronikai felderítőcsoport stabil – konténerekben elhelyezett – állomásokban a kontingensparancsnokság körletében célszerű telepíteni.

A válságtérségben telepített stabil rádióelektronikai felderítőállomásokat az adott térség rádióelektronikai helyzetét figyelembe véve általában VHF, UHF és SHF frekvenciatartományban üzemelő felderítő berendezésekkel indokolt felszerelni.

A stabil állomások szaktechnikai eszközeit alkalmassá kell tenni arra, hogy honi területről – műholdas összeköttetés segítségével – távvezérelhetők legyenek.

A stabil állomásokon szolgálatot teljesítő állomány alapvetően felfedő feladatokat lát el. A felfedett rádióelektronikai objektumok lehallgatását – a paraméterek beállítását követően –, a rendszeresített technikai eszközök automatikusan végzik, illetve a rögzített információkat titkosított műholdas adatátviteli csatornákon honi területre továbbítják.

Az állomásnak rendelkeznie kell analizáló és jelfeldolgozó képességgel, illetve az adatok és jelentések archiválásához szükséges tárolókapacitással is.

A stabil rádióelektronikai felderítőállomásokkal felfedhetők és lehallgathatók a szemben álló fél rádió-, rádiótelefon- és mikrohullámú rendszerei.

Az önálló felelősségi körzettel rendelkező kontingens rádióelektronikai felderítő rendszerét nemcsak stabil rádióelektronikai felderítő állomásokkal célszerű kiegészíteni, hanem kis létszámú mobil rádióelektronikai felderítőcsoporttal is. A csoport tervezett létszáma 3-4 fő.

A parancsnoknak ez a rádióelektronikai felderítőcsoport biztosíthatja a felderítés rugalmasságát, viszont nem szabad elfelejteni, hogy egy háborús térségben alkalmazott mobil állomás nagy kockázatnak van kitéve.

A mobil rádióelektronikai felderítő-alegységek által rögzített felderítési információkat a rendelkezésre álló híradó rendszeren keresztül a stabil állomásokban kialakított felderítőközpontba továbbítják, ahol megtörténik azok előzetes feldolgozása (3. ábra).

Az értékelő csoportot a stabil rádióelektronikai felderítőállomás konténerében célszerű elhelyezni. Az értékelő csoport hajtja végre a megszerzett adatok és információk azonnali értékelését, jelentését. Az értékelő csoport létszáma 3–5 főre tervezhető.

Az adatszerző munkahelyeken megszerzett adatok és információk feldolgozására és jelentésére a nemzetközi gyakorlatban két módszert alkalmaznak:

- A rádióelektronikai felderítőberendezések által szolgáltatott adatok és információk kezelését – szelektálását, előértékelését és fordítását, majd értékelését és elemzését, valamint a jelentések elkészítését, illetve az adatbázisok vezetését –, az értékelő csoport szakemberei helyben hajtják végre.

  Az adatfeldolgozást követően a jelentéseket egyidejűleg továbbítják a nemzetközi parancsnokság J–2 törzse és a nemzeti kontingens törzse részére, valamint honi területre a mélyelemzések és értékelések végrehajtása céljából. Természetesen, jelentései elkészítéséhez az értékelő csoport a honi felderítő rendszertől folyamatosan kiegészítő információkat is kap.

  A módszer előnye, hogy valósidejű információkat szolgáltat. Hátránya azonban, hogy a felfedett, nagy mennyiségű információk miatt adatvesztés is előfordulhat. Ez kiküszöbölhető különböző előszelektáló programok alkalmazásával.

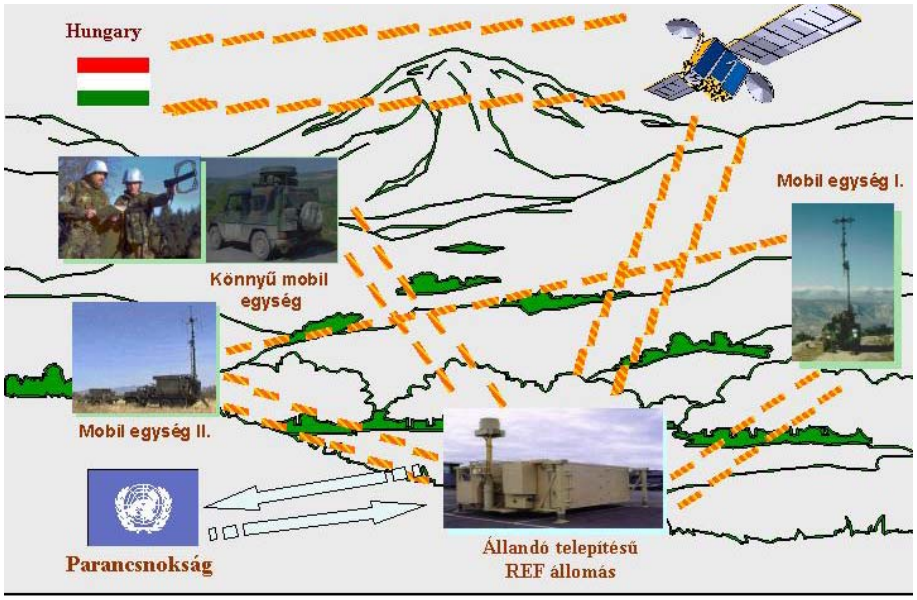
- Az adatszerzők által megszerzett adatokat és információkat az értékelő csoport által végrehajtott előzetes szelektálás után elemzésre és értékelésre honi területre továbbítják, ahol a már meglévő komplex adatfeldolgozó rendszer segítségével végrehajtják az adatok értékelését és elemzését, majd az elkészült értékelt információkat kapja meg az értékelő csoport, valamint a nemzetközi és a nemzeti parancsnokságok.

  A módszer hátránya a valósidejű jelentőképesség elvesztése, előnye viszont az alapos és minden szempontra kiterjedő elemző–értékelő tevékenység végrehajtása.

A fent bemutatott két módszer közül előnyösebb az adatok megszerzését követő azonnali adatfeldolgozás, mert az biztosítja a jelentések reálidejűségét.

A válságreagáló műveletek végrehajtása során önálló felelősségi körzettel nem rendelkező kontingens tevékenységét is indokolt rádiófelderítő-csoporttal támogatni. Ebben az esetben célszerű egy terepjáró-képességgel rendelkező, mobil, nagy mozgékonyságú rádiófelderítő-gépjármű alkalmazása. A csoport a nemzeti kontingens parancsnoka alárendeltségében 5-6 fővel hajtaná végre feladatait.

A válság körzetében tevékenykedő erők által üzemeltetett rádióelektronikai eszközök ismérveit figyelembe véve kell az alkalmazásra kerülő rádióelektronikai felderítő-gépjárművet szaktechnikai eszközökkel felszerelni. Tapasztalatok alapján a gépjárműbe alapvetően VHF frekvenciasávban üzemelő, valamint digitális és analóg rádiótelefonok lehallgatására alkalmas berendezések célszerű telepíteni.



3. ábra. Válságreagáló művelet rádióelektronikai felderítő támogatásának elvi vázlata

Hogyan dolgozzuk fel a rögzített adatokat?

Napjainkban a felderítési adat előállításához rendelkezésre álló idő jelentősen lerövidült és természetesen jelentkezik a „túl sok információ" problémaköre is.

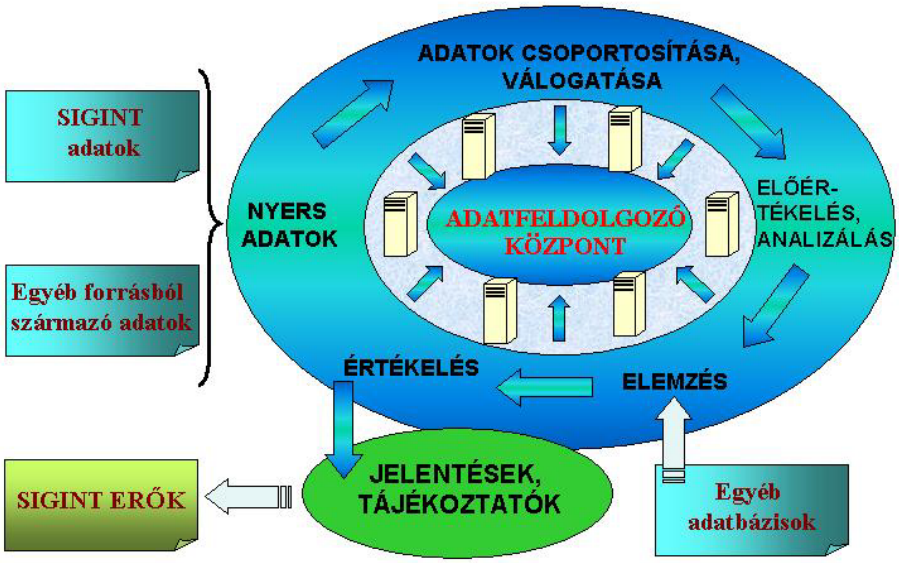
A rádióelektronikai felderítő rendszer „bemeneti adatai" zömét a különböző frekvenciatartományban üzemelő automatizált szaktechnikai és rádióelektronikai eszközök szolgáltatják. Ezeket alapadatoknak nevezzük (például vivőfrekvencia, frekvencialöket, modulációs mód stb.) (4. ábra).

A rendszer az óriási adatmennyiség kezelésére nagy számítástechnikai tárolókapacitást igényel, ebben az esetben több terrabyte-ról beszélhetünk. A bejövő adatokat egységes adatbázisba kell rendezni, majd a különálló adatbázisokat összekapcsolva, már lehetőség nyílik az ezekben történő keresésre, az összefüggések vizsgálatára. (Például a rögzített faxok karakterfelismerő programok segítségével viszonylag egyszerűen digitalizálhatók, s így már beilleszthető az adatbázisba.)

Ezt követően történhet az adatbázisban rögzített adatok fordítása, előértékelése, vagyis az adott adathalmazból a megfelelő rendező elvek alapján az információ kinyerése, illetve egységes bonyolultabb jelstruktúrájú jelek analizálása. A kinyert információk elemzését, majd értékelését követően új érték hozzáadásával, magasabb tartalmi értékkel bíró felderítési információhoz juthatunk.

Ezek az információk a meghatározott szinteken működő vezetők számára alapvetően fontosak az optimális döntések meghozatalához.

Nagyon fontos ebben a folyamatban a rádióelektronikai felderítőerők felé történő visszacsatolás, amely tovább növelheti a felderítés hatékonyságát.



4. ábra. Adatfeldolgozó rendszer elvi felépítése

A katonai rádióelektronikai felderítésről

A katonai rádióelektronikai felderítés 1947-től napjainkig, azon belül hadászati, hadműveleti, mind hadászati szintű feladatait végrehajtó erők több átszervezésen, szervezeti korszerűsítésen, s az utóbbi években létszámcsökkentésen mentek át. Az egyes időszakokban változott a rádióelektronikai felderítő erők vezetési és irányítási rendszere is.

Minden katonai szervezethez hasonlóan a rádióelektronikai felderítő rendszer struktúrája és vezetése a bürokratikus szervezeteknek megfelelően épült és épül fel, amely magán hordozta az alábbi főbb jellemzőket:

- centralizált irányítás;
- a feladatok pontos és részletes meghatározása;
- a legapróbb részletekig kidolgozott szabályok;
- a vezetők és beosztottak éles különválasztása;
- a vezetők és beosztottak személytelen viszonya.

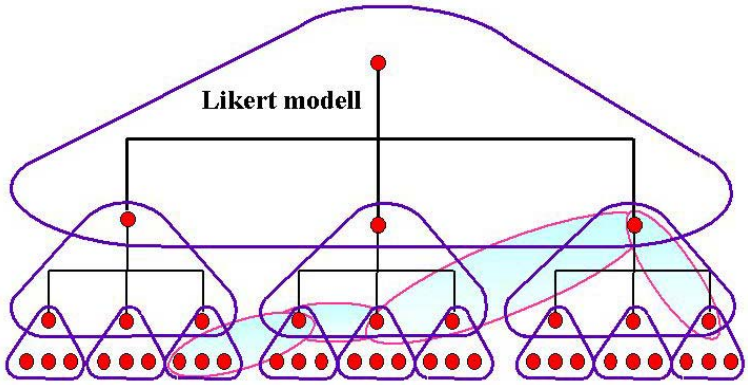
A katonai szervezet szempontjából természetesen a bürokratikus szervezetnek vannak előnyös és hátrányos tulajdonságai. Wéber a következő gondolatokban foglalta össze a bürokrácia hátrányait:

- a bürokrácia természetében rejlő alapvető tendencia, hogy növekedésre törekszik: minél több a beosztottak száma, annál nagyobb a bürokratikus vezető tekintélye;
- az előléptetési szabályok ahhoz a képtelen helyzethez vezetnek, hogy mindenki addig emelkedik a hierarchiában, míg olyan szintre nem jut, ahol már nem tud megfelelni a feladatnak;
- a bürokrácia a szervezet eredeti célja helyett saját bürokratikus céljait követi, saját maga működése válik céllá;
- a bürokráciában „benne van" az oligarchizálódási tendencia;
- mindezek miatt a bürokratikus szervezetek merevekké válnak.

A bürokratikus rendszer fölött ma már bizonyos mértékben eljárt az idő, mivel gyorsan változó globalizálódó világunkban a rendszernek csekély az alkalmazkodóképessége, lassú reakcióideje miatt hatékonysága jelentősen lecsökkent. A változás fő mozgatórugója az információs társadalom fejlődésének rendkívül gyors ütemében keresendő, amely a rádióelektronikai felderítés vezetési rendszerében is fokozottan jelentkezik.

Természetesen egy katonai szervezet irányítása esetén nem szakadhatunk el teljesen a bürokratikus szervezettől, de a Likert-féle modell alapján jelentősen javíthatunk a működésén. A Likert modell azon alapul, hogy a szervezet minden tagja összekötő kapocsként szolgál az alatta és felette álló szervezet között. Az ilyen rendszerben minden dolgozó – a legfelső és a legalsó szint kivételével – két csoport tagja: a felette lévő csoportnak beosztottként, az alatta lévő csoportnak pedig vezetőként. Ebben az esetben az egyének közötti kapcsolat helyébe a csoportok közötti kapcsolat kerül, viszont az adott csoport vezetőjének továbbra is meghatározó szerepe van. A modell alapvető jellemzője a hatékony „team" munka (5. ábra).

A katonai rádióelektronikai felderítés naponta találkozik új kihívásokkal, amelyre megpróbál választ adni, illetve reagálni. A felmerülő problémák megoldására, nem célszerű minden esetben új szervezetet létrehozni. Egy adott cél elérése, vagy egy feladat megoldása érdekében – meghatározott időtartamra, időszakra – a „hierarchiát megsértő", a feladatmegoldásához szükséges magasan képzett szakembergárda összeállításával létrehozhatunk egy mátrix-szervezetet. A mátrix-szervezetben a munkaerő hatékonyabb, a feladatokhoz jobban igazodó kihasználását teszi lehetővé.



5. ábra. A Likert modell és a mátrix-szervezet

A rádióelektronikai felderítő szervezetek vezetése során megítélésem szerint, az alapvetően bürokratikus katonai szervezet kombinálva a Likert modellel és a mátrix-szervezetekkel, hatékonyabban tudna reagálni a kor kihívásaira.

Összefoglalás

A rádióelektronikai helyzet gyors változásait követni kell a rádióelektronikai felderítő rendszernek, ezért annak hatékony irányítása alapvető fontosságú.

A rádióelektronikai felderítés a 21. században magas technológiai színvonalú és bonyolult spektrumú elektromágneses környezettel áll szemben, ezért folyamatosan fejleszteni kell a rádióelektronikai felderítő-szaktechnikai eszközöket, módszereket, illetve a vezetési rendszerét.

Megítélésem szerint a magyar katonai felderítésnek a jövőben is kiemelt feladata lesz a válságkörzetekben alkalmazott magyar erők felderítőtámogatása. A missziós feladatokat ellátó magyar kontingensek felderítőtámogatása napjainkban nem minden esetben kielégítő. Ezért a külföldön válságreagáló feladatokat ellátó magyar kontingensek szervezetébe célszerű rádióelektronikai felderítőerőket is kiküldeni, amelyek képesek a parancsnokok részére folyamatos és időszerű információkat szolgáltatni.

FELHASZNÁLT IRODALOM

- AJP–1 *Szövetséges összhaderőnemi doktrína.*
  HVK Védelmi-tervezési Főnökség, 1999, Budapest.

- FM 34-2-1. *A felderítés-elhárítás felderítő és hírszerző támogatása.* Nemzetvédelmi Minisztérium Törzs, Washington DC, 1990.
- MC-101 NATO Signals Intelligence Policy.
- Marton Csaba: *A békefenntartó műveletek rádióelektronikai felderítő támogatása.* Felderítő Szemle II. évfolyam 4. szám, 2003. december.
- Pászka Tibor: *Szükség van-e rádióelektronikai felderítésre?* Felderítő Szemle III. évfolyam 2. szám, 2004. június.
- Kein Sándor: *Szervezet- és vezetéspszichológia.*
- Juhász József – Dr. Szternák György – Tóthné Szternák Nóra: *A fegyveres erő jelene és jövője a képességek kialakításának tükrében*. Tanulmány, 2006.
- John Keegan: *A háborús felderítés*. Budapest, 2005, Európa Könyvkiadó.
- *A válságreagáló műveletekre történő felkészítés néhány jellemzője.* Egyetemi Közlemények. Budapest, 2005, ZMNE.
- Bolgár Judit – Kiss Zoltán László – Dr. Szternák György: *A válságreagáló műveletekre történő felkészítés.* Tanulmány, 2005.

DR. HAIG ZSOLT MK. ALEZREDES

AZ INFORMÁCIÓS MŰVELETEK, A SIGINT ÉS AZ ELEKTRONIKAI HADVISELÉS KAPCSOLATRENDSZERE

BEVEZETÉS

Napjainkban az emberiség nagy léptekkel halad az információs társadalom globális, regionális és lokális méretű kiépítésében. Az iparilag fejlett országokban gyors ütemben alakulnak ki az információra alapuló új típusú társadalmak. Az információs társadalom a felülről szervezett, de alulról építkező digitális demokrácia társadalma, ahol megvalósul a vezetők és vezetettek hálózatos kapcsolata és egysége. Ugyanakkor érvényre jut a központi szándék és akarat, amely a vezetési rendszereken és a kritikus információs infrastruktúrákon keresztül valósul meg. Az információnak – mint a tudáshoz vezető út kiinduló elemének –, a tudás alapú társadalomban kitüntetett és meghatározó szerepe van.

Az információs társadalom működése az információk és információs rendszerek támadásán keresztül jelentősen befolyásolható, károsítható, hatékonysága csökkenthető. Ezért e társadalmak elért vívmányait korszerű vezetésű, információra alapozott hadviselési formákat alkalmazó haderők védelmezik.

A korszerű fegyveres erők széleskörűen használják az elektromágneses teret a kommunikáció, a fegyverirányítás, az ellenőrzés, a felderítés, a navigáció és a csapatok megóvása érdekében. Az e területeken alkalmazott elektronikai eszközök jelentősen növelik a katonai erő alkalmazási lehetőségeit. Ebből következően a katonai műveleteket irányító parancsnokoknak kiemelt figyelmet kell fordítaniuk – felelősségi és hadműveleti körzetükben – az elektromágneses spektrum felhasználására.

Napjaink hadszínterén – ami az elektromágneses dimenzióban végzett műveletek szempontjából joggal nevezhető **elektronikus harcmezőnek** –, számtalan különböző típusú és rendeltetésű elektronikai eszköz található. Ezek az eszközök ugyanazon információs és elektromágneses környezetben működnek, amely szükségessé teszi a köztük lévő interoperabilitási képességek erősítését.

Az információs környezetben folytatott tevékenységek összehangolására való törekvések egy teljesen új elmélet és gondolkodásmód megszületéséhez vezettek, amely nem más, mint **az információs műveletek koncepciója**. E koncepció szerint a katonai műveletek során folytatott információszerzés, -továbbítás, -feldolgozás, -tárolás és -felhasználás; illetve a saját információs képességek megóvása és a másik fél hasonló rendszerei működési folyamatainak akadályozása egységes elvek mentén, egymással összehangoltan az eddigieknél jóval nagyobb sikerrel kecsegtet.

AZ INFORMÁCIÓS ÉS A VEZETÉSI FÖLÉNY KIALAKÍTÁSA

A katonai műveletek során az információszerzés sok forrásból történik, amelyek rétegesen át- és lefedik egymást. A többszörösen ellenőrzött és az automatikus adatfúziós és korrelációs információs technológiával szinkronba hozott, minőségileg új és tömörített információk a hadsereg számára **információs fölényt**, illetve **vezetési fölényt** biztosítanak az ellenség felett.

Az információs fölény értelmezése

Az információs fölény birtokosának lehetővé teszi, hogy információs rendszereit és azok képességeit kihasználva hadműveleti fölényre tegyen szert, vagy a hadműveleti helyzetet folyamatosan úgy alakítsa, irányítsa, hogy emellett az ellenséget megfossza e képességeitől.

Az információs fölény megléte (többek között) lehetővé teszi, hogy:

- többet tudjon a szemben álló félről, mint amit ő tud a saját erőiről;
- eredményesen tudja korlátozni a szemben álló fél vezetési és információs rendszereit, illetve döntési folyamatait, miközben ilyen behatásoktól képes megóvni a saját rendszereiket;
- a sajátoldali vezetési folyamat gyorsabb legyen, mint a másik fél vezetési folyamata [F.i. 1; 2][*].

Az információs fölény megszerzése és megtartása az alábbiakat jelenti:

- az ellenségről, a harctéri környezetről és a saját erőkről szerzett információkkal megteremteni az információs fölény alapját;
- kihasználni és megvédeni a saját információs képességeinket;
- gyengíteni, lerontani az ellenség információs lehetőségeit (1. ábra).

Az információs fölény és uralom megszerzéséért folytatott erőfeszítések elmélete – többek között – a kommunikációelméleten (a rendszerek közötti kapcsolatok és viszonyok elmélete), valamint a káoszelméleten alapul.

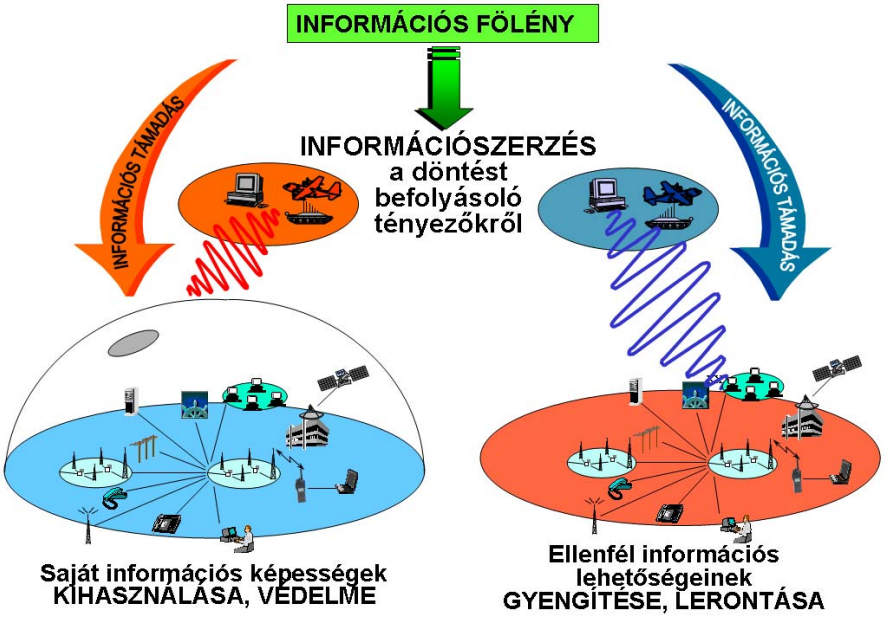
A kommunikációelmélet szerint a társadalmi szervezetek között alapvetően kétféle kapcsolati csatornán áramlik az anyag, energia és az információ, úgymint:

- a közlekedési, a szállítási és a logisztikai csatornákon; valamint
- a távközlési és információs hírcsatornákon, amelyek fenntartják a szervezetek belső integritását.

Az információs fölény megszerzéséért folytatott erőfeszítések lényege abban áll, hogy amennyiben a szervezetek, rendszerek közötti információs csatornákat elvágják, elszigetelik, működésüket bénítják vagy korlátozzák, akkor bekövetkezik a rendszerek önzáródási effektusa, amelyben az érintett szervezet vagy rendszer csak saját információs és egyéb erőforrásaira tud támaszkodni.

[*] **Megjegyzés:** Felhasznált irodalom (F.i.) 1. és 2. pontja. (Végig.)

Ezek pedig tudvalevőleg nem elegendőek hosszú távú tevékenységre. A saját erőforrások intenzív belső felhasználásának törvényszerű eredménye, hogy az érintett rendszerben beindul a káosztörvény érvényesülése, vagyis a szervezett rendből, az irányíthatóságból és vezethetőségből öntörvényűen kialakul a szervezetlenség, irányíthatatlanság, vezethetetlenség állapota. Az információáramlástól megfosztott katonai szervezeteknél is érvényesek ezek a hatások, vagyis megtörténik a szervezeti, rendszeri és tevékenységi összeomlás. A támadó fajtájú információs műveletek esetében az ellenség oldalán pontosan ilyen helyzet előidézése a cél [F.i. 1; 2].



1. ábra. Az információs fölény értelmezése

Mivel a tökéletes és hosszan tartó információs fölény kialakítása nem lehetséges, ezért keresni kell a lehetőséget, hogy az információs fölényt a számunkra legjobb helyen, a legjobb időben és a legjobb körülmények között érjük el. Az információs fölény megléte esetén képesek vagyunk befolyásolni az ellenségnek a helyzetről alkotott képét, megteremteni a feltételeket a kezdeményezés megragadására, valamint szabályozni a katonai műveletek ütemét.

Az információs fölény a parancsnok számára kedvező feltételeket biztosít a vezetés megvalósításához és elősegíti a kezdeményezés megragadását. Az információs fölény azt jelenti, hogy birtokosai a kulcsfontosságú területeken a szembenálló félnél több, fontosabb és pontosabb információval, információs eszközzel és módszerrel rendelkeznek, és azokat eredményesebben tudják felhasználni. Az információs fölény azt is jelenti, hogy a sajátoldali információ felhasználás és hasznosítás legalább egy nagyságrenddel jobb és többre képes az ellenség hasonló rendszereinél [F.i. 1; 2].

Az információs fölény kialakulásához jelentős mértékben járul hozzá a legújabb információtechnológiai eszközök és vezetési módszerek alkalmazása. Ezért az információs fölény megszerzésének és megtartásának nélkülözhetetlen előfeltétele a korszerű, integrált vezetési, információs és felderítő rendszerek (C^4ISR) széleskörű alkalmazása. A különböző fajtájú és spektrumú felderítő eszközök, szenzorok folyamatosan ontják a fizikai és állapotváltozások műszeres mérési adatait. Ezekre az adatokra támaszkodva szervezik meg az ellenőrző, megerősítő felderítéseket, majd pedig az ellentevékenységet. A korszerű C^4ISR rendszerek képesek az objektív döntést alátámasztó pontos és részletes információk szolgáltatására [F.i. 1; 2]. Az információs fölény elérése és megtartása tehát szorosan függ a különböző szenzorok, felderítő eszközök és rendszerek minőségétől, a vezetési folyamat gyorsaságától, a végrehajtó erők képességeitől és az eszközök egységes hálózatba kapcsolásától.

A vezetési fölény értelmezése

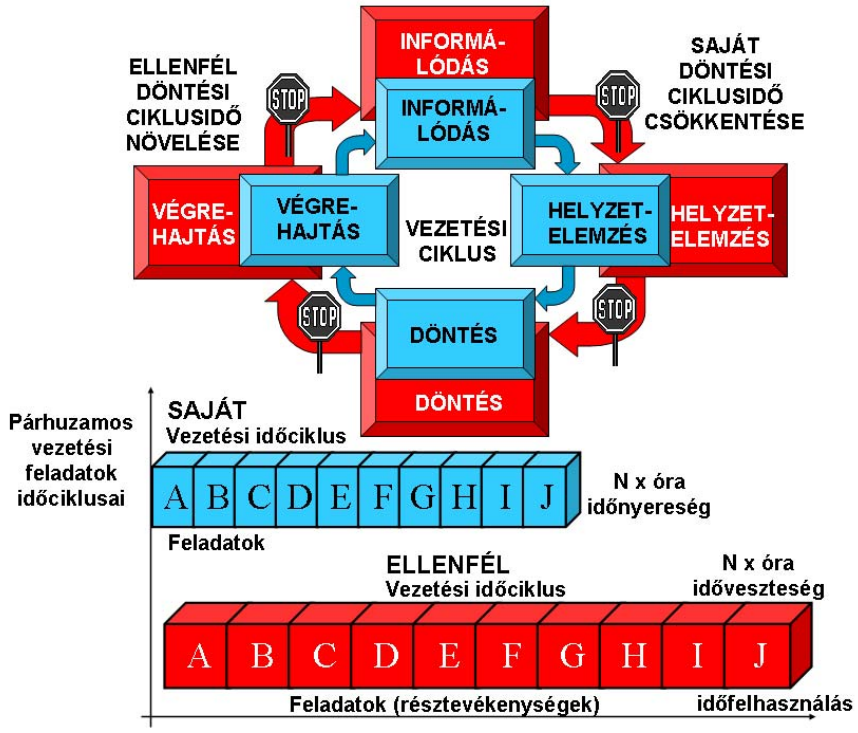
A tartós információs fölény elvezet az ellenség feletti tartós és szilárd **vezetési fölény** kialakulásához, amely a siker egyik fontos záloga. A vezetési fölény a szemben álló felek vezetési folyamatai között olyan minőségi különbséget jelent, amikor az egyik fél tevékenységét meghatározó parancsok, utasítások tartalma és időbelisége lényegesen jobban tükrözi a kialakult helyzetet, és az ahhoz alkalmazkodó célszerű cselekvésmodellt, mint a másiké.

A vezetési fölény kivívásának szükséges, de nem elégséges feltétele az információs fölény kivívása. Az információs fölény kivívása ugyanis nem mindig jelenti egyúttal az ellenség feletti vezetési fölény megteremtését is, mivel a rendelkezésre bocsátott információkat a döntéshozatal és végrehajtás során hatékonyan fel kell tudni használni. Ezen túlmenően annak érdekében, hogy a katonai műveletek célját az adott fél a lehető legkisebb veszteséggel és erőforrás bevonásával legyen képes elérni, a vezetési és információs rendszert optimálisan kell működtetni.

A rendelkezésre álló korszerű, hatékony, gyors és hálózatba kötött információszerző, -feldolgozó, -értéknövelő és -szétosztó eszközök és rendszerek segítségével, a vezetési fölény birtokában levő parancsnok megalapozottabban, több cselekvési változatot figyelembe véve, határozottan és gyorsabban hozza meg döntését, mint a szemben álló fél. A korszerű hadviselésben a parancsnokok döntési képessége és gyorsasága meghatározó jelentőséggel bír a siker elérésében. Az időben meghozott helyes döntés hatására új helyzet áll elő harctéren, ami előnyös a vezetési fölényben lévő számára, és hátrányos az ellenségre nézve. Az új helyzetet azért célszerű kikényszeríteni, mert így a parancsnok magához tudja ragadni a kezdeményezést. A vezetési fölény birtokában lévő parancsnok jobban tudja irányítani csapatainak manővereit és precíziós fegyvereinek csapásait is, mint az ellenség.

A vezetési fölény birtokában a saját vezetési tevékenységet gyorsabban, pontosabban és objektívebben lehet folytatni, ami által **vezetési időfölényre** tehetünk szert. Az időfölény természetesen magában rejti a hadműveleti fölény megszerzésének, illetve a kezdeményezés megragadásának a lehetőségét is. Mindezeket elősegíti az ellenség megtévesztése, meglepése és más váratlan lépések megtétele is.

Ennek következtében a saját vezetési tevékenységünk a szembenálló fél vezetési tevékenységén belülre kerül, gyorsabbak vagyunk, gyorsabban észlelünk, döntünk és intézkedünk, mint az ellenség [F.i. 1]. Ezt a folyamatot követhetjük nyomon az alábbi ábrán.



2. ábra. A vezetési fölény [F.i. 1]

Saját vezetési képességeink maximális kihasználása, és az ellenség vezetési képességeinek részleges vagy teljes akadályozása jelentős erősokszorozó tényező, amely a harcfeladatok végrehajtásában nyilvánul meg. A saját erők pontos és hiteles információkon alapuló elhatározás alapján végzik feladataikat. Az elöljáró folyamatosan kapcsolatban van az alárendeltjeivel, akik a valós helyzetre reagáló feladataikat szervezetten képesek végrehajtani.

Ezzel szemben az ellenség információhiányban szenved, a parancsnok döntései pontatlan és csak valószínűsíthető információkon alapulnak. Az alárendeltjeivel való kapcsolattartás bizonytalan vagy lehetetlen, aminek következtében parancsait, intézkedéseit nem tudja lejuttatni a végrehajtói szintre, illetve azok képtelenek helyzetükről tájékoztatni az elöljárót. Ennek következményeként a feladat végrehajtása irányítatlan, kaotikus. Az ellenség csapatai nem képesek a valós helyzetre reagáló szervezett erőkifejtésre. Ebben az értelmezésben a sokak által ismert klasszikus erőviszony számvetés is értelmét veszti [F.i. 3].

Az információs fölény és a vezetési fölény elérése és megtartása merőben új típusú hadviselési elvek, formák, módok alkalmazását teszik szükségessé. Ezek az új elvek gyökeresen más aspektusból közelítik meg a katonai siker eléréséhez vezető utat. A háborúra, hadviselésre oly jellemző pusztítás, rombolás, az emberi élet kioltása helyett a hatékonyság, az élőerő megóvása, a manipuláció, és a vezethetetlenségi állapot előidézése a cél. Ez azt jelenti, hogy a katonai műveletekben az információ alapú hadviselési módok a végső sikert jelentősen befolyásoló szerepet kapnak.

E hadviselési módok az információt egyrészt a vezetési folyamatban és a fegyverirányításban használják fel, mint **vezetési eszközt**, másrészt, pedig mint **támadó és védelmi fegyvert** alkalmazzák. Ezek az említett új típusú hadviselési elméletek és eljárások a **hatás-alapú műveletek**, a **hálózatközpontú hadviselés** és az **információs műveletek** köré csoportosíthatók, és amelyek új jelenségként jelennek meg a hadviselés területén.

Az információs műveletek fogalma, célja

Az információs műveletek első koordinált megnyilvánulása az első Öböl-háborúban volt érzékelhető, ahol a szövetséges erők sikerének döntő eleme volt az információs fölény, az információs uralom és a vezetési fölény, amelyet multiszenzoros adatszerzéssel, adatfúziós feldolgozási technológiával, számítógép-hálózatokra alapozott harcvezetéssel, az ellenség felderítő, vezetési és fegyverirányítási rendszereinek bénításával és félrevezetésével értek el. Mindezen tevékenységeket tervszerűen, egységes vezetés alatt végezték, ami az információs műveletek egyik alapvető elve [F.i. 1].

Napjainkban a hagyományos háborús terekben folyó katonai tevékenységek mellett, azokkal párhuzamosan, egyrészt azok támogatására, az információs hadszíntéren információs tevékenységek – információs műveletek – zajlanak. Minden olyan tevékenységet az információs műveletek közé sorolhatunk, amelyek a szemben álló fél információs rendszereire, végső soron információira gyakorolnak olyan hatást, amelyekkel a saját döntéshozók a politikai, gazdasági és katonai célkitűzéseik elérése érdekében támogathatók, illetve amelyek biztosítják a saját információs rendszerekben rejlő képességek maximális kihasználását és megvédését.

Az információs műveletek tehát azon koordinált tevékenységeket jelentik, amelyek a szemben álló fél információira, információ-alapú folyamataira és infokommunikációs rendszereire gyakorolt ráhatásokkal képesek támogatni a döntéshozókat a politikai és katonai célkitűzéseik elérésében úgy, hogy e mellett a saját hasonló folyamatokat és rendszereket hatékonyan kihasználják és megóvják [F.i. 4].

Az információs műveletek célja az információs és a vezetési fölény kivívása, a saját oldali vezetési ciklus számára időcsökkentés, a szemben álló fél vezetési időciklusa tekintetében pedig időnövelés elérése érdekében, és ezek által a hadműveleti fölény elérésének elősegítése [F.i. 1]. Megszerzésének és megtartásának két azonos fontosságú oldala van, úgymint: **kihasználni és megvédeni a saját információs képességeket**, illetve **gyengíteni az ellenség információs lehetőségeit**.

Mindezek érdekében adott szervezetek béke, válság és konfliktus időszakában információs műveleteket hajtanak végre.

A fenti célok elérését biztosító támadó jellegű információs műveleteket **közvetlenül** – egyes kijelölt célpontokra koncentráló direkt támadási módszerrel –, vagy **közvetett módon** – a mélységben lévő kritikus célpontok, hálózatok, rendszerek elleni indirekt támadással – lehet végrehajtani. Nem ritka a közvetlen és közvetett támadási eljárás, módszer kombinálása. Az információs műveletek a célpontok szövevényes összefüggése, több szintű rétegződése és mátrix jellegű hálózatos kapcsolódása következtében gyakran nem egyes célpontok ellen irányulnak. Ehelyett inkább az egész rendszert érintő és káros hatást kifejtő, háborús teljesítményt csökkentő, úgynevezett degradáló, deregulációs hatás elérését célzó eredményre törekszenek a hatás-alapú műveletek keretében.

Saját vonatkozásban az információs műveletek célkitűzéseinek másik oldala: védeni a saját vezetési és fegyverirányító rendszereket, központokat, összeköttetéseket, távközlési és logisztikai vonalakat, kritikus infrastruktúrákat.

Az információs műveletek különböző, elkülönülten is létező, komplex információs tevékenységek közötti **integráló és koordináló tevékenységek**, melyek szükségességét és létjogosultságát az összehangolt információs tevékenységek nagyságrendekkel növelhető hatékonysága adja. Az információs műveletek egymással összhangba hozott széles tevékenységi területen, számos külön-külön is alkalmazható információs vagy információ alapú tevékenység révén érvényesülnek. Hatékony alkalmazásuk békeidőben elkerülhetővé teheti a pusztító katonai tevékenységet.

Az információs műveletekkel olyan újfajta eljárások jelennek meg a hadművészetben, amelyek ugyanarra a célra irányulnak, mint a hagyományos hadviselés, azonban módszerei, eszközei és tárgyai az esetek többségében jelentős mértékben eltérnek attól. Míg a hagyományos elveket tükröző hadművészet alapvetően az ellenség tűzzel való pusztítására irányul, addig az információs műveletek elsősorban az ellenség vezetési és információs rendszereinek felderítésére, támadására, illetve a saját hasonló rendszerek alkalmazására és védelmére törekszik, a maga sajátos eszközrendszerével és módszereivel.

Az ellenség harcoló csapatainak pusztítása nélkül háborús körülmények között nem érhető el tartós siker. Az információs műveletek alkalmazása azonban lényegesen kevesebb erőforrás bevonásával és a veszteségek jelentős mérséklésével lehetővé teszi a győzelem kivívását.

A hagyományos hadviselési elvek szintén tartalmazzák az ellenség vezetési pontjainak pusztítását, a parancsnokságok és a harcoló csapatok közötti híradás és a fegyverirányítás zavarását. Mivel azonban e tevékenységek eddig többnyire önállóan – egymással nem összehangoltan – kerültek végrehajtásra, ezért azok csak kivételes esetekben voltak képesek döntő mértékben befolyást gyakorolni a harctevékenységek eredményességére. A gyakorlati tapasztalatok azt mutatják, hogy az esetek többségében a vezetési rendszerek támadása korábban csupán

megkönnyítette az ellenséges csapatok szétverését, de rendszerint nem vált a siker alapvető tényezőjévé. Az információs műveletek lényege éppen az, hogy **elemeinek integrált, összehangolt alkalmazása** döntő módon képes befolyásolni a fegyveres küzdelem kimenetelét, a katonai és politikai célok elérését. Ez minőségi változást jelent a korábbi helyzethez képest, amelynek a hadművészeti elvek változásában is érvényre kell jutnia [F.i. 3].

Az információs műveletek elemei és fajtái

Az információs műveletek erőfeszítéseit az alábbi **támadó és védelmi fajtájú tevékenységeken** keresztül valósítják meg:

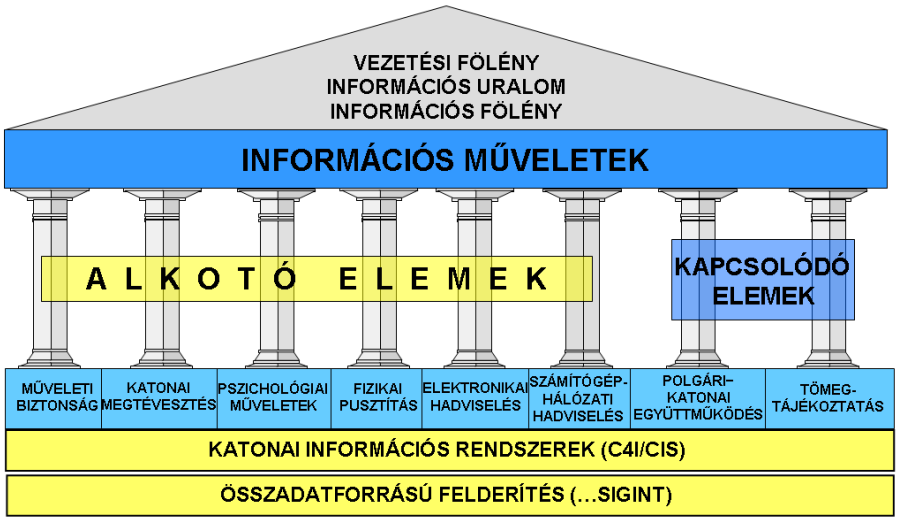
- az információs infrastruktúrák, vezetési objektumok fizikai pusztítása;
- a katonai megtévesztés;
- a műveleti biztonság;
- az elektronikai hadviselés;
- a pszichológiai műveletek;
- a számítógép-hálózati hadviselés.

E tevékenységek **alapvető alkotóelemei** az információs műveleteknek. Az alkotó elemeken kívül az ún. **kapcsolódó elemek**, mint a civil–katonai együttműködés (CIMIC) és a tömegtájékoztatás is hozzájárulnak az információs műveletek céljai eléréséhez [F.i. 3].

Mindezek mellett az információs műveletek hatékony végrehajtásához elengedhetetlen a hatékony és jól megszervezett **összadatforrású felderítés** és nem utolsósorban a korszerű információs technikára és technológiára alapozott saját **katonai információs rendszerek** megléte (3. ábra).

Az információs műveletek minden eleme egyaránt fontos szerepet játszik az információs fölény kivívásában, megtartásában, majd vezetési fölénnyé és hadműveleti fölénnyé való konvertálásában. Az információs műveletek erősokszorozó szerepe éppen abban áll, hogy az elemek együttesen, koordináltan, egymással együttműködve, egymás hatásait kihasználva, szinergikusan kerülnek alkalmazásra. Ez jóval nagyobb hatásfokot eredményez, mintha az információs műveletek elemei önállóan, koordinálatlanul lennének végrehajtva. Az információs műveletek elemeinek koordinálása a tervező, szervező és irányító törzsektől és a végrehajtó erőktől nagyfokú összehangoltságot követel meg.

Az információs műveletek elemei között szoros kapcsolatok és összefüggések állnak fenn. Az egyes elemek a végrehajtás szintjén egymást érintik, átfedik, és hatással vannak egymásra, miközben nem veszítik el önállóságukat.



3. ábra. Az információs műveletek elemei

A különböző fajtájú információs műveletek a fenti képességek alkalmazásával nagymértékben lehetővé teszik a hagyományosnak tekinthető erők és eszközök gazdaságos felhasználását. Ez azt jelenti, hogy a különböző koordinált információs tevékenységekkel kivívott információs fölény adott esetben kevesebb repülőgép, tüzérségi eszköz, harckocsi, légvédelmi eszköz stb. bevetését teszi szükségessé. Mindez annak köszönhető, hogy egyrészt a saját, korszerű integrált információs rendszerünk képességei – az alkalmazott védelmi fajtájú információs műveletek és a pontos összadatforrású felderítés következtében – maximálisan kihasználhatók, a saját vezetési ciklusunk ideje jelentősen lerövidül; másrészt a szemben álló fél hasonló rendszereinek – az alkalmazott támadó fajtájú információs műveletek következményeként – működése leromlik, vezetési ciklusuk ideje jelentősen megnövekszik. Ebben a helyzetben a szemben álló fél képtelen megfelelően irányítani alárendeltjeit, pontosan meghatározni számukra a harcfeladatokat, tehát a vezetési folyamatban káosz jelentkezik, bekövetkezik a „vezetetlenség” állapota. Így a szemben álló fél tűzeszközeinek alkalmazása kaotikussá válik, esetleg azok a teljes használhatatlanság állapotába kerülnek [F.i. 3].

AZ ÖSSZADATFORRÁSÚ FELDERÍTÉS ÉS A SIGINT

A felderítés egyidős a háborúval. Az egymással szemben álló felek mindenkor törekedtek arra, hogy a legtöbb és leghitelesebb információt gyűjtsék be a másik fél erejéről, várható tevékenységéről. Napjainkban e célra a legkülönfélébb módszereket és technikai eszközöket használják fel, amelyek jelentősen megnövelik, megsokszorozzák az emberi érzékelés határait. A felderítés céljára alkalmazott technikai eszközök képesek a teljes frekvenciaspektrumban adatokat gyűjteni, azokat akár automatikusan is a fúziós technológián alapuló adatfeldolgozó központokba továbbítani, ahol értékes felderítési információkat nyerhetünk belőlük [F.i. 5].

Az összadatforrású felderítés elve

A felderítés olyan harci támogató tevékenység, amelyet információk megszerzése érdekében különböző aktív módszerekkel folytatnak az ellenség (potenciális ellenség) tevékenységeinek, képességeinek és erőforrásainak, valamint a hadműveleti terület egy meghatározott részére vonatkozó, jellemző időjárási, földrajzi és vízrajzi viszonyainak megállapítása érdekében. Célja, hogy időben, megbízható adatokat szolgáltasson az ellenségről (a lehetséges ellenségről), az adott terület katonaföldrajzi viszonyairól, valamint az időjárásról, a politikai vezetés és a parancsnokok számára a műveletek tervezéshez és vezetéséhez, békében, válság időszakában és háborúban egyaránt [F.i. 4]. Más szavakkal megfogalmazva, a felderítés a **ki (mi), mikor, hol, mit tevékenykedik** kérdésre keresi a választ abból a célból, hogy **következtetni** tudjon a szemben álló fél **szándékára**.

A szenzorok által megszerzett adatok mennyisége egy fejlett, integrált és komplex felderítő rendszer esetén elérheti az óránkénti 1200 felderítő jelentést is. Minden részinformációra a parancsnoknak nincs szüksége, nem is tudja azokat időben feldolgozni, és a túl sok információ esetében fennáll az **információs túlterhelés** veszélye. Annak elkerülése érdekében az említett óriási adathalmazt gépi úton kell – illetve lehet – szétválogatni, csoportosítani, rendezni, adott célpontra és változásra vonatkoztatva összegyűjteni és értékelni.

Az információs műveleteknek igen jelentős a célinformáció-igénye. Ezeket egyrészt az általános felderítő tevékenység során megszerzett és értékelt **felderítési információk** biztosítják, másrészt ún. speciális felderítő tevékenység (például elektronikai támogató tevékenység) szolgáltatja a rövid érvényességű, gyorsan – nem részletesen – értékelt ún. **harci információk** formájában.

A felderítési információk az ellenségről rendelkezésre álló valamennyi adat részletes feldolgozásának eredményeként jönnek létre, amelyek az ellenség összetételére, felépítésére, szándékára, elhelyezkedésére, mozgásának irányára és sebességére, valamint harci készenlétére vonatkoznak. A felderítő információkat a felderítő nyers adatok megszerzésével, begyűjtésével, osztályozásával, kiegészítésével, elemzésével és gondos értékelésével, vagyis részletes felderítő mélyértékelés útján nyerjük. A felderítő információk előállításához bizonyos idő kell. Az automatizált adatfeldolgozó központok ezt a folyamatot jelentősen felgyorsítják. A gyors adatfeldolgozás, az időben történő jelentés és az értékelt felderítési információk gyors eljuttatása a felhasználóhoz igen fontos a csapatok közvetlen harcérintkezésben vívott harcának tervezése, irányítása és támogatása szempontjából.

A harci információk gyors értékelésű felderítési adatok, amelyeket a harcoló csapatok és a különböző adatszerző eszközök gyűjtenek, és különösebb további feldolgozás nélkül, azonnal és közvetlenül felhasználhatók a célok megsemmisítéséhez, vagy az elektronikai hadviseléshez. Az ilyen típusú harci információk a gyorsan elavuló jellegük, vagy a helyzetre gyakorolt kritikus hatásuk miatt azonnali válaszintézkedéseket követelnek, ugyanakkor a harci információkból – amennyiben azok részletes mélyértékelésre, tehát további feldolgozásra kerülnek – előállíthatók felderítési információk.

A sikeres információs műveletek folytatásához nélkülözhetetlen a katonai felderítés legújabb eljárásának, az **összadatforrású felderítésnek** az alkalmazása. A katonai műveletekhez – benne az információs műveletekhez is szükséges általános és szakirányú felderítési adatokat és információkat egy komplex, ún. fúziós elven működő automatizált felderítő rendszer képes szolgáltatni. Ez a rendszer lehetővé teszi, hogy az egyes célobjektumokra és a lényegi változásokra vonatkozó különböző paraméterű, időpontú, formájú adatokat és információkat összegyűjtsék, feldolgozzák, használható formátumra átalakítsák és az illetékesek számára eljuttassák, hogy azokat a döntést támogató parancsnoki munka során időben felhasználják.

Az összadatforrású felderítés különböző fajtájú önálló felderítő rendszereket, valamint változást érzékelő adatgyűjtő szenzorrendszereket integrál magába. Feladata, hogy az ellenségről és a hadszíntéri környezet változásairól minden lényeges és fontos adatot, információt időben összegyűjtsön, és az illetékesek számára átadja. Az összadatforrású felderítő rendszer tehát fontos információ-átalakítási műveletet végez, vagyis a nyers adatokból és a nyers információkból felhasználható információkat hoz létre. Működése azon az elven alapszik, hogy a különböző felderítő és adatgyűjtő rendszerektől folyamatosan érkező részadatokat, paramétereket idő, hely és fontosság szerint rendezi, adott célobjektumokra összegyűjti. Ezt a folyamatot **adatfúziónak** nevezik [F.i. 3].

A rádióelektronikai felderítés

Az összadatforrású felderítés minden felderítési fajtát integrál, így a **rádióelektronikai felderítés**, vagyis a **SIGINT** is annak szerves részét képezi. A SIGINT passzív eszközökkel az elektromágneses kisugárzások összegyűjtéséből, értékeléséből, analizálásából, feldolgozásából szerzi információit. A SIGINT tevékenység is, mint minden más felderítő tevékenység, felderítési információt állít elő.

A SIGINT fő feladatai az alábbiakban foglalható össze:

- felfedés;
- az elektromágneses kisugárzások irányának és helyének meghatározása;
- lehallgatás, adatok rögzítése, továbbítása;
- a kisugárzott jelek technikai paramétereinek elemzése;
- adatelőkészítés, előértékelés;
- adatfeldolgozás;
- a jelentések továbbítása.

Mindezeknek a feladatoknak megfelelően, a SIGINT eszközeinek a következő követelményeket kell kielégíteniük:

- gyors és hatékony alkalmazkodás a változó elektromágneses környezethez;

- a modern és hagyományos, egyszerű és összetett jelek vételének képessége;
- a kis valószínűséggel felderíthető (LPI) kisugárzások felfedése és irányának meghatározása;
- valós idejű jelfeldolgozás;
- könnyű kezelhetőség és fenntarthatóság;
- interoperabilitás más eszközökkel és rendszerekkel;
- a fejlesztés lehetősége [F.i. 6].

AZ ELEKTRONIKAI HADVISELÉS

Az elektronikai hadviselés fogalma, értelmezése

Az elektronikai hadviselés azon katonai tevékenység, amely az elektromágneses energiát felhasználva meghatározza, felderíti, csökkenti, vagy megakadályozza az elektromágneses spektrum ellenség részéről történő használatát, és biztosítja annak a saját csapatok általi hatékony alkalmazást [F.i. 4; 7]. Az elektronikai hadviselés a harcképességet jelentősen befolyásoló tényező. Fontossága abból adódik, hogy feltárja az ellenség gyenge pontjait, védi a saját cselekvési szabadságot, növeli a katonai információs rendszerek biztonságát és csökkenti a sebezhetőségüket.

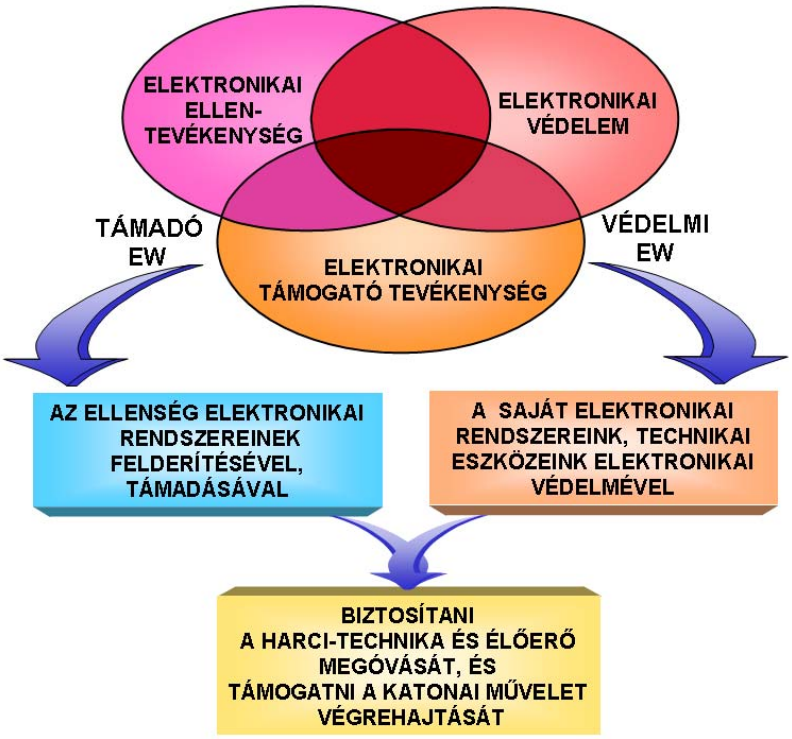
Az elektronikai hadviselés szerves része mindenfajta katonai műveletnek és egyike az információs műveletek elemeinek. Az elektronikai hadviselés elősegíti az értékelő és döntéshozó folyamatot, hozzájárul a szervezéshez és a hadműveleti irányításhoz, óvja a csapatokat az ellenséges tevékenységektől, és biztosítja az elektronikai eszközeink működését a saját csapatok kisugárzó eszközeinek nem szándékos elektromágneses interferenciái mellett is.

Az elektronikai hadviselés az alábbi három, egymást kiegészítő területre osztható:

- az elektronikai támogató tevékenységre;
- az elektronikai ellentevékenységre és
- az elektronikai védelemre [F.i. 4; 7; 8] (4. ábra).

