

**NEMZETI KÖZSZOLGÁLATI EGYETEM  
KATONAI MŰSZAKI DOKTORI ISKOLA**

**Horváth József Sándor**

**A MAGYAR HONVÉDSÉG  
ELEKTRONIKAI HADVISELÉSI  
KÉPESSÉGÉNEK FEJLESZTÉSE  
SZOFTVERRÁDIÓK  
ALKALMAZÁSÁVAL**

**Doktori (PhD) értekezés**

**Témavezető: Prof. Dr. Ványa László okl. mk. ezredes, PhD**

.....

**Társ-témavezető: Dr. habil. Négyesi Imre alezredes, PhD**

.....

**BUDAPEST, 2018.**

## TARTALOMJEGYZÉK

|                                                                                                                               |    |
|-------------------------------------------------------------------------------------------------------------------------------|----|
| BEVEZETÉS .....                                                                                                               | 4  |
| A tudományos probléma megfogalmazása .....                                                                                    | 6  |
| Kutatási hipotézisek .....                                                                                                    | 8  |
| Kutatási célkitűzések.....                                                                                                    | 9  |
| Kutatási módszerek .....                                                                                                      | 10 |
| Releváns szakirodalom áttekintése.....                                                                                        | 11 |
| A kidolgozás során érvényesült korlátozások .....                                                                             | 12 |
| 1. A BIZTONSÁGPOLITIKAI HELYZET VÁLTOZÁSÁNAK ÉS A TECHNIKAI<br>FEJLŐDÉS HATÁSA AZ ELEKTRONIKAI HADVISELÉS ALKALMAZÁSÁRA ..... | 13 |
| 1.1. Biztonságpolitikai változások .....                                                                                      | 13 |
| 1.2. Elektronikai hadviselés és a rádióelektronikai felderítés napjaink konfliktusaiban .....                                 | 17 |
| 1.3. Az elektronikai hadviselés tervezési folyamata a művelettervezési módszerek<br>változásainak tükrében .....              | 23 |
| 1.4. Elektronikai hadviselési vonatkozású fejlesztések megvalósulása .....                                                    | 30 |
| 1.4.1. Elektronikai hadviselési vonatkozású fejlesztések az egyes haderőknél .....                                            | 30 |
| 1.4.2. Elektronikai hadviselés és a rádióelektronikai felderítés a Magyar Honvédségben .....                                  | 37 |
| Összegzés, részkövetkeztetések .....                                                                                          | 52 |
| 2. A SZOFTVERRÁDIÓ TECHNOLÓGIA ALKALMAZÁSA A KÜLÖNBÖZŐ<br>TECHNIKAI RENDSZEREKBEN .....                                       | 55 |
| 2.1. Frekvenciagazdálkodás .....                                                                                              | 55 |
| 2.2. A szoftverrádió technológia felhasználása .....                                                                          | 59 |
| 2.2.1. A szoftverrádió technológia alapjai.....                                                                               | 59 |
| 2.2.2. Szoftverrádió fejlesztések az egyes nemzeteknél.....                                                                   | 66 |
| 2.2.3. Harcászati rádiók.....                                                                                                 | 71 |
| 2.2.4. Globális helymeghatározó rendszerek .....                                                                              | 74 |
| 2.2.5. Vezeték nélküli kommunikációs és adatátviteli rendszerek.....                                                          | 77 |
| 2.2.6. Radarok .....                                                                                                          | 82 |
| 2.2.7. Az Integrált elektronikai felderítő és zavaró rendszer (INTERJAM) projekt részletes<br>bemutatása.....                 | 83 |
| 2.2.8. Az SDR koncepció által nyújtott előnyök az MH-ban történő alkalmazásuk bevezetése<br>esetén.....                       | 87 |
| Összegzés, részkövetkeztetések .....                                                                                          | 93 |

|                                                                                                                                                                           |     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| 3. A SZOFTVERRÁDIÓ TECHNOLÓGIÁN ALAPULÓ ELEKTRONIKAI HADVISELÉS<br>ESZKÖZRENDSZER ALKALMAZÁSA AZ MH RENDSZERÉBEN.....                                                     | 95  |
| 3.1. A szoftverrádió technológia alapú EHV eszközzel szemben támasztott követelmények .....                                                                               | 95  |
| 3.2. Az elektronikai hadviselési rendszer beszerzésének, hazai fejlesztésének, gyártásának<br>főbb kérdései .....                                                         | 109 |
| 3.3. A szoftverrádió alapú elektronikai hadviselési eszköz és rendszer elleni támadás és a<br>védelem módszerei, kiemelten az informatikai támadások vonatkozásában ..... | 117 |
| 3.3.1. A hordozójárművek/objektumok felderíthetősége .....                                                                                                                | 118 |
| 3.3.2. Az elektromágneses kisugárzás alapján történő felderítés .....                                                                                                     | 119 |
| 3.3.3. Informatikai támadás és védelem .....                                                                                                                              | 120 |
| 3.3.4. Az SDR koncepció alkalmazása következtében fellépő új támadási módszerek és az<br>ellenük kialakítandó védelem.....                                                | 123 |
| 3.4. A szoftverrádió technológia alkalmazása esetében javasolt szervezeti változások .....                                                                                | 126 |
| Összegzés, részkövetkeztetések .....                                                                                                                                      | 130 |
| Összegzett következtetések .....                                                                                                                                          | 133 |
| Új tudományos eredmények.....                                                                                                                                             | 136 |
| Ajánlások.....                                                                                                                                                            | 137 |
| Témakörből készült publikációim.....                                                                                                                                      | 138 |
| Köszönetnyilvánítás .....                                                                                                                                                 | 141 |
| Hivatkozott irodalom.....                                                                                                                                                 | 142 |
| Rövidítések jegyzéke.....                                                                                                                                                 | 157 |
| Ábrák jegyzéke.....                                                                                                                                                       | 163 |
| Képek jegyzéke .....                                                                                                                                                      | 164 |
| Táblázatok jegyzéke.....                                                                                                                                                  | 165 |

## BEVEZETÉS

Napjaink gyorsan változó világában számos új biztonsági kihívással kell szembenéznünk. Ez nemcsak a különböző földrészeken zajló konfliktusokat jelenti – amelyek megoldásában a Magyar Honvédség katonái is jelentős szerepet vállalnak – de figyelembe kell vennünk a globalizáció által generált problémákat, az egyre növekvő számú terrortámadásokat is, melyek az európai emberek számára is testközelbe hozták az erőszakot. A hadviselés változása, **az aszimmetrikus<sup>2</sup> és hibrid hadviselés megjelenése alapjaiban változtatta meg a konvencionális hadviselésre kialakított hadseregekkel szemben támasztott követelményeket.** Mindenképpen fontos az, hogy az egyes országoknak – saját szuverenitásuk, gazdaság érdekeik, valamint állampolgárainak védelme érdekében – nemzeti haderőre van szükségük, amelyet folyamatosan fejleszteni szükséges.

Ez a kötelezettség a különböző gazdasági helyzetben lévő államokra eltérő mértékű terhet ró. **Az európai államok esetében a terroristatámadásokat követően számos alkalommal vetik be a nemzeti haderőt a saját országuk területén a belső rend helyreállítása és a lakosság megnyugtatósa érdekében. Az így megjelent új feladatok újabb és újabb elvárásokat jelentenek, melyekkel a haderőknek meg kell birkóznuk.** Nem elhanyagolható tény az sem, hogy az aszimmetrikus és hibrid hadviselés, valamint a terrortámadások esetében az események időbelisége nehezen behatárolható, a legtöbb esetben hosszú ideig tartó, többször fellángoló cselekményekre kell felkészülnünk.

A NATO tagállamainak esetében a haderőre fordítandó összeg a GDP<sup>3</sup> 2%-a, azonban ezt az európai tagállamok közül 2016-ban csak Görögország és Észtország teljesítette. [3] Bár itt mindenképpen meg kell jegyezni, hogy az egyes tagállamok között az adott százalékos érték összességében jelentős különbséget jelenthet, azonban az is fontos jelzés, hogy ez a kérdés 2017-ben az USA és többi tagállam között jelentős feszültséget okozott. A szövetség katonai költségvetésének csaknem háromnegyedét az Egyesült Államok biztosítja, 2016-ban ez 72 százalék volt. [4] Magyarország a kormányzati bejelentések szerint 2026-ra tervezi elérni a 2%-os költségvetést. [5]

---

<sup>1</sup> Sir Winston Churchill az elektronikai hadviselésről a II. világháborúban. [1]

<sup>2</sup> Aszimmetrikus hadviselés esetében nem hagyományos fegyveres erők közötti, hanem legtöbb esetben hagyományos fegyveres erők és irreguláris, kevésbé kiképzett és felszerelt erők közötti hadviselésről beszélünk. [2]

<sup>3</sup> Gross Domestic Product, bruttó hazai termék

Napjainkban **a katonai tevékenység minden szintjét és formáját áthatja az elektronikai és információtechnológiai eszközök és rendszerek alkalmazása.** Mindenképpen meg kell említeni, hogy a katonai fejlesztéseket nagymértékben befolyásolják a polgári életben kifejlesztésre kerülő egyre újabb és újabb technikai újítások, melyek rövid idő alatt beintegrálódnak mindennapi életünkbe. Korábban az volt a tendencia, hogy a különböző katonai fejlesztések rövidebb-hosszabb idejű alkalmazásukat követően kerültek át a polgári életbe, azonban napjainkra ez tendencia megfordult, a jelentősen felgyorsult polgári fejlesztéseket próbálja alkalmazásba venni a haderő. **Ez a folyamatos fejlődés jelentősen befolyásolja az egyes szakterületek fejlesztését, fejlődését, kiváltképpen a már említett elektronikai eszközök és az információtechnológia alkalmazásán alapuló szakterületeket.**

Az információtechnológia és az elektronikai eszközök alkalmazása érinti a katonai tevékenység teljes spektrumát, beleértve a lövészkatona bevetését (pl. barát-ellenség felismerő rendszerek, a katona helyzetét és állapotát figyelő-ellenőrző elektronikai rendszerek, kommunikációs eszközök, stb.) és a legbonyolultabb műholdas felderítő vagy infokommunikációs eszközök alkalmazását egyaránt. Ennek természetesen számos előnye, de hátránya is van. Előnyök között tarthatjuk számon a rendkívül gyors információáramlást, az aktuális helyzetkép folyamatos biztosítottóságát, a korai előrejelző rendszerek gyors és megbízható működését, de akár az időbeni cselekvés elrettentő hatását is. Ugyanakkor az elektronikai és információtechnológiai alkalmazások a már korábban ismerteken felül további sebezhetőséget hoztak be a rendszerbe, legyen az informatikai támadás, vagy akár csak egy egyszerű technikai meghibásodásból eredő pontatlan helyzetismeret.

Ezzel kapcsolatban egy példán keresztül bemutatom, hogy mennyire komplex, összetett rendszerekkel foglalkozunk, mennyire nehéz kiküszöbölni az egyes hibaforrásokat, és egy viszonylag kisméretű, helyinek gondolt probléma is okozhat jelentős, akár országokon átnyúló problémákat. A 2014-ben tartott NATO Elektronikai Hadviselési Integrációs Program (a továbbiakban: NEWFIP<sup>4</sup>) Ramstein Guard gyakorlat alatt az a vád érte a Magyar Honvédséget, hogy a gyakorlat során üzemeltett eszközök által generált elektronikai zavarás problémát okozott az osztrák, cseh, szlovák és német légiirányításban, a levegőben lévő gépek nem voltak képesek radarjaik üzemszerű használatára, pozíciójukat rádióan egyeztetették a légirányítással. [6] A többnemzeti elektronikai hadviselési gyakorlat során a Magyar

---

<sup>4</sup> NATO Electronic Warfare Integration Programme, NATO Elektronikai Hadviselési Integrációs Program

Honvédség légierének NATINAMDS<sup>5</sup> feladatba bevont erői és eszközei számára az elektronikai zavarást alapvetően repülőgépekre szerelt zavaró konténerekkel, POD-okkal biztosítják, melyek a kiképzési céloknak megfelelően kerülnek felprogramozásra. A zavarókonténereket, valamint a földi – gépjárműbe épített zavarókomplexumokat a NATO-val egyetértési szerződés<sup>6</sup> alapján együttműködő partnere, az Összhaderőnemi Elektronikai Hadviselés Törzs<sup>7</sup> biztosítja. A repülőgépre szerelhető konténerekkel a 2014. évi gyakorlatunk során a szintén NATO szerződött partner COBHAM Aviation repült, melynek DA-20 Learjet repülőgépei elektronikai hadviselési gyakorlatokra kerültek átalakításra és beépített kommunikációs zavarási képességgel rendelkeznek. Az elektronikai zavaró POD-ok többféle elektronikai zavar generálására képesek, így bevetethetők repülőgépek fedélzeti és a földi telepítésű radarok ellen. [7] A Honvédelmi Minisztérium közleménye szerint „Az Észak-atlanti Szövetség által előírt NEWFIP (NATO Electronic Warfare Force Integration Programme) 2014 gyakorlaton a katonai eszközök nem használtak semmilyen, a polgári légiközlekedés biztonságát veszélyeztető frekvenciát. Emellett a gyakorlat helyszíne miatt az is kizárt, hogy mindez bármilyen kihatással lehetett volna az osztrák vagy a cseh légiközlekedésre.” [8] Természetesen az eseményt számos repülésirányítási- és biztonsági szervezet kivizsgálása követte. A vizsgálat eredménye szerint a légi forgalom irányításában tapasztalt fenti problémát egy alvállalkozó által a radarrendszerek egyikén végzett fejlesztés/tesztelés okozta. [9]

## A tudományos probléma megfogalmazása

Mint azt a bevezetőben már említettem, a világ különböző részein **a biztonsági helyzet folyamatos változása, sok esetben romlása** egyre nagyobb terhet ró az országok biztonsággal foglalkozó szervezeteire, **ebbe beleértve a különböző titkosszolgálatokat, rendőri és határvédelmi szervezeteket, haderőket**. Az utóbbi időszakban az európai országokban a tervezett és elkövetett terrorista támadásokkal kapcsolatban folyamatosan növekszik a nyomás a védelmi szervezeteken, mind a politikai oldalról, mind a lakosság részéről. A különböző európai országok haderői nemcsak az adott országban, de sok esetben más országban, más kontinensen próbálják elérni a terrorista elemek fészkeit, illetve a politikai döntésnek megfelelően segítenek az adott országban a demokrácia helyreállításában

---

<sup>5</sup> NATO Integrated Air and Missile Defence System

<sup>6</sup> Memorandum of Understanding, MoU

<sup>7</sup> Joint Electronic Warfare Core Staff, JEWCS

vagy kiépítésében. Ezeken a területeken azonban sok esetben a napjainkra jellemző aszimmetrikus hadviseléssel találják szembe magukat.

**A hadviselési módok változásai nagy kihívás elé állítják a művelettervezéssel foglalkozó szakembereket, hiszen nagyon gyakran olyan ellenfél ellen kell harcolni, akik nem használnak fejlett technikai eszközöket, rejtőzködnek, nem viselnek egyenruhát, illetve sok esetben a polgári – az úgynevezett puha célpontokat – támadják.** E problémák mellett természetesen nem szabad elfelejtenünk a hibrid hadviselést sem, amely a katonai tevékenységek mellett magában foglal számos egyéb, nehezen megfogható vagy értelmezhető tevékenységet, például a számítógépes hadviselést, a politikai és gazdasági nyomásgyakorlást.

**Annak érdekében, hogy ezen feladatok haderőre háruló részei megfelelő szinten végrehajthatóak legyenek, egy kompetens nemzeti haderőre – és a nemzeti haderőkre alapozva – megfelelően skálázható képességű és interoperabilis nemzetközi haderőre van szükség.** Mint azt a bevezetőben már bemutattam, a nemzetek különböző mértékben fordítanak erőforrásokat a saját haderejükre, azonban ennek következménye lehet például akár a közös együttműködést negatívan befolyásoló kompatibilitási probléma is.

A különböző katonai feladatok egyik alkotó eleme az elektronikai hadviselés (a továbbiakban EHV), amely napjaink konfliktusaiban folyamatosan jelen van, a művelettervezési folyamatokban és a feladatok végrehajtása során hatássokszorozó<sup>8</sup>, hatásművelő képességként veszik figyelembe. Korábban az információs műveletek<sup>9</sup>, az ellenséges légvédelem lefoglalása<sup>10</sup> vagy a célmeghatározás/céltervezés<sup>11</sup> szerves alkotóelemeként tekintettek rá, míg napjainkban a gyakran emlegetett Anti-Access – Area-Denial (hozzáférést gátló – területmegtagadó, A2/AD) eljárás szerves részeként is kezelik.

**Ahhoz, hogy az elektronikai hadviselési képesség alkalmazása valóban hatékony legyen, fejlett, a kor legújabb technikai újításait felhasználó technikai eszközökre van szükség.** A különböző tanulmányokból, a katonai technikai bemutatókról megjelenő cikkekből, illetve a különböző konfliktusok leírásaiból, elemzéséből egyértelműen látható, hogy a különböző államok – kiemelten az Amerikai Egyesült Államok, Oroszország és Kína [10] – jelentős összegeket fordítanak az elektronikai hadviselési képesség fejlesztésére, illetve a fejlesztésekkel kapcsolatban gyakorlati, harci tapasztalatok szerzésére. Itt fontos kihangsúlyozni azt is, hogy az így megszerzett tapasztalatok beépítése, felhasználása nemcsak

---

<sup>8</sup> A művelettervezés során sok esetben az angol terminológiában alkalmazott „Enabler” szóval párosítják.

<sup>9</sup> Information Operations, INFOOPS

<sup>10</sup> Suppression of Enemy Air Defence, SEAD

<sup>11</sup> Targeting, AAP-6 (2011)

az újabb fejlesztések vagy a szükséges módosítások végrehajtásakor lehetséges, hanem az elektronikai hadviselési Taktikák, Technikák és Eljárások<sup>12</sup> felülvizsgálatakor is.

**Szakmai álláspontom szerint a Magyar Honvédségnek Magyarország gazdasági és katonai teljesítőképességével arányos védelmi és támadó célú elektronikai hadviselési képességgel kell rendelkeznie, melyhez az aktuálisan elérhető fejlesztéseket, eljárásokat fel kell használnunk.**

Az eddig végzett kutatómunkám eredményei alapján szakmai véleményem az, hogy a szoftverrádió technológia alkalmazása megfelelő alap a képesség fejlesztésére úgy, hogy a későbbi fejlesztés lehetősége a már meglévő eszközökben biztosított lesz. Fontos azt megjegyezni, hogy az ad-hoc jellegű, a különböző katonai szervezeteknél eltérő típusú és képességű eszközök beszerzése, vagy más szervezetektől történő eszközök átvétele nem tekinthető megfelelő szintű fejlesztésnek.

## Kutatási hipotézisek

Az eddig megfogalmazottak alapján az alábbi hipotéziseket szándékozom igazolni:

- **Az elektronikai hadviselési képesség és annak konfliktusokban történő alkalmazása minden nemzet számára fontos kérdés lesz a jövőben is. A hadviselési módoknak és eljárásoknak továbbra is szerves részét fogja képezni az elektronikai hadviselés, a nemzetek továbbra is jelentős erőforrásokat fordítanak a fejlesztésére, a különböző technológiák együttes alkalmazásával tovább növelve hatékonyságát.**

- **A szoftverrádió technológia mára már szerves részét képezi a különböző technikai eszközöknek és rendszereknek. Az SDR technológia alkalmazása alapvető követelmény kell, hogy legyen a Magyar Honvédség elektronikai hadviselési képességének fejlesztésekor, feltételezve azt is, hogy más fejlesztések egyidejű alkalmazásával a technológia által nyújtott előnyök tovább fokozhatóak.**

- **A Magyar Honvédség részére a szoftverrádió technológián alapuló elektronikai hadviselési eszközök/rendszerek beszerzése jelentős előnyt nyújthat a későbbi fejlesztések során.**

- **A szoftverrádió technológia alkalmazása a különböző elektronikai hadviselés szervezeti elemek feladatrendszerére is kihatással van, amelyet a különböző szintű szervezeti elemek kialakításakor le kell követni.**

---

<sup>12</sup> Tactics, Technics and Procedures – TTP



## Kutatási célkitűzések

Napjainkban a különböző szövetségi tagságokból (NATO, EU, Visegrádi Négyek, stb.) eredően az országra és a Magyar Honvédségre (a továbbiakban MH) jelentős elvárások nehezednek, melyeknek eleget kell tenni. Az MH feladatainak végrehajtása során **az elektronikai hadviselés – a megfelelő képzettséggel és szakmai tapasztalattal rendelkező állomány, valamint a fejlett technikai eszközpark megléte esetén – képes hozzájárulni a különböző szintű katonai vezetés számára szükséges aktuális helyzetkép biztosításához, illetve az alkalmazott kötelék/kötelékek támadó és védelmi képességének fokozásához.**

Értekezésemben alapvetően az elektronikai hadviseléssel foglalkozom, az MH elektronikai hadviselési rendszerével kapcsolatban teszek javaslatokat, azonban figyelembe kell venni, hogy hadműveleti szintig az így megszerzett információk a rövidtávú döntéshozatali rendszerben is felhasználhatóak úgy, mintha azok rádiófelderítő információk lennének. Fontos természetesen az is, hogy az értekezésben elemzett szoftverrádió technológia a kimondottan rádióelektronikai felderítő célú eszközök vonatkozásában is felhasználható. A korábbi időszak MH vonatkozású szervezeti és technikai változásainak vizsgálatokor **mind az elektronikai hadviselési, mind a rádióelektronikai felderítő szervezeteket bemutatom, elemzem, mivel több esetben összefonódtak egymással.** Esetünkben lényeges, hogy a szárazföldi haderőnem vonatkozásában jelenleg az MH egy elektronikai hadviselés századdal rendelkezik, amely Debrecenben települ és az MH ÖHP szakmai irányításával végzi feladatait, illetve az, hogy a korábbi harcászati és hadműveleti szintű rádióelektronikai felderítés feladatrendszerébe beolvadt a Magyar Honvédség elektronikai hadviselési szervezetének feladatrendszerébe. A fentiek tükrében – amikor az elektronikai támogatással kapcsolatban teszek megállapítást – az megfeleltethető a rádiófelderítésre is harcászati, hadműveleti szinten.

**Témaválasztásomat alapvetően az elektronikai hadviselés alkalmazásának egyértelműen bizonyítható aktualitása, a különböző katonai – hazai, NATO és békeműveleti – beosztásokban eltöltött éveim során megszerzett tapasztalatom határozta meg.** Mindegyik beosztással kapcsolatban elmondható, hogy a különböző tervezési feladatok, valamint az elrendelt feladatok végrehajtása során, rövid időn belül felmerült, hogy az elektronikai hadviselés valamely eleme milyen formában lehet jelen, vagy támogathatja munkánkat.

Jelen kutatásommal kettő célt kívánok elérni. Egyrészt bemutatom, hogy a Magyar Honvédség jelenlegi elektronikai hadviselési képessége a szoftverrádió technológia által nyújtott előnyök felhasználásával jelentős mértékben fejleszthető, másrészt pedig vizsgálom az SDR technológia alkalmazásával kapcsolatban megjelenő, az elektronikai hadviselési elemekbe integrálandó új feladatrendszerek vonatkozásában szükséges új szervezeti elemek/képességek kialakítását.

A kutatási célkitűzéseimet a következő részekre bontva érem el:

1. Az elektronikai hadviselés különböző **konfliktusokban és a hadviselés különböző területein történő alkalmazásának, valamint az egyes nemzetek EHV területen végrehajtott fejlesztési tevékenységének vizsgálatával értékelni és igazolni az elektronikai hadviselési képesség folyamatos fejlesztésének szükségességét.**

2. Napjaink korszerű haditechnikai eszközeiben és rendszereiben kiemelt fontosságú a legkorszerűbb technológia és alkalmazások beépítése. Sok esetben kettő új fejlesztés egyidejű beépítésével/bevezetésével hatványozottan érhetünk el eredményeket. **Céлом vizsgálni a szoftverrádió technológia különböző technikai eszközökben történő alkalmazását, illetve elemezni a szoftverrádió technológián alapuló elektronikai hadviselési eszközök Magyar Honvédségben történő alkalmazásával elérhető előnyöket.**

3. Az első és második pont kutatási eredményeinek felhasználásával **meghatározni a szoftverrádió technológia alkalmazásán alapuló EHV eszközzel szemben támasztott perspektivikus harcászati-műszaki követelményeket**, figyelembe véve az előző pontokban elemzett egyéb technikai lehetőségeket is.

4. A kutatás során **megvizsgálni és javaslatokat kidolgozni a szoftverrádió technológia alapú EHV eszközrendszer alkalmazásához szükséges szervezeti változtatásokra az alakulatok sajátosságainak és a vezetési szinteknek megfelelően.**

## Kutatási módszerek

Az értekezésem elkészítéséhez az alábbi kutatási módszereket alkalmaztam:

- irodalomkutatás, amely magában foglalta a szoftverrádió technológiával kapcsolatban megjelent nemzetközi és hazai szakirodalom tanulmányozását és feldolgozását;
- korábbi kutatások másodelemzése, **a szoftverrádió technológia és az elektronikai hadviselés vonatkozásában készült kutatási eredmények elemzése és feldolgozása**, ebbe beleértve a korábban az MH érdekében végzett technikai fejlesztések vizsgálatát is;

- összehasonlító elemzés, a korábban elért kutatások, valamint fejlesztések eredményeinek összevetése;
- empirikus kutatások, **a saját – a különböző hazai, NATO és békeművelési beosztásokban eltöltött éveim során megszerzett – szakmai tapasztalataim felhasználása;**
- a párhuzamosan –, „Az Emberi Erőforrások Minisztériuma ÚNKP-17-3-IV-NKE-16 kódszámú Új Nemzeti Kiválóság Programjának támogatásával” végzett kutatásom eredményeivel történő összehasonlítás;
- konferenciákon, releváns szakmai bemutatókon és rendezvényeken, különböző szabályzatfejlesztési tevékenységekben történő részvétel;
- a kutatási eredmények feldolgozása, cikkek, könyvfejezetek és egyéb publikációs formában történő ismertetése, valamint konferenciákon és oktatásban történő előadása.

## Releváns szakirodalom áttekintése

Az értekezésem elkészítése során jól alkalmazható forrásként szolgáltak **a hazai szakemberek, tudományos fokozattal rendelkezők publikációi, korábbi kutatási eredményei.** Az értekezés kidolgozása során feldolgoztam a Nemzeti Közszerződési Egyetem, illetve a Katonai Műszaki Doktori Iskola oktatóinak és doktorhallgatóinak szoftverrádió technológiával és elektronikai hadviseléssel kapcsolatos tudományos munkáit, oktatási anyagait, doktori értekezéseit.

A kutatási téma szempontjából szintén relevánsak a hazai ipar fontosabb szereplőinek kutatásairól, fejlesztéseiről elérhető publikációk, termékismertetőik. **A fejlesztésekkel kapcsolatban külön kiemelem az Integrált elektronikai felderítő és zavaró rendszer fejlesztésével, az INTERJAM projekttel kapcsolatos eredményeket, elérhető publikációkat.**

A Magyar Honvédség tevékenységével kapcsolatos forrásokkal kapcsolatban lényegesek továbbá a vonatkozó biztonsági stratégiák, illetve a különböző jogszabályok, ebbe beleértve nemcsak az Magyar Honvédségre közvetlenül vonatkozó jogszabályokat, hanem a tevékenységéhez közvetve kapcsolódókat is.

**Az idegen nyelvű források vonatkozásában fontos és jól alkalmazható ismeretanyagot biztosítottak a NATO különböző szervezeteinek nyílt forrásokban elérhető szakanyagai, publikációi.** Az idegen nyelvű források vonatkozásában kiemelem még a szakkiadóként nyilvántartott Artech House könyveit is, melyeket a korábban említett,

az Emberi Erőforrások Minisztériuma által támogatott kutatásomhoz kapcsolódóan sikerült a Nemzeti Közszerológiai Egyetem könyvtára részére beszerezni.

Számos külföldi kutató publikációja is elérhető a témában, azonban fontos, hogy az értekezésem fő forrásait a hazai tudományos publikációk alkották.

### **A kidolgozás során érvényesült korlátozások**

Az értekezésben a témától való jelentős eltérés, valamint terjedelmi korlátok miatt nem vizsgáltam az alábbi kapcsolódó kérdésköröket:

- A Magyar Honvédség elektronikai hadviselési szervezeteinek számát, képességét, funkcióját, illetve az ezekben szükséges módosításokat.
- Az elektronikai hadviselési eszközök ellen alkalmazható „kemény típusú”, pusztító támadásokat.
- A kialakítandó rendszerrel szemben támasztandó funkció specifikáció mellett a műszaki specifikáció számszaki adatai csak részben kerülnek meghatározásra, mivel az időközben történő kutatások-fejlesztések, illetve az így elérhetővé váló új elemek és képességek jelentős változást okozhatnak az eszköz egyes paramétereiben, és emiatt akár a teljes rendszerben.
- A perspektivikus kidolgozás miatt felmerülhet olyan, jelenleg még nem megoldott műszaki kérdés, amely további elemzést/kutatást igényel. Ilyen például a mintavételezés megoldása magas frekvencián.