Az elektronikai hadviselés egy olyan kétoldalú tevékenység, aminek alapvető célja az ellenség katonai információs rendszereinek elektronikai úton való támadása, illetve a saját hasonló rendszerek működésének biztosítása, az élőerő és a csapatok megóvása. Eszerint az elektronikai hadviselésnek van egy **támadó** és egy **védelmi** oldala.

A **támadó oldal** az elektronikai hadviselés olyan alkalmazását jelenti, amely lehetetlenné teszi, akadályozza, vagy korlátozza az ellenség elektronikai eszközeinek hatékony alkalmazását. Ide tartozik az elektronikai ellentevékenység és az e tevékenység számára célinformációkat biztosító elektronikai támogató tevékenység.



4. ábra: Az elektronikai hadviselés célja és területei [F.i. 1]

Az **elektronikai hadviselés védelmi oldalához** tartoznak azok a tevékenységek és rendszabályok, melyek elősegítik az elektromágneses spektrum hatékony felhasználását. Mivel a parancsnokok a harc, hadművelet során nagymértékben alapoznak a vezetést és fegyverirányítást kiszolgáló elektromágneses kisugárzó eszközökre, ezért a védelmi célú elektronikai hadviselés elsődleges feladata védeni ezen eszközöket a felderítés, helymeghatározás, azonosítás és az elektronikai úton végrehajtott támadások ellen. Ugyanakkor a saját elektronikai eszközökre jelentős hatással lehetnek a saját csapataink által véletlenül, vagy akaratukon kívül generált nem szándékos zavarok is, amelyek kiküszöbölése szintén a védelmi oldal feladata.

Az elektromágneses spektrum általunk történő felhasználásának biztosításában az elektronikai hadviselés mindhárom területe részt vesz. Az elektronikai hadviselést – mint a frekvenciaspektrum feletti részleges vagy teljes uralom megszerzésének alapvető módszerét, tevékenységét és eszközét –, illetve annak egyes területeit az elektronikai hadviselés szakcsapatok végzik, más feladatait viszont a haderőnemek, fegyvernemek és szakcsapatok hajtják végre. Az elektronikai hadviselés **aktív** – érzékelhető –, és **passzív** – rejtett, nem érzékelhető – tevékenységeket foglal magában.

Az elektronikai támogatás passzív, az elektronikai ellentevékenység és az elektronikai védelem pedig mind aktív, mind passzív tevékenység lehet.

Az elektronikai támogató tevékenység

Az elektronikai támogató tevékenység az elektronikai hadviselés azon része, amely magába foglalja – a fenyegetés azonnali jelzése érdekében – az elektromágneses kisugárzások felkutatására, elfogására, és azonosítására, valamint a források helyének meghatározására irányuló tevékenységeket [F.i. 4; 7; 8].

Az elektronikai támogatás minden időben folytatott tevékenység, így béke, válság és háború esetén egyaránt alkalmazható. A békeidős alkalmazás alapvetően az elektronikai hadviselés hadműveleti adatbázisának feltöltésére irányul. A legtöbb elektronikai támogató tevékenység – hadműveleti és harcászati szinten, napszaktól és időjárástól függetlenül – hozzájárul a nagy hatótávolságú információgyűjtő rendszerek működéséhez. Az elektronikai támogatás saját vezetési rendszerét kivéve passzív tevékenység.

Az elektronikai támogatás feladatai**:**

- a kisugárzott elektromágneses energiaforrások kutatása, befogása, azonosítása és helyének meghatározása;
- a fenyegetések, veszélyhelyzetek felismerése, azonosítása;
- az elektronikai támadó és védelmi tevékenységek célinformációval való támogatása;
- a parancsnok és a törzs harci információval való támogatása.

Az elektronikai támogatás által gyűjtött **harci információkat** elsősorban a **közvetlen fenyegetés azonnali felismerésére**, illetve **célmegjelölésre** alkalmazzák, ezenkívül természetesen hozzájárulhat az összfegyvernemi (összhaderőnemi) parancsnokság felderítő adatgyűjtéséhez is.

Az elektronikai támogatás **fenyegetést jelző funkciója** azt jelenti, hogy speciális elektronikai eszközök érzékelik a tér különböző irányaiból érkező elektromágneses hullámokat. Értékelik azokat, s döntenek arról, hogy milyen típusú fenyegetés érte az oltalmazott objektumot, és az eredményről jelzést küldenek a kezelőknek, valamint az önvédelmi rendszert vezérlő automatika felé. E funkcióra jó példa a repülőgépek önvédelmi elektronikai rendszereinek fenyegetettség jelző alrendszere, amely képes a repülőgép ellen indított radar-, infra-, lézer- stb. vezérlésű rakéták közeledését érzékelni, kijelezni, riasztani, és automatikus működés esetén az elhárító eszközöket (radarzavaró, infracsapda stb.) működésbe hozni. Az elektronikai támogatást, az eszközök és földi létesítmények önvédelme érdekében együtt alkalmazzák más szenzorokkal és az ellentevékenységi rendszerekkel. Ez különösen igaz a repülőterekre, a kommunikációs és logisztikai központokra, a hajókra, repülőgépekre és helikopterekre valamint a földi erők harcjárműveire, újabban pedig a földi és légi robotokra is.

Az elektronikai támogatás **célmegjelölő funkciója** azt jelenti, hogy az iránymérő eszközei elegendő pontossággal rendelkezhetnek ahhoz, hogy a modern irányított, vagy hagyományos fegyverek alkalmazásához célmegjelölési adatokat biztosítsanak. Ahol ez nem lehetséges – például a földi közvetett irányzású fegyvereknél –, az iránymérési pontosság gyakran elegendő más felderítő, megfigyelő és célmegjelölő rendszerek tájékoztatására. Az elektronikai támogatás ezenkívül célmegjelölést biztosít az elektronikai ellentevékenység részére is. A hatékony zavarás kiváltásához elengedhetetlenek azok az elektronikus céladatok (frekvencia, üzemmód, sávszélesség, impulzus-paraméterek stb.), melyeket az elektronikai támogató rendszerek nyújtanak az elektronikai zavaró eszközök számára [F.i. 3].

Az elektronikai ellentevékenység

Az elektronikai ellentevékenység az elektronikai hadviselés azon területe, amely magába foglalja az elektromágneses és irányított energiák kisugárzását abból a célból, hogy megakadályozza vagy csökkentse az elektromágneses spektrum ellenség által való hatékony használatát [F.i. 4; 7; 8].

Az elektronikai ellentevékenységnek három területe van:

- az elektronikai zavarás;
- az elektronikai pusztítás; és
- az elektronikai megtévesztés.

Az elektronikai ellentevékenység az elektronikai hadviselés **támadó fegyvere**, ami abban nyilvánul meg, hogy minden olyan technikát, módszert és eszközt felhasznál, ami az elektromágneses és más irányított energiák alkalmazásával képes működésképtelenné tenni az ellenséges elektronikai eszközöket. Ugyanakkor egyes elektronikai ellentevékenységi módszerek alkalmasak védelmi természetű funkciók ellátására is. Az elektronikai ellentevékenység erőket és eszközöket oltalmazó módszerei komoly mértékben képesek csökkenteni az ellenség célfelderítésének, valamint a fegyverek felderítő és irányító rendszerének hatékonyságát, ezáltal hozzájárulnak a csapatok túlélőképességének növeléséhez.

Az új technológiák megjelenésével az elektronikai ellentevékenység túlmutat a tradicionális zavaráson és megtévesztésen. Az **irányított energiájú fegyverek** új rongáló és pusztító dimenziót jelentenek az elektronikai harctéren, megkövetelve azok körültekintő alkalmazását. Manapság az elektronikai hadviselés eszköztárában nagy számban jelennek meg az elektromágneses impulzus fegyverek, a mikrohullámú, lézer és infrazavaró berendezések, illetve a navigációs műholdakat zavaró eszközök.

Az elektronikai védelem

Az elektronikai védelem az elektronikai hadviselés azon területe, ami biztosítja az elektromágneses és egyéb fizikai tartományok saját részről történő hatékony használatát az ellenség elektronikai támogató és ellentevékenysége, valamint a saját csapatok nem szándékos elektromágneses interferenciái ellenére [F.i. 4; 7; 8].

Az elektronikai védelem lehetetlenné teszi, vagy csökkenti az ellenség frekvenciaspektrum feletti fölény megszerzésére irányuló törekvéseit. Az elektronikai védelmi tevékenységek védelmi természetűek és többet jelentenek, mint az elektronikai rendszerekbe tervezett és beépített technikai lehetőségek összessége.

Az elektronikai védelem megvalósítása parancsnoki felelősség is, mely a következőket jelenti:

- a passzív és aktív rendszabályok meghatározását az elektronikai eszközök és rendszerek számára, valamint – a csapatok és a harci-technikai eszközök alkalmazási elveivel összhangban – e rendszabályok bevezetésére vonatkozó irányelvek meghatározását;
- a kiképzésen keresztül magas fokú jártasság kifejlesztését, ami biztosítja a csapatok és technikai eszközök harcászati követelményeknek megfelelő alkalmazását az ellenséges elektronikai hadviselési környezetben.

Az elektronikai védelem **a felderítés és az elektronikai ellentevékenység** – ezen belül a saját, nem szándékos interferenciák – megakadályozására irányuló **aktív és passzív** tevékenységek, módszerek és rendszabályok alkalmazását, bevezetését jelenti.

A passzív elektronikai védelem olyan rendszabályok alkalmazását jelenti – úgy, mint a technikai eszközök üzemmódjaival, működési módjaival és technikai jellemzőivel való manőverezés –, amelyekkel biztosítható, hogy a saját csapatok akadálymentesen használják fel az elektromágneses és más spektrumot.

Az elektronikai védelem aktív rendszabályait – a frekvenciák, az adóberendezések paramétereinek megváltoztatását – az ellenség is érzékeli. Ezekkel a rendszabályokkal – spektrumkiterjesztés, periodikus vagy rendszertelen frekvenciaváltás, modulációs módok és a kimenő teljesítmény megváltoztatása stb. –, biztosítani lehet az elektromágneses és más fizikai spektrumtartományok saját csapatok által történő zavartalanabb felhasználását [F.i. 3].

AZ INFORMÁCIÓS MŰVELETEK, A SIGINT ÉS AZ ELEKTRONIKAI HADVISELÉS KÖZÖTTI ÖSSZEFÜGGÉSEK

Az információs műveletek, a SIGINT és az elektronikai hadviselés szoros kapcsolatban állnak egymással, valamint magával a katonai műveletekkel. Ez a kapcsolat egyrészt adatok, célmegjelölési információk átadása formájában valósul meg, másrészt pedig azáltal, hogy az egyes területeken végzett tevékenységek hatásukban egy másik terület célkitűzéseinek elérését is szolgálják.

Az információs műveletek hatékony folytatásának elengedhetetlen feltétele a folyamatos, pontos, részletes és valós idejű információ megléte, amit az összadatforrású felderítés szolgáltat. A felderítő információk alapvető támogatást nyújtanak az információs műveletek számára azáltal, hogy biztosítják az ellenség vezetési rendszereinek elemzését, meghatározzák információs műveleti képességeit, valamint visszajelzést nyújtanak a saját végrehajtott feladatok eredményességéről.

A SIGINT az összadatforrású felderítés többi fajtájával együttműködve képes kielégíteni az információs műveletek általános és specifikus felderítési igényeit. Az **információs műveletek általános felderítő támogatása** azt jelenti, hogy a felderítés megszerzi azokat az általános felderítési információkat, amelyek az információs műveletek integrált és komplex vezetéséhez szükségesek. Az információs műveletek általános felderítő igényei magukban foglalják mindazon információk megszerzését az ellenségről és a harctéri környezetről, amelyek a parancsnok elgondolásán belül, az információs műveletek eredményes megvalósítását segítik elő. Az információs műveletek általános felderítési információinak megszerzése szinkronban van a katonai művelet általános felderítési adatainak megszerzésével.

Az **információs műveletek specifikus felderítő támogatása** azt jelenti, hogy a felderítés megszerzi mindazon felderítő információkat és specifikus céladatokat, amelyek az információs műveleteket alkotó elemek, vagyis a műveleti biztonság, katonai megtévesztés, pszichológiai műveletek, elektronikai hadviselés, számítógép-hálózati hadviselés és a fizikai pusztítás, sikeres végrehajtásához szükségesek.

Az információs műveleteknek és azon belül az elektronikai hadviselésnek igen jelentős a célinformáció-igénye. Az információkat egyrészt az elektronikai támogató tevékenység szolgáltatja harci információk formájában, másrészt az általános felderítő tevékenységen belül a SIGINT során megszerzett és értékelt felderítési információk biztosítják az elektronikai helyzet adatbázis folyamatos karbantartását.

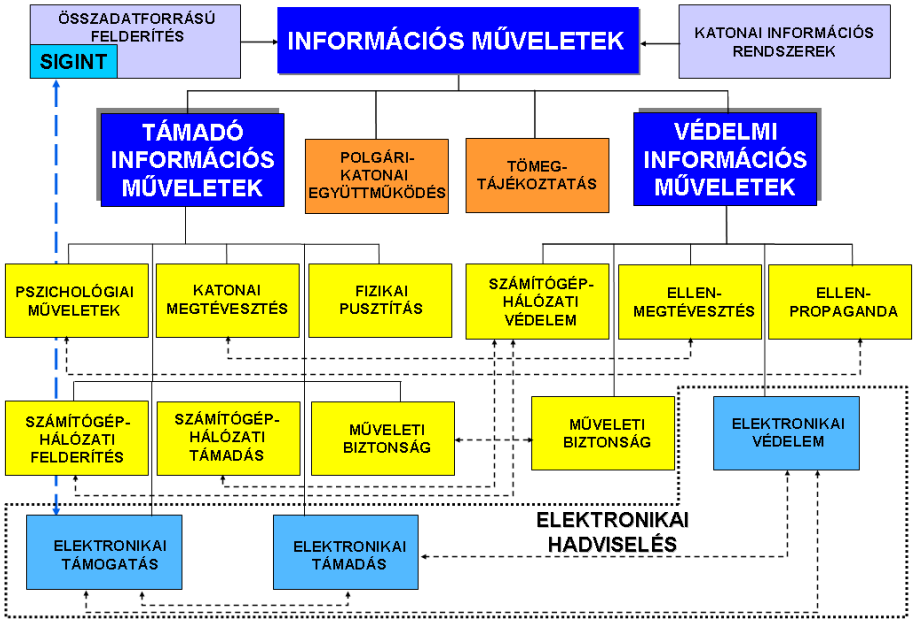
Az elektronikai támogató tevékenység – hasonlóan a SIGINT-hez – az ellenség által használt elektromágneses spektrumból nyeri információit, vagyis az elektromágneses és más tartományú kisugárzások jeleinek érzékelésével, azonosításával és azok felhasználásával kapcsolatos tevékenység. Az elektronikai támogatás fontos információkkal szolgál arról, hogyan használja az ellenség a frekvenciaspektrumot, érzékeli, azonosítja és felhasználja az ellenség szándékos (például rádióadás) és a nem szándékos (például kipufogógázok infravörös hullámtartományú) kisugárzásait.

Az elektronikai támogató tevékenységnek gyakorlatilag azonosak a feladatai a SIGINT-tel, de feladatait a közvetlen harcoló parancsnok követelményei alapján végzi. Az alapvető különbséget a két tevékenység között az határozza meg, hogy a megszerzett információt mire használják. Az elektronikai támogatás **harci információkat** szolgáltat, amelyeket fel lehet használni elektronikai ellentevékenységhez, tüzérségi tűz-, vagy repülőcsapások kiváltásához, a csapatok manőveréhez, vagy a veszély elhárításához. Mindezt a vett információ gyors analizálása és feldolgozása, valamint viszonylagosan rövid érvényességi ideje jellemzi. A SIGINT ugyanakkor **felderítési információkat** továbbít az összfegyvernemi törzs felé a parancsnoki döntéstámogatás céljából [F.i. 3].

A hatékony tűztámogatáshoz szintén elengedhetetlenek a pontos célmegjelölési adatok, melyeknek struktúrája hasonló az elektronikai hadviselési célinformációkhoz. Ennél fogva kézenfekvő, hogy az elektronikai hadviselés számára szükséges célinformációk biztosítása céljából egyrészt az elektronikai

támogatás harci információit beintegrálják az adatfúziós felderítő rendszerbe, másrészt ugyanezen rendszerből elérhetővé válnak számára a már előbb említett kiértékelt felderítési információk.

Az elektronikai hadviselés által szolgáltatott harci információkhoz, illetve a SIGINT felderítési információihoz ugyanazon adatszerző eszközökkel lehet jutni. Közöttük az alapvető különbség a feldolgozás mélységében, és az információk érvényességi idejében van (5. ábra).



5. ábra. Az információs műveletek, a SIGINT és az elektronikai hadviselés kapcsolata

Az elektronikai támogatásnak és a SIGINT-nek fel kell használnia az információs kor technikai vívmányait ahhoz, hogy feladatukat el tudják látni, illetve, hogy követni tudják a kommunikációs vagy akár a radartechnikában bevezetett és ma már általánossá vált, forradalmian új technikai eszközöket és eljárásokat.

A teljesség igénye nélkül néhány kihívás, amely óriási feladat elé állítja mind az elektronikai támogatást, mind pedig a SIGINT tevékenységet:

- megjelentek a kis valószínűsséggel felderíthető adásmódok (LPI), amelyek további térnyerése várható;
- a kriptográfia és az elektronikus kriptográfia óriási fejlődésen ment keresztül az elmúlt ötven év során, amely gyakorlatilag már ma is rendkívül nehézzé teszi az elfogott, titkosított elektronikus adások információtartalmának kinyerését;

- egyre szélesebb körben jelennek meg a frekvenciaugratásos, vagy a kiterjesztett spektrumú kommunikációs rendszerek, ami szintén az információtartalomhoz való hozzáférést teszi lehetetlenné;
- a radartechnika szintén jelentős fejlődésen ment keresztül, amely – a teljesség igénye nélkül –, a CHIRP vagy a szekunder-radarrendszerekben követhető a leginkább nyomon;
- az elfogott elektromágneses jel kisugárzási helyének megállapítása, vagyis az iránymérés, a frekvenciaugratásos, illetve kiterjesztett spektrumú adások esetén igen nehéz [F.i. 9].

Ezek a kihívások – amelyek mind a SIGINT, mind pedig az elektronikai támogatás területén egyaránt jelentkeznek –, azt eredményezik, hogy a rádió-elektronikai felderítés, és azon belül különösen a rádiófelderítés (COMINT) korábban alkalmazott módszerei egyre kevésbé használhatók. Napjaink korszerű felderítő eszközei alapvetően csak ezen digitális adások (DSSS, FHSS) jeleinek detektálására, illetve irányának és helyének meghatározására képesek.

A nagy sebességű (paramétereit gyorsan változtató) adások vételére napjainkban úgynevezett keresés nélküli vevőket alkalmaznak, amelyek egyidőben dolgozzák fel a teljes sávot. Ilyenek a mátrixvevők elvén felépített, digitális szűrőbank-vevők és a Bragg-cellás vevők. Az utóbbi években a gyors adások, a frekvenciaugratásos kisugárzások megfigyelése céljából egy egészen más típusú megjelenítő eszközt dolgoztak ki, a vízesés típusú displayt, amely frekvencia–idő rendszerben mutatja a vett jeleket.

A korszerű adásmódok felderítésekor azonban ezen eszközök és eljárások egyike sem (vagy csak nagyon kis valószínűséggel) alkalmas a rádióforgalom lehallgatására, és így az információ tartalmának rögzítésére. Ez annál is inkább igaz, mivel az átvitt információ eleve digitális formában, általában további adatvédelmi kódolással van ellátva. Ez a dekódolási feladat speciális apparátust, a legmodernebb technológiát és óriási számítási kapacitást igényel, ami a harcászati és hadműveleti szintű COMINT tevékenységnél nem alkalmazható [F.i. 5].

Ebből következően a rádiófelderítés számára sem az információtartalom, hanem az adók által hagyott „elektromágneses ujjlenyomat” lesz az elsődleges azonosító jellemző. Ez azt is jelenti, hogy a COMINT, mint tevékenységi forma ELINT típusúvá válik, vagyis csak a vett jelek paramétereit és a kisugárzás helyét képes meghatározni. Mivel az információtartalom megfejtésére nincs lehetőség, ezért a rádióforgalom további lehallgatása is értelmetlenné válik. Ehelyett az így felderített elektronikai objektumokkal szemben ellentevékenységet kell folytatni. Ha ezzel párhuzamosan megnézzük az elektronikai támogatás funkcióit, akkor azt látjuk, hogy ott is csak a vett jelek paramétereinek elemzése a cél, a fenyegetés jelzése vagy a célmegjelölés érdekében. Tehát harcászati és hadműveleti szinten a SIGINT és az elektronikai támogatás közötti különbség eltűnik.

A fenti megfontolások alapján a korszerű haderőkben harcászati és hadműveleti szinten az információs igények kielégítése céljából, valamint a párhuzamos tevékenységek kiküszöbölése érdekében a SIGINT tevékenységet, az elektronikai hadviselést és a célok meghatározását azonos elvek és egységes vezetés alapján, ún. **integrált felderítő és elektronikai hadviselés** struktúrában hajtják végre.

Az integrált felderítés és elektronikai hadviselés feladatok négy fő terület köré csoportosíthatók, úgymint:

- a helyzetértékelés;
- a célpontok meghatározása;
- az ellenséges felderítés elhárítása;
- az elektronikai hadviselés.

Mind a négy feladat jól körülhatárolható, önállóan is végrehajtható, azonban egymáshoz való viszonyuk, az adatok felhasználhatósága, illetve a több feladatra alkalmazható eszközök miatt ezek **egységes tervezése, szervezése és irányítása** szükségszerű.

Az elektronikai hadviselés sikeres végrehajtása érdekében felderítést kell folytatni és e tevékenység során maga is szerez adatokat. Hasonló sajátosságokkal rendelkezik a manőver és a tűztámogató tevékenység is. Az elektronikai hadviselés akkor a leghatékonyabb, ha integrálják, illetve együttesen alkalmazzák a tűzcsapásokkal és a manőverekkel. Az említett integrált alkalmazás tervezése során olyan felderítési információkra is szükség van, amelyek lehetővé teszik a parancsnok rendelkezésére álló tevékenységi formák eredményességének összevetését.

A SIGINT biztosítja az ellenség **elektronikai harcrendjének** felvázolását, elemzését és megértését. Az elektronikai harcrend ismerete alapvetően fontos az információs műveletek – azon belül különösen az elektronikai hadviselés – megvívásához, hiszen az információs infrastruktúrák döntő hányada nagy mennyiségben különböző típusú és fajtájú elektronikai eszközökből áll. Az erre vonatkozó információk tájékoztatnak a kommunikációs és a nem kommunikációs jellegű eszközök paramétereiről, az adók típusáról és rendeltetéséről, modulációjáról, csatornaképzési lehetőségeiről, impulzus-időtartamáról, impulzusismétlődési frekvenciájáról, sávszélességéről, a hozzá kapcsolódó fegyverrendszerekről, és az elektromágneses sugárzás egyéb jellemző adatairól. Ezek az adatok elősegítik az ellenség elektronikai harcrendjének modellezését.

A technikai adatok ismeretében pontosabban fel lehet mérni:

- az ellenség elektronikai rendszereinek az elektronikai ellentevékenységgel és a megtévesztéssel szembeni sebezhetőségét;
- könnyebben végrehajtható az eszközök figyelése és iránymérése az elektronikai felderítés eredményes végrehajtása érdekében;
- az ellenség elektronikai hadviselési képességeire vonatkozó adatokkal támogatni lehet a saját csapatok elektronikai védelmi feladatainak végrehajtását [F.i. 3].

Az integrált felderítő és elektronikai hadviselési erők és eszközök részét képezik az összfegyvernemi köteléknek. Feladatuk, hogy olyan pontos, időszerű és hatékony felderítési, ellenséges felderítés elhárítási adatokat és elektronikai hadviselési támogatást nyújtsanak a parancsnoknak, amelyek a sikeres harctevékenység megtervezéséhez, irányításához és végrehajtásához szükségesek. Az integrált felderítő és elektronikai hadviselési rendszerbe ténylegesen beletartozik minden szinten az összes olyan eszköz, részleg, és szervezet, amely alkalmas információk gyűjtésére és feldolgozására, a felderítési adatok elosztására, az ellenséges felderítés elhárítására, valamint az elektronikai hadviselés irányítására és végrehajtására. Az egyes szinteken meglévő integrált felderítő és elektronikai hadviselési eszközök szoros kapcsolatban vannak más, magasabb és alacsonyabb vezetési szinteken, és így egységes, integrált és összefüggő felderítő és elektronikai hadviselési struktúrát alkotnak.

ÖSSZEGZÉS

Az elektronikai hadviselés és a SIGINT alapvető fontosságú az információs műveletek sikeres megvívásához. A SIGINT információi alapján felvázolható a szemben álló fél elektronikai harcrendje, és hatékonyan lehet vezetni és végrehajtani az információs műveleteket. Az ellenség elektronikai harcrendjének modellezése alapján sikeres elektronikai ellentevékenységet lehet folytatni a másik fél elektronikai rendszerei és objektumai ellen, illetve hatékonyan lehet védeni a saját hasonló rendszereinket.

A korszerű, képesség-alapú haderő kialakításának alapvető feltétele az információs képességek kialakítása, továbbá az információs fölény megszerzésére, fenntartására való törekvés. Ezért a korszerű haderőkben – harcászati és hadműveleti szinten – az információs igények kielégítése céljából, a SIGINT és az elektronikai hadviselés összehangolt alkalmazása érdekében integrált felderítő és elektronikai hadviselési rendszereket alakítanak ki. A Prágai Képességvállalások keretén belül Magyarország is képesség alapú haderő kialakítását célozta meg, és hitet tett az információs fölény biztosítása mellett [F.i. 10]. Ez azonban csak korszerű elektronikai felderítő és elektronikai hadviselési eszközök és szervezetek kialakításával valósítható meg.

Tehát e képességeket nem megszüntetni, hanem erőteljesen fejleszteni kell!

FELHASZNÁLT IRODALOM

1) Haig Zsolt – Várhegyi István: *A vezetési hadviselés alapjai.* Egyetemi jegyzet. Budapest, 2000, ZMNE.

2) Várhegyi István – Makkay Imre: *Információs korszak, információs háború, biztonságkultúra.* Budapest, 2000, OMIKK.

3) Haig Zsolt–Várhegyi István: *Hadviselés az információs hadszíntéren.* Budapest, 2005, Zrínyi Kiadó.

4) *Magyar Honvédség Összhaderőnemi Doktrína.*
Honvédelmi Minisztérium Honvéd Vezérkar Hadműveleti Csoportfőnökség, Budapest, 2002.

5) Ványa László: *Az elektronikai hadviselés eszközeinek, rendszereinek és vezetésének korszerűsítése az új kihívások tükrében, különös tekintettel az elektronikai ellentevékenységre.*
Doktori PhD értekezés. Budapest, 2002, ZMNE.

6) Kovács László: *Az elektronikai felderítés korszerű eszközei, eljárásai és azok alkalmazhatósága a Magyar Honvédségben.*
Doktori PhD értekezés. Budapest, 2004, ZMNE.

7) *AJP–01 Allied Joint Operations Doctrine.*
September, 1999.

8) *Magyar Honvédség Elektronikai hadviselés doktrínája.*
Honvédelmi Minisztérium Honvéd Vezérkar Felderítő Csoportfőnökség. Budapest, 2005.

9) Kovács László: *Az elektronikai hadviselés helye és szerepe a jövő információs hadviselésében.*
Hadtudomány 2001/2. száma, Budapest. 33–40. o.

10) *Úton a XXI. század hadserege felé.*
http://www.honvedelem.hu/cikk.php?cikk=13776. (2003.08.12.)

DR. BARTOLITS ISTVÁN

A 21. SZÁZAD HÍRKÖZLÉSI TRENDJEI

A hírközlés fejlődési üteme az utóbbi évtizedekben felgyorsult. A technológiai fejlődés sorra hozza az újdonságokat, amelyeknek egy része ugyan hamar feledésbe merül, többsége azonban beépül a hírközlő hálózatokba, majd mindennapjaink részévé válik. Ebben a színes világban nem könnyű megjövendölni, mely technológiák lesznek a jövő nyertesei, illetve vesztesei. Kapaszkodót jelenthet azonban, ha megismerjük az általános trendeket, a fejlődés fő irányvonalait és azok várható következményeit a jövő kommunikációjának a fejlődésére vonatkozóan.

Előadásomban először a hírközlés múlt század végén azonosított hat megatrendjét mutatom be, amelyek az általános irányvonalat adják meg. Ezek után arról az öt jellemző trendről lesz szó, amelyek a közeljövőnket alakítják. Az öt trend közül különösen kettőnek, **a fejlett vezeték nélküli technológiáknak és a széles sávú platformoknak van meghatározó jelentősége** a konferencia szűkebb szakterülete számára, ezért ezekkel részletesebben is foglalkozunk.

A TÁVKÖZLÉS MEGATRENDJEI

A távközlés fejlődésének nagy, jellemző folyamatait – megatrendjeit – az 1990-es évek végén fogalmazták meg utoljára, s ezek a megatrendek mind a mai napig érvényben vannak. **Az azonosított hat megatrend** a következő:

- A globalitás.
- A regionális szövetségek megjelenése.
- A mobilitás.
- A konvergencia.
- A széles sávú infrastruktúra előretörése.
- A liberalizáció.

A következőkben ismerkedjünk meg a hat megatrenddel.

A globalitás

A globalitásnak, azaz a távközlési szolgáltatók illetve szolgáltatások globalizációjának számos jelét lehet tetten érni. Maguk a technológiák is a globalizálódást segítik, erre jó példa a kontinenseket összekapcsoló optikai kábelek megjelenése, vagy a műholdas rendszerek elterjedése. Ezek a technológiák lehetőséget adnak olyan transznacionális szolgáltatók kialakulására, amelyek világméretekben képesek szolgáltatásokat nyújtani, minden kontinensen jelen vannak. A technológiai adottság piaci kísérőjelensége a nemzetközi akvizíciók növekvő száma, szövetségek, fúziók létrejötte.

A regionális szövetségek megjelenése

A távközlésben a másik nagy, területi jellegű megatrend a regionális szövetségek megjelenése. Ezt a folyamatot két területen is nyomon követhetjük. Az egyik a regionális szabványosítás igénye. Mivel a szabványosításban igen erős gyártói érdekkörök működnek közre, nehéz a regionális érdekeknek érvényt szerezni összefogás, egységes fellépés nélkül. Ezen túlmenően pedig fontos a regionális szabványosítási szervezetek munkája is, mint például az európai ETSI (European Telecommunications Standards Institute) vagy az amerikai ANSI (American National Standards Institute). Előbbinek a munkájaként jött létre például az azóta már világméretekben sikeres GSM rendszer.

A regionális szövetségek megjelentek a szabályozás területén is, mivel hamar világossá vált, hogy a különböző országok nemzeti szabályozását célszerű valamilyen regionális rendező elvek szerint összehangolni. Erre jó példa az Európai Unió új szabályozási keretprogramja, az NRF (New Regulatory Framework).

A mobilitás

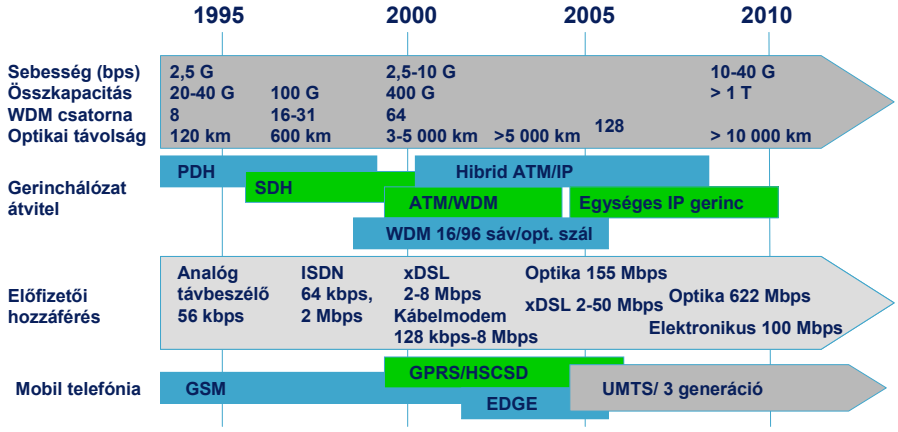
Magát a fogalmat nem is kellene magyarázni, azonban mégis érdemes megemlíteni, hogy a mobilitás itt kétféle értelemben értendő. Az egyik értelemben valóban arról van szó, hogy a vezeték nélküli, mobil eszközök terjedése alapvető trendként jelenik meg. Erre a korábbi analóg NMT és a digitális GSM rendszer mellett már a harmadik generációs mobilhálózatok jelentik az újabb példát. A mobilitás azonban egy másik értelemben, az internetcímmel rendelkező laptop számítógépek esetében is értelmezhető, ezt szokták nomaditásnak is nevezni és azt jelenti, hogy a számítógéppel tetszőleges hálózaton feljelentkezve az e-mailek, üzenetek stb. ugyanazon az internetcímen érnek el, mint az otthoni hálózatban. Ennek a fajta mobilitásnak tovább nő a jelentősége a VoIP-alapú beszédkapcsolatok elterjedésével.

A konvergencia

A konvergencia mint megatrend a legmeghatározóbb trend a hírközlés területén. A fogalom lényege, hogy a távközlés, az informatika és a média világa egyre inkább közeledik egymáshoz, szinte megkülönböztethetetlenül összefonódnak. A konvergencia jelensége szinte minden területen érezteti hatását, akár végberendezésekről, akár szolgáltatásokról beszélünk. Tipikus konvergenciatermék például az internetelérés mobiltelefonon keresztül, vagy a telefonként is használható PDA-eszközök (Personal Digital Assistent). A korai konvergencia jeleként értékelhetjük már azt is, hogy a távközlési eszközökben megjelentek a számítógép-vezérelt eszközök, de a konvergencia igazi kiteljesedésének most kezdünk a tanúi lenni. A konvergencia előbb a távközlés és a számítástechnika közeledésével indult meg, mára azonban már a média is integráns része a konvergenciának (erre jó példa az IPTV), sőt a szórakoztató elektronika is belépett ebbe a folyamatba (például Play Station 3).

A széles sávú infrastruktúra előretörése

Az ötödik megatrend a széles sávú kommunikáció elterjedése, általánossá válása. Természetesen, ha az Internetre gondolunk, akkor rögtön a konvergencia trendje is párosul ezzel a gondolattal, de ettől függetlenül is egy jellemző megatrend a sávszélesség növekedése, mind a vezetékes, mind a vezeték nélküli kommunikációban. A sávszélesség növekedési trendje egyaránt érvényesül a gerinchálózatok, illetve a végberendezéseket a hálózathoz kapcsoló hozzáférési hálózatok terén.



1. ábra. A sávszélesség fejlődése

A liberalizáció

A hatodik megatrend nem technológiai, hanem inkább távközléspoltikai tartalmat hordoz, azonban nagy hatása van a hálózatok és szolgáltatások fejlődésére. A távközlésben hosszú ideig az állami monopólium volt a jellemző, ami a történelmi hagyományokból fakadt a legtöbb esetben, a beruházásigényes hálózatépítést a távközlés korai szakaszában így lehetett a legjobban segíteni. Mára azonban a helyzet gyökeresen megváltozott, miközben a kialakult monopóliumok igyekeznek megtartani kényelmes piaci helyzetüket. Ennek a helyzetnek a megváltoztatása a hatodik megatrend a távközlés fejlődésében. Ehhez hozzátartozik a verseny serkentése, a regionális szabályozás (például EU-szabályozás) egységesítése, az állami tulajdon visszaszorulása.

AZ ITU ÖT MEGHATÁROZÓ TRENDJE

A fentiekben megismertük azt a hat megatrendet, amely hosszabb ideig – várhatóan évtizedekig – fogja a hírközlés fejlődését befolyásolni. Ugyanakkor a meghatározó trendek ennél gyorsabban változnak, a technológiai fejlődés, a piaci helyzet ennél gyorsabb változásokat kényszerít ki a fejlődés során.

Az ITU (International Telecommunications Union – Nemzetközi Távközlési Egyesület) 2004 végén éppen ezért úgy döntött, hogy meghatározza azokat a trendeket, amelyek a közeljövő fejlődésében alapvető szerepet játszanak, meghatározzák a fejlődés irányát. Ezek a trendek természetesen nem a megatrendek ellenére, hanem azok mellett – vagy ha jobban tetszik, azokkal együtt – érvényesülnek. A trendek meghatározását dr. Tim Kelly, az ITU Stratégiai és Távközléspolitikai Csoportjának a vezetője irányította, a munkában széles tanácsadói kör vett részt.

A jövőre vonatkozó öt trend – az ITU szerint – tehát a következő:

- A fejlett vezeték nélküli technológiák.
- A mindenütt jelen lévő kommunikáció.
- A széles sávú platformok elterjedése.
- Minden tartalom IP felett.
- Az információs társadalom kibontakozása.

A következőkben az öt trendet illetve a mögöttük húzódó technológiai vonulatot fogjuk kifejteni, elsősorban arra a két trendre koncentrálva, amelyek a konferencia fő témájának az irányába esnek. A másik három trendet éppen ezért csak nagyon tömören ismertetjük.

A fejlett, vezeték nélküli technológiák

A közeljövő egyik nagyon ígéretes trendje a vezeték nélküli technológiák elterjedése, a köznapi használatban való egyre intenzívebb felhasználás megjelenése. A vezeték nélküli technológiák egyaránt terjednek a nagy, országos lefedettséget nyújtó szolgáltatások terén, a kisebb, LAN (Local Area Network) jellegű alkalmazások terén, illetve a néhányszor tíz méteres hatótávolságú, helyi összeköttetéseket nyújtó alkalmazások terén. Ennek megfelelően megkülönböztethetünk nagy hatótávolságú, közepes hatótávolságú (néhányszor száz méter) és kis hatótávolságú (néhányszor tíz méter) vezeték nélküli technológiákat. A különböző megoldások fantázianevét, illetve szabványszámait a táblázat foglalja össze, de ezek közül is kiemelünk kettőt, az IEEE 802.11 szabványcsaládját, amelyet a Wi-Fi szövetség minősít, és ennek neve alapján a köznapi életben is Wi-Fi rendszernek nevezünk, illetve az IEEE 802.16 szabványcsaládot, amely a WiMAX összefoglaló néven ismert.

Nagy távolságú	Közepes távolságú (néhányszor 100 méter)	Kis távolságú (néhányszor 10 méter)
IMT-2000 (3G mobil) WiMAX (IEEE 802.16) W-WAN (IEEE 802.20) HiperMAN Satellite HAPS/LAPS LMDS MMDS WiBro	WLAN Wi-Fi (IEEE 802.11b) IEEE 802.11a IEEE 802.11g IEEE 802.11i HiperLAN2 Ultra Wideband	Bluetooth RFID ZigBee

A Wi-Fi rendszer

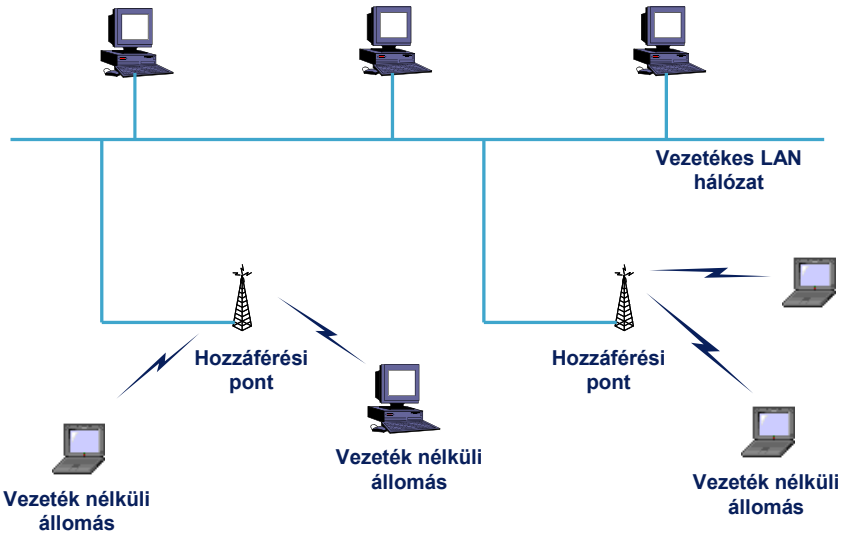
A széles sávú hozzáférés új, egyre jobban terjedő módja **a vezeték nélküli helyi hálózatok kiépítésén alapuló technológia**. A WLAN (Wireless Local Area Network – vezeték nélküli helyi hálózat) rendszerek lényege szintén egy cellás lefedettség, ahol a bázisállomások néhányszor száz méteres körzetében lehet kapcsolatba kerülni a hálózattal. A WLAN rendszereket elsődlegesen olyan helyen kezdték használni, ahol nagyon fontos volt, hogy nagy mennyiségű hordozható számítógép tudjon néhány órára vagy napra rákapcsolódni egy közös hálózatra. Tipikusan ilyen esemény egy konferencia vagy számítógépes tréning, de ugyancsak komoly érdeklődés mutatkozik a WLAN rendszerek használata iránt munkabizottsági üléseken, és újabban munkahelyi tárgyalásokon is. A legutóbbi időkben pedig megjelent a WLAN rendszerek nyilvános alkalmazása is. A gondolat abból a felismerésből született, hogy olyan helyeken, ahol üzletemberek, szakemberek vagy bármilyen módon laptophoz kötődő emberek nagy számban fordulnak meg és hosszabb ideig várakozni kénytelenek (például repülőterek, pályaudvarok, szállodák stb.), ott célszerű számukra biztosítani a hálózathoz kapcsolódást. A WLAN rendszerek nyilvános alkalmazásának ez volt a kiindulópontja.

A WLAN rendszerek alapjait jelentő egyik legfontosabb szabványcsaládot az IEEE (Institute of Electrical and Electronics Engineers) égisze alatt dolgozták ki a kilencvenes évek első felében. Az IEEE 802-es szabványosítási bizottsága már korábban sok helyi hálózati szabvány kidolgozásában vett részt, nevükhöz fűződik a 802.3 (Ethernet), a 802.5 (Token Ring) és a 802.3z (Fast Ethernet) szabvány is. Mivel a vezeték nélküli elérésre több technológia is alkalmasnak mutatkozott, olyan szabványt igyekeztek létrehozni, mely mindegyik megoldást magában foglalja. Hétéves munka után így született meg 1997-ben az IEEE 802.11, majd 1999-ben a továbbfejlesztett IEEE 802.11b szabvány. A mai napig ezen a szabványon alapulnak a WLAN rendszerek.

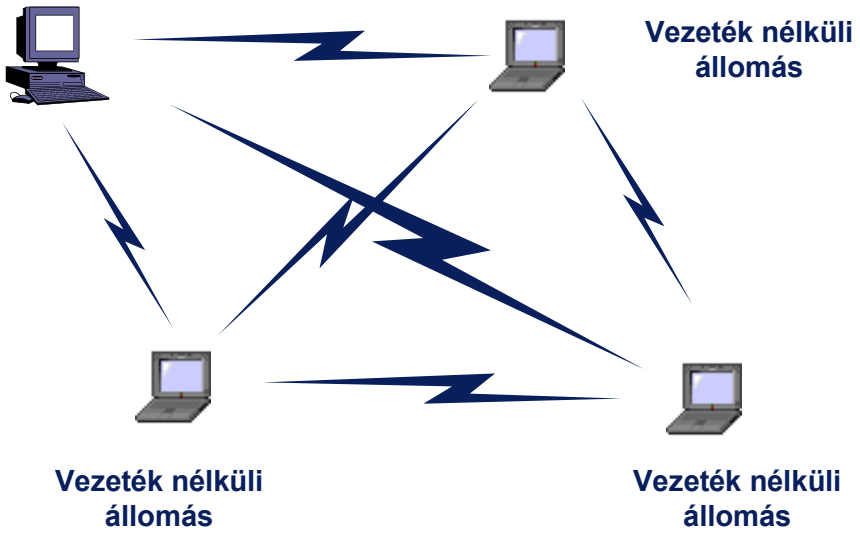
Az IEEE 802.11 szabvány alapvetően két eszközt definiál. Az egyik a vezeték nélküli állomás (wireless station), ami a leggyakrabban egy vezeték nélküli hálózati interfész kártyával kiegészített hordozható vagy asztali számítógép. A másik elem a hozzáférési pont (access point), ami a vezetékes LAN-hálózathoz vagy más hálózathoz csatlakozik és a vezeték nélküli állomásokkal kommunikál. A vezetékes oldalon ennek megfelelően egy LAN-interfésszel (például egy 802.3 Ethernettel), a vezeték nélküli oldalon pedig a 802.11-ben definiált három fizikai átvitel közül valamelyikkel rendelkezik. A három átviteli módból kettő rádiófrekvenciákkal, míg a harmadik infravörös átvitellel dolgozik.

A 802.11 szabvány két eltérő üzemmódot is kidolgozott. Az egyik az infrastruktúra mód, amikor egy meglévő LAN-hálózathoz egy vagy több hozzáférési pont csatlakozik és a vezeték nélküli állomások ezeken keresztül kapcsolódnak a WLAN-hálózatra (2. ábra). Ekkor egy vezetékes LAN-hálózat vezeték nélküli bővítése, kiegészítése jön létre. Egy hozzáférési pont esetén szokták alapszolgálatnak (Basic Service Set – BSS), több hozzáférési pont esetén bővített szolgálatnak (Extended Service Set – ESS) is hívni. A másik üzemmód az ad hoc mód, amikor a vezeték nélküli állomások közvetlenül egymással kommunikálnak, a hálózatban nincs hozzáférési pont (3. ábra). Sokszor hívják ezt „peer to peer” módnak vagy

független alapszolgálatnak (Independent Basic Service Set – IBSS) is. Ebben az esetben a vezetékes LAN-hálózattól távol, attól teljesen függetlenül léphetnek egymással hálózati kapcsolatba vezeték nélküli állomások gyorsan és hatékony módon, különösebb befektetés nélkül.



2. ábra. WLAN-hálózat a vezetékes LAN-hálózathoz illesztve



3. ábra. Ad hoc WLAN-hálózat bázisállomás nélkül

Mint már említettük, a fizikai réteg három különböző technológiát szabványosít. Röviden bemutatjuk a három réteget, de részleteiben a legnépszerűbb rádiófrekvenciás kapcsolatot ismertetjük.

Az első technológia az infravörös hullámokkal működő kapcsolat. A rendszer ugyanazt a 850–900 nm-es hullámhosszat használja, mint az optikai kábelek. A megoldás előnye, hogy nincs sávszélességet korlátozó tényező, ezért az átvitel sebessége igen nagy lehet. Ugyancsak előny, hogy semmiféle engedély nem szükséges az infrasáv használatához. Amennyiben az infravörös sugárzás irányított, akkor a hatótávolság akár kilométeres nagyságrendű is lehet. Ha azonban az inravörös sugárzás irányítatlan, akkor a hatótávolság néhányszor tíz méternél nem nagyobb. Hátránya viszont a rendszernek, hogy a napfény és néhány más, a tartományban is sugárzó fényforrás egyes esetekben megzavarhatja a kapcsolatot, továbbá az, hogy az átlátszatlan tárgyak megakadályozzák a kapcsolat felvételét.

Az elterjedtebb forma a szórt spektrumú rádiófrekvenciás kapcsolat, a másik két technológia ezt a megoldást használja. Mivel a rádiófrekvenciás WLAN rendszerek kezdenek egyre több alkalmazásban terjedni, ezért ezt a technológiát részletesebben is bemutatjuk.

A 802.11 a rádiófrekvenciás kapcsolatot két olyan sávban valósítja meg, amelyeket a világ szinte összes hatóságai szabadon tartanak, és ebben a sávban nem szükséges engedély a kommunikációs eszközök működtetéséhez. Cserében viszont ebben a sávban sok egyéb berendezés is működhet, amelyek például az iparban, az orvosi készülékekben stb. keletkeznek. Ezért is hívják ezt a sávot ipari, tudományos és orvosi sávnak (Industrial, Scientific and Medical – ISM band). Az egyik ilyen sáv a 902–928 MHz-es tartományban, míg a másik a 2,4–2,483 GHz-es tartományban helyezkedik el. Mivel ebben a sávban a fentiek miatt nincsen biztosíték a zavartalan kommunikációra, így a hagyományos rádiókapcsolat nem működőképes. Éppen ezért a szabvány kidolgozói két szórt spektrumú rendszert specifikáltak a hozzáférési pont és a vezeték nélküli állomás közötti kapcsolatra. Az egyik a frekvenciaugratásos szórt spektrumú (Frequency Hopping Spread Spectrum – FHSS), a másik a közvetlen sorrendű szórt spektrumú (Direct Sequence Spread Spectrum – DSSS) technika. Mindkét technikának az a lényege, hogy a kisugárzásra kerülő információ széles sávban kerüljön átvitelre oly módon, hogy kellő redundanciát is tartalmazzon. Ebben az esetben ugyanis a vevő akkor is venni tudja a teljes, sértetlen információt, ha egy-egy frekvencián éppen folyamatos zavar van jelen az ISM sávban.

Az FHSS technikában a rendelkezésre álló sávot 75 darab 1 MHz-es sávra osztották. Az adó és a vevő egy adott frekvenciaugratási sablon szerint váltja a csatornákat igen sűrűn, másodpercenként is igen sokszor. A kisugárzott jel így széles sávú zajként jelenik meg a külső szemlélő számára. Ugyanakkor a vevő követni tudja a frekvenciaváltásokat, és ezzel egy jó interferenciatűrő átvitel valósul meg.

A DSSS technikában a sávot 14 darab 22 MHz-es csatornára osztották fel, amelyek átlapolódnak. Egy kapcsolat egy csatorna szélességében épül fel oly módon, hogy az adatjeleket egy, az adatjelnél jóval nagyobb bitsebességű kóddal megszorozzuk. A küldött információ így jelentős redundanciával érkezik meg a vevőoldalra, ahol a kód ismeretében visszaállítható.

Az FHSS technika az 1 MHz-es felosztás miatt maximálisan 2 Mbit/s-os átvitelt tesz lehetővé, ennek következtében a 802.11 szabvány csak az 1 Mbit/s-os illetve a 2 Mbit/s-os átviteli sebességet teszi lehetővé. A DSSS technika azonban nagyobb átviteli sebességet is lehetővé tesz, ezt használja ki a 802.11b szabvány, amelyik az 5,5 Mbit/s-os és a 11 Mbit/s-os átvitelt is lehetővé teszi a DSSS technikával. Ehhez azonban a korábbi 11 bites kód – a Barker-szekvencia – helyett a Complementary Code Keying (CCK) szekvenciát használják, mely 64 darab 8 bites kódszó sorozatából áll. Ez a kódolás kényesebb a zavarokra, ezért amennyiben a 11 Mbit/s-os átvitelhez a környezeti zajok túl erősek, akkor a kapcsolat egy alacsonyabb sebességen – 5,5 Mbit/s-on, 2 Mbi/s-on, vagy akár 1 Mbit/s-on – jön létre. A 802.11 DSSS technikája és a 802.11b DSSS technikája – természetesen az alacsonyabb sebességen – képes az együttműködésre, azonban az FHSS kódolással az újabb szabvány nem működik együtt.

A WiMAX rendszer

A WiMAX Szövetség által minősített IEEE 802.16. szabvány kidolgozásának **a gondolata 1998 augusztusában született meg**, amikor az U.S. National Institute of Standards and Technology mérnökei elhatározták, hogy az akkor már formálódó 802.11 szabvány szerinti WLAN-hálózatok forgalmát egy univerzális vezeték nélküli ernyővel, a Wireless MAN hálózattal kellene összefogni. Az ehhez szükséges munkát az IEEE égisze alatt megszervezett 16-os Study Group kezdte meg 1999 júliusában. Az IEEE 802.16 szabvány **2001 októberében nyerte el végleges változatát, s 2002 áprilisában publikálták**.

Az IEEE 802. 16 szabvány a 10–66 GHz-es tartományra dolgozta ki annak a rádióinterfésznek a részleteit, ami néhány kilométeres körzetben 32 és 134 Mbit/s közötti sebességgel képes összegyűjteni és továbbítani a lefedett WLAN-hálózatok forgalmát. A rendszert 20 és 25 MHz-es csatornaosztással dolgozták ki az Egyesült Államok frekvenciakiosztásához illeszkedően, és 28 MHz-es csatornaosztással az európai frekvenciakiosztáshoz illeszkedően. A tartományban többféle modulációt használnak, a QPSK mellett a 16QAM és a 64QAM kvadratúra-moduláció jellemző a technológiára. A 10–66 GHz-es tartományt azért választották a szabványosítók, mert ebben a tartományban bőven vannak szabad kapacitások a rendszer megvalósítására, azonban ennek a sávnak a nagy hátránya, hogy terjedési jellemzői miatt csak tiszta rálátás esetén működik kielégítően. Tekintettel arra, hogy a WLAN rendszerek jellemző alkalmazási területei időközben azok a forgalmas helyszínek lettek, melyeken a rálátás sok esetben nehezen vagy egyáltalán nem biztosítható, így a szabvány kidolgozása közben előtérbe került azoknak a sávoknak a felhasználása, amelyeknél a rálátás nélküli terjedés még lehetséges.

Ennek a folyamatnak a következményeként kezdődött meg az IEEE 802.16a szabványkiegészítés kidolgozása, ami 2003 januárjában fejeződött be. A 802.16a szabvány a 2–11 GHz-es tartományban elhelyezkedő sávokat használja fel. Ebben a sávban ugyanis nem csak a közvetlen rálátás esetén működik a kommunikáció. Mivel ebben a tartományban egyaránt vannak szabadon használható sávok és engedélyköteles sávok, ezért két eltérő jellegű modulációs rendszert használ a szabvány. A modulációs technikáknál a 802.16-hoz képest megjelenik az OFDM (Orthogonal Frequency Division Multiplex) technika 256 mellékvivős

változata. A csatornakiosztás 1,25 MHz és 20 MHz között változik, s ezzel a módszerrel maximálisan 75 Mbit/s-os átviteli sebességet lehet elérni tipikusan 5–10, maximálisan 40–50 km-es körzetben.

A fenti általános adatok mellett figyelemre méltó a szabványcsaládban rögzített megoldás felépítése is. Az alapvetően pont–multipont széles sávú vezeték nélküli elérést nyújtó megoldás egyaránt nagy sávszélességet használ a letöltési és a visszirányban, megteremtve ezzel a teljes értékű kommunikációs lehetőséget a WLAN-hálózatok különböző használói részére. Ezenkívül azonban igen gondosan alakították ki a szabványt kidolgozók a különböző, egymástól teljesen eltérő paraméterű alkalmazások kiszolgáló algoritmusait is. A szabvány képes kezelni a hagyományos TDM-alapú beszéd- és adatforgalmat, az IP-forgalmat, valamint a csomag alapú VoIP-alkalmazásokat is. Ezt az az összetett MAC (Medium Access Control) réteg teszi lehetővé, mely a szabvány lelkét jelenti. A szabványosított MAC réteg egyaránt támogatja a folytonos terhelésű és a börszt jellegű adatforgalmat, s széles lehetőségeket nyújt az adott kapcsolat QoS (Quality of Service) jellemzőinek a garantálására is. Az ATM alapelveihez hasonlóan a 802.16 MAC rétege képes a konstans és a változó bitsebességű, valamint a maradékelvű bittovábbítás szolgálattípusait kiszolgálni, sőt ezek mellett definiálja a garantált keretsebesség (Guaranted Frame Rate – GFR) szolgálatot is.

A MAC réteg és a fizikai réteg között átviteli konvergencia alrétegek (Transmission Convergence Sublayer – TC) helyezkednek el. Ezek szerepe, hogy az eltérő fizikai rétegeket az egységes MAC réteghez illesszék. Ezzel a megoldással sikerült megvalósítani a 802.16a alkalmazkodását az eltérő jellegű frekvenciasávokhoz és az azokhoz tartozó különböző szabályozási előírásokhoz. A megoldás nagymértékben javítja a WiMAX versenyképességét.

Ugyancsak megoldott a MAC és a különböző protokollt használó alkalmazások illesztése is. Erre szolgálnak a szolgálat-specifikus konvergencia alrétegek (service-specific convergence sublayer – SSC). Ezek közül az ATM konvergencia alréteg (ATM Convergence Sublayer) az ATM szolgálatokat, a csomag konvergencia alréteg (Packet Convergence Sublayer) az IPv4, IPv6, Ethernet és WLAN átviteli szolgálatokat támogatja.

A 802.16 és 802.16a szabvány összedolgozásának az eredményeként elfogadta az IEEE a 802.16REVd szabványt, amelynek az a lényege, hogy mindkét említett szabvánnyal kompatibilis, ugyanakkor egyesíti a kettő előnyeit.

Hasonlóan a 802.11 szabványcsaládhoz, a 802.16 esetében is alapvető fontossága van a szabvány alapján megszülető eszközök együttműködési tesztelésének. Ezt a WiMAX Forum végzi és a sikeresen vizsgált berendezéseket a „WiMAX Certified” címkével látja el. Innen származik a technológia összefoglaló neve, amelyet sok helyen egyszerűen WiMAX-nak hívnak.

Mint említettük, a 802.16 alapgondolata az volt, hogy a WLAN-hálózatok feletti infrastruktúrát valósítsa meg. A szabvány kidolgozói azonban továbbléptek és IEEE 802.16e néven egy olyan interfészt is létrehoztak, ami közvetlenül alkalmas – a laptopokba helyezett PCMCIA kártya segítségével – a WiMAX rendszerre csatlakozni. Ezzel lehetővé válik a lefedett területen való mozgás is, mert a 802.16e

mozgó állomások kiszolgálását is biztosítja, sőt a barangolást is lehetővé teszi az átfedő WiMAX-ernyők között. Az Intel cég már megkezdte azoknak a chipeknek a gyártását, melyek a WiMAX-szabvány szerinti PCMCIA kártyákhoz szükségesek és ezzel a laptopok, illetve PDA-k további mobilitása is lehetségessé válik.

A mindenütt jelen lévő számítástechnika

A mindenütt jelen lévő számítástechnika **a jövő egyik ígéretes trendje**. Lényege, hogy az egyre kisebbé váló informatikai eszközök fokozatosan átfonják mindennapi életünket, minden eszközbe beköltöznek. Az angol terminológiában „ubiquitous communications" vagy „pervasive computing" néven elterjedt megoldások abban az irányban fejlődnek, hogy eszközeink bárhol, bármikor képesek akár hálózatba is kapcsolódni és önállóan ellátni bizonyos feladatokat, amelyeket eddig csak emberi beavatkozásra tettek meg. A tipikus köznapi példa, amikor a hűtőszekrény automatikusan megrendeli a tejet, ha az már fogytán van, és persze a példákat hosszan sorolhatnánk. A trend egyenes következménye, hogy a fejlődés egy adott szintje felett már a tárgyak is internetezni fognak, s jó értelemben megjelenik az automaták világa. A trend elterjedésének fontos eleme a rádiós érzékelők (RFID) elterjedése, valamint a nanotechnológia további előretörése.

A széles sávú platformok elterjedése

Az ITU által azonosított harmadik trend a széles sávú platformok elterjedése mind a vezetékes, mind a vezeték nélküli rendszerek esetében. A vezetékes világban az xDSL egyre nagyobb sebességek átvitelére képes, a mindenki által jól ismert ADSL-nek is megjelentek a fejlettebb változatai ADSL2, illetve ADSL2+ néven, amelyek már – igaz, csak korlátozott távolság esetén – a 10 Mbit/s-os sebességet is képesek túllépni. Eközben a DSL Forum dolgozik a VDSL (Very High Speed DSL) szabványon, ami első változatában is képes 52 Mbit/s-os átviteli sebességre, de fejlettebb változata már akár a 100 Mbit/s-os sávszélességet is lehetővé teszi. Ugyancsak nőnek az átviteli lehetőségek a kábeltévé-hálózatokon, de a jövő egyre inkább az optikai kábelé lesz. Itt az FTTH (Fiber to the Home) az a távoli megoldás, amely a szinte korlátlan sávszélességet fogja kínálni az otthonok számára.

Ugyancsak **intenzív fejlesztés folyik a vezeték nélküli rendszerekben a sávszélesség növelésére**. A 3G rendszerek általános sávszélesség-ígérete mellett a HSDPA (High Speed Download Packet Access), illetve a HSUPA (High Speed Upload Packet Access) jelenti a nagyobb sebességet, de emellett a már említett MMDS, LMDS illetve a WiMAX rendszerek is képesek lesznek nagy sebességű szolgáltatásokat kiszolgálni.

Minden tartalom IP felett

Ez a trend talán az egyik leginkább figyelemre méltó trend jelenleg, hiszen **következményeiben a hírközlés legnagyobb paradigmaváltását fogja hozni a fejlődéstörténetben**. A valós idejű tartalmat – beszédet, videojelet stb. – hordozó hálózatok ugyanis Alexander Graham Bell találmánya, a telefon megjelenése óta a vonalkapcsolás elvén működnek. Az első manuális telefonközpont 1878-ban kezdte

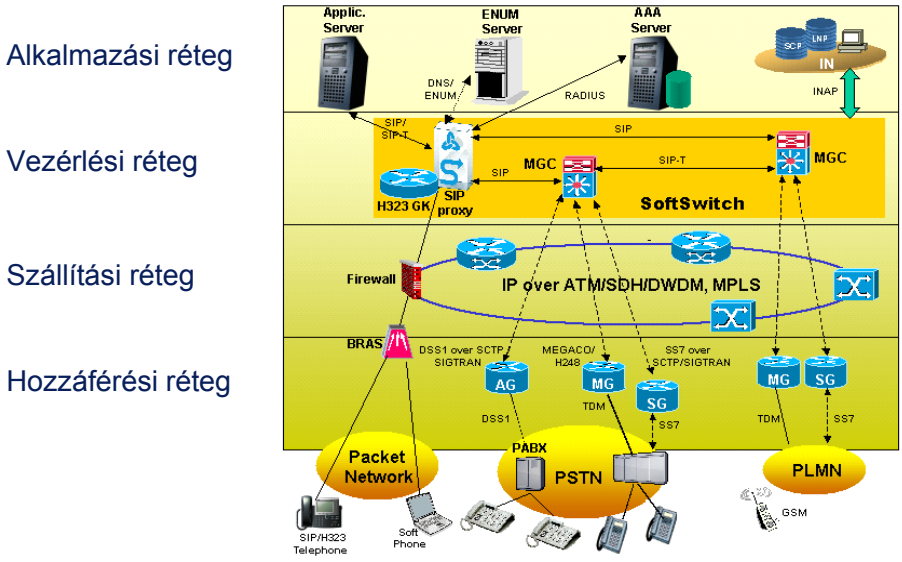
meg működését, azóta léteznek tehát a vonalkapcsolt hálózatok, amelyek lényege, hogy a két egymással forgalmazó felet egy, csak a számukra fennálló kapcsolattal összekötik, s ezen a vonalon folyik a kommunikáció. Hosszú ideig ez a kapcsolat fémes kapcsolatot is jelentett, a digitális telefonközpontok megjelenésével ugyan a fémes kontaktus már nem jön létre a két fél között, de az alapelv továbbra is a vonalkapcsolás maradt.

A számítógépek egészen máshogy kommunikálnak egymással. Az első számítógép-hálózat, az ARPANET 1969-ben történt létrehozása óta – ami éppen katonai célú indíttatásból jött létre, hogy az információk katasztrofális támadáskor is tovább tudjanak létezni –, a számítógépek között az ún. csomagkapcsolt üzemmód a jellemző. Ennél az elvnél az információt a feladó oldal kis csomagokra bontja és címmel látja el, majd ezek a csomagok a hálózaton egymástól függetlenül jutnak el a címzettig, aki sorba rakja őket és így visszanyeri a küldött üzenetet. Ezt az elvet sokáig nem lehetett beszéd átvitelére használni a hálózatban lévő útvonalválasztók (routerek) lassú sebessége és a késleltetések ingadozása miatt. Mára viszont a feldolgozási kapacitás elérte azt a mértéket, amelynek segítségével már a valós idejű forgalom biztonsággal lebonyolítható a csomagkapcsolt hálózatok segítségével, a technológia szabad utat nyitott a paradigmaváltás előtt. Természetesen ez nem jelentene a piacon nagyobb változást, ha a szolgáltatóknak különösebben nem állna érdekükben a csomagkapcsolt hálózatok alkalmazása. Mivel azonban a csomagkapcsolt átvitel a hálózat hatékonyabb kihasználását teszi lehetővé, összességében tehát olcsóbb, ezért az új technológiák bevezetése lavinaszerűen indult meg. Az internet-telefon mellett megjelentek a professzionális VoIP-megoldások, ahol már menedzselt IP-alapú hálózaton, tervezhető forgalmi viszonyok mellett jó minőségű szolgáltatást lehet nyújtani. Megjelent **az IPTV**, ami ugyan még **fejlődése kezdeti stádiumában van, de lehetőségei nagyon tágak**. Az IPTV várhatóan hasonló fejlődési görbét fog leírni, mint a VoIP: a kezdeti nehézségek leküzdése után igen meredeken fog felfutni az alkalmazása, terjedése.

Ennek a lavinaszerű jelenségnek a motorját természetesen az IP-protokoll adja, hiszen ez a protokoll alkalmas arra, hogy a legkülönbözőbb tartalmakat egyaránt képes legyen kezelni. Ezzel viszont megnyílt annak a lehetősége, hogy egy adott IP-alapú hálózaton a legkülönfélébb típusú információkat (hang, zene, kép, beszéd, video stb.) lehessen átvinni adott pontok között, akár valós idejű módon. Ennek következtében jelent meg a piacon a „triple play”, majd a mobil rendszerek IP-alapra helyezésével a „quadruple play”.

A csomagkapcsolásra való áttérés és az egységes protokoll együttesen közel hozta azt, amire a digitalizáció önmagában még nem volt képes: megteremtette a gyakorlati lehetőségét a hálózatok konvergenciájának. A konvergencia mint trend már szerepelt az előadás első felében: beszélhetünk a végberendezések konvergenciájáról, a szolgáltatások konvergenciájáról, az infokommunikáció és a média konvergenciájáról, azonban a hálózatok konvergenciája a paradigmaváltás előtt nem tudott széles körben megvalósulni. A legbiztatóbb eredményeket ebben a témában talán az ATM rendszerek fejlesztése jelentette, azonban az ATM nagyon jól kitalált, csomaghosszra optimalizált protokollja – és persze az ezt körülbástyázó megoldások – messze nem lettek olyan költséghatékonyak, mint az IP-megoldások.

A hálózatok konvergenciája természetszerűen kínálja azt a gondolatot, hogy **egyetlen hálózattal lehessen a szolgáltatások széles skáláját nyújtani, mindezt tetszőleges típusú információkra vonatkozóan**. Ezt az elvet fogják megvalósítani azok a hálózatok, melyeket összefoglaló néven Next Generation Networks, azaz NGN néven ismerünk.



5. ábra. Az NGN sematikus rendszertechnikája

Az ITU-T az NGN-re adott meghatározásában – amely talán a leginkább elfogadott a piaci szereplők között –, a következőket követeli meg az NGN hálózattól:

- csomagkapcsolt hálózaton alapul;
- többszolgálatú, széles sávú, QoS-képes átvitelre képes;
- a szolgáltatási funkciók függetlenednek az átviteltől;
- korlátok nélküli hozzáférést nyújt a szolgáltatókhoz;
- egységes és mindenütt elérhető mobilitást ad.

Ezzel a gondolattal jutunk el a teljesen IP-alapú, csomagkapcsolt kommunikációhoz, az újgenerációs hálózatok megjelenéséhez, amely hamarosan a vonalkapcsolt hálózatok helyére léphet, megdöntve ezzel egy több mint 120 éves alapelvet. Ez az, amit joggal nevezhetünk a hírközlés eddigi legnagyobb paradigmaváltásának!

Az információs társadalom kibontakozása

Az ötödik azonosított trend az információs társadalom kialakulása, amelyet ugyan a technológiai fejlődés mozgat és sebességét is részben az határozza meg, azonban alapjában véve itt egy komplex társadalmi kategóriáról van szó. Az információs társadalom kialakulása ugyan egy hosszadalmas folyamat, azonban a kibontakozást azért fogalmazta meg az ITU aktuális trendként, mert a folyamat első fázisában már jelentkezhetnek mindazok a társadalmi hatások, amelyek következtében a társadalom kisebb-nagyobb csoportjai kiszorulhatnak a digitális írástudók táborából, és kialakulhat a társadalmon belül a digitális szakadék. Ennek elkerülésére az ITU több akcióprogramot is indított, ezzel azonban – lévén, hogy ez a téma távolabb esik a konferencia témájától –, most nem foglalkozunk.

ÖSSZEFOGLALÁS

A hat megatrend és az ITU által azonosított öt aktuális trend világosan kirajzolja, milyen fejlődési irány várható a 21. század első két évtizedében. Hogy ezek a trendek mennyiben lesznek meghatározóak az évszázad további részében, azt persze nem lehet most még tudni, sejteni. A valószínű irány azonban nyilván nem változik, és a hírközlés – persze újabb és újabb technológiákkal, hatékonyabb kódolási és modulációs technikákkal, a digitális jelfeldolgozás további bravúrjaival – egyre inkább mindennapi életünk részévé, természetes kiszolgálónkká válik.

DR. KOLLER ISTVÁN

A DIGITÁLIS JELFELDOLGOZÁS KORSZERŰ HARDVER ELEMEI

A klasszikus analóg jelátviteli, jelfeldolgozó láncokat egyre inkább kiszorítják a digitális megoldások. A digitális jelátvitelben alkalmazható redundancia révén elérhető veszteségmentes átvitel, a távoli javíthatóság, az elérhető kis méret, és ezek mellett a viszonylag olcsó realizálás csak néhány az előnyök közül, amik további várható térhódítását indokolják.

Akár analóg, akár digitális megoldásokról beszélünk, a jelfeldolgozás alapfeladatai hasonlóak. Ezek például a szűrés, az erősítés, a frekvenciatartományi áthelyezés, a moduláció, demoduláció. Ezeknek a feladatoknak a digitális megvalósításában alapvető szerepe a szorzás-akkumulálás (MAC) műveletének van. A digitális jelfeldolgozó (DSP) hardver elemeknek ezt a műveletet kell a lehető leghatékonyabban végrehajtani.

A digitális jelfeldolgozó elemek fejlődése

A digitális jelfeldolgozás a híradástechnikai ipar napi gyakorlatában az 1970-es években jelent meg, majd az 1980-as években a PCM távközlési alkalmazások révén vált elterjedtté. Ezekben az években a hardver elemekre a diszkrét TTL-kapus megoldások, drága SRAM-ok, valamint igen drága, nagy fogyasztású bipoláris szorzóáramkörök voltak a jellemzőek. A ’80-as évtized volt az általános célú mikroprocesszorok elterjedésének az időszaka is. Akkor jelentek meg az egyszerű programozható likai áramkörök, a PAL-ok, amik lehetővé tették több TTL-kapu funkcióinak egy tokon belüli realizálását. A ’80-as évek második felében jelentek meg azok a mikroprocesszorok, amiket speciálisan jelfeldolgozási célokra terveztek, a DSP-chipek. Az egyik első DSP-chip volt az 1983-ban megjelent nagy klasszikus, a Texas Instruments 16-bites, fixpontos, TMS32010-es DSP-je, ami megjelenése idején a leggyorsabb, legnagyobb teljesítményű chip volt a piacon.

Az 1990-es évek az egyre hatékonyabb fixpontos és lebegőpontos DSP-chipek és az egyre több logikai elemet tartalmazó SRAM-alapú programozható logikák, az FPGA-k megjelenésének és gyors elterjedésének az ideje.

A 2000 óta eltelt években a DSP-chipek választékának hihetetlen növekedését láthatjuk, ami lehetővé teszi az adott alkalmazáshoz leginkább illő típus kiválasztását. A másik jellegzetesség az FPGA áramkörök logikai elemeinek igen nagy száma, a nagy méretű memóriacellák és szorzómagok, amik az FPGA áramkörök eddigi tipikus alkalmazási területét az úgynevezett „glue-logic”-ot kiegészíti egy új alkalmazási területtel, a digitális jelfeldolgozó algoritmusok implementálásának lehetőségével.

Az FPGA-k mint digitális jelfeldolgozó elemek

Az FPGA (Field Programmable Gate Array) áramkörök programozható logikai elemeket, és azok belső összeköttetéseit tartalmazzák A logikai elemek képesek kombinációs és szekvenciális hálózatok megvalósítására, mivel tároló elemeket is tartalmaznak. Sőt nemcsak egyszerű flip-flopok, hanem elkülönült, nagyméretű memóriablokkok is jellemzik az újabb típusokat. A program, azaz a megvalósítandó logikai funkciók, illetve az összeköttetések definíciója, az áramkör konfigurációs memóriájába, egy sztatikus RAM-ba töltendő a használat helyszínén, azaz a „field"-en. Innen ered Ross Freemannak, a Xilinx cég fiatalon elhunyt társalapítójának nagyszerű, 1984-ben közreadott találmányának az elnevezése.

A RAM-ban való konfiguráció-tárolás azt jelenti, hogy minden bekapcsolás után ezt a RAM-ot fel kell tölteni, azaz az FPGA-t konfigurálni kell. Ez az első pillanatbeli hátrány valójában előny, hiszen a megvalósított hardver újradefiniálható, azaz az áramkör átkonfigurálható, a tartalom mint processzor esetében a program betölthető. Így jutottunk el a programozható, újrakonfigurálható hardverig. Sőt sok típusnál részleges átkonfigurálásra is lehetőség van, ami megengedi azt, hogy míg az interfész-funkciókat megvalósító áramköri részek állandóak maradnak, addig az alkalmazás specifikus részek átkonfigurálhatók a rendszer működése közben.

Napjaink FPGA-jában azonban az előzőekben említetteken túl speciális áramköri elemek is, például összeadók és szorzók is megtalálhatók. Ezek az új elemek, illetve az áramkörök újrakonfigurálhatósága teszi azt lehetővé, hogy az FPGA-áramkörök a hagyományos alkalmazásokon túlmenően digitális jelfeldolgozó célhardvereket realizáljanak.

Az összeadókon, szorzókon kívül sok FPGA tartalmaz komplett processzor-struktúrát is. Így aztán az integráltsági fok, az áramkörök egyre nagyobb komplexitása teszi ma azt lehetővé, hogy teljes rendszerek kerüljenek az FPGA-chipekbe, létrehozva a System on a Chip struktúrát. Ez azt jelenti, hogy a processzor, a memória, a glue-logic, a jelfeldolgozó célhardver – később talán még analóg feladatok is –, mind-mind egy chipen, a helyszínen programozható logikai áramkörön, azaz az FPGA-n kerül megvalósításra. A nyomtatott áramkörök tervezőinek tehát várhatóan egyre egyszerűbbek lesznek a feladatai, hiszen egy áramköri lapon várhatóan tipikusan egy FPGA lesz a most még távoli jövőben, aminek minimális számú lábai a külvilági csatlakozást, illetve a tápellátást szolgálják.

Itt kell megjegyezni, hogy ez a flexibilitás, konfigurálhatóság, amit az FPGA-k nyújtanak, ötletet adott a mikroprocesszor-konstruktőröknek is, és létrehozták a szoftverből átkonfigurálható mikroprocesszor-struktúrát. A Strech Inc. által létrehozott konfigurálható processzortömb az S5000 chip. A processzortömb az általános mikroprocesszorokhoz hasonlóan C-nyelven programozható, és a fordító határozza meg az optimális processzor-struktúrát az adott programhoz.

Az FPGA-kat a fenti tulajdonságaik miatt sikeresen alkalmazzák a digitális jelfeldolgozás, szoftverrádió területeken. Az alkalmazást fejlett, esetenként igen magas szintű fejlesztői környezetek segítik. Napjainkra az FPGA-k által megvalósítandó hardver definiálására a régebben használatos kapcsolási rajzot teljesen kiszorította a hardverleíró nyelvek alkalmazása, valamilyen HDL (Hardware Description Language)

vált elsődleges tervezői definíciós eszközzé. Ezek közül kiemelkednek a VHDL- és a VERILOG-nyelvek. A HDL alkalmazásának kétségtelen előnye a hordozhatóság, az általa leírt hardver nem kötődik konkrét áramkörhöz, FPGA-gyártóhoz, hasonlóan viselkedik, mint egy C-ben megírt szoftver-szubrutin, ami közismert módon hordozható. Így egy megtervezett hardvert az egyik gyártó FPGA-járól a másikéra viszonylag egyszerűen adaptálni tudunk. Ez a hordozhatóság az alapja az IP (Intellectual Property) core-oknak is, ahol egy funkciót nem egy konkrét chip formájában vásárolunk meg, hanem annak definícióját egy hardverleíró nyelven, amit aztán a saját áramköri megoldásainkkal ki tudunk egészíteni és implementálni egyetlen FPGA-chipen. Nagyon sok szabadon, díjmentesen felhasználható core is a tervezők rendelkezésére áll.

Ma az FPGA-k piacán két óriás, az ALTERA és a XILINX versenyez a vásárlók kegyeiért. Mindkét cégnek teljes a választéka az FPGA-k kisebb-nagyobb változataiból. A chipek mellett mindkét gyártó kényelmes, hatékony, könnyen kezelhető fejlesztői környezetet is ad a chipek használóinak.

Például a Xilinx ISE Fundation a logikai tervezés, szimuláció igen hatékony eszköze. Ezt egészíti ki a jelfeldolgozási algoritmusok tervezését, szimulációját segítő Xilinx Sytem Generator, ami a Mathwork Matlab Simulink tervezői környezetével köti össze a Xilinx ISE tervezői rendszert. Ezek segítségével a tervező a Simulink magas szintű blokkvázlataival definiálhatja a jelfeldolgozó algoritmust, és ebben a környezetben szimulálhatja is azt. A már tesztelt, jól működő rendszert a Matlab alatt működő System Generator fordítja egy Xilinx ISE HDL-alapú projektté, amit aztán az ISE környezetben integrálhatunk az FPGA-nkba.

A DSP-chipek mint digitális jelfeldolgozó elemek

A DSP (Digital Signal Processor) chipek is mikroprocesszor architektúrájúak, rendelkeznek központi egységgel, perifériákkal, memóriákkal. Van azonban néhány speciális tulajdonságuk, amik alapján egy új processzorcsaládot, a DSP-k családját alkotják.

A DSP-kre egyik legjellemzőbb tulajdonság a program- és az adatmemória elkülönülése, azaz a Harvard-architektúra. Ez az architektúra lehetővé teszi az utasításkód és az operandus egyidejű lehívását, így a gyorsabb működést. Többszörös Harvard-architektúrák is jellemzők, amikor több adatmemóriából történhet egyidejű adatlehívás. Ezek az architektúrák tipikusan csak a DSP-chipen belül realizálódnak, míg az eszköz külső memóriáit egy, vagy esetleg két memóriabuszon keresztül éri el.

Igen fontos az előzőekben említett szorzás-akkumulálás – MAC (Multiply Accumulate) alapművelet – gyors végrehajtása. Erre a feladatra a DSP-chipekben széles, nagyon gyors szorzók és összeadók találhatók.

Mivel a digitális jelfeldolgozás valós idejű követelményei mintavételi időnként újabb bemeneti minta elvételét és újabb kimeneti minta generálását követeli (amit gyakran interruptokkal időzítünk), igen fontos a gyors reagálás a különböző interrupt-forrásokra. Jellemző ezekre a chipekre a hosszú pipeline alkalmazása is.

A DSP-chipek tipikusan rendelkeznek speciális külvilági interfészekkel, például primer PCM jelfolyam fogadására alkalmas soros interfésszel. Gyakran rendelkeznek még speciális koprocesszor jellegű célhardverekkel, például Viterbi, vagy Turbo dekóderrel is.

A DSP-chipek igen fejlett, könnyen használható fejlesztői környezettel rendelkeznek. Ma tipikus a C-nyelv használata, de bizonyos feladatok hatékonyabban oldhatók meg assembly-betétek alkalmazásával. Itt is lehetőség van Matlab Simulink környezetben definiálni, szimulálni az algoritmusunkat, és a Simulink-be illesztett DSP-kódgenerátorral egy C-nyelvű projektet előállítani, hasonlóan az FPGA-tervezés folyamatához.

DSP-chipek és FPGA-k egy rendszerben

A DSP-chipek és az FPGA-k egyaránt alkalmasak digitális jelfeldolgozási feladatok végrehajtására.

Az FPGA beágyazott szorzói és gyorsműködésű áramkörei igen alkalmasak nagysebességű, de viszonylag kisebb komplexitású feladatok végrehajtására. Ilyen lehet például egy nagy sebességű (megaszimbólum per másodperc) digitális demodulátor realizálása.

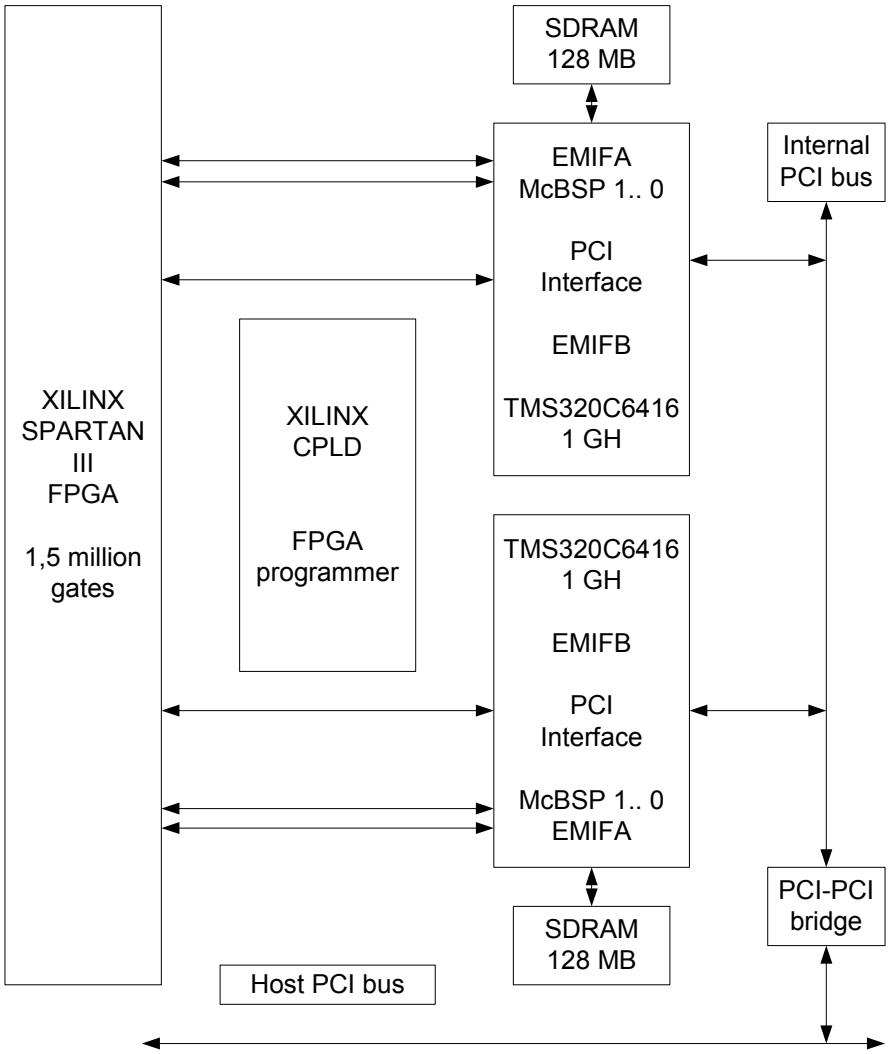
A DSP-chip ideális igen nagy komplexitású, az előzőnél kisebb sebességű feladatok megoldásában, például az előző példában szereplő nagy sebességű digitális demodulátor kimenetén létrejövő bitfolyam hibajavító dekódolására, keretfelismerésére, további demultiplexálására, csatornánkénti feldolgozására.

Ilyen típusú, az FPGA- és a DSP-chip előnyeit kiaknázni tudó jelfeldolgozó kártyacsaládot fejlesztett ki a RELCOM Kft. A PCDSP6 kártyacsalád közös jellemzője a PC 32bit/33MHz formafaktor, két darab, a világ legnagyobb sebességű 1GHz-es Texas Instruments DSP chipje és egy DSP alkalmazásokban jól használható Xilinx FPGA.

A PCDSP6 DSP/FPGA kátyacsalád

A jelfeldolgozó kártya két DSP-chipjét egy PCI/PCI hídáramkör illeszti a gazda PC-hez. A DSP-k külső memória interfészéhez csatlakoznak a nagyméretű, nagysebességű memóriák, illetve az FPGA-áramkör. Ezek az eszközök a DSP memóriatartományába vannak ágyazva, és a PC felől is bármikor, DSP-program segédlete nélkül elérhetők. Ez azt jelenti, hogy a kártya teljes erőforráskészlete megosztott a DSP és a gazda PC között.

A kártyán lévő DSP, a TMS320C6416T a legnagyobb számítási teljesítményű digitális jelfeldolgozó processzor ma a piacon. Ciklusideje 1 ns, amely alatt 8 darab 32 bites utasítást képes végrehajtani. A nagyméretű 1MB-os, 1 ns-os ciklusidővel elérhető on-chip memória szintén hozzájárul a DSP hatékonyságához. A Viterbi és a Turbo társprocesszorok a híradástechnikai alkalmazások esetén egyszerűsítik és gyorsítják a program végrehajtást.



1. ábra. A PCDSP6 kártyacsalád közös magja

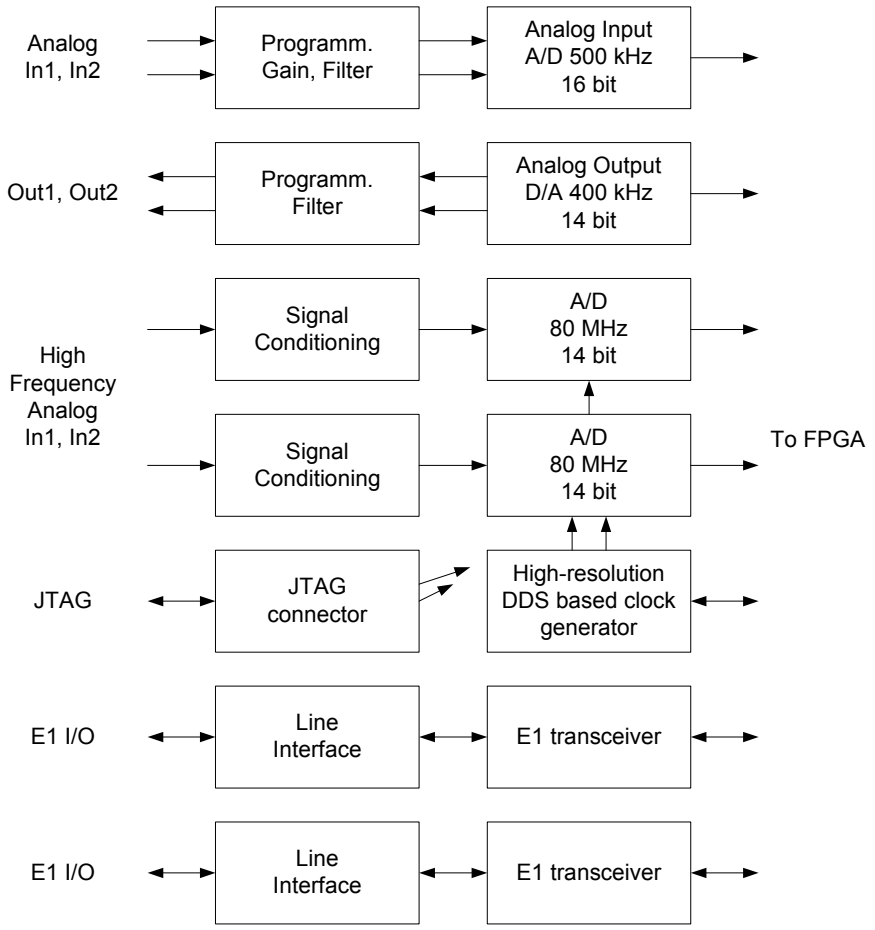
A kártyán lévő FPGA egy 1,5 millió kapus Spartan 3 FPGA, ami 32 db 18x18 bites hardver szorzót, 770 kbit memóriát is tartalmaz. Ez az FPGA lehetővé teszi például egy 2Msymbol/s-os 16QAM demodulátor megvalósítását adaptív szűrővel, vagy 8 darab digitális lekeverő modul implementálását.

Az FPGA konfigurációs területe – hasonlóan a DSP memóriájához –, a gazda PC-ből, vagy a DSP-ből érhető el. Az FPGA által megvalósított hardver tehát hasonlóan betölthető az FPGA-ba, mint egy program a processzor memóriájába.

Ez a konstrukció tehát képes az FPGA és a DSP-chip jelfeldolgozásban előnyös tulajdonságait együttesen kiaknázni.

Ehhez a maghoz kétféle külvilági front-end tartozik, létrehozva a PCDSP6UNI és a PCDSP6TEL kártyákat.

A PCDSP6UNI univerzális jelfeldolgozó kártya külvilági interfésze a 2. ábrán látható. Ez a front-end három részből áll: kétcsatornás alapsávi analóg ki-bemenetek, kétcsatornás nagysebességű bemenetek, és kétcsatornás primer PCM (E1/T1/J1) ki- és bemenetek.

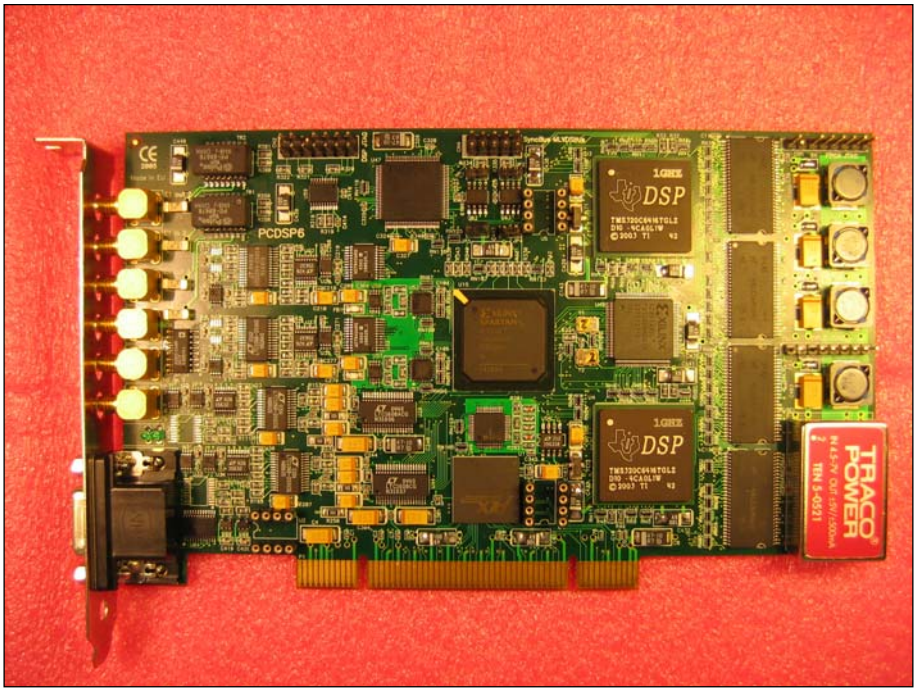


2. ábra. A PCDSP6UNI univerzális jelfeldolgozó kártya külvilági interfésze

Az alapsávi analóg interfész a mérésadat-gyűjtésben szokásos minőségű, offset-kiegyenlítést, pontos erősítésbeállítást tesz lehetővé. A fokozatban mind a bemeneteken, mind a kimeneteken programból állítható töresponti frekvenciájú alul áteresztő szűrőket tudunk bekapcsolni.

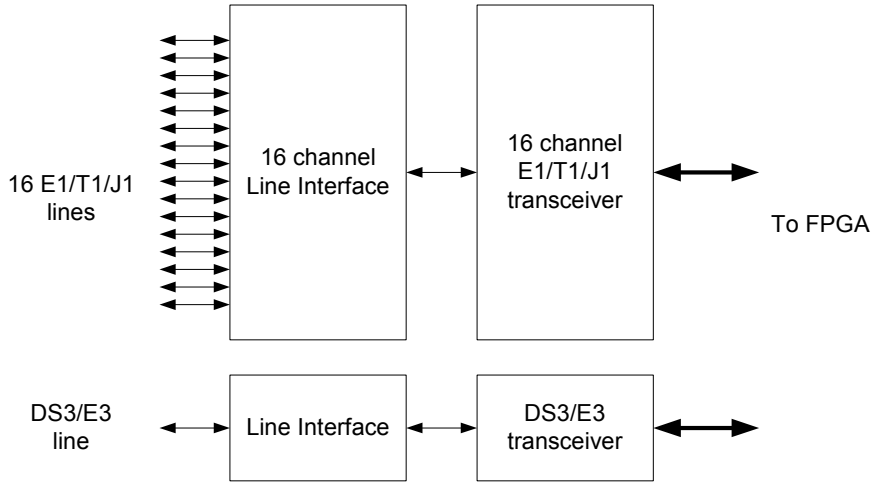
A nagy sebességű analóg bemenet ideális például szoftverrádió-alkalmazásokban, hiszen a 80 MHz-es mintavételi sebesség elegendő még egy műholdvevő 70 MHz-es, maximum 40 MHz sávszélességű jelének mintavételezésére is.

A primer PCM-fokozat az európai, japán és amerikai szabványok szerint működő primer PCM-jelek előállítására, illetve vételére alkalmas, két csatornán. A kártyán lévő számítási kapacitás lehetővé teszi például azt, hogy két E1-es jelfolyam 60 beszédcsatornájának jelét analizáljuk, a benne lévő FAX-adásokat detektáljuk, demoduláljuk, dekódoljuk. A PCDSP6UNI fényképe az alábbi ábrán látható.

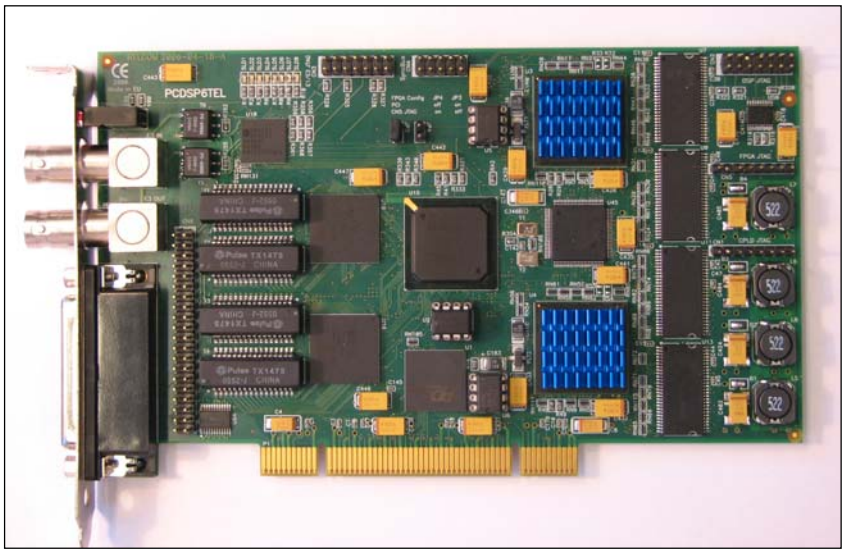


3. ábra. A PCDSP6UNI fényképe

A PCDSP6 család másik tagja a PCDSP6TEL telekommunikációs alkalmazásokra specializált jelfeldolgozó kártya. A kártya 16 darab E1/T1/J1, illetve egy E3/DS3 be- és kimenetet képes kezelni. Külvilági interfészének blokkvázlata a 4., míg fényképe az 5. ábrán látható.



4. ábra. A PCDSP6TEL telekommunikációs alkalmazásokra specializált jelfeldolgozó kártya külvilági interfészének blokkvázlata



5. ábra. A PCDSP6TEL telekommunikációs alkalmazásokra specializált jelfeldolgozó kártya

PAPP PÁL EZREDES

A SIGINT ÉS A REJTJELZÉS

Bevezetés

Az angol SIGINT (SIGnal INTelligence) rövidítéssel jelzett technikai hírszerzési eszköztár általában a szélesen értelmezett jel/információ érzékelését, feldolgozását jelenti információs előny megszerzéséért valamilyen katonai, diplomáciai, gazdasági versenyhelyzetben. A SIGINT-eszközök további osztályozása ellentmondásos, a szakirodalom szűkössége miatt nem születtek meg közmegegyezésen alapuló terminológiák.

A SIGINT megjelenése az elektronikus kommunikáció megjelenéséhez, annak tömegessé válásához kapcsolódik. A rádiótávíró megjelenése után az első világháborús konfliktusokban már kiterjedten alkalmaztak lehallgatásokat az információs előny megszerzésére. A SIGINT-eszközrendszer fejlődése követte az információtovábbításra használt technológia fejlődését.

A **SIGINT-technológiák** a mai komplex kommunikációs környezetben is megőrizték szerepüket az információszerző módszerek között. Az eszköztárt a következők jellemzik:

Előnyök:

- hatékony, olcsó információszerzés;
- kockázatmentes.

Hátrányok:

- az adatcsatornához való hozzáférés is nehéz lehet;
- követni kell a távközlési technológiák fejlődését;
- a szűrés, elemzés, válogatás, szintézis komoly elvi és gyakorlati problémákat vet fel;
- beruházás- és szaktudásigényes tevékenység.

Arra törekszem, hogy a távközlési és rejtjelzési technológiák fejlődésének együttes hatásaként napjainkra kialakuló helyzet néhány aspektusát bemutassam.

Az informatika fejlődése

Az informatika fejlődése több szálon is szoros kapcsolatban van a hírszerzési lehetőségekkel. Az alábbiakban felvázoljuk a leglényegesebb informatikai mérföldköveket:

1943-1944 – Colossus, az első – részben programozható, de még nem Turing–teljes számítógép.

1946 – ENIAC

1951 – UNIVAC

1971 – Megjelenik az Intel 4004 processzora, négybites regiszterekkel.

1969 – Arpanet, az Internet magja.

1990 – Windows 3.0

1991 – *„Hello everybody out there using minix – I'm doing a (free) operating system (just a hobby, won't be big and professional like gnu) for 386(486) AT clones.”* – írta Linus Torwalds, elindítva ezzel a Linux ma is tartó térhódítását.

1993 – Windows NT

WWW, hipertext, Tim Berners-Lee.

1994 – Megjelent a Linux kernel 1.0 változata, és Netscape Navigator 1.0 is, amely akkor nagy technológiai ugrást jelentett, s tömegek számára tette érdekesebbé az Internetet.

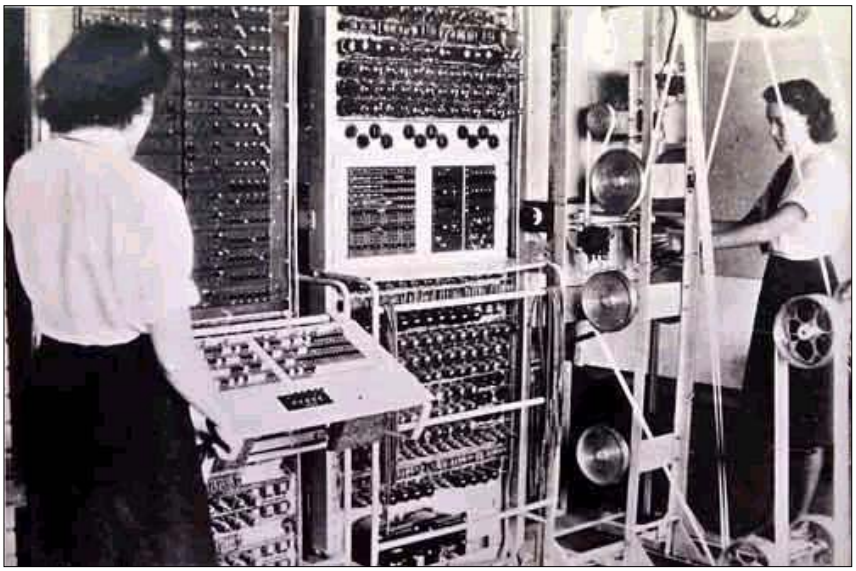
1995 – Internet (TCP/IP) áttörés, az Interneten elérhető hoszt-szerverek száma exponenciálisan növekszik.

Windows 95 beépített TCP/IP stack.

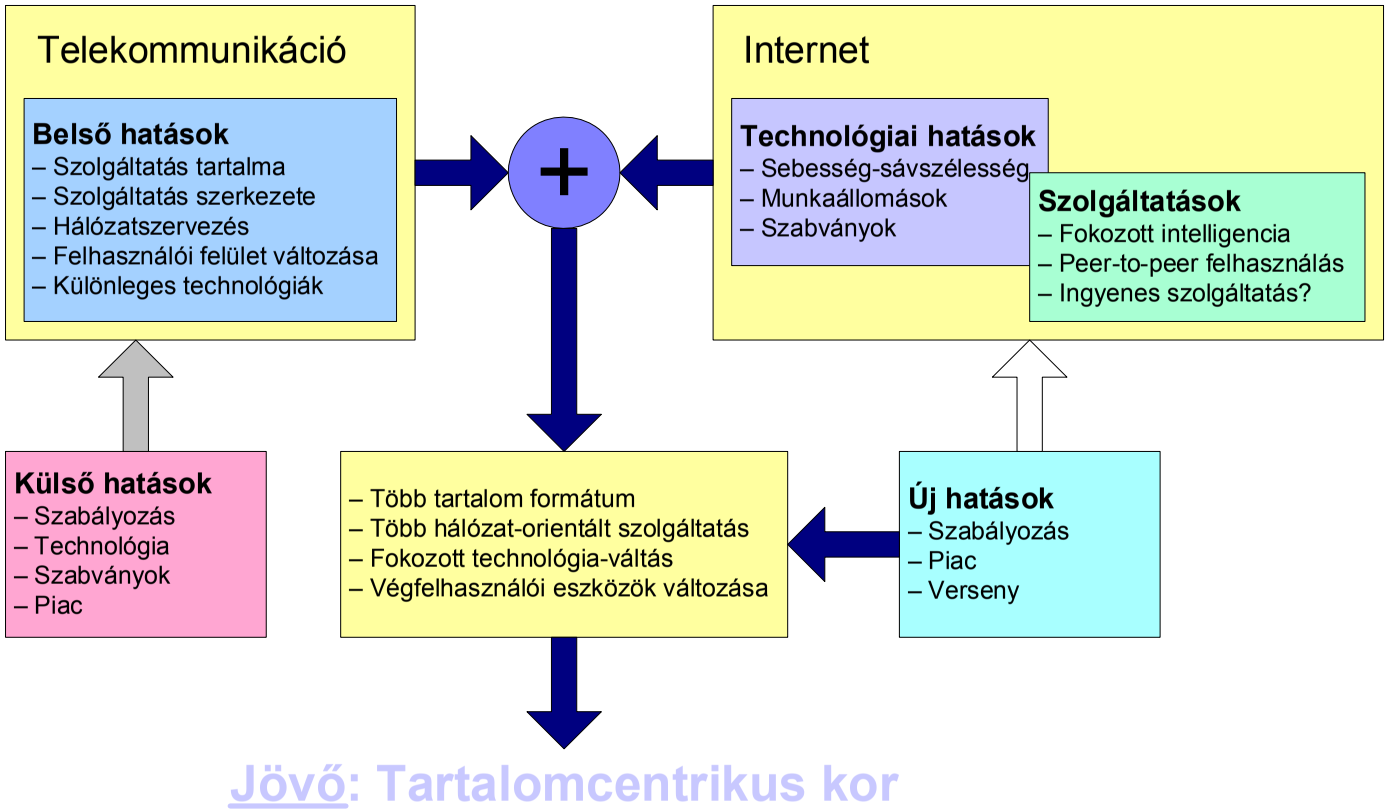
1996 – 200 MHz Pentium.

2005 – AMD Athlon X2, kétmagos, 64 bites.

2007 – Windows Vista.



1. ábra. A Colossus computer



2. ábra. A telekommunikáció és az informatika

A számítástechnikai eszközök és technológiák forradalmi fejlődése visszahatott a távközlési technológiákra is. Több más, mondandónk szempontjából kevésbé fontos hatás mellett kiemelem az alábbiakat:

- az eszközök árának csökkenése extra kommunikációs igényeket generált, pont–pont közötti dedikált digitális kapcsolatok létrejöttét segítette;
- az Internet terjedése és a technológiai szinten jelentkező konvergencia jelentős fejlesztési igényt hozott létre a távközlési kapacitások növelésére.

A távközlési technológiák fejlődése

A távközlési technológiák fejlődésének felvázolása – a rádiótávírótól napjainkig –, meghaladja e cikk lehetőségeit. Néhány címszó csupán:

- **vezetékes:**
  - Circuit switching,
  - private line,
  - packet switching,
  - CCS7,
  - Active Networks.
- **vezeték nélküli:**
  - Cellular,
  - Smart Phones,
  - PDAs,
  - PCs,
  - satellites,
  - fixed wireless loops,
  - Wireless LANs,
  - Wireless Trunking (LMCS).
- **széles sávú:**
  - ADSL,
  - Cable Modems,
  - LMCS,
  - B-ISDN,
  - ATM,
  - Frame Relay,
  - Fiber Optical.
- **multimédia:**
  - Voice,
  - data,
  - video,
  - digital imaging,
  - Internet & Web based.

Mint azt már korábban is említettük, a telekommunikációs és informatikai technológiák konvergenciája mellett a két terület szinergikusan is hat egymásra, kölcsönösen gyorsítva egymás fejlődését.

Külön kiemelendő tendencia az optikai hálózatok térnyerése. Az optikai hálózatok kialakulását segítette a két terület egymást gerjesztő hatása. A tőzsdei internet-boom idején hatalmas pluszkapacitások épültek ki, ezeken a hálózatokon ma nyomott piaci áron, költséghatékonyan lehet forgalmat bonyolítani, szinte függetlenül annak jellegétől.

Az üvegszál-alapú földi hálózat tehát:

- olcsó;
- hatalmas többletkapacitások épültek ki;
- kiszorítja a műholdas kommunikációt;
- egy ország (földrajzi hely) SIGINT-megfigyelői számára már elvileg is csak a kommunikáció egyre kisebb hányada érhető el.

A műholdas kommunikáció térvesztése szinte törvényszerű, hiszen azonos minőség, olcsóbb ár mellett nagyon sok alkalmazásnál zavaró a műhold távolságából adódó késleltetés.

A SIGINT szempontjából ez a lehetőségek korlátozását jelenti, hiszen a műholdas kommunikációs nagy területről hozzáférhető a lehallgatást végző számára, míg az optikai hálózat alkalmazása esetén elvileg is csak a saját területén elérhető forgalmat tudja megszerezni a támadó.

A kriptográfia terjedésének néhány mérföldköve

A SIGINT lehetőségeinek újabb korlátját jelenti a kriptográfiai eszköztár széles körű elterjedése. Tekintsük át a mai helyzethez vezető folyamat főbb lépéseit:

1948 – Claude Shannon megírja híres cikkét, amely megalapozza az információelméletet.

1967 – Kiadják David Kahn *The Codebreakers* című könyvét.

1974 – Feistel feltalálja a róla elnevezett algoritmus struktúrát.

1976 – A Data Encryption Standard hivatalos FIPS szabvánnyá válik.

Diffie és Hellman megjelenteti a *New Directions in Cryptography* című cikkét.

1977 – Megszületik az RSA algoritmus.

1981 – Richard Feynman felveti a kvantumszámítógép ötletét.

Az első CRYPTO konferencia.

1982 – Az első EUROCRYPT konferencia.

1991 – Phil Zimmermann elkészíti a PGP-t, és forráskóddal együtt nyilvánosságra hozza.

1994 – A Secure Sockets Layer (SSL) protokollt elkészíti a Netscape.

Az RC4 nyilvánosságra kerül.

1995 – Az NSA kiadja az SHA1 hash függvény és a Digital Signature Standard specifikációját.

Az IPSEC megjelenése RFC-ként (RFC 1825–1829).

1997 – Megjelenik az Open PGP (RFC 2440).

2000 – Lazulnak az amerikai exportkorlátozások.

Az RSA algoritmus része lesz a public domain-nek, azaz bárki ingyen használhatja.

2001 – Advanced Encryption Standard (AES), az új, biztonságos rejtjelző algoritmus-szabvány.

2002 – NESSIE, az Európai Unió programja közös kriptográfiai alapelemek kidolgozására.

Az áttekintett időszakban a kriptográfia egy titkos, zárt tudományból része lett informatikai mindennapjainknak. Az amerikai exportkorlátozási kísérletek kudarca után ma mindenki hozzájuthat olyan kriptográfiai alap-építőkövekhez, amelyek a tudomány mai állása szerint biztonságosak, sőt több-kevesebb bizonyossággal azt is meg lehet becsülni, hogy mi az, amire biztosan nem képes a rejtjelfejtés zárt, nem publikus világa sem.

A kriptográfiai eszközök alkalmazhatóságának másik szintjét jelenti az, hogy ezek a módszerek nemcsak elvi szinten, hanem forráskódban és végrehajtható formában egyaránt rendelkezésre állnak. Jó példa erre a PGP, az Open PGP, és az Open SSL projekt is.

A kriptográfiai eszközök elérhetőségének harmadik szintjét az jelenti, hogy a rejtjelzési eszközök alkalmazás-szinten is megjelennek, beépítve kommunikáció eszközeinkbe, a kommunikációs protokollba. Használatukhoz csupán be kell kapcsolni egy opciót. Ez a tény önmagában jelentősen korlátozhatja a SIGINT-ben rejlő lehetőségeket. Lassíthatja ezt a folyamatot, hogy a kriptográfia alkalmazása jelenthet kulcskezelési terhet, továbbá problémát a működtető szervezetnek mind technikai mind szervezeti, szabályozási szempontból.

A kriptográfiai módszerek megkerülésére elvi lehetőséget adhatnak a rejtjelzési rendszerben használt kriptográfiai vagy implementálási hibák. Elmondható, hogy egy új protokoll, egy új implementáció meglehetősen hosszú idő, esetenként több év alatt válik kiforrottá, hibamentessé.

Néhány példa a protokollhibákra:

2000 – PGP alkalmazáshiba 5.5-től 6.5.3-ig.

Kulcsgenerálási hiba a PGP 5.0-ban, kicsi a kulcs szabadsági foka.

2002 – Tanúsítvány-ellenőrzési hiba az Internet Explorerben.

2005 – IPSEC protokoll alkalmazáshiba.

Implementálási hiba a Word és az Excel által használt rejtjelzésben.

Összegzés

A SIGINT-eszközök alkalmazása ma is fajlagosan olcsó, hatékony hírszerzési eszközrendszer. Alkalmazását megnehezítette ugyan a kriptográfia elterjedése és ugyanebbe az irányba mutat a távközlési hálózatok, útvonalak átstrukturálódása is, de ezeket a hatásokat kompenzálja, hogy a műholdas kommunikáció aránya továbbra is jelentős, s esetenként a kriptográfia alkalmazása is megkerülhető. Emellett a továbbított információ mennyisége exponenciálisan növekszik, ami szintén javítja a SIGINT-eszközrendszer hatékonyságát.