Fontosnak tartom itt megjegyezni, hogy a 2019.01.01-től megalakításra kerülő Magyar Honvédség Parancsnokság az értekezésben szereplő, az összhaderőnemi/hadműveleti szintre, valamint a harcászati szintre vonatkozó javaslatokat/megállapításokat nem befolyásolja, mivel a fent felsorolt szintek feladatait a megnevezéstől függetlenül valamelyik katonai szervezetnél végezni kell.

# **1. A BIZTONSÁGPOLITIKAI HELYZET VÁLTOZÁSÁNAK ÉS A TECHNIKAI FEJLŐDÉS HATÁSA AZ ELEKTRONIKAI HADVISELÉS ALKALMAZÁSÁRA**

**Napjaink biztonságpolitikai helyzetére jellemző annak komplexitása, melyben a felmerülő problémák kezelése során a politikai, a gazdasági és a diplomáciai eszközök, valamint a fegyveres erők alkalmazása szinkronizálást és megfelelő egyensúlyt igényel. A biztonságpolitikai helyzetben bekövetkező változások, illetve a tudomány minden területén folyamatosan megjelenő újítások jelentős hatással bírnak a haderők alkalmazásának tervezésére, a műveletek végrehajtására, az egyes szakterületek esetében a Taktikák, Technikák és Eljárások<sup>13</sup> változásaira.**

## **1.1. Biztonságpolitikai változások**

Az egyes országok, régiók **biztonságpolitikai helyzetét a környező és távolabbi országokban zajló események és a különböző szervezetek** (pl. Észak-atlanti Szerződés Szervezete<sup>14</sup>, a továbbiakban: NATO, Európai Unió<sup>15</sup>, a továbbiakban: EU, stb.) **tevékenysége egyaránt befolyásolja.** Az utóbbi években/évtizedekben jelentős változások mentek végbe nemcsak Európában, de az Amerikai Egyesült Államokban, illetve a Közel-Keleten is. Emiatt Magyarország biztonságpolitikai helyzetének elemzésekor is számos fontos állomást meg lehet, illetve meg kell jelölni, amelyek a politikai, a gazdasági vagy a biztonsági helyzetre – és így a Magyar Honvédség helyzetére (létszám, felszerelés, stb.) és feladataira – is nagy hatással bírtak. Ilyen események például a **Varsó Szerződés** katonai szervezetének 1991. április 01-jén történt felbomlása, 1999-ben a **NATO**-hoz és 2004-ben az **EU**-hoz történt csatlakozás, de az Amerikai Egyesült Államok ellen 2001. szeptember 11.-én elkövetett támadás is befolyásolta Magyarország katonai tevékenységét.

---

<sup>13</sup> Tactics, Technics and Procedures – TTP

<sup>14</sup> NATO – North Atlantic Treaty Organization

<sup>15</sup> EU – European Union

Magyarország szuverenitásának és integritásának védelme a Magyar Honvédség alaprendeltetéséből eredő feladata és emiatt Magyarország aktívan részt vállal a NATO 5. cikkely<sup>16</sup> alá, illetve az 5. cikkely alá nem tartozó<sup>17</sup> műveleteiben, az EU és az Egyesült Nemzetek Szövetsége (a továbbiakban ENSZ) válságkezelő tevékenységében, az fenti feladatokhoz szükséges képességek nemzeti és kollektív keretek közötti fejlesztésében. [13] Emellett fontos a **Visegrádi Négyekhez** való tartozásból eredő kötelezettségek teljesítése is. Mindezen feladatok teljesítése érdekében számos jogszabályi változtatás is történt, a korábbi Alkotmányt, illetve az 1993. évi, a honvédelemről szóló CX. törvényt idővel felváltotta az Alaptörvény [14], illetve a Honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvény, amelyek alapját Magyarország Nemzeti Biztonsági Stratégiája [15], valamint a Nemzeti Biztonsági Stratégia alapján kidolgozott Nemzeti Katonai Stratégia [16] képezi.

A biztonságpolitikai helyzet gyors és éles változásának lehetőségét fogalmazták meg a Nemzeti Biztonsági Stratégiában, miszerint *„globalizált világunkban a biztonság nem a határainknál kezdődik. A távoli biztonsági kockázatok, kihívások és veszélyforrások drámai gyorsasággal kerülhetnek határainkon belülre.”* [15] A dokumentumban megfogalmazásra került, hogy Magyarország elleni hagyományos fegyverekkel végrehajtott támadás veszélye csekély, azonban nem szabad figyelmen kívül hagyni más országokban és régiókban zajló eseményeket, konfliktusokat. [15]

A Nemzeti Katonai Stratégia Magyarország Alaptörvényében, a védelmi szféra tevékenységét meghatározó jogszabályokban, a NATO Stratégiai Konceptiójában, az Európai Biztonsági Stratégiájában, valamint a Nemzeti Biztonsági Stratégiában megfogalmazottak alapján került összeállításra. Az értekezésem vonatkozásában fontos és emiatt kiemelek néhány, a Nemzeti Katonai Stratégiában meghatározott alapelvet. Ezek között szerepel a

<sup>16</sup> 5. cikkely: „A Felek megegyeznek abban, hogy egyikük vagy többjük ellen, Európában vagy Észak-Amerikában intézett fegyveres támadást valamennyiük ellen irányuló támadásnak tekintenek és ennél fogva megegyeznek abban, hogy ha ilyen támadás bekövetkezik, mindegyikük az Egyesült Nemzetek Alapokmányának 51. cikke által elismert jogos egyéni vagy kollektív védelem jogát gyakorolva, támogatni fogja az ekként megtámadott Felet vagy Feleket azzal, hogy egyénileg és a többi Féllel egyetértésben azonnal megteszi azokat a intézkedéseket - ideértve a fegyveres erő alkalmazását is -, amelyeket a békének és biztonságnak az észak-atlanti térségben való helyreállítása és fenntartása érdekében szükségesnek tart. Minden ilyen fegyveres támadást és ennek következtében fogantatott minden intézkedést azonnal a Biztonsági Tanács tudomására kell hozni. Ezek az intézkedések véget érnek, ha a Biztonsági Tanács meghozta a nemzetközi béke és biztonság helyreállítására és fenntartására szükséges rendszabályokat.” [11]

<sup>17</sup> Nem az 5. cikkely alá tartozó műveletek: humanitárius segítségnyújtás, kimenekítési művelet, a természeti katasztrófák esetén nyújtandó támogatás, a különböző szankciók és embargók megvalósítása, valamint a válságreakáló művelet.

A válságreakáló művelet fogalma a Magyar Honvédség Összhaderőnemi Műveleti Doktrína alapján: A válságreakáló műveletek általában a harci (háborús) katonai műveletekhez képest eltérő, más jellegű, ugyanakkor komplex környezetben folynak, így a fegyveres küzdelem elveitől, törvényeitől eltérő sajátosságok érvényesülhetnek a műveletek végrehajtása során. [12]

**modern technológia** alkalmazása, a **nemzeti önerő** fejlesztése, a **haderő lehetséges alkalmazása a műveletek teljes spektrumában** (alacsony - magas intenzitású műveletekben egyaránt), a **megváltozott műveleti körülmények** (professzionális haderő, lakott területek és a polgári lakosság érintettsége, stb.), valamint az **új elemek megjelenése** (hálózatalapú hadviselés, a civil-katonai együttműködés, a pszichológiai hadviselés, stb.). [16]

**Az új típusú kihívások egyik tipikus példája és az 5. cikkely alkalmazhatóságának próbája egy NATO tagállam elleni gazdasági vagy kibertámadás.** A kibertámadással kapcsolatos kérdések 2007-ben váltak valóssá, amikor Észtország bejelentette, hogy a Tallinn központjában található második világháborús orosz katonai emlékművet a városban található katonai temetőbe helyezik át, és rövid időn belül kibertámadás célpontjává vált a balti állam. [17]

Amennyiben Magyarország tényleges katonai szerepvállalásait vizsgáljuk, látható, hogy katonáink a NATO, az EU és az ENSZ műveletek során különböző feladatokat hajtanak végre a világ minden részén, Irakban, Afganisztánban, Afrikában, illetve a Balkánon. [13] Az MH a Visegrádi Négyek együttműködésén belül 2016. január 01. - 2016. június 30. között 716 fővel részt vett az V4 EU Harccsoport állományának biztosításában. [18] Ez a feladat 2019. évben újra szerepel majd az MH feladatai között.

Napjaink válságait elemezve mindenképpen meg kell említeni Európa, a NATO, valamint Oroszország kapcsolatát is befolyásoló **ukrán – orosz konfliktust**, valamint **Iszlám Állam (IS)**, vagy más forrásokban az **Iraki és Szíriai Iszlám Állam<sup>18</sup> (a továbbiakban ISIS) elleni nemzetközi fellépést**, illetve a 2015-ben jelentős méreteket öltött **migráció Európára gyakorolt hatását**.

2013-ban Viktor Janukovics ukrán elnök nem írta alá az EU uniós szabadkereskedelmi egyezményt, emiatt tüntetések kezdődtek. A tüntetések eredményeképpen ideiglenes elnököt neveztek ki, az általa vezetett kormányt az USA és az EU elismerte, azonban Oroszország nem. Az ország keleti felében a tüntetések erőszakossá váltak. 2014-ben oroszbarát fegyveres erők fokozatosan átvették az ellenőrzést a Krím-félsziget fölött, amely egy népszavazást követően csatlakozott Oroszországhoz. Ukrajna a NATO-hoz és a gazdasági nagyhatalmakhoz fordult segítségért, illetve 2014-ben az orosz nyomás ellenére aláírták a társulási egyezményt az EU-val. Több alkalommal tartottak egyeztetést az érdekelt felek a konfliktus megszüntetése érdekében, azonban minden résztvevő fél számára megfelelő

---

<sup>18</sup> Islamic State of Iraq and Syria, ISIS

megoldást azóta sem sikerült találni. A konfliktus már a tüntetések idején is számos polgári és katonai áldozatot követelt, ez a szám a kialakult fegyveres konfliktus során tovább növekedett. A legnagyobb polgári áldozattal járó eset 2014 júliusában a Malaysia Airlines 17-es járatának lelövése volt a donyecki terület felett, amelyben majd 300 fő veszítette életét. [19]

Napjaink egyik legfenyegetőbb terrorszervezete az Iszlám Állam (IS), vagy korábbi nevén Iraki és Szíriai Iszlám Állam (ISIS). A szervezet Irakban és Szíriában tűnt fel, céljuk egy tálib-típusú kalifátus létrehozása az iszlám törvények szerint. Irakban jelentős területeket foglaltak el, azonban Szíriában már nem voltak ilyen sikeresek. Alkalmazott módszereik között vannak a rajtaütésszerűen szervezett akciók, katonai demonstrációk, felvonulások. A brutálisan végrehajtott akciók hatására széleskörű nemzetközi katonai válaszlépések kerültek végrehajtásra az ISIS ellen, azonban szövetséges katonai válaszlépések hatékonysága a nehezen beazonosítható erők, illetve sok esetben ismeretlen, vagy nehezen behatárolható települési helyük miatt erősen megkérdőjelezhetőek voltak a kezdeti időszakban. A szövetséges erők 2016-2017-ben azonban jelentős sikereket értek el, az ISIS területeit jelentős mértékben sikerült visszafoglalni. [20]

A már korábban említett konfliktusok helyszíneiről, így Irakból, Afganisztánból, Szíriából jelentős tömegek indultak el Európa felé 2015. év nyarán. A háborús menekültek kiegészültek a gazdasági okokból hazájukat elhagyókkal és az így kialakult migráns hullám Európa néhány államára jelentős terhet rótt. Emiatt az államok többsége egyéni megoldásokat választott saját érdekei védelme érdekében, azonban emellett támogatva az egységes megoldás kialakítását. A migrációs problémák hatékony kezelése érdekében a szükséges jogszabályi változtatásokat követően a Magyar Honvédség a honi területen történő alkalmazhatóság érdekében szélesebb jogkörrel került felruházásra.

Bár a modern nyugati világ átlagembere sok tekintetben a korábbi időszakokhoz képest tájékozottnak mondható, kevés információval rendelkezik arról, hogy számos helyi konfliktus és kisebb-nagyobb háború van folyamatban. A Conflict Barometer 2013 című elemzésében megtalálható, hogy 2013-ban összesen 414 olyan konfliktus volt, amely veszélyeztette az érintett államok működését is. A fenti konfliktusok 80 százaléka az adott államon belül zajlott. A kutatócsoport összesen **45 konfliktust sorolt a fegyveres erőszak szervezett alkalmazásának jegyeit mutató súlyos válságok közé, melyből 20-at helyeztek a konfliktusok ötfokozatú skáláján a legsúlyosabb kategóriába, vagyis a háborúk közé.** [21]



A különböző konfliktusok során számos változás következett be mind az egyes államok politikai hozzáállásában, mind a hadviselés módjában. A hadviselés módjának változása alatt a szembenálló felekben, a Taktikában, Technikában és Eljárásokban<sup>19</sup>, valamint az alkalmazott technikai eszközökben bekövetkezett változásokat értem. **Napjaink legtöbb konfliktusát aszimmetrikus hadviseléssel vívják, amely a hadviselés negyedik generációja.** Legfontosabb jellemzője, hogy nem reguláris seregek/csatatok vesznek részt benne, illetve megjelent a hálózat alapú hadviselés. **A környezet értékelésénél nagy hangsúlyt kapott nemcsak a katonai, hanem a polgári környezet (kultúra, társadalom, stb.) befolyása is. Az egyik legfontosabb feladattá az ellenség stratégiai súlypontjának<sup>20</sup> helyes beazonosítása vált.** A nem reguláris hadviselő feleket nem állami szereplők (etnikai és vallási csoportok, politikai mozgalmak, bűnszervezetek) is alkothatják, akik rendelkeznek megfelelő képességgel és szándékkal arra, hogy céljaikat elérve támadják a központi hatalmat vagy egy másik államot. [22] Az elektronikai hadviselés a napjainkban megjelent hibrid hadviselés során is alkalmazásra kerülhet. A hibrid hadviselés fogalmára is több meghatározást találhatunk, vannak, akik úgy beszélnek róla, mint ami a hagyományos és az irreguláris hadviselés együttes alkalmazását jelenti, míg mások a diplomácia, a katonai erő és a gazdaság eszköztárának kombinált igénybevételét értik alatta. Fontos szempont az, hogy a hibrid hadviselés esetében *„jelentősen lecsökken az előrejelzés ideje”, ami „az azonnali reagáló erők készenléti szintjének és létszámának további növelését, illetve a politikai vezetés döntéshozatali folyamatának újragondolását”* [23] igényli.

## 1.2. Elektronikai hadviselés és a rádióelektronikai felderítés napjaink konfliktusaiban

Az elektronikai hadviselést már alkalmazták az első és második világháborúban, illetve azóta is jelen van a különböző hadszíntereken lezajlott vagy az éppen napjainkban is folyamatban lévő konfliktusokban. Példaként említhetem a kezdeti időszakból az arab-izraeli háborúkat, a Falkland-szigetekért folytatott harcot, de alkalmazásra került a hidegháború időszakában is.

Értekezésemben az 1991. évet követő eseményeket vizsgálom részletesebben, mivel ebben az évben **kezdődött el az első Öböl-háború, amely a vezetési hadviselés elveinek, céljainak, módszereinek és teljes technikai rendszereivel került megvívásra.** [24] Napjaink konfliktusainak rövid elemzésével célom, hogy bemutassam, az elektronikai hadviselés, illetve a rádióelektronikai felderítés szerves része a különböző műveleteknek,

<sup>19</sup> Tactics, Techniques, and Procedures (TTPs)

<sup>20</sup> Center of Gravity

illetve a korábbi időszakhoz képest jelentős képességfejlődést elérve biztosíthatja a szükséges hadműveleti célok gyors elérését.

Az elektronikai hadviselés az utóbbi években, évtizedekben rendkívüli változásokon ment keresztül. Ennek oka, hogy az elektromágneses spektrumot külön műveleti szintérnek ismerik el, új és veszélyes irányított fegyverek jelentek meg, amelyekben jelentős mennyiségű elektronikai elem van jelen, melyek befolyásolják a pontosságát és a halálosságát ezeknek a fegyvereknek. [25]

**Az elektronikai hadviselés alkalmazásának változását leginkább a technikai fejlődés, az újabb és újabb technikai eszközök megjelenése okozta, amely magában foglalta a doktrínális változásokat is, beleértve ebbe az eljárások és definíciók változását is.** A Varsói Szerződés felbomlásával egyre inkább megfigyelhető, hogy az addig vallott harcászati (hadműveleti, hadászati) elvek és a hozzájuk kapcsolódó katonai terminológiák átértékelődnek, esetenként új megfogalmazást nyernek. [26]

**Az Öböl-háború első időszakában az elektronikai hadviselési képességgel bíró repülőgépeknek jutott nagy szerep, feladatuk az ellenség légtérelenőrző és fegyverirányítási rendszereinek lokátorainak felfedése, elektronikai zavarása, elnyomása<sup>21</sup> vagy AGM-88 HARM<sup>22</sup> rakétával történő pusztítása volt.** [27] Ilyen célokra az amerikai légierő F-4G Wild Weasel, EF-111A Raven, az amerikai haditengerészet és a tengerészgyalogság F/A-18 Hornet, EA-6B Prowler, A-6 Intruder és A-7 Corsair repülőgépei, a nem-kommunikációs felderítési<sup>23</sup> feladatokra pedig az amerikai légierőhöz tartozó EC/RC-135 Rivet Joint, az amerikai haditengerészethez tartozó EP-3 és EKA-3B repülőgépek, valamint a brit légierő Nimrod R.1. repülőgépei kerültek bevetésre. A repülőgépekre telepített elektronikai hadviselési és nem-kommunikációs felderítő eszközökkel képesek voltak az iraki erők kommunikációs és nem-kommunikációs eszközei telepítési helyeinek feltérképezésére, a jellemző paraméterek meghatározására, majd azok működésének eredményes blokkolására vagy az eszközök pusztítására. [28]

Az 1995-ben kezdődött IFOR<sup>24</sup> misszióban az USA RC-135 és RC-12 Guardrails, a brit Nimrod R2-es, a francia C-160 Transall, a német Atlantiques repülőgépek kerültek

<sup>21</sup> Suppression of Enemy Air Defenses - SEAD

<sup>22</sup> High-speed Anti-Radiation Missile, nagy sebességű radarromboló rakéta

<sup>23</sup> Electronic Intelligence – ELINT, nem-kommunikációs felderítés

<sup>24</sup> Bosznia-Hercegovina területére telepített NATO vezetésű, többnemzetiségű béketámogató haderő megnevezése, Implementation Force, IFOR

alkalmazásra SIGINT feladatokra. [29]

**Az iraki és afganisztáni hadműveletek esetében a szövetségesek részéről szintén alkalmazásra kerültek EHV, illetve SIGINT eszközök, azonban a szembenálló felek nem rendelkeztek ilyen eszközökkel, elektromágneses kisugárzó eszközeik között leginkább a kapcsolattartásra és a rádió-távírányítású improvizált robbanóeszközök (RC-IED<sup>25</sup>) indítószerkezeteként is használt mobiltelefonok, kis hatótávolságú kézi rádiók voltak megtalálhatóak.** Emiatt a szövetségesek sem alkalmazták a rendelkezésre álló erők teljes spektrumát, így a nem-kommunikációs felderítő és zavaró eszközök meg sem jelentek. [30] A kommunikációs felderítő eszközök célja a felderítési információk biztosítása és megerősítése volt. Az elektronikai zavarás alkalmazása a kommunikációs eszközök zavarására, valamint a RC-IED-k indítószerkezetének semlegesítésére korlátozódott. Számos esetben itt is alkalmazásra került a légierő EHV képessége, az utak mentén telepített RC-IED eszközök ellen az úgynevezett „burning”<sup>26</sup> eljárásra alkalmazták a német Panavia Tornado repülőgépeket. **A különböző hadműveleti területeken az alkalmazott eszközök/képességek is eltérnek egymástól,** míg Afganisztánban a rádió-távírányítású improvizált robbanóeszközök lázadók általi alkalmazása jelentős volt, addig ez a veszély a Balkáni műveleti területen napjainkban kevésbé jellemző. [31]

Nem kimondottan háborús helyszín, azonban folyamatosak a diplomáciai konfliktusok Észak- és Dél-Korea között. A konfliktusok egyikének alapja elektronikai hadviselési vonatkozású. 2012. április 28. és május 6. között több száz repülőgép, illetve száznál is több hajó is jelezte, hogy műholdas helymeghatározó készülékük nem működött, mivel nem vették a műholdak által sugárzott jeleket. Dél-Korea Észak-Koreát vádolta meg azzal, hogy a zavarójel sugárzása az egyik határmenti városukból történt. Ebben az esetben fontos azt kihangsúlyozni, hogy alapvetően polgári személyeket veszélyeztettek. [32]

2014-től kezdődően az egyik legújabb hadszíntér az Iszlám Állam<sup>27</sup> (ISIS) ellen folytatott háború, amelyhez folyamatosan csatlakoztak újabb és újabb országok. Az USA és az általa vezetett művelethez csatlakozott államok légitámadásokkal igyekeztek az állásokat és utánpótlási útvonalakat rombolni, bevetésre kerültek az elektronikai hadviselési és a már korábban is említett SEAD képességgel rendelkező F-16CJ/CG, az EA-6B Prowlers és EA-18G Growlers típusú repülőgépek, de sok információ érhető el drónok vagy az F-22 típusú

<sup>25</sup> RC-IED, Radio controlled improvised Explosive Device

<sup>26</sup> Burning: égetés

<sup>27</sup> ISIS vagy IS, Islamic State of Iraq and Syria

repülőgépek alkalmazásáról is. A korábbi afganisztáni és iraki példákkal ellentétben, ahol a lázadó erők nagyon csekély mértékben használták ki az elektronikai hadieszközök illetve vezetési módszerek nyújtotta lehetőségeket, az ISIS nagymértékben beintegrálja eljárásaiba a fejlett technológiák által nyújtott lehetőségeket, az internet alkalmazásával információs hadviselést folytat, drónokat alkalmaz bombák célba juttatására. [32] Az amerikai légierő 2014 novemberében valószínűsíthetően olyan ISIS bázisra mért légicsapást, ahol az ISIS egyik hacker csoportja mellett egy hozzájuk tartozó elektronikai zavaró állomás is telepítésre került. [33] Több forrásban is található utalás arra, hogy Szíriában is telepítésre került az orosz haderő egyik elektronikai hadviselési eszköze, a Krasukha-4 (Belladonna) is. [34]

Nem szabad elfelejtenünk azonban azt, hogy nemcsak a távolabbi földrészeken, hanem közelünkben is zajlanak konfliktusok. Ezekben is fontos szerep jut az elektronikai hadviselésnek természetesen, így például a 2013-ban elkezdődött orosz-ukrán konfliktusban is alkalmazásra került az elektronikai hadviselés. A nyílt forrásokban elérhető információk és fényképek alapján nagy bizonyossággal vélelmezhető, hogy az eszközök Oroszország irányából érkeztek a hadszíntérre, véleményem szerint önmagukban a szakadár erők nem juthattak volna ilyen eszközökhöz. Ukrajna, elektronikai hadviselési képesség hiányában a NATO-hoz és az Amerikai Egyesült Államokhoz fordult segítségért, rádiótechnikai zavaró eszközöket kért a szeparatisták birtokában lévő légvédelmi eszközök radarjainak megtevesztése vagy elektronikai zavarása érdekében. A kérés indokoltságát igazolja, hogy valószínűsíthetően valamilyen légvédelmi eszközzel lőttek le egy MI-17-es helikoptert és egy utasszállító repülőgépet Ukrajna felett. Az utasszállító repülőgép a malajziai légitársasághoz tartozott, fedélzetén mintegy 300 ember utazott. [36] Frederick Ben Hodges altábornagy, a NATO Szövetséges Szárazföldi Parancsnokság parancsnoka szerint az ukrán erőknek támogatásra van szükségük annak érdekében, hogy képesek legyenek használni rádióikat, mobiltelefonjaikat, mivel **az orosz elektronikai hadviselési eszközöket nemcsak a katonai híradórendszerek, de a polgári mobiltelefon rendszerek ellen is alkalmazták.** [37] Az 1.1 képen orosz gyártmányú elektronikai hadviselési eszköz látható, amelyről a Donbass területén készítettek fényképet.



1.1. kép: Orosz eredetű elektronikai hadviselési állomás Donbass területén. [38]

Mindenképpen szem előtt kell tartanunk azt, hogy az **elektronikai hadviselést** – az általa biztosított hatások leghatékonyabb felhasználása érdekében - számos más szakterületen/feladatban felhasználják, a tervezés és végrehajtás során azt beintegrálják. Ilyen szakterületek/feladatok például **a felderítés, az információs műveletek, az ellenséges légvédelem lefogása**<sup>28</sup> **vagy a célmeghatározás/céltervezés**<sup>29</sup>. Napjaink hadviselésével kapcsolatban gyakran olvashatunk az A2/AD mozaikszóról, amely az Anti-Access – Area-Denial, hozzáférést gátló – területmegtagadó szavak rövidítéséből származik. Annak vizsgálata, hogy az elektronikai hadviselés hogyan alkalmazható az A2/AD környezetben, egy rendkívül komplex kérdés. Értekezésemben azért tartom fontosnak ennek elemzését, mivel napjaink fejlett technológiai világában jelentős mennyiségben kerülnek alkalmazásra ebben a környezetben is az elektromágneses spektrumot használó haditechnikai eszközök, így radarok, kommunikációs és vezeték nélküli adatátviteli eszközök. Emiatt **egy fejlett elektronikai hadviselés képesség nagy hatékonysággal alkalmazható a saját műveleti céljaink elérése érdekében.**

A különböző szakirodalomban kisebb-nagyobb eltérésekkel ugyanazon definíciót találhatjuk a fenti szóösszetétel jelentésével/tartalmával kapcsolatban. Az egyik értelmezés szerint az „*A2 eljárás stratégia célja, hogy megakadályozza, megnehezítse a szemben álló fél*

<sup>28</sup> Suppression of Enemy Air Defenses, SEAD

<sup>29</sup> Targeting, AAP-6 (2011)

*erőinek bejutását a hadszíntérre, az Area-Denial – AD, területmegtagadó – műveletek célja pedig az, hogy egy adott területen minél kisebbre szorítsa, vagy megakadályozza a szemben álló fél cselekvési szabadságát.”* [39] Ugyanakkor azt is meg kell megjegyezni, hogy hivatalos NATO definíció még nem érhető el. Tovább pontosíthatjuk a fogalmat, ha hozzátesszük, hogy az A2 esetén nagy hatótávolságú eszközök, míg az AD esetén kis hatótávolságú eszközök alkalmazásáról beszélünk. [40] Ahhoz, hogy a különböző fegyverrendszerekkel létrehozott A2/AD buborék<sup>30</sup> leküzdhető legyen, egyik legfontosabb eszköz a légierő, amely azonban a célok támadása során szintén nagy veszélynek van kitéve, beleértve a rakétarendszerek és az elektronikai hadviselés által támasztott fenyegetést. Ennek kiküszöbölésére nagy hatótávolságú és precíziós, földről indítható rakéták használhatóak, melyek hatótávolsága néhány száz kilométertől néhány ezer kilométerig terjedhet. [41] Amennyiben valamely állam felépíti a fentiek szerint leírt fegyverrendszerek alkalmazásán alapuló képességet, már a birtokában van egy hatékony, az A2/AD képességet támadni képes rendszer.