GYEBROVSZKI TAMÁS ALEZREDES

A RÖVIDHULLÁMÚ COMINT ÚJ KIHÍVÁSAI

Beléptünk az információs korba, amelynek sajátos szabályait elfogadva tevékenykedünk. Csak nézzünk magunkra és a maroktelefonunkra! Gépkocsivezetés közben is telefonálunk, és folyamatosan tájékoztatást kapunk. A távközlési infrastruktúra folyamatos fejlődése igen sok gátat döntött le az elmúlt tíz évben, ami nagy megelégedést váltott ki a gazdasági szereplők körében és a magánszférában. A napokban döntötték meg a SMS-írás sebességének világcsúcsát. Hét éve még nem ismertünk ilyen csúcsot.

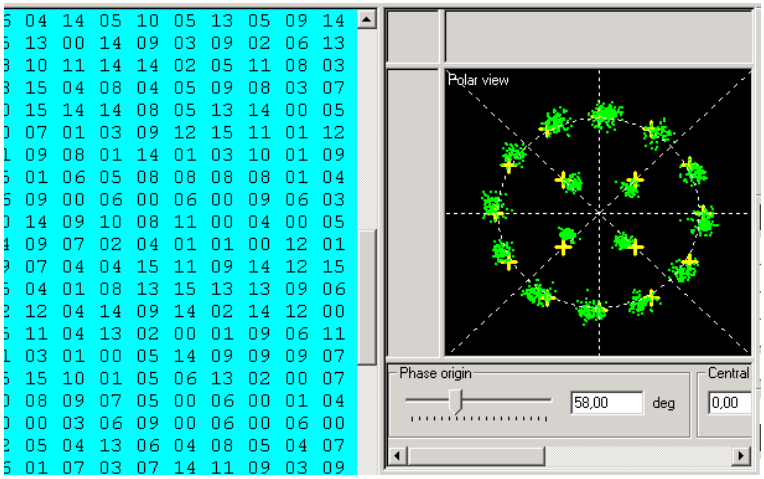
A nemzetbiztonsági szolgálatok tevékenységi körébe tartozik a távközlési hálózatokból, megrendelésre történő adatgyűjtés, így a szolgálatok kötelesek a fejlődést követni.

Az adatszerzés egyik részterülete a rövidhullámú rádiófelderítés (HF-COMINT). Általában elavult távközlési módnak tekintik, de messzemenően nem az, ugyanis képes nagy távolságokat áthidalva, stratégiai szintű híranyag beszerzésére.

A rövidhullámú rádiótávközlés jelenleg bithibátlan adatátvitelre is képes, a multimédia-alkalmazások kivételével a legtöbb igény kielégítésére alkalmas.

Az új ajánlások és szabványok alkalmazásában rejlő lehetőségek kiaknázása az 1990-es évek végére olyan megoldásokat hozott létre, amely az Y2K félelem miatt beindított fejlesztésekre reális választ adott. 1995 és 2000 között több mint 50 ország hajtott végre fejlesztést stratégiai távközlési rendszereiben, amelyek során a rövidhullámú hírrendszerekre nagy hangsúlyt fektettek.

A számtalan új adásmód megjelenése meglepte a COMINT szakterületeket. Az ismeretlen jelek elemzésére alkalmas **technikai elemzés** új feladatai sokasodtak, ennek kapcsán eszközeik fejlődtek. A kilencvenes években a szögmoduláció nem volt széles körű használatban a rövidhullámon, míg 2000-re robbanásszerűen elterjedt. A technikai elemzés képes meghatározni a lényeges ismérveket, amelyek alapján a szakemberek a szükséges erőforrás-allokációt elvégezhetik. Az 1. ábrán egy QAM–16 modulációs móddal rendelkező adás valós időn túli demodulációja látható.



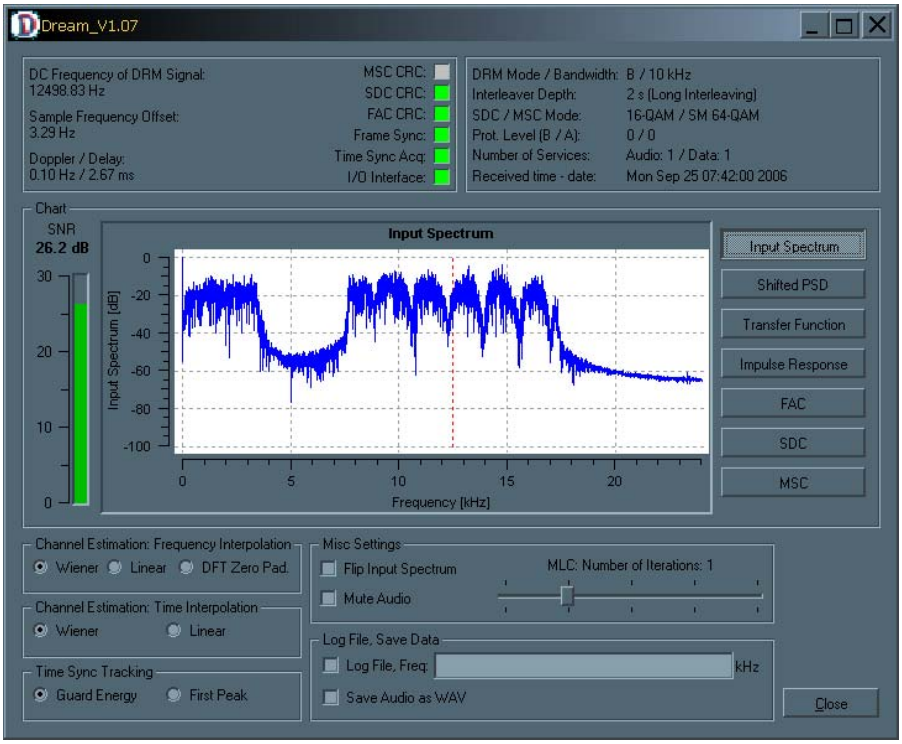
1. ábra. QAM–16 moduláció

A fejlődés lényeges állomása a bithibátlan átvitel, valamint az adatátvitel sebességének nagy mérvű emelése volt. Ezek a lépcsőfokok néhány specifikumtól eltekintve nyomon követhetők voltak.

Így például a QAM–64 moduláció több mint száz vivővel történő alkalmazása jól érzékelteti az egyvivős, távgépíró-átvitel korszerűtlensége közötti technológiai fejlettségbeni szakadékot. A vételtechnikában nagy hangsúlyt fektetnek a fading-hatások kiküszöbölésére, valamint az összeköttetések tervezésére és a csatorna használhatóságának valós idejű ellenőrzésére.

A továbbfejlődés elsősorban a sávszélesség hatékonyabb felhasználásában rejlik. A sávszélesség emelésének az elméleti határát 50–70 kHz közöttinek tartom. Ennek első lépéseként, 2008-ban a 12 kHz-es sávszélességű adások elterjedése várható.

Jó példaként hozható fel a DRM (Digital Radio Mondiale) – a digitális műsorszórás egyik technológiája –, ami elsősorban a 30 MHz alatti (RH, KH, HH) sávtartományokban képes magas minőségű műsorszolgáltatásra és egyebekre, de akár a 67–107 MHz-es sávokban is alkalmas az FM műsorszórás leváltására, a DAB-bal karöltve. A DRM több mint 100 COFDM-modulált vivője akár 24 kbit/s átviteli sebessége és igen gazdaságos sugárzási lehetőségei miatt elterjedését 2010-re valószínűsítem. A 2. ábra a Dream-szoftveres DRM-vevő Evaluation modulját mutatja, ahol egy erős fadinggel terhelt adást látunk, kitűnő hangminőség mellett.



2. ábra. DRM-vevő Evaluation modulja

Mit tegyen ebben a változó környezetben a COMINT terület? Elsősorban a technikai elemzés erősítése, az észlelés sebességének növelése, valamint a technológiai fejlődés követése a fontos.

A sikeres fejlesztések megismerése kulcsfontosságú feladat. Így nem hagyható figyelmen kívül az eleinte rádióamatőr célokra készült fejlesztések piaci változatainak figyelemmel kísérése. Így például a PACTOR és a CLOVER adástípusok sikertörténete, amelyek mindegyike egy-egy rádióamatőr saját elképzelésének megvalósításaként indult, majd a SCS Gmbh., illetve a HAL Ltd. cégek érdeklődését felkeltve vezették be a piacra.

A 3. ábrán egy olyan modemet látunk, amelyet **bárki** megvásárolhat, és teljesen függetlenül, nagy távolságú adatátvitelt végezhet, akár a szolgálatok látóköréből is kikerülve.

3. ábra. PACTOR modem

Ezenkívül a nyílt szabványokat megvalósító modemek alkalmazása, az azokkal kapcsolatos elemző tevékenység megnövekedése súlyponti kérdéssé vált. Egyszerűbb a feladatvégzés irányítása, ha az elemzések más kvázi-online történnek, csak az ismeretlen adásmódok elemzése történik valós időn túl.

A kapcsolatteremtő, szelektív hívó eljárások nagyfokú fejlődése messzemenően hozzájárult a rövidhullámú sávtartomány hatékony alkalmazásához, ami további feladatokat ró a COMINT területre. Az észlelés után azonnali döntések szükségesek, ami a valós idejű feldolgozás és a valós időn túli feldolgozás ésszerű ötvözetének alkalmazását teszi szükségessé.

Az észlelés sebessége fontos paraméter bizonyos rendszerekben. A rövidhullámú adatszerzésben napjainkban általában nincs szükség a valósidejűségre. Ez azért van így, mert technológiailag lehetséges a keresés nélküli módszerek alkalmazása, ami a széles sávú és a teljes sávú vétel megvalósítását jelenti. Ez nem azt jelenti, hogy nem kell a jelet megkeresni, hanem azt, hogy a keresésre fordított idő nem lényeges szempont, mert nem mulasztjuk el az adatszerzést, hiszen valós időn túl, bármikor kinyerhető a kívánt adás forgalma.

Lényeges azonban az a kérdés, hogy az adatszerzés melyik OSI szintig tartson. Ez azért fontos, mert a fizikai csatornában megjelenő adás – a bonyolult modulációs módon és kódoláson túlmenően – adaptivitást és tömörítést alkalmaz, valamint rejtjelzi közleményét. Nyilvánvaló hogy a rejtjelzés felismeréséig tart az adatszerzés, ami azt jelenti, hogy roppant fontos a technikai elemzés további fejlesztése.

NÉMETH ZSOLT

HARCÁSZATI RÁDIÓFELDERÍTŐ ESZKÖZÖK

A Rohde & Schwarz Rádiómonitoring Divízió (München) termékcsaládjait a védelmi és békefenntartó erők, speciális kormányzati szervezetek, kormányzati frekvenciagazdálkodási és hírközlési hatóságok világszerte széles körben alkalmazzák. A rádiófelderítésben alkalmazott termékeink: antennák, felderítővevők, rádió-iránymérők, jelanalizátorok, egyéb rendszerkomponensek, a felhasználó igényei szerint kialakított alrendszerek, illetve kulcsrakész rendszerek.

Az előadás a professzionális rádiófrekvenciás szakterületen szerzett, sok évtizedes tapasztalatokon alapuló legújabb fejlesztésű, az elektronikai harcászatban alkalmazható rádiófelderítő eszközeinket és rendszereinket mutatja be, a teljesség igénye nélkül.

Felderítővevők

1. ábra. R&S EB200
széles sávú, hordozható, akkumulátoros üzemű vevőkészülék

2. ábra. R&S EM010 és R&S EM050
RH és VHF/UHF, VXI interfész-alapú vevőmodulok a R&S AMMOS rendszerhez

3. ábra. R&S EM510 és R&S EM550
RH és VHF/UHF multifunkciós széles sávú vevőkészülékek

1. táblázat

A felderítővevők alkalmazási területei és főbb rádiófrekvenciás jellemzői

	EB200	EM010	EM050	EM550
	Manpack	VXI plug-in module		Rackm.
Applications	H/V/UHF	HF	V/UHF	
Freq. range	10k - 3GHz	300Hz - 30MHz	20M-3,6GHz	
Freq.resolution	1 Hz			
typ. NF	14 dB	8 - 17 dB	12-17 dB	
Synth. set time	max. 3 ms	max. 10 ms	typ. 1ms	
IF BW	150Hz - 1 MHz	52 Hz - 20 kHz	150 Hz - 10 MHz	
Demodulation	AM,FM,USB,LSB,CW			
		ISB	ISB,PM,PULSE,I/Q, TV(an)	

Rádiófekvenciás iránymérő berendezések

4. ábra. R&S DDF195
RH és VHF/UHF kompakt felderítő rádió-iránymérő berendezés

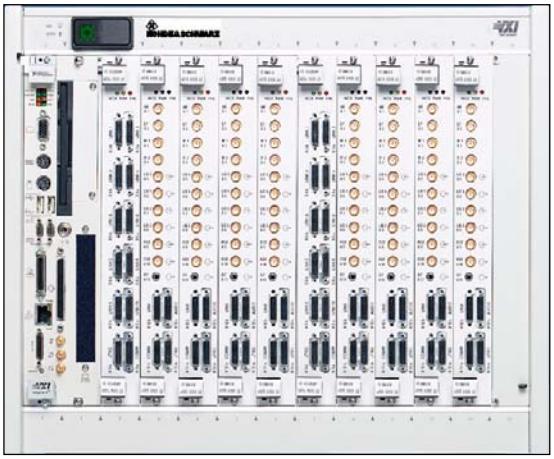
5. ábra. R&S DDF0xA
RH és VHF/UHF széles sávú, gyors letapogatású rádió-iránymérő berendezés

2. táblázat

Az iránymérők alkalmazási területei és főbb rádiófrekvenciás jellemzői

	DDF195	DDF0xA
Applications	H/V/UHF	
Freq. range	500kHz - 3 GHz	300kHz - 3 GHz
Freq.resolution	1 Hz	
Methods	Correlative Interferometer: less DF error Watson-Watt: higher DF/scan speed	
Min. signal duration = f(BW settings)	10 ms	Corr.I. : 0.35 ms W.W.: 0.15 ms
IF BW	250Hz - 100kHz	600 Hz - 150 kHz
Instrument DF acc.	1° RMS	0,5° RMS

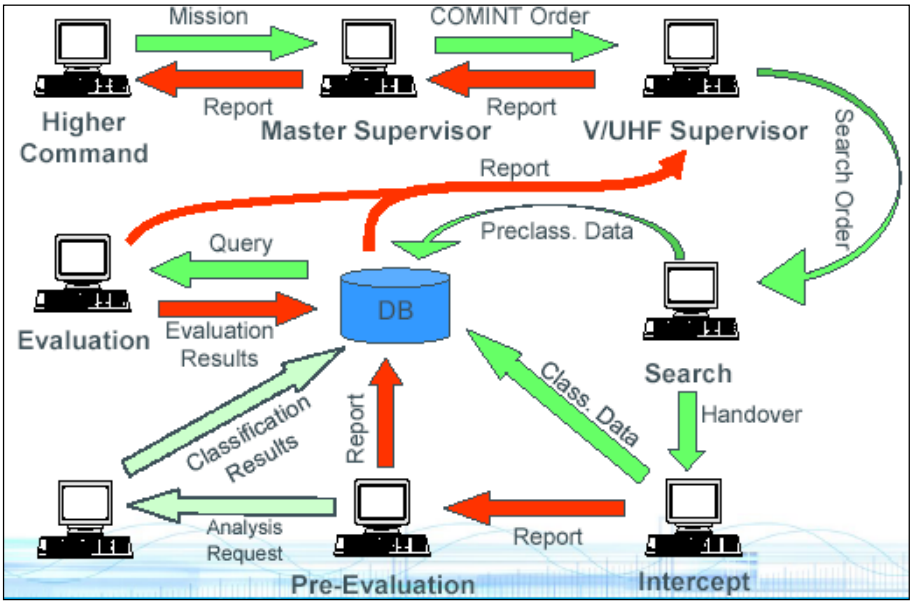
A Rohde & Schwarz komplex rádiófelderítő rendszerei



6. ábra. R&S AMMOS
automatikus moduláris rádiófelderítő és analizáló rendszer

A nagy érzékenységű és széles sávú jeldetektálás, jelanalízis és jelarchiválás többcsatornás moduláris rendszere – kliens–szerver alapú rendszer – moduláris rádiófrekvenciás felderítő munkaállomásokból, kiértékelő munkaállomásokból és digitális jelrögzítő egységekből áll. Az RF felderítő-állomások VXI interfészes rack-vevőmodulokat, digitális jelfeldolgozó DSP-modulokat, illetve rendszervezérlőt tartalmaznak. A 2. ábrán az RF VXI interfész-alapú szenzoregység látható. A felderítőállomások frekvenciatartománya 300 Hz-től 3,6 GHz-ig terjedhet. A szenzoregységek a DSP-modulok számától függően egyidejűleg más-más és teljes mértékben automatizált feladatokat hajtanak végre a R&S AMMOS-IT algoritmusok futtatásával: jeldetektálást a fixfrekvenciás állandó jelektől az impulzusjellegű, frekvenciaugratásos és folyamatosan változó vivőjű jelekig, automatikus modulációanalízist és dekódolást. A vett jelek digitális KF adatfolyama hosszú időtartamokban felvehető a R&S AMREC típusú merevlemezes tárolóeszközökre. A rögzített KF adatfolyamok a R&S AMLAB analizátor-munkaállomásokon off-line üzemmódban is kiértékelhetők. A jelfelderítési, demodulálási, dekódolási, rögzítési és adatbázis alapú kiértékelési folyamatok adaptívak és igény szerint változtathatók, valamint ún. rutineljárásokba menthetők.

A moduláris felépítésnek köszönhetően bármely rádiófelderítési alkalmazási igényt kielégít, az egyállomásos kiviteltől az osztott, többszintű stratégiai és harcászati felderítő-, illetve kiértékelő-hálózat biztosításáig.



7. ábra. R&S RAMON
harcászati rádiófelderítést és a hatékony kiértékelést biztosító rendszerszoftver

Feladatai a rádiófelderítő-bevetéstervezés, a jelfelderítés és iránymérés eredményeinek rögzítése, a felderített jelforrások települési körzetének meghatározása, a jelek előkiértékelése, igény szerinti technikai analízise, összehasonlítása az adatbázisban már rendelkezésre álló előző felderítési adatokkal és az erről készített jelentések továbbítása a magasabbegységekhez. A jelentések részletes és átfogó képet nyújtanak az aktuális rádióelektronikai harcászati helyzetről. A rendszerszoftver egyes moduljai, a feladatkörökkel összhangban, a különböző feladatkörű munkaállomásokon üzemelnek, komplex EW harcászati hálózati alkalmazást alkotva. A 7. ábra a különböző feladatkörű munkaállomások R&S RAMON rendszerszoftver által biztosított információcseréjének folyamatait szemlélteti. A felderítőállomásokra a R&S AMMOS-IT szoftvermoduljai is integrálhatók, egységes rendszert képezve.

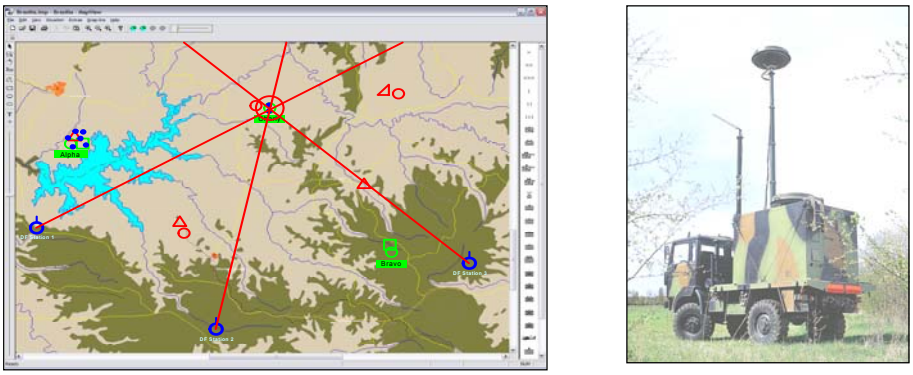
A rendszercsalád nagy hatékonysággal használható harcászati mélységben tevékenykedő erők rádiókommunikációs eszközeinek, állomásainak felderítésére, megfigyelésére és települési körzetük meghatározására, valamint a megszerzett mérési adatok rendszerezésére és kiértékelésére. A rendszert alkotó rádióelektronikai felderítő, megfigyelő berendezések a hozzájuk csatlakoztatható antennákkal a vizsgálni kívánt rövid és ultrarövid hullámhosszú frekvenciasávot teljes egészében lefedik (8. ábra).

8. ábra. R&S TMSR
mobil harcászati rádiófelderítő- és rádió-iránymérő állomások

A rendszer a hadműveleti területen, gépjárműfedélzeti vagy fix telepítésű felderítőállomásokból építhető ki, amelyek között az információforgalmat vezetékes, GSM, vagy harcászati rádiót alkalmazó adatcsatornák biztosítják, egy harcászati informatikai hálózatot képezve.

A felderítőállomások alapkiépítésben R&S EB200 típusú gyorskereső felderítővevőt, R&S DDF195 típusú rádió-iránymérő berendezést, valamint a vezérlésüket ellátó laptop-számítógépet és kommunikációs felületet tartalmaznak. A rendszer elemei és azok kiépítése a terepen történő alkalmazás időjárási- és mechanikai igénybevételi követelményeinek is teljes mértékben megfelelnek.

A hordozható felderítővevő a rendszerből gyorsan és egyszerűen kivehető, így kézi iránykereső antennával együtt közeltéri és épületeken belüli keresésre is felhasználható. A modulfelépítésű R&S RAMON vezérlőszoftver szintén a speciális harcászati jellegű rádiófelderítési feladatokra szabott, segítségével előre meghatározott feladatok futtatása és a megfigyelt kommunikáció digitális rögzítése, archiválása is végrehajtható.



9. ábra. R&S ScanLock
mobil nagyteljesítményű és gyorsletapogatású rádiófelderítő- és rádió-iránymérő állomások

A rendszer harcászati alkalmazási köre a R&S TMSR rendszerhez hasonló. A rendszert alkotó mobil állomásokon a R&S DDF0xA típusú RH és VHF/UHF széles sávú, gyorsletapogatású rádióiránymérő berendezések működnek, melyek szinkronizált üzemmódban pásztázzák a felderítésre kijelölt frekvenciatartományokat. A szinkron üzemmód a rövid kisugárzási időtartamú jelek – kisebb mint 1 ms – hatékony és gyors iránymérését és helymeghatározását biztosítja. A felderítőállomások képességei a R&S AMMOS rendszer moduljaival és a R&S RAMON rendszerszoftver alkalmazásával tovább bővíthetők.

A bemutatott rendszerek és berendezések adatlapjai és műszaki adatai az internetről is letölthetők.

További információkat a *www.rohde-schwarz.com* internet-címen lehet találni.

FÜRJES JÁNOS MK. ŐRNAGY

A DIGITÁLIS JELFELDOLGOZÁS ALKALMAZÁSA

Bevezető

A rádiófelderítés egyik ágát a távközlési mesterséges holdról történő adatszerzés képviseli. A műholdas adatszerzés egyik kiemelkedő jelentőségű területe a távbeszélő központok közötti kis és közepes sebességű digitális távbeszélő szolgáltatások továbbítására alkalmas IDR (Intermediate Data Rate) típusú rendszerek lehallgatása, amely szolgáltatásokat az INTELSAT műholdjain találhatjuk meg. Ezek fő jellemzője, hogy általában néhányszor 10 kbit/s-tól néhányszor 10 Mbit/s körüli sebességgel történik az adattovábbítás. Ezt a sebességtartományt ha beszédre vonatkoztatjuk, akkor 1-től 480-ig terjedő csatornaszámot jelent.

A szolgáltatások indításának idején, az 1980-as évek derekán, a gazdasági szempontokat figyelembe véve egy meglehetősen drága termékről lehetett beszélni. Már akkor fokozott igény mutatkozott a távbeszélő-csatornán átvitt információk (beszélgetés, adat) valamilyen típusú valós idejű tömörítésére. Bebizonyosodott, hogy egy adott mennyiségű információ eljuttatása a forráspontból a cél irányába leghatékonyabban – mind a költségeket, mind a felhasznált energiát tekintve –, valamiféle digitális jelfeldolgozási processzus beiktatásával lehetséges, amely a lehető legnagyobb mértékű tömörítést hajtja végre az eredeti adatfolyamon. A következőkben ennek a tömörítő algoritmusnak a leírása következik.

A digitális távbeszélő-csatorna

A digitális távbeszélő-csatorna eredeti forrása mindig analóg jel, amiből a digitalizálás során keletkezik a digitális jel. A digitális jel az analóg jelből meghatározott időközönként vett mintákból áll. Az egyes minták értékét bináris kódszavak tartalmazzák.

C. E. Shannon 1948-ban készült munkájában kifejti, hogy a mintavétellel nyert diszkrét mintákból álló impulzussorozat információtartalma megegyezik az eredeti, időben folytonos analóg jel információtartalmával. Ez viszont csak bizonyos feltételek érvényesülése esetén igaz. Ezeket a feltételeket a Shannon-féle mintavételi tétel tartalmazza, miszerint a mintavételezett jelből akkor állítható vissza információveszteség nélkül az eredeti analóg jel, ha a mintavételi frekvencia (fm) legalább kétszerese az analóg jelben előforduló legmagasabb frekvenciának (fmax). A mintavételi frekvencia értékének állandónak kell lennie. Képlettel:

$$f_m > 2 * f_{max} \qquad \text{(ahol a * a szorzás jele)}$$

Az f_{max} frekvenciát Nyquist-frekvenciának is nevezik.[1]

Az emberi beszéd vizsgálata során kiderült, hogy a 300–3400 Hz-es tartományt fedi le. Ez a frekvenciatartomány alkalmas a beszéd felismerésén túl a beszélő felismerésére is (a megfelelő felharmonikus tartalom miatt). A beszéd dinamikai viszonyaiból kiderül, hogy a legkisebb és a legnagyobb jel aránya 1:4096.

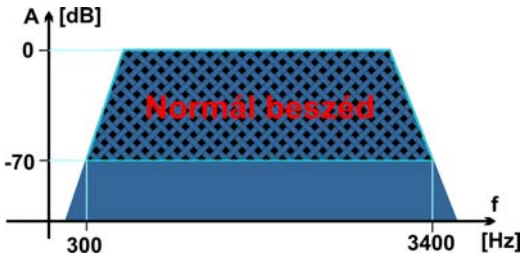
[1] http://vip.tilb.sze.hu/~wersenyi/Kiegeszites.pdf.

A dinamika jelölésére a dB érték használatos, amely :

$$20 * log_{10} (U_{kimax} / U_{kimin})$$

Ha digitális számokban szeretnénk leírni, akkor

$U_{kimax} = U_{kimin} * 2^n$, ahol n a leírására szolgáló bitek száma.

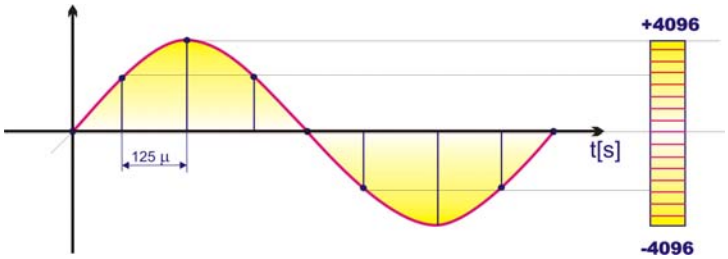


1. ábra. A beszédfrekvencia és dinamikai viszonyai

Ezen adatokat figyelembe véve a következő megállapításra jutunk:

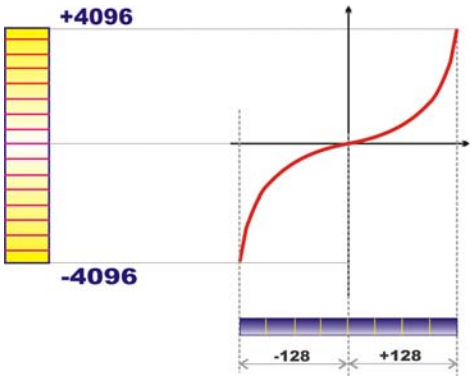
- a mintavételi frekvencia minimum 6800 Hz;
- a bináris szó szélessége 13 bit kell, hogy legyen.

A megvalósíthatóság miatt a mintavételi frekvencia értékét 8000 Hz-ben határozták meg, azaz 125 μs-ként keletkezik egy új minta.



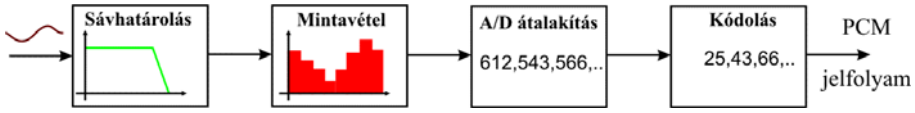
2. ábra. Digitalizálás és kvantálás

Az információ-technológiában a bináris alapú rendszerek terjedtek el, amelyeknél a 13-bites ábrázolás nem egy megszokott érték. Az emberi hallás vizsgálata során megállapítást nyert, hogy a hallás logaritmikus törvényszerűséget követ. Ezen eredmények alapján egy logaritmikus skálájú konverziót követően 8-bites minták állnak elő, amelyek mérete már jobban illeszkedik a bináris rendszerekben előforduló adatszerkezetekhez. Ennek a kódolásnak a leírása megtalálható az ITU G.711-es szabványban.



3. ábra. A-law kódolás

Összegezve az eddig leírtakat, a következőképpen működik a rendszer:



4. ábra. A digitális jelképzés egyszerűsített blokkvázlata

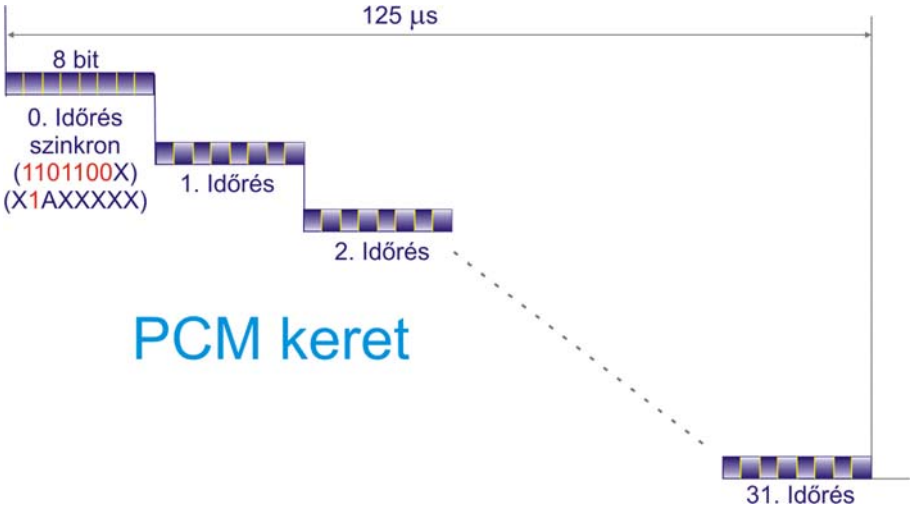
A PCM-keret szervezése

A távközlési hálózatok nem egy, hanem több felhasználó jeleit továbbítják egyszerre, ezért ennek a sokcsatornás továbbító rendszernek valamilyen módon össze kell fogni a beszédcsatorna jeleit. Ezt a módszert nevezik PCM-hierarchiának. Az alaphierarchia neve, amely 30 beszédcsatorna továbbítására alkalmas, a **primer PCM**. A PCM-struktúrában a beszédcsatornákat továbbító biteket időrésnek nevezik.

Az alábbi táblázat a különböző hierarchiaszinteken továbbított beszédcsatorna-kapacitásokat, illetve az azok átviteléhez szükséges sebességet mutatja be.

Hierarchiaszint	Jelölése	Beszédcsatornák száma	Sebesség (kbit/s)
Primer	E1	30 (32)	2 048
Szekunder	E2	120 (128)	8 448
Tercier	E3	480 (512)	34 368
Negyedrendű	E4	1920 (2048)	139 264

A beszédcsatornák számánál a zárójelben a ténylegesen továbbított érték került feltüntetésre, mivel két kitüntetett beszédcsatornát továbbítanak a beszéddel párhuzamosan. A 0. csatorna a szinkron továbbítására van fenntartva, a 16. pedig általában a csatornák közös jelzéseit továbbítják. A jelzéscsatornákban továbbítják például a telefonszámokat, a csatorna aktuális állapotát, és számos más funkciójú jelzést. A következő ábrán egy primer PCM-keret látható.



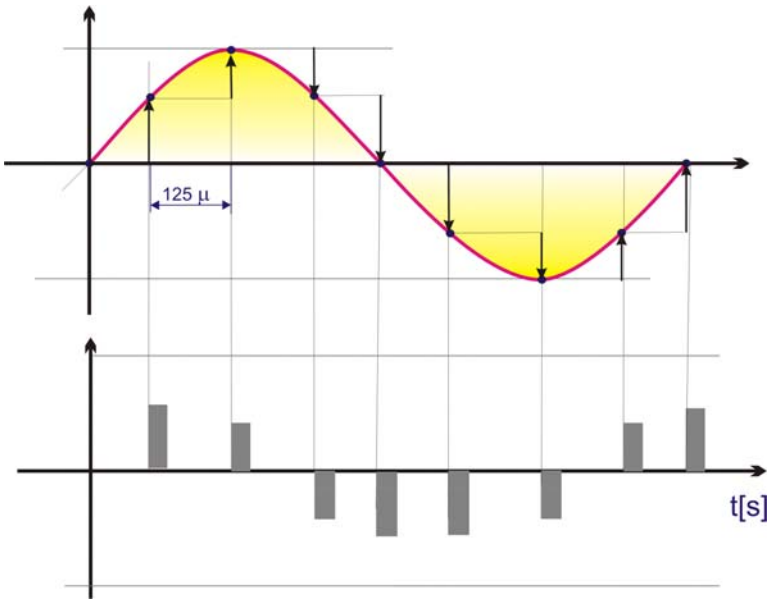
5. ábra. A normál PCM-keret

A 0. időrésben található szinkron időrés funkciója a keret elejének jelzése, amely után könnyű a megfelelő bitek összerendelése a megfelelő beszédcsatornával.

A keretek felépítésére az ITU G.704-es szabványában foglaltakat kell alkalmazni, primer és szekunder hierarchia esetén. Nagyobb sebességnél a (tercier és negyedrendűnél) az ITU G.751-es szabványa a meghatározó.

A hangtömörítés

A hangminták vizsgálata során egyértelművé vált, hogy az egymást követő minták nem teljesen függetlenek egymástól. Az aktuális minta és azt megelőző közti különbség lényegesen kisebb, mint az abszolút értékük. Tehát a jelben csak meghatározott mértékű ugrások lehetségesek. Ennek figyelembe vételével kb. 20%-os tömörítés érhető el úgy, hogy az eredeti minta információtartalma nem változik. Ezt az eljárást differenciális kódolásnak nevezzük. Jelölése: **DPCM**.

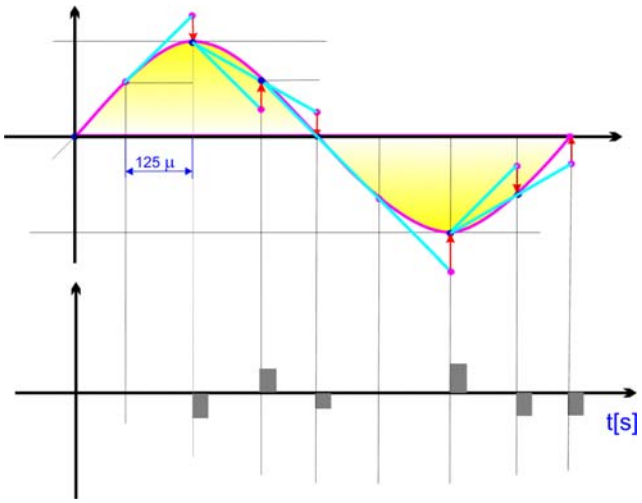


6. ábra. A differenciális kódolás

Az ábráról egyértelműen látszik, hogy az abszolút minták legnagyobb értékének kb. fele a legnagyobb különbségi minta nagysága. A tömörítés ebből adódik. Ha figyelembe vesszük a tömörítés során, hogy a minta abszolút helyétől függően változik az esetleges különbség nagysága, és ezt mintáról mintára meghatározzuk, akkor szintén nyerhetünk vele. Ezt az eljárást adaptív kvantálásnak hívjuk.

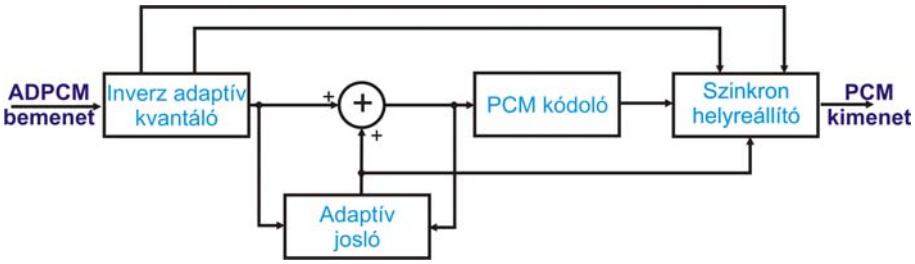
További tömörítést is elérhetünk a következő módon: feltesszük, hogy a két egymást követő minta, meghatározza a következő mintát, azaz megjósoljuk ügyesen a következő minta lehetséges értékét, viszont a jósolt és a valódi minta közti különbséget visszük csak át.

A következő ábrán egy olyan jósló algoritmust alkalmaztunk, amely a két előző mintát egy egyenessel kötötte össze. Az így kialakult egyenes és a valódi minta közti különbséget ábrázolva lényegesen kisebb adatok ábrázolását kell megvalósítani. Ha ezt kiegészítjük a helyzetfüggő adaptív kvantálással egy nagyon könnyen skálázható, viszonylag egyszerűen dekódolható eljáráshoz juthatunk. Ezt az eljárást nevezzük Adaptív Differenciális ImPulzus (C) Kód Modulációnak, rövidítve: **ADPCM**.



7. ábra. ADPCM-minták keletkezése

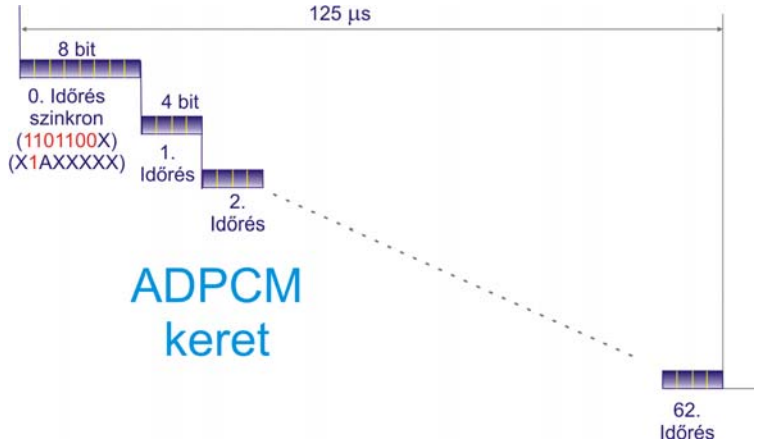
Ha egyszerűsítve szeretnénk egy blokkvázlatot rajzolni egy ADPCM kódolóról, az a következő módon nézne ki:



8. ábra. Az ADPCM kódoló

Minden egyes kódoló lényege és bonyolultsága az adaptív jósló áramköri blokk megvalósításában rejlik. Természetesen ennek a területnek is van egy ITU által jóváhagyott szabványa, nevezetesen a G.726-os.

Amennyiben az így létrehozott csatornákat fogjuk össze (4-bites kódolással), akkor az előbbi E1-es vonalon 30 beszédcsatorna helyett 60 (62) darabot tudunk átvinni. Az így felépített keret a 9. ábrán látható.



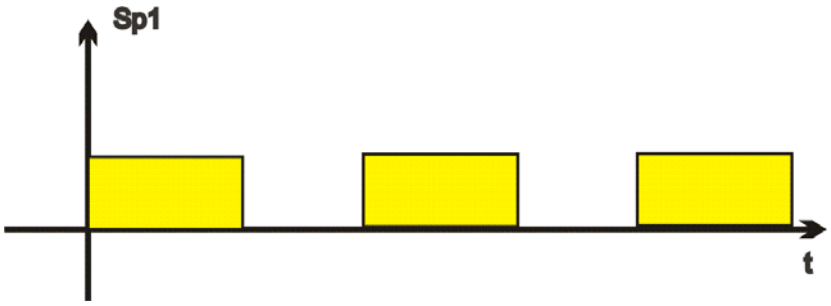
9. ábra. ADPCM-keret felépítése

Megfigyelhető, hogy a szinkron csatorna itt is megtalálható, mivel ez egy felsőbb szintű rétegen megvalósított eljárás, tehát a PCM-berendezésekkel kompatibilisnek kell lennie!

Az ADPCM skálázható eljárás, mivel a bitszám csökkentése csak a kvantálási zajt növeli, amely a normál beszédre nincs kihatással (tompábban halljuk a partnert, illetve kissé zajosabban). A modem típusú berendezések (például a FAX), érzékenyebbek ezen kvantálási zaj nagyságára, így ezeket minimum 5-bites kódolással kell továbbítani.

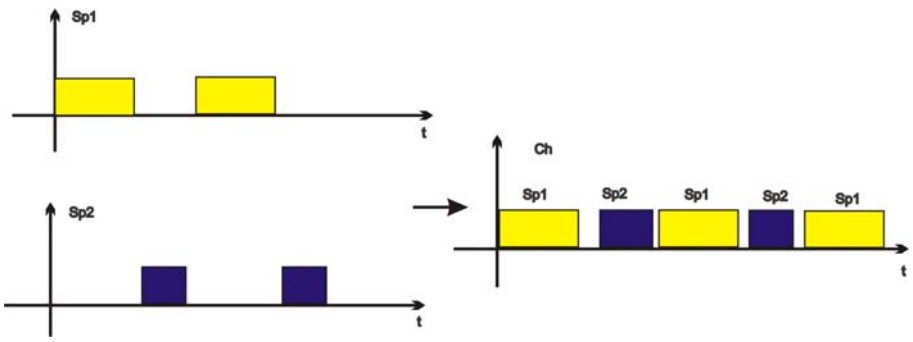
A beszéd-interpolálás

Az eddigiekben a jelre mint fizikai létezőre gondoltunk, a mögötte lévő (azt létrehozó) emberi sajátosságokat még nem vizsgáltuk. Amennyiben megvizsgáljuk egy hétköznapi párbeszéd időbeliségét, megállapíthatjuk, hogy egy beszélő a párbeszéd során 40%-ban aktív, 60%-ban passzív befogadóként nem bocsát ki magából hangot. Az idő függvényében a 10. ábrán látható egy aktivitási függvény.



10. ábra. Egy aktivitási függvény

Amennyiben sikerül egy olyan felhasználót találnunk, aki pont ellentétes aktivitással folytatja a párbeszédét, akkor e két csatornát összefoghatjuk.



11. ábra. Ellentétes beszédaktivitású csatornák összefogása

Az előzőekben vázolt eljárást nevezik beszédaktivitás-figyelésnek, vagy Digital Speech Interpolation-nak (DSI).

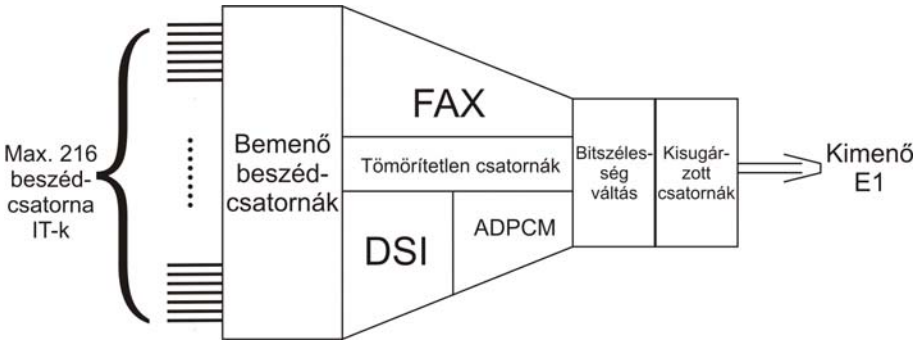
DCME (Digital Circuit Multiplicaton Equipment)

Ezzel az eljárással megtaláltuk a DCME-berendezések alapelvét. Nem történik semmi más egy ilyen típusú berendezésben, mint folyamatosan figyeljük a csatornákban folyó beszélgetéseket, és az üres (éppen passzív) csatornák helyére aktívakat kapcsolunk.

Az előző fejezetben leírtak alapján ezeknek a berendezéseknek a következő funkciókat kell megvalósítaniuk:

- beszédaktivitás-figyelés;
- ADPCM-kódolás;
- modem-demodulálás;
- adatcsatorna-áteresztés;
- bitszélesség-manipulálás;
- vezérlés.

A következő oldalon látható 12. ábra egy DCME-berendezés felépítését mutatja.



12. ábra. DCME-berendezés felépítése

A bemeneten található csatornákat IT-nek (Intermediate Trunk), nevezik. Ebből 216 darab lehet, tehát elméletileg 216 beszédcsatorna jele továbbítható egyidőben. Ha ezt a számot összevetjük a leírás elején található 30-cal, akkor megállapíthatjuk, hogy több mint 7-szeres tömörítést sikerült elérni! A kisugárzásra kerülő csatornák neve Bearer Channel, azaz **BC**.

A következő fejezetekben az eddig nem tárgyalt technológiákat ismertetem.

Modem-demoduláció, adatcsatorna-kezelés

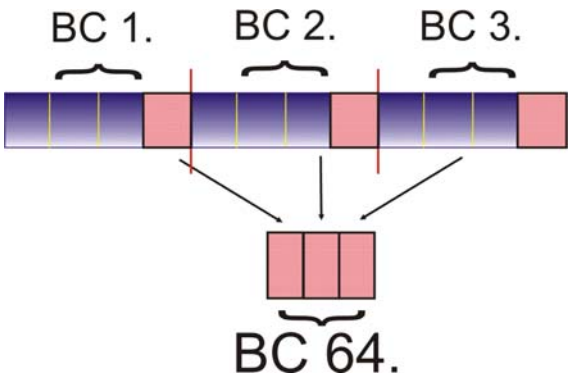
Amennyiben egy telefonhálózaton keresztül egy modem típusú berendezés (például egy FAX) jelét szeretnénk továbbítani a DCME-berendezésben, ezt el kell tudni választani a normál beszéd csatornáktól, mert ezek a jelek teljesen más paraméterekkel bírnak. Itt nem figyelhető meg a 40%-os aktivitás, mivel itt közel 100%-os! Ráadásul, amíg a beszéd tömörítésére elegendő 4-bites ADPCM-kódolást alkalmazni, addig a modemek minimum 5-bites kódolással képesek csak a kapcsolat felépítésére és fenntartására. Ennek következtében egy olyan blokkra is szükség van a DCME berendezésekben, amely elkülöníti azon csatornákat, amelyek beszélgetést tartalmaznak attól, amelyek modem típusú összeköttetést létesítenek. Amennyiben a berendezés rendelkezik FAX opcióval, akkor az adatait demodulált formában továbbítják, ahol elegendő 2 bit csatornánként (a normál FAX maximum 14,4 kbit/s sebességgel ad, amihez a 2 bit 16 kbit/s-os csatorna sávszélessége több mint elegendő). Amennyiben nem rendelkezik ilyen opcióval, akkor marad az 5-bites időrés.

Az adatcsatornák kezelése, amit **clear channel** névvel illetnek (vagy preassigned), egyszerű feladat. Itt semmilyen manipuláció és tömörítés sem engedhető meg tehát ezeket egy az egyben kell továbbítani. Ilyen típus lehet egy bérelt vonali kapcsolat.

Bitszélesség-manipulálás

Mi történik akkor, ha mindenki egyszerre beszél és még egy plusz felhasználó is szeretne beszélgetést kezdeményezni? Ekkor extra csatornákat kell kialakítani a meglévők mellé. Ezt úgy lehet elérni, hogy négy aktív csatornát négy

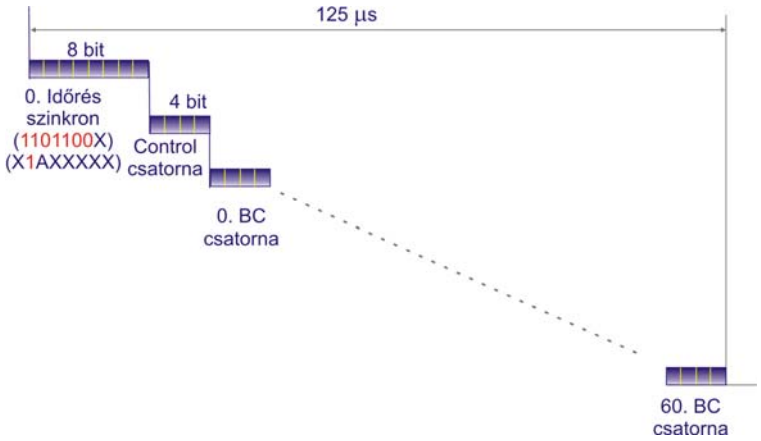
helyett 3 bittel kell kódolni (némi minőségromlás árán), és az így keletkezett biteket összefogva egy extra beszédcsatorna alakítható ki. Ezt az eljárást over-load (túlterhelés), vagy „bit-robbing” (bit-lopás) névvel illetik. Az alábbi példában az első három csatornától ellopott bitekből kerül kialakításra egy új extra csatorna, 64-es sorszámmal.



13. ábra. Bit-lopással történő extra csatorna kialakítása

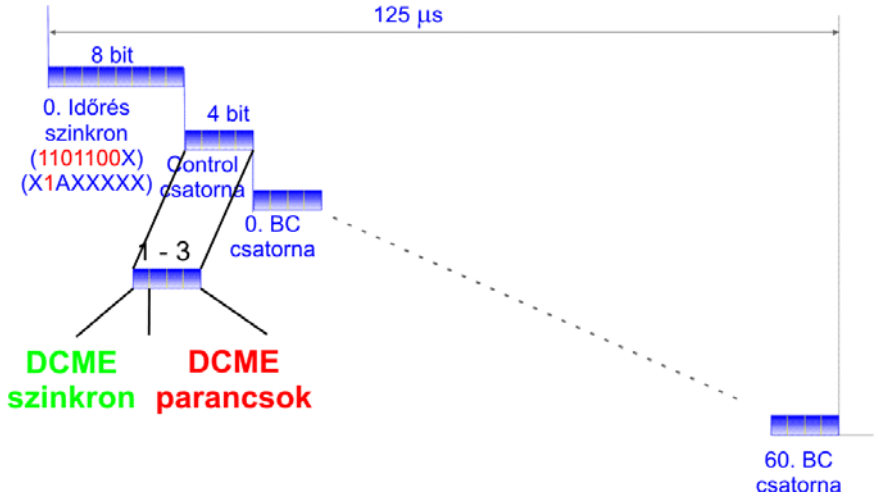
Vezérlés

Az eddig leírt eljárások csak akkor működnek, ha a vevőoldalon a dekóder egység minden lépést az adóberendezéssel szinkronban végez. Ha belép egy új beszélgető, akkor ez a másik oldalon is egy másik beszélgetőként jelenik meg (új beszédcsatorna). A DCME-berendezéseknél nincs a hagyományos értelemben vett beszédcsatorna a vonalon, hanem ún. „bearer channel”-ek lettek kialakítva. Egy DCME-berendezés jele a következő módon ágyazódik a PCM-jelfolyamba:



14. ábra. A DCME-keret felépítése

A DCME-vezérlés lényege abban határozható meg, hogy a bemenő IT csatornákat úgy ágyazza be a BC csatornákba, hogy a vevőberendezés a dekódolás végeztével 100%-ban vissza tudja állítani az eredeti IT csatorna tartalmát. Ezen vezérlés logikai helye a PCM-keretben a szinkron szó után található első 4-bites csoport. A vezérlő-, vagy kontrollcsatorna felépítése az alábbi ábrán látható:



15. ábra. Kontrollcsatorna felépítése és elhelyezkedése

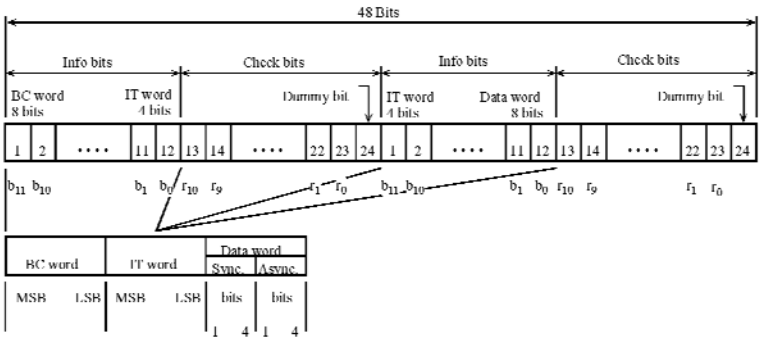
A vezérlő szó két részre osztódik:

- szinkron szó,
- parancs szó.

Természetesen ebben a csatornában is kell lennie egy szinkront biztosító mechanizmusnak, amivel meg lehet állapítani a vezérlő parancs kezdetét. Erre szolgál a szinkron szó. Minden 16. PCM-keret tartalmaz egy teljes vezérlőblokkot, ami azt jelenti, hogy 2 ms időnként történhet változás. Visszafelé gondolva, 2 ms (a másodperc 1/500-ad része) beszédszünet elég ahhoz, hogy egy másik beszélő megkaphassa a csatorna használatát!

A DCME-szinkronnak van egy különleges tulajdonsága, mégpedig az, hogy 1 keretben a 0001010011011110 bitsorozatot találjuk, a következő 63 keretben ennek negáltját, a 1110101100100001 bitsorozatot fogjuk találni. Ez azért történik így, mert bizonyos információk ebben a 64 DCME keretben vannak elosztva. (Figyeljünk oda, hogy ha PCM-keretben számolunk, akkor ez 16x64 azaz 1024 keretet jelent, ami időben 128 ms.)

A 15. ábrából látszik, hogy a vezérlő szó hossza 3x16 azaz: 48 bit, ebből 24 valódi információt tartalmazó bit és 24 hibajavító bit. A 16. ábrán ezen bitek valódi elhelyezkedését láthatjuk.

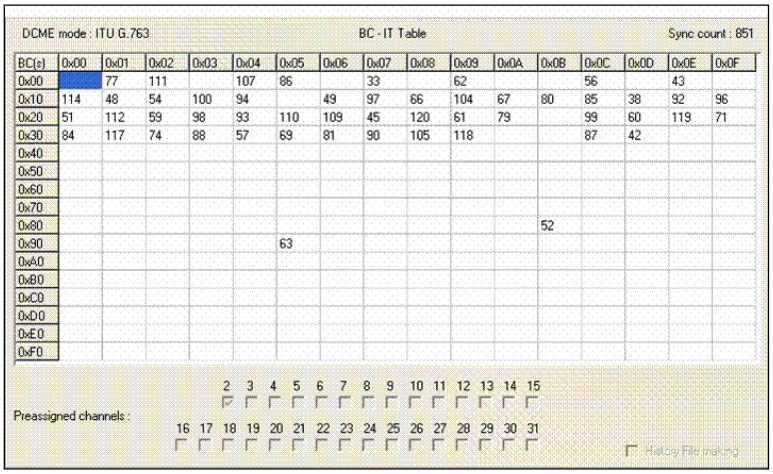


16. ábra. A DCME-vezérlőszó felépítése

A robosztus hibajavító kódolásnak köszönhetően (23, 12)-es Golay-kód, 1-3 hiba javítható, az e fölöttiek pedig detektálhatók. A hibás üzenetek nem kerülnek felhasználásra, de a rendszer általában egy állapotváltó üzenetet többször megismétel. A 24-bites kontroll-adat felépítése a következő:

- 8 bit BC szám;
- 8 bit IT szám;
- 4 bit parancs;
- 4 bit állapot.