Napjainkban egyre több információ jelenik meg Oroszország A2/AD képességéről, míg a NATO nem rendelkezik ilyen képességgel. A NATO egyes tagállamainak vannak részképességei, azonban ezek nincsenek hálózatba vagy egy rendszerbe integrálva. Oroszország és az USA mellett Kína és Irán is rendelkezik A2/AD képességgel. Miközben a különböző országok próbálják kialakítani vagy fejleszteni saját A2/AD képességüket, Oroszország már négy A2/AD zónát alakított ki a világban, Kalinyingrádban, a Fekete-tenger térségében, Szíriában és az Arktiszon. [42] Oroszország a kalinyingrádi, a fekete-tengeri és a szíriai A2/AD környezet kialakítását biztonsági és önvédelmi okokkal indokolta. A kalinyingrádi és a fekete-tengeri buborék a különböző NATO fejlesztésekre és együttműködésekre (pl. Európai rakétavédelmi program, stb.) adott válasz, míg a szíriai A2/AD környezet kiépítése a területen műveletet végrehajtó erőinek védelmét szolgálja. A fekete-tengeri buborék emellett stratégiai jelentőséggel is bír a Fekete-tengeri Flotta szevasztopoli bázisa miatt. [43] Az Arktiszon kialakított A2/AD buborék célja az ott elérhető nyersanyagokhoz történő hozzáférés biztosítása, melynek érdekében Oroszország *„a többi arktiszi államnál korábban elkezdte – a térségben amúgy is domináns – északi flottájának korszerűsítését, és rendszeresítette a járőrözést az északi légterében.”* [44] Kína legfontosabb indoka szintén gazdasági jellegű, mivel a Dél-kínai-tenger térségében szintén az elérhető nyersanyagokhoz történő hozzáférés biztosítása a cél. [45] Irán esetében az A2/AD környezet

---

<sup>30</sup> Az angol szakirodalmakban az A2/AD environment és az A2/AD bubbles szóösszetételeket alkalmazzák, melyeket A2/AD környezetnek, illetve A2/AD buboréknak fordítottam.

alkalmazása szintén gazdasági célú, mivel Teherán befolyása alá akarja vonni a Perzsa-öbölt és a Hormuzi szorost, melyen naponta 17 millió hordó kőolaj halad át. [46] Az USA leginkább az A2/AD buborékok leküzdésére koncentrál, emiatt több koncepció került kidolgozásra, illetve áll fejlesztés alatt. Elektronikai hadviselés vonatkozásában fontos az ‘Airborne Electronic Attack Platform (AEA)’, melynek részét képezik a Boeing EA-18G Growler és a Lockheed EC-130H Compass Call elektronikai hadviselési repülőgépek. [47]

Mint az amerikai fejlesztési elgondolásokból is látható, **az elektronikai hadviselésnek jelentős szerepet szánunk az A2/AD feladatokban.** Mind földi, mind légi EHV vonatkozásában történnek képességfejlesztések a nagyobb katonai potenciállal rendelkező államokban. Az új eszközök között egyre nagyobb távolságról üzemeltethető, a különböző radarok, műholdak, kommunikációs és vezetési eszközök és központok, korai előrejelző repülőgépek vagy drónok zavarására képes technikák találhatók, akár földi telepítésű, akár repülőre függeszthető konténerekbe vagy repülőgépbe beépített változatban. [41]

### **1.3. Az elektronikai hadviselés tervezési folyamata a művelettervezési módszerek változásainak tükrében**

Mielőtt részletesen bemutatnám és elemezném az EHV alkalmazásának tervezését, az EHV fogalmainak és felosztásának változásait, néhány szót kell ejtenem az azokat befolyásoló, a művelettervezéssel kapcsolatos eljárásokban történt változásokról.

**A korábban alkalmazott művelettervezési eljárások megváltoztak, a célkitűzés alapú megközelítést felváltotta a hatásalapú művelettervezés,** mellyel a „*katonai tevékenységek olyan hatásokat, illetve a rendszerben olyan változást idéznek elő, melyek az adott célkitűzés elérését biztosítják*”. [48; 134. o.] A műveletek hatásalapú megközelítését<sup>31</sup> azonban később felváltotta az átfogó megközelítés alapú művelettervezés, úgy hogy a hatásalapú megközelítés fogalma és módszere is érvényben maradt. [48]

Napjainkban alkalmazott művelettervezés alapját összhaderőnemi szinten az „Átfogó művelettervezési direktívában”<sup>32</sup> lefektetett eljárásrend képezi, amely az MH Törzsszolgálati szakutasításban is kialakításra került. **A tervezés fő eleme az összhaderőnemi művelettervező csoport (a továbbiakban: ÖMTCS<sup>33</sup>), amely alapvetően hadművelleti tervezőkből és a haderőnemek, fegyvernemek és szakcsapatok funkcionális szakértőiből áll.** Felállításra kerül több más munkacsoport is (pl. célkezelő, hatáselemző, információs

<sup>31</sup> Effects Based Approach to Operations, EBAO

<sup>32</sup> Comprehensive Operations Planning Directive, COPD

<sup>33</sup> Joint Operational Planning Group, JOPG

műveletek<sup>34</sup>, stb.), melyek a tervezés során rendkívül szorosan együtt dolgoznak. Az ÖMTCS részét képezik a kék, piros és zöld tervezőcsoportok. A kék tervezőcsoportok száma a lehetséges cselekvési változatok számától függ, amelyek a parancsnoki útmutatóban kerülnek meghatározásra. A kék tervezőcsoportok feladata a saját és baráti erők helyzetének elemzése, feladatuk tervezése egy-egy kijelölt cselekvési változat érdekében. A piros tervezőcsoport feladatai között szerepelnek a szemben álló fél helyzetének elemzése, lehetséges cselekvési változatainak kidolgozása, helyzetértékelő vázlat, felderítési terv és céllisták elkészítése. A zöld tervezőcsoport végzi a nem katonai szereplők helyzetének elemzését. [49]

**Alapvetés az, hogy az elektronikai hadviselési szakértőknek a fenti tervezőcsoportok munkájában folyamatosan részt kell venniük.** Az elektronikai hadviselési tevékenység alkalmazásra kerülhet például az információs műveletek vagy a célmeghatározás/céltervezés támogatása érdekében. Ahhoz, hogy megfelelően koordinált legyen minden szinten és minden időben, a különböző munkacsoportok számára szükséges javaslatokat az elektronikai helyzetértékelés eredményét felhasználva kell megtenni. Az elektronikai hadviselési tevékenység hatását folyamatosan figyelemmel kell kísérni és a munkacsoportok tevékenysége szerint a szükséges módosításokat meg kell tenni. Célmeghatározás/céltervezés esetében lehetséges például az, hogy az elektronikai zavarás hatástalansága vagy egyéb okok miatt az adott cél tűzérési eszközzel történő pusztítását rendelik el. Egy másik lehetséges változás például az is, hogy az összhaderőnemi korlátozott frekvenciák jegyzékén<sup>35</sup> szereplő frekvencia már nem szolgáltat érdemi információt az elektronikai támogatás vagy a rádióelektronikai felderítés (SIGINT<sup>36</sup>) részére és a harcászati-hadműveleti helyzet módosulása miatt annak zavarását határozzák meg. Ezen példákban látható, hogy **a megalakított elektronikai hadviselési elemnek már a tervezés kezdeti fázisában meg kell kezdenie a tevékenységét és azt a művelet teljes időszakában fenn kell tartania.** [30]

*„Az elektronikai hadviselés eredményes végrehajtása érdekében el kell készíteni az elektronikai helyzetértékelést, az ÖMTCS kék tervezőcsoportjai által készített cselekvési változatokba be kell építeni az elektronikai hadviselési válaszlépéseket. A kék tervezőcsoportok által kidolgozott saját cselekvési változatok kidolgozását a parancsnoknak*

<sup>34</sup> Information Operations, InfoOps

<sup>35</sup> Joint Restricted Frequency List, JRFL.

<sup>36</sup> Az angol terminológiából átvett SIGINT mozaikszó (Signal Intelligence, rádióelektronikai felderítés) kettő területből tevődik össze, ezek a COMINT (Communication Intelligence, kommunikációs felderítés) és az ELINT (Electronic Intelligence, nem-kommunikációs felderítés). A SIGINT megnevezést akkor használjuk, amikor nem szükséges a két terület megkülönböztetése vagy a kettő szakterületről együttesen beszélünk. [50]



*történő jelentés követi. Amennyiben szükséges, előzetes intézkedéseket kell kiadni. A parancsnoki döntés meghozatala után kezdődik hadműveleti terv/parancs elkészítése, melynek egyik melléklete az elektronikai hadviselési melléklet.”* [30; 69. o.] Természetesen a kék tervezőcsoportokkal párhuzamosan dolgozik a piros tervezőcsoport is, annak érdekében, hogy a kidolgozott piros cselekvési változattal az időszakos egyeztetések/helyzetjelentések során hatékony támogatást nyújthasson a JOPG számára. **Mindenképpen törekedni kell arra, hogy az elektronikai hadviselési melléklet jól értelmezhető, az adott műveleti környezetre jellemző értékelést tartalmazzon**, ne pedig az elektronikai hadviselés doktrína másolata legyen.

Figyelembe kell venni azt is, hogy azon haderőknél, ahol a haderőnemi parancsnokságok felállításra kerültek, ott az együttműködő tervezés<sup>37</sup> elveinek megfelelően a haderőnemek szintjén is folyik a tervezés. A komponens parancsnokságoknál felállításra kerülő tervezőcsoportok a szárazföldi tervezőcsoport<sup>38</sup>, a légierő tervezőcsoport<sup>39</sup>, illetve a különleges műveleti tervezőcsoport<sup>40</sup>. Mivel a haderőnemi komponensek a végrehajtó katonai szervezetekkel közvetlen kapcsolatban vannak, elgondolásaik/terveik sokkal részletesebben fogják tartalmazni a tervezett feladatokat, egyre jobban közelítve az elektronikai hadviselés vonatkozásában a funkciók alkalmazásához.

Mindenképpen elemezni kell a folyó műveleteket vezető hadműveleti központ<sup>41</sup> feladatrendszerét is, melyben az elektronikai hadviselés szakértőjének időszakos/állandó jelenlétét biztosítani kell, annak érdekében, hogy a különböző műveletek során az elektronikai hadviselés mindhárom funkciójának területei a szakmai elveknek megfelelően kerüljenek alkalmazásra, illetve a veszélyjelzés megfelelően kiadásra kerüljön.

A művelettervezésben és vezetésben bekövetkezett változások természetesen kihatással voltak az elektronikai hadviselés alkalmazásának tervezésére is. Az MH elektronikai hadviselésének doktrínális alapját a NATO dokumentumai képezik, melyek közül a legfontosabbak:

- az MC 64/11 NATO elektronikai hadviselési irányelvek<sup>42</sup>;
- az AJP–3.6 Szövetséges összhaderőnemi elektronikai hadviselési doktrína<sup>43</sup>;

---

<sup>37</sup> Collaborative planning

<sup>38</sup> Land Operational Planning Group, LOPG

<sup>39</sup> Air Operational Planning Group, AOPG

<sup>40</sup> Special Operational Planning Group, SOPG

<sup>41</sup> Joint Operational Centre, JOC

<sup>42</sup> NATO Electronic Warfare Policy (NATO Unclassified, letölthető a NATO Standardization Office honlapjáról kormányzati email címmel történő regisztrációt követően.)

- a STANAG 6010 (EDITION 3) – Elektronikai hadviselés a szárazföldi műveletekben<sup>44</sup> (ATP-3.6.2).
- a STANAG 3873 (EDITION 6) – Elektronikai hadviselés a légi műveletekben<sup>45</sup> (ATP-3.6.3).

Az MH Összhaderőnemi Elektronikai Hadviselés doktrínájának 2015-ben kiadott második kiadása – melynek szerkesztésében én is részt vettem – már harmonizál a hadviselésben bekövetkezett változásokkal (pl. hatásalapú műveletek megjelenése, az elektronikai hadviselés fogalmának és felosztásának változása).

A doktrína második kiadása alapján **az elektronikai hadviselés „olyan hatás-alapú katonai tevékenységek/műveletek összessége, amelyek elektromágneses környezetben, az elektromágneses energia tudatos használatával biztosítják az elektromágneses műveletek részeként végrehajtott támadó és védelmi jellegű hatások/célok elérését.”** [51]

A doktrína első – hosszú ideig alkalmazott – kiadásában megfogalmazottak szerint az *„elektronikai hadviselés azon katonai tevékenység, amely az elektromágneses energiát felhasználva meghatározza, felderíti, csökkenti vagy megakadályozza a frekvenciaspektrum ellenség részéről történő használatát és biztosítja annak a saját csapatok általi hatékony alkalmazását.”* [52] Egy időben nagyobb lépést visszalépve a Frunze Katonai Akadémia megfogalmazásához, a *„rádióelektronikai harc magában foglalja a speciális rádióelektronikai technika alkalmazását, azokat a technikai és taktikai fogásokat, amelyek az ellenségnél lévő rádióelektronikai rendszerek, csapatvezetési eszközök és fegyverek irányítását szolgáló berendezések felfedését szolgálják, - továbbá ezek munkájának zavarását, rádió- és rádiótechnikai felderítésük elleni ellentevékenységet, valamint a saját rádióelektronikai rendszerek megbízható üzemelésének biztosítását az ellenséges rádió ellentevékenység feltételei mellett.”* [53] **A fenti fogalmakat összehasonlítva látható, hogy a jelenleg érvényben lévő fogalom a korábbiakhoz képest már nemcsak a feladatokat tartalmazza, hanem utal azok végrehajtásának módjára, a hatás-alapú tevékenységre is.**

---

<sup>43</sup> Allied Joint Electronic Warfare Doctrine (NATO Restricted minősítésű, korlátozottan hozzáférhető.)

<sup>44</sup> Electronic Warfare in the land battle (NATO Unclassified, letölthető a NATO Standardization Office honlapjáról kormányzati email címmel történő regisztrációt követően.)

<sup>45</sup> Electronic Warfare in air operations (NATO Unclassified, letölthető a NATO Standardization Office honlapjáról kormányzati email címmel történő regisztrációt követően.)

Az elektronikai hadviselés területei a doktrína második kiadása alapján:

• elektronikai támadás<sup>46</sup>, a korábban alkalmazott elektronikai ellentevékenység helyett;

- elektronikai védelem<sup>47</sup>,
- elektronikai megfigyelés<sup>48</sup>, a korábban alkalmazott elektronikai támogatás helyett.

A funkciói pedig az alábbiak:

- elektronikai támogatási funkció;<sup>49</sup>
- elektronikai ellentevékenységi funkció;<sup>50</sup>
- elektronikai védelmi funkció.<sup>51</sup>

Az elektronikai hadviselés **terület és funkció szerinti szétválasztása biztosítja** azt, hogy a stratégiai szinten meghatározható legyen **a politikai/stratégiai célkitűzés** eléréséhez szükséges elektronikai hadviselési hatás, illetve a stratégiai szint útmutatása alapján a **hadműveleti szinten** kiválasztható legyen az alkalmazandó funkció, **a harcászati szinten** pedig a funkcióhoz tartozó eszköz.

Ahhoz, hogy az EHV eszközök képességének alkalmazhatóságát megértsük, mindenképpen szükségesnek látom az elektronikai hadviselés funkciói alkalmazásának elemzését. Az első elemzett funkció az elektronikai támogatási funkció, *„amely az ellenség helyzetére vonatkozó tájékozottság és a fenyegetés késedelem nélküli felismerése céljából magában foglalja az elektromágneses kisugárzások kutatását, felfedését és azonosítását, valamint a kisugárzók helyének meghatározását.”*[51; 2-4]

Az elektronikai támogatás – annak passzív jellege miatt – békeidőben is végezhető, mind a konfliktus kialakulása, mind a helyzet eszkalálódása során alkalmazhatjuk a szembenálló fél tevékenységének nyomon követése, felderítési információk megerősítése, az elektronikai ellentevékenység megtervezése, valamint az önvédelmi tevékenységek megszervezése érdekében. [51]

Az elektronikai ellentevékenységi funkcióval megakadályozzuk, vagy korlátozzuk az elektromágneses spektrum ellenség által történő hatékony használatát. Területei az elektronikai zavarás<sup>52</sup>, az elektronikai megtévesztés<sup>53</sup> és az elektronikai pusztítás<sup>54</sup>. „Az

---

<sup>46</sup> Electronic Attack - EA

<sup>47</sup> Electronic Defence - ED

<sup>48</sup> Electronic Surveillance - ES

<sup>49</sup> Electronic Support Measures ESM

<sup>50</sup> Electronic Counter Measures ECM

<sup>51</sup> Electronic Protective Measures EPM

<sup>52</sup> Electronic Jamming - EJ

*elektronikai zavarás az elektromágneses energia szándékos kisugárzása, visszasugárzása vagy visszatükrözése azzal a céllal, hogy korlátozza vagy megakadályozza az ellenség által használt elektronikai eszközök, berendezések és rendszerek rendeltetésszerű működését.” [51; 2-6]* Az elektronikai megtévesztéssel célunk az, hogy elektromágneses energia szándékos kisugárzásával, átalakításával, visszasugárzásával, elnyelésével, vagy visszatükrözésével megtévezzük, félrevezessük és összezavarjuk a szembenálló felet. Főbb módszerei a szimulációs<sup>55</sup>, a manipulációs<sup>56</sup> és az imitációs elektronikai megtévesztés<sup>57</sup>. Az elektronikai pusztítás az ellenség elektromágneses spektrumhasználaton alapuló rendszereinek elektromágneses és egyéb irányított energiákkal, vagy önrávezetésű fegyverekkel történő időleges, vagy tartós rombolása. [51]

*Az elektronikai védelmi funkció biztosítja az „elektromágneses spektrum saját részről történő hatékony használatát az ellenség elektronikai támogató és ellentevékenysége, valamint a saját csapatok által okozott nem szándékos (kölcsonös) rádiózavarok előfordulása ellenére.” [51; 2-8]*

Az MH ÖEHVD segít választ adni a szárazföldi és a légierő csapatai elektronikai hadviselési tevékenységének különböző környezetben történő alkalmazhatóságának további vizsgálatához is. Fontos az, hogy a szárazföld és a légierő elektronikai hadviselési képességének alkalmazási lehetőségei és időtartama jelentősen eltérnek egymástól. A légierő eszközein alapuló elektronikai hadviselési tevékenységek koncentráltabb, egy adott területre vagy műveletre fókuszáló hatást biztosíthatnak, azonban alkalmazási idejük rövidebb, mint a földi eszközöké. A szárazföldi erők alkalmazhatnak stacioner vagy mobil elektronikai hadviselési eszközöket, különböző méretben (hordozható, gépjárműbe épített, stb.) és képességgel. A légierő esetében a különböző légi eszközök hozzáadott (pl. függesztett elektronikai támogató vagy zavaró konténer, a repülőeszköz rendszerébe integrált rendszerek, stb.) vagy beépített, önvédelmi elektronikai hadviselési rendszerei alkotják a támogatás alapját. A harcászati repülő eszközök önvédelmi célú elektronikai hadviselési rendszerének elemei a fenyegetettség alrendszer és az ellentevékenység alrendszer. [51] *„A fenyegetettség alrendszer rendeltetése az elektromágneses spektrum szemben álló fél részéről történő aktív használatának észlelése, a fenyegetés azonosítása, a veszély jelzése (riasztás) és az*

---

<sup>53</sup> Electronic Deception - ED

<sup>54</sup> Electronic Neutralisation - EN

<sup>55</sup> Simulative Electronic Deception - SED

<sup>56</sup> Manipulative Electronic Deception - MED

<sup>57</sup> Imitative Electronic Deception - IED

*ellentevékenységi alrendszerek működtetésének kezdeményezése. Az ellentevékenység alrendszerek a fenyegetettség alrendszerek sávjában felfedett fenyegetésekkel szemben nyújtanak alternatívát - a megfelelő manőverek mellett - az aktív vagy a passzív ellentevékenységre.[51; 3-4]”*

A két haderőnem eszközei nemcsak a fent említett rendszerek üzemeltetésével nyújthatnak segítséget, hanem kijuttathatnak például **egyszeri felhasználású** – akár **elektronikai támogató**, akár **elektronikai zavaró funkcióval rendelkező** – elektronikai hadviselési eszközöket is egy adott területre. Ez történhet pilóta által vezetett vagy pilóta nélküli repülőgépekről, illetve tüzérségi eszközök alkalmazásával.

Fontos és mindenképpen figyelembe kell venni, hogy hagyományos hadviselés esetén az elektronikai hadviselési eszközök alkalmazása nemcsak a szembenálló fél egyes eszközei, hanem komplex képességei ellen is irányulhat a megfelelő önvédelmi és támogató rendszerek megléte esetén. Ezek között szerepelhet többek között az integrált felderítés, a csapásmérések, a kommunikációs és vezetési rendszerek akadályozása, bénítása vagy megtevesztése. [54]

Sok cikkben foglalkoznak a korábban már említett rádióelektronikai felderítés (SIGINT<sup>58</sup>) és az elektronikai megfigyelés (korábban elektronikai támogatás) közötti hasonlósággal és különbséggel, sok esetben azonban hibásan említik és össze is keverik azokat. A SIGINT és az elektronikai megfigyelés végezhető ugyanazon eszközökkel is, azonban a megszerzett információk felhasználásának más a célja. Az elektronikai megfigyelés harci információkat szolgáltat például az elektronikai támadáshoz, tüzérségi tűzhöz, légicsapásokhoz, míg a SIGINT felderítési információkat biztosít az összefegyvernemi törzs részére a parancsnoki döntéstámogatás érdekében. [55] Itt jegyzem meg azt is, hogy elérhetőek olyan szakirodalmak is, ahol a SIGINT szakterület felbontásához hasonlóan (COMINT, kommunikációs felderítés és ELINT, nem-kommunikációs felderítés) az elektronikai megfigyelést is kettő területre, kommunikációs illetve radar elektronikai támogatási területekre osztják fel. [25; 409. old.]

A korábbi bekezdésekben említettem, hogy az elektronikai hadviselési szakértőknek a tervezés lehető legkorábbi időszakában be kell kapcsolódnia a feladatba. **Figyelembe kell venni azt is, hogy az elektronikai támogató tevékenység – annak passzív jellege miatt –**

---

<sup>58</sup> Rádióelektronikai felderítés, Signal Intelligence

**békeidőben is végezhető/végzendő feladat, melynek tervezése/koordinálása így állandó feladatot jelent.** Ennek érdekében indokoltnak látom egy **Elektronikai Hadviselési Koordinációs Részleg<sup>59</sup>** felállítását és állandó jelleggel történő működtetését **összhaderőnemi/hadműveleti szinten.**

#### **1.4. Elektronikai hadviselési vonatkozású fejlesztések megvalósulása**

Az elektronikai hadviselési eszközök fejlődése – más elektronikai eszközökhöz hasonlóan – folyamatos. A fejlesztéseknél természetesen figyelemmel kell követni a céltechnikák, így a kommunikációs és nem-kommunikációs eszközök és rendszerek fejlődését, valamint az alkalmazott eljárások változásait is. A **korábbi**, híradó vagy rádiótechnikai eszközök ellen folytatott **elektronikai hadviselési feladatok kibővültek, megjelent a globális helymeghatározó eszközök vagy a műholdak ellen alkalmazható elektronikai zavarás** képessége is. A fejlődés egyik lépcsője az volt, hogy az elektronikai hadviselési eszközökben is megjelent az információtechnológia. A szoftverrádiós technológia felhasználása jelen van a nagymennyiségű adat feldolgozásában, értékelésében, továbbításában, szükség esetén a működési jellemzők megváltoztatásában. Az elektronikai hadviselésben bekövetkezett változásokat azonban nem szabad egyértelműen csak a technikai fejlődés számlájára írni, mindenképpen fontos szempont a biztonságpolitikai környezet változása, a háború természetében bekövetkezett változások, illetve a szembenálló fél hadviselési elveinek módosulása vagy fejlődése.

##### **1.4.1. Elektronikai hadviselési vonatkozású fejlesztések az egyes haderőknél**

Érdekes és mindenképpen átgondolandó a NATO Szövetséges Legfelsőbb Átalakítási Parancsnokság<sup>60</sup> azon megállapítása, miszerint **a NATO** közelmúlt műveleteiben birtokolt jelentős **technikai fölénye** a jövőben a lehetséges ellenfelek által végrehajtott – **a relatíve olcsó és egyszerű technológiákat magukban foglaló – innovációk miatt erodálódik.** [56; iii old.] Ugyanezen dokumentumban az elektronikai hadviselés egyik területét, az elektronikai megfigyelést is kiemelik, mint kiemelten fontos területet, hiszen az általa biztosított adatok fuzionálásra kerülnek más szenzorok adataival. Napjaink kisugárzó eszközei rövidebb kisugárzási idővel, kis valószínűséggel felderíthető adásmódokkal<sup>61</sup>, passzív vevőkkel üzemelnek, melyek – mintegy macska-egér játék – magukkal hozták az elektronikai

<sup>59</sup> Electronic Warfare Coordination Cell - EWCC

<sup>60</sup> NATO Supreme Allied Commander Transformation, NATO SACT

<sup>61</sup> Low Probability of Intercept (LPI)

megfigyelés szükségszerű fejlődését, ebbe beleértve a modern antenna technológiát, az informatika és a kognitív rendszerek nyújtotta lehetőségek felhasználását. [56; 49. old.]

A modern **szárazföldi parancsnokok egyre növekvő mértékben függenek az „információs kor” kommunikációs és információs rendszereitől**, a különböző hálózatoktól és szenzoroktól. Fontos figyelembe venni, hogy a kommunikációs és információs rendszerek jelentős változást generálhatnak a harc megvívásában, azonban a meglévő elektronikai rendszerek megbízhatóságát csökkentik a szemben álló fél elektronikai hadviselési eszközei által létrehozott hatások. [57] A fenti eszközök által biztosított lehetőségek, akkor használhatók ki – az elektronikai hadviselés erősokszorozó szerepét megerősítve – ha az információ gyors feldolgozása automatizált adatfeldolgozó és vezetési rendszerek felhasználásával biztosított. [58]

Az elektronikai hadviselés fontossága nem lehet kérdés, a NATO 1999-ben elfogadott Stratégiai Koncepciójában is kiemelték az EHV-t, a felderítés, a stratégiai légiszállítás, illetve a vezetési elemek és az alegységek telepíthetősége mellett. [59] Ezt támasztja alá az is, hogy a Szövetséges Legfelsőbb Átalakítási Parancsnokság parancsnoka is megemlíti a 2015 augusztusában kiadott elgondolásában, hogy a jövőben **a NATO és a nemzeti objektumok kiber- és elektronikai hadviselési támadások célpontjai lehetnek**. A célpontok között azonban nemcsak katonai, hanem polgári, például energiaellátó objektumok is szerepelhetnek majd. [60]

Fontos azt is mindenképpen megemlíteni, hogy **a különböző technikai eszközök és a kiépíthető képességek kialakítása és fenntartása, valamint a szükséges technikai fejlesztések végrehajtása jelentős humán, technológiai, valamint pénzügyi erőforrást igényel**, amely nem áll rendelkezésre valamennyi országban, illetve a többféle szakterületen végrehajtott feladatok szétforgácsolják az adott ország részére rendelkezésre álló erőforrásokat.

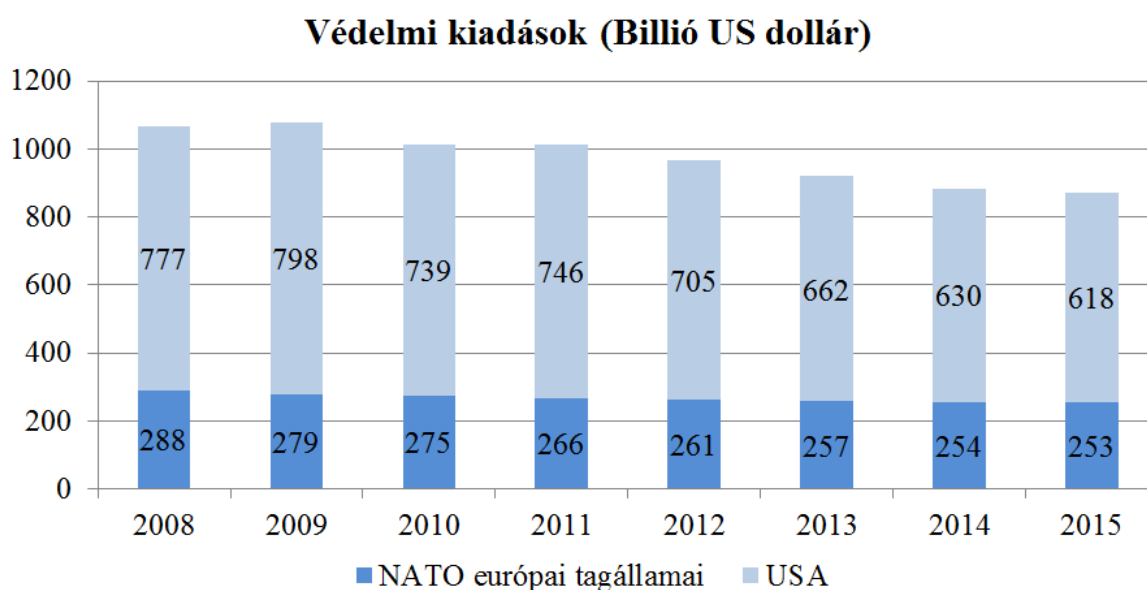
Ennek érdekében kezdődött meg a NATO „Smart Defence”<sup>62</sup> elnevezésű programja, amelynek célja a szövetség tagjai által kialakított képességek, fejlesztések és eredmények megosztása. Az elgondolás főbb alapkövei a prioritizálás, specializálás és az együttműködés. A fontosabb területek között megtaláljuk a precíziós fegyverek alkalmazását, a kibervédelmet, a ballisztikus rakéták elleni védelmet és az összhaderőnemi hírszerzési, megfigyelési és felderítési rendszert. Természetesen számos más program is folyamatban van, ezek közül

---

<sup>62</sup> Okos védelem

megemlíteném a felderítés és elektronikai fejlesztések vonatkozásában is kiemelkedő Szövetségi Felszínellenőrzési Rendszer (Alliance Ground Surveillance – AGS) programot. [61]

A védelmi kiadások bemutatása érdekében a NATO egyik kiadványából emelek át adatokat, amely a haderőre költött összegeket mutatja be éves bontásban az Amerikai Egyesült Államok – európai NATO tagállamok viszonylatában. Az 1.1. ábrán látható, hogy az USA az évek folyamán csökkenő, de az európai NATO tagállamok összegzett kiadásához képest mégis jelentősen nagyobb összeget fordít hadikiadásokra. [62]



1.1. ábra: NATO államok védelmi kiadásai. [62]

Arra, hogy fenti összegekből a különböző szakterületek milyen bontásban részesülnek, nehéz pontos információt találni. Az elektronikai hadviselés vonatkozásában fontos és érdekes, hogy az USA az 1956-57-es pénzügyi évben 400 millió dollárt, 1983-ban 5,2 milliárd dollárt fordított ilyen jellegű kiadásokra. [63] 2012-ben az USA 2013. évi védelmi kiadásainak tervezett tételei között az elektronikai hadviselési és az elektro-optikai ellentevékenységre a korábbi évekhez képest is nagyobb költségvetés keret, 4,95 milliárd dollár szerepelt. A fenti pénzügyi keret egy része 12 db U.S. Navy Boeing EA-18G Growler<sup>63</sup> elektronikai hadviselési feladatokra képes repülőgép vásárlására került lebiztosításra. Egy

<sup>63</sup> A repülőgéptípus képességei között szerepel a szemben álló fél légvédelmének elnyomása, radarok zavarása, valamint aktív elektromágneses kisugárzással működő légvédelmi radarok rombolása Raytheon AGM-88 (High-speed Anti-Radiation Missile, HARM) típusú rakétával



másik tétel a Joint IED Defeat Organization (JIEDDO) szervezet „Attack the network”<sup>64</sup> projektjének támogatása, melynek célja az improvizált robbanóeszközök előállító hálózatok (pénzügyi támogatók, készítők és kiképzők, valamint a tevékenységüket támogató infrastruktúra) rombolása felderítési, targeting, biometrián alapuló azonosítási, illetve helyszínelő képességek biztosításával. [64] A 2014. évi tervekben is kiemelt prioritásként kezelték az elektronikai hadviselést úgy, hogy a tudomány és technológia alprogramon belül 500 millió dollárt terveztek be az elektronikai hadviselés fejlesztésére. [65]

A fejlesztésekre az USA hadseregének nagy szüksége van, mivel katonái a világ számos pontján vesznek részt különböző fegyveres konfliktusban. Irakban és Afganisztánban az EHV egyik területe, az elektronikai ellentevékenység kerül alkalmazásra a rádió-távírányítású improvizált robbanóeszközök elleni harcban. A US Army több, mint 32.000 rövid hatótávolságú zavaróeszközzel rendelkezik a különböző eszközeiben, melyet **a különböző fejlesztések révén hálózatba terveznek kötni és egy rendszerként üzemeltetni.** A jelenlegi tervek szerint a kiépített rendszer 2023-tól kezd üzemelni és a teljes műveleti képességet 2027-ig érik el. [66]

A fenti bekezdésekben szereplő koncepcionális elgondolások mellett az USA vonatkozásában konkrét eszközök, rendszerek terveiről is érhetünk el leírásokat. Az 1990-as évek végéig az Egyesült Államok szárazföldi hadseregének felderítő és elektronikai hadviselési képességét az Intelligence and Electronic Warfare Common Sensor (IEWCS) rendszerrel tervezték biztosítani. A fejlesztési célkitűzések alapján a rendszerek már szélesebb frekvenciatartományban (COMINT<sup>65</sup>: MF-SHF /300 kHz - 30 GHz/, ELINT<sup>66</sup>: UHF-EHF /300 MHz - 300 GHz/) dolgoztak volna. A tervezett rendszerek:

- AN/MLQ-38, Ground-Based Common Sensor-Heavy (GBCS-H);
- AN/MLQ-39, Ground-Based Common Sensor-Light (GBCS-L);
- AN/ALQ-151(V)3 Advanced QUICKFIX (AQF);
- Mobile Electronic Warfare Support System - MEWSS.