Ebből a felsorolásból látszik, hogy ebből tudjuk helyesen visszaállítani a megfelelő BC átirányítását a megfelelő IT kimenetre. Tulajdonképpen a DCME-dekódolás legfőbb feladata, hogy az úgynevezett BC/IT tábla felépítése és ennek megfelelően irányítsa a BC adatcsomagokat a megfelelő IT kimenetre. Ezt a táblát 2 ms-onként kell frissíteni. Egy ilyen tábla pillanatnyi állapotát láthatjuk a 17. ábrán.



BC(s)	0x00	0x01	0x02	0x03	0x04	0x05	0x06	0x07	0x08	0x09	0x0A	0x0B	0x0C	0x0D	0x0E	0x0F
0x00		77	111		107	86		33		62			56		43	
0x10	114	48	54	100	94		49	97	66	104	67	80	85	38	92	96
0x20	51	112	59	98	93	110	109	45	120	61	79		99	60	119	71
0x30	84	117	74	88	57	69	81	90	105	118			87	42		
0x40																
0x50																
0x60																
0x70																
0x80												52				
0x90						63										
0xA0																
0xB0																
0xC0																
0xD0																
0xE0																
0xF0																

17. ábra. BC/IT tábla

Természetesen ezt az összekötetés-vezérlést is szabványosították, az ITU G.763-as szám alatt.

A gyakorlati megvalósítás

A 17. ábrán egy olyan programból kivágott részlet található, amely dekódolja az ITU G.763-as szabvány szerint tömörített jeleket. Ezen program egy teljesen hétköznapi PC-n (2 GHz-es P4-es processzor) valós időben képes dekódolni egy teljes E1-es jelfolyamban található DCME-jelet. Ez is mutatja, hogy a technológia kifejlesztésekor 240 cm magas állványban található kb. 30 darab diszkrét kártya jelfeldolgozási teljesítményét a mai technológia egy asztali számítógép házába zsugorította!

Összefoglalás

A távközlési mesterséges holdak rendszerbe állításának kezdetén az összeköttetések költségét a kisugárzásra került jel sávszélessége drasztikus mértékben befolyásolta. Akkor a törekvés (amely természetesen ma is igaz) az volt, hogy minél kisebb sávszélességen minél több felhasználó osztozzon. Ennek egyik, az 1980-as évek végén létrejött megvalósításával foglalkoztam, melynek neve: Digital Circuit Multiplication Equipment, röviden **DCME**. Ezen túl, a PCM-rendszerek működésének alapjait, a Multiplex-rendszerek felépítését, valamint a DCME-rendszerek PCM-hierarchiába történő integrálását tárgyaltam. Ezenkívül röviden bemutattam a DCME-berendezések működését is.

FELHASZNÁLT IRODALOM

- http://vip.tilb.sze.hu/~wersenyi/Kiegeszites.pdf
- ITU-T Recommendations ITU G.704
- ITU-T Recommendations ITU G.711
- ITU-T Recommendations ITU G.726
- ITU-T Recommendations ITU G.751
- ITU-T Recommendations ITU G.763

VISKY KÁROLY NYÁ. MK. EZREDES –
LÁSZLÓ ATTILA MK. ŐRNAGY

A VPN-HÁLÓZATOK LEHALLGATÁSÁNAK LEHETŐSÉGEI

A rádióelektronikai felderítés területén az elérhető adatforrások állandó mennyiségi és minőségi átalakuláson mennek keresztül, az aktuális feladatoknak megfelelően új irányok jelennek meg. A feladatok megoldása során az alapok változatlanok maradnak, de a rendszertechnikai felépítést tekintve a részterületek más-más műszaki megoldásokkal töltődnek fel.

Megjelentek a rádiócsatornákon elérhető számítógép-hálózatok, amelyek adott összeköttetési irányokban képesek Internet- vagy zárt hálózati forgalmat szolgáltatni az adatszerző szervezeteknek is. Korábban az adott frekvencia és üzemmódok használata, a közlemények tartalma és mennyisége egyértelművé tette, hogy katonai, diplomáciai vagy polgári forrásokkal állunk szemben. A polgári nyílt Internet-hálózaton viszont komoly szűrő- és feldolgozó-eljárások bevezetésével lehet a technikailag összetett környezetből, a többségében polgári felhasználástól eltérő értékes források jelenlétét felderíteni.

Az adatvédelem fejlődése, a számítógépek személyi és szervezeti felhasználású elterjedése, a hagyományos adatvédelmi megoldások fenntartási költségeinek viszonylagos növekedése, mind-mind az olcsóbbnak tekintett védett számítógép hálózatok egy új típusának kialakulásához vezetett. A VPN berendezések és programozási megoldások tömeges elterjedése a közfelhasználói területen, egészen az otthoni felhasználás lehetővé válásáig a legális távközlési felhasználókon kívül az Internet szürke és fekete területeiről érkezőknek, például a CCTT (Covert Channel Tunneling Tool)[1] alkalmazás, valamint a hozzá kapcsolódó és hasonló megoldások szintén lehetővé teszik az illegális, illetve esetleges terrortevékenység érdekében történő kommunikációt, a nyílt és szabad Internet felhasználásával.

A felderítő szervezeteknél egy újabb gyakorlati terület jelent meg, a DNI (Data Network Intelligence), ami egyre hangsúlyosabbá válik. A polgári távközlési hálózatok hagyományos rendszereiből származó közlemények hatékony megszerzésére, továbbá a kiválasztott és prioritással rendelkező célpontok eléréséhez a DNI esetében a DNR-hez (Dialled-Number Recognition) igen hasonló területről beszélhetünk. A megvalósíthatóság és hatékonyság itt is a jól kihasznált technikai lehetőségeken, az automatizáláson, a megfelelően megválasztott kritériumokon és érzékeny feldolgozáson múlik.

Ezen a területen a VPN-hálózatok felderítése, a hozzáférés lehetősége és képessége (jelenleg úgy tűnik) egy-egy felderítő szervezet komoly minőségi mutatója.

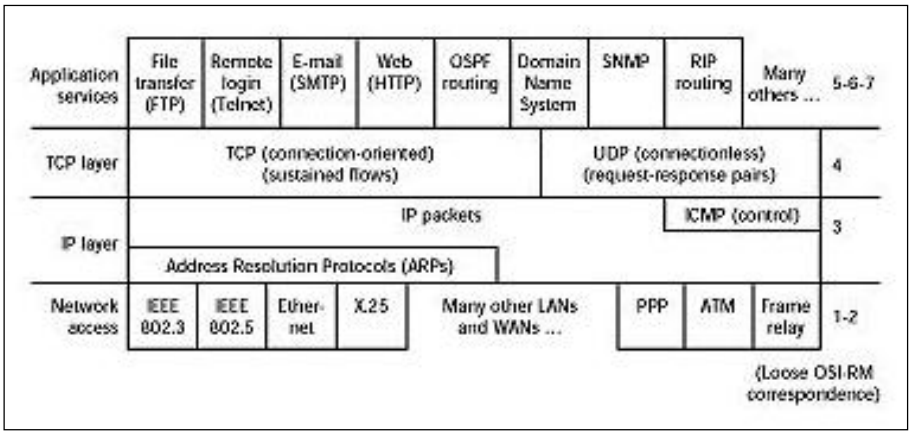
[1] CCTT – Covert Channel Tunneling Tool – rejtett/fedett csatornán alagúttechnikát megvalósító programozási eszköz; egy konkrét kedvelt hacker-megoldás.

A virtuális magánhálózatok kialakulása

Jelenleg mintegy 2000 különféle protokoll van alkalmazásban az egész világra kiterjedő Internet távközlési hálózatban. Az Internet az 1960-as évek végén az ARPANET, valamint a katonai MILNET hálózatot tekintheti közvetlen elődjének. 1993 májusától, az akkor NAP-nak (Network Access Point) nevezett rendszerösszetevőkön keresztül már kereskedelmi célra is lehet kiterjedten használni. A fejlődés olyan gyors volt, hogy ma már egy teljesen új, dominánsan polgári, nyílt hozzáférésű és technikai rendszerű hálózattá vált.

Katonai és diplomáciai területen a számítógépek adatátvitelre történő alkalmazása jelentős múltra tekint vissza. Az Interneten kívül igen sok korábbi terminál-alapú (például klasszikus VT 52, VT 100, az ún. AN/UYK-alapú Fielddata stb.) és modem-alapú összeköttetéssel találkozhatunk még ma is. A pont–pont jellegű összeköttetéseknél ezek még mindig versenyképes megoldásoknak tekinthetők. Az ARPANET-nél és a MILNET-nél megjelent csomagkapcsolás, torlódásirányítás, az elkerülő utak megjelenése, a hálózati csomópontok és azok programvezérelt megvalósítása, a statikus telepítés és az ideiglenes mobil bejelentkezés közvetlenül vezetett el a mai katonai területi hírrendszerekhez.

A protokollok „csatáját”, vagyis a rendelkezésre álló nyílt rendszerek gazdasági, műszaki és elterjedtségi versenyét az IP, azaz az Internet Protocol nyerte.



1. ábra. Alapvető fontosságú protokollok és alkalmazások modellje

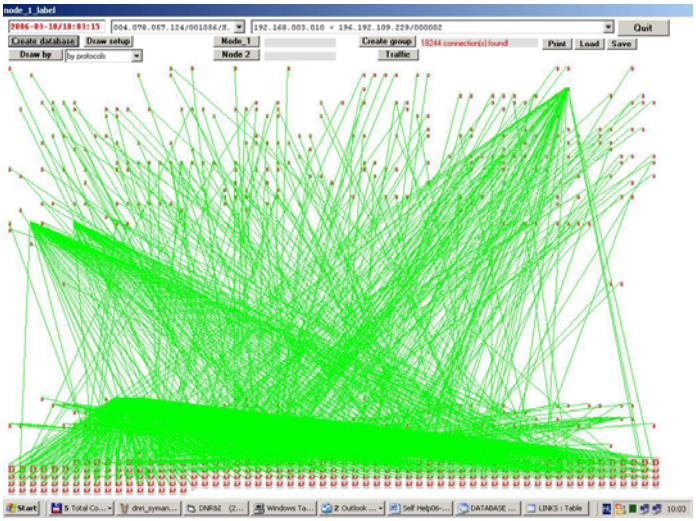
Ahhoz, hogy műszakilag egy távközlési hálózatot felépítsünk, illetve a felderítés számára adathozzáférést biztosítsunk, az 1. ábrán látható egyszerűsített modell összetevőit mindenképpen alkalmaznunk kell. Egyfajta analízis–szintézis megoldást felhasználva, a rendszerben továbbított információt közös formátumba hozva, azt részekre felbontva (tördelve, Ipv–4-nél maximum 1500 byte, X.25-nél 576 byte stb.), ezeket a modellrétegnek megfelelően hozzáadott információval ellátva, vezérelt módon továbbítva, majd a célnál a megérkező részeket hiánytalan módon egyesítve, a rendszer forráshűen szolgáltatja a továbbításra szánt adatokat.

Jelenleg a rádióelektronikai felderítő rendszerekben már megoldott a különböző forrásból (távközlési mesterséges hold, rövidhullámú rádiókészülékek) származó IP-forgalomhoz való hozzáférés. Egyetlen jelentősebb nehézséget kellett leküzdeni, a Frame Relay rendszerbe befoglalt IP-forgalom elérését, de már ezt is sikerült megoldani.

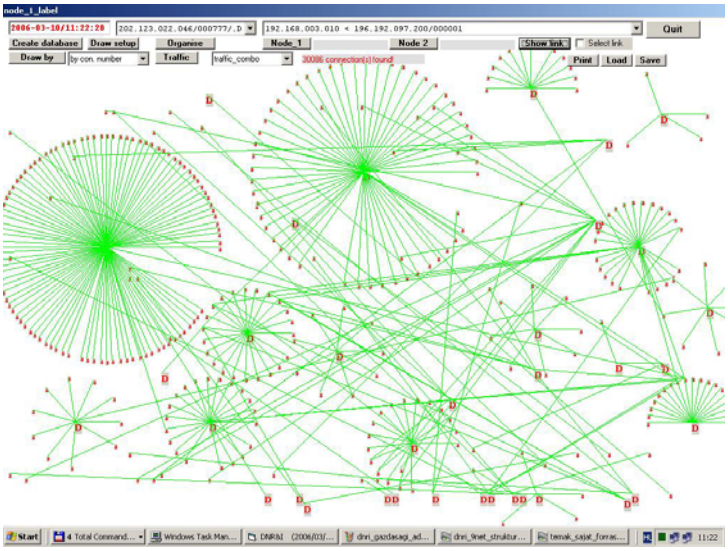
A folyamatos vétel esetén passzív módon keletkező adatmennyiség (1 db 64 kbit/s csatorna esetén napi maximum 675 Mbyte; 2Mbit/s-nél napi 21 Gbyte; 34 Mbit/s-nél 337,5 Gbyte), ha nem kerül feldolgozásra, akkor céltalanná, fizikailag tárolhatatlanná válik.

A hagyományos elemző–értékelő adatfeldolgozás alapját jelentő közleménytípusok előállításához a fragmentálási információ, illetve az IP-hálózat önvezérlése jelent nagy segítséget. A különböző vezérlési információk a közlemények előállításán túl (jelenleg kimenetként e-mail, html, pop3, http, kép, tömörített, css, xml, ftp, plain nyílt közlemények keletkeznek), a hálózatról nyújtanak kiterjedt információt.

A legelső rendezési lehetőség a címzés szerinti rendezés. A két alkalmazott címzés az Ipv–4-es és Ipv–6-os csomag változatának megfelelő forrás-célrendezés pontosabb képet ad a hálózatokról. A címtartomány egy jelentős részéhez emellett állandó felhasználói, illetve állandó földrajzi települési hely rendelhető. A hálózat olyan mértékben bővül, hogy 2010-re mintegy 1,6 milliárd IP-képes eszközzel számolnak (elsősorban számítógépek és IP-képes mobiltelefonok), s ez jelentősen nehezíti a követést, másrészt pedig a címálcázás, a címfedés (masquerading / maskirovka) és a dinamikus kiosztás (DHCP) csökkenti a címazonosítás értékét.



2/a. ábra. Nyers, rendezetlen, csak adattovábbító protokollok szerint ábrázolt hálózat, több száz csomópont, több ezer viszonylat (session), több százezer adattovábbítási esemény (connection)



2/b. ábra. Ugyanaz a hálózat, cím szerint rendezve, összevonva és strukturálva

Sokkal pontosabb képest ad a hálózatról a vezérlés feldolgozása. Az alapvető ICMP, DNS, DHCP, ARP információ mellett más minőséget biztosítanak az IP-kapcsolással, -útválasztással kapcsolatos megoldások. A helyi hálózatok összekötésére azok nagyobb kiterjedésű hálózatokba szervezésére „céleszközök" állnak rendelkezésére a hálózatokat felépítő szakembereknek: ezek a hub-ok, útválasztók (routerek), hálózati átjárók (gateway-ek), sorrendben az egyszerűbbtől a nehezebb, összetettebb felé haladva egyre több feladatot oldanak meg a működő hálózatok kialakításáért. Ezek az eszközök is hasonlóan lényeges minőségi változáson mentek át, mint a végpontokat képező számítógépek. A hálózati sebesség növekedése (Ethernet10 UTP/AUI, Ethernet100, Gigabit Ethernet 1000, Gigabit 10 000) mellett egyre bonyolultabb belső programvezérlést tettek lehetővé, majd megjelentek az autonóm beágyazott számítógépek ezekben az eszközökben, illetve az ezeket vezérlő megoldások, programok igény szerint kikerültek az általános célú számítógépekbe, így ezeket is lehet IP-kapcsolási, illetve -útválasztási célokra használni. Jelenleg a földi optikai gerinchálózat gyakorlati legnagyobb sebessége – az OC–768 rendszerben, amely például európai nagyvárosokat köt össze – 47 Gigabit/s, ezen és a hasonló tengeralatti interkontinentális optikai hálózatokon zajlik a nemzetközi forgalom nagy része.

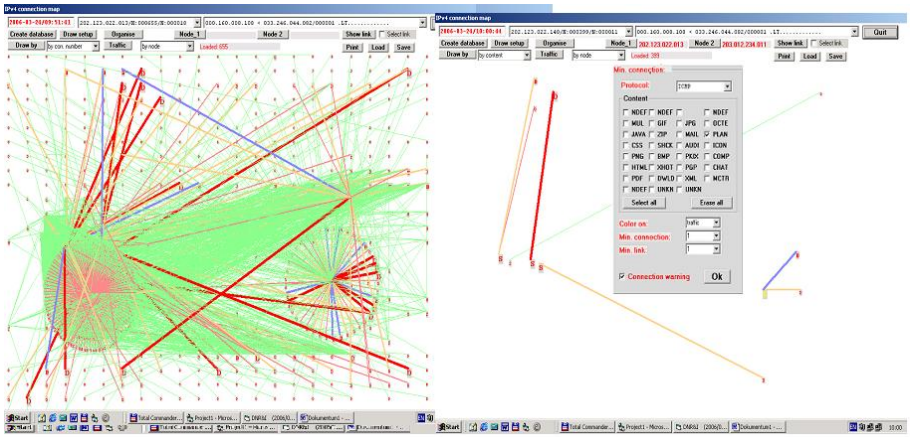
Az útválasztás és a kapcsolástechnika lehetséges megoldásai közül legalább az öt lényeges adatátviteli eljárással: a BGP[2], RIP[3] és OSPF[4] szolgáltatásokkal,

[2] BGP – Border Gateway Protocol – autonóm rendszerek közötti forgalom irányítást segítő protokoll.
[3] RIP – Routing Information Protocol – útválasztási információs protokoll, távolságvektor-alapú útválasztási protokoll.
[4] OSPF – a legrövidebb úton először algoritmust (Dijkstra) használó protokoll.

valamint a címke-alapú MPLS[5] és LDP[6] feldolgozásával értelmezhető, észlelhető és felderíthető a különböző hálózatok összekötése. Itt már láthatóvá válik az egyedi gép–gép mellett LAN–LAN struktúra is, amelynek a megjelenítése és a feldolgozása is lehetséges.

Ezeknek a megoldásoknak a létrehozásával, valamint a bejövő csatornákon „tömeges” online, vagyis folyamatos módon is, minimalizált adatvesztéssel lefogható a célzott IP-forgalom. Kifejthető az a TCP-, illetve UDP-alapú információ-mennyiség is, ami a nyílt források eléréséhez szükséges.

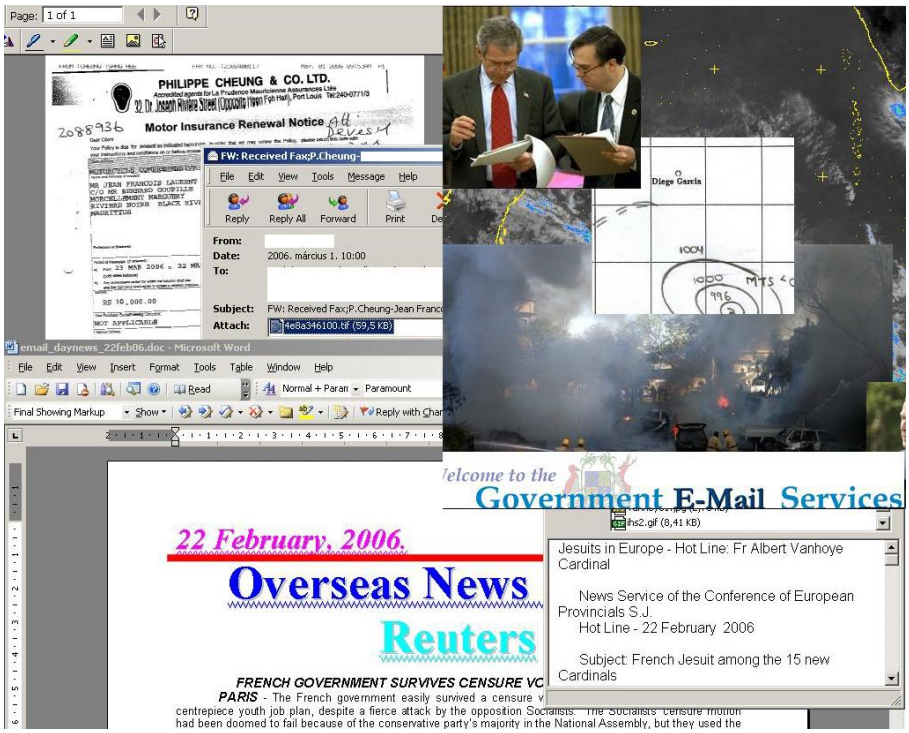
A nyílt forrásokban az elektronikus kormányzás (e-government) elérhető nyílt üzenetei, a hírügynökségek, egyes esetekben a magánlevelezés (VIP, diplomáciai személyek) e-mail és e-fax közleményei is értéket jelenthetnek, azonban komoly keresési, célpontmeghatározási és szűrési feladatot jelentenek. Adott időszakban a forgalom töredékét jelentik csak ezek az értékes adatok, és az elért forgalom lineáris növelése nemlineárisan hathat az eredményekre. Kétszer annyi vevő, demodulátor stb. nem feltétlenül jelent kétszer annyi eredményt!



3. ábra. Balra az adatáramlás és a vezérlés együttese, míg jobbra a vezérlés és a hozzá kapcsolódó protokoll-szűrés eredménye egy adott célhálózatra, illetve a riasztás beállítása egy várt kapcsolat megjelenésének észlelésére

[5] MPLS – Multiprotocol Label Switching – többprotokollos címkekapcsolás; az OSI második és harmadik rétege közé beépülő új technológia.

[6] LDP – Label Distribution Protocol – címkekiosztási protokoll, MPLS-címkék útválasztók közötti cseréjét biztosító kapcsolati protokoll.



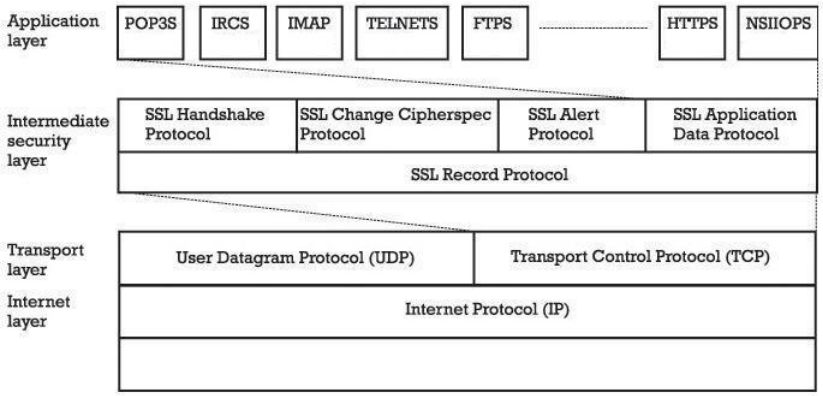
4. ábra. E-fax, Reuters, Jezsuita-híradó, egy adott kormány e-mailjei, időjárási térképek stb. – példák az elérhető nyílt anyagokra

Az adatvédelmi eljárások közül már ezen, az adatszerzési szintet elért rendszeren is megjelenik a PGP, a PKCS, X509, esetleg az X.400-as stb. szabványok szerinti forgalom. Azonban, mivel az elektronikus levelek védelme fizikailag ugyanabban az elérhető formában jelenik meg, mint a nyílt forgalom, ezért az üzenetek és a nyilvános kulcsok keresése automatizálható. Egyes szabványoknál 6–15-féle üzenettípussal kell számolnunk (például PGP MESSAGE, RSA AUTH, X.509 CERTIFICATE stb.), s így kiszűrhető és rendezhető az adott forgalom.

Ennél a forgalomnál adatszerzési szempontból előnyös bizonyos összetevők számossága és megjósolható bekövetkezése. Itt elsősorban a hitelesítési és kulcsforgalomra, illetve a kulcscsere-folyamatok forgalmának megbízható elérésére gondolunk.

A védett hálózati összeköttetések minőségi fejlődésének következő állomása a **SSL** (Secure Socket Layer) és **SSH** (Secure Shell). Ezek a hálózati megoldások strukturáltan épülnek fel, és pontosan körülhatárolható feladatok végrehajtására képesek, eltérő lehetőségeket biztosítanak, de alkalmazásuk korlátozott.

Az SSL feladata egy kapcsolatorientált szolgáltatás (TCP, OSI 4. szint) biztonságossá tétele, gyakorlatban felhasználva a TCP programozói interfésze, az ún. socket-absztrakció használata során az 1990-es évekig kialakult tapasztalatokat, biztonságossá téve az egyébként TCP-t használó alkalmazásokat. A hierarchikus felépítésben elfoglalt helyzete azt jelenti, hogy az SSL alkalmazható alacsonyabb szinteken, már védett számítógépes hálózatban (link/bulk rejtjelezés), vagy védelemmel nem rendelkező hálózatokban egyaránt. Az utóbbiakban, protokollszűréssel, nagy biztonsággal azonosítható.



5. ábra. Az SSL felépítése.
A rekord (Record), a kapcsolat-felépítés (Handshake),
a rejtjelező beállítás cseréje (Cipherspec Change) és
a riasztó eseményt kezelő/jelző (Alert) összetevő protokollok elhelyezkedése,
valamint a rájuk épülő, biztonságosnak tekintett alkalmazások

Az SSL, a rekord-protokollon alapulva, négy összetevőből épül fel:

- a kapcsolat-felépítő;
- rejtjelező beállításváltó;
- figyelmeztető és hibaüzenet továbbító;
- maga az alkalmazások felé továbbított adatprotokoll.

Az SSL rekord-protokoll a hosszú üzeneteket fragmentálja, a töredékeket tömöríti, a fragmenseket fejléccel látja el, majd a fejléccel ellátott, tömörített fragmensre üzenethitelesítő kódot (MAC[7]) számol és ennek csatolása után a bővített töredéket rejtjelezi. Maga az észlelhető SSL rekord-bitmező egyes részei nyíltnak tekinthetők (típus, verzió, hossz), míg mások nem (fragmens, MAC, kitöltés).

[7] MAC – Message Authentication Code – üzenethitelesítő kód.

Az SSL alapértelmezett rejtjelező algoritmusa az RC4 kulcsfolyamatos rejtjelező, de kapcsolat-felépítés során a felek másban is megegyezhetnek (RC2, DES, három kulcsos 3DES, IDEA, Fortezza), a blokkrejtjelezők CBC módban kerülnek felhasználásra. A megegyezés után a rejtjelezés előtt a rekord üzeneteit ki kell tölteni, hogy hossza a rejtjelező algoritmus blokkméretének egész számú többszöröse legyen. A CBC üzemmódnál úgynevezett IV (Initializing Variable) kezdeti változóra van szükség, az első üzenet rejtjelezéséhez használt IV-t a kapcsolat-felépítés során. Gyakorlatilag ez azt jelenti, mintha a kapcsolat során elküldött összes üzenetet egyetlen nagy üzenetként CBC módban rejtjeleznék.

A handhsake-protokoll SSL-ben is a viszony, munkamenet (session) és kapcsolat (connection) fogalmakon keresztül értelmezhető, két fél között több párhuzamos viszony lehetséges, és a viszonyokon belül több kapcsolat lehet elméletileg.

A lehetőségek közül azonban a legtöbb gyakorlati megoldás csak az egy viszonyon belül több kapcsolatmodellt támogatja; ez a felfedésüknél előnyös, a feldolgozó munkát könnyíti. A viszony, mint a kapcsolatok halmaza, a felek közös állapotának egy-egy részletét írja le. A viszony tartalmazza az állapot azon részleteit, amit a viszonyon belüli kapcsolatok megosztanak, közösen használnak. A viszony része például az azonosító, a felek nyilvános kulcs-tanúsítványa, tömörítő algoritmus, a rejtjelező és MAC algoritmus, ezek méretei, jelzőbitek stb. A kapcsolat része pedig maga a kapcsolatban használt rejtjelező kulcs, üzenetsorszámok, valamint az IV-k. Fontos látni, hogy a kapcsolatnak saját kulcsai vannak, ezek a kapcsolat részét képezik, ugyanakkor az egy viszonyhoz tartozó különböző kapcsolatok ugyanazokat az algoritmusokat használják, és a mestertitok is közös, amiből a kapcsolatkulcsokat generálják. Az algoritmus és a mestertitok a viszonylathoz tartozik. Ez a katonai szintű algoritmus és kulcskezelés (algoritmuskészlet, MK[8], SK[9], KEK[10], OTAR[11] stb.) polgári alkalmazásának egy viszonylag átgondolt megoldása. Maga a SSL handshake-protokoll váza egy 11-lépéses üzenet- és állapotrendszerben valósul meg.

Az évek során intenzív analízisnek vetették alá az SSL-algoritmust, melynek 2.0 verziójában számos gyengeséget fedeztek fel, amit a 3.0 verzióban már kijavítottak. A javítások után alapvetően stabillá és biztonságossá vált, bár kisebb hiányosságok még akadnak benne.

---

[8] MK – Master Key – mesterkulcs; egy hierarchikus kulcskiosztó-rendszerben a legmagasabb prioritást elfoglaló kulcsinformáció, gyakran nem közvetlenül, hanem a belőle, matematikai tulajdonságai alapján szerkesztett titkos vagy származtatott kulcsok kerülnek felhasználásra.

[9] SK – Secret Key / Session Key – titkos kulcs / munkamenet kulcs; kapcsolatkulcs Internet-közegben általában származtatott, egy-egy információs munkamenet információvédelmére felhasznált kulcsinformáció.

[10] KEK – Key Encryption Key – kulcsrejtjelező kulcs, kulcsok tárolása, vagy egyszerűbb továbbítása során az alkalmazásra kerülő kulcsinformáció védelmére felhasznált rejtjelezéshez felhasznált kulcsinformáció.

[11] OTAR – Over The Air Rekeying – rádiócsatornán keresztüli átkulcsolás általános módszere; rádiórendszerek azon képessége, hogy egy központi állomás a rendszerhez tartozó állomásokat védetten el tudja látni kulcs-információval, a nyílt kétirányú rádiócsatorna felhasználásával.

A SSL rekord-protokoll egyik ereje a különböző irányokban történő külön kapcsolatkulcsok használata. Az amerikai exportszabályok miatt az alkalmazott algoritmusok csonkított 40-bites kulcsokkal történő használatát is támogatja, ami esetleges, nem átgondolt rendszergazdai munkánál lehetőséget ad egy sikeres támadásra. Nagyobb gyengesége az SSL-nek, hogy nem védekezik a forgalomanalízissel szemben. Nem védi az IP-címeket és -portokat, ami adódik a helyzetéből, de az üzenetek méretét sem rejti. Így a támadó (RC4 és kis bizonytalansággal a blokkrejtjelezők esetében is) meg tudja tippelni az üzenet hosszát. Visszajátszás típusú támadással szemben egy 64-bites sorszámmal védekezik, ami emellett az üzenethitelesítő kódba (MAC) is beépül. Integritásvédelmét a rekord MAC kód HMAC[12] egy korábbi változatával, 128-bites kulccsal védi, amelyek kapcsolatonként változnak.

Az SSL 2.0 változatban a kapcsolat-felépítésnél több sikerrel kecsegtető támadási megoldás került kidolgozásra:

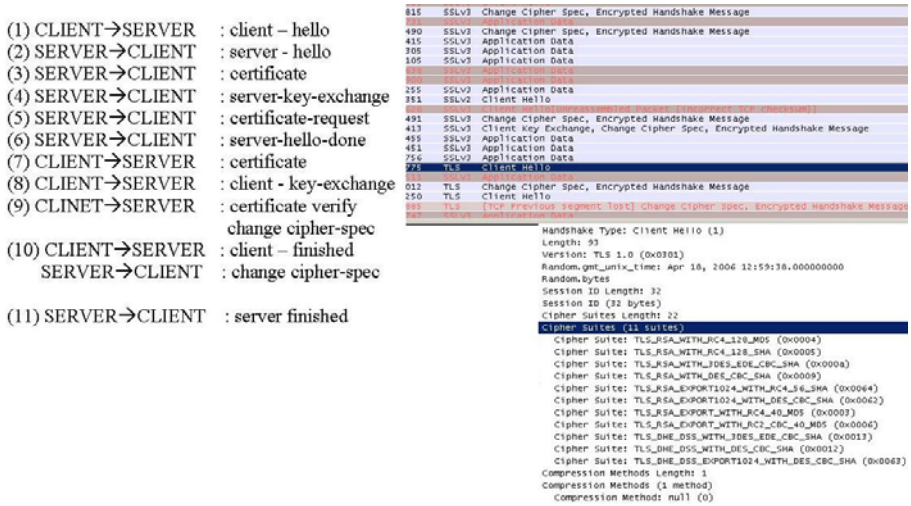
„Cipher suite rollback" támadás – a client-hello üzenetek módosításával egy támadó el tudná érni, hogy a felek 40-bitesre csonkított kulcsokkal használják a rejtjelező algoritmusokat. Ez ellen a SSL 3.0-ban és a TLS-ben a finished-üzenettel védekeznek, azonban még fennáll az a sikerességi feltétel, hogy a mestertitok valóban titkos és hiteles. A megvalósított megoldásoknál ez nem mindig van így, ezért vannak olyan állapotok, amikor a szerver nem tudja biztosan, hogy ki a kliens.

„Version rollback" támadás – amikor a támadó 2.0 változat használatára akarja kényszeríteni a legális feleket. Ez a kliens client-hello verziómezőjét változtatva érhető el, és ha ez megvalósult, akkor a finished-taktikával észrevétlen marad. Kidolgoztak az SSL 3.0-ban egy megoldást, ami az automatikus legmagasabb szintre léptetésen alapul. Amennyiben szerverinformációt szerez arról, hogy a kliens képes a 3.0-ra vagy 3.1-re áttérni, de ennek ellenére a 2.0-t erőlteti, akkor a szerver védekezésként kapcsolatot bont.

„Change-cipher-spec" üzenet elnyelésén alapuló támadás. Van olyan változat (SSL Ref 3.0b1) ami lehetővé teszi finished-üzenet feldolgozását annak ellenére, hogy nem kapott „change-cipher-spec" üzenetet; ami nem logikus, de lehetőség van rá. Ez súlyos hiba és ezzel a támadó élni tud, például rejtjelezés kikapcsolására kényszerítéssel (SSL-RSA-with-NULL-SHA stb. és hasonló üzenetekkel). Az újabb változatok kialakításakor a fejlesztők erre már figyeltek.

„Key exchange algorithm rollback" – amikor a támadó arra akarja kényszeríteni a klienst, hogy RSA-alapú kulcscserét, míg a szerver Diffie-Hellman kulcscserét javasoljon ugyanazon a kapcsolat-felépítésen belül. Ezzel szintén végzetes támadást lehet indítani a rendszer ellen, aminek a támadó által alkalmazott hatékony számítások után az lesz a vége, hogy mindkét legális fél a támadóval osztja meg titkát, lehetővé téve a támadónak a K1 és K2 mestertitok kiszámítását. Ráadásul erről a szerver és a kliens nem is szerez tudomást.

[12] HMAC (Keyed Hash Message Authentication Code)– az üzenethitelesítő kódok egy típusa; amit egy kriptográfiailag erős hash függvény és egy titkos kulcs segítségével számítanak ki. VPN (IPSec/TLS) területen a legelterjedtebb a HMAC–SHA1 és HMAC–MD5 megoldás.



6. ábra. Az SSL kapcsolat-felépítési protokoll fázisai, illetve egy gyakorlati SSL/TLS forgalom analízise

A TLS-protokoll az SSL 3.1 változatának tekinthető, amiben ezeket a hiányosságokat elvileg kijavították. A gyakorlati SSL jellegű forgalomban még nem terjedt el kizárólagosan, és emiatt komoly támadási folyamatokat lehet észlelni. Amikor negyedik félként észleljük a két legális fél és az aktív támadó küzdelmét, az adatszerző fél még a rejtjelezés esetleges feldolgozása nélkül is tud következtetést levonni az összeköttetésekről.

A hálózati biztonsági eljárások egy másik elterjedt megoldása a **SSH** (Secure Shell), első lépésben a telnet-protokoll alapú szerverhozzáférésből keletkezett, majd fejlődött. Az SSH szolgáltatások alkalmazói programok (VanDyke-Vshell, OpenSSH stb.) használata nélkül is elérhetők. Az SSH szolgáltatások magukon a hálózati eszközökön is működhetnek, ezek kapcsolók (switch), útválasztók (router), tűzfalak (firewall), terheléselosztók (load balancer) vagy az adattárolók (storage filer / Storage Area Network). Ezek nemcsak a szolgáltatások kiszolgálását, hanem a hálózatok biztonságos felügyeletét is támogatják. A felügyelet folyamata a rendszergazda és a felügyelt rendszer biztonságos elérését, vagy két eszköz egymással történő felügyeleti adatcseréjét is jelentheti.

A fizikai eszközök területén jelenleg a Cisco vállalat berendezései olyan kiemelkedő helyzetet értek el, hogy megoldásaik egyeduralkodók, vagy gyakorlatilag mintegy szabványként funkcionálnak. A fizikai eszközök jelentős része programvezérelt, és kidolgoztak számukra egy sajátos operációs rendszert, a Cisco Internetworking Operating System-et (IOS). Ennek IOS12.05S változatától támogatja az SSH-kiszolgálókat, IOS12.1.3T változatától pedig az ügyfeleket SSH1 változatban.

Mindez fejlett kapcsolókon is létezik, itt a Catalyst-kapcsolók CatOS 6.1-es operációs rendszer + változatától támogatják a SSH1-et. A hálózati eszközökön lévő operációs rendszerprogramozási lehetőség és a nagysebességű hardver által támogatott hálózati cél feladatvégzés, amely jelentős előrelépés volt a VPN-hálózatok kialakulása felé.

Nagy vonalakban ezek a hálózati adatvédelmi eljárások alakultak ki a VPN-hálózatok kialakulása előtt, némely technológia ötvöződött a VPN-ekben, némely függetlenül fejlődött tovább.

A VPN-hálózatok

Mintegy 1996-tól lehet a VPN-hálózatok kialakulásáról beszélni. A VPN elnevezéssel és a mögöttes fizikai háttérrel, továbbá annak értelmezésével kapcsolatban több félreértés alakult ki. A legfontosabb hatás, amely létrehozta őket, az a költséghatékonyság.

A megelőző megoldások igen sok lehetőséget biztosítottak a hatékony adatvédelemre, azonban a professzionális felhasználók (állami, diplomáciai és katonai körből) igen szigorú, többé-kevésbé szabványosított, minősíthető megoldásokat igényeltek (például a FIPS–140-2, vagy az EAL szoftverminősítő rendszer szerint). Ezekkel teljes körűen a megelőző megoldások nem rendelkeznek, komoly fejlesztésekkel lehetet csak ezeket teljesíteni. Igényeltek egy rendszert, ami alapkiépítésben képes ezeket teljesíteni, sőt gyakran a FIPS–140-2 alapkövetelmény.

Alapdefiníció: *a VPN egy kommunikációs hálózat, egy vállalkozási vagy vállalkozás nagyságrendű szervezet (katonai szervezetek, NATO CENTRICS CFNC VPN, US SIPRNET VPN, KÜM-ok és diplomáciai szervezetek) kizárólagos, saját használatára az elosztott nyilvános adathálózat felhasználásával. Két fő elsődleges megoldást fed ez a definíció: a távoli hozzáférést a saját hálózathoz és a telephelyek a fizikailag távoli szervezeti egységek közötti biztonságos összeköttetést.*

Ezzel a számítógép-hálózatok **típusai**, a LAN, MAN és WAN osztályozás közé került a VPN.

Könnyen összekeverhető a VPN a virtuális hálózattal (IEEE 802.1Q) és a frame-relay hálózat virtuális áramkörével (VC). Ezek önmagukban csak az összeköttetést szervezik, de adatvédelmi lehetőséget nem tartalmaznak. Támadó, illetve lehallgató műveletek eredményeként ezekből azonnal nyílt formátumú adatok biztosíthatók.

Katonai szervezeteknél a nyilvános adathálózat értelmezése kissé eltolódhat, módosulhat, mivel ezek rendelkeznek kizárólagos frekvenciahasználattal, globális hozzáférést is biztosítva, ezért a nyilvános adathálózat inkább nyilvánosan hozzáférhető médiumot használó adathálózatot is jelenthet számukra.

A felhasználás itt is az IP-forgalmon alapul, de nem mindig veszik igénybe VPN-hálózat kialakításához a nyilvános hálózatot, a zárt rendszereiken belül is alkalmaznak VPN-t.

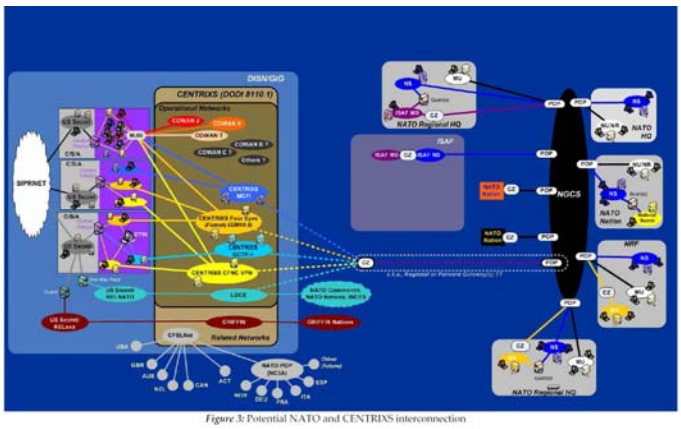


Figure 3: Potential NATO and CENTRIXS interconnection

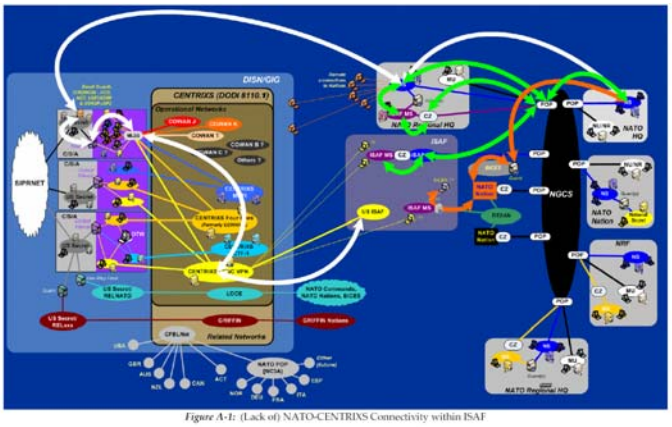


Figure A-1: (Lack of) NATO-CENTRIXS Connectivity within ISAF

7. ábra. A NATO CENTRIXS és az ISAF gyakorlati üzemelő távközlési hálózata 2004 körül. A terv és a gyakorlat: a leglényegesebb megfelelően működő komponens a CENTRIXS CFNC VPN; és a tervezett, de meg nem valósult gateway-struktúra

A VPN-hálózatok többféleképpen oszthatók fel.

Az egyik felosztás, amely a Cisco vállalat nézeteit tükrözi:

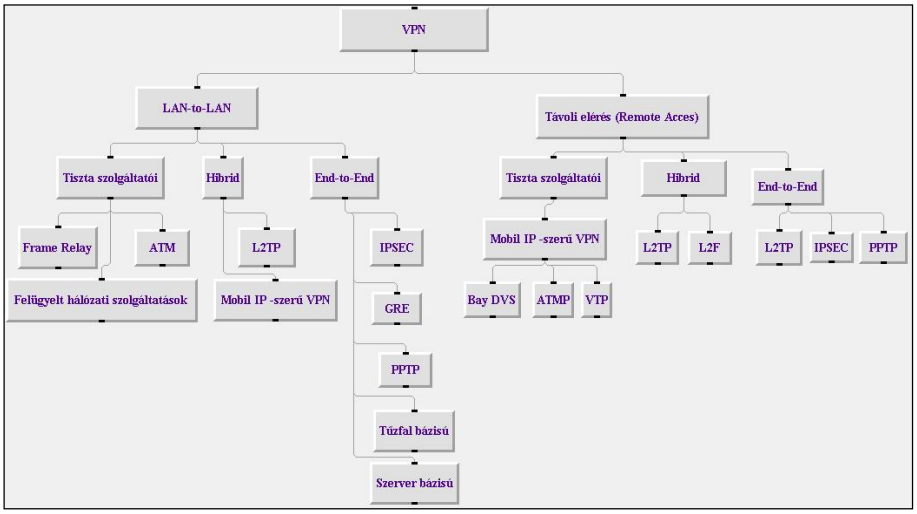
- **Távoli elérésű VPN (RAS VPN)** – Lehetővé teszi az egyéni felhasználók (laptop, PDA, diplomata, terepen lévő egyes parancsnok stb.), hogy biztonságosan kapcsolódjanak Interneten, vagy más IP-alapú adathálózaton keresztül egy központi helyhez. A kapcsolatról általában ideiglenességet feltételezünk. Mivel gyakran a távoli félnél ehhez elegendő csak egy szoftver (VPN-kliens) telepítése, gyakran „puha” (soft) vagy szoftveralapú VPN-nek is nevezik.

- **Telephelyközi VPN** – Egy már létező hálózat más épületekbe, távoli helyekre történő biztonságos kiterjesztése. Az ilyen jellegű VPN-t állandó hozzáférést biztosító virtuális magánhálózatnak tekintjük. Mivel gyakran stabil, nagyteljesítményű hardver eszközökön alapul, néha „kemény” (hard) vagy hardver-alapú VPN-nek, VPN intranetnek, esetleg LAN-to-LAN VPN-nek is nevezzük.
- **Extranet VPN** – Két, eredetileg független VPN-hálózat biztonságos összekötésével létrejövő kapcsolati megoldás. Egyik lehetséges megoldása (például) a VPN-to-VPN bridge.

Egy másik felosztás szerint, amely elsősorban a Bay Networks és más, kisebb gyártó vállalatok tapasztalatain alapul, az alkalmazott protokollokat is rendezve:

Ez a felosztás a szolgáltatói (ISP, Internet Service Provider) függés és az ismert összeköttetési protokollok rendezésére épül. Hiányossága a kulcscsere (IKE, Oakley, ISAKMP stb.), adatbiztonság, alagúttechnika, és olyan sajátos megoldások, mint az AAA (Authentication, Authorization, Accounting) technológiák, a RADIUS szolgáltatás és a TACACS nem kerül rendszerezésre benne. Mindezen hiányosságok ellenére ez a rendszerezés a feltérképezés, illetve a hálózatok felderítése szempontjából ad gyors áttekintést.

Az áttekintésben, és általában a VPN-hálózatok megismerésében nehézséget jelent a már elérhető megoldások sokasága, valamint az, hogy egyes műszaki és programozási elképzelések még nem kerültek szabványosításra.



8. ábra. A szolgáltatói függés és protokollok szerinti VPN-felosztás

A gyakorlatban, amire a kísérleti tevékenységünk során szert tettünk, néhány szempont vizsgálatával eldönthető, hogy VPN-hálózattal állunk-e szemben, és milyen minőségűvel:

- Alagúttechnika (tunnelezés) használata, megoldása.
- A SAL (Security Association List) a biztonsági kapcsolati listák, valamint a SAD (Security Association Database) a biztonsági kapcsolatok adatbázisainak a megléte, kifinomultsága.
- Alagút, tunnel-táblák használata.
- Útvonalválasztó táblák kezelése.
- Csomagszűrés használata.
- A minősíthető titkosító megoldás képessége, értéke és a kulcscsere-protokoll használata.

Alagúttechnika vagy tunnelezés – egy IP-csomag becsomagolása egy csomagnak egy másik csomagba. Itt az OSI PDU[13] fejlécezéses és ellenőrző összeges berakáshoz képest a transzformáció eredménye rejtjelezésre, hitelesítésre és tömörítésre is kerül. Az alagúttechnika VPN-szolgáltatási funkciók az eredeti, hálózati nyílt tartalmú csomagok felcserélésére irányulnak.

A kizárólag VPN megoldásokban alkalmazott protokollok (PPTP, L2TP, IPSec, MPLS)

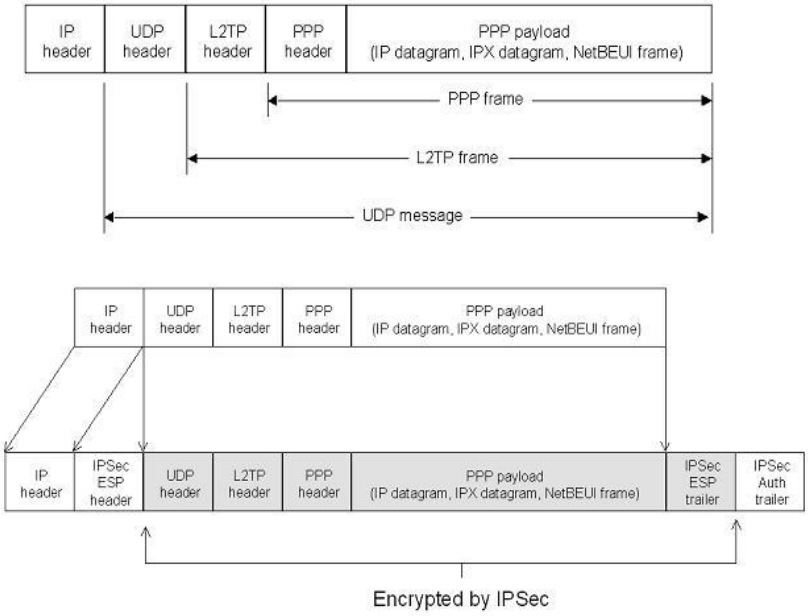
A pont–pont alagút-protokoll (**PPTP** – Point to Point Tunneling Protocol) a betárcsázó, behívó OSI PPP (Point to Point Protocol) protokollra épül. A PPP az OSI második (adatkapcsolati) rétegében működik. A PPTP tartalmazza a PPP lehetőségeit, lehetővé téve emellett alagúttechnika használatát. A PPTP az adatokat PPP-csomagokba pakolja, amit Internet-alapú VPN csatornán továbbít, támogatva a csomagok tömörítését és titkosítását. A mindkét irányú adattovábbítás során használja az általános alagúttechnika (GRE – Generic Routing Encapsulation) egy formáját. Az alagút létrehozása után kétfajta csomag küldhető rajta keresztül: vezérlő üzenetek (amelyek az alagutat kezelik) és adatcsomagok.

PPTP csomagformátum

[13] PDU – Protocol Data Unit – protokoll adategység; az az információmennyiség, amit a hierarchiában alacsonyabb helyett elfoglaló protokoll-megoldás a magasabb felé feldolgozásra továbbít.

A PPTP AAA technológiái: a felhívásos kézfogás hitelesítő-protokoll (CHAP – Challange Handshake Authentication Protocol) vagy a jelszó-hitelesítő protokoll (PAP – Pasword Authenticatoin Protocol). A PPTP az otthoni eszközökben jelentősen terjed, különösen a Microsoft termékekben való megjelenése és tömeges elterjedése után. Viszont jelentős korlátokkal rendelkezik, biztonsági szempontból 40–128-bites titkosítás használható, a gyakorlatban azonban sok megoldás csak a 40-bitest támogatja. Emellett a biztonsági vizsgálatok során, az együttesen használt tűzfalak kijátszásával azokon keresztül sikeres kapcsolatot tudtak nyitni, és szolgáltatásmegtagadási támadásokat indítani a PPTP hiányosságai kihasználásával.

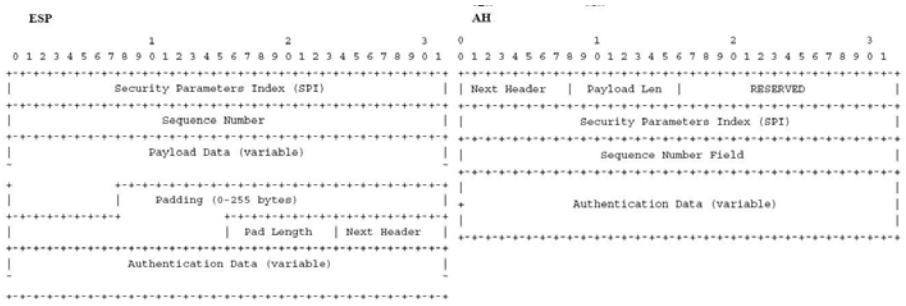
Az **L2TP** (Layer 2 Tunneling Protocol) protokoll a PPTP kiterjesztéseként fogható fel, ami két jelentős gyártó, a Microsoft és a Cisco megegyezéséből született. A két összetevő technológia: a PPTP (Microsoft) és L2F (Layer 2 Forwarding) a második rétegbeli továbbítás. UDP-csomagokat, illetve fejlesztett változata IPSec-be ágyazott UDP-csomagokat használ.



Technikailag két fő komponense a LAC (L2TP access concentrator), amely a kapcsolat egyik végén elhelyezkedő végberendezés, a másik az L2TP szerver (L2TP Network Server), ami egyben hitelesítője is az adatfolyamnak. A protokoll előnye, hogy hatékonyan támogatja az AAA feladatokat (AAA Server, RADIUS/TACACS+ támogatás).

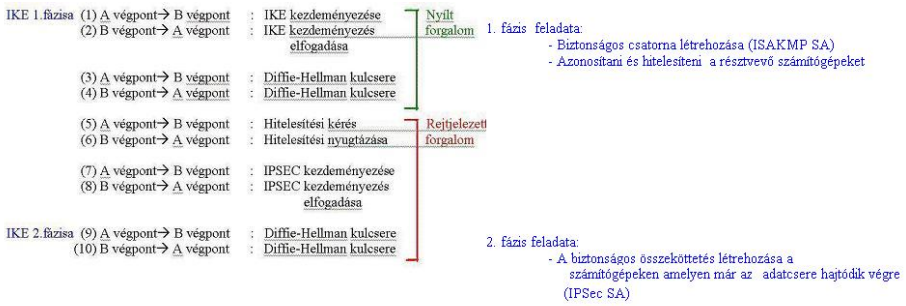
IPSec

Az IPSec protokoll a TCP/IP architektúra hálózati rétegének szabványosított biztonsági protokollja. Az IP és minden más, fölötte elhelyezkedő megoldás (TCP, UDP, ICMP[14] stb.) számára biztosít védelmet. Két alprotokollja van: az AH (Authentication Header) és az ESP (Encapsulated Security Payload). Az AH-protokoll feladatai közé tartozik az IP-csomagok integritásának védelme, eredetének hitelesítése és esetleges visszajátszásának észlelése. Az ESP-protokoll fő feladata az IP-csomagok tartalmának a rejtése, kiegészítésként az ESP is nyújthat integritásvédelmi szolgáltatást. Az IP-csomagok teljes körű védelme érdekében az AH- és ESP-protokollok kombinálhatók.



9. ábra. Az ESP (Encapsulated Security Payload) és AH (Authentication Header) protokollok bitmezői

Az IPSec-hez tartoznak még a kulcskezelést megoldó ISAKMP (Internet Security Association and Key Management Protocol) és az IKE (Internet Key Exchange) protokollok. Az ISAKMP általános célú keretprotokoll, amely bármely konkrét kulcscsere megoldás üzeneteit képes szállítani. Ilyen konkrét kulcssere megoldás az IKE, amely az IPSec hivatalos kulcscsere eljárásának a szerepét tölti be.