*„A fenti rendszerek főbb feladatai az alábbiak voltak:*

- a kisugárzó objektumok helyének pontos meghatározása;*
- külön adatcsatorna fenntartása a tűzérségi rendszerek felé;*
- a vett jelek gyors feldolgozása, a célok kiválasztása, jelentése;*

<sup>64</sup> „Támadd a hálózatot!”, a szerző saját fordítása

<sup>65</sup> Kommunikációs felderítés, Communication Intelligence, COMINT

<sup>66</sup> Nem-kommunikációs felderítés, Electronic Intelligence, ELINT

- **felderítési adatok korrelációja;**
- **intelligens zavarás végrehajtása**, amely csökkenti a nemkívánatos interferenciát, de a zavarandó rendszerre optimalizálva nagyobb hatékonyságú;
- **modern modulációs módok és az úgynevezett nehezen felderíthető** (Low Probability of Intercept – LPI) **jelek elleni tevékenység;**
- **a továbbfejlesztés lehetőségének egyszerűsítése;**
- **interoperabilitás** biztosítása a felderítési adatfúzió, a tűztámogatáson és az IEW rendszereken keresztül.” [24; 5. sz. melléklet]

A fenti IEWCS rendszer azonban nem készült el, a programot módosították és a PROPHET (Próféta) elnevezésű programban folytatták. A PROPHET harcászati-műszaki követelményeit az amerikai hadsereg Kiképzési és Doktrínakidolgozó Parancsnoksága<sup>67</sup> 1999. április 26-án hagyta jóvá.

Feladatai:

- a harcterület elektronikus feltérképezése;
- elektronikai csapás mérése;
- navigációs hadviselés;
- pontos helymeghatározással támogatni a Targeting folyamatot;
- a kiválasztott jelek feldolgozása. [67]

A rendszer három fő egységre tagolható:

- PROPHET légi elem (PROPHET Air);
- PROPHET földi állomás (PROPHET Ground);
- PROPHET vezetési pont (PROPHET Control). [24; 6. sz. melléklet]

A NATO-n kívüli államok közül leginkább Oroszország és Kína az, amelyeket meg kell említeni, amikor elektronikai hadviselési képesség vonatkozásában jelentős államokról beszélünk. Robert Work amerikai helyettes védelmi miniszter egy konferencián kijelentette, hogy bár az USA jelentősebb képességgel rendelkezik az elektromágneses spektrum vonatkozásában, mint a lehetséges ellenfelek, de **más államok is jelentős fejlesztéseket hajtanak végre.**<sup>68</sup> [68]

Oroszország meglévő elektronikai hadviselési képességét az USA és Ukrajna hadereje a gyakorlatban is megtapasztalta, kiemelten a már említett ukrajnai konfliktus során. Több új

<sup>67</sup> U.S. Army Training and Doctrine Command, TRADOC

<sup>68</sup> „United States still had greater capabilities in the electromagnetic spectrum than potential adversaries, but other countries were investing heavily.” A szerző fordítása.

elektronikai hadviselési vonatkozású orosz fejlesztésről láthatunk képet a nyílt forrásokban, legyen az a Khibiny szárnyvégi zavarókonténer, vagy a Krasukha 2 és 4, Rychag és Infauna, a Murmansk-BN vagy a Leyer-3. [69] Oroszország az EHV eszközök valós alkalmazása mellett további fejlesztési tervekkel is rendelkezik, irányított energiájú fegyvereket fejlesztenek, melyeket repülőgépeken, rakétákon és műholdakon alkalmazott elektronikai irányító és navigációs rendszerek ellen terveznek alkalmazni a jövőben. [70] Fontos azt is megjegyezni, hogy nemcsak az elektronikai hadviselési képességet fejlesztik, hanem a saját radar és kommunikációs berendezéseiknél nagy hangsúlyt fektetnek az **elektronikai zavarás elleni védelmi megoldások alkalmazására**. Ennek egyik példája az orosz légvédelem alapját képező 64L6 „Gamma-SZ1” háromdimenziós centiméteres hullámsávú, felderítő rádiólokátor, melyben a passzív és aktív zavarok elnyomása automatikusan történik. Nagyfokú zavarvédetségét többek között kisteljesítményű, ám széles kisugárzott impulzusok vagy több üzemmód használata biztosítja. [71]

Kína esetében kevés elérhető információ áll a rendelkezésünkre, azonban mindenképpen meg kell említeni a Kínai Népi Felszabadító Hadsereg<sup>69</sup> újonnan kialakított Stratégiai Támogató Egységét<sup>70</sup> (a továbbiakban SSF). Az SSF feladatai között szerepel a felderítés, kommunikáció biztosítása, a technikai felderítés a kiber- és elektronikai hadviseléssel együtt, így várhatóan valóban képes lesz az SSF az információs dominancia kialakítására. A kiberegység hackerekből áll, akik egyaránt foglalkoznak védelemmel és támadással, az **elektronikai hadviselési erők pedig a radar és kommunikációs eszközök zavarására és rombolására koncentrálnak**. [72] Lényeges dokumentum Kína kiberhadviselési doktrínája is, mely szerint 2050-re eléri a globális elektronikai dominanciát. [73] Természetesen már jelenleg is rendelkeznek különböző eszközökkel, így például a Shaanxi Y-8 szállítórepülőgép különböző változataival képesek elektronikai felderítő vagy elektronikai zavaró feladatok végrehajtására, illetve információs hadviselési vagy lélektani műveletek kivitelezésére. Jelenleg az F-16 Wild Weasel<sup>71</sup> kínai verzióját építik. [74] Kína elektronikai hadviselési képességével kapcsolatban meg kell említenünk még egy fogalmat, mégpedig a **Hálózatalapú elektronikai hadviselést**<sup>72</sup>, amely az információs hadviselésre,

<sup>69</sup> Zhōngguó Rénmín Jiěfàng Jūn, angol megnevezéssel Chinese People's Liberation Army (PLA)

<sup>70</sup> Strategic Support Force, SSF

<sup>71</sup> Wild Weasel az US Air Force koncepciója radar-kereső fejekkel ellátott rakéták hordozására alkalmas repülőgépre, a különböző légtérelenőrző, légvédelmi radarok ellen. Korábban az F-4 változatait, jelenleg az F-16 típust használják erre a célra.

<sup>72</sup> Integrated Network-Electronic Warfare (INEW), a szerző fordítása.

valamint a hadszíntereken fellépő, a műveletek tervezéséhez és végrehajtásához szükséges információs igényre utal. [75]

Természetesen a kisebb NATO és nem NATO államok is rendelkeznek elektronikai felderítő vagy elektronikai zavaró képességgel, azonban a rendelkezésre álló eszközök mennyisége eltörpül a korábban említett államok által birtokolt eszközök mennyisége mellett. Az SGS-2000 TOR elektronikai ellentevékenységi rendszert a német Daimler Chrysler Aerospace vállalat gyártotta a norvég hadsereg számára. [24; 8. sz. melléklet] Franciaország és Olaszország 2014-ben SIGINT hajókat telepített a Fekete-tengerre, a Krím szigeten alkalmazott mobil és rádió kommunikáció, valamint radartevékenység felderítésére. [76] Az Egyesült Királyság SIGINT repülőgépekkel támogatja az USA-t Szíriában. [77] Fontos azt is megemlíteni, hogy nemcsak az államok rendelkeznek elektronikai hadviselési képességgel, 2014-ben az USA egyik légicsapása egy EHV laktanyát és egy ISIS elektronikai zavaróállomást pusztított el Rakkában. [78]

Korábban már említettem a **kezelő állományt**, melynek **magas színvonalú képzettsége** a munkaállomások hatékony üzemeltetésében mindenképpen **alapvető kritérium**. Nagy hangsúlyt kell fektetni nemcsak az alapvető szakmai és az állomások üzemeltetéséhez szükséges ismeretek elsajátítására, hanem a változó eljárasmódok megismerésére is. Ezekre megfelelő lehetőség például a NATO által szervezett gyakorlatokon történő részvétel. Napjaink ilyen jellegű gyakorlatai a NEWFIP Ramstein Guard elnevezésű, többnemzeti elektronikai hadviselési gyakorlat, valamint a Unified Vision elnevezésű, összhaderőnemi felderítő rendszergyakorlat, amely 2014-ben például műholdak, repülőgépek, pilóta nélküli repülőgépek, hadihajó, földi érzékelők és humán felderítési elemek bevonásával került végrehajtásra. A NEWFIP Ramstein Guard gyakorlatba – melynek jelenleg én vagyok a szakmai fő szervezője – tapasztalatszerzés érdekében a légierő haderőnemhez tartozó magyar katonai szervezetek mellett az EHV század állománya is bevonásra került számos alkalommal. Fontos megemlíteni, hogy a NEWFIP gyakorlat az MH részére olyan komplex elektronikai hadviselési (zavarási) környezetet biztosít, melyet az MH önmagában nem képes létrehozni.

#### **1.4.2. Elektronikai hadviselés és a rádióelektronikai felderítés a Magyar Honvédségben**

Az MH elektronikai hadviselési és rádióelektronikai felderítő szervezeti elemeinek változásaiban az 1.1. fejezetben bemutatott biztonságpolitikai változások nagy szerepet játszottak.

##### **A legfontosabb hatások:**

- A biztonságpolitikai változások hatására végrehajtott **haderőreform** a korábbi időszakban kialakított szervezetek kiképzett **személyi állományának jelentős csökkenésével és nagy mennyiségű technikai eszköz kivonásával járt együtt.** Az 1995-1997 közötti időszakban az átalakítás célja a korábban 100 ezer fős haderő NATO-val közös feladatok végrehajtására képes, finanszírozható haderővé történő átalakítása volt. A feladatok legfontosabb irányelvei és feladatai a Magyar Honvédség közép- és hosszú távú átalakításáról szóló 88/1995. (VII. 6.) számú Országgyűlési határozatban kerültek meghatározásra. A haderő átalakítását ebben az időszakban a haderő létszámának csökkentése jelentette, 1995. január 15. és 1997. december 31. között az MH összlétszáma 98.566-ról 53.519-re csökkent, ami 46 %-os állománycsökkenést jelentett. A következő időszak fő feladatai a NATO csatlakozáshoz kapcsolódó feladatok végrehajtása volt, amely további létszámcsökkenést is magában foglalt. A változtatások során a szárazföldi csapatoknál megtörtént a lövészdandárok 2+1-es zászlóaljra és a 4 rajos szervezetre való átalakítása, a zászlóaljaknál az önjáró tűzerőegységek kialakítása és a harcjárművek részleges cseréje, valamint a szárazföldi és logisztikai csapatok szervezeteinél folytatódott a befogadó nemzeti támogatási képesség javítása. A légierő haderőnemnél repülő és harci helikopter ezredeinél megkezdődött a hadműveleti központok kialakítása, valamint megtörtént a légtérellenőrző ezred átalakítása radar szervezetté. [79]

- Az MH alaprendeltetéséből adódó **feladatai jelentősen megváltoztak, kiegészültek** például a különböző nemzetközi szövetségekhez történő csatlakozással együtt járó, a **szövetségek által** vezetett műveletekben **elvárt** szerepvállalásból fakadó **kötelezettségekkel.** Azzal, hogy Magyarország 1999-ben a NATO, majd 2004-ben az Európai Unió tagjává vált, olyan – főképpen a NATO tagságból eredően – katonai feladatokban, válságreakáló műveletekben kell szerepet vállalnia, mely a korábbi évtizedekre kevésbé volt jellemző. Az MH katonái ezekben a műveletekben a nem hagyományos hadviselés elvei alapján tevékenykednek, számos helyszínen voltak és vannak jelen, mint az EU vagy a NATO erőknél át/alárendelt alegységek. Szolgáltak és szolgálnak Irakban, a Balkáni hadszíntéren, Afganisztánban, Afrikában, csak a legveszélyesebbeket kiemelve. Ezen **műveleti területeken**

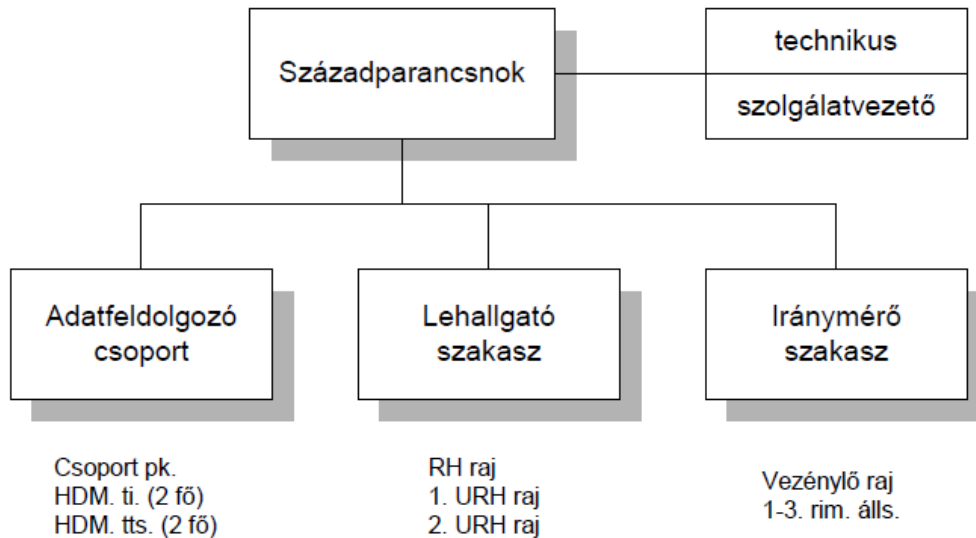
**az elektronikai hadviselés vagy rádióelektronikai felderítés eszközei is jelen voltak/vannak**, emiatt is fontos mindenképpen elemezni a különböző helyszíneken alkalmazott erők részére szükséges technikai erőforrásokat.

A következő részben a Magyar Honvédség korábbi és jelenlegi elektronikai hadviselési és rádióelektronikai felderítő szervezeteinek/elemeinek legfontosabb eseményeit mutatom be, külön kiemelve az MH érdekében történt fejlesztéseket.

A magyar rádiófelderítés története már az első világháborúban elkezdődött, melynek során lehallgatták a Monarchia és Olaszország közötti politikai válság során a nyílt olasz rádióforgalmat és az így megszerzett információkat fel is használták a döntéshozatal során. 1911-ben az olasz-török háború során lehallgatták a Róma és Tripoli közötti rádióközleményeket is. [80] Az első világháborúval kapcsolatban mindenképpen meg kell említenünk Pokorny Hermann nevét, aki az általa vezetett csoporttal mintegy 240 orosz táviratot hallgatott le és fejtett meg, az így **megszerzett információk segítségével** a támogatott osztrák-magyar és német erők **képesek voltak az előrenyomuló orosz csapatokat San Visztula területén megállítani**. 1915-ben ismét sikeresen hajtottak végre lehallgatási feladatot, melynek eredményeképpen az osztrák-magyar és német erők elfoglalták Breszt-Litovszk-ot 1915 augusztusában. [81]

A későbbi időszakban folyamatosak voltak a szervezeti változások, melyek végigkövették a szakma életét. Az **alegységek nemcsak** a különböző országok **gyakorlatainak lehallgatásában** vettek részt, **de éles műveleti feladatban is**, mivel a jugoszláviai események során a 2. Önálló Rádió- és Rádiótechnikai Felderítő Zászlóalj 1991. november 15-től - 1991. december 21-ig, majd 1991. január 9-től február 4-ig a déli határszakaszon került alkalmazásra. Ez a zászlóalj 1992. augusztus 1-jével szűnt meg, amikor a hadműveleti és a harcászati rádióelektronikai felderítés feladatrendszerbe beintegrálódott a Magyar Honvédség elektronikai-harc szervezeteinek feladatai közé. Az alakulat Szombathelyről Kiskunfélegyházára települt át, és a korábbi 63. Önálló Rádió- és Rádiótechnikai Zavarózászlóaljjal (Békéscsaba) együtt megalakította az 5. Kiskun Elektronikai-harc Ezredet. [82]

A harcászati rádiófelderítéssel kapcsolatban fontos esemény a Magyar Néphadsereg (a továbbiakban MN) első rádiófelderítő századának 1964. szeptember 1-jén történt megalakulása. A század szervezeti felépítése az 1.2. ábrán látható. [82; 110 o.]



1.2. ábra: Az MN első rádiófelderítő századának felépítése. [82; 111 o.]

A fenti rádiófelderítő század állományának bázisán további három század alakult meg 1965-ben, illetve még egy 1966-ban. A megalakításkor során átvett technikai eszközeik mellett 1971-ben rendszeresítésre kerültek a Mechanikai Laboratórium által gyártott technikai eszközök, melyek egy része napjainkban is megtalálható az MH 24. Bornemissza Gergely Felderítő Ezred Elektronikai Hadviselés Század eszközei között:

- RH: R–1250M vevő;
- URH: VU–21M vevő, UP–3MA panorámavevő;  
VU–32 M vevő, UP–3MB panorámavevő;
- RIM: IU–6M rádió-iránymérő;
- UAE–63 antennaerősítő. [82; 114 o.]

Mindenképpen meg kell említeni az 1974. december 16-án<sup>73</sup> Budaörsön megalakult **Rádióelektronikai Ellenőrző Központot (RELEK)** is, amely később Gödöllőre települt át. [83] A RELEK feladatai között szerepelt a **saját híradó rendszereink feletti ellenőrzési funkció** gyakorlása, illetve a **fejlesztési tevékenység támogatása**. [84] A híradó rendszerek vonatkozásában az elektromágneses kisugárzási rendszabályok betartásának ellenőrzését az Északi-középhegység, a Dunántúli-középhegység és az Alpokalja magaslataira telepített „Egérfogó” rendszerrel végezték. [85] 1990-ben 18, 91-ben 21, 92-ben 19, 93-ban 18, 94-ben 17 zavarkivizsgálást végeztek. Ez a szám nem tartalmazza a hiányos adatok miatt visszautasított zavarbejelentéseket. 22%-nál időközben megszűnt a zavarás, 40,7%-nál saját

<sup>73</sup> December 16. az Elektronikai Hadviselés Napja a Magyar Honvédségnél.

üzemeltetési fegyelmezetlenség vagy technikai meghibásodás okozta a zavarást, 12%-át pedig a szovjet Déli Hadseregcsoporthoz tartozó alakulatai okozták. [86]

A rádiófelderítő szervezetek mellett a korábbi évtizedekben megjelentek a kezdetben rádióelektronikai harc, illetve később elektronikai harc feladatkörrel rendelkező alegységek, például a Győrben történt megalakítása után hét évvel később MH 78. Gróf Pálffy Miklós Elektronikai-harc Századra átszervezett MN 78. Rádiózavaró Század [83], a pécsi 29. Elektronikai-harc Század, az egri 92. Elektronikai-harc Század. Később a fent említett századok is az 5. Kiskun Elektronikai-harc Ezredbe kerültek beintegrálásra. [87]

A Magyar Néphadsereg kötelékében, a Csapatrepülő Parancsnokság alárendeltségében 1983-ban, a 87. Szállító Helikopter Ezreden belül került kialakításra egy vegyes rádióelektronikai harc szakasz. [88] A technikai fejlődés hatására a szakasz 1987-ben zavaró századdá alakult, tevékenysége főként a szárazföldi erők támogatását biztosította. A helikopterek vonatkozásban meg kell említeni több eszközt, illetve képességet. Eszközök vonatkozásában a LEFOGÓ-1A, -B és -C típusú, **saját fejlesztésű zavaró berendezések** olyan képességet jelentettek, melyet a Magyar Néphadsereg rádióelektronikai szolgálatának mérnökei fejlesztettek ki. **A fejlesztés egyik kritériuma az volt**, hogy a kijelölt helikopterbe történő **be- és kiszerezés viszonylag rövid idő alatt végrehajtásra kerülhessen**, illetve saját áramellátással kellett rendelkezniük. A fenti kritériumok azért kerültek meghatározásra, mivel az akkor rendelkezésre álló helikopterek alacsony száma nem tette lehetővé dedikált elektronikai hadviselési helikopter kialakítását. A felderítő vevők, a zavaróeszközök, a kijelzők, az antennacsatoló elemek és akkumulátorok guruló állványokra kerültek beszerelésre, melyek mellett foglalt helyet a kezelőszemélyzet. A LEFOGÓ-1A típus a harcászati rövid- és ultrarövid-hullámú frekvenciatartományban, 1,5-100 MHz között üzemelt, míg a LEFOGÓ-1B rádiórelé zavarási feladatokra, a LEFOGÓ-1C rádiólokátorok, légvédelmi rakétakomplexumok elleni zavarási feladatokra került kialakításra. Jelentős előrelépést jelentett, amikor a szentkirályszabadjai bázisra 1990 februárjában a Varsói Szerződés fegyverexportján belül a Szovjetunióból kettő darab Mi-17PP zavaró helikopter került. A helikoptertípus rendeltetése a *„földi rádiólokátorok, irányadók és más, a légvédelmi rendszerben üzemelő felderítő eszközök felfedése, aktív zavarókkal való lefogása volt.”* [89] A helikopter LO-24 berendezése az E és F, míg az LO-27 jelölésű egysége a D frekvenciasávban<sup>74</sup> üzemelt, teljesítménye mintegy 250 W volt. [84] Sajnálatos módon

<sup>74</sup> D sáv: 1000-2000 MHz, E sáv: 2000-3000 MHz, F sáv: 3000-4000 MHz.



később a rendelkezésre álló helikopterek számának csökkenése miatt előjárói döntés született az egy ideje már nem használt, elektronikai harcra kialakított 2 helikopter deszant helikopterekké történő átalakításáról, amely a tököli Dunai Repülőgépgyárban 2004 januárjában kezdődött meg. [90]

A fegyvernem életében a következő fordulópontot az 5. Kiskun Elektronikai Harc Ezred 2001-ben Egerbe történt átdiszlokálása és századdá alakulása jelentette. Az átszervezés során is jelentős volt a szakállomány lemorzsolódása, illetve ez sem járt technikai fejlesztéssel, a korábbi szaktechnikával hajtották végre a feladataikat továbbra is. Az egri Elektronikai Harc (a továbbiakban EHC) század 2004. szeptember 30-án felszámolt, illetve ezzel egy időben MH 5. Bocskai István Lövészdandár (a továbbiakban MH 5. B.I. ldd) kötelékében lévő 5/24 Bornemissza Gergely Felderítő Zászlóaljnál megalakításra került az elektronikai harc század, amely az egri század jogutódja is volt egyben. [91]

Az 5/24 Bornemissza Gergely Felderítő Zászlóalj felépítése (a 2017.07.31-i állapotnak megfelelően):

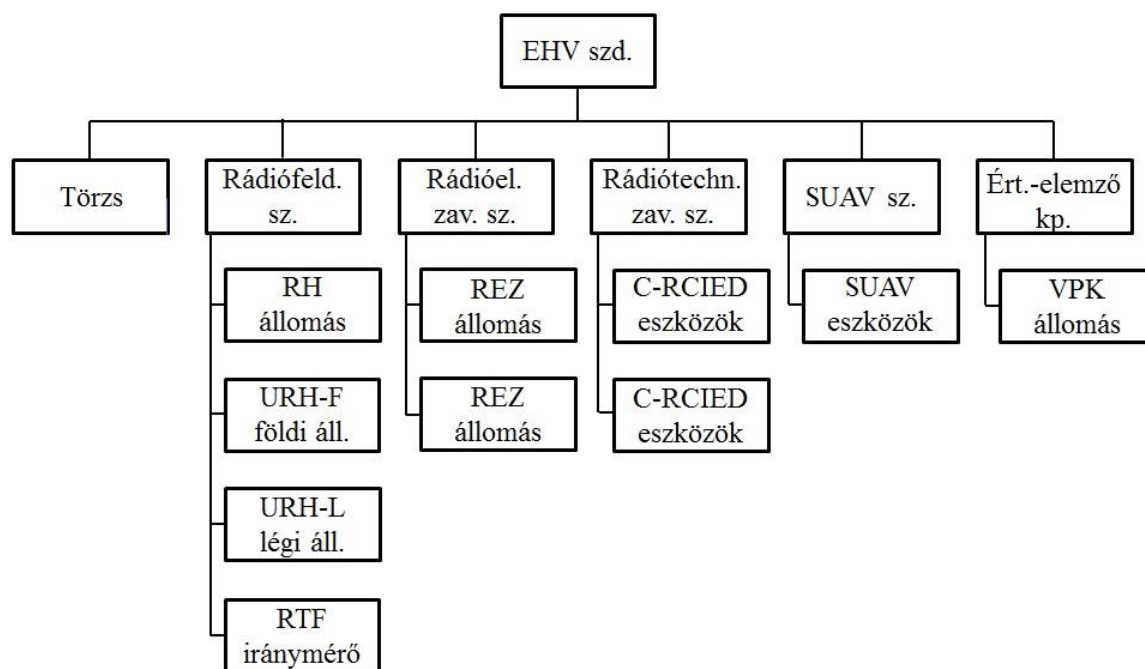
- „- zászlóalj parancsnokság,
- felderítő-adatértékelő csoport,
- csapatfelderítő század,
- felderítő század,
- harcászati hírszerző század,
- elektronikai hadviselés század,
- támogató szakasz.” [92]

Az Elektronikai Hadviselés század (a továbbiakban EHV század) 2017.07.31-i állapotnak megfelelő, a technikai eszközök vonatkozásában elkészített felépítését az 1.3. ábrán mutatom be. Az EHV század Debrecenben települt, technikai eszközei között megtalálhatóak voltak a korábbi, jogelőd szervezeteknél rendszeresített technikai eszközök és újabb gyártású eszközök is. A jogelőd alakulatoktól átvett technikai eszközök között voltak **a hagyományos, analóg adatforrások felderítésére alkalmas** R-1378 rövidhullámú rádiófelderítő állomás (RH állomás, FLÓRA), illetve az URH/F (URH/földi állomás) és az URH/L (URH/légi állomás) rádiófelderítő állomások. Az újabb technikai eszközök között voltak a C-RCIED-k<sup>75</sup> – amelyek azonban nem alkalmasak a szemben álló fél elektronikai

---

<sup>75</sup> Counter Radio Controlled Improvised Explosive Devices, C-RCIED

eszközeinek támadó célú, nagy hatótávolságú lefogására – illetve pilóta nélküli repülőgépek<sup>76</sup>. [92]



1.3. ábra: Az EHV század felépítése az eszközök vonatkozásában.<sup>77</sup>

2018. január 01-i hatállyal az 5/24. Bornemissza Gergely Felderítő Zászlóalj kivált az MH 5. B.I. Idd-ből és bázisán megalakult az MH 24. Bornemissza Gergely Felderítő Ezred. Települési helye Debrecen maradt és az EHV század teljes egészében átkerült az ezred struktúrájába.

A **légierő haderőnem** életében fontos állomást jelentett a kor technikai színvonalának megfelelő JAS-39 GRIPEN<sup>78</sup> többcélú repülőgép beszerzése, amely **fejlett önvédelmi célú elektronikai hadviselési képességgel rendelkezik**. A repülőgép önvédelmi célú elektronikai hadviselési képességének kihasználása érdekében a szükséges fenyegetettség és ellentevékenységi könyvtárak kialakítása, fejlesztése, valamint a könyvtárak fedélzeti számítógépbe való betöltése céljából kialakításra került az MH 59. Szentgyörgyi Dezső Repülőbázis (továbbiakban MH 59. SZD RB), Harcászati Repülőszázad, Elektronikai Hadviselési Támogató Központ. A központ a repülések után végrehajtja a mért eredmények kiértékelését, a kiértékelés alapján a könyvtárak pontosítását, majd a módosított könyvtárak tesztelését. A fenyegetés és ellentevékenységi könyvtárak kialakítása, a mért eredmények kiértékelése a különböző elektronikai kisugárzó eszközök kisugárzással kapcsolatos

<sup>76</sup> Small Unmanned Aerial Vehicle, SUAV

<sup>77</sup> [93] alapján szerkesztette a szerző.

<sup>78</sup> JAS: Jakt (vadász), Attack (támadó), Spaning (felderítő)

jellemzőit tartalmazó adatbázisok alapján történhet. Ilyen adatbázis például a NATO kisugárzó eszközök (NEDB<sup>79</sup>) adatbázisa, illetve kialakításra kerülhet egy speciális, magyar méréseken alapuló hazai adatbázis.

2018. december 31-ig stratégiai szinten a Felderítő Csoportfőnökség végzi az elektronikai hadviseléssel kapcsolatos feladatokat, melyek között a béke és különleges jogrend, illetve háborús feladatok tervezése, követelmények kidolgozása, okmányrendszerek és tervek előkészítése, a kidolgozás felső szintű koordinálása szerepel. [94] Hadművelési szinten pedig az Összhaderőnemi Parancsnokság Felderítő főnöksége a felelős az EHV vonatkozású tevékenységekért, országvédelmi és békeművelési feladatok, illetve a gyakorlatok végrehajtása során egyaránt. [95] 2019. január 01-től, az MH Parancsnokság megalakításával egyidőben a korábbi helyzet megváltozik.

Az MH elektronikai hadviselési szaktechnikával rendelkező alegységei közé tartozik a szárazföldi alakulatok vonatkozásában a már említett MH 24. Bornemissza Gergely Felderítő Ezred Elektronikai Hadviselés Százada, míg a légierő haderőnemnél a szintén említett MH 59. Szentgyörgyi Dezső Repülőbázis Gripen repülőgépeinek elektronikai hadviselési képességét kezelő Elektronikai Hadviselési Támogató Központja. A fentiekén kívül távirányítású robbanóeszközök ellen alkalmazható elektronikai zavaróeszközökkel (továbbiakban C-RCIED<sup>80</sup> eszközök) más alakulatok is rendelkeznek. A szaktechnikával rendelkező alegységek mellett mindenképpen **meg kell említeni az olyan alakulatokat is, melyek bár nincs EHV alegysége, mégis békeidős tevékenységük fontos része az elektronikai hadviselési környezetben<sup>81</sup> történő feladat végrehajtás begyakorlása.** Az említett alakulatok a Győrben települő MH 12. Arrabona Légvédelmi Rakétaezred, a Veszprémben települő MH 54. Veszprém Radarezred, illetve a szintén Veszprémben települő MH Légi Vezetési és Irányítási Központ, melyek szintén részt vesznek a NEWFIP Ramstein Guard többnemzeti elektronikai hadviselési gyakorlaton.

A már felsorolt alakulatokon kívül más katonai szervezetek is bevonásra kerülhetnek időszakosan elektronikai hadviselési vonatkozású feladatokba. 2013-ban szervezésében az alakulatoknál rendszeresített rádiólokációs álcázó eszközök, az úgynevezett szögviszszaverők telepítésének gyakorlására került sor. [31] A feladat során az MH 37. II. Rákóczi Ferenc Műszaki Ezred szakállománya a szentesi, tiszai vízi gyakorlótéren két szögviszszaverő típussal

<sup>79</sup> NATO Emitter Database

<sup>80</sup> Counter Radio Controlled Improvised Explosive Devices, C-RCIED

<sup>81</sup> Elektronikai hadviselési környezet fogalma alatt értem azon körülményeket, melyben az elektronikai hadviselés valamely funkciója alkalmazásra került, így például az elektronikai ellentevékenység funkció területe, az elektronikai zavarás. Más dokumentumban a fenti fogalommal nem találkoztam.

(Szféra és Piramida) hidat imitált az ott telepített PMP szalaghíd mellett, illetve a hékédi gyakorlótéren az OMU szögviszazaverőkkel a szárazföldi erők mozgását álcázták. A telepítést követően az MH 59. SZD RB repülőgépeinek PS-05/A radarjaival került tesztelésre a telepítés hatékonysága. [96]

Az elektronikai hadviselési és rádiófelderítő erők nemcsak honi területen, békeidőben kerülnek alkalmazásra, hanem részt vesznek a különböző válságreagáló műveletek biztosításában is. Fontos megjegyezni, hogy az egyes válságreagáló műveletekkel kapcsolatban az **adott feladat elemzését** követően kerül meghatározása, hogy **milyen elektronikai hadviselési vagy rádiófelderítő támogatásra** van szükség. Példaként említeném az anno az Magyar Honvédség Tartományi Újjáépítési Csoport (a továbbiakban MH PRT) érdekében dolgozó, a rádió-távírányítású improvizált robbanóeszközök elleni védelemre szolgáló zavaróeszközök kezelését végző vagy a rádiófelderítő állomást üzemeltető állományt. [97] Az 1.2. képen az MH PRT-nál végrehajtott felkészítésem során készített fényképen az amerikai féltől átvett HMMWV zavaróadójának antennája látható. A **zavaróeszköz üzemeltetését a készülék amerikai fél általi felprogramozását követően a magyar állomány végezte.**



1.2. kép: Magyar jelzésű HMMWV<sup>82</sup> beépített elektronikai zavaróeszközének antennái az MH PRT<sup>83</sup> táborában.<sup>84</sup>

<sup>82</sup> Nagy mozgékonyaságú többcélú kerekes jármű, High Mobility Multipurpose Wheeled Vehicle, HMMWV

<sup>83</sup> Magyar Honvédség Tartományi Újjáépítési Csoport, MH PRT

<sup>84</sup> Saját felvétel, Afganisztán, Pol-e Khomri, 2010.10.

Nemcsak a szárazföldi, hanem a légierő haderőnem elemei is részt vesznek békeműveleti elektronikai hadviselési vonatkozású tevékenységekben. Mindenképpen meg kell említenünk a NATINAMDS feladat mellett a Balti Légtérrendészeti feladatot is, melynek során a Magyar Honvédség JAS-39 Gripen vadászpilótái 2015. szeptember 01. – december 31. között teljesítettek szolgálatot. A légtérrendészeti feladat során a Baltikumban észlelhető elektronikai kisugárzó eszközök azonosításában a gépek önvédelemi rendszerét képező elektronikai hadviselési rendszerre fontos szerep hárult. Ez a feladat 2019. május 01-től újra megjelenik az MH feladatai között.

Az MH elektronikai hadviselési képességének fejlesztésével kapcsolatban számos terv és elképzelés, valamint tanulmány vagy értekezés született. Ezek sok esetben – **a terület komplexitása miatt** – érthető módon **csak egy-egy részterület fejlesztésére** vonatkozóan tartalmaztak javaslatot.

A NATO 2006-2016 közötti időszakra vonatkozó haderőtervezési javaslata (2006 Force Proposals for Hungary) Magyarország részére **egy dandár elektronikai hadviselési képességére** az alábbiak szerint tett javaslatot:

„- **kettő iránymérő alap** (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.**” [98]

A javaslattal kapcsolatban ki kell emelni, hogy MH jelenleg kettő lövészdandárral rendelkezik, ezek a Tatán települő MH 25. Klapka György Lövészdandár, illetve a Debrecenben települő MH 5. Bocskai István Lövészdandár. A fenti katonai szervezetek mellett foglalkozni kell a Szolnokon települő, az MH 34. Bercsényi László Különleges Műveleti Zászlóalj és az MH 88. Könnyű Vegyes Zászlóalj bázisán 2016. január 1-jén MH vitéz Bertalan Árpád 2. Különleges Rendeltetésű Ezreddé, majd 2017. szeptember 1-jén MH vitéz Bertalan Árpád 2. Különleges Rendeltetésű Dandárrá (a továbbiakban: MH 2. KRDD) alakult egységgel, valamint a szintén Debrecenben települő MH 24. Bornemissza Gergely Felderítő Ezreddel is. Így az is könnyen belátható, hogy ezen alakulatok részére **teljes képességgel rendelkező elektronikai hadviselési alegységek egy időben történő**

**biztosítása** – beleértve ebbe a kiképzett, felkészített személyi állományt, illetve a korszerű elektronikai hadviselési eszközöket is – **az MH részére jelentős kihívást jelentene.** Az egy időben történő megalakítás és technikai eszközzel történő felszerelés lényege a homogén szervezeti elemek kialakításának lehetősége és így azok kombinálhatósága lenne, ezáltal biztosítva a műveleti feladatok függvényében kisebb-nagyobb komplexitású feladatok nagy hatékonyságú végrehajtását.

A korábban rádióellentevékenységeknek hívott elektronikai zavarás megvalósításával kapcsolatban megfogalmazásra került, hogy *„olyan korszerű rádióellentevékenységi eszközökre van szükség, amelyekkel minden időben és bármely helyzetben képesek vagyunk a rádióellentevékenységekben megszabott feladatokat végrehajtani”*. [99] A rádióelektronikai eszközök robbanásszerű fejlődését az elektronikai ipar intenzív fejlesztései tették lehetővé, melynek egyik legfontosabb következménye, hogy az eszközök súlya, mérete, energia felvétele, előállítási költsége csökken, míg a nyújtott szolgáltatások száma, gyorsasága, megbízhatósága nő. [100] A fenti állítás napjainkban is megállja a helyét, a technikai fejlődés továbbra sem állt, folyamatosan jelennek meg újabb és újabb technikai megoldások, illetve fejlesztések. Fontos az is, hogy az egyes fejlesztések bevezetésénél, alkalmazásánál vizsgálni kell az újítás hatását a már meglévő rendszerekre és azt a tervezés folyamatába is be kell illeszteni.

A Magyar Honvédséggel és Magyarország iparával kapcsolatban mindenképpen fontos, hogy a Varsói Szerződés (a továbbiakban VSZ) tagországai fejlett hadiipari gyártók voltak, azonban a feladatok leosztásában és a termelésben a szovjet érdekek érvényesültek. A VSZ felbomlását követően a fenti hadiipari képességek eltűntek, valamennyi tagállam elvesztette az érintett iparágának nagy részét. Magyarország elsődlegesen a kommunikációs és elektronikai szektorba tartozó eszközöket gyártott. [101] Azt is fontos megjegyezni, hogy már a korábbi évtizedekben is foglalkoztak magasabb vezetési szinteken a fejlesztésekkel, a VSZ tagállamok hadseregei rádióelektronikai vezetőállományának 1978. évi értekezletén *„a hadosztályok speciális lefoglaló eszközökkel való ellátásának és ezek vezetése automatizálásának kérdései”* [102] kerültek meghatározásra, mint feladat. Problémát jelentett azonban már akkor is az MH EHV képességét érintő fejlesztések egyik alapvető gátja a technikai eszközök és a megalapozó képzések hiánya. [103] A Katonai tanács 1974. szeptember 10-én készült jelentésében az a megállapítás szerepel, miszerint a rádióelektronikai harc vonatkozásában *„jelenleg elmaradás van a Magyar Néphadsereg*

*általános technikai, fegyverzeti és felkészültségi színvonalához viszonyítva.*” [63; IV fejezet (II. kötet) 3. o.]

A későbbi kutatásokban is megjelentek a különböző fejlesztési javaslatok. A korábban már említett elektronikai harc és rádióelektronikai felderítő erők integrációja miatt a szakfeladatokat egységes vezetés alatt javasolták végrehajtani, azonban *„megvizsgálva és szembeállítva egymással a hadosztály elektronikai felderítésének adatforrásait, és a gépesített hadosztálynál jelenleg szervezetszerűen meglévő elektronikai felderítő erőket, megállapítható, hogy azok sem mennyiségileg, sem minőségileg nem biztosítják a hatékony feladat végrehajtást.*” [58; 6-7. o.] Felmerült az is, hogy *„az elektronikai hadviselési csapatokat, intézményeket nem csökkenteni, hanem tudományos laboratóriumi háttérrel megerősítve, intenzíven fejleszteni lenne szükséges.*” [24; 134. o.] A korábbi kutatásokban szükségesnek látták továbbá azt is, hogy *„egészen újfajta felderítő eszközökre és eljárásokra van szükségünk, egyrészt az adatok és információk, az információs technika és technológia által biztosított védelme, másrészt az információszerzés számára rendelkezésre álló idő nagyon rövid volta miatt.*” [103] Mindezt úgy kell megvalósítani, hogy a Magyar Honvédségnek is képesnek kell lennie elemeivel szövetséges keretek között hálózatközpontú műveletekben tevékenykedni. [104]

Amikor az MH vonatkozású elektronikai hadviselési fejlesztési javaslatokat vizsgáljuk, meg kell említenünk a különböző megvalósítási szintig eljutott fejlesztéseket is. Ilyen például a PRIZMA rendszer, vagy az INTERJAM projekt. Az INTERJAM projektet a második fejezetben mutatom be részletesen, mivel működésének alapja az SDR technológia alkalmazása.

A fenti két projekten kívül számos további fejlesztés is volt, köztük több olyan, amely nemzetközi környezetben, más országgal együttműködve indult, sajnálatos módon azonban később eredménytelenül befejeződött. Ilyen volt például a Balaton fedőnevű harcászati rádiófelderítő komplexum, amelynek mintája ZIL gépkocsikban került kialakításra, de a szovjet fél részéről páncélozott szállítójárműbe történő beépítés volt az igény. Egy évvel később a szovjet fél bejelentette, hogy elkészítette páncélozott szállító harcjárműbe szerelt TARAN rendszert, amit felajánlottak licenccsereért. Erről megkezdődtek a tárgyalások, de az időközben a VSZ-ben bekövetkezett változások miatt a megvalósítás meghiúsult. A Balaton nevű fejlesztés az 1988-89-es években román-magyar együttműködésben folytatódott, egy páncélozott URH iránymerő fejlesztése kezdődött a Technikai osztály

irányításával a Mechanikai Laboratóriumban. A szállító PSZH -t (BTR-70A) a román fél adta, azonban az eszköz fejlesztése nem fejeződött be a Ceausescu rezsim megbuktatásával kapcsolatos események miatt. [105] További **elektronikai hadviselési vonatkozású magyar fejlesztések** is voltak még, csak a fontosabbakat említve, így a **„Kaktusz” URH felderítő-iránymérő állomás, az IU-6M URH iránymérő állomás, a VU-21M vevő, a VU-141M mobil rádiórelé-felderítő állomás.** A sort természetesen lehetne még folytatni, nem elfelejtve például a „Boleró” fedőnevű 18-40 GHz között üzemelő vevőt és más eszközöket. A Kaktusz egy 20-500 MHz között üzemelő, konténerbe épített rádiófelderítő állomás volt, 32 méter magasra kitolható antennaárboccal. Az irányítást, az adatfeldolgozást és adatkommunikációt számítógépek segítségével biztosították. A rövidhullámú vevő bemeneti fokozatai analóggként üzemeltek, jelek digitális jellé konvertálása a középfrekvenciás fokozatban történt meg. Az eszköz a rendszerváltást követően került rendszeresítésre. Az RH iránymérés vonatkozásában kifejlesztésre került az IU-6M állomás, amely 20-100 MHz között üzemelt, kettő URH lehallgató munkahellyel. A munkahelyekhez tartozott egy 20-100 MHz között működő VU-21M vevő és egy UP-3MA panorámavevő. Később kifejlesztésre kerültek még a 20-100 MHz között üzemelő IU-60 és a 100-500 MHz között üzemelő IU-70 eszközök. Ezekben UREV és VREV típusú vevőket alkalmaztak. Az irányszög méréseket ezen eszközöknél már automatizáltan is végre lehetett hajtani. [106]

A PRIZMA rendszer a rövidhullámú rádiózavaró berendezések modernizálási programjában készült az R-378 – ZIK – ZVK rendszerállomások leváltására. A rendszer a tervek szerint 1 rövidhullámú zavarásirányító (VERA), 3 zavarást vezérlő (ZITA), 3 felderítő (FLÓRA), 1 rádió iránymérő vezérlő (RITA), 3 iránymérő (TAKER) és 12 komplex zavaró (ÁRBOC) állomásból állt volna úgy, hogy automatizált és hagyományos vezető, irányító és végrehajtó tevékenység végrehajtása volt a tervezés alapja. Ténylegesen azonban 1 VERA, 1 ZITA, 1 FLÓRA, 5 mobil ÁRBOC, 1 RITA és 3 TAKER állomás került csak kiépítésre. Ezeken felül még 1 ÁRBOC tantermi rendszer került kiépítésre. A rendszer működésének alapját egy hierarchikus, háromszintű kiépítés képezte, melynek legmagasabb szintjén a rendszer mindhárom funkcióját irányító és a VPK (ORIGO) rendszerhez csatlakozó VERA állomás volt. Középső szinten helyezkedtek el az egyes alrendszereket vezérlő ZITA és RITA állomások, míg a legalsó szinten helyezkednek el a felderítési, iránymérési és zavarási feladatokat végrehajtó FLÓRA, TAKER és ÁRBOC állomások. A VERA állomás **főbb feladatai a ZITA zavarást vezérlő központok irányítása, a RITA iránymérő alrendszer részére iránymérési parancsok kiadása, a kapott eredmények feldolgozása,**



**megjelenítése volt. A ZITA zavarást vezérlő állomások feladatai között szerepeltek a parancsok vétele és továbbítása, a felderítési adatok feldolgozása, tárolása és jelentése a VERA állomásnak. A FLÓRA felderítő állomás feladata a parancsok fogadása és a felderítési adatok jelentése volt. Az ÁRBOC zavaró állomás feladata az üzem módtól függően felderítési, iránymérési, lehallgatási, zavarási feladatok végrehajtása volt, mind autonóm, mind távvezérelt működési módban. A RITA iránymérő vezérlő állomás feladata a parancsok vétele, az alárendelt TAKER iránymérő állomások irányítása, az adatok feldolgozása és jelentése volt. A TAKER (R-1301) iránymérő állomás feladata az iránymérési parancsok fogadása és a mért adatok automatikus jelentése volt. Valamennyi állomás folyamatos adatátviteli és diszpécser összeköttetést tartott fenn az előjáró és alárendelt állomásokkal. [24; 4. sz. melléklet]**

Napjaink fejlett technikai lehetőségeit felhasználó kezdeményezés volt az Integrált elektronikai felderítő és zavaró rendszer fejlesztése, az **INTERJAM projekt**, melyet egy négy tagból álló konzorcium nyújtott be a Nemzeti Kutatási és Technológiai Hivatal nevében a Kutatás-fejlesztési Pályázati és Kutatáshasznosítási Iroda által 2007-ben hirdetett Jedlik Ányos Programra. A fejlesztés célja egy **két fő egységből álló felderítő-zavaró berendezés kifejlesztése és prototípusának megépítése volt**. A fejlesztésben az alábbi szervezetek vettek részt:

- SAGAX Informatikai Szervező és Tanácsadó Kft;
- Budapesti Műszaki és Gazdaságtudományi Egyetem, Szélessávú Hírközlés és Villamosságtan Tanszéke;
- Zrínyi Miklós Nemzetvédelmi Egyetem Információs Műveletek és Elektronikai Hadviselés Tanszéke;
- HM Elektronikai, Logisztikai és Vagyonkezelő ZRt. [107]



1.3. kép: Interjam zavaró állomás labormintája.[107]

A korábbi rádióelektronikai fejlesztésekkel kapcsolatban több magyar céget is meg kell említenünk, mivel ezen vállalatok dolgozói számos, a HM és BM által alkalmazott eszközt fejlesztettek ki és gyártottak le. Ezek között ott van a német licencek alapján eszközöket gyártó Siemens, majd később Telefongyár, illetve a Fulmen szövetkezet, amely az államosítást követően 293-as Hadiipari Vállalat, majd Elektromechanikai Vállalat néven üzemelt és később beolvadt a Beloianniszi Híradástechnikai Gyárba (a továbbiakban BHG). 1952-ben a katonai rádiófelderítő és a BM rádióelhárító szolgálatok kezdeményezésére létrejött a Mechanikai Laboratórium Híradástechnikai Kísérleti Vállalat, melynek feladata a HM és BM részére rádiófelderítő eszközök fejlesztése és gyártása volt. A vállalat **szakembereinek magas szintű tevékenységét** mutatja, hogy a volt szocialista országok között **elsőként alkalmaztak félvezető technológiát és berendezésekbe épített mikroprocesszorokat a vezérléshez, jelfeldolgozáshoz és automatizáláshoz.** A rendszerszemlélet miatt **komplex munkahelykészleteket**, gépkocsiba épített állomásokat, majd ezek összekapcsolásával **komplex automatizált rendszereket alakítottak ki.** A rádiófelderítő eszközök fejlesztése terén jelentős szerepe volt a Távközlési Kutató Intézetnek (a továbbiakban TÁKI), amely a Finommechanikai Vállalattal együtt jött létre (a továbbiakban FMV). Az elgondolás az volt, hogy a korábban nem létező lokátortechnikát a TÁKI meghonosítja, az FMV pedig legyártja. A fenti cégek együttműködésében került kifejlesztésre a mobil műholdfelderítő és lehallgató „Napraköröző” állomás. A felsorolt cégek

számos további technikai eszközt fejlesztettek ki, amelyek egy része exportálásra került. A felsorolt vállalatok tevékenységét a 2. Csoportfőnökség Rádióelektronikai Felderítő Szolgálat vezetői, kijelölt szervei (Rádiófelderítő Technikai Osztály, majd később Elektronikai Igazgatóság) koordinálták, irányították. **Ez a fejlesztési tevékenység a 80-as években is folytatódott, azonban később mind a hazai igények, mind a keleti és harmadik világba történő exportlehetőségek lecsökkentek** és ez a már kialakult **magyar vállalati háttér megszűnését jelentette.** [106]

Az ilyen leépülések az egyik példája a BHG megszűnése. 1874-ben Egger Bernát megnyitotta budapesti távirdaszerelő- és javító műhelyét, amely később a Posta és a MÁV beszállítója lett. A siker generálta növekedés során felvették az "Első Osztrák-magyar Villanyvilágítási és Erőátviteli Gyár" nevet, ahol már gépekkel és gyári szervezettséggel termeltek. Az 1896-os millenniumi kiállítás után jelentős külföldi megrendeléseket is kaptak. Több átnevezést követően a fejlődés folytatódott, önállóan terveztek telefonközpontokat, így például a 10.000 vonalas budapesti Teréz központot. Később L. M. Ericsson felvásárolta a céget, így jött létre az Ericsson Magyar Villamossági Rt., aki a hadsereg legfőbb beszállítója lett. 1926-tól kezdődött a rádiógyártás, 1928-ban pedig az ITT érdekeltségi körébe tartozó "International Standard Electric Co." leányvállalata lettek. Kormányzati pályázat elnyerését követően az egész ország ellátására alkalmas műsorszóró adóhálózatot építettek ki, majd rádiókat gyártottak. Ők gyártották a Standard rádiókészülékeket, amelyek minőségi eszközök voltak. Az államosítás miatt azonban a külföldi partnerek kiléptek az együttműködésből, haladó külföldi technológiát már nehezebb volt követni, mégis képesek voltak megújulni. Két év alatt elkészítették az első hazai tv adót, amellyel elkezdődhettek a kísérleti adások. Telefonokat gyártottak a szovjet piacra, telefonközpontokat fejlesztettek. **A fejlődés olyan mértékű volt, hogy vidéken hoztak létre új üzemeket,** Tatabányán, Szekszárdon, Kunhegyesen és Debrecenben. A 80-as években is jelentős fejlődéseket produkáltak, így **integrált áramköröket, kétoldalas nyomtatott paneleket alkalmaztak.** A leépülés kezdete a vidéki körzetek digitalizálására irányuló 1989-es, majd a főközpontokra kiírt 1990-es pályázatok elvesztése volt. A Szovjetunió széthullásával az a piac is elveszett. A fénykorában 22.000 embert foglalkoztató cégnek 1992-ben már csak 4.500 dolgozója volt. A túlélés érdekében partnereket kerestek, megalakult két vegyesvállalat, a BHG-TeleCOM Távközléstechnikai Kft., valamint a Hirschmann-BHG Híradástechnikai Kft. A piacok elvesztése azonban folytatódott, 1995-ben a Matáv második tenderén sem nyertek és ez megpecsételte a vállalat sorsát. A következő években folytatódott a leépítés, az anyavállalat

2000-es években bezárta a kapuit. A cégből mindössze az 1995-ben alakult BHG Alkatrészgyártó Kft. maradt fenn. [108]

### **Összegzés, részkövetkeztetések**

Értekezésem első fejezetében három fő kérdéssel foglalkoztam. Az első kérdéskör az utóbbi évtizedekben bekövetkezett biztonságpolitikai változásokra fókuszált, rámutatva a Magyar Honvédség megváltozott szerepére. Mindenképpen ki kell hangsúlyozni, hogy a Varsói Szerződés felbomlását követően a NATO-hoz történő csatlakozás okán ismét fel kellett készülni arra, hogy haderőnk nemcsak a határokon belül, hanem azon kívül is alkalmazásra kerül majd. Katonáink számos nemzetközi műveletben vettek és vesznek részt napjainkban is, ahol már nemcsak a korábban tanult konvencionális harcéljárásokkal találkozhatnak/találkozhatnak, hanem az egyre nagyobb területen elterjedt aszimmetrikus, illetve a hibrid hadviselés elemeivel is. Európa területén a délszláv válság óta nem folyt fegyveres harc, azonban a hibridhadviselés megjelenése Ukrajnában, illetve az egyre gyakoribbá váló, a különböző európai nagyvárosokban elkövetett és nagyszámú emberáldozatot követelő terroristatámadások a fejlett, nyugati társadalmak esetében is testközelbe hozták a korábban csak a médiában látott brutalitást, vérontást.

**Ezen események alapvetően ingatták meg az európai emberek biztonságérzetét, amely miatt a különböző országok politikai és a katonai vezetése egyre erősebb nyomás alá került.** A hadviselési elvekben és módszerekben bekövetkezett változások újabb és újabb fenyegetéseket hordoznak magukban a katonákra nézve is, az elektronikai hadviselés vonatkozásában például a rádió-távírányítású improvizált robbanóeszközök megjelenése és elterjedése az egyik legrelevánsabb példa. Számolnunk kell azonban azon eszközökkel is, amelyek szemben álló fél általi alkalmazása nem jár közvetlenül emberáldozattal, azonban a későbbiekben ez számunkra nagy kockázattal járhat. Ebben az esetben az ellenünk alkalmazható fejlett felderítő technológiákra vagy éppen a saját kommunikációs és nem-kommunikációs eszközeink ellen bevethető elektronikai zavaróeszközökre gondolok. **Vizsgáltam azt is, hogy a művelettervezés és műveletvezetés elveiben is jelentős változások mentek végbe,** melyek az elektronikai hadviselés tervezésében is változásokat indukáltak.

A második fő gondolatkörben az elektronikai hadviselés és a rádiófelderítés alkalmazásával foglalkoztam a különböző konfliktusok, illetve a Magyar Honvédség vonatkozásában. Napjaink konfliktusainak bemutatásával, illetve az egyes konfliktusok során az elektronikai hadviselés és a rádiófelderítés alkalmazási módjának ismertetésével

rámutatott annak **létjogosultságára**, illetve szükségességére. Vizsgáltam az MH vonatkozásában **a különböző időszakban végrehajtott szervezési feladatokat**, beleértve ebbe a **haderőreformok során végrehajtott létszámleépítések következményeit**, valamint a **vizsgált feladatrendszer szervezetei közötti átadását**.