10. ábra. Az IKE két fázisának elvi lépéseinek modellje, minimum 10 lépésben

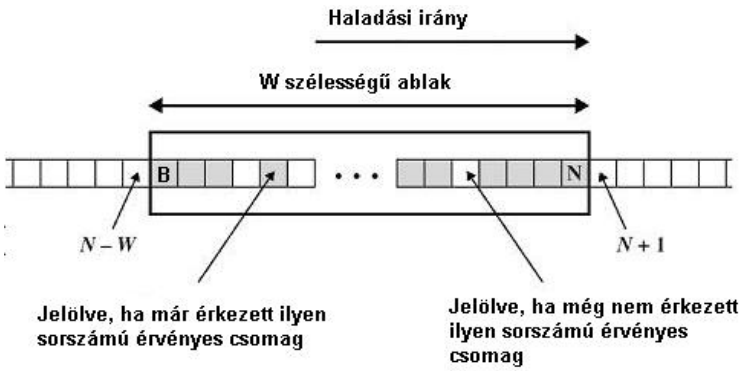
[14] ICMP – Internet Control Message Protocol – internetes vezérlőüzenet protokoll.

Az **AH**-protokoll az integritásvédelmet és az eredethitelesítést úgy éri el, hogy az IP-fejléc és az azt követő felsőbb szintű fejléc közé beszúr egy AH-fejlécet, mely a teljes IP-csomagra számolt üzenethitelesítő kódot (MAC) tartalmaz. A visszajátszások detektálásának érdekében az IP-csomagokat sorszámozza. Az AH-fejlécben található MAC-érték a MAC-sorszámot is védi.

Az AH-fejlécben az SPI (Security Parameter Index) egy azonosító, amivel a küldő azt jelzi a vevő számára, hogy milyen módon és mely kulcsokat használva kell az AH-fejlécet feldolgozni. Az AH-protokoll feltételezi, hogy a küldő és a vevő korábban már megegyezett az alkalmazott algoritmusokban és kulcsokban, tipikusan az ISAKMP/IKE protokollokat használva. A sorszám mező az aktuális IP-csomag sorszámát tartalmazza. A MAC visszaírásos módon a teljes csomagra (TTL, teljes tartalom) számolt üzenethelyettesítő kódot.

Az aktív támadó általi visszajátszást az AH-mező sorszáma alapján végzi. A vevő egy konstans W méretű ablakkal teszi ezt. A vételi ablak jobb széle N, N megegyezik az addigi legnagyobb sorszámú sikeresen vett csomag sorszámával. Az ablak bal széle pedig mindig B = N–W+1. A vevő számon tartja, hogy a [B, N] intervallumban mely csomagokat vette már egyszer. Egy **s**-sel jelölt sorszámú újonnan érkező csomaggal a következőt teszi:

- Ha **s** < N, akkor a vevő eldobja a csomagot.
- Ha B < **s** < N és **s** sorszámmal már vett egy csomagot a vevő, akkor eldobja a csomagot.
- Ha B< **s** <N és **s** sorszámmal a vevő még nem vett csomagot, akkor a vevő ellenőrzi a csomag AH-fejlécében található MAC-értéket. Ha az ellenőrzés sikeres, akkor a vevő megjegyzi az **s** sorszámot és elfogadja a csomagot.
- Ha **s** > N, akkor a vevő ellenőrzi a csomag AH-fejlécében található MAC-értéket. Ha az ellenőrzés sikeres, akkor a vevő megjegyzi az **s** sorszámot, a vételi ablak jobb szélét **s**-re állítja, és elfogadja a csomagot.



11. ábra. A visszajátszás elleni W vételi ablak ábrázolása

A vételi ablakra azért van szükség, mert az IP-protokoll nem garantálja a csomagok sorrendhelyes kézbesítését. A több lehetséges átviteli út miatt lehetségesek a felcserélődések. Az ablak véges mérete miatt „túl régi" csomagokat már nem fogad el a vevő, és nem kell az összes vett csomaggal műveleteket végezni, azokat számon tartani, tárolni.

Az **ESP-**protokoll feladata az IP-csomag tartalmának rejtése, és opcionálisan a tartalom integritásának védelme. Az előbbi feladatot a csomag tartalmának rejtjelezésével oldja meg, az utóbbit pedig úgy, hogy az ESP-fejlécre és a csomag tartalmára számít MAC-kódot , majd azt a csomaghoz csatolja. Az előbbi AH-val szemben az ESP MAC nem védi az IP-fejléc mezőit. Az ESP-fejléc tartalmaz egy azonosítót (SPI – Security Parameter Index), ami az AH-hoz hasonlóan itt is azt jelzi, hogy a vevőnek milyen adatvédelmi megoldással, milyen módon és mely érvényes kulcsokat kell az egyes csomagokat feldolgoznia. Az ESP-protokoll, a forgalom megkezdése előtt, a küldő fél és a vevő fél feltételezhetően már megállapodott az alkalmazható algoritmusokban és kulcsokban, leggyakrabban az ISAKMP/IKE protokollokat használva. Az ESP fejlécéhez tartozik még a csomag sorszáma is.

Blokk-kódoló használata esetén a csomagot természetesen ki kell tölteni. A kitöltés hossza és az ESP-fejlécet követő fejléc típusa (azaz a felsőbb szintű protokoll, ami szállításra kerül, fajtája) a kitöltés után kerül, és szintén rejtjelezve van. Végül az ESP MAC zárja le a csomagot, amely opcionális, és nincs rejtjelezve. A blokkrejtjelezőt CBC[15] módban használja a protokoll. Az ehhez szükséges IV (Initializing Variable) nyíltan kerül átvitelre a csomag tartalomrészének elején (az ESP sorszáma után).

IPSec a gyakorlatban, gyakorlati megoldások

Az AH-protokollt és az ESP-protokollt két üzemmódban lehet használni. Elnevezésük szállítási (transport mode) és alagút mód (tunnel mode).

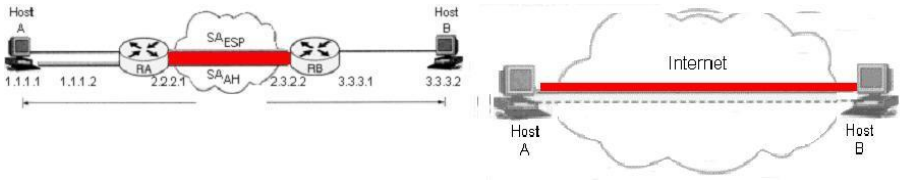
Szállítási módban az AH-vagy az ESP-fejléc a csomag eredeti IP-fejléce közé, továbbá a felsőbb szintű protokoll (TCP, UDP stb.) fejléce és tartalma közé kerül. Ekkor csak a tartalom kerül rejtjelezésre, és általában végpont–végpont között kerül felhasználásra.

Alagút módban az eredeti IP-csomagot teljes egészében beágyazzuk egy másik csomagba, és az AH- vagy az ESP-fejléc az új, és az eredeti IP-fejléc közé kerül. Ekkor az AH-fejléc vagy az ESP-trailer következő mezője IP-re utal.

Ahhoz, hogy könnyen el tudjuk különíteni az egyes módokat, nézzünk meg egy tipikus példát.

Az alagút módot általában biztonsági átjárók (security gateway), hatékony tűzfalak között használjuk. Nyilvános adathálózaton, az Interneten továbbítva a forgalmát, a tűzfalakhoz, routerekhez kapcsolódó belső hálózatokat, IPSec segítségével biztonságosan összekötjük.

[15] CBC – Cipher Block Chaining – rejtjelző blokkláncolás; a szimmetrikus blokkrejtjelező megoldások egy alkalmazási módja, létezik még például ECB, CFB, OFB, CTR.



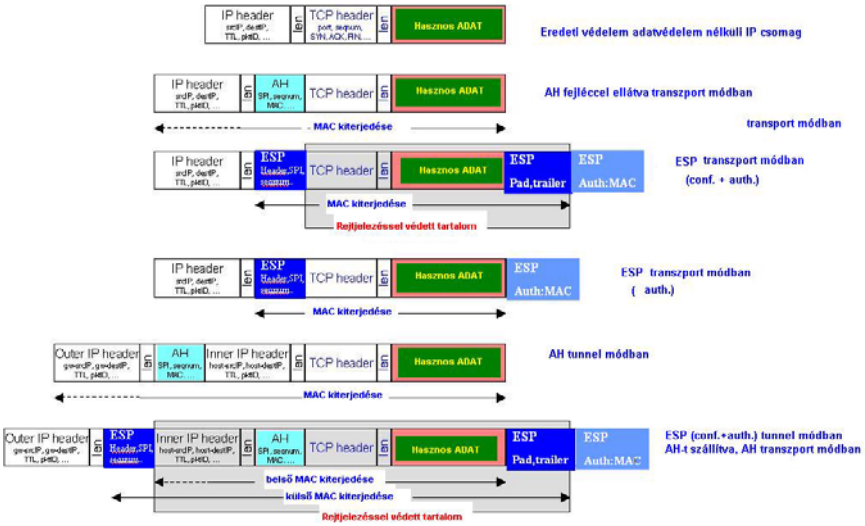
12. ábra. IPSec-alagút módot alkalmazó,
internet-részhálózatból és belső hálózatból felépülő modellhálózat,
és egy minimális hálózat a szállítási mód bemutatására

Tegyük fel, hogy a 12. ábrán, baloldalon látható VPN modellt a RA jelű routerhez kapcsolódó belső hálózaton lévő A jelű gép egy IP-csomagot küld az RB-routerhez kapcsolódó belső hálózathon lévő B jelű gépnek. Amikor az IP-csomag eléri RA routert – amelyről tételezzük fel, hogy hatékony tűzfalmegoldást alkalmaz, valamint képes VPN/IPSec-re –, IPSec védelemmel küldi tovább a piros színnel jelölt nyílt adathálózaton. A modellből látható még a címfordítás megvalósulása is. Így a csomag adatvédelemmel ellátva jut el az Interneten az RB jelű routerhez. Az RB hasonló képességekkel rendelkezik, mint az RA útválasztó. Az RB elvégzi az IPSec feldolgozást (dekódolja a csomagot, ellenőrzi a MAC-kódot, elvégzi a címfordítást stb.), majd a csomagban található eredeti IP-csomagot (most már nyíltan) továbbküldi a címzettnek.

Ebben a modellben az RA és RB útválasztók, egymás között, **alagút módban** használják az AH- és ESP-protokollokat. Ekkor az IP-csomagok az A jelű számítógép az RA útválasztó és a B jelű gép és RB útválasztó szakaszon védelem nélkül kerülnek továbbításra, az alapfeltételezés szerint a belső hálózatokat megbízhatónak tekintjük. Ha ez nincs így, akkor biztonságos vég–vég kommunikációra is szükség van, vagyis a belső hálózatban és a külső nyílt adathálózatban sem megengedett egyetlen nyílt szakasz sem, akkor az A–RA és az RB–B szakaszokon az AH- és ESP-protokollokat **szállítási módban** alkalmazzák. (Természetesen az RA–RB szakaszon a csomagformátumokhoz az alagút mód használata hozzáadódik).

Szállítási mód tisztának tekinthető modelljét az ábra jobb oldalán tekinthetjük meg, ekkor A és B végpontokon elhelyezkedő számítógépek, címfordítás nélkül és eredeti IP-cím rejtés nélkül, tartalomrejtés mellett alakítanak ki VPN-összeköttetést az AH- és ESP-protokollokkal.

Az AH- és ESP-protokollok szállítási módú alapkombinációja (transport adjacency) tehát először végezzük el az ESP-feldolgozást, majd az AH-protokoll szerinti feldolgozást, és így alakulnak ki a sorrendek.



13. ábra. Néhány alapkombináció.
Könnyen alkothatók további megoldások is, például többszörös alagutak

Alagút módban többféle kombinációt hozhatunk létre. Elképzelhető az AH- és/vagy ESP-szállítással védett csomagot még egy AH- és/vagy ESP-alagút móddal védett csomagba ágyazzuk (lásd alagút mintapélda). Sőt ebből kiindulva alagutak egymásba ágyazása is lehetséges. Ennek alapkombinációi lehetnek:

- a többszörös alagutak két végpontja azonos (tipikusan hosztok között);
- az alagutak egyik végpontja azonos (tipikusan hoszt és VPN képes tűzfal között);
- az alagutak egyik végpontja sem közös.

Időrendben a protokollok kialakulása után kerültek kialakításra a VPN-rendszerek felügyeleti, vezérlési adminisztrációs megoldásai. Az első ilyen megoldáscsoport a SAL (Security Association List – biztonsági kapcsolatok listája), a kapcsolódó alagúttábla és a hálózatszervezést segítő megoldások; router-táblák és a tűzfal-kialakítások, csomagszűrés, alkalmazott címtranszformáció. Később a listákból adatbázisokat alakítottak ki, majd az aktív támadó jellegű tevékenység ellen behatolás jelző (IDS – Intrusion Detection System) és elhárító kivédő (IPS – Intrusion Prevention System) megoldásokkal fejlődött a rendszerek vezérlési területe.

Ahogyan a nyílt Internet forgalmi területnél is fontos volt a vezérlési információ kezelése, úgy itt is fontos a rendszervezérlés megismerése és egyfajta inverz megoldás kidolgozása a felderíthetőség és a hatékony lehallgatási hozzáférési módszerek kialakításához.

A biztonsági kapcsolat (SA – security association) a gép–gép kapcsolat során a bizalmi viszonyt hozza létre, amely meghatározza a lehetőségek közül a kölcsönösen megfelelőnek tartott átviteli szabályokat. Magát az SA-t, a biztonsági kapcsolatot az IP-címmel, a biztonsági azonosítóval és az egyedi SPI (security parameter index) segítségével azonosítjuk.

Időrendben az első vezérlési, felügyeleti megoldások a biztonsági kapcsolati listák az alábbiak szerint néztek ki:

Index	IP cím (a másik fél címe)	SPI_{RX}	SPI_{TX}	Timer állapot	Timer
018888	172.16.112.10	177167388	182216143	Lejárt	- – - -
018889	172.16.112.10	936633295	2644745047	Él	Maximum 86 400
018890	172.16.112.50	871121178	1522211121	Él	15 078
018891	...	...	...	...	...

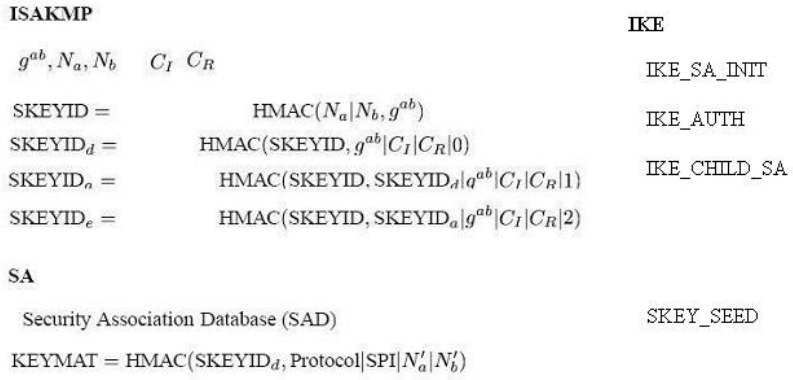
Tartalmaznak egy indexmezőt a magának a táblázatnak a kezeléséhez, de ez elmaradhat. Ilyenkor a vett SPI-értékek (SPI_{RX}) alapján indexelünk a táblázatba, ennek mindenképpen szerepelnie kell a táblázatban. Tartalmazhatják az általunk küldött SPI_{TX}-et, de ennek feladata csak az esetleges azonosságok, a kétszeri azonos kulcsértékek kiszűrése és elkerülése, ezért ez opcionális mezője a listának, valamint az időtartamokra vonatkozó bejegyzések. A kulcscsere létrejötte után adott irányokban eltérő kulcsélettartamokat állapíthatunk meg, az SA élettartama másodpercben maximum 86 400, vagyis 24 óra. A rövidebb élettartamok egy adott pontig növelik a biztonságot, viszont a jövőbeni IPSec biztonsági kapcsolatot lassítják, hiszen ekkor újra végre kell hajtani a paraméteregyeztetést és a kulcscserét, mintha egy ismeretlen partnerrel kezdenénk kapcsolatfelvételt. A timer állapot jelzi, hogy a paraméterek még élnek-e, valamint az aktuális választott beállítást. Ha a timer lejár, a bejegyzés törlődik.

Jelenleg az IPSec-ben, az ISAKMP beállítására két módszer létezik:

- előre megbeszélt kulcsok használatával, előnye a könnyű beállíthatóság;
- egy központi hitelesítő hatóság (CA – Certificate Authority) használatával.

Képes valamennyi hozzátartozó eszközt kezelni, illetéktelen támadásokra, rendszerbetörésekre hatékonyabban válaszolni.

Ez meghatározza az SAL értékeinek származását, előre megbeszélt kulcsok esetében saját kulcsértékeinket helyileg állítjuk be manuálisan az állandókat, és ennek megfelelően képezzük a változókat, míg a második esetben kapjuk őket. Az alábbi ábra részletesebb matematikai értelmezés nélkül foglalja össze ezeket.



14. ábra. A kulcsbeállításhoz, SAL-kezeléshez az SPI előállítás szükséges értékei, változók, a sikeres feldolgozáshoz minimálisan szükséges adatok

A fenti ábrából látható a SAD, a biztonsági kapcsolatok adatbázisa bevezette a KEYMAT értéket, ami a korábbi alapértékekből és a képzett ideiglenes változókból áll elő.

Rendszerezve, a SAD adatbázis a következő elemi bejegyzésekből, minden egyes biztonsági kapcsolatra vonatkozóan tárolja:

- a szekvencia-számlálót;
- a visszajátszás elleni védelem ablakszélességét, a W-t;
- az AH-protokoll algoritmus adott beállítását, kulcsait;
- az ESP-protokoll algoritmus adott beállítását, kulcsait;
- az ESP protokoll hitelesítési beállítását, kulcsait;
- az SA élettartamát;
- az IPSec-protokoll üzemmód beállítását.

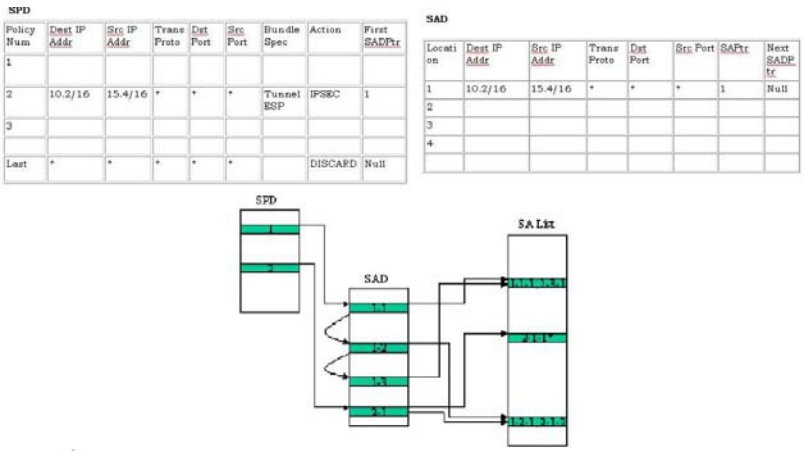
A számítógépes biztonsági megoldások gyors fejlődése során az utóbbi időben már megjelentek a **számítógépes „biztonságpolitikai", biztonsági eljárás adatbázisok** (SPD – security policy database). Ezeknek az adatbázisoknak az adategységei „biztonságpolitikai" bejegyzések, amelyek a biztonsági kapcsolatoknak a feldolgozási típusát, a szelektorokat és a biztonsági kapcsolatok beállításait tartalmazza. Ezek az adatok meghatározzák a hálózat belső és külső forgalmi beállításait, mind az IPSec- és a nyílt IP-forgalmat. A biztonsági kapcsolatok feldolgozásának esete lehetséges: ezek elvetése, IPSec nélküli beállítás (csak AH, SSL/TLS stb.), IPSec alkalmazása.

A szelektorok a következő adatokból épülnek fel: mint forrás és cél IP-címek, számítógép-azonosítók, a szállítandó információ érzékenységi biztonsági szintje, a szállítási szint protokollja, cél- és forrásportok, Ipv6-osztály, Ipv4-szolgáltatás típusai.

A célcímeket az SAL-listák, SAD-adatbázisok az alagút táblázatokból (tunnel table) nyerik, illetve rajtuk keresztül érvényesítik. Az alagúttáblázat elvi felépítése, például:

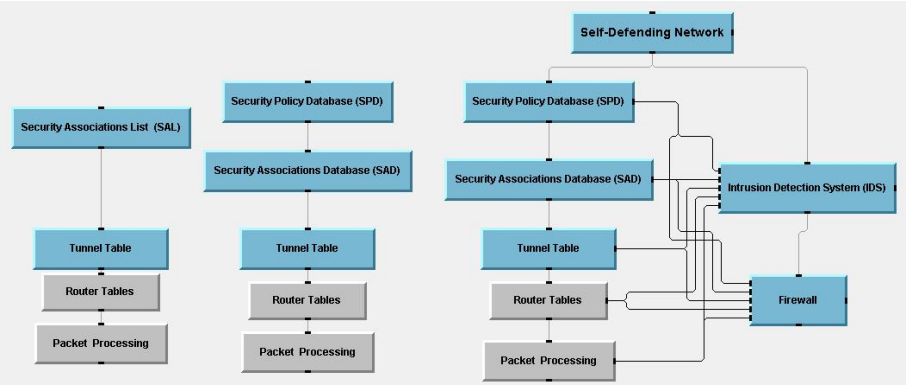
Alagútazonosító (Tunnel ID)	Időszakosság	IP-cím a csatorna túlsó végén	SPI_{RX}	Alagút állapota
178001	Nem	192.5.5.3	177167388	Kiépítve
178003	Igen	192.168.7.7	871121178	Lebontva
178004	Nem	192.124.7.9	671177818	Kiépítve

Minden egyes sor a táblázatban egy-egy alagutat definiál. A IP-címeket kézzel, vagy MMI, vagy SNMP, vagy MIB segítségével automatizálhatóan lehet képezni. A táblázatok minden más adata automatikusan képződik. Az alagúttáblázat megléte mindkét kapcsolatot kialakító VPN-berendezésben feltétele a biztonsági kapcsolat kialakulásának, mivel nem hajtódik végre a kulcsprotokollok befejezése.



15. ábra. Az IPSec-hez köthető adatbázisok egyszerűsített mintái és az adatösszefüggésük

A hálózatok továbbfejlődését nagyban elősegítette a VPN-ek elterjedése, a nagy teljesítményű program- és hardver-megoldások, amelyek képesek voltak több száz, vagy akár több ezer tunnel párhuzamos kezelésére. Ezek létrejötte, valamint a magánfelhasználók felé kínált megoldások és a kormányzati tevékenység egy szemlélete, az E-Government, továbbá annak adatvédelmi kérdései jelentős motivációt jelentettek a hálózatok és az adminisztrációjuk fejlesztésének. Mivel például egy adóbevallás intézése VPN-n keresztül elvileg megoldható, és az informatikai megoldásnak ki kell akár minden állampolgárt szolgálnia, így az adatvédelmi adminisztráció bejegyzéseinek száma adott országonként milliós, illetve néhány tízmilliós független rekordnagyságokat érhet el.



16. ábra. A VPN-hálózatok fejlődésének, adminisztrációjának, vezérlésének három fő fázisa a SDN-hálózatig

A növekvő igény mellett a „támadó" tevékenység is fokozódott. Mind passzív, mind aktív módszerekkel éves, kétéves rendszerességgel sikerült például a Cisco egyes eszközeit (PIX) feltörni, folyamatosan jelentkeznek biztonsági rések, amelyek nemcsak tudományos kutatási célból lettek kidolgozva. Komoly támadási megoldások születtek a CBC padding és a TLS1.0 protokoll CBC-módú rejtjelezése (Vaudenay-módszer, kulcs ismerete nélkül, 2002) elleni támadásra, amelyek a vezérlés és esetlegesen a kulcscsere gyakorlati megoldásainak gyengeségei mellett magának a matematikai biztonságnak megingatására törekedtek.

A fejlesztők erre válaszul, az alapok többé-kevésbé változatlanul hagyása mellett úgy reagáltak, hogy a tűzfal-technológia kifinomult megoldásait ötvözték (NAT, csapdagépek, csapdaállítás, adaptív adminisztráció és vezérlés) a VPN-ek korábbi megoldásaival. Céljuk: a hálózat elleni behatolások észlelése, majd az ezután bekövetkező változtatások létrehozásával a hálózat folyamatosan működőképes és megfelelő biztonságot szavatoló állapotban tartása.

A VPN-hálózatok „önvédelmi képességét" szerették volna elérni, ezért az ilyen követelményeknek megfelelő hálózatokat SDN (Self-Defending Network) nevezzük. A legkézenfekvőbb megoldás az aktív ellentámadás megkezdése lenne, (riasztás, e-mail az USAF Special Investigation Agency vagy az FBI felé, sync attack, spam-roham, az ellenfél operációs rendszere elleni támadás stb.), de erről megbízható adattal jelenleg nem rendelkezünk. A védelmi módszerek fejlesztése a belső hálózaton belülre fókuszált.

2004-re elodázhatatlan lett, hogy az alapokban is változást érjenek el. Ezt a többprotokollos címkekapcsolás, az MPLS (Multi-Protocol Label Switching) protokoll felhasználásával kívánták elérni.

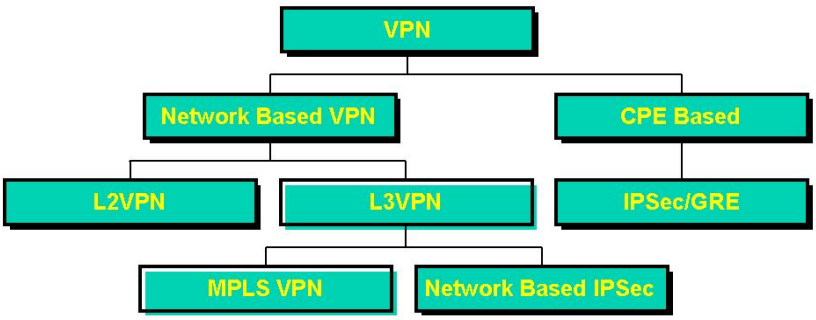
Hagyományos VPN esetén a forgalmat bonyolító és közvetlen, annak vezérlését biztosító protokollok mellett a BGP, ICMP, RIP, OSPF, RSVP vezérlő-protokollok forgalmának felderítésével, értelmezésével és feldolgozásával a teljes hálózatról nyerhettünk információkat.

Ez egy régi katonai problémának egy lehetséges megoldásaként értelmezhető. A korai ún. területi hírrendszereknél (RITA, Ptarmigan, Autokonnetz, MSE stb.) az elkerülő utak és a csomóponti intelligens katonai vezérlő-számítógépek alkalmazásával kívánták a felderíthetőséget csökkenteni, illetve lehetetlenné tenni. Itt a a csomóponti gépbe történő behatolás jelentett elvi megoldást, mivel ez táblázatos formában tartalmazta a teljes csomóponti rendszert és az elkerülő utakat. A polgári területen ma a router-táblázatokban ez az információ ugyanúgy megtalálható és feldolgozható. Egyes elért hálózatrészekből pedig nagy valószínűséggel szintetizálható, rekonstruálható egy-egy célhálózat.

Az MPLS VPN-ekben a címkézet adattartalom (labelled data) úgy kerülne alkalmazásra, hogy csak az érintett útválasztóknak lenne tudomásuk az összeköttetés kiépítéséről, asszociatív módon a többi router tábláinak feldolgozásával az összeköttetés és a tunnel nem lenne észlelhető triviálisan. Ebben a megoldásban az elemeket LSR címkekapcsolt útválasztók, illetve LSP címkekapcsolt útvonal fogalmakkal definiálják. A router-táblát az útvonal leképezési táblázat váltaná fel, a nagy sebességű működést pedig a címkeverem támogatná. Az MPLS-protokoll alkalmazásával létrejönnek az ún. harmadik szintű VPN hálózatok, az L3VPN-ek.

Ez a megoldás a „frame relay" távközlési megoldáshoz hasonlít, ahol a DLCI[16] azonosító segítségével ún. virtuális kapcsolatok kerülnek kialakításra. Itt a hardverelem VPI – virtuális útvonal választó elnevezéssel, a kapcsolat VCI – virtuális kapcsolatazonosítóval definiálódik. Ennek a rendszernek az előnyei inspirálták az MPLS kialakítását. Azonban a „frame relay" is feldolgozható, a „frame relay"-be ágyazott IP is. Valószínű, hogy kidolgozható eljárás az MPLS VPN-ekkel szembeni hatékony adatszerzés érdekében is, azt viszont nehezíti a viszonylag ritka elterjedtségük.

A Cisco vállalat – amely de facto monopólium a hálózati eszközök fejlesztése és gyártása terén –, jelenleg így osztályozza a VPN-hálózatokat:

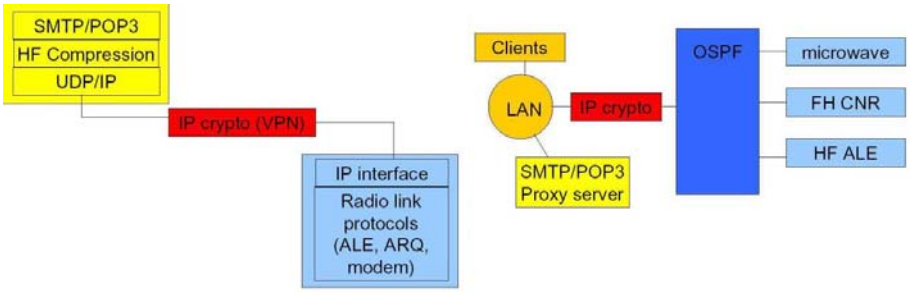


17. ábra. A professzionális felhasználású VPN-hálózatok jelenlegi felosztása

[16] DLCI – D Link Control Information – adatkapcsolati azonosító.

A VPN-hálózatok katonai és diplomáciai felhasználása

A katonai hálózatok tervezése követ bizonyos szabályokat, amelyre jó példa a 9. ábrán vázolt NATO ISAF, US SIPRNET hálózat. Itt három fontos hírrendszert illesztenek IP-alapú adathálózatokhoz, a rövidhullámú rádiórendszereket, a „harcos hírrendszer" URH-rádiórendszereit (CNR-SS/FH, Combat Net Radio-Spread Spectrum/ Frequency Hopping) és a mikrohullámú katonai gerinchálózatot. Az egyes gyártók által létrehozott megoldások különböznek egymástól, de műszakilag közös felhasználásukra az elfogadott szabványok adnak lehetőséget. Kis sebességű adatátviteli rendszerekben a NATO-ban a STANAG–5066, míg a jövőben a tervezett nagy sebességű megoldásokban a TCP-J a szabvány. Az ennek nem megfelelő megoldások egyedi adatvédelmi elbírálás alá esnek. A nemzeti szabályozások mellett a katonai megoldásoknak az EAL minősítés és a FIPS–140-1 Level 3-4 szabványok irányadók.

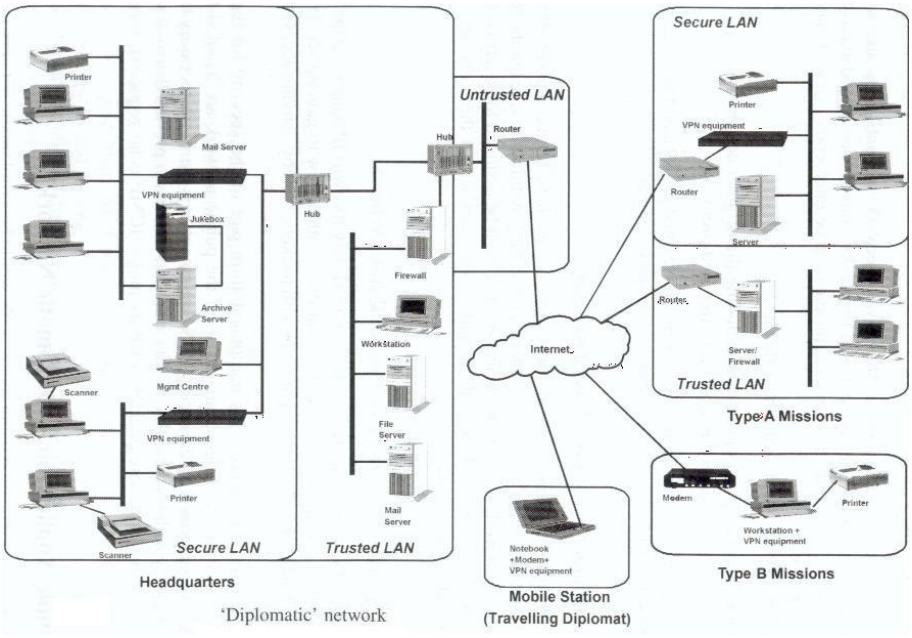


18. ábra. Bal oldalon a rövidhullámú VPN-t alkalmazó rádiórendszer elvi összetevői, illetve egy elvi lehetőség egységes hírrendszer létrehozására

Sikeres kísérletek folytak kézi katonai PDA-számítógépek rendszerszerű illesztésére (például Harris RF6705 szoftver, ELTA PDA-terminál) VPN-hálózatokba, valamint nagy teljesítményű hírközpontok bekapcsolására. A katonai vezetés kezdeményezett egy koncepciót, amely a VoIP hangösszeköttetésekkel váltanák fel a DNVT/DSVT[17] berendezéseket és kialakulna egy olyan hírrendszer, ahol minden adatnem IP-technológia alkalmazásával kerülne továbbításra. Ez az EoIP (Everything on IP) koncepció, ennek fő hardverelemei a NET Promina 800-as VoIP szerverek Cisco 3725 és Cisco 1760 VPN-útválasztók, KG–175 rejtjelező berendezések. A megoldást az Egyesült Államok III. Hadtest hírközpontjaiban és különböző hadgyakorlatokon tették próbára, 2004-től.

Diplomáciai területen inkább az ún. nagyvállalati modell irányába indultak el.

[17] DNVT/DSVT – Digital Narrowband Voice Terminal / Digital Secure Voice Terminal – digitális keskeny sávú (4kHz~16 kbps) beszédterminál / digitális titkosított beszédterminál.



19. ábra. A Crypto-AG (Hagelin) diplomáciai VPN-rendszer modellje

Ennél a modellnél a központ szerepét a külügyminisztériumok töltik be, a különböző feladatok végrehajtására a missziók méretének megfelelően skálázható a hálózat, lehetővé téve a mobil bejelentkezést.

Ezekben a rendszerekben (HC–7500, AEP, CORRENT, Cisco–PIX, Symantec, ANCORT REDUT stb.) külön veszélyt jelentenek a nem kívánt megosztott alagutak (unwanted split tunnels). Ez abból a lehetőségből indul ki, hogy lehet egy adatküldő és két vagy több fogadó végpont közé konfigurálni *„kvázi ugyanazt”* az alagutat. Ekkor, ha a Külügyminisztérium a célpontja a támadónak, gyakorlatilag az onnan induló teljes forgalom szinte kiömlik a támadóhoz (impostor station) is. A gyártók saját algoritmusokkal és egyedi belső fejlesztéseikkel elképzeléseik szerint a VPN adta lehetőségeket minőségileg javítják, és próbálják az ilyen és ehhez hasonló támadásokat elhárítani.

Jelenleg folyik az AES algoritmuson alapuló megoldások fejlesztése, 3DES helyett, illetve az RSA algoritmus mellett elliptikus görbék felhasználásán alapuló VPN-megoldások kidolgozása. A VPN-ek újabb minőségi megoldásainál várható ezek megjelenése, jelenleg alkalmazásuk még nem kiterjedt.

A VPN-adatforrások feldolgozása

Jelenleg professzionális eszközök elsősorban a SSL- és IPSec-alapú megoldásokat alkalmaznak. A többi megoldástól terjedelmi korlátokból eltekintenék.

Az összetevők biztonságával több forrás foglalkozik, például RSA–640 törése, SSL, DES, 3DES támadások stb., az egész rendszer feldolgozása már kisé nehezebb kérdés. A következő példa egy IPSec-en alapuló VPN-forgalom analízisét mutatja:

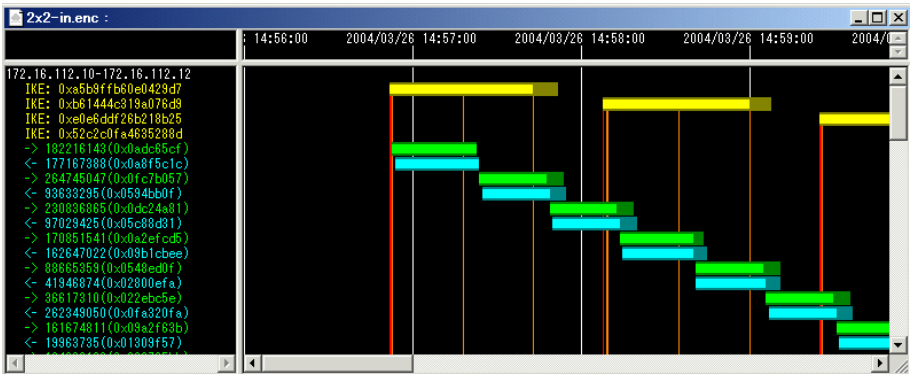
Az IPSec-VPN feldolgozása

A feladat egy háromfázisú feladatként oldható meg:

- első fázis: IP-adatgyűjtés, analízis, célpontfeldolgozás;
- második fázis: VPN-feldolgozás (IKE, AH, ES, Hash stb.);
- harmadik fázis: az előállított már védelem nélküli IP-forgalom feldolgozása.

Az első fázisról feltételezzük, hogy az előfeldolgozó rendszer IP-cím, SPI, szekvenciaszám szerint rendezi a forrás forgalmát és nem VPN2VPN bridge-el állunk szemben. Egy DNI alapképességű szoftver erre általában képes.

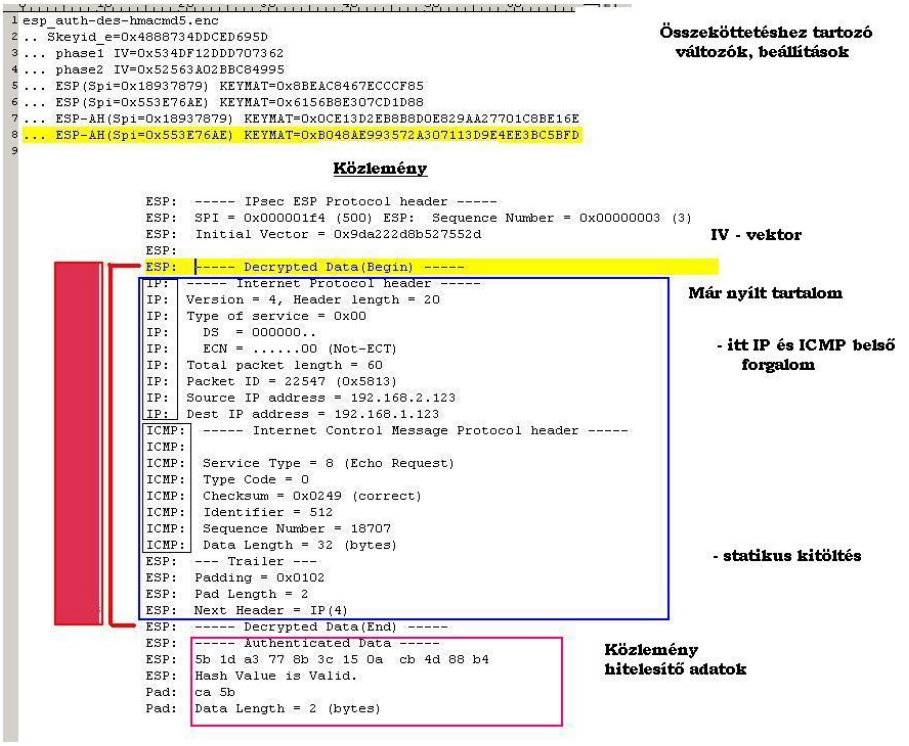
A második fázis első lépése a kulcscsere és a kulcstovábbítás analízise, azoknak az elérhető nyilvános kulcsösszetevőknek, illetve a szimmetrikus rejtjelző algoritmusok IV-inek kinyerése és rendezése. Általában akár a szoftver-, akár a hardver-megoldásokban a kulcsérvényesség időtartama beállítható, ez állandóként tartható, de egyes támadások kivédésére változtatható is, ezek tények a feldolgozást végző számára fontos információk.



20. ábra. Az IKE alap kulcscsere-események és az időszakos kulcsinformáció rendezése egy alagútnál

Ennél a lépésnél az adott protokollhoz szükséges kulcsváltozóval a feldolgozó rendszernek már rendelkeznie kell (például IPSec-nél SKEYID(a,d,e), Na,Nb, Ci,Cr,KEYMAT). Ezek egy része egymásból számítható, sikeres kriptoanalitikai erőfeszítések adhatják a feldolgozó kezébe; műveleti tevékenység, felelőtlen magatartás, a fizikai biztonság megsértése könnyítheti meg az egyáltalán nem triviális számításokat.

A következő lépésben az egyes adatvédelemmel ellátott csomagok feldolgozása során, ami a különböző hitelesítési értékek ellenőrzésével történik, előáll a nyílt adattartalom.



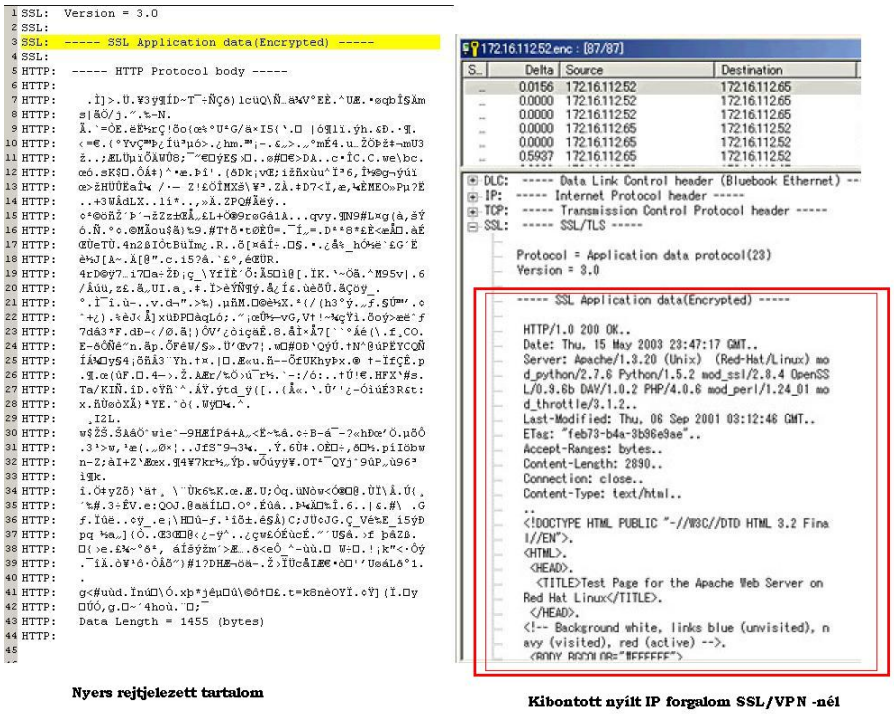
21. ábra. IPSec-feldolgozás egyetlen ESP-csomagon

A végső fázisban ezeket az IP-csomagokat, illetve IP-csomagtöredékeket újra értelmezhető forgalommá kell összeállítani, és ezt már könnyen, az ismertetett módon fel lehet dolgozni. A feldolgozás után előáll az adott számítógép-hálózat felnyit forgalma.

A SSL/VPN forgalom feldolgozása is hasonló, eltekintve az eltérő számítási feladattól és a változóktól.

A kísérleti programfejlesztési tevékenységet nagyban megkönnyíti bizonyos változók ismerete. Gyakorlatilag az ún. mestertitok szerepben lévő információ ismeretében a számítások az adatfeldolgozásnál jelentősen felgyorsulnak, ez jelentheti a távközlési rendszer adatátviteli sebességének a megközelítését is, ez azonban az esetek többségében még idealizált eset. A műszaki rendszer, még utólagos szisztematikus kereső és célpontfeldolgozással is, egy nagyságrenddel könnyebben kialakíthatónak tűnik, mint egy kiszolgáló nagyteljesítményű, erre a feladatra specializált kriptoanalitika-célrendszer.

A jelenlegi hardverekkel az n-szer E1 / E3 távközlési sebességtartomány, ami számítógép-hálózatok, LAN–WAN területen 10–100 Mbit/s Ethernet hálózatnak felel meg, megoldható egy hatékony IP-alapú adatszerző rendszer kialakítása.



22. ábra. Az SSL/VPN csomag kibontása

Összegzés

Az adatszerző rendszerben egyre jelentősebb mértékben jelen lévő, a feladatot képező korszerű digitális rendszerekben lévő adatforrások eléréséért két technikai alapú terület vált az utóbbi időben jelentőssé: a hívószám-felismerés alapú célpontkiválasztás elvén (DNR) üzemelő rendszerek területe, illetve az adathálózatok felderítését (DNI) végző különféle rendszerek területe.

A DNR-és a DNI-képességek célszerű kialakításával kiegyensúlyozott rádióelektronikai felderítő technikai rendszereket hozhatunk létre, amelyek a távközlési csatornákon továbbított bármely adatnem elérésével képesek lefedni a változatos adatforrásokat.

Úgy tekintjük, hogy az adatáthálózatok felderítésére kialakításra kerülő rendszerek megvalósításánál is ezek a szempontok és követelmények hasonló minőségi javulást képesek előidézni. A több lehetséges irány közül mi a kísérleti tevékenységhez több okból egy kissé nehéz területet, a virtuális magánhálózatok területét választottunk. Egyrészt, mert nem triviális, másrészt a célpontok fontossága miatt jelentőssé válhat. A kidolgozott módszereknél törekedtünk a minél szélesebb alkalmazhatóságra. A kísérleti adatszerző munkahely és a feldolgozó munkahely kialakításánál törekedtünk mind az off-line, mind az on-line feldolgozás folyamatos működtetésére. A különböző időszakokban eltérő tapasztalatokat szereztünk, amelyek nagyban segítették a sikerhez vezető megoldások keresését.

DR. EGED BERTALAN

SZOFTVERRÁDIÓK

Bevezetés

A szoftverrádió-technológia fontos szerepet fog játszani a közeljövő rádiókommunikációs eszközeinek és kommunikációs rendszereinek kialakításában. Az egyre gyorsabb ütemben fejlődő rádiókommunikációs rendszerek megkívánják, hogy a rendszerek ellenőrzésében és felügyeletében felhasznált infrastruktúra is lépést tudjon tartani a célrendszerek fejlődési ütemével. Ez megköveteli a legkorszerűbb módszereket, valamint a készülék- és a rendszerépítési elvek felhasználását.

Az előadás rövid összefoglalót tartalmaz a közelmúltban elindult technológiai fejlesztések eredményeként létrejött technológiáról, a fejlesztések motivációiról, valamint felhasználásának előnyeiről. A hagyományos és a szoftver rádióelven felépített rádióelektronikai berendezések funkcionális modelljének ismertetése után az egyes funkcionális blokkok jellemző megvalósítási lehetőségei kerülnek áttekintésre, valamint a hazai kutatás–fejlesztési tevékenység eredményeivel és a rendelkezésre álló eszközökkel ismerkedhetünk meg. Az előadásban példát láthatunk az erre a technológiára épülő, megvalósított radar-, illetve kommunikációs adás- és vételtechnikai berendezésekre, valamint képet kapunk a jelenleg folyó készülék- és rendszertechnikai fejlesztések irányáról, várható eredményeiről.

A szoftverrádió-technológia bemutatása

A szoftverrádió-technológia

A szoftverrádió elnevezés olyan rádióra alkalmazható, amely változatos modulációs technikákat, széles vagy keskeny sávú üzemmódot, biztonsági és még számos egyéb funkciót biztosít szoftveres úton. Azaz a hagyományos rádióktól eltérően, az antennáról érkező (digitalizált, azaz mintavételezett és kvantált) jelek feldolgozását programok végzik. Egy szoftverrádió, amelyben a jelfeldolgozás lehető legtöbb lépését szoftveres egységek valósítják meg, könnyen tud alkalmazkodni az eltérő igényekhez, mivel egy funkció beépítése vagy megváltoztatása lényegében csak a szoftver cseréjét jelenti. A teljesség kedvéért azonban meg kell jegyezni, hogy egyetlen rádió sem valósítható meg tisztán szoftveres úton. A programokat futtató hardveren túl valamilyen szintű analóg jelkezelésre is szükség van.

A szoftverrádió-megoldás az előbb említett képesség miatt a vezeték nélküli ipar területein széles körben alkalmazható technológia, amely hatásos és költséghatékony megoldásokat biztosít számos, a jelenlegi rendszerek állította akadályra is. Például a szoftverrádió-alapú felhasználói készülékek és hálózati eszközök dinamikusan programozhatók, így tulajdonságaik módosíthatóak a jobb teljesítmény, a gazdagabb képességek, vagy új (fejlettebb) szolgáltatások érdekében.

Azaz alternatív lehetőségeket biztosítanak a végfelhasználóknak és új bevételi forrásokat a szolgáltatóknak. A szoftverrádió-technológia egyedülállóan alkalmas a hadi, civil és kereskedelmi szektorok közös igényeinek kielégítésére.

A szoftverrádió ötlete nem újszerű, de a megfelelő nagyságú számítási kapacitás hiányában a technológia első bemutatójára csak 1995-ben került sor az Egyesült Államok Védelmi Hivatalának egyik projektje formájában.

Software Defined Radio Forum

A szoftverrádió témájához fűződő egyik legfontosabb szervezet az SDR Fórum. Ennek elsődleges érdeklődési területe a rádiótechnológiával megvalósított kommunikáció, sőt maga a szoftverrádió-technológia elősegítése a Fórum létrejöttének oka. Az eredeti névvel – moduláris többfunkciós információtovábbító rendszer (angolul Modular Multifunction Information Transfer System – MMITS) –, az alapítók széles érdekeltségi területet szándékoztak megcélozni. Amikor a tapasztalatok viszont azt mutatták, hogy az MMITS név sokakat megtévesztett, SDR Fórumra változtatták annak ellenére, hogy az SDR jelentése nem volt világosan definiálva. A szoftverrádió (angolul Software Radio) kifejezést és számos, jelzőkkel ellátott változatait, mint például „definiált" vagy „alapú" (angolul Defined, Based) javasolták, hogy tükrözzék a részlegesen szoftverrel működő rádiók változatos tulajdonságait.

Az SDR Fórum mára több mint száz nemzetközi szervezet ipari együttese, amely elkötelezte magát a vezeték nélküli Internet, valamint civil és katonai rendszerek fejlett képességeinek biztosítása mellett. A Fórum elősegíti a szoftverrádiók fejlesztését, telepítését és korszerű, vezeték nélküli rendszerekben történő használatát. Támogatja továbbá az SDR-technológia modulokban, termékekben és hálózati rendszerekben felhasználható, létező szabványokkal kompatibilis, globális szabványainak fejlesztését.

A Fórum küldetése az SDR-technológiák elterjedésének felgyorsítása a hadi, civil és kereskedelmi szektorok igényelte vezeték nélküli hálózatokban.

A Fórum szándékai:

„Igények támasztása az SDR technológiával szemben és/vagy szabványok fejlesztése a technológia részére. Függetlenül és más felekkel együttműködve szándékozunk biztosítani, hogy az általunk kifejlesztett szabványok könnyen alkalmazhatók a létező és fejlődő vezeték nélküli rendszerekben.

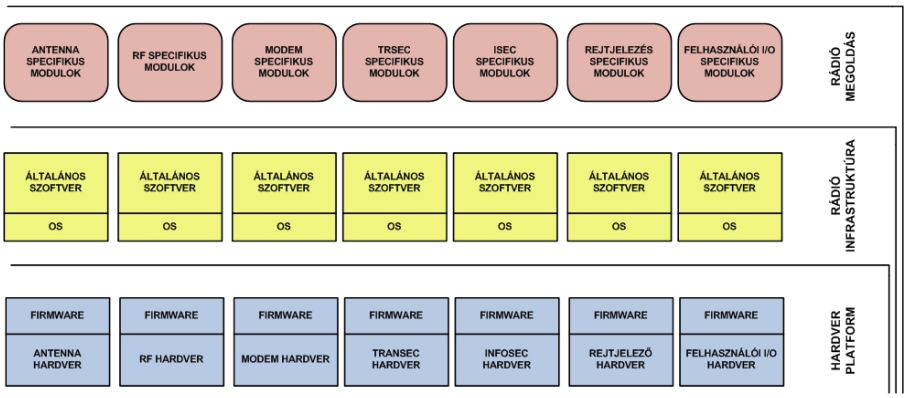
Kialakítani az érdekelt felekből álló, nemzetközi csoportot, amely közös kutatásokkal segítheti a globális kompatibilitást és együttműködést a vezeték nélküli iparban.

Együttműködve szeretnénk megcélozni az egyes országok és/vagy piaci szektorok egyedülálló biztonsági és szabályozási igényeit, miközben meg szeretnénk őrizni a közös alapokat és módszertant."

Az SDR-architektúra

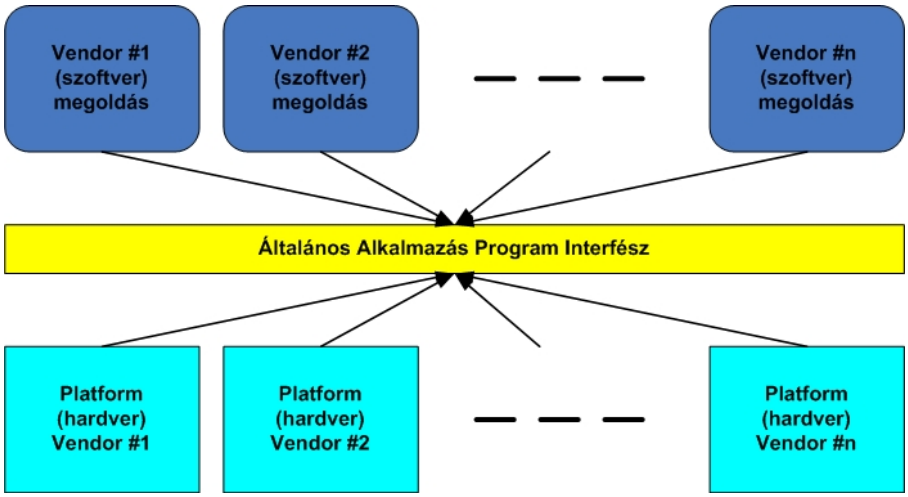
Az SDR-architektúra alapját meghatározott feladatú egységekből álló, magas szintű, általános modell adja, amelynél az egységek kapcsolatait nyílt interfész-szabvány ajánlások adják. A szoftver implementálása hierarchikus és egyenrangú modulok formájában valósul meg, amelyek támogatják a skálázhatóságot és a rugalmas alkalmazás kiterjesztést. Nyílt rendszerekben a modularitás a sikeres szoftveralkalmazások fejlesztésének kulcsa. A modulokat szabványosított interfészek határolják, de egy modulon belül a fejlesztő szabad kezet kap, hogy a leghatékonyabb módszerrel oldja meg a feladatot.