A harmadik kérdéskörben az elektronikai hadviselés és a rádiófelderítés fejlődésével, néhány, a témában jelentős technológiai előnnyel bíró ország hadseregében végrehajtott fejlesztések elemzésével foglalkoztam. Mindenképpen fontos figyelembe venni azt, **hogy a kiemelt államok által végrehajtott fejlesztésekre mintegy iránymutatásként kell tekinteni**, és fel kell készülni **a digitális kor háborúira**, melyben a korábbi műveleti környezetek mellett már **az elektromágneses spektrumban és a kibertérben is tervezni kell a végrehajtandó műveleteket**, legyen az támadó vagy védelmi jellegű. Ebben a fejezetben bemutattam és elemeztem az MH elektronikai hadviselési és rádiófelderítő szakterületével kapcsolatban a különböző szintű tudományos munkákban tett javaslatokat, illetve a javaslatok megvalósulását. Kiemelten kezeltem a részben megvalósult PRIZMA rendszer fontosabb elemeinek, valamint egy konzorcium INTERJAM elnevezésű projektjének bemutatását. Sajnálattal kellett megállapítanom, hogy a bemutatott javaslatok, valamint a fenti két fejlesztési lehetőség egyike sem került teljes mértékben kihasználásra. Elemeztem és néhány példán keresztül bemutattam, hogy a korábbi évtizedekben Magyarországon jelentős ipari háttér volt elérhető, amely képes volt a különböző haditechnikai eszközök kifejlesztésére és más országokba történő exportálására. Egyúttal azt is meg kellett állapítanom, hogy mára a korábban létezett vállalatok nagy része – a képességgel együtt – megszűnt vagy elvesztve korábbi piacait jelentősen visszaszorult a műszaki életben.

A fentiek alapján az alábbi következtetéseket fogalmazom meg:

1. Napjaink **katonai műveleteiben** továbbra is fontos szerepet játszik **a fejlett technológia alkalmazása** valamennyi műveleti környezetben, valamennyi hadviselési mód (konvencionális, aszimmetrikus vagy hibrid) esetében. **Mindegyik műveletben vizsgálnunk kell** az elektromágneses spektrumért vívott harc egyik legfontosabb elemének, **az elektronikai hadviselésnek lehetséges alkalmazását**. Ebbe beletartozik a más szakterületekkel történő együttműködés (felderítés, információs műveletek, targeting), de az új eljárásokban, így például az A2/AD környezetben történő alkalmazás is.

2. A művelettervezésben bekövetkező változások az elektronikai hadviselés tervezésében is változásokat generáltak. Annak érdekében, hogy a különböző szintű és méretű katonai műveletek hatékony, hatásalapú elektronikai hadviselés támogatása, illetve a

különböző elektronikai hadviselési funkciókhoz tartozó feladatok folyamatos koordinációja biztosított legyen, **hadműveleti szinten egy Elektronikai Hadviselési Koordinációs Részleg<sup>85</sup> felállítását és állandó jelleggel történő működtetését látom indokoltnak.**

3. **A szükséges fejlesztések és az eljárásokban szükséges módosítások beazonosítása** érdekében **folyamatosan követni és elemezni kell** a különböző konfliktusokban történt **elektronikai hadviselési vonatkozású incidenseket**, kiemelt figyelemmel az új technikai fejlesztések alkalmazására. A fenti elemzésekből a következtetések levonása után **az új elgondolásokat be kell építeni** az MH-nál végrehajtandó vagy folyamatban lévő **fejlesztésekbe**. Figyelembe kell venni, hogy több különböző technikai fejlesztés egyidejű alkalmazása, beintegrálása – a megfelelő interoperabilitás megléte esetén – megnövelheti az elérhető képességfejlődést.

---

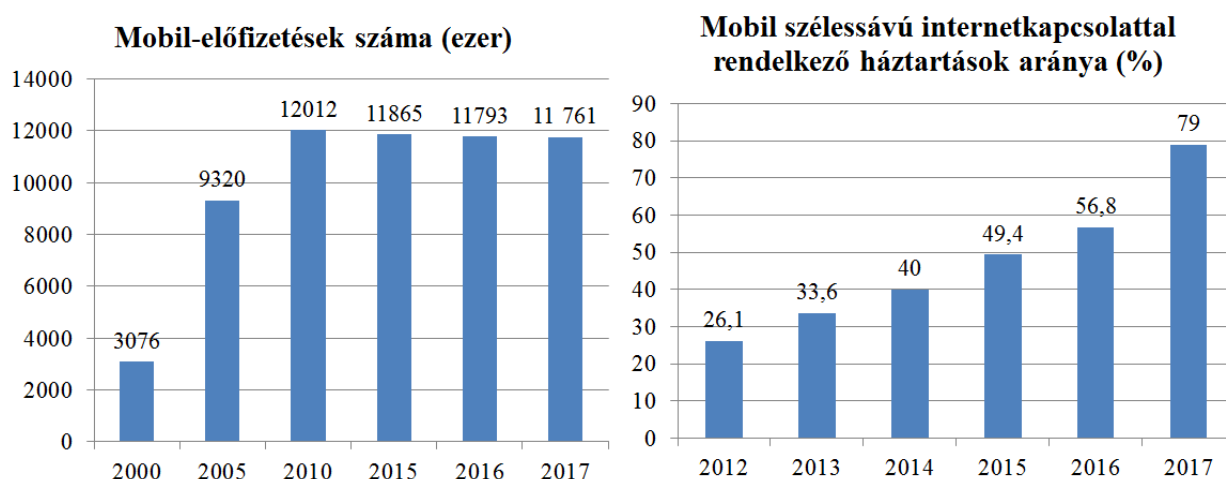
<sup>85</sup> Electronic Warfare Coordination Cell - EWCC

## 2. A SZOFTVERRÁDIÓ TECHNOLÓGIA ALKALMAZÁSA A KÜLÖNBÖZŐ TECHNIKAI RENDSZEREKBEN

Napjaink biztonságpolitikai helyzetének változása mellett a folyamatos technikai fejlődés az, ami szintén jelentősen befolyásolja, illetve megváltoztatja a hadviselés módját. Jelen fejezetben az értekezés vonatkozásában fontos területek fejlődését vizsgálom.

### 2.1. Frekvenciagazdálkodás

Az 1. fejezetben bemutatott technikai fejlődés következtében megjelenő újabb és újabb elektronikai eszközök nagymértékben befolyásolják, általában megkönnyítik, de sok esetben bonyolultabbá is teszik mindennapi életünket. Mivel számuk folyamatosan emelkedik, nem szabad elfelejtenünk, hogy az ilyen eszközök többsége esetében a működés az elektromágneses spektrum felhasználásán alapul. A Központi Statisztikai Hivataltól származó adatokon alapuló 2.1. ábrán látható, hogy a magyar háztartásokban is jelentős változások mentek végbe ezen eszközök számának vonatkozásában. A mobil előfizetések száma 2000. és 2005. között a háromszorosára nőtt, míg ez a szám további 30%-val nőtt a következő öt évben. 2016-2017. között már nem volt további kimutatható növekedés. Itt meg kell jegyezni, hogy a McAfee Labs előrejelzése szerint az okostelefonok száma a világban 2020-ra 5,9 milliárd (a 2015-ös értéknek majdnem kétszerese) lesz. [109] A másik, szintén az elektromágneses spektrum kihasználtságát jól mutató jellemző a mobil szélessávú internetkapcsolattal rendelkező háztartások számának változása, mivel a vizsgált öt év alatt az ilyen típusú internetkapcsolattal rendelkező háztartások száma megháromszorozódott. [110]



2.1. ábra: Háztartások mobil-előfizetéseinek száma, valamint mobil szélessávú internet előfizetéseinek aránya. [110]

Fontos azt is kihangsúlyozni, hogy bemutatott felhasználások mellett jelentős az elektromágneses spektrum használatán alapuló további eszközcsoportok száma is, amelyek közé tartoznak továbbá a távirányítók (beleértve a szórakoztató elektronikai eszközöket, játékokat, kapunyitókat, stb.), a különböző WLAN eszközök, rádiók, okos televíziók is.

**Az elektromágneses spektrum használatán alapuló technikai eszközök számának növekedése a spektrummenedzsment szempontjából is egyre növekvő koordinációs kihívást jelent.** Mivel a rádióhullámok terjedése nem köthető az egyes államok országhatárához, nemzetközi szervezetek együttműködésének keretén belül szükséges meghatározni az elektromágneses spektrum alkalmazásának alapvető szabályait, melyet utána az egyes országok a saját területükre vonatkozóan szabályoznak tovább.

A spektrumgazdálkodásért nemzetközi szinten felelős szervezet a Nemzetközi Távközlési Egyesület<sup>86</sup>, Magyarországon a frekvenciagazdálkodásért felelős országos szintű szervezet a Nemzeti Média és Hírközlési Hatóság. A Magyar Honvédség vonatkozásában a frekvenciagazdálkodással kapcsolatos feladatokat több szervezetnél is végezték korábban, többek között a Magyar Néphadsereg idejében a Rádióelektronikai Főnökségnél [59; IV fejezet (II. kötet), 72. o.], míg napjainkban frekvenciagazdálkodást és zavarkivizsgálást a MH vitéz Szurmay Sándor Budapest Helyőrség Dandár végzi. [111]

A nemzetközi frekvenciagazdálkodási szervezet a hatékony frekvenciagazdálkodás érdekében három földrajzi körzetet alakított ki, Magyarország az 1. Körzetbe tartozik. **A nemzetközi felosztásban meghatározott frekvenciák nemzeti szinten a vonatkozó nemzetközi szabályzók alapján további felosztásra kerülnek és azokat az aktuálisan érvényben lévő NMHH rendelet tartalmazza,** így „a nemzetközi felosztás keretein belül a nemzeti felosztás meghatározza Magyarország területén a rádiószolgálatok részére felosztott frekvenciasávokat szolgálati kategóriáiknak megfelelően, beleértve a polgári, nem polgári és együttes célú felhasználásra történő felosztást is. A tengeri mozgószolgálat részére felosztott frekvenciasávok Magyarország területén - a rendelet alapján - a belvízi mozgószolgálat részére is fel vannak osztva.” [112] Fontos az is, hogy a polgári és nem polgári felhasználók a másik kategóriába tartozó frekvenciák használatára is nyújthatnak be igényt és annak felhasználására vonatkozó engedélyt – az engedélyben történő feltételek betartásával – meg is kaphatják. „A NATO, valamint a NATO felhasználók magyarországi frekvencia felhasználását a katonai tevékenységgel kapcsolatban nem polgári célúnak, a műsorszórással kapcsolatban pedig polgári célúnak kell tekinteni.” [112] A fenti rendelet meghatározza azt

---

<sup>86</sup> International Telecommunication Union, ITU



is, hogy a különböző állomások alkalmazásuk során okozhatnak-e zavarást más állomások működésében, illetve milyen feltételek mellett kénytelenek a más rádióeszközök által okozott zavarást tűrni. Az adott frekvenciasávban üzemelő rádiószolgálat állomás<sup>87</sup> a működés és zavarvédelem szempontjából lehet elsődleges vagy másodlagos. *„Az elsődleges rádiószolgálat állomása nem okozhat káros zavarást az azonos vagy más elsődleges rádiószolgálat olyan állomásainak, illetve nem tarthat igényt védelemre az azonos vagy más elsődleges rádiószolgálat olyan állomásai által okozott káros zavarásokkal szemben, amelyek részére a frekvenciákat korábban már kijelölték, vagy amelyek részére a frekvenciahasználati jogot korábban már megszerezték.”*[112]

**Az elektromágneses spektrum katonai vonatkozású felhasználása esetében is egyre több a koordinációt igénylő feladat azért, hogy a különböző rendszerek egymástól függetlenül, egymás működésében zavartatást nem okozva üzemelhessenek.** Számos rendszer interferenciamentes működését kell biztosítanunk, többek között radar-, különböző kommunikációs, idegen-barát felismerő<sup>88</sup> és elektronikai hadviselési rendszereket. Ennek megoldására egyrészt adminisztratív módszerek, másrészt különböző technikai fejlesztések állnak a rendelkezésünkre. Adminisztratív megoldás a korábban már említett frekvencia-, fejlettebb technikai környezetben spektrumgazdálkodási tevékenység folytatása. A Magyarországon végzett frekvenciagazdálkodási feladatokkal kapcsolatban meg kell említenünk az NMHH által működtetett NATO Nemzeti Rádiófrekvencia Hivatal<sup>89</sup> tevékenységét is, amely többek között *„a hazánkba érkező szövetséges és partnerségi erők, valamint a külföldre vezényelt magyar csapatok frekvenciaigényeinek”* biztosításával kapcsolatos teendőket végzi, illetve a katonai frekvenciahasználat jogszerűségét is ellenőrzi. [113]

Számos kutatás alátámasztja, hogy **az engedéllyel rendelkező felhasználók által a frekvenciahasználat a spektrum egy részére koncentrálódik, míg a spektrum jelentős része részben, vagy teljesen kihasználatlan.** Erre a problémára megoldás a dinamikus spektrum elérés<sup>90</sup>, amely a rádióeszközök működésének valós idejű figyelésén, a spektrum helyi megfigyelésén, próbák elvégzésén, valamint a különböző kognitív elemekből és hálózatokból kialakított vezeték nélküli hálózat működtetésén alapul. A spektrum

<sup>87</sup> „Állomás: egy vagy több adó- vagy vevőberendezés vagy adó- és vevőberendezés-csoport a tartozékokkal együtt, valamely rádiótávközlési szolgálatnak vagy a rádiócsillagászati szolgálatnak egy adott helyen történő megvalósítása céljából.” [112]

<sup>88</sup> Identification Friend or Foe, IFF

<sup>89</sup> National Radio Frequency Agency, NARFA

<sup>90</sup> Dynamic Spectrum Access

megfigyelésének célja, hogy a nem használt spektrumszegmenseket, az úgynevezett fehér tereket („white spaces”) megtaláljuk, annak érdekében, hogy a másodlagos felhasználók az elsődleges felhasználók zavarása nélkül használhassák eszközeiket. [114]

Az 1.4.2. alfejezetben már említettem a RELEK-et, ezzel kapcsolatban mindenképpen fontosnak tartom megemlíteni, hogy a kezdetektől nagyon hosszú ideig a „*Magyar Honvédségben az elektromágneses (rádió) zavarok kivizsgálása és azok megszüntetése az elektronikai harc szolgálat feladata (MNVKF 07/1979 intézkedése a rádióelektronikai eszközök összeférhetőségének biztosítására. Budapest, HM 1979.)*” [86; 48. o.] volt. Az általuk kivizsgált esetekben az **elektromágneses zavarások okai** között az alábbiak szerepeltek:

- „- az eszközök nem az engedélyezett frekvencián, teljesítménnyel, stb. üzemeltek;
- a szomszédos frekvencián üzemelő adók egymáshoz közel települtek;
- frekvenciaengedély nélküli eszközöket üzemeltettek;
- a térbeli korlátozást figyelmen kívül hagyták.” [86; 57. o.]

A frekvencia spektrum hatékony felhasználása érdekében – az előbb említett problémák elkerülése érdekében – számos technikai fejlesztés áll a rendelkezésünkre, így a frekvenciaugratásos rendszerek<sup>91</sup>, a szoftverrádió technológia vagy a különböző adaptív eszközök (azaz az újrakonfigurálhatóságot, többsávúságot és többmódúságot biztosító eszközök).

A különböző rádióállomások - így természetesen az **SDR alapú rádióállomások** **kisugárzásának is** - **összhangban kell lennie a szigorú elektromágneses zavarásra<sup>92</sup> és az elektromágneses kompatibilitásra<sup>93</sup> vonatkozó**, a különböző nemzetközi, nemzeti, és regionális szabványügyi testületek és hatóságok által megadott **előírásokkal**. Fontos azt is megjegyezni, hogy a tervezés végén meg kell vizsgálni, hogy a digitális részben történt változtatásokat az analóg elemek képesek-e kezelni, így biztosítva azt, hogy az eszköz képes legyen a vele szemben támasztott követelményeknek (működés, stabilitás, költséghatékonyság, stb.) megfelelni. Ez természetesen kihatással van az élettartamra is. [115]

Napjainkban az elektromágneses spektrum felhasználása számos fegyvernemnél és szakcsapatnál a megfelelő szintű feladatvégrehajtás alapja, így nagyon fontos egy hatékony, jól koordinált spektrummenedzsment működtetése.

---

<sup>91</sup> Frequency hopping

<sup>92</sup> Electromagnetic interference, EMI

<sup>93</sup> Electromagnetic compatibility, EMC

**Az SDR alapú technológia alkalmazása lehetővé teszi eszközeinkben az üzemi frekvencia és egyéb paraméterek módosítását.** A többi felhasználóval történő interferencia elkerüléséhez, vagy akár egy EHV vonatkozású gyakorlás/kiképzés előkészítéséhez szükséges, hogy a spektrummenedzsment által kezelt frekvenciaadatok az EHV elemek számára folyamatosan elérhetőek legyenek. **Mivel az elektronikai hadviselés a teljes frekvenciaspektrumban folytatott tevékenységet jelent, véleményem szerint szükséges egy elektronikai hadviselési vonatkozású frekvenciamenedzsmenttel foglalkozó elem kialakítása, amely részét képezné a korábban már említett, a hadműveleti/összhaderőnemi szinten felállításra javasolt Elektronikai Hadviselési Koordinációs Részlegnek.**

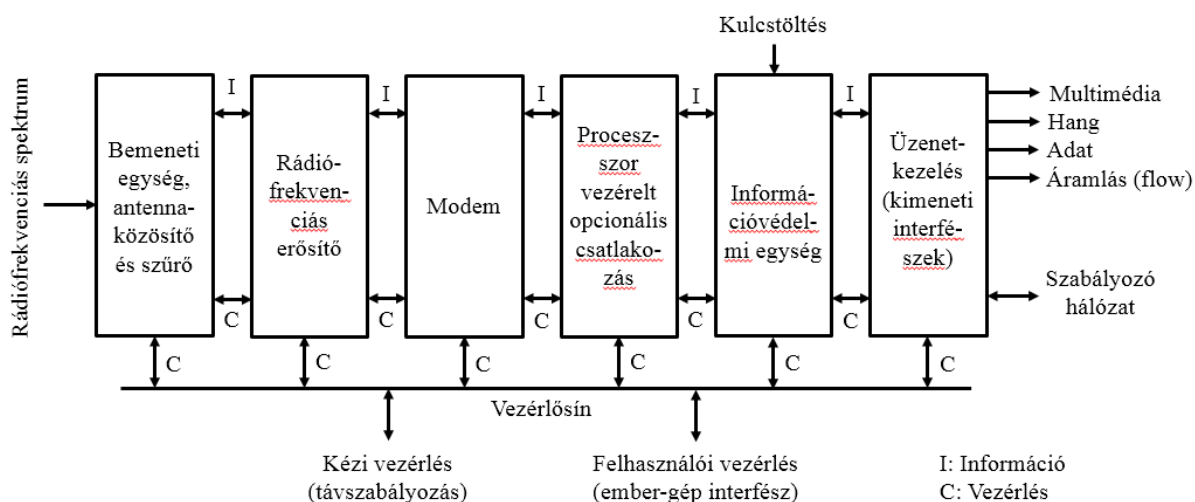
## **2.2. A szoftverrádió technológia felhasználása**

Ebben az alfejezetben a szoftverrádió technológia kezdeti felhasználását vizsgálom annak érdekében, hogy a későbbiekben megalapozott javaslatok kialakítása biztosított legyen.

### **2.2.1. A szoftverrádió technológia alapjai**

Az elektronikai eszközök fejlődésében jelentős mérföldkő a szoftverrádió koncepció alapuló eszközök megjelenése. Ennek oka az, hogy **a korábban kifejlesztett és alkalmazott eszközök esetében a további fejlesztések lehetőségét a hardverek cserélhetősége befolyásolta, illetve korlátozta le.** Az egyes elemek sok esetben már kisebbek voltak a korábbiaknál, más foglalatra készültek, más hűtési vagy adatátviteli módot követeltek meg annak érdekében, hogy a kifejlesztett képességeiket hatékonyan ki lehessen használni. Ez további módosításokat, illetve további elemek cseréjét generálta, amely miatt már a korábbi részegységek felhasználása gazdaságtalanná tette az ilyen módon végrehajtott fejlesztéseket. Később megjelent a komplett modulok cseréjének lehetősége, azonban ez is csak időleges megoldás volt a gyorsan fejlődő elektronikai eszközök világában. Az említett fejlesztési problémákra jelenthet és jelent is megoldást sok esetben a szoftverrádiós technológia megjelenése és elterjedése. A szoftverrádió technológia alkalmazása azonban azt is biztosítja, hogy ugyanazon eszköz különböző feladatokra, adatátviteli módokra is felhasználható legyen, így például alkalmazható lehet Bluetooth és WLAN adatkapcsolatra, rádióállomások és rádióhálózatok hallgatására. Emellett magában hordozza annak lehetőségét is, hogy ugyanazon eszköz a föld bármely pontján alkalmazható lehet, hiszen a működést az implementált szoftverrel határozzuk meg.

A polgári alkalmazású szoftver-vezérlésű rádiók kutatása és fejlesztése érdekében a 90-es években megalakult a Moduláris, Többfunkciós Információátviteli Rendszer (Modular Multifunction Information Transmission System, MMITS) Fórum, amely a későbbi 'Software Defined Radio' Forum elődje volt. A szoftverrádió a 'Software Defined Radio' Forum megfogalmazása szerint „Rádió, melyben a fizikai réteg egy vagy több funkciója szoftver által meghatározott”<sup>94</sup>. **A szoftverrádió koncepció alapgondolata az, hogy ugyanaz az eszköz többféle rádióalkalmazásra használható, mivel képesek vagyunk annak néhány paraméterét (pl. frekvenciasáv, hullámforma, teljesítmény, stb.) szoftveresen változtatni.** [116] A 2.2. ábrán bemutatom a szoftver-vezérlésű rádió egy csatornájának blokkvázlatát. Egy eszközben a kialakítandó csatornák száma az eszközbe beépített SDR eszközök számától függ.



2.2. ábra: A szoftver-vezérlésű rádió egy csatornájának blokkvázlata. [117]

A Wireless Innovation Forum megállapítása szerint az SDR<sup>95</sup> alkalmazása a különböző eszközökben folyamatosan növekvő tendenciát mutat, a napjainkban eladott harcászati rádiók mindegyike alkalmazza az SDR elvet, a polgári és katonai műholdas alkalmazások esetében a középfrekvenciás és az alapsávi jelfeldolgozás során jelent előnyt. [116] Sok esetben, még ha nem is jelzik, hogy SDR alapú az adott eszköz, mégis felhasználják annak előnyeit, a fejlesztők és gyártók esetében a költséghatékony fejlesztést vagy termelést, a szolgáltatók és a végfelhasználók számára a költséghatékony karbantartást, vagy az aktuálisan alkalmazott eszközök esetében a meglévő infrastruktúra alkalmazásával új képesség bevezetését, illetve a későbbiekben egyszerűbb fejlesztési lehetőséget. Az SDR

<sup>94</sup> „Radio in which some or all of the physical layer functions are software defined”.

<sup>95</sup> Software Defined Radio koncepció esetében általánosan alkalmazott rövidítés.

alkalmazás egyik legnagyobb előnye a dinamikus spektrum hozzáférés vagy felhasználás, amely mind a gyártók, mind a végfelhasználók számára jelentős előnyöket nyújt. [118] Ezzel kapcsolatban visszautalnék a fejezet bevezető részében a frekvenciaspektrum telítettségére vonatkozó megjegyzéseimre.

**Az SDR koncepció alkalmazása az alábbi előnyöket nyújthatja:**

- **multi-funkcionalitás:** ugyanaz a rádióplatform többféle rádiófunkciót képes támogatni;
- **globális mobilitás:** ugyanaz a rádióplatform alkalmazható a világ minden táján (feltételezve, hogy nincs lekorlátozva egy szabványra);
- **kompaktság és hatékonyság:** több kommunikációs szabvány támogatható ugyanazzal a rádióplatformmal;
- **könnyű gyártás:** az alapsávi feladatok végrehajtása szoftverfeladat, nem
- **könnyű fejlesztés:** firmware/szoftver módosításával/cseréjével megváltoztatható az SDR eszköz funkciója, működése. [114; 3. old.]

A szoftverrádió technológia alkalmazásának egyik kulcseleme a digitális jelfeldolgozás. A mai korszerű berendezések digitális középfrekvenciás jelfeldolgozással működnek, ahol az analóg fokozat feladata a középfrekvenciás lekeverés. A klasszikus értelemben vett szoftverrádiók – azaz a digitális rádiófrekvenciás feldolgozás – esetében a bemenő jel minimális kondicionálás (erősítés, sávszűrés) után azonnal A/D átalakítóra kerül. [119]

Az A/D konverter a vételi oldalon az analóg jelet digitálissá alakítja, melynek célja a jel digitális rendszerekben történő feldolgozhatóságának biztosítása, illetve az analóg csatornán továbbított jelhez hozzáadódó csatornazaj okozta problémák megszüntetése. [121] Az átalakítás első feladata a mintavételezés.

*„A mintavételezés során a folyamatos jelet csak adott időpontokban értelmezett, az adott időpontban a folyamatos jel értékével megegyező értékű (mintavett) értékekkel helyettesítjük. Az így előálló mintavett jel végtelen sok lehetséges értéket felvehet, és így nem rendelhető hozzá véges hosszúságú kódsorozat. Le kell tehát csökkenteni a mintavett jel értékkészletének elemszámát – erre szolgál a kvantálás, ami véges sok lehetséges érték közül egy kiválasztottra való kerekítést jelent.”* Az így kapott jel már digitalizált jel, amelyhez egy kódoló segítségével rendelhetünk bináris kódsorozatokat. [121; 3. oldal] A Nyquist-Shannon

mintavételi elv alapján „az  $f_m$  mintavételi frekvenciának legalább az  $f_{max}$  legnagyobb jelfrekvencia kétszeresének kell lennie.” [122]

**Figyelembe kell azonban azt is venni, hogy** ahogyan az analóg jelátvitelnél, úgy a digitális jelátvitel esetében is lépnek fel hibák, amelyek különböző mértékben csökkenthetők, azonban meg kell jegyezni, hogy valamely jellemző tulajdonság rovására.

*Az A/D átalakítók legfontosabb statikus hibái a következők:*

- kvantálási hiba,
- jel-zaj viszony,
- ofszet hiba,
- erősítés hiba és a
- linearitás hiba. [122; 29. oldal]

*Az A/D átalakítók dinamikus hibáit a következő paraméterekkel lehet megadni:*

- a konverziós (átalakítási) idő és a mintavevő-tartó beállási idejének összege,
- pontosság,
- apertúradzsitter (mintavételezési idő bizonytalansága),
- különböző zajok. [122; 31. oldal]

A technikai megoldások lehetővé teszik nagysebességű és nagyfelbontású A/D átalakítók kialakítását, illetve azok tovább fejlesztését. Az ún. direkt (flash) A/D átalakítással a folyamat kb. 10 bites felbontásig történhet meg nagy sebességgel, míg ennél nagyobb felbontás esetére kialakításra kerültek az úgynevezett pipeline típusú átalakítók, „amelyekben több fokozatban kerül végrehajtásra az átalakítás. Minden egyes fokozatban egy kis felbontású A/D és egy D/A átalakító működik. A fokozatban a bemenő jelből kivonódik a kis felbontású jel a D/A átalakító segítségével.” [119; 27. oldal]

Fontos elem a nagy frekvenciatartomány miatt gondos tervezést igénylő tuner is, mivel a rendszernek néhány tíz MHz-től néhány GHz-ig terjedő frekvenciatartományba eső jelek vételére kell alkalmasnak lennie. Mindezt úgy, hogy egyszerre legyen gyors frekvenciabeállítású és kis fáziszajjal rendelkező. Megfelelő tartományi konverzió esetén képes lehet rádiótechnikai berendezések, vagy műholdakon folyó kommunikáció jeleinek vételére is. [123] A tunerek a vételi oldalon (digital-down conversion, DDC) demodulációt és az adásoldalon (Digital-Up-Conversion, DUC) modulációt hajtanak végre. A nagy számítási kapacitás igény miatt programozható logikai áramköröket, alkalmazás specifikus integrált

áramköröket<sup>96</sup> vagy szabadon (felhasználó által) programozható logikai áramkörti elemeket<sup>97</sup> alkalmaznak. Az alkalmazás specifikus integrált áramkörök esetében az egység a felhasználó által már nem módosítható, nem programozható. Mivel a tervezés folyamata bonyolult, emiatt csak kis bonyolultságú részekből lehet nagyobb bonyolultságú áramkört kialakítani. Az összetett programozható logikai eszköz egy logikai cellamátrixból és az összekötő rendszerből áll. Az elemek működését a felhasználó saját maga képes egy programozással meghatározni. Az FPGA jól alkalmazható bonyolult és nagyméretű áramkörök kialakításához. [124]

**A meglévő technológiai megoldások biztosítják, hogy a felhasználó által meghatározott elvárásoknak megfelelő rendszer kerüljön kialakításra.** Példaként mutatom be, hogy kialakítható olyan DDS<sup>98</sup> alapú vevőkészülék, amely a korábban már említett gyors reagálás és kis fáziszaj biztosítása mellett, 50-3500 MHz közötti üzemelve, 10 $\mu$ -os beállási idővel 100.000 hangolást képes végrehajtani másodpercenként. Ebben az esetben a vevőegység a vezérlő számítógéptől fizikailag elválasztva, külön egységben került elhelyezésre, ahol a tartományi konverziót végrehajtó A/D is elhelyezhető. A fenti paraméterekkel olyan söprési eredmény érhető el, amelynél a „*vevő nem korlátozza a szkennelést.*” [119; 39. oldal]

**A szoftverrádió koncepcióra már létezik további fejlesztési lépcső, ez a kognitív rádió.** A kognitív rádió az International Telecommunication Union (ITU) Radio Communication Study Group szerint „*Egy rádió vagy rendszer, amely érzékeli és figyelemmel követi a műveleti környezetét, és képes dinamikusan és automatikusan ezek szerint beállítani a saját működési paramétereit,*”<sup>99</sup>. [125] **Azaz a kognitív eszköz - amennyiben zavart vagy zavartatást észlel saját működésében - képes meghatározni a módosítandó paramétert, megválasztani a probléma elhárítása érdekében szükséges módosítást és azt végrehajtani.** A változtatás lehet például frekvenciaváltás, teljesítmény vagy egyéb más paraméter módosítása.

---

<sup>96</sup> Application-Specific Integrated Circuit, ASIC

<sup>97</sup> FPGA, Field Programmable Gate Array

<sup>98</sup> Direct Digital Syntheser - magas órajelből kisebb frekvenciájú komponensek szintetizálására alkalmazott áramkörti elem, amely analóg kimenő jelet biztosít a kimenetén.

<sup>99</sup> „A radio or system that senses, and is aware of, its operational environment and can dynamically and autonomously adjust its radio operating parameters accordingly”, a szerző fordítása.

Ahhoz, hogy a fenti feladatok végrehajtásra kerüljenek egy adott berendezés által, az alábbi elemek integrálására van szükség:

- spektrum figyelő-analizáló egység: az egység feladata az aktuálisan alkalmazott és lehetséges paraméterek alapján történő működés elemzése, a vett jellemzők továbbítása a kognitív egység részére;
- kognitív egység: a bejövő információk alapján dönt a szükséges paramétermódosításokról;
- végrehajtó egység: a beállított paraméterek alapján biztosítja a stabil üzemelést, illetve a kognitív egységtől kapott paraméterek alapján végrehajtja a meghatározott módosításokat és folytatja az üzemelést. [125] [126]

A fentiek alapján megállapítható, hogy **a kognitív rádió koncepció „kvázi” ellenfele az elektronikai zavarásnak, vagy pontosabban fogalmazva, megoldás az elektronikai zavarás által okozott problémára.** Az azonban mindenképpen fontos, hogy a kognitív rádió hatékony működéséhez egy nagyon precízen kialakított és folyamatosan pontosított frekvencia adatbázis szükséges.

A már említett 'Software Defined Radio' fórum az alábbi öt lépcsőben határozta meg a rádiórendszerek fejlődését.

- Hardverrádió<sup>100</sup>, melyben csak a részelemek fizikai cseréjével hajtható végre a fejlesztés.
- Szoftver kontrollált rádió<sup>101</sup>, melyben a kontroll funkciók érhetőek csak el a szoftverben, a jellemzőknek csak egy limitált része változtatható.
- Szoftver vezérelt rádió<sup>102</sup>, melyben a szoftverrel számos paraméter változtatható, ebbe beleértve a hullámformát, széles és keskenysávi műveleteket, stb.
- Ideális szoftverrádió<sup>103</sup>, amely az SDR-hez képest jelentős fejlesztéseket tartalmaz. Teljes mértékben digitális feldolgozás történik, kivéve az antenna és a mikrofon esetében.
- Végző szoftverrádió<sup>104</sup>, főként összehasonlítási céllal került létrehozásra. Elméletben számos kiegészítő szolgáltatást is biztosít, így például a felhasználó GNSS alapú követését. [127]

---

<sup>100</sup> Hardware Radio

<sup>101</sup> Software Controlled Radio (SCR)

<sup>102</sup> Software Defined Radio (SDR)

<sup>103</sup> Ideal Software Radio (ISR)

<sup>104</sup> Ultimate Software Radio (USR)



**A szoftverrádió technológiával működő eszközök hatékonyságának alapja a legkorszerűbb digitális jelfeldolgozó processzorok<sup>105</sup> és szabadon programozható logikai áramköri elemek beépítése<sup>106</sup>, amelyekkel a digitális adásmódokat széles tartományban kezelhetjük.** A DSP-k használatának számos előnye van, többek között a nagymértékű pontosság, a korábban már említett rugalmasság – amely által ugyanaz a hardver egy szoftvercserével számos feladatra alkalmazható – illetve az, hogy a korábban az analóg áramkörökkel megvalósíthatatlan alkalmazások is megvalósíthatók (adaptív szűrési algoritmusok, lineáris fázismenet). A programozható gate-array logikák alkalmazásának tervezésekor fontos szempont, hogy egy adott funkció megvalósításának határfoka két határ között mozog. *„Ha azt szeretnénk elérni, hogy kevesebb kivezetése legyen egy eszköznek, akkor összetettebb logikai blokkok használata szükséges, ami viszont az eszköz kihasználtságát rontja. Ha az adott függvényt egyszerűbb logikai blokkokkal próbáljuk megvalósítani, akkor a kivezetések száma növekszik, de az eszköz kapacitásának kihasználtsága sokkal jobb lesz. Szoftverrádiós eszközök szempontjából mindkét tulajdonság nagyon fontos, ezért cél egy optimum megtalálása.”*[124; 32. oldal]

**A szoftverrádiók a korábban már említett előnyökön kívül további szolgáltatásokat is biztosítanak,** így a korábbi rádiók által is biztosított beszéd és adatátvitel mellett megjelennek többek között az alábbi lehetőségek:

- „**valós idejű videó és a szélessávú videokonferencia;**
- **egységes harctéri helyzetkép;**
- **fejlett hely- és helyzetmeghatározás;**
- **hozzáférés a különböző hálózatokhoz, így az internet protokoll (IP) alapú hálózatokhoz, a műholdas rendszerekhez, a tűz- és manőver-vezetési, illetve a funkcionális adathálózatokhoz”.** [128]

Mielőtt továbblépnék az SDR koncepció különböző rendszerekben történő alkalmazására, mindenképpen fontos megvizsgálni a hullámforma leíró nyelv<sup>107</sup> kérdését is. A később bemutatásra kerülő angol szoftverrádió fejlesztések során kialakított hullámforma leíró nyelv egy egyszerű, valamennyi fejlesztő által könnyen alkalmazható megoldás volt. A kialakítása során számos, már korábban ismert programozási nyelvet és formulát

<sup>105</sup> DSP, Digital Signal Processor – Digitális jelfeldolgozási algoritmusok végrehajtására optimalizált processzor.

<sup>106</sup> FPGA, Field Programmable Gate Array – szabadon (felhasználó által) programozható logikai áramköri elem

<sup>107</sup> Waveform Description Language, WDL

felhasználtak, így például a funkcionális programozási nyelvet<sup>108</sup> (pl. Haskell, Miranda), az objektumorientált programozási nyelvet<sup>109</sup> (C++, Java, stb.), a blokk diagram nyelvet<sup>110</sup> (Cossap, Ptolemy, stb.), az állapotgép programozási nyelvet<sup>111</sup> (Argos, SDL, stb.), a szinkron programozási nyelvet<sup>112</sup> (Esterel, Lustre, stb.), illetve a programspecifikációt<sup>113</sup>. A felsorolt programnyelvek és ismeretek felhasználásával kialakított hullámforma leíró nyelv így képes *„elegendő szélességet biztosítani a specifikációs problémák teljes skálájának lefuttatásához, valamint az erőteljes paraméterezhetőség alapján a valóban újrafelhasználható specifikációs könyvtárak támogatására.”*[129] A hullámforma leíró programnyelv előnyeiként alább felsorolt szempontok fontosak a jövőben kifejlesztésre kerülő programnyelvek esetében is, annak érdekében, hogy mind az általános, mind a speciális célú hardvereket minél hatékonyabban támogatni lehessen. [129]

Ezen szempontok az alábbiak:

- kétértelműség eltávolítása;
- ellentmondások eltávolítása;
- egy végrehajtható referencia modell hozzáadása;
- megnövelt érthetőség;
- megnövelt újrahasználhatóság. [129]

### 2.2.2. Szoftverrádió fejlesztések az egyes nemzeteknél

Az SDR koncepció által nyújtott előnyöket számos hadsereg már alkalmazza saját eszközeiben vagy legalábbis már tett lépéseket a szükséges fejlesztések érdekében. A polgári életben kifejlesztett, a boltok polcáról levehető<sup>114</sup> alkatrészek, áramkörü elemek beépítése nagyban elősegíti a különböző fejlesztéseket, azonban a katonai alkalmazás sajátosságai (pl. extrém üzemi hőmérsékleti tartomány, rázkódás, por, stb.) miatt nem minden esetben lehet a boltok polcáról levett elemeket változtatás nélkül felhasználni.

Korábban is több példa volt elérhető arra, hogy **a NATO államok „nagy figyelmet fordítanak a REH eszközök folyamatos (további) fejlesztésére, főleg a saját nemzeti rádióelektronikai iparuk által gyártott (gyártásra tervezett) berendezésekkel.”** [100; 142. oldal] Természetesen ez nemcsak a NATO tagállamokra volt azonban igaz.

---

<sup>108</sup> Functional languages

<sup>109</sup> Object oriented languages

<sup>110</sup> Block diagram languages

<sup>111</sup> State machine languages

<sup>112</sup> Synchronous languages

<sup>113</sup> Specification languages

<sup>114</sup> Commercial-off-the-shelf, COTS

A különböző hadseregek, rendvédelmi erők több esetben az adott országban elérhető gyártóval közösen fejlesztenek ki szoftverrádió koncepción alapuló kommunikációs vagy nem-kommunikációs rendszert. A képesség más eszközökkel kombinálva is alkalmazásra kerülhet, például egy amerikai elképzelés alapján minden lövészkatonát ellátnának egy globális helymeghatározóval ellátott SDR-rel, amely folyamatosan képes lenne a katona pozícióját továbbítani a hadműveleti központ részére. [130]

**A szoftverrádió technológia korai időszakában mind a polgári, mind a katonai eszközök alapját azonban ugyanazon, a civil szférában elérhető elemek, A/D konverterek, DSP chipek, RF erősítők, kijelzők, tápellátó akkumulátorok és adattárolási egységek jelentették, melyek megfeleltek, vagy kismértékű módosítást követően megfelelhettek a katonai követelményeknek is.** Ezzel a katonai alkalmazás vonatkozásában jelentős fejlesztési erőforrások voltak megtakaríthatóak. A különbség a felhasználás módjában volt, mivel a polgári felhasználásra tervezett eszközök esetében általában egy viszonylag szűkebb frekvenciaspektrumban és állandó telepítési helyen történő üzemelés a cél. Ehhez képest a katonai változatok lényegesen nagyobb frekvenciatartományban működnek, legtöbbször mobil változatban, számos speciális hullámformát alkalmazva. Emiatt jelentős eltérés jelentkezett az antennák fejlesztésében, a polgári eszközökben alkalmazott kisméretű, adaptív antennák inkább a bázisállomások lefedési cellájában való üzemelésre kerültek kifejlesztésre, annak érdekében, hogy állandó körülmények között stabil, megbízható szolgáltatásokat legyenek képesek biztosítani.

A katonai követelményeknek való megfelelés érdekében több irányban történtek antennafejlesztések is, így például **„széles frekvenciatartományban üzemelő, megnövelt hatásos felületű antennák vagy kisméretű, fázisváltozásokra kevésbé érzékeny, könnyűsúlyú elektronikus hangolász antennák”** [117; 32. oldal] kifejlesztése érdekében.

A katonai fejlesztések kezdeti időszakából három jelentős fejlesztési irányt kell megemlíteni, ezek az amerikai, az angol és a német-francia programok. Az amerikai kutatás során a SPEAKEasy program kettő fázisból állt. Az első fázisában a teljes digitális frekvencia-átalakítás és a szélessávú jelfeldolgozás volt a cél, míg a második fázisban moduláris rádióelemeket integráltak egy nyitott architektúrájú adatsínen, hogy a megjelenő hullámformák fejlesztéséhez egy egyszerű hardverfelépítést határozzanak meg. Öt csoportban kezdődtek meg a fejlesztések, melyek tervezett felhasználói között ott volt a szárazföldi, a különleges, a légierő és a haditengerészeti komponens is. Az 1. csoport szoftverrádióiban a kézirádiókban hat, míg a hátirádiókban 10 hullámforma került eltárolásra a memóriában. A 2.

csoport fejlesztései dedikáltan az AN/PRC-148 kézirádióhoz kapcsolódott, míg az 5. csoport fejlesztései a felügyelet nélküli földi szenzorokhoz<sup>115</sup>, a pilóta nélküli repülő járművekhez<sup>116</sup>, a felügyelet nélküli földi járművekhez<sup>117</sup>, az intelligens lövedékekhez<sup>118</sup> és a hálózatos tűzősszpontosításhoz<sup>119</sup> kapcsolódnak. A szárazföldi haderőnem részére kézi, háti, és járműbe épített rádiók, a különleges komponens részére kézirádiók, míg a légierő és a haditengerészet részére fedélzeti rádiók kerültek kifejlesztésre.

A SpeakEasy programon kívül több más, az Amerikai Védelmi Minisztérium által finanszírozott program is elindult. Ilyen volt a Joint Combat Information Terminal (JCIT), a Global Mobile (GloMo), az Ultracomm vagy a Wideband Radio Networking (WRN) Program. A JCIT a Haditengerészeti Kutatólaboratórium<sup>120</sup> programja volt, amely egy korábbi rendszer továbbfejlesztésével 2 MHz – 2.5 GHz között üzemelt. Számos modulációs módban üzemelt (többek között AM, FM, SSB, BPSK, QPSK, CDMA, TDMA módokban<sup>121</sup>), szoftveresen újraprogramozható volt a különböző műveleti helyzetnek megfelelően. Az „összhaderőnemi harcászati rádiórendszer program”<sup>122</sup> felhasznalta az itt elért eredményeket. A DARPA által vezetett GloMo program célja a technológiák és technikák kifejlesztése és alkalmazásokba, hálózatokba és vezeték nélküli kapcsolatokba történő integrálása volt annak érdekében, hogy a felhasználók elérhessék és teljes mértékben kihasználhassák a Védelmi Információs Infrastruktúrában elérhető szolgáltatásokat. **A programban több mint húsz egyetem és ipari cég vett részt.** A szintén DARPA által vezetett Ultracomm program célja a SDR technológia további fejlesztése a méretcsökkentő technológiák alkalmazásával. A Wideband Radio Networking (WRN) Programban a cél egy új, szélessávú rádióhullámforma kialakítása volt a hozzá kapcsolódó elemekkel együtt, úgy hogy **a rendszernek újraprogramozhatónak, így funkciókban fejleszthetőnek kellett lennie minimális hardverváltoztatással, mindezt a boltok polcáról levehető alkatrészek, áramköri elemek<sup>123</sup> felhasználásával.** [117; 33-34. old.] Napjainkban az amerikai

<sup>115</sup> Unattended Ground Sensors, UGS

<sup>116</sup> Unmanned Aerial Vehicle, UAV

<sup>117</sup> Unattended Ground Vehicles, UGV

<sup>118</sup> Intelligent Munitions

<sup>119</sup> Network Fires, Netfire

<sup>120</sup> Naval Research Laboratory (NRL)

<sup>121</sup> AM: amplitúdómoduláció, FM: frekvenciamoduláció, SSB: Single Side Band modulation – egy oldalsávú moduláció, BPSK: Binary Phase Shift Keying – kétállapotú fázisbillentyűzés, QPSK: Quadrature Phase-Shift Keying – 4 állapotú fázisbillentyűzés, CDMA: Code Division Multiple Acces – kódosztásos többszörös hozzáférés, TDMA: Time Division Multiple Acces – kódosztásos többszörös hozzáférés.

<sup>122</sup> Joint Tactical Radio System (JTRS)

<sup>123</sup> Commercial-off-the-shelf, COTS

kommunikációs tervek már rögzítik, hogy **a szoftverrádiónak be kell épülnie a C4ISR<sup>124</sup> infrastruktúrába**, annak elemeiben kiemelt szerepet kap a már korábban ismertetett képességek, szolgáltatások biztosításával. [128]

Az angol szoftverrádió fejlesztések során a fő hangsúlyt a szoftverek fejlesztésére fordították, például új szoftveres hullámformák, üzemelési és alkalmazói szoftverek létrehozására. Kifejlesztésre került a korábban már említett hullámforma leíró nyelv, amely a szimulációs és a végrehajtási (felhasználói) környezetben alkalmazható hullámformák kidolgozását segíti. A német-francia szoftverrádió kutatás főként **katonai beszállító cégek közötti kooperációban fejlesztett többfunkciós, többsávós rádiók (MMR) fejlesztését, gyártását jelentette** az Eurorádió program keretében. Az Eurorádió program – amely egyúttal Európa leglényegesebb szoftverrádiós fejlesztési programja – figyelembe veszi a polgári felhasználók jelenlétét, igyekszik számukra az interoperabilitást biztosítani. Erre egy példa a TETRA rendszer és a német Rohde & Schwarz cég M3TR<sup>125</sup> nevű, **többsávós – több üzemmódú – többcélú** szoftverrádiója közötti interfész kialakítása. Többsávós, mivel a 1,5 – 108 MHz, és a 20 – 512 MHz sávban képes üzemelni. Több üzemmódú, mivel a letölthető katonai és civil hullámformáknak köszönhetően nagy sebességű adatátvitelre képes (5,4 – 9,6 kbps RH-n és 64 kbps URH-n), valamint digitálisan kódolt, 16 kbps CVSD<sup>126</sup> hangátvitelt biztosított. A többcélú jelentés tartalma a műholdas, a GPS és a LAN, ISDN és intranet vagy internet szolgáltatások lehetősége. Ebben a fejlesztésben *„a harcászati (tábori) kommunikációs rendszerben a szoftverrádió csomópontként szerepelt, rugalmas hálózatkonfigurálást és fejlett információvédelmet biztosítva az interoperabilitás mellett, míg a szoftverrádió terminálok a szoftveralapú hullámformák révén a különböző harctéri helyzetekre kialakított harcászati rádióhálókból és fegyverirányítási rendszerekben kapnak szerepet.”* [117; 36-37. oldal]

**Napjainkban az SDR kommunikációs és nem-kommunikációs rendszerekbe történő beépítése továbbra is tendencia.** A Harris cég 2013-ban elnyerte a U.S. Army pályázatát egy új, gépjárműves rádiórendszer kialakítására vonatkozóan, ennek alapja a Falcon III szélessávú rádiótechnológia, amely teljesíti az amerikai védelmi minisztérium által

<sup>124</sup> C4ISR, Command, Control, Communications, Computer, Intelligence, Surveillance, Reconnaissance: Vezetési, Irányítási, Hírközlési, Számítógépes, Hírszerző, Megfigyelő és Felderítő rendszerek információit egyesítő integrált híradó és informatikai rendszer.

<sup>125</sup> Multiband, Multimode, Multirole Tactical Radio, Többsávós, több üzemmódú és többcélú harcászati rádió

<sup>126</sup> Continuously variable slope delta, folyamatosan változó meredekségű delta modulációjú hangkódolás

meghatározott, az összhaderőnemi harcászati rádiórendszerre<sup>127</sup> vonatkozó követelményeket.

[131] A német hadsereg részére a Rohde & Schwarz cég fejlesztett ki SDR alapú rendszert.

[132] **Az SDR elv az elektronikai hadviselési eszközökben is jelen van**, erre számos példát találhatunk a különböző gyártók termékpalettáján.

Természetesen Oroszországgal kapcsolatban is számos hírt találhatunk arról, hogy az SDR technológiát alkalmazzák katonai eszközeikben. 2014-ben jelentette be Khalil Arslanov dandártábornok, az orosz védelmi erők kommunikációs igazgatóságának főnöke, hogy foglalkoznak ilyen irányú fejlesztésekkel és rövidesen a védelmi erők és a helyi szervezetek felszerelésre kerülnek olyan SDR alapú eszközrendszerekkel, amelyeket már sikeresen használtak a 2014-ben, Szocsiban rendezett olimpia biztosítása során. [133]

A finn nemzeti SDR program lényege az volt, hogy a nagy intenzitású katonai vagy békefenntartó műveletekben történő hatékony alkalmazhatóság mellett a rendszer biztosítsa a katonai, a katasztrófavédelmi és a nem-kormányzati szervezetek közötti interoperabilitást is. [134]

**Fontos azt is megjegyezni, hogy az SDR alkalmazása nem öncélú, szorosan kapcsolódik olyan követelményekhez/feltételekhez, melyek biztosítják a szükséges feltételeket a működéshez, illetve egyben követelményt, igényt támasztanak a szoftverrádió nyújtotta szolgáltatások további fejlődéséhez:**

- **digitális harcmező**, melynek lényege, hogy a kommunikáció az adott szinteken horizontálisan, a szintek között pedig vertikálisan megvalósuljon;
- **a műveletek maximális információval való ellátása**, a művelet minden fázisában, előreprogramozott, zavarásmentes üzemmódokban;
- **a kommunikációs eszközök gyors telepítése és alkalmazása;**
- **önkonfigurációra és automatikus üzemelésre képes rádiórendszerek** kifejlesztése és alkalmazása;
- **maximális interoperabilitás;**
- **integrált hálózatmenedzsment.** [117; 37-38. oldal]

Fejlett elektronikai hadviselési eszközökre a Magyar Honvédségnek is szüksége van. Példaként említeném a folyamatos fejlesztésre azt, hogy már a JAS-39 Gripen – amely a modern negyedik generációs repülőgépek közé tartozik – önvédelmi célú elektronikai

---

<sup>127</sup> Joint Tactical Radio System, JTRS

hadviselési rendszeréhez is érhetőek el – a könyvtárrendszerek szerkesztését támogató rendszerek vonatkozásában – újabb fejlesztések.

**Egy-egy ország elektronikai hadviselési eszközeinek fejlesztésére** többféle megoldási lehetőség van, **beszerzésre kerülhet valamely gyártó által már kifejlesztett termékcsalád, illetve a saját ipar bevonásával kifejlesztésre kerülhet egy saját termékpaletta.** Egy gyártó termékeinek választásának előnye, hogy a beszerzési eljárást követően rövid időn belül rendelkezésre áll, minimális, a felhasználó igényeit kielégítő módosításokat követően használatba vehető. Ebben az esetben azonban az is fontos, hogy más ország is megismerheti a kérdéses technika képességét, rosszabb esetben paramétereit. Biztonsági kérdésként merül fel továbbá az is, hogy milyen egyéb programok kerülnek/kerülhetnek telepítésre a tudtunk nélkül, így például az úgynevezett back-door programok. Saját fejlesztés esetén az alkalmazásba vétel időpontja a fejlesztés ütemétől és sikerességétől függ. Ezen megoldás előnye viszont az, hogy más országok előtt nem lesz ismert a rendszer minden képessége, csak az, amit a tesztelés és a saját alkalmazás esetén megismerni engedünk. Az MH vonatkozásában a fenti kérdések vizsgálata mellett fontos érv az a kormányzati szándék is, amely a magyar ipar felélesztésére irányul. Erre a korábbi programok helyett jelenleg a 2017-ben elindított Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program [135] szolgálhat.

### 2.2.3. Harcászati rádiók

A harcászati rádiók, rádiórendszerek fejlődésére nemcsak a technikai fejlesztések, de akár a jelentősebb történelmi események is jelentős befolyással lehetnek. Adrian Graham szerint a berlini fal 1989. évi leomlása alapjaiban változtatta meg az addigi katonai rádiókkal szemben támasztott követelményeket. A korábbi vízió, amely a Nyugat-Európa elleni agressziót vélelmezte, hirtelen a múlté lett. Már ekkor megjelent azon vélemény, miszerint a későbbi háborúkat távoli helyszíneken vívják majd, illetve az, hogy a nagy intenzitású műveletek realitása jelentősen lecsökkent. Felmerült azon elvárás is, hogy a távoli területeken rendkívül rossz körülmények között is biztosítani kell az összeköttetést a vezetési elemek és a csapatok között, illetve képesnek kell lenni a légítámogatást biztosító repülőerőkkel történő kapcsolat felvételre. Fontos az is, hogy már nemcsak hangkapcsolat, de a képek és adatok átvitelére vonatkozó elvárás/igény miatt egyre nagyobb sáv szélesség biztosítása is szükségessé vált. **Mindezen elvárásokat pedig úgy kell kielégíteni, hogy az is szempont, hogy a katonai eszközöknek együtt kell működni a szintén üzemelő polgári rendszerekkel.** [136]

A fenti események mellett természetesen nem felejtkezhetünk el a technikai fejlesztések hatásairól sem. A harcászati rádiók könnyű felfedése és lehallgathatósága már a múlté. Napjaink fejlett technikai világában a rendelkezésre álló, a rádiórendszerek megbízhatóságát növelő megoldások már beépítésre kerülnek az új fejlesztésű rendszerekbe. Ilyen megoldás például a kiterjesztett spektrumú adásmódok alkalmazása, amelyek többek között az alábbiak lehetnek:

- *fázisugratásos vagy direkt szekvenciális mód (Direct-sequence Spread Spectrum Technique – DS-SST);*
- *frekvenciaugratásos mód (Frequency-hopping Spread Spectrum Technique – FH SST);*
- *időugratásos mód (Time-hopping Spread Spectrum Technique – THSST);*
- *pulzus-FM mód (Chirp Spread Spectrum Technique – Chirp-SST);*
- *vegyes eljárás, ami az előbbiekből kombinációjából állítható elő.*” [103; 14. oldal]

A fenti adásmódok kategorizálhatóak úgy is, mint kis valószínűséggel felderíthető<sup>128</sup>, kis valószínűséggel észlelhető<sup>129</sup> vagy kis valószínűséggel megfejthető/kiaknázható<sup>130</sup> adásmódok. A három jel karakterisztikája eltér egymástól. LPI típusú technika például a frekvenciaugratásos mód<sup>131</sup>. LPD típusú technika a direkt szekvenciális mód<sup>132</sup>. Ilyen eljárást alkalmaznak a kódosztásos többszörös hozzáférési moduláció<sup>133</sup> esetében. Szintén LPD típusú technika az időugratásos mód<sup>134</sup>. [137]

Fontos azt is megjegyezni, hogy **a fejlett rádiókat, rádiórendszereket már nemcsak hangátvitelre használhatjuk**, hanem a szükséges egyéb elemek megléte esetén **adatátvitelre** (műveleti parancsok<sup>135</sup>, tűztámogatási tervek<sup>136</sup>, logisztikai jelentések, harcászati helyzetismeret<sup>137</sup>, videók, egyéb adatok, stb.) is különböző adatátviteli sebességgel, de **rendelkezhetnek beépített globális helymeghatározóval**. A felsorolt feladatok során természetesen különböző kimenő teljesítménnyel, titkosítási lehetőséggel üzemelhetnek úgy, hogy akár beépített, akár sivatagi környezetben vagy dzsungelben is használhatóak legyenek

<sup>128</sup> Low Probability of Interception, LPI

<sup>129</sup> Low Probability of Detection, LPD

<sup>130</sup> Low Probability of Exploitation, LPE

<sup>131</sup> Frequency-hopping Spread Spectrum Technique, FHSST

<sup>132</sup> Direct-sequence Spread Spectrum Technique, DSSST

<sup>133</sup> Code Division Multiple Access, CDMA

<sup>134</sup> Time-hopping Spread Spectrum Technique, THSST

<sup>135</sup> Operation order, OPORD

<sup>136</sup> Fire support plan

<sup>137</sup> Situational awareness, SA



megfelelő zavarállósággal. Képesek lehetnek önállóan vagy hálózatban, autonóm vagy távvezérelt módon, de akár átjátszóként is üzemelni. Emellett azt is szükséges biztosítani, hogy az egyes rendszerek lehetőség szerint képesek legyenek egymással együttműködni.

A különböző rádiórendszerekhez különböző hullámformák kerültek kialakításra. A legismertebbek a hagyományos AM és FM modulációk, a SINCGARS<sup>138</sup>, a HaveQuick I. és II., a SATURN, a JTRS<sup>139</sup>. A hullámforma a szoftverrádió esetében magában foglalja a „*készülék-specifikus modulációs módot, a jelpolarizáció értékét, a forrás- és csatornakódolást illetve dekódolást, a hibajavítást, az időzítési paramétereket, a bemenet /kimenet (Input/Output, I/O) interfész vezérlő információit, valamint a rendszer üzemeltetéséhez és az alkalmazások futtatásához szükséges adatokat is*”. [117; 28. oldal]

A rádiók esetében mindenképpen meg kell említenünk az antennákat is. Természetesen itt sem alkalmazhatjuk teljes mértékben a polgári életben alkalmazott antennákat, mivel sok esetben a katonai felhasználásból származó igénybevétel (nagyobb üzemi hőmérséklet tartomány, por és rázkódás) jelentősebb.

Ez kihat az antennákkal szemben támasztott követelményekre is, esetükben alapvetés, hogy „*az antennák képesek legyenek a frekvenciaváltozások okozta fázis és amplitúdó eltéréseket lekezelni*”. [117; 32. oldal] Ez akkor valósítható meg, ha a beépített elemek képesek széles frekvenciatartományban, minőségromlás nélkül biztosítani az adott és vett jelek áramlását.