Az SDR fő alapelve, hogy a rádió lényeges része szoftverként kerül megvalósításra, amely programozható és átkonfigurálható hardver egységeken fut. Ez az elrendezés univerzális és újrafelhasználható elemeket biztosít, amelyek költséghatékonyak és könnyen fejleszthetők. Fontos hangsúlyozni, hogy az SDR technológia nem egy termék, hanem sokkal inkább egy alapelv, amelyre építve rádiókészülékek tervezhetők. Az SDR technológiát jelentő különböző típusú hardver és szoftver komponenseket, konkrét SDR-alapú megoldásoknál viszont már föl lehet használni önálló termékekként.



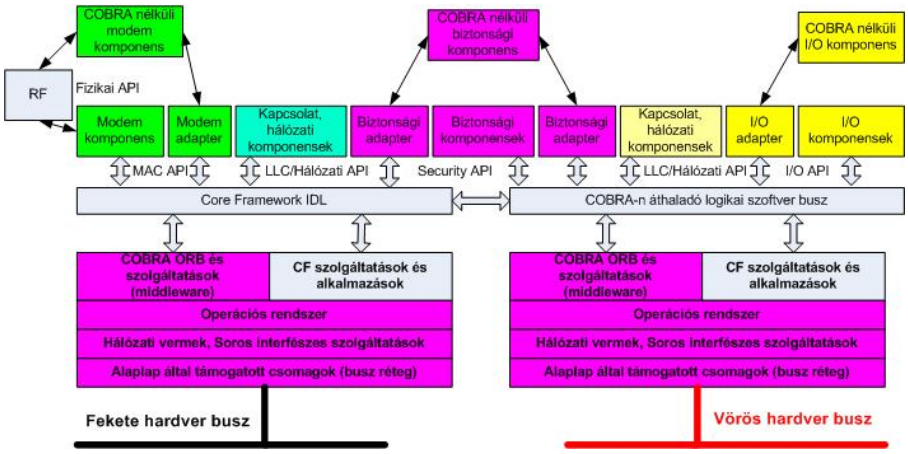
1. ábra. Az SDR-architektúra modellje

Az 1. ábra az SDR nyílt architektúráját mutatja, hét független alrendszerrel. Az architektúra nyílt interfészeken keresztül összekapcsolt funkcionális hardver elemekből és a hardvert működtető firmware-ekből áll, amelyeknek specifikus feladatok adhatók meg. A modell ezen részeit együttesen „hardver platform”-nak vagy „rádió platform”-nak nevezik. A működéshez szükséges szoftvert, mely firmware-el irányított hardveren fut, „operációs szoftvernek” (OS) nevezik. Ez a környezet közös interfészt biztosít a felsőbb rétegnek. A közös interfésszel olyan rádióinfrastruktúrát kaptunk, amely képes alkalmazásspecifikus szoftvermodulok futtatására, így teljessé válik a megoldás. A különböző szoftverrétegeket együttesen „alkalmazási keretrendszer” (angolul application framework) névvel illetik.



2. ábra. Az SDR nyílt architektúra

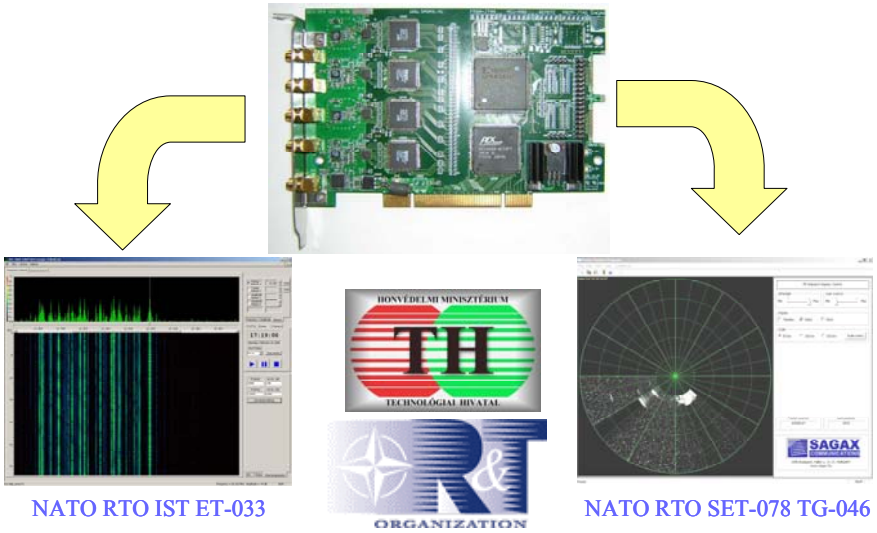
A közös interfész vagy API (angolul Application Programming Interface) igen fontos, mivel lehetővé teszi, hogy a különböző eladóktól származó szoftvermegoldások és hardverplatformok együttműködjenek. A közös szoftver API réteg (2. ábra), megosztott függvényekkel kerül szabványosításra, amelyek nyílt interfészekkel rendelkeznek.



3. ábra. A szoftver-kommunikációs architektúra

A szoftver-kommunikációs architektúra (angolul Software Communication Architecture – SCA) a jelenleg elfogadott közös API katonai alkalmazásoknál, amelyet a Joint Tactical Radio System (JTRS) projekt fejleszt.

A JTRS projektről, saját honlapjukról idézve: *„The Joint Tactical Radio System is a DoD initiative. JTRS is designed to provide a flexible new approach to meet diverse warfighter communication needs through software programmable radio technology.”* Vagyis: Az Egyesített Harcászati Rádiórendszert (EHRR) a Védelmi Minisztérium kezdeményezésére fejlesztették ki. Az EHRR a szoftveresen programozható rádió technológia alkalmazásával kellő rugalmasságot biztosít a diverziós harcosok kommunikációs igényeinek kielégítéséhez.



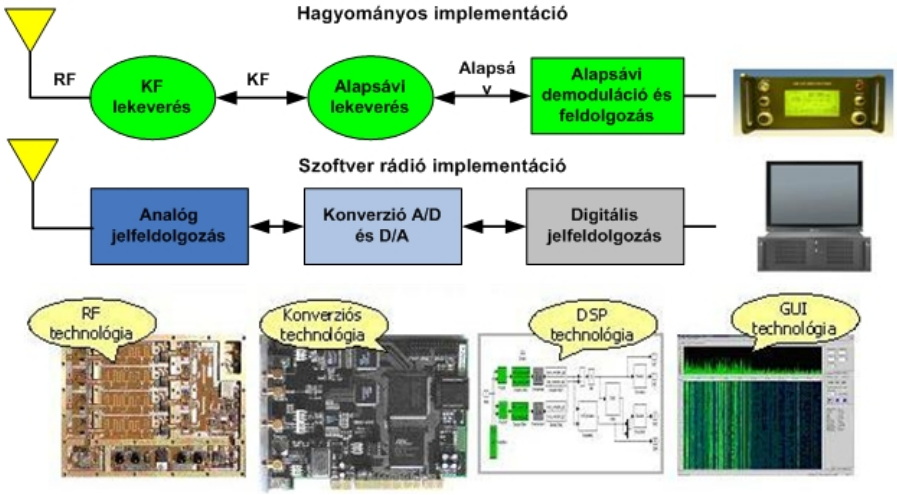
4. ábra. Azonos hardvert használó, eltérő szoftverek

A JTRS program kulcseredménye az SCA specifikáció (3. ábra), amely szabványként szolgál (majdnem) minden katonai SDR-nél. Egy nyílt, elosztott, objektumorientált architektúra keretrendszere, és elválasztja az alkalmazást (hullámalak-funkcionalitást) az operációs környezettől. Az SCA közös interfészeket határoz meg a szoftverkomponensek viselkedéséhez és telepítéséhez, továbbá közös szolgáltatásokat és API-t definiál az eszközök és alkalmazások hordozhatóságának érdekében.

A hordozhatóságra egy konkrét példa a 4. ábrán látható. Ennél a példánál, ugyanarra a DCU–214 típusú kártyára építkezve, széles sávú spektrum megfigyelő és radaralkalmazást megvalósító szoftverkomponenseket láthatunk.

A szoftvervevő / -vevőrendszer koncepció

A hagyományos rádiót számos rendszerterv különálló alrendszerekre bontja: RF–KF lekeverés, alapsávi átalakítás és demoduláció, ember–gép interfész elemek. Az SDR-platform magas szintű működési modellje (5. ábra) azonban pusztán három főelemből áll: az analóg front-end, a tartomány átalakítás és digitális back-end.



5. ábra. SDR-alapú rádió

Az analóg front-end felelős a frekvenciakeverésért, az átvitt jelek frekvenciája és a digitálisan feldolgozható frekvencia és sávszélesség között. A front-end analóg erősítőkből, keverőkből, szűrőkből és frekvenciaforrásokból áll. A tartomány-átalakítók, amelyek az analóg és digitális tartományok közti átalakításért felelősek, nagy sebességű, széles sávú analóg–digitális (A/D) és digitális–analóg (D/A) átalakítókra épülnek. A tartomány-átalakítás tulajdonságai nagymértékben befolyásolják a szoftverrádió-platform funkcionalitását. A digitális back-end a szoftverkomponensek futtatásához FPGA-alapú konfigurálható és/vagy DSP-alapú programozható számítási erőforrásokat tartalmaz.

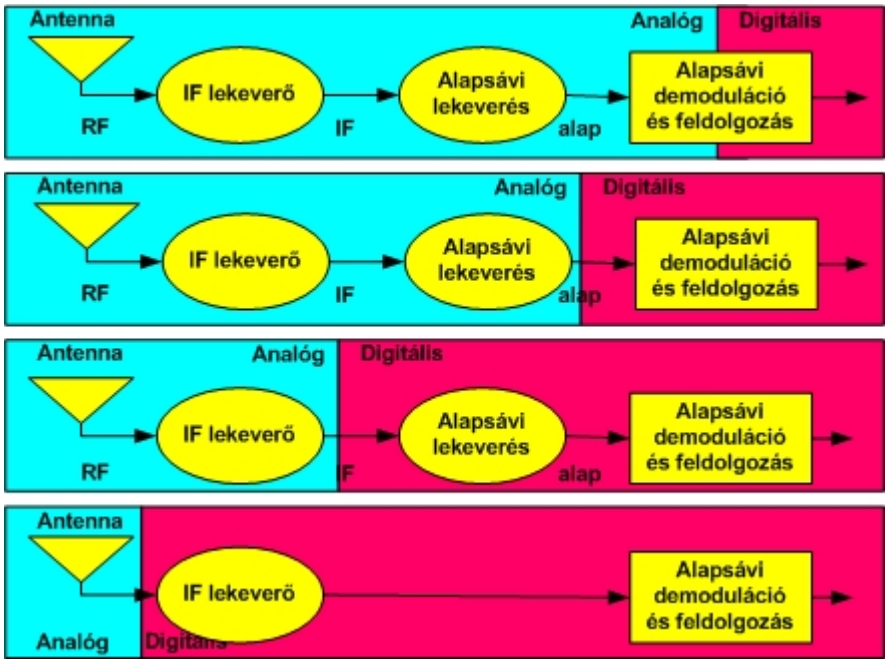
A fentiekben bevezetett felosztással a rádió célja, hogy lekeverje és szűrje a kívánt frekvenciasávot és utána digitalizálja a jelet. Hasonlóképpen, a digitális feldolgozó egység célja a digitális adatok fogadása és az információ kinyerése.

Fontos pont, amit meg kell érteni, hogy a digitális vevő nem egyezik meg a digitális rádiózás és digitális rádiómoduláció fogalmával! A digitális vevőkészülékek felhasználhatók bármely típusú moduláció vételére, beleértve bármilyen analóg vagy digitális modulációs szabványt, azaz kiválóan alkalmas AM vagy FM modulált analóg jelek vételére is.

Továbbá, mivel a jel feldolgozásának nagy része digitálisan történik, az egész rádió számos működési paramétere szoftveres úton szabályozható. A digitális rádió alapvető tulajdonsága az átkonfigurálhatóság lehetősége, ami lehetővé teszi, hogy szoftverrádió-alkalmazások hardverplatformjaként szolgáljon. Az SDR technológia tehát arra az alapelvre épül, hogy az analóg és digitális tartományok közti átalakításnak olyan közel kell kerülnie az antennához, amennyire csak lehet, biztosítva ezáltal a jelek digitális kezelhetőségét. A tartomány-átalakítás helyétől függően szoftverrádió-implementációk különböző szintjei létezhetnek.

Az átkonfigurálhatóság alapfunkciójának eléréséhez azonban rugalmas hardverplatformnak kell rendelkezésre állnia, függetlenül a megvalósított implementációs szinttől.

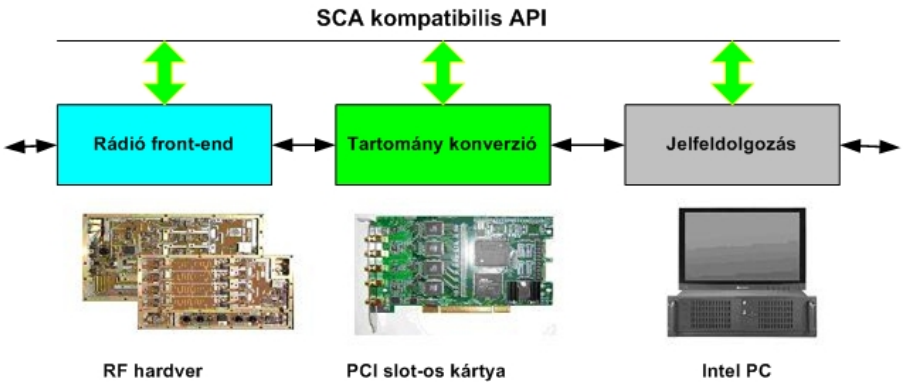
Az analóg–digitális tartomány átalakításának helyétől függően (6. ábra) az SDR technológia megvalósítási szintje a digitális jelkezeléstől kezdve, a digitális alapsávon keresztül, digitális KF vagy akár digitális RF szintekbe sorolható be. Ez az oka annak, hogy az átalakítók tulajdonságai miért annyira fontosak. Meghatározhatja az egész megoldás implementációs szintjét.



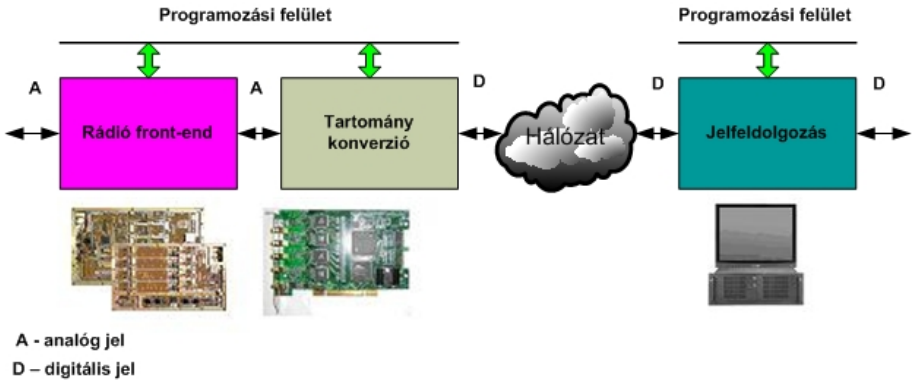
6. ábra. A megvalósítási szintek

A 7. ábrán egy kísérleti SDR-platform elemei láthatók. Készen használható megoldásokat fejlesztettünk ki az analóg rádió front-endhez (hagyományos rádiófrekvenciás hardver formájában) és a széles és keskeny sávú tartománykonverzióhoz (PCI-interfészhez csatlakoztatható kártya formájában). A jelfeldolgozás kereskedelmi forgalomban kapható PC-vel történik, amely vezérlési platformként is szolgál.

A vevőkészülék funkcióinak fenti szeparálása lehetővé teszi, hogy a rendszer egyes elemei egymástól távol üzemeljenek és az interneten keresztül tartsák a kapcsolatot (8. ábra). A megfelelő hálózati erőforrással lehetővé válik a jel mintáinak real-time továbbítása, hogy a feldolgozás egészen máshol történhessen meg.

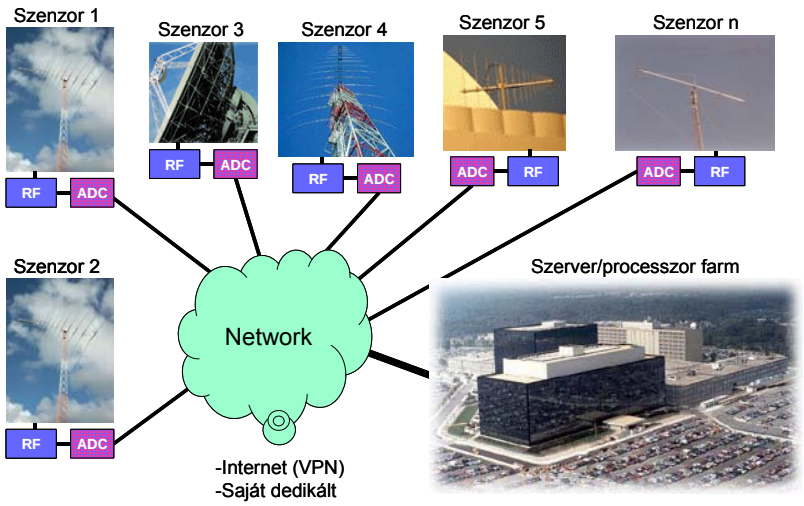


7. ábra. A kísérleti SDR-platform



8. ábra. Vevőkészülék-funkciók szeparálása

Az ilyen módon felépített szoftverrádiókból összetett rendszer hozható létre (9. ábra), amelynél a rádiós szenzorokból álló hálózat nagy területeket fedhet le. A szenzorok hálózata pedig komplex feladatok valósíthat meg, mint például iránymérés, vagy rádióforrás helyének meghatározása.

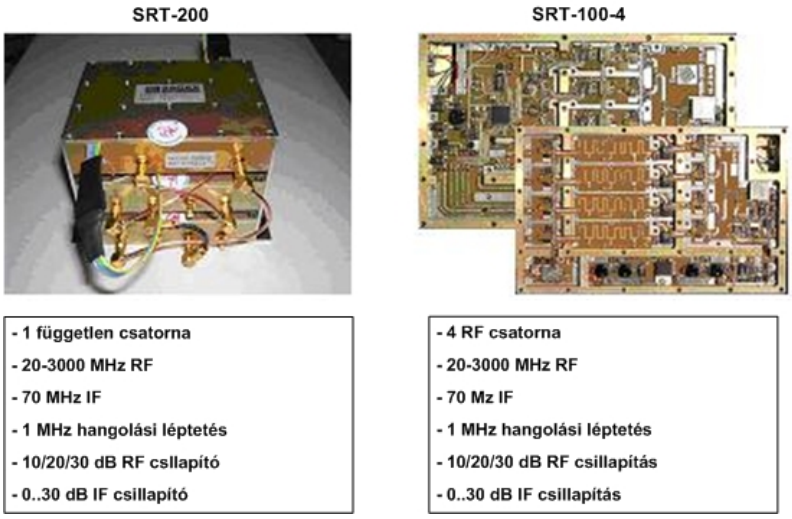


9. ábra. Szoftverrádió-alapú vevőrendszer

Rendszerkomponensek

Rádió front-end

Az alapvető építőelemek száma alkalmazástól függ, amely lehet vevő, adó vagy adóvevő, egy- vagy többvivős rendszer, és többvivős esetben független vagy fázissoros. A frekvenciát és erősítést szabályozó elemeket belső beépített mikrokontrollerek, vagy közvetlenül az alkalmazás, vagy digitális processzor vezérelheti, ha nagy sebességű feldolgozásra van szükség.

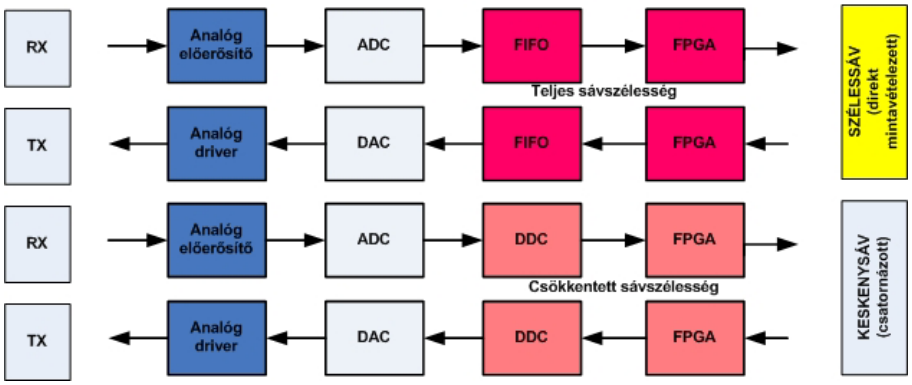


10. ábra RF front-endek

VHF/UHF alkalmazás esetén, ahol akár 3 GHz-es frekvencia-lefedettség is szükséges, egy pótlólagos frekvencia-kiterjesztő egység és még egy helyi oszcillátor kerül alkalmazásra. Az alkalmazás igényei határozzák meg az egységek számát. A 10. ábrán két RF front-end megvalósítás látható. Az első front-end 1 független csatornával rendelkezik, míg a második 4 RF csatorna szimultán feldolgozására képes. A többi paraméter meglehetősen hasonló.

Átalakítási technológia

Jelenleg két alapvető tartomány-átalakító kártyát kínálunk (blokkvázlatuk az alábbi ábrán látható).

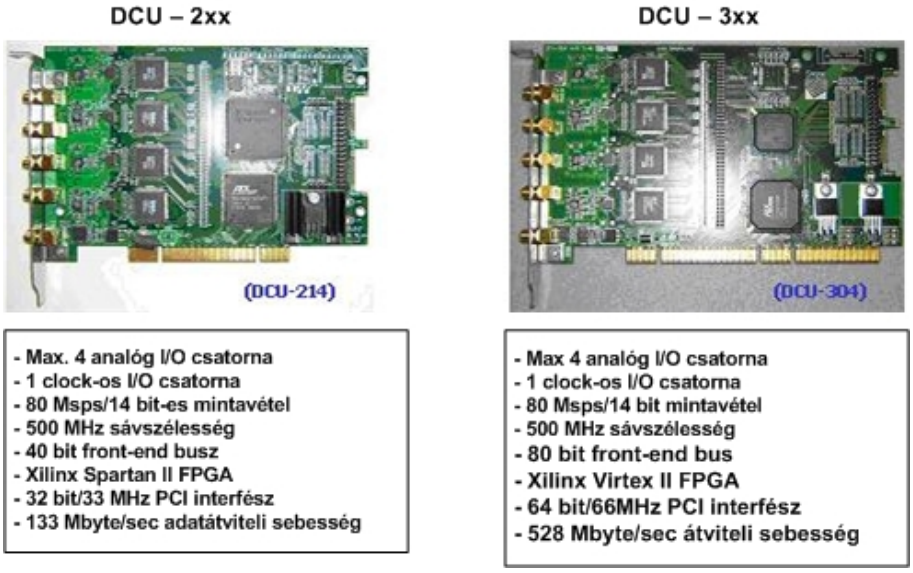


11. ábra. Széles és keskeny sávú átalakítók

Az egyikük széles sávú, ami azt jelenti, hogy a digitalizált mintákat egy nagy sebességű FIFO memóriában tárolja. A mintákhoz az FPGA-ban megvalósított digitális pre-processzor is hozzáférhet, olvasás vagy írás céljából, küldés vagy vétel üzemmód esetén. Ilyen módon az átalakító hardver nem limitálja az adat sávszélességét. Általában a sávszélességet az átalakító és digitális processzor közti digitális interfész határolja be, például a PCI-busz. Feltételezve, hogy rendelkezünk elég erőforrással, sávszélesség-csökkentést is meg lehet valósítani a kártyán lévő, konfigurálható FPGA-val.

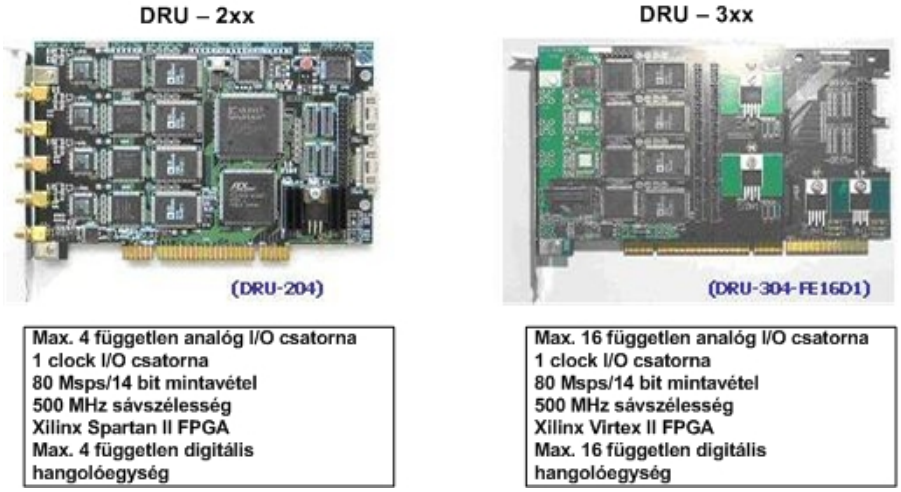
A konverter-család második típusa egy keskeny sávú vagy egy csatornás átalakító. Ennél az esetnél dedikált, csatorna választó, hardverkomponenseket építettünk be a pre-processzor és átalakítók közé. A sávszélesség-csökkentést digital down-converter (DDC) és digital up-converter (DUC) oldja meg rendre a vételi és az adó oldalon. A digitális hangolók ASIC-chipekben kerültek megvalósításra a feldolgozó elemek terhelésének optimalizálása végett.

A 12. ábrán két széles sávú átalakító látható. Az első átalakító a DCU-2xx termékcsalád tagja; 4 csatornával és egy 32-bites PCI-interfésszel rendelkezik. A DCU-3xx termékcsalád átalakítói szintén 4 csatornát képesek feldolgozni, és 64-bites PCI-interfésszel csatlakoznak a számítógéphez.



12. ábra. Széles sávú átalakítók

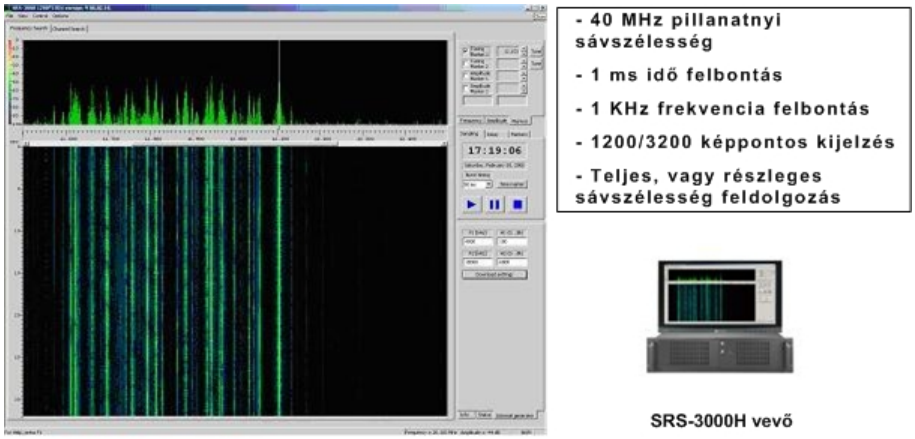
A 13. ábrán két keskeny sávú átalakító látható. Az első átalakító a DRU-2xx termékcsalád tagja; 4 csatornával és egy 32-bites PCI-interfésszel rendelkezik. A DRU-3xx termékcsalád átalakítói 16 csatornát képesek feldolgozni, és 64-bites PCI-interfésszel csatlakoznak a számítógéphez.



13. ábra. Keskeny sávú átalakítók

Megvalósított berendezések

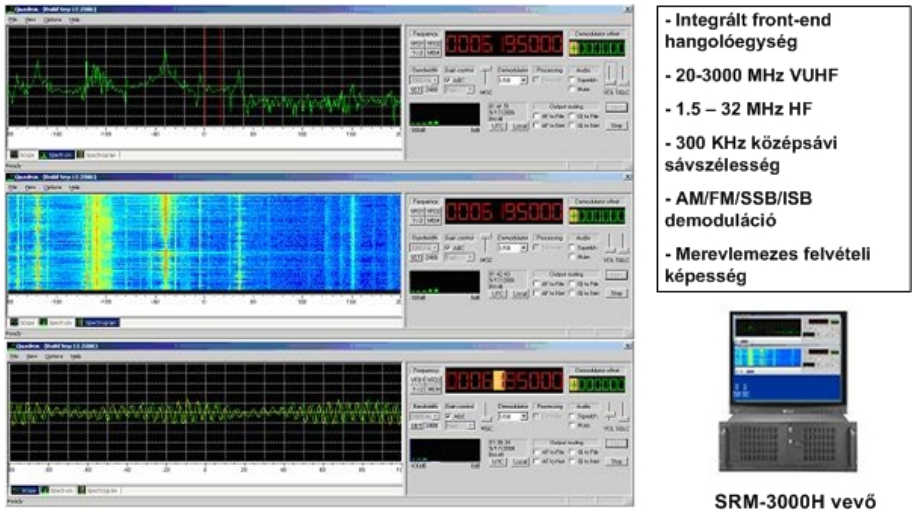
Széles sávú panoráma-vevőkészülék



14. ábra. Széles sávú panoráma-vevőkészülék

Az első példa (14. ábra) egy megvalósított berendezésre a széles sávú átalakítóra épülő széles sávú panoráma-vevőkészülék, amely képes a spektrum 40 MHz-es pillanatnyi sávszélességét megjeleníteni, 1 kHz-es felbontással. Ebben az esetben a spektrumbecslés digitális feldolgozás útján történik, és a Windows grafikus interfész használatával válik lehetővé a széles frekvenciatartomány megjelenítése. Ez a típusú vevőkészülék összetettebb spektrumkezelő rendszerbe is integrálható.

Monitoring-vevőkészülék



15. ábra. Monitoring-vevőkészülék

A monitoring-vevőkészüléknél (15. ábra) a keskeny sávú átalakító kerül felhasználásra a bejövő 40 Mhz sávszélességű és 1,5 MHz-től 32 MHz-ig behatárolt HF sáv digitalizálására, tehát ebben a sávban direkt digitális vevőnek tekinthető (direct digital receiver – DDR). A készülék a teljes 40 MHz-es sávszélességből 300 kHz pillanatnyi sávszélességet biztosít a digitális demodulátorok számára, azaz képes az ebbe a tartományba eső rádióállomások vételére.

Összegzés

Az előadás célja a szoftverrádió-technológia rövid ismertetése volt, amelynél először a technológia alapjai és a technológiához kapcsolódó legfontosabb szervezetek kerültek bemutatásra. Ezután egy SDR technológiára épülő, összetett feladatokat is elvégezni képes vevőrendszer-koncepció ismertetése következett, majd a cikket konkrét, megvalósított rendszerkomponensek áttekintése zárta.

A fent bemutatott, gyakorlatban is azonnal hasznosítható eredmények, termékek mutatják a nemzetközileg is versenyképes kutatás–fejlesztési kapacitást a szoftverrádió-technológia területén. Ezzel kapcsolatban záró gondolatként érdemes megjegyezni, hogy a nemzeti ipart a nemzeti megrendelések teremtik meg.

MISKOLCZI JÓZSEF OKL. MK. ALEZREDES

A MAGYAR HONVÉDSÉG ELEKTRONIKAI HADVISELÉSI ERŐI ÉS ESZKÖZEI, ALKALMAZÁSUK LEHETŐSÉGEI

A jelenlegi helyzet

A haderő-átalakítás, valamint a kor színvonalának megfelelő technikai fejlesztések elmaradása következtében egyre inkább háttérbe szoruló EHV[1] erők lehetőségei napjainkra teljesen beszűkültek.

A szárazföldi erőknél a haderő-átalakítás következtében mindössze **egy szakasz szintű elektronikai-harc alegység** maradt meg.

A légierőnél jelenleg nincs elektronikai hadviselési képesség, a légvédelmi zavarózászlóaljat 2001-ben felszámolták, a Mi–17PP zavaróhelikoptereket kivonták. A JAS–39 EBS HU Gripeneknél az elektronikai hadviselési képesség csak a repülőgépek aktív és passzív önvédelmére korlátozódik. A PCC vállalás keretében felmerült egy NATO által támogatott, többnemzeti összefogással történő zavarókonténer-fejlesztés, amelyben Magyarország megfigyelői minőségben tanúsított érdeklődést. A program célja az európai légierők jelenleg elégtelen támogató zavaróképességének 2009 nyarától – esetleg már egy-két évvel korábbi időponttól – történő ütemes pótlása. A támogató zavarás (Support Jamming) jellemzően a csapásmérő légikötelékek védelmét szolgáló harcbiztosítás a földi telepítésű légvédelmi fenyegetéssel szemben (SEAD – Suppression of Enemy Air Defence). A programnak magas a költségigénye, országonként elérheti a 2–4 milliárd forintot. Egy ilyen szervezeti elem rendszeresítése, rendszerben tartása – esetlegesen felajánlott erőként –, az egyszeri beszerzési és integrálási költségeken túlnyúló jelentős költségigényű kötelezettségvállalást jelentene. A tervezett zavaró konténer csak a kétüléses repülőgép-változatba integrálható, mivel kezelőszemélyzetet igényel.

A szárazföldi csapatoknál rendszerben lévő elektronikai hadviselési szakasz **jelenleg csökkentett képességekkel** rendelkezik.

A rádióelektronikai védelem területén a jelenleg alkalmazott híradó és fegyverirányító eszközök paraméterei miatt a szervezési és technikai rendszabályok csak korlátozott védelmet biztosítanak, a rendszabályok ismeretszintje alacsony.

Az elektronikai ellentevékenység elleni védelemre a kezelőállomány ilyen irányú kiképzés hiányában nincs felkészítve.[2]

Jelenleg technikailag és szervezetileg még nincs kialakítva a szövetségi felderítő és elektronikai-harc informatikai rendszerhez való kapcsolódás (ISTAR[3], EWCC[4], SEWOC[5]).

---

[1] EHV – elektronikai hadviselési (elektronikai-harc).

[2] Kivéve a légierőnél évente végrehatott NATINADS gyakorlatba bevont erőket és eszközöket.

[3] ISTAR – Intelligence, Surveillance, Target Acquisition, Reconnaissance – hírszerzés, megfigyelés, célmegjelölés, felderítés.

Az elektronikai hadviselés doktrinális alapjai

A Magyar Honvédség Összhaderőnemi elektronikai hadviselési doktrínájából:

„Az elektronikai hadviselés tervezése egy egységes elektronikai hadviselési értékelési folyamat része, melynek célja, hogy hiteles képet nyújtson az elöljárónak az elektronikai hadviselési helyzetről, és a rendelkezésre álló adatokból levont következtetésekre alapozott, cselekvési változatba foglalt javaslat kerüljön kidolgozásra a katonai művelet támogatására."

„A katonai műveletek elektronikai hadviselési támogatását biztosító szakcsapatokra a szövetségben nem alakult ki egységes gyakorlat. A támogatás a szárazföldi erő szervezeti szintjétől függően szakasz, század vagy zászlóalj erő. A szakasz, mint bázisszervezet, a dandárszintű telepíthető erő elektronikai hadviselési támogatását hivatott biztosítani."

„A válságreagáló műveletek a korábbi fejezetekben az elektronikai hadviselés aspektusában tárgyalt műveletektől eltérően – a Magyar Honvédség Összhaderőnemi Doktrínájának 20. főcímében lefektetett elveknek megfelelően –, minden esetben többnemzeti műveletek. Ezekben a műveletekben az elektronikai hadviselés elsődleges feladata a biztonságot fenyegető veszélyek előrejelzéséhez való hozzájárulás, valamint a cselekvési szabadságot támogató elektronikai védelem biztosítása. A válságreagáló műveletekben a nemzeti erők hadműveleti és harcászati szintű elektronikai hadviselési támogatása nemzeti felelősség, amelyet az azokban történő részvétel esetén figyelembe kell venni."

„Az elektronikai védelem valamennyi válságreagáló művelethez szervesen hozzá tartozó tevékenység. Minden szintű parancsnoknak számolnia kell azzal, hogy a válság bármely szereplője rendelkezhet a koalíciós erők tevékenységének megfigyelésére, fenyegetésére vagy akadályozására alkalmas elektronikai eszközökkel. Az elektronikai védelem a válságreagáló műveletekben az elektromágneses spektrum saját célokra történő rendelkezésre állásának biztosítása mellett hozzájárul az átfogóan értelmezett műveleti biztonsághoz[6]."

A doktrinális követelmények az alábbi szövetségesi szabályzók alapján lettek kialakítva:

- AJP–3.6 Szövetséges összhaderőnemi elektronikai hadviselési doktrína;
- ATP–44 (AJP 3.6.1) Elektronikai hadviselés a légi hadműveletekben;
- ATP–51 (AJP 3.6.2) Elektronikai hadviselés a szárazföldi harcban;
- MC 64/9 – NATO elektronikai hadviselési (EW) irányelvek.

[4] EWCC – Electronic Warfare Coordiantion Cell – elektronikai hadviselési koordinációs részleg.
[5] SEWOC – SIGINT and Electronic Warfare Opreation Centre – jelfelderítő és elektronikai hadviselési műveleti központ, ami a SIGINT COMINT-ból (rádiófelderítés) és az ELINT-ből (rádiótechnikai felderítés) áll.
[6] OPSEC – Operations Security – műveleti biztonság.

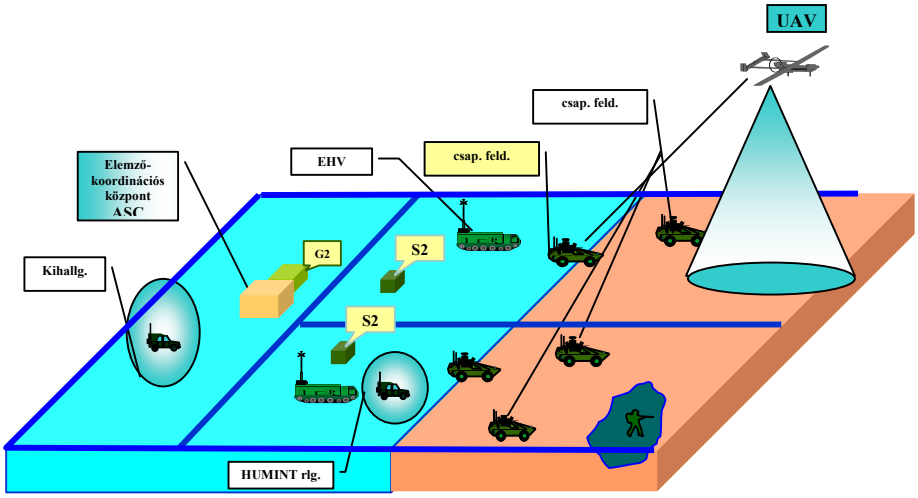
A szövetségesi követelmények

A NATO 2006–2016 közötti időszakra vonatkozó haderőtervezési javaslata Magyarország részére (2006 Force Proposals for Hungary) **több, az elektronikai hadviselési képességgel kapcsolatos feladatot határoz meg. Ezek közül** az okmány összemérhető elektronikai hadviselési képességet jelöl meg **a NATO vezette nemzeti kötelékek támogatására**.

A konkrét technikai követelmények egy-egy dandár elektronikai hadviselési képességének kialakításához:

- kettő iránymérő alap[7] (minimum három rádió-iránymérő állomás egységes vezénylésével);
- lehallgató munkahelyek, amelyek egyidejűleg hat HF, VHF, UHF és SHF frekvenciasávban működő eszközök felderítésére képesek;
- rádiótechnikai felderítő képesség meghatározott frekvenciatartományban;
- értékelő–elemző központ, ahol megvalósul a NATO szövetségi felderítő és elektronikai hadviselési informatikai rendszerhez történő kapcsolódás;
- kettő kommunikációs mobil zavaróállomás.

Az AJP 2.1 (Felderítő eljárások) 1. fejezet IX. rész 114. pontja a felderítést – és ezen belül az elektronikai felderítést – a **nemzeti felelősség körébe** utalja.



1. ábra. Az ISTAR-képességek

[7] Az iránymérő alap URH tartományban állomásonként 30–50 km (a metszésponti hibaháromszög minimális értékére való törekvés érdekében).

A NATO az EL 0583 számú haderő-fejlesztési célkitűzésben azt az elvárást rögzíti, hogy az általa vezetett műveletekhez felajánlott erők 2006-tól – a felderítés vonatkozásában – ISTAR-képességekkel rendelkezzenek. Ez magában foglalja a hagyományos és technikai felderítés mellett a tüzérségi röppálya-felderítő radarok, valamint pilóta nélküli repülőgépek és elektronikai-harc elemek alkalmazását.

Az ISTAR-alegységek vezetése és irányítása C2 (vezetési és irányítási) modulon keresztül valósul meg.

Az ISTAR-elemek feladatai

a) **Harcászati felderítés és megfigyelés** páncélozott felderítő járművekkel, illetve pilótanélküli eszközökkel, szenzorokkal, földi mozgócél felderítő radarokkal.

b) **Célfelderítés végrehajtása** automatizált tűzvezetési rendszeren keresztül, a tüzet kiváltó eszközökről közel valós idejű adatcserét biztosító radarrendszerekkel.

c) **Elektronikai hadviselési képesség** (EL 3140, 1/b szerint).

Egy dandár alkalmazásakor egy EHC század tevékenységével kell számolni.

d) **A HUMINT- és SIGINT-képességek szövetségesi** információihoz és adatfeldolgozó képességeihez való hozzáférési lehetőség.

A korszerűsítés és fejlesztés fő célkitűzései

A fenti követelmények elérése érdekében elengedhetetlen a technikai és szervezeti korszerűsítés végrehajtása, az alábbi alapelvek szem előtt tartása mellett:

- egyedi képesség növelése, az erők védelme (Force Protection);
- kapcsolódás más rendszerekhez;
- hatékonyság és szükségszerűség;
- finanszírozhatóság.

Az ISTAR-képességekkel rendelkező alegység hatékonysága nagyságrendekkel növekszik a hagyományos felépítésű szervezetekkel szemben. Alkalmazása sokrétű, a rendelkezésre álló technikai lehetőségek békében, veszélyeztetettség időszakában, konfliktus során, és a terrorizmus elleni küzdelemben is bevethetők.

Az ISTAR-képességek kialakítása azért is különösen indokolt, mert Magyarország 2005-től nem folytatja az AGS[8] programban való részvételét, így a szövetségi rendszerben csak ez a felület marad meg **harcászati felderítő információszerzésre és -cserére**.

[8] AGS – Allied Ground Surveillance – szövetségi földfelszíni megfigyelés.

A 2015-ig terjedő haderőfejlesztési tervben rögzített, az ISTAR-képességek létrehozására vonatkozó beszerzések megvalósulása esetén – a harcászati szintű pilóta nélküli eszközök rendszeresítését is beleértve –, hazánk megfelel az ISTAR alapvető követelményeinek. A korszerű elektronikai-harc eszközök alkalmasak lesznek analóg és digitális jelforrások felfedésére, lehallgatására, a helyzettől függően annak lefogására vagy dezinformálására, valamint a parancsnoki döntés támogatására.

Napjainkban a műveleti területeken naponta kapunk híreket házi készítésű robbanóeszközök alkalmazásáról. Ezek között a távvezérelt eszközök is megtalálhatók. Az ellenük való védekezés összetett, nagyfokú körültekintést, valós információs és technikai biztosítási hátteret igényel.

Kiegészítő elektronikai-harc elemek alkalmazása esetén (RCIED[9] zavaróberendezések) biztosíthatóvá válik a katonai konvojok, VIP[10] személyek, katonai objektumok, harcálláspontok oltalmazása a távvezérelt házi készítésű robbanó szerkezetekkel szemben.

Az új kihívások megfelelő kezelése és az erők megóvása érdekében a Magyar Honvédségnek is fel kell készülni ilyen típusú, speciális elektronikai hadviselési eszközök beszerzésére.

A javasolt technikai fejlesztések

Az elektronikai hadviselés előírt szintjének elérése érdekében megfogalmazásra kerültek azok az alapvető elvárások, amelyeket a Haditechnikai Fejlesztési Kabinet 2006 márciusában jóváhagyott. Az alábbiakban ismertetésre kerülő technikai fejlesztési elképzelések nem egy konkrét technikai eszközre vonatkoznak, általános követelményeket írnak le, amelyek az alapjait képezhetik a tíz éves tervidőszak aktualizálása során kiírásra kerülő beszerzéseknek. A technikai lehetőségek rohamos fejlődése, a műveleti tapasztalatok értékelése és feldolgozása következtében adott esetben új kihívásoknak is meg kell felelnünk.

- **Értékelő–elemző központ**

Az eszköznek képesnek kell lennie egy-két főkészlet rádiótechnikai felderítő állomásról, három–hat RH–URH rádiófelderítő és -iránymérő állomásról érkező előfeldolgozott adatok kiértékelésére, feldolgozására, az EWCC (SEWOC) részére a döntéshozatalhoz szükséges adatok előállítására, valamint a rádió-iránymérés vezénylésére.

- Az **informatikai rendszer** fejlesztése részét képezi a NATO rendszerű elektronikai hadviselési erőforrás-tervezést és -vezetést biztosító Elektronikai Hadviselési Koordinációs Részleg (EWCC), illetve a napjainkban egyre inkább alkalmazásra kerülő Rádióelektronikai felderítő és Elektronikai Hadviselési Műveleti Központ (SEWOC) kialakításának. Az EWCC, illetve a SEWOC az elsődleges eszköz a rádiófelderítés és az elektronikai hadviselés közvetlen irányításában.

[9] RCIED – Remote/Radio Controlled Improvised Exposive Devices – távirányítású robbanó eszközök.
[10] VIP – Very Important Person – kiemelten fontos személy.

■ A HM Hadműveleti és Kiképzési főosztály – NATO forrásból – rendelkezik (vagy a későbbiekben rendelkezni fog) azon szoftverek többségével, amelyek a SEWOC vagy EWCC hardver eszközeire telepítendők a rendszer kialakítása érdekében. Ezek **a szoftverek** a következők:

- **NATO kisugárzási adatbázis program** (NEDB), mely biztosítja mind a vezetési, mind a végrehajtói szinteken a nem kommunikációs kisugárzó eszközök (radarok) kisugárzási paramétereinek NATO egységes formátumú menedzselését és használatát;

- **frekvencia menedzsment adatbázis**, amely biztosítja a kommunikációs rádióberendezések kisugárzási paramétereinek, valamint az MH rádióforgalmi rendszerek nyilvántartását, a tiltott (TABOU) és lehallgatásra kijelölt frekvencia táblázatot;

- **NATO elektronikai hadviselés helyzetértékelő szoftver** (NEOBAT), amely a rádiólokációs eszközök lefedettség értékelését biztosítja;

- **láthatósági ábrázoló terepmodell és terjedés előrejelző–számító program**, amelyek a két pont közötti láthatóságot és az összeköttetés valószínűségét határozzák meg.

■ **Az értékelő elemző munkahelyek működtetéséhez szükséges:**

- a **GeoMedia**[11] térinformatikai szoftver és digitális térkép;

RH/URH rádiófelderítő-iránymérő állomás gépkocsin

Az eszköznek képesnek kell lenni a HF, VHF, UHF és SHF frekvenciatartományú analóg és digitális modulációjú jelek vételére, iránymérésre, illetve biztosítani kell a távvezérelhetőséget (master/slave) az adatfeldolgozó-értékelő központból. Lehetőséget kell biztosítani a helyi (előzetes) és a táv-adatfeldolgozásra (analízis, szintézis) a hozzá tartozó megfelelő sávszélességű adatcsatorna kialakításával.

Biztosítani kell a felfedett és lehallgatásra kijelölt csatornák digitális jelrögzítését későbbi elemzés, fordítás (esetleg dezinformációs anyag elkészítése) érdekében.

A könyvtárban letárolt korábbi mérési adatokra támaszkodva a rendszernek ki kell mutatnia, hogy az észlelt sugárzás milyen rádióforgalmi rendszerből származik, az saját vagy idegen, meg lehessen határozni annak harcrendben elfoglalt helyét, szerepét, veszélyességi fokát, veszélyesség szerinti prioritási sorrendet lehessen felállítani.

Az eszköznek öntanulónak kell lenni, azaz az először mért jelparamétereket a parancsnok döntése alapján be kell tudni írni a saját adatkönyvtárába, egyre bővítve a könyvtár tartalmát.

[11] A GraphIT Kft. által forgalmazott GeoMedia programcsomagból a GeoMedia Professional, Terrain, ActiveFlight és GeoDex modul katonai alkalmazása.

Rádiótechnikai felderítő állomás gépkocsin

Az eszköznek képesnek kell lenni autonóm üzemmódban működni az önálló, három sávra felosztott (100–1000 MHz, 1–18 GHz és 18–40 GHz frekvenciatartományú) vevő- és iránymérő munkahelyeken, illetve biztosítani kell a távvezérelhetőséget (master/slave) az értékelő–elemző központból. Lehetőséget kell biztosítani a helyi (előzetes) és a táv-adatfeldolgozásra (analízis, szintézis), a hozzá tartozó megfelelő sávszélességű adatcsatorna kialakításával.

A könyvtárban letárolt korábbi mérési adatokra támaszkodva a rendszernek ki kell mutatnia, hogy az észlelt sugárzás milyen rádióforgalmi rendszerből származik; az saját vagy idegen, hogy meg lehessen határozni annak harcrendben elfoglalt helyét, szerepét, veszélyességi fokát (felderítés–követés–tűzvezetés), veszélyesség szerinti prioritási sorrendet lehessen felállítani.

A berendezésbe beépített precíziós mérőműszerek (például spektrumanalizátor) segítségével lehetővé kell tenni a nem kommunikációs adatbázisban szereplő adatok ellenőrzését, pontosítását.

Az eszköznek öntanulónak kell lenni, azaz az először mért jelparamétereket a parancsnok döntése alapján be kell tudni írni az adatkönyvtárba, egyre bővítve a könyvtár tartalmát.

A felderítés során maximális detektálási valószínűséget és nagy vételi dinamika tartományt kell elérni.

RH–URH zavaró állomás

Az eszköznek képesnek kell lenni az értékelő–elemző központból távvezérelt üzemmódban vagy autonóm üzemmódban működni HF, VHF, UHF és SHF frekvenciatartományban, megfelelő sávszélességű adatcsatorna kialakításával.

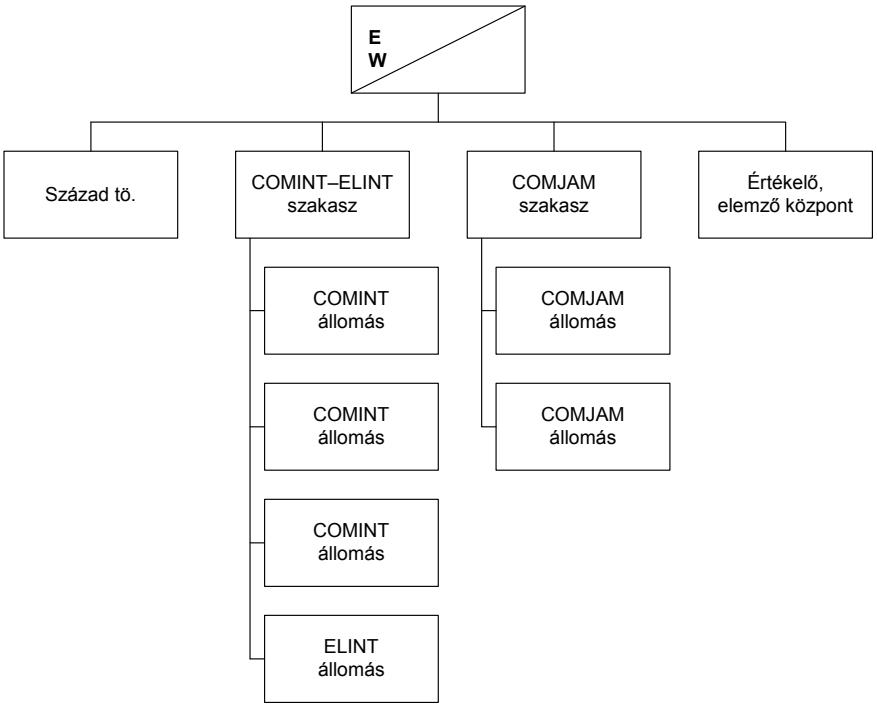
Biztosítani kell a felfedett, lehallgatásra kijelölt és zavarásra kijelölt csatornák adatbázisban történő rögzítését csakúgy, mint a tiltott frekvenciák tárolását. A zavaró állomás legyen alkalmas széles sávú és célzott zavarások végrehajtására analóg és digitális modulációs módok alkalmazásával.

A javasolt szervezeti módosítás

A felderítő-zászlóalj kötelékében kialakításra kerülő elektronikai hadviselési század a 2006. évi NATO Blue Book ajánlásait és a most ismertetett fejlesztési elképzeléseket figyelembe véve került megtervezésre (2. ábra).

A javasolt ütemezés

A rádióelektronikai felderítő és elektronikai hadviselési erők (aktív és passzív eszközök) fejlesztését, alkalmazásra történő készenlétük elérését **két lépcsőben tervezik megvalósítani**.



2. ábra. Elektronikai hadviselési (EW) század felépítése (tervezet)

Az első lépcsőben tervezett feladatok (2008-ig)

- A MH ÖHP alárendeltségében a MH 5/24. felderítő-zászlóalj felderítő támogató század EHV szakaszának századdá alakítása, a személyi állomány feltöltése, a kijelölt technikai eszközök alkalmazása.

- A személyi állomány szakharcászati, nyelvi és szaktechnikai felkészítésének megkezdése, illetve folytatása az MH oktatási rendszerében, együttműködésben a NATO kiképzési és felkészítési rendszerével.

- A rádióelektronikai felderítő szakbeosztású tiszthelyettesek célirányos felkészítése és gyakoroltatása.

- A század – meglévő eszközeivel és hordozó járműveivel –, alkalmazásra történő felkészítése, a technikai eszközök kiegészítése.

- A GRIPEN vadászrepülőgépek felderítő és elektronikai hadviselési eszközei alkalmazói követelményeinek kidolgozása.

- A felhasználói követelmények meghatározása és felterjesztése a kialakítandó végleges rádióelektronikai felderítő és elektronikai hadviselési (aktív és passzív) szaktechnikai eszközpark kutatási, fejlesztési és rendszerbe állítási feladataihoz. A rádióelektronikai felderítő eszközök esetében a hazai fejlesztés lehetőségeinek vizsgálata, az elektronikai hadviselési eszközök esetében a külföldi piackutatás és beszerzés részesíthető előnyben.

A második lépcsőben tervezett feladatok (2009–2015)

- Egy készlet értékelő–elemző központ beszerzése és rendszerbe állítása a beszerzésre kerülő felderítő–iránymérő berendezések irányítására, a felderített adatok feldolgozására és a szövetségi felderítő–elektronikai hadviselési adatközpontokkal való kapcsolattartásra.

- Három készlet RH–URH rádiófelderítő és -iránymérő állomás beszerzése és rendszerbe állítása.

- Egy készlet mobil rádiótechnikai felderítő állomás beszerzése és rendszerbe állítása.

- Az elektronikai ellentevékenység eszközrendszerének fejlesztése két készlet kommunikációs zavaró állomás beszerzésével és rendszerbe állításával.

A távlati célok

A pilóta nélküli repülőeszközre épülő felderítő rendszer fejlesztésének folytatása (harcászati mélységben alkalmazható eszközök), különös tekintettel a rádióelektronikai felderítő eszközök fedélzeten történő elhelyezésére.

A perspektivikus elektronikai hadviselési eszközök alkalmazói követelményeinek megfogalmazása a digitális technológiára alapozott mobil távközlés (GSM, E-GSM), műholdas összeköttetést biztosító, navigációs (GPS), rendszerek felderítésére és lefogására.

A második lépcső 2015-re történő befejezésével a Magyar Honvédség a legfontosabb területeken olyan elektronikai hadviselési képességekkel rendelkezhet, amilyet a nemzeti katonai biztonság és a szövetségesi kötelezettségek megkövetelnek, ugyanakkor arányban vannak mind a várható nemzetbiztonsági kockázatokkal, a fenyegetettség mértékével, mind pedig a költségvetési lehetőségekkel.

SIMON GYULA MK. ŐRNAGY*

A SIGINT SZEREPE A NATO-MŰVELETEKBEN

„*Mint hidegháborús tömeghadsereg a NATO korábbi katonai gépezete átalakul és olyan erőkből fog állni, amelyek fő jellemzője a hatékonyság és a mozgékonyság lesz*." – jelentette ki James L. Jones tábornok, az Európai Szövetséges Csapatok főparancsnoka, évekkel ezelőtt egy tanácskozáson.

Ebben a szellemben hozta létre a NATO a Reagáló Erőit (NRF), melyről az Észak-atlanti Tanács (NAC) a 2002. november 21-én megtartott csúcstalálkozón döntött Prágában (1. ábra).

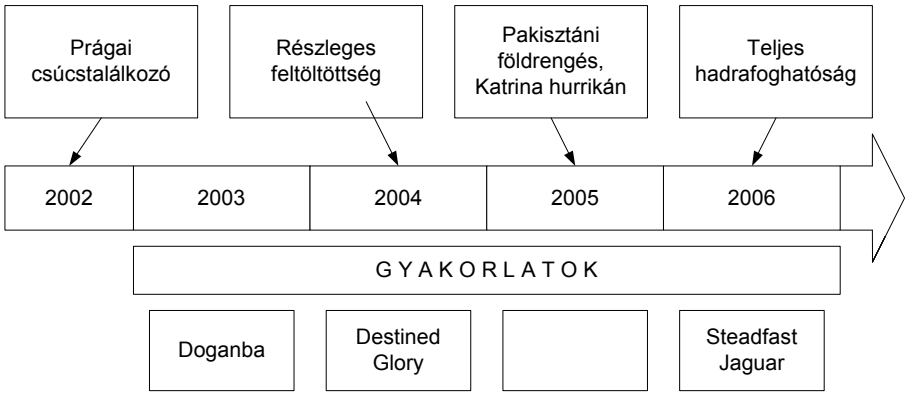
Az új haderő 2003. november 21-én, egy gyakorlat keretében mutatkozott be először, Törökországban, ahol 11 NATO-tagország elit alakulatai terrorelhárítási és mentési feladatokat hajtottak végre. A fő cél azonban az volt, hogy az NRF demonstrálja, miként igyekszik megfelelni a NAC által megfogalmazott alapelveknek. Ennek lényege egy olyan új képesség létrehozása, amely a tagországok felajánlásai alapján mindenkor biztosítja a Szövetség számára a katonai erő expedíciós alkalmazásának lehetőségét. Alapkövetelmény az együttes alkalmazhatóság, a fenntarthatóság és a folyamatos bevethetőség. 2004-re az NRF erők létszáma részleges, 68%-os feltöltöttséggel elérte a 17 ezer főt.

Egy évvel később a reagáló erők katasztrófahelyzetben is bizonyíthatták létjogosultságukat, 2005 szeptemberében a „Katrina" hurrikánnal, majd októberben a pakisztáni földrengéssel kapcsolatos segélyakciókban.

2005. október 8-án hatalmas földrengés rázta meg Pakisztánt, ami falvakat törölt el a föld színéről, kórházakat, iskolákat pusztított el. A halottak és a sebesültek száma meghaladta a 180 ezret, és mintegy 3,5 millió ember maradt fedél nélkül. Egyes pakisztáni források szerint teljes generációk tűntek el. Négy nappal azután, hogy Pakisztán 2005. október 10-én segítséget kért a NATO-tól, elindult az első segélyszállítmány a Németország és Islamabad között létesített légihídon. Öt nappal később az Incirlik (Törökország) és Islamabad között létrehozott második légihídon már az NRF repülőgépe szállított takarókat, sátrakat, tűzhelyeket a fedél nélkül maradt embereknek. A mentőakcióban az NRF műszaki és orvoscsoportja is részt vett. Összességében a reagáló erők keretében 17 NATO-tagország 1200 katonáját mozgósították.

Kijelenthetjük, hogy 2006-ra az NRF, már jelentős tapasztalattal a háta mögött, tagadhatatlanul megváltoztatta a NATO-ról addig kialakult képet. Jól bizonyított számos nemzetközi gyakorlaton. Ezek közül is ki szeretném emelni a „Steadfast Jaguar 2006" gyakorlatot, amelynek fő üzenete a tagországok felé az volt, hogy a szövetség reagáló erői kialakításának tapasztalatait, elveit és módszereit a nemzeti katonai képességek újjáformálásánál alkalmazni kell. Ezenfelül, ha a szükség úgy hozta, az NRF jól szerepelt éles helyzetekben is, ha a „Katrina" hurrikánra, vagy a pakisztáni földrengésre gondolunk.

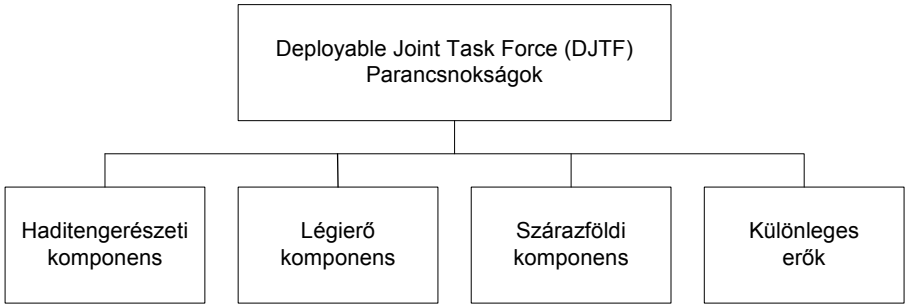
* A szerzőt időközben előléptették alezredessé.



1. ábra. A NATO Reagáló Erők (NRF) létrehozásának állomásai

Az NRF felépítése és konkrét feladatai

Az NRF a szövetség expedíciós képességének alapvető eleme. Feladata, hogy megfeleljen az új típusú kihívásoknak, a biztonságot és a stabilitást megszilárdító teljesen új követelményrendszernek.



2. ábra. Az NRF Szövetséges Gyorsreagálású Erők (DJTF) felépítése

Az NRF Szövetséges Gyorsreagálású Erők (DJTF) négy alapvető összetevőből állnak:

- haditengerészeti komponens;
- légierő komponens;
- szárazföldi komponens;
- különleges erők.

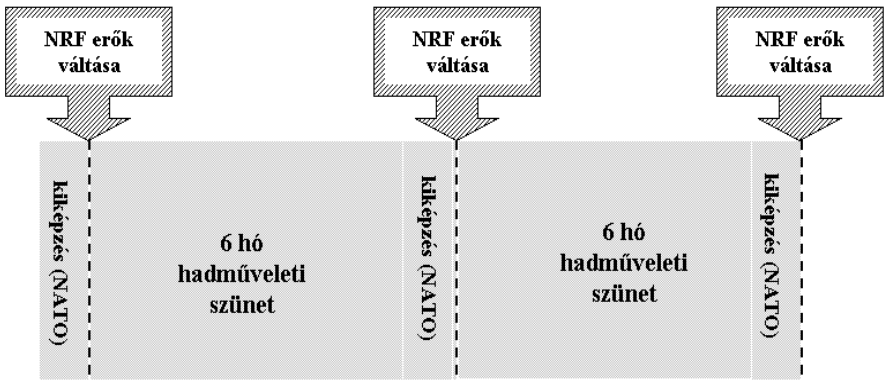
Az NRF feladatköre négy összetevő köré csoportosul:

- terrorelhárítás;
- katasztrófa-elhárítás;
- válságkezelés;
- humanitárius feladatok végrehajtása.

Az NRF alapvetően önállóan, valamint más szervezetekkel együttműködve hajtja végre feladatait. Az NRF expedíciós erők alkalmazásáról – minden esetben konszenzussal – az Észak-atlanti Tanács dönt, a személyi állományt és a technikai eszközöket pedig a tagországok biztosítják.

A SIGINT szerepe az NRF műveleteiben

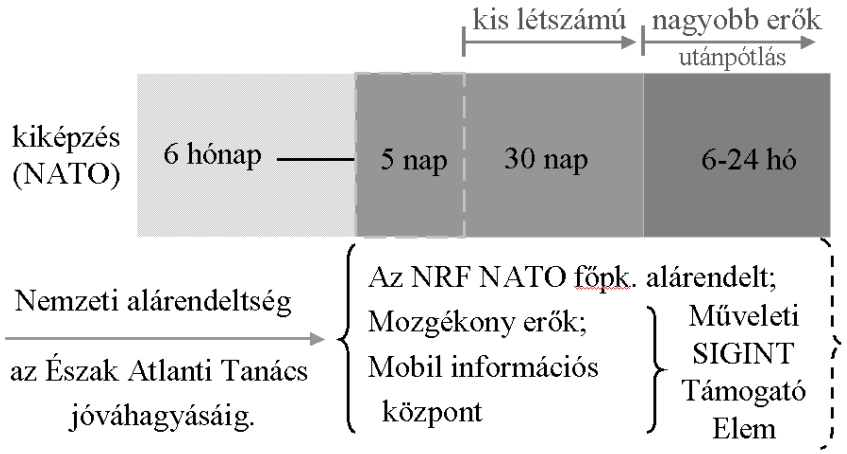
A NATO Gyorsreagálású Erők tevékenységében a SIGINT is részt veszt. Ahhoz, hogy ezt milyen módon teszi, ismernünk kell a reagáló erők kiképzésének és alkalmazásának menetét.



3. ábra. Az NRF erők alkalmazásának és váltásának rendje

A NATO Reagáló Erők létrehozása és felkészítése a még nemzeti alárendeltségbe tartozó, de az NRF-be felajánlott alakulatok kiképzésével kezdődik, melyet 6-hónapos hadműveleti szünet követ. Ebben az időszakban a felkészített expedíciós erők gyakorlatilag bármikor bevethetők. A hat hónap elteltével, ha a felkészített erők nem kerülnek alkalmazásra, végrehajtják azok váltását az időközben a NATO által kiképzett állománnyal.

A 4. ábra azt a helyzetet ábrázolja, amikor a 6 hónapos hadműveleti szünet alatt az NRF – ezen belül a SIGINT-erők – alkalmazásáról döntés születik, ahogy arra 2005 októberében is sor került.



4. ábra. NRF SIGINT-erők alkalmazása

A NAC döntését követően 5 napos készenléti idő áll rendelkezésre az expedíciós erők összeállítására és a bevetés megkezdésére. Ekkor a még nemzeti alárendeltségben lévő erők a NATO főparancsnok alárendeltségébe kerülnek. A NATO kezdetben olyan kis létszámú feladatorientált, mozgékony erőket alkalmaz, amelyek utánpótlás nélkül maximum 30 napot képesek önállóan műveleti területen működni. Harminc nap elteltével ezeket az erőket megerősítik.

Az 5 napos készenlét alatt az NATO SIGINT azokat a forrásait (eszközök, személyi állomány) használja, amelyek egyébként is rendelkezésre állnak a Parancsnoksági SIGINT Támogató Elemeknél. Ezen időszak alatt a NATO SIGINT mobil információs központok telepítésével járul hozzá az NRF munkájához, és látja el a NATO parancsnokságot SIGINT-információval. Azonban itt is végesek a tartalékok és 30 nap elteltével utánpótlásra van szükség.

Ekkor veszi át a szerepet a Műveleti SIGINT Támogató Elem. A személyi állomány biztosításáról – mint ahogy az a Parancsnoksági SIGINT Támogató Elemeknél is megfigyelhető –, nemzeti felajánlás keretében a tagországok gondoskodnak, annyi különbséggel, hogy a SIGINT személyi állomány kibővül elektronikai hadviselési (EW) szakemberekkel.

A Parancsnoksági SIGINT Támogató Elemek munkájának időtartama feladatfüggő. Alapesetben 6 hónap, de rendszerint jóval tovább, akár évekig is eltarthat.

Ehhez a munkához az NC3A[1] olyan szoftverrendszereket biztosít, mint a SAFE[2], az ASAS[3] és az RFIM[4].

- A SAFE olyan hálózati alkalmazás ami lehetővé teszi a SIGINT-információk tárolását, a rendszerből való kinyerését és szétosztását, minden olyan NATO-tagállam és arra jogosult felhasználó részére, amely rendelkezik ilyen képességgel.

- A parancsnok összadatforrású felderítési információk alapján hozza meg döntését. Ezt az igényt elégíti ki a az ASAS, amelyben a SIGINT-adatok mellett megtalálhatók más felderítési nemek (HUMINT, SIGINT, IMINT, MASINT, OSINT) adatai is, így egyfajta adatfúzió valósul meg. Az ASAS a felhasználóknak hozzáférést biztosít a BICES hálózathoz, ahová a NATO-tagországok töltik fel jelentéseiket.

- A NATO, ezen belül a NATO-SIGINT kezében egy másik fontos eszköz az RFIM rendszer. Ez teszi lehetővé a kapcsolattartást a NATO-on belül más SIGINT- és nem SIGINT-szervezetekkel, szervezeti elemekkel. Alapvető feladata a beérkező felderítési információigények és az erre érkező válaszinformációk gyűjtése nyilvántartása, szétosztása.

A NATO-SIGINT eddigi tevékenységét figyelembe véve, a Parancsnoksági SIGINT Támogató Elemek személyi állománya és mobil technikai képessége már 2003-tól támogatta és segítette a NATO gyorsreagálású erők felkészülését.

A SIGINT szerepe a jövőbeni műveletekben

A jövőben várhatóan a reagáló SIGINT-erők felépítése és alkalmazása is megváltozik. Jelenleg a Parancsnoksági SIGINT Támogató Elemek létszámhelyzete csak korlátozott mértékben teszi lehetővé az NRF személyi állománnyal történő támogatását. Ez felveti egy önálló SIGINT reagáló „csoport" kialakítását, aminek létrejötte és tevékenysége nem járna a már meglévő elemek képességcsökkenésével. Mindamellett megfelelően biztosítaná a reagáló erők információval történő ellátását, képes lenne expedíciós feladatokat ellátni és megfelelni azoknak a normatíváknak, amelyeket az NRF meghatároz számára. Természetesen ez maga után vonná a jelenlegi nemzeti hozzájárulási rendszer átgondolását. A Parancsnoksági SIGINT Támogató Elemnél eltöltött munkám során azt tapasztaltam, hogy ez jelenleg is meglehetősen problematikus pontja az együttműködésnek.

---

[1] NC3A – NATO Consultation, Command and Control Agency – NATO Műveleti Informatikai és Technikai Kutató-fejlesztő Hivatala.

[2] SAFE – SIGINT Analyst Functional Environment – SIGINT Elemző Funkcionális Környezet.

[3] ASAS – NATO All Source Analyst System – NATO Összadatforrású Elemző Rendszer.

[4] RFIM – Request for Information Management System – NATO Információs Igényeket Menedzselő rendszere.

A NATO-SIGINT is a tanulási, és ezzel együtt átalakulási időszakát éli. A kezdeti nehézségek ellenére is jó úton halad, mivel képes információkat biztosítani a NATO Reagáló Erők részére. Természetesen a magyar rádióelektronikai felderítés folyamatosan részt vesz a NATO-SIGINT munkájában. Jelen van az évről-évre megrendezésre kerülő NATO-SIGINT találkozókon, személyi állományából pedig többen dolgoznak különböző SIGINT-beosztásokban.

FELHASZNÁLT IRODALOM

- *NATO Disaster Relief Operation in Pakistan.* Brüsszel, 2006. február 28. .http://www.nato.int/shape/news/2005/news/2005/pakistan_contributions.htm
- *NRF Structure*. Brüsszel, 2006. április 5. http://www.nato.int/shape
- *Operations Research Applications Development*. Brüsszel, 2006. november. http://www.nc3a.nato.int/organization/cis.html
- *Prague Summit Declaration*. Brüsszel, 2002. november 21. http://www.nato.int/home.htm
- *The NATO Response Force – NRF*. Brüsszel, 2006. április 5. http://www.nato.int/shape/news/
- *Válasz a jövő kérdéseire*. Sir Mark Stanhpe admirális, a NATO Transzformációs Parancsnokságának parancsnokhelyettese. Magyar Honvéd, XVII. évf. 46. szám, 2006. november 17.

MAGYAR LÁSZLÓ MK. ŐRNAGY

A SIGINT SZEREPE AZ ASZIMMETRIKUS FENYEGETÉSEK ELLENI KÜZDELEMBEN

Bevezető

A rádióelektronikai felderítés (SIGINT) működésének feltételrendszere a kétpólusú világrendszer felbomlásával, valamint az új típusú fenyegetések megjelenésével jelentősen átalakult. Előadásomban a SIGINT aszimmetrikus fenyegetések elleni küzdelemben betöltött szerepével és lehetőségeivel foglalkozom.

Hazánkban e fontos felderítési nem elmúlt másfél évtizedben történt változásait leginkább a következő tényezők befolyásolták:

- a nemzetközi biztonsági környezet változásai;
- a katonai felderítés feladatrendszerének változása;
- az ország integrációja az európai szervezetekbe;
- a nemzeti haderő átalakulása;
- a kommunikáció robbanásszerű fejlődése;
- az információs társadalom kialakulása.

Amikor arra keressük a választ, hogy a SIGINT miként járulhat hozzá az aszimmetrikus fenyegetések elleni harc sikeréhez, akkor alapvetően arra kell választ adnunk, hogy melyek a felderítési nem működésének sajátos jellemzői, a végrehajtását leginkább befolyásoló tényezők, illetve beszélnünk kell azokról a követelményekről, amelyeket korunk biztonsági kihívásai állítanak a szolgálat elé.

Globalizáció és biztonság

A hidegháborút követően a konfigurált ellenségkép megszűnt, biztonságpolitikai vákuum alakult ki. A rohamosan terjedő globalizációnak azonban nemcsak az előnyei mutatkoztak meg, hanem egyre inkább nyilvánvalóvá váltak hátrányai is, a gazdaság, a társadalom és a biztonság területén egyaránt. Az új kihívások kezelésére a nemzetközi közösség akkor még nem készült fel.

A nemzetbiztonsági kockázatok vonatkozásában, a hagyományos jellegű, tömeghadseregek által vívott háborúk esélyének csökkenésével előtérbe kerültek a nem katonai jellegű, ún. aszimmetrikus fenyegetések, mint például a terrorizmus, a tömegpusztító fegyverek proliferációja, a migráció és a szervezett bűnözés, melyek szorosan összefonódtak egymással.

A katonai hírszerzés/felderítés feladatrendszerében – a fenyegetések és biztonsági kockázatok megváltozott jellegének megfelelően –, prioritást képez a terrorizmussal és a proliferációval kapcsolatos információszerzés.

Nemzetközi, illetve nemzeti szinten a biztonságpolitikai gyakorlatban általánossá vált az ilyen típusú veszélyforrások folyamatos elemzése, valamint valószínűségi és kockázati mutatók alapján történő besorolása (prioritás). Mindezeket figyelembe véve napjainkban a legnagyobb fenyegetést a nemzetközi terrorizmus, ezen belül az iszlám fundamentalista szervezetek jelentik. Magyarországon ezen szervezetek jelenléte nem számottevő, azonban térségünkben, főként a Nyugat-Balkánon az utóbbi években fokozott tevékenységük volt tapasztalható. A fenyegetés földrajzi közelsége miatt a katonai felderítés egyik legfontosabb feladata a terrorista fenyegetés országhatáron kívül tartása.

A 2001. szeptember 11-én, az Egyesült Államok területén végrehajtott terrorakciók ráirányították a figyelmet arra, hogy az aszimmetrikus fenyegetések valamennyi formája ellen összehangoltan kell fellépni. A veszélyforrások globális jellege miatt az ellenük folytatott küzdelem is kizárólag szilárd alapokon nyugvó, kölcsönös érdekeken alapuló, jól koordinált nemzetközi együttműködés keretében lehet eredményes.

Az egykori szocialista országokban a terrorizmusnak és a szervezett bűnözésnek nem voltak hagyományai, ezért a nemzetbiztonsági szolgálatok és rendvédelmi szervek nem rendelkeztek tapasztalatokkal azok kezelésében. Ezt is figyelembe véve kell törekedni az együttműködés kiszélesítésére azokkal az országokkal, amelyek már jelentős tapasztalatokat szereztek az új típusú fenyegetések elhárításában. Mindez akkor is igaz, ha tudjuk, hogy az elmúlt másfél évtizedben – a globalizáció következményeként – a terrorizmus is jelentős átalakuláson ment keresztül.

A SIGINT szerepének növekedése

Az aszimmetrikus fenyegetések vonatkozásában minden eddiginél meghatározóbb a hírszerzés/felderítés megelőző–figyelmeztető („early warning”) funkciója, illetve a csapatok magas szintű felderítő támogatása a műveleti területeken.

A SIGINT az adatforrásaihoz történő hozzáférést tekintve különleges és egyedi képességgel rendelkezik, mely különösen fontos az „early warning” szempontjából. Az információ gyakorlatilag a felhasználókkal egyidejűleg a SIGINT birtokába is kerül, ezért reálidőben képes annak továbbítására a megrendelő részére. Egyúttal a SIGINT irányában követelményként fogalmazódik meg, hogy ezirányú sajátos képességét olyan információk megszerzésére fordítsa, amelyekhez más felderítési nemek egyáltalán nem, vagy csak részben képesek hozzájutni. Meg kell említeni azonban, hogy a rádióelektronikai felderítés sikeressége, hatékonysága mindenekelőtt az adatforrások működésének intenzitásától és bizonyos fizikai fényezőktől függ.

A figyelmeztető/megelőző funkció megfelelő működésén keresztül a SIGINT hatékonyan képes részt venni a műveleti területen tevékenykedő csapatok felderítőtámogatásában. A SIGINT-erők alkalmazásának biztonságosságát jelentős mértékben növeli, hogy passzív eszközökkel szerez információkat, ezért nehezen felderíthető. A megszerzett adatok időszerűségének biztosítása különösen az „időérzékeny” célpontoknál kiemelt fontosságú.

Kommunikáció és informatika

A globalizáció következményeként a két terület robbanásszerű fejlődésen ment keresztül, aminek következtében a SIGINT szerepe jelentősen felértékelődött. Globális hírközlő rendszerek épültek ki, amelyek egymással történő összekapcsolásával lehetővé vált az információk földrajzi és időkorlát nélküli továbbítása. A fentieket figyelembe véve napjainkban már nem feltétlenül szükséges a SIGINT-erőket a célobjektumok körzetébe telepíteni, s ez a lehetőség tovább növeli alkalmazásuk biztonságosságát.

A mai digitális világban a szolgáltatások széles körben elérhetőek, a katonai hírközlés dominanciája megszűnt. Az adatátviteli kapacitás sokszorosára növekedett, és az adatbiztonság is számottevően javult. A kommunikáció változásai következtében elméletileg szinte végtelen a SIGINT részére potenciálisan hozzáférhető adatforrások száma.

Az információforrásokhoz való gyakorlati hozzáférés lehetősége mégis lényegesen korlátozott, mivel az egyre nagyobb méreteket öltő ipari kémkedés miatt fokozottan védettek a kommunikációs technológiákkal kapcsolatos információk.

Nemzetközi vonatkozásban a SIGINT részére a következő időszak egyik legnagyobb technológiai kihívása a számítógép-hálózatok felderítése, elemzése, illetve az adatforgalom lehallgatása, vagyis a C2C-SIGINT. A fenti technológia rendkívül költséges, ezért széles körű elterjedése a közeljövőben nem várható.

Összességében megállapítható, hogy napjainkban a SIGINT elvi lehetőségei az adatforrásokhoz történő hozzáférés vonatkozásában olyan mértékben kiszélesedtek, hogy a rádióelektronikai felderítés elnevezés helyett inkább az elektronikus hírszerzés használata indokolt.

A SIGINT fejlesztése

Magyarországon a katonai felderítés feladatrendszerének átalakulásakor a SIGINT objektív okok miatt nem volt és nem is lehetett felkészült az aszimmetrikus fenyegetésekkel összefüggő feladatok végrehajtására. Az elmúlt években célirányosan megkezdődött a szolgálat racionalizálása, ezen belül az adatszerző erők technikai képességeinek fejlesztése, illetve az adatfeldolgozás átalakítása, amelynek során új munkamódszerek kidolgozására és meghonosítására került sor. A fentiek kapcsán különleges figyelmet kell fordítani az adatforrás-kutatásra, mint funkcióra, valamint az adatszerzésnek a korábbi időszaknál hatékonyabb operatív irányítására.

Az adatforrások kutatása és az informatív adatforrások kiválasztása jelentős kutató–fejlesztő tevékenységet igényel, azonban a digitális technológiák kutatása bonyolult és költséges. A költséghatékonyság növelése érdekében a korszerűsítéseket célirányosan, prioritások mentén kell végrehajtani.

A 2003-ban megkezdett fejlesztési folyamat eredményeként a SIGINT egyre inkább képessé válik az aszimmetrikus fenyegetésekkel kapcsolatos adatok és információk megszerzésére.

A további korszerűsítés középpontjába – a kommunikáció és az informatika fejlődésének távlatait, valamint a SIGINT várható feladatait figyelembe véve –, a távközlési műholdas képességek növelését kell állítani. A technológiai fejlődés a mérnöki és informatikai végzettségű szakemberek, míg a feladatrendszer változása a speciális nyelvtudással és szakismeretekkel rendelkezők számának növelését teszi szükségessé.

A modernizációra vonatkozó elgondolás fontos részét képezi a mobil képességek fejlesztése és kialakítása, a külföldön tevékenykedő magyar alegységek felderítő biztosítása (force protection), illetve a Nemzeti Hírszerző Csoportok (National Intelligence Cell – NIC) támogatása érdekében. Jelenleg a műveleti területen tevékenykedő nemzeti kontingensek nem rendelkeznek SIGINT-képességgel.

A megszerzett adatok mennyiségének növekedése, valamint az automatizáltság jelenlegi és várható foka egyre inkább indokolttá teszi az adatfeldolgozó kapacitás növelését, az informatikai támogatás folyamatos fejlesztését, illetve új munkamódszerek kidolgozását és alkalmazását az adatfeldolgozás hatékonyságának növelése, valamint az adatszerzés operatív irányításának javítása érdekében.

A SIGINT legfontosabb feladatai

Az aszimmetrikus fenyegetések elleni küzdelemben a SIGINT-nek

- a terrorista (szervezett bűnözői) szervezetek felépítésére;
- vezetési struktúrájuk és működési sajátosságaik megállapítására;
- kapcsolatrendszereik feltárására;
- tevékenységük nyomon követésére;
- a támogató hálózatok és személyek felderítésére, illetve felfedésére (humán és anyagi erőforrások, pénzügyi támogatás)

kell a fő figyelmet fordítania.

Az aszimmetrikus fenyegetések elleni küzdelemben a fentieken túl kiemelt hangsúlyt kap az együttműködés kérdése, amely a következő szinteken valósulhat meg:

- az MK KFH szintjén;
- a hazai társszervezetekkel;
- a NATO-val és az EU illetékes szerveivel;
- a külföldi partnerszolgálatokkal.

Az együttműködés szükségességét főleg a képességek és a kapacitások szűkössége indokolja, ugyanakkor a feladatmegosztás lehetővé teszi a rendelkezésre álló erőforrások hatékonyabb felhasználását. A kooperáció kiterjedhet a SIGINT-adatok és -információk cseréjére, a technikai jellegű kérdésekre, az adatok feldolgozása és értékelése során szerzett tapasztalatokra, illetve megvalósulhat technikai támogatás formájában.

Összegzés

A SIGINT szerepe a jövőben – figyelembe véve a kommunikáció várható fejlődési irányait – tovább növekszik az aszimmetrikus fenyegetések, köztük kiemelten a terrorizmus elleni küzdelem területén.

A rádióelektronikai felderítéssel szemben támasztott követelmények teljesítése érdekében a képességeket célirányosan, a kor színvonalán álló eszközök és technológiák alkalmazásával kell kialakítani, amelyben fontos szerepet kell kapnia az adatforrás-kutatásnak.

Növelni, illetve folyamatosan magas szinten kell tartani a SIGINT adatszerző erők operatív irányításának hatékonyságát („target development”), új módszerek meghonosításával javítani kell az adatszelektálás mennyiségi teljesítőképességét és automatizáltságát, az adatfeldolgozás minőségét, valamint a fejlesztésekkel párhuzamosan biztosítani kell az állomány szakirányú alapképzését, továbbképzését és átképzését.

A rendelkezésre álló erők és eszközök mennyiségi korlátai, valamint SIGINT szakmai szempontok figyelembevételével tovább kell erősíteni a hazai, a szövetséges és a nemzetközi együttműködést.

FELHASZNÁLT IRODALOM

- Pászka Tibor mk. ezredes: *Szükség van-e a rádióelektronikai felderítésre?* Felderítő Szemle, III. évf. 2. szám, 2004. június.
- Prof. Dr. Kőszegvári Tibor nyá. vezérőrnagy: *A katonai felderítés helye, szerepe és problémái a terrorizmus elleni küzdelemben*. Felderítő Szemle, IV. évf. 3. szám, 2005. szeptember.
- *Response to Terrorism*. NATO Briefing, March 2005., NATO Public Diplomacy Division, Brussels – Belgium
- http://www.afio.com/sections/wins/2005-08.html
- http://www.cryptome.org/nsa-reorg-net.htm
- http://www.sg.hu/

MURAI LÁSZLÓ MK. ALEZREDES*

SIGINT-ADATFELDOLGOZÁS – MÁSKÉPP

A SIGINT-adatfeldolgozás eszközeinek és módszereinek fejlődése az elmúlt 25 év során

Visszatekintve az elmúlt negyedszázadra, a SIGINT-adatfeldolgozás eszközei és módszerei e történelmi távlatokban viszonylag rövid időszak alatt is hatalmas változáson mentek keresztül.

25 éve még egy adatfeldolgozó tiszt legfőbb „adatbázisa" egy 200 lapos munkafüzet volt, amelybe bejegyezte mindazt, amit a felderítési feladatot képező országok haderejével, valamint a nyomon követett rádióforgalmi rendszerek működésével kapcsolatban fontosnak tartott.

Ha pedig a rövidhullámú rádió-iránymérési (RIM) adatokra volt kíváncsi, akkor lesétált a földszintre az iránymérő-értékelőkhöz, akik a falra vagy asztalra rögzített térképeken, gumiszalagok segítségével úgymond „kihúzták" az egyes rádió-iránymérő állomások által mért irányszögeket, és behatárolták a kérdéses rádióállomás települési körzetét.

Az utóbbi évtizedek során a SIGINT-adatfeldolgozás szorosan kapcsolódott a számítástechnikai eszközök, a hardverek és szoftverek fejlődéséhez.

Az első nagy lépést ezen a területen a rádió-iránymérési adatok számítógépes feldolgozása jelentette, mivel lehetővé vált hosszabb időszakokról készített RIM-összefoglalók viszonylag gyors összeállítása, nagy méretű, plotterrel nyomtatott, térképes, vizuális megjelenítése.

Az első, központi számítógépre alapozott zárt feldolgozói hálózat kialakítása újabb mérföldkövet jelentett, amely már nem csak az előértékelő és értékelő, de a jelentő tevékenységet is támogatta.

Az adatfeldolgozó alosztályokon korábban mechanikus írógépekkel készültek a különféle jelentések, amelyeket az ügyeletes szerkesztő öntött végleges formába. Ezt követően a jelentés egyrészt a hírközpontba került, ahol lyukszalagra történő átgépelés után továbbították az elöljáró részére, másrészt – mivel az akkori lapnyomtató csak nagybetűkkel volt képes nyomtatni – egy titkárnő az előírt „törzskultúra" miatt elektromos írógéppel vetette papírra az Irattár, illetve más címzettek számára.

* A szerzőt időközben előléptették ezredessé.

Hasonló módszerrel készültek a tervezési, illetve az adatszerzés és adatfeldolgozás irányításával kapcsolatos egyéb okmányok is.

A 1990-es évek elején az asztali 286-os, 386-os és 486-os számítógépek rendszeresítése újabb lökést adott az adatfeldolgozás támogatásának.

A feldolgozó állomány a számítástechnikában jártasabb szakemberek segítségével, de általában autodidakta módon sajátította el a ma már mindennaposnak tűnő szövegszerkesztő-, táblázatkezelő-, rajzolóprogramok kezelését, az adatbázisok feltöltését és a lekérdezéshez szükséges „varázsigéket”.

A titkárnők nagy örömére a PE2-es szövegszerkesztő program volt az első, amely lehetővé tette, hogy a begépelt dokumentumot megszerkesztett formában közvetlenül, a számítógéppel összekapcsolt Panasonic elektronikus írógéppel (amit stílusosan Jolánkának becéztünk) lehessen kiíratni.

A tárolókapacitások folyamatos bővülésével, illetve az egyre fejlődő nyilvántartó-szoftverek alkalmazásával a papír-alapú adatrögzítést fokozatosan a digitális adatrögzítés váltotta fel, következésképpen a SIGINT-adatfeldolgozás módszereit is a megváltozott körülményekhez kellett igazítani.

A jelenleg alkalmazott eszközök és módszerek, lépések az automatikus adatfeldolgozás (ADP) irányába

Már évekkel Magyarország NATO-taggá válása előtt rendszeresítésre került egy olyan, a rádióelektronikai felderítési adatok rögzítésére, archiválására, előfeldolgozására alkalmas program, amely jelenleg is alap-adatbázist biztosít az együttműködési feladatokból adódó napi adatcsere végrehajtásához.

Az adatfeldolgozást legsikeresebben támogató szoftvereket természetesen saját szakembereink készítették, akik a felhasználókkal napi kapcsolatot tartva, állandóan tökéletesítették a programokat. Tevékenységük során igyekeztek adaptálni mindazokat a külföldi tapasztalatokat, amelyekhez kétoldalú nemzetközi kapcsolataink útján jutottunk.

A jelenleg rendszerben lévő, saját fejlesztésű **adatbeviteli és nyilvántartó programok** reálidőben biztosítják az adatfeldolgozók számára a rögzített adatokhoz való hozzáférést, egyben alkalmasak különféle statisztikai elemzésekre is.

Igazgatóságunkon mintegy két évvel ezelőtt telepítésre került egy, a NATO által kifejlesztett és alkalmazott szoftvercsomag is, amely széles körű lehetőséget biztosít a kapcsolati rendszerek, interperszonális kapcsolatok nyilvántartására is. Véleményem szerint ez a program tekinthető az első lépcsőfoknak az ADP[1] irányába.

A programcsomag előnye, hogy a Microsoft által kifejlesztett, kereskedelmi forgalomban is kapható szoftverek integrált egysége, amely kiválóan alkalmas a hadrendre, a szervezetekre és személyekre vonatkozó adatok gyűjtésére, értékelésére, az adatok térképi megjelenítésére, egyéb háttér-információk rendszerezésére.

Lehetséges válaszok a 21. század kihívásaira

A SIGINT-adatfeldolgozás szoftveres támogatásának hatékonyabb megoldása NATO szinten is kiemelt feladat. Ezzel kapcsolatban 2005 októberében Hágában tartottak egyeztető fórumot, amelyen a Rádióelektronikai Felderítő Igazgatóság is képviseltette magát.

A tanácskozás célja volt, hogy a szakértők áttekintsék a felderítőadatokhoz hozzárendelt metadata-k kategorizálásának, osztályozásának rendszerét, megosszák tapasztalataikat, illetve javaslatokat dolgozzanak ki a változtatásokra. Igazgatóságunk részt vett a szoftver tesztelésében is, amelynek célja a rendszer alkalmazhatóságának ellenőrzése, valamint annak megállapítása volt, hogy milyen új funkciókra van szükség a későbbi, „éles" használathoz. Tapasztalatainkat – a kísérleti üzemeltetést követően – megküldtük az illetékesek részére.

Megállapítottuk, hogy az információk mennyiségének tömeges növekedésével egyre nagyobb a rés a felhasznált és a fel nem dolgozott, felhasználatlan információk mennyisége között.

Az elsődleges cél a beérkező információk „automatikus" feldolgozása lenne, amit azonban nehezít azok strukturálatlan felépítése.

Az osztályozás megkönnyítésére hivatott szoftver kifejlesztése már 2003-ban megkezdődött. Ez a program a jövőben képes lehet arra, hogy „végignézi" a dokumentumot, szövegfájlt, majd indexeli azt a meghatározott kulcsszavak alapján. Ezután létrehoz egy „könyvtárkártyát" (library card), amely funkcióját tekintve nagyban hasonlít a metadata-hoz, csak annál részletesebb.

[1] ADP – Automatic Data Processing – automatizált adatfeldolgozás.

Ahhoz azonban, hogy a rendszer hatékonyan működjön, minden felhasználónak meg kell határozni azokat a témaköröket, kulcsszavakat, amelyek az egyes feldolgozási szinteken fontosak lehetnek.

A kategóriák létrehozásánál és a rendszer felállításánál az az alapelv, hogy először országok szerint csoportosítunk, majd azt követően létrehozzuk a minden országra vonatkozó általános jellemzőket, kulcsszavakat. Ezek alapján már egy-egy országra, illetve azok ismérveire rá lehet keresni, majd a speciális kategóriákra kerül sor. Így próbálják létrehozni azt a kulcsszó / kategória halmazt, rendszert, amely „lefedhet" minden országot.

Az a tény azonban, hogy a különböző szintű szervek hírigénye más és más, nagyon megnehezíti egy egységes rendszer létrehozását.

Az országok szerinti csoportosítással az lehet a probléma, hogy egy hír esetén sok esetben nem is az ország a lényeg, hanem maga a cselekvés, a történés.

A konferencia alapján is levonható az a következtetés, hogy **az adatfeldolgozás hatékonysága növelésének jövőbeni kulcsa az információk automatikus kategorizálásában rejlik**.

Igazgatóságunk már évekkel ezelőtt kereste az informatikai piacon azokat a megoldásokat, amelyek alkalmazhatók lennének a SIGINT-adatfeldolgozás, illetve a Hivatal más területein is. Több alkalommal vettünk részt önállóan, illetve más igazgatóságokkal közösen a témakörrel kapcsolatos szoftverbemutatókon, szakmai napokon.

Megállapítottuk, hogy léteznek – sajnos meglehetősen magas árfekvéssel –, olyan szoftverek, melyek alkalmasak lennének nagy mennyiségű, különböző formátumú, illetve típusú szöveges információ automatikus feldolgozására.

Kiegészítő programokkal lehetőség nyílhat (például) a magyar nyelven megadott keresési szempontok alapján, más nyelven megjelent dokumentumok kiválasztására is.

A program továbbfejlesztett változatai képessé válhatnak hanginformációk szöveggé történő átalakítása útján a fenti funkciók ellátására.

Igazgatóságunk rendelkezik néhány tehetséges, programozásban jártas szakemberrel, azonban az nem lehet reális elvárás, hogy olyan bonyolultságú szoftvereket fejlesszenek ki, amelyek még a világ vezető szoftverkutató cégeinek is nem kis fejtörést okoznak.

Mit célszerű tehát „költségtakarékosan" tennünk az ADP mielőbbi megvalósítása érdekében?

Mivel az intelligens szoftverek beszerzése a piacról a pénzügyi források hiánya miatt a következő időszakban sem látszik megvalósíthatónak – **saját programok továbbfejlesztése, valamint a nemzetközi tapasztalatok felhasználása mellett** –, a jövőben **fokozott figyelemmel kell kísérnünk a NATO-fejlesztések alakulását**, aktívan részt kell venni a további kísérletekben, egyeztető konferenciákon, s (a lehető legjobban) **fel kell készülni a kialakításra kerülő szoftverrendszerek integrálására, mielőbbi adaptálására**.

DR. BOTZ LÁSZLÓ NYÁ. ALTÁBORNAGY

BÁRMI TÖRTÉNIK A VILÁGBAN, A SIGINT NEM VESZÍT JELENTŐSÉGÉBŐL

Tisztelt Konferencia,
Hölgyeim és Uraim!

Engedjék meg, hogy először köszönetet mondjak a szervezőknek a meghívásért. Nagy megtiszteltetés számomra – aki több mint negyven éve, 1963-ban találkoztam először a szakmával –, hogy egy ilyen magas szintű konferencián hallhattam a szakma elismert képviselőinek gondolatait, sikereit és gondjait.

Szeretném kihangsúlyozni, hogy bármi is történik a világban, a SIGINT soha nem veszít a jelentőségéből! Bár az elmúlt években egyre többször hangzott el a kicsit hamisnak tűnő értékelés, mi szerint az elkövetkező tíz évben nem fenyegeti országunkat katonai jellegű veszély, ez nem jelentheti a SIGINT leértékelését. Hazánk választott döntéshozóinak mindig szükségük volt és van az ország szűkebb és tágabb környezetére vonatkozó információkra, amelyek jelentős része a SIGINT tevékenységéből származhat.

A 21. század elejére jelentősen átalakultak a fenyegetések, az új kihívások megjelenésével valóban háttérbe kerültek a konkrét katonai megoldások, de ez nem jelenti azt, hogy a katonai felderítés, s annak szerves része – a SIGINT – elveszítette volna fontosságát. **Fontosnak tartom a helyes arányok kialakítását, azaz az új kihívások, veszélyek időbeni felderítését biztosító képességek fejlesztése mellett továbbra is szükséges a katonai vezetés igényeinek kiszolgálása is.**

A Magyar Köztársaság – mint a NATO és az Európai Unió tagja –, elkötelezte magát az integrációkban tapasztalható paradigmaváltás mellett. A két szervezet már nem a helyét keresi a nemzetközi biztonságpolitikai környezetben, hanem határozott céllal fordult a béketámogatás területéhez, amely környezetben a katonai feladatok mellett egyre nagyobb hangsúlyt kapnak az ún. „civil" megoldások: a béketeremtés és békefenntartás katonai feladatai mellett a békeépítés, a humanitárius műveletek támogatása, a polgári lakosság segítése. Mindezen feladatokban – legyen az katonai, vagy civil erőkkel végrehajtott művelet –, szükséges, hogy a SIGINT legyen képes alkalmazkodni, és ezen körülmények között is biztosítania kell a műveletek sikeres megoldásához elengedhetetlen információkat.

A jelzett műveletek igényei már eddig is rámutattak arra, hogy vissza kell állítani a „műveleti SIGINT" – korábbi terminológia szerint hadműveleti, illetve harcászati SIGINT – képességeket is. Sőt ebben a kérdésben fontos az is, hogy a műveleti SIGINT képes legyen az alkalmazási terület sajátosságainak megfelelő tevékenységre mind nyelvi, mind technikai vonatkozásokban.

Példaként emlékeztetni szeretném a hallgatóság idősebb tagjait 1968-ra, amikor a RÁF-nak – a vezetés igénye szerint – információkat kellett biztosítani a jugoszláv fegyveres erők tevékenységéről, s bizony nem volt egyszerű előtalálni azokat, a szolgálatból időközben távozott munkatársakat, akik még „emlékeztek" a régi feladatokra. Tehát arra irányítom rá az érintettek figyelmét, hogy a kapott és várható feladatoknak megfelelően fejlesszék képességüket a műveleti szinteken is.

A mai konferencia örömmel töltött el azért is, mert **bemutatta annak a helyes törekvésnek az eredményességét, hogy nagyobb hangsúlyt kell helyezni az együttműködésre mind országon belül, mind a nemzetközi környezetben.** A hazai társszervek konferencián részt vett és felszólalt vezető munkatársai jelenlétükkel, és a szinte kézzel fogható „partneri szerepkörben" jelentős pozitív elmozdulást jelentenek a múlthoz képest. Ugyancsak dicséretes az ország tudományos műhelyeivel, az egyetemekkel, a kutatóintézetekkel való szoros kapcsolat, ami ugyancsak plasztikusan jelent meg a mai konferencián.

Nem utolsósorban szólnom kell a szolgálat nemzetközi kapcsolatairól, ami egyrészt képességünk, tudásunk elismerését, másrészt a partneri viszonyban játszott, esetenként meghatározó, de semmiképpen sem alárendelt szerepüket tükrözik. Tekintettel a térségünk bizonytalan régióiban, nemzetközi partnereinket is fokozottan érdeklő kihívásokra, talán nem túlzás kijelenteni, hogy ezirányú tevékenységünket külföldi partnereink jobban értékelik, mint országunk vezetése. Ez tükröződik a NATO szakterületi vezetőinek reagálásaiban is, amire büszkék lehetnek a SIGINT vezetői és munkatársai.

Befejezésül engedjék meg, hogy kimondjam: büszke vagyok, hogy négy évtizedes katonai felderítő/hírszerző szolgálatomat annak idején a rádiófelderítés tagjaként kezdhettem. Gratulálok a SIGINT mai vezetőinek és munkatársaiknak, mindannyiuknak további eredményes munkát kívánok!

SVIGRUHA GYULA MK. ALEZREDES*

AZ 1. SZEKCIÓ MUNKÁJÁRÓL

A hírközlés felgyorsuló fejlődése sorra hozza az újdonságokat, amelyeknek egy része beépül a hírközlő hálózatokba és így a rádiófelderítés technikai fejlesztésének célpont rendszerébe is. Az általános trendek ismerete segít abban, hogy a kommunikáció fejlődését követhessük. A megszerzett elméleti tudás működő gyakorlati eredményekre váltása a mérnöki fejlesztő munka látványos része. Fürjes János mk. őrnagy **Digitális jelfeldolgozás alkalmazása** című előadásában speciális távközlési berendezések lehallgatásának lehetőségét a digitális jelfeldolgozó processzorok gyakorlati felhasználásával mutatta be. Egyes távközlési berendezések ugyan alkalmassá tehetők korlátozott szintű monitorozási feladatokra, de azok az átalakítással sem teljesítik a SIGINT felhasználók különleges igényeit. Az átalakításokba fektetett munka nem minden esetben térül meg, sokszor egyszerűbb megalkotni egy új, saját rendszert, ami minden felhasználói igényt kielégít, mint az átalakítással bajlódni.

Az Internet elterjedésével a kommunikáció biztonsága is lényeges kihívása a felfedő és lehallgató rendszereknek. Visky Károly tanácsos **A VPN-hálózatok lehallgatásának lehetőségei** című előadása – mint jövőbe mutató kutatási téma –, az adatszerzés szemszögéből közelíti meg a virtuális magánhálózatok (VPN) témakörét. Foglalkozik a kialakítás lehetőségeivel, valamint az alkalmazott protokollokkal, röviden ismerteti az Internet működését, a monitorozás bonyolultságát. Az adatforgalom egy lehetséges analizálási módjának bemutatása mellett egy adatgyűjtő program működését is láthattuk.

Sokat tapasztalt régi nyugdíjas munkatársainktól megtanulhattuk azt az alap bölcsességet, mely szerint a rádiófelderítés az antennánál kezdődik és a jelentés megírásával végződik. A leggyengébb láncszem elve alapján a struktúra minden egyes elemének lényeges szerepe van. Az állandóan fejlődő rádiókommunikációs rendszerek megkívánják, hogy ellenőrzésük és felügyeletük során felhasznált infrastruktúra is lépést tudjon tartani a célrendszerek fejlődési ütemével. Ez megköveteli a legkorszerűbb módszerek, készülék valamint rendszerépítési elvek felhasználását. Dr. Eged Bertalan **Szoftverrádiók** című előadásában rövid összefoglalót kaphatunk a technológia fejlesztések eredményeiről, a fejlesztések motivációiról, valamint azok felhasználásának előnyeiről. Az előadásban láthatunk példát megvalósított radar, illetve kommunikációs adás- és vételtechnikai berendezésekre, valamint képet kapunk a jelenleg folyó készülék és rendszertechnikai fejlesztések irányáról, várható eredményeiről.

* A szerzőt időközben előléptették ezredessé.

A távközlési szolgáltatók illetve szolgáltatások globalizációjának számos jelét tapasztalhatjuk. Maguk a technológiák is a globalizálódást segítik, erre jó példa a kontinenseket összekapcsoló optikai kábelek megjelenése vagy a műholdas rendszerek elterjedése. A műholdas műsorszórás területén a felhasználók növekvő igényei miatt a kapacitásnövelés érdekében, a sávkihasználást hatékonyabban kezelő digitális adatátviteli rendszer jelent meg, a műholdas digitális műsorszórás DVB-S szabványa (Digital Video Broadcasting via Satellite). Makkai Zsolt mk. törzsőrmester **Integrált szolgáltatású digitális műsorszórás** című előadásában bemutatta a DVB-S, valamint a továbbfejlesztett DVB-RCS integrált adatátviteli rendszer felépítését, a vételéhez szükséges eszközöket, az IP protokoll átviteli mechanizmusát, valamint az elérhető szolgáltatásokat. (Szerkesztett formában megjelent a Felderítő Szemle 2006/2. számában. A szerk.)

A rendelkezésünkre álló idő szűke és a téma szerteágazósága miatt csak ízelítőt adhattunk a SIGINT technikai kihívásaiból. Remélem a különféle területekről válogatott témák további közös gondolkodásra adnak lehetőséget.

A Rádióelektronikai Felderítő Igazgatóság emblémája
(tervezet, csak belső használatra)

PADOS LÁSZLÓ MK. EZREDES

A 2. SZEKCIÓ MUNKÁJÁRÓL

Tisztelt Elnökség,
Tisztelt Konferencia,
Hölgyeim és Uraim!

A konferencia 2. szekciójának munkáját az aktivitás és újszerű, innovatív gondolatok felvetése jellemezte.

A szakmai műhely a **SIGINT-műveletek a 21. században** témakört vizsgálta meg, természetesen a teljesség igénye nélkül. Elsősorban azokra a kérdésekre igyekeztünk koncentrálni, amelyek a SIGINT-tevékenységek eredményessége szempontjából meghatározóak, és újszerű megközelítést kell kapjanak a jövőben.

Az elhangzott előadások, hozzászólások a szakmai munka egymástól látszólag távol eső, ugyanakkor mégis kölcsönhatású kérdéseit ölelték fel. A vizsgált témakörök önmagukban is szerteágazók, és talán éppen ez a sokrétűség, valamint a szűkös időkeret volt az akadálya annak, hogy a mondanivaló egységes gondolatsorrá álljon össze. Sikerült ugyanakkor rámutatni jónéhány kulcsfontosságú területre, ahol változtatás szükséges, és számos értékes előremutató javaslat is megfogalmazódott azok tartalmára vonatkozóan.

A globalizáció és a felgyorsult tudományos–technikai fejlődés, az információrobbanás, az információs társadalmak együttes hatástényezői, a fogyasztói információigény változása diktálta új elvárások, az új biztonsági fenyegetésekre és kockázatokra adandó adekvát válaszok kényszerítő ereje a rádióelektronikai felderítés felé is a változás, az alkalmazkodás, a folyamatos fejlődés igényét közvetíti.

Már a jelen, de még inkább a jövő szakmai eredményessége a mindezekre való nyitottságnak, a szükséges képességek rendelkezésre állásának és célirányosan rugalmas alkalmazásának, valamint nem utolsósorban a szakmai állomány felkészültségének, elhivatottságának, szellemi megújuló-képességének a függvénye is.

Emellett egyre fokozódó jelentőséggel bír az együttműködésre való képesség a nemzeti intézményrendszer, a társszolgálatok, a szövetségi és a nemzetközi kapcsolatok szintjén. **Mindez a potenciál a mai rádióelektronikai felderítésben és a szakmát művelőkben megvan**.

Azt gondolom, hogy a szekció munkájának, de talán az egész konferenciának is ez a legfontosabb üzenete.

Köszönöm megtisztelő figyelmüket!

PÁSZKA TIBOR MK. EZREDES

ZÁRSZÓ

Tisztelt Tudományos Konferencia!
Tábornok és Tiszt Urak!
Hölgyeim és Uraim!

A katonai rádióelektronikai felderítés modern kori történetében első alkalommal került sor olyan tudományos rendezvényre, amely a résztvevők körét tekintve túlmutatott a Hivatal keretein.

A tudományos konferencia megszervezésével az a szándék vezetett bennünket, hogy bemutassuk a rádióelektronikai felderítés megváltozott helyét, szerepét, lehetőségeit és megújult képességeit a felderítés/hírszerzés nemzeti, valamint integrált szövetségi rendszerében. Vizsgáltuk a hírközlés, a távközlés, az információtechnológia, az informatika dinamikus változásban, fejlődődésben lévő, egyre inkább globalizálódó világát, amely a rádióelektronikai felderítés működési környezetét adja. Érzékeltettük azokat az új követelményeket, amelyek egyrészt a fentiekből következnek, másrészt az információ igény változásával összhangban a felhasználói oldalról közvetítődnek a szakma felé.

Úgy gondolom, hogy ezen túlmenően, részletesen összegezni az elhangzottakat nem szükséges, mivel azt megtették a szekcióvezetők.

Lényegesnek tartom ugyanakkor azt rögzíteni, hogy a katonai rádióelektronikai felderítés ma már olyan felderítési nem, amely a katonai felhasználók mellett az állami felső vezetés, a NATO és az EU információigényeinek teljesítéséhez is hozzájárul.

A globalizálódó világ és az információs társadalom kihívásaival lépést tartani képes rádióelektronikai felderítés össznemzeti jelentőségű ügy. Ez a megállapítás a konferencia legfontosabb üzenete.

Tisztelt Kollégák!

Zárszóként köszönetemet fejezem ki mindazoknak, akik részt vállaltak a tudományos konferencia előkészítésében és zökkenőmentes megrendezésében. A tanácskozás szerkesztett anyagát a Felderítő Szemle különszámaként adjuk ki, azzal a szándékkal, hogy a szakmai munkánk során az itt elhangzott értékes gondolatokat közkinccsé tegyük.

Biztos vagyok abban, hogy a mai alkotó véleménycsere és a közös gondolkodás érdemi módon járul hozzá a feladatok eredményes végrehajtásához.

A további közös tevékenységhez sok sikert kívánok!

CONTENTS

Tisztelt Olvasó!

A FELDERÍTŐ SZEMLE a honvédelemmel, a biztonságpolitikával és a nemzetbiztonsággal összefüggő kérdések felvetésének és megválaszolásának fóruma. A kiadványban közzétett tanulmányokban megjelenő vélemények nem feltétlenül azonosak a Magyar Köztársaság Katonai Felderítő Hivatal és a Tudományos Tanács hivatalos álláspontjával.

Elérhetőségeink

Postacím: MK Katonai Felderítő Hivatal Tudományos Tanácsa
1111 Budapest, Bartók Béla u. 24-26.

MK Katonai Felderítő Hivatal Tudományos Tanácsa
1502 Budapest, Pf. 117

Telefon: Dr. Tömösváry Zsigmond nyá. dandártábornok, főtanácsos,
a Tudományos Tanács elnöke
06(1) 386-9344/1300, HM 02/61-300
e-mail: zsiga07@t-online.hu

Dr. Sallai Imre nyá. ezredes, tanácsos,
a Tudományos Tanács titkára
06(1) 386-9344/1332, HM 02/61-332

Tóth András mk. ezredes,
a Szerkesztőbizottság elnöke
06(1) 386-9344/1500, HM 02/61-500

Vass Jenő nyá. ezredes,
felelős szerkesztő
06(1) 386-9344/1306, HM 02/61-306
telefax: 06(1)372-1842, HM 02/61-842

Gerencsérné Tóth Krisztina főtörzsőrmester,
általános ügyintéző
06(1) 386-9344/5401, HM 02/65-401
e-mail: mkkfh_szemle@freemail.hu

Várjuk jelentkezését és írásait!

A Szerkesztőbizottság