Ahhoz, hogy a megfelelő antennát válasszuk ki, számos szempontot figyelembe kell vennünk. Ezek között van az adott frekvenciatartományra jellemző terjedés és az azt befolyásoló tényezők változása, az áthidalható távolság és a műveleti környezet jellemzői.

A rövidhullámú eszközök alkalmazásával tudjuk a legnagyobb távolságokat áthidalni, a kisebb távolságokon a felületi hullámok, nagyobb távolságokon pedig a térhullámok útján történik a jelterjedés. A rövidhullámok esetében a jelterjedést az ionoszféra állapota befolyásolja, emiatt fontos, hogy az ionoszféra állapota napszakonként és évszakonként eltér, amelyet a megfelelő minőségű kapcsolat érdekében figyelembe kell venni. Az ionoszféra különböző rétegei (D-réteg, E-réteg, F-réteg) különböző mértékben befolyásolják a jelterjedést. Az ultrarövid hullámok terjedésével kapcsolatban kvázioptikai jelterjedésről beszélhetünk. Ennek egyik legfontosabb jellemzője, hogy amennyiben a jel az optikailag sűrűbb közegből kisebb sűrűségű közegbe lép, akkor az átlépési pontban emelt merőlegetől

<sup>138</sup> Single-Channel Ground and Airborne Radio System

<sup>139</sup> Joint Tactical Radio System

elfelé törik. Az ultrarövid hullámok esetében is beszélhetünk nagyobb távolságok áthidalásáról, az ionoszférikus szórthullám-terjedés esetén a 25-60 MHz közötti frekvenciatartományban 1000-2500 km között lehet. [138]

**Az antennaválasztást a katonai alkalmazás során befolyásolhatja az is, hogy milyen műveleti környezetben fogjuk alkalmazni az adott eszközöket,** legyen az hideg időjárási, dzsungel, sivatagi vagy hegyvidéki terület, de külön elemzést igényel a beépített, lakott területen történő alkalmazás. Például a beépített, lakott területen történő alkalmazást számos tényező befolyásolja, korlátozza, így az ellenséges tevékenység miatt kisebb az alkalmazható teljesítmény, az elérhető átjátszók száma, kommunikálni kell az épületek között és az épületekben is. Az ilyen komplex körülmények természetesen nemcsak a beépített/lakott környezetre igazak, számos, sok esetben egyedi, az adott környezetre jellemző nehezítő körülmény lép fel. [139]

A harcászati rádiók esetében arról sem szabad elfelejtkeznünk, hogy a rádióeszközök/terminálok szinkronizációja a globális helymeghatározó rendszerek üzemképességétől is függ, mellyel a következő alfejezetben még foglalkozom.

#### **2.2.4. Globális helymeghatározó rendszerek**

A globális helymeghatározó rendszerek esetében gyűjtőfogalomként sokszor tévesen a GPS megnevezést alkalmazzák, amely az amerikai fejlesztésű rendszertől (Navigation System with Timing and Ranging Global Positioning System, NAVSTAR GPS) származik. A globális helymeghatározó rendszer hivatalos neve a Global Navigation Satellite Systems (GNSS). A négy legnagyobb GNSS rendszer az amerikai NAVSTAR GPS, az orosz GLONASS, az Európai Unió által fejlesztett GALILEO és a kínai COMPASS. A GNSS jel erősségét számos tényező befolyásolhatja, így például a lakott vagy ipari környezet, de akár a Föld mágneses terét megváltoztatni képes geomágneses viharok.

A globális helymeghatározó rendszerek alkalmazásának célja a helymeghatározás és a pontos idő szolgáltatása, emiatt alkalmazzák esetükben a PNT<sup>140</sup> jelzöt. [140]

Általánosságban elmondható, hogy a GNSS rendszereknek három eleme van, ezek az űrben lévő, a földi irányító és a felhasználói elem. Az űrszegmens a rádiójeleket a felhasználóhoz továbbító műholdrendszert foglalja magában. Az irányító rendszer egy olyan földi hálózatot jelent, amely ellenőrzi a műholdak mozgását, jelkibocsátását és szükséges esetén beavatkozik. [141]

---

<sup>140</sup> Positioning, Navigation, Timing – pozíció, navigáció, pontos idő

Az amerikai NAVSTAR GPS pontos működése érdekében az Amerikai Egyesült Államok legalább 24 műhold üzemelését biztosítja azok üzemidejének 95 %-ában. Ennek érdekében több műhold van az űrben, 2017. április 18-án 31 darab. [142]

Az orosz GLONASS (Globalnaya navigatsionnaya sputnikovaya sistema) rendszer 1982-ben kezdte meg a működését és 1993-ig 24 műhold került pályára állításra. Pénzügyi okok miatt volt egy rövid idejű üzemelési szünet, azonban ez megoldódott, mivel a rendszer megléte és fenntartása az orosz kormány részéről prioritás volt. Jelenlegi fejlesztési célok között a pontosság növelése, a megbízhatóság és az üzemelési költségek csökkentése szerepel. [143]

Az Európai Unió és az Európai Űrügynökség (European Space Agency, ESA) által fejlesztett GALILEO rendszer 30 műholdat tartalmaz. A fejlesztés célja Európa függetlenségének biztosítása más GNSS rendszerektől és az azokat üzemeltető államoktól. [144]

A kínai BeiDou, más néven COMPASS műholdas navigációs rendszer célja pedig Kína ilyen vonatkozású függetlenségének biztosítása, valamint az ázsiai térség lefedettségének biztosítása. [145]

| Rendszer             | Első műhold pályára állítása | Aktív üzem | Aktív műholdak száma |
|----------------------|------------------------------|------------|----------------------|
| <b>GPS (USA)</b>     | 1978                         | 1993       | 24                   |
| <b>GLONASS (RUS)</b> | 1982                         | 1993/2011  | 24                   |
| <b>COMPASS (CHI)</b> | 2007                         | 2011       | 23                   |
| <b>GALILEO (EU)</b>  | 2011                         | 2011       | 11                   |

2.1. táblázat: Globális helymeghatározó rendszerek alapadatai a 2018. 08. 24-i helyzetnek megfelelően. [146] [147]

**Az SDR technológia a GNSS rendszerfelhasználói szegmensébe, azaz a vevőkészülékekbe került beépítésre, így képesek kettő vagy több GNSS rendszer jelének vételére.** Az amerikai Légierő Kutató Laboratórium (U.S. Air Force Research Laboratory, AFRL) és a GPS Igazgatóság (GPS Directorate) megbízásából került kidolgozásra a Secure Software Defined Radio (S-SDR) GNSS vevő képesség, melynek célja maximális pontosság elérése a magas szintű jelszint biztosítása mellett. [148]

**A GNSS rendszerek a fejlődésüktől kezdve jelentős változásokon mentek keresztül és úgy váltak mindennapi életünk részévé – beépítve a különböző eszközeinkben – hogy arról a hétköznapi emberek nem is tudnak. Vég nélkül lehetne**

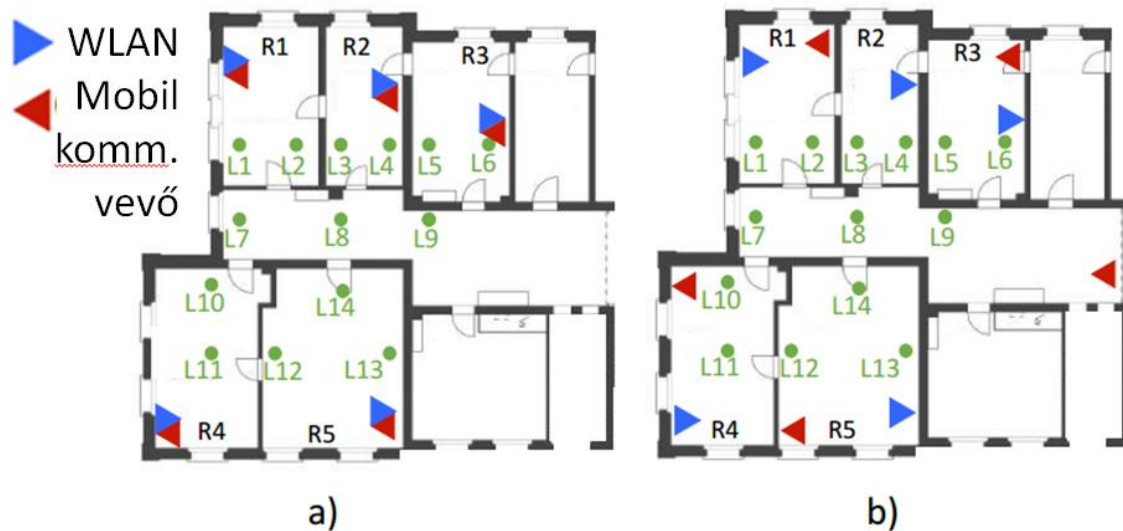
sorolni azon eszközöket, melyekben jelen van valamely GNSS vevő, legyen az egy okosóra, mobiltelefon, bankautomata, közlekedési eszközök, katonai berendezések, stb. Fontos azt is kihangsúlyozni, hogy GNSS rendszer által nemcsak nagy pontosságú helymeghatározás lehetőségét biztosító jel, hanem a különböző eszközök számára alapvető fontosságú órajel is kisugárzásra kerül. Ez az órajel az, ami nagyon sok eszköz és rendszer egymással történő együttműködésének, szinkronizációjának az alapja. A harcászati rádiók esetében például a műholdak órajel-frekvenciába kódolt szekvencia hiánya interoperabilitási problémákat okozhat. Természetesen **további fejlesztések is vannak az SDR és a GNSS technológia kombinálására** annak érdekében, hogy a kettő rendszer által biztosított képességek hatványozottan kerüljenek kihasználásra.

**Fontos** azonban azt is figyelembe venni, hogy **számos esetben, sűrűn beépített vagy zsúfolt ipari környezetben a GNSS rendszerek jelének vétele nem biztosított, a rálátás<sup>141</sup> nincs meg.** Ebben a témában is folyik kutatás, amelynek eredménye – megfelelő kiegészítéssel katonai célú alkalmazássá is fejleszthető – **az SDR alapú eszközbe épített WLAN és mobil kommunikációs vevő helymeghatározási célokra történő felhasználása.** Kutatások és eszközfejlesztések irányulnak arra, hogy az említett kommunikációs csatornákat felhasználva – az egyes módszerekre jellemző előnyöket és hátrányokat figyelembe véve – belső térben (pl. kórházakban, üzemekben) az egyes eszközök alapján a keresett személy helyzete megállapítható legyen. A tesztelés során WLAN és mobil kommunikációs antennák alkalmazásával, kettő darab Google Nexus Smartphones felhasználásával. A feladat során két antennatelepítést teszteltek, az első esetben azonos, míg a második esetben különböző helyekre telepítették a WLAN és a mobil kommunikációs antennákat. Az antennák telepítése a 2.3. ábrán látható, az a) jelű az azonos, a b) jelű a különböző telepítési helyeket mutatja.

[149]

---

<sup>141</sup> Line of Sight, LoS



2.3. ábra: A hibrid helymeghatározó rendszer tesztkörnyezetének felépítése. [149]

A teszt során külön vizsgálták a mobil kommunikációs alapú, a WLAN alapú és a hibrid megoldás által generált pontatlanságot. Az első kettő esetben hét, a harmadik esetben 14 helyen végeztek méréseket, minden helyszínen 45 percig tartó folyamatos mobil kommunikációs és WLAN forgalmat generáltak. A vett jelek erőssége és a kalkulált távolságok alapján adatbázist hoztak létre, melyek elemzését követően az alábbi megállapításokat tették:

- A mobil kommunikációs alapú helymeghatározás esetén az átlaghiba az antennák azonos helyre történő elhelyezése esetén 3.41 méter, különböző helyekre történő telepítés esetén 3.20 méter volt.
- A WLAN alapú helymeghatározás mindkettő esetben 2.61 méter volt az átlaghiba.
- Hibrid alapú helymeghatározás során az átlaghiba az antennák azonos helyre történő elhelyezése esetén 1.95 méter, különböző helyekre történő telepítés esetén 1.71 méter volt. [149]

A fenti eredmények a különböző katonai felhasználási területek vonatkozásában is fontosak, azonban ebben az esetben törekedni kell a még nagyobb pontosság elérésére.

### 2.2.5. Vezeték nélküli kommunikációs és adatátviteli rendszerek

Az elmúlt évtizedekben a kisebb-nagyobb távolságot áthidalni képes vezeték nélküli adatátviteli rendszerek is jelentős fejlődésen mentek keresztül. Ez a fejlődés magában foglalta a különböző eljárások és a működést biztosító hardver módosulását. Ebben az alfejezetben a mobiltelefon-rendszerek és néhány, a katonai felhasználás vonatkozásában

fontos vezeték nélküli megoldás fejlődését vizsgálom. Természetesen nem állt meg a fejlődés, napjainkban is folyamatosan jelennek meg újítások.

### Mobil telefonrendszerek

A mobiltelefonia fejlődése az Európában egyeduralkodónak tekinthető 450 és 900 MHz-es első generációs mobil távközlési rendszerrel kezdődött, melyet a hang és keskenysávú adatátvitelre képes második generációs GSM rendszer követett. Az előfizetők számának rohamos növekedése miatt a GSM rendszerben az elterjedt 900 MHz mellett alkalmazni kezdték az 1800 MHz-et is. Itt is egyértelműen látható, hogy az alkalmazott technológia változtatása, módosítása a technikai eszközök fejlődésével együtt történik. A mobiltelefonok mérete a kezdeti időszak aktatáskányi méretéről az évek során karóraméretűvé zsugorodott úgy, hogy az eszközök által biztosított szolgáltatások jelentősen kibővültek, hiszen napjaink okostelefonjainak alkalmazásai között már megtalálható a fényképezőgép, naptár, zene és videolejátszás, Bluetooth és WLAN adatkapcsolati lehetőségek, GNSS alkalmazás is.

Az adatátvitel fejlődése során számos szabvány került bevezetésre a Nemzetközi Távközlési Egyesület (International Telecommunication Union, ITU) által. Ezek között van a HSCSD (High Speed Circuit Switched Data), a GPRS (General Packet Radio Service), az EDGE (Enhanced Data GSM Environment), az UMTS (Universal Mobile Telecommunications System).

A HSCSD fejlődését igazából a mobilhálózatok adatátviteli képességét kihasználó laptopok fejlődése generálta. Bevezetésével megtörtént a kódolás javítása, amivel az átviteli sebesség megnövekedett, valamint akár 4 beszédcsatorna is felhasználható volt. A rendszer hátránya az volt, hogy a felhasználó részére biztosított volt mindaddig, amíg ő nem bontotta a kapcsolatot, akkor is, ha nem volt adatforgalom a csatornán. A HSCSD hátrányát küszöbölték ki a GPRS bevezetésével, amely a csomagkapcsolt Időosztásos Többszörös Eléréses (Time-division multiple access, TDMA) kommunikációs módszert alkalmazta. A GPRS-nél több felhasználó egyszerre használhatja ugyanazt a csatornát, hiszen csak akkor van adatforgalom, amikor van továbbítandó adat. A fentiek miatt webes elérés, email fogadás vagy üzenetküldés esetén GPRS, míg letöltés esetén a HSCSD kerül alkalmazásra. Az EDGE egy olyan nagy sebességű adatátviteli szabvány, amely a korábban alkalmazott modulációs módok megváltoztatásával nyújt nagyobb adatátviteli sebességet ugyanazon a 200 kHz-es sávszélességen. Az EDGE hátránya, hogy sokkal jobb minőségű rádiós jelet igényel, mint a hagyományos GSM kommunikáció, így további bázisállomások felállítása vált szükségessé.

A működő mobil kommunikációs szolgáltatók számára az UMTS szolgáltatás bevezetése jelentős pénzügyi forrásigénnyel járt a frekvencia használati engedély megvásárlása és a szükséges rendszerfejlesztések miatt. További problémát jelentett az mobiltelefonok alacsony akkumulátor kapacitása és az, hogy a tényleges sebességet csak úgy tudja az UMTS biztosítani, ha viszonylag kis távolságban van elérhető bázisállomás. [124; 11-18. old.]

**A szoftverrádiós technológia a mobiltelefonok esetében a bázisállomásokban került felhasználásra, így a hardver képes többféle rádiótechnológiát kezelni párhuzamosan és azok között dinamikusan váltani.** [150]

A GSM telefonrendszerek mellett további rendszerek is kialakításra kerültek, melyek szintén folyamatos fejlesztéseken mennek keresztül.

Vezeték nélküli helyi kiterjedésű hálózat (WLAN)<sup>142</sup>

*„A WLAN hálózatok olyan összetett hardver-szoftver rendszerek, melyek alkalmasak egy már meglévő hagyományos Ethernet, LAN<sup>143</sup> hálózat vezetékes nélküli kiterjesztésére, mely a felhasználók számára kényelmes, nagysebességű és biztonságos adatkapcsolat létrehozását teszi lehetővé az említett hálózatokkal megegyező szolgáltatási színvonal biztosítása mellett.”* [151]

A Villamos- és Elektronikai Mérnökök Intézete<sup>144</sup> kidolgozta a WLAN rendszerekre vonatkozó nemzetközi szabványokat, melyek többek között tartalmazzák az átviteli sebességeket és az alkalmazott frekvenciasávokat. Ilyen szabvány többek között az IEEE 802.11, az IEEE 802.11a, az IEEE 802.11b és az IEEE 802.11g szabvány.

Az IEEE 802.11, az IEEE 802.11b és az IEEE 802.11g szabványok üzemi frekvenciája az ipari, tudományos és orvosi sáv (Industrial, Scientific and Medical, ISM band) 2,4 GHz-es tartományába esik. Mivel a frekvenciasáv használata ingyenes, így nem kell engedély annak használatához, azonban egyúttal ez a hátránya is, hiszen bárki más is használhatja ezt a frekvenciasávot a közelünkben. Fontos tudni azonban azt is, hogy az ilyen eszközök jogszabályban maximalizált teljesítménnyel üzemelhetnek csak. Annak érdekében, hogy ne forduljon elő interferencia, kettő technika kerül ezen eszközökben alkalmazásra, ezek a frekvenciaugratásos, szórt spektrumú (Frequency Hopping Spread Spectrum, FHSS), illetve a közvetlen sorrendű, szórt spektrumú (Direct Sequence Spread Spectrum, DSSS) moduláció.

<sup>142</sup> WLAN, Wireless Local Area Network

<sup>143</sup> Local Area Network, Helyi Hálózat

<sup>144</sup> IEEE, Institute of Electrical and Electronic Engineers

A WLAN hálózatok alkalmazása rendkívül elterjedt, bárhol kapcsolódhatunk – természetesen amennyiben az beállításra került, akkor az adott hálózatban érvényes jelszó birtokában – ezekhez, például repülőtereken, üzletekben, munkahelyi hálózatokban vagy az úgynevezett nyílt hotspot-okhoz.

### Bluetooth

A Bluetooth adatkapcsolat szintén a 2,4 GHz-es tartományban üzemel. Lényeges, hogy a WLAN nagyobb távolságon, míg a Bluetooth kisebb távolságon használható az eszközök összekapcsolására. Pont ez a kis hatótávolság az, amely a zavarhatóságát gátolja. Egy hálózatban maximum 8 eszköz vehet részt, úgynevezett Personal Area Network-öt (PAN) hozva létre.

A Bluetooth által alkalmazott master-slave típusú összeköttetésben egyszerre egy master és több slave eszköz lehet. A master feladata az ugratási szekvencia meghatározása, ehhez szinkronizálnak a slave egységek. A kialakított hálózatok csatorna felhasználása is nagyban támogatja a magas fokú zavarállóságot. [152]

### WIMAX

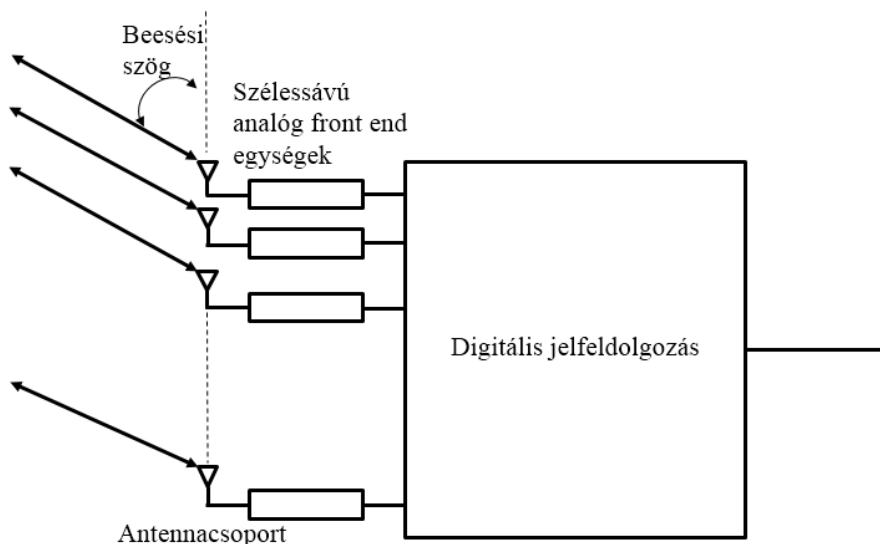
A WIMAX egy fix szélessávú vezeték nélküli kapcsolatot nyújtó szabvány (IEEE 802.16), amely a WLAN és a Bluetooth adatátvitelhez képest nagyobb távolságon nagy adatátviteli sebességet tesz lehetővé. A WIMAX esetében már több tíz kilométeres átviteli távolságokról beszélhetünk úgy, hogy nem szükséges a közvetlen rálátás. Hatékonyan alkalmazható mind városi, mind pedig vidéki területeken is. A WIMAX csatornakódolást, valamint adaptív BPSK, QPSK vagy QAM modulációt alkalmaz. A rendszerben használt ortogonális frekvenciaosztásos multiplexálás (OFDM, Orthogonal Frequency Division Multiplexing) kisebb távolságokon (4-6 km) sokkal előnyösebb átvitelt tesz lehetővé a WLAN és a Bluetooth hálózatokhoz viszonyítva.

Fontos azonban az is, hogy az OFDM csak idődimenzióban képes a többszörös hozzáférést megvalósítani (egy időszakban az egyik, a következő időszakban a másik állomás kommunikál), melynek fejlettebb változata az OFDMA (Orthogonal Frequency Division Multiple Access, ortogonális frekvenciaosztásos többszörös elérés) moduláció. Ebben az esetben, egy időben több eszköz is használhatja az adott sáv szélességet, akár aszimmetrikus elosztással, akár időosztásos alapján, mivel az OFDMA rendszerben a hozzáférések időben és frekvencián is osztottak. [152]



A fenti vezeték nélküli rendszerek elemzése az értekezés szempontjából azért fontos, mivel egyrészt ezeknél is alkalmazásra került a szoftverrádió technológia, másrészt pedig a harmadik fejezetben az SDR alapú elektronikai hadviselési rendszerek közötti adatátvitelnél még foglalkozom velük.

Mindegyik – az ebben a fejezetben ismertetett – rendszernél fontos a megfelelő antennarendszer kialakítása, mivel a szoftverrádió technológia alkalmazásával jóval nagyobb frekvenciaspektrumot vagyunk képesek átfogni, ugyanazon rendszer más-más alkalmazás futtatására is alkalmas. Emiatt nem elegendő szélesebb frekvenciatartományban üzemelő antennák kifejlesztése, hanem valóban fejlett, programozható antennamegoldásokra van szükség. A mobilkommunikációban az „okos antenna” fejlesztés a bázisállomásokat érintette. A fejlesztés elindulásakor annak elvárt eredményeül a szükséges bázisállomások számának csökkenését, a rendszer kapacitásának fejlődését és a frekvenciaspektrum felhasználásának csökkenését határozták meg. Már 2001-ben mérésekkel tudták igazolni, hogy egy CDMA2000 rendszer esetében a korábban alkalmazott antenna 20W lesugárzott teljesítménye lecsökkenthető 5,9W-ra. A 2.4. ábrán látható okos antennarendszer esetében a kétirányú nyíl azt jelzi, hogy a rendszer természetesen lehet adó és vevő is. A lenti ábrán látható megoldásnál minden antenna elemhez egy külön front end biztosítása szükséges. [115; 224-225. oldal]



2.4. ábra: Okos antenna rendszer SDR-rel [115; 225. oldal]

Az okos antenna rendszerek fejlődésében három lépcsőt különböztetnek meg, ezek a nyaláb-kapcsolásos (SB – Switched Beam), az optimális/adaptív és az érkezési irány (DoA -

Direction of Arrival) szerinti kialakítás. Sok esetben a kapacitás növelése megoldható lehet további bázisállomások kialakításával is, azonban ahol nem, ott megoldást jelent az okos antenna alkalmazása, például olyan nagy forgalmú rendszerek esetében, amikor szélesebb spektrum és több bázisállomás kiépítése nem költséghatékony megoldás. [115; 225. oldal]

### 2.2.6. Radarok

A radar az egyik leggyakrabban alkalmazott nagy hatótávolságú felderítő szenzor, amely többféle helyszínen/platformon telepíthető, így szárazföldön, levegőben, vízi járművön, stb. [153] Megkülönböztethetünk polgári (meteorológiai, légi- és vízi közlekedési, halradar, stb.) és katonai felhasználású radarokat (légvédelmi, korai előrejelző, ballisztikus rakéta védelmi, mozgócél felderítő, rakétákra telepített, stb.) [154]

A radarok alkalmazásának legfontosabb célja a légtérelőőrzés megvalósítása, melynek során az alábbi feladatokat kell biztosítani:

- a különböző hatásos radar keresztmetszettel rendelkező repülő eszközök detektálása;
- a detektált céltárgyak útvonalba fogása és követése, megbízható azonosítása.

Ahhoz, hogy a fenti feladatok a lehető legnagyobb hatékonysággal végrehajthatóak legyenek, a legújabb fejlesztések (pl. SDR technológia), illetve a különböző védelmi megoldások (kibervédelem, alacsony pályán tevékenykedő pl. zavarást alkalmazó műholdak elleni védelem, stb.) beépítése szükséges. [155] A polgári és katonai radarokat rendszerbe integrálják - a NATO vonatkozásában ez a NATO Integrált Lég- és Rakétavédelmi Rendszer<sup>145</sup> - melynek célja a valósídejű, azonosított légihelyzet-kép<sup>146</sup> előállítása. [156]

Az utóbbi évtizedekben a radarok esetében is jelentős változások történtek, melyek közül a legjelentősebb az alábbiak:

- **Az új típusú radarok tényleges kisugárzott teljesítménye jelentősen lecsökkent** a korábbi évtizedekhez radarjainak jellemzőihez képest. **Ez hatással van a szükséges zavarójel teljesítményre.**

- **A radarok hatékony elektronikai védelmi megoldásokkal rendelkeznek. Emiatt új EHV eszközökre és eljárásokra van szükség.**

- **A radarjel feldolgozásban is jelentős változások történtek, amely növeli az EHV feladatok komplexitását.** [25; 86. old.]

<sup>145</sup> NATO Integrated Air and Missile Defence, NATINAMDS

<sup>146</sup> Recognised Air Picture, RAP

A katonai radarok esetében fontos az, hogy a lehető legjobb technikai paraméterek elérésére koncentráljanak a fejlesztések során, azonban könnyen belátható, hogy az egyes paraméterek javulása negatívan befolyásolhatja más jellemzők értékeit. Emiatt minden rádiólokátort úgy terveznek, hogy az adott feladat végrehajtása során az ahhoz szükséges *„paraméter maximális értékeinek biztosítását figyelve a többi paraméter optimális értéket vegyen fel.”* [157] A rádiólokátor egyik legfontosabb paraméterének, a maximális hatótávolságának értékét az adó teljesítménye és frekvenciája, a tápvonal és az antenna jellemzői, a vevő érzékenysége és sáv szélessége, a moduláló jel impulzusideje, a céltárgy letapogatásának módja és sebessége, az indikáció módja és a felbontóképesség, a cél hatásos radarkeresztmetszete, valamint az elektromágneses hullámok terjedési viszonya határozza meg. [157]

Az SDR technológia természetesen a radarokban is felhasználásra kerül/került. **A radareszközök vonatkozásában a radar érzékenységet, hatótávolságát és a képzett radarkép minőségét képes jelentős mértékben javítani az FPGA-n alapuló digitális jelfeldolgozás alkalmazása.** [158] Számos kutatás és kísérlet eredménye elérhető, de meg kell jegyezni, hogy bár elméletben könnyen megvalósítható, azonban a gyakorlati megvalósítás során többféle probléma is felmerülhet. Ilyenek például a megfelelő antennaméretezés hiánya miatt fellépő pontatlanság. [159] [160]

### **2.2.7. Az Integrált elektronikai felderítő és zavaró rendszer (INTERJAM) projekt részletes bemutatása**

Mint azt már az első fejezetben említettem, az „Integrált elektronikai felderítő és zavaró rendszer (INTERJAM)” négy szervezet részvételével került kifejlesztésre. A fejlesztés céljaként egy olyan, két fő egységből álló felderítő-zavaró berendezés kifejlesztése volt a cél, amely a 20-3000 MHz frekvenciasávban képes elektronikai felderítést és a legfontosabb sávban mintegy 800 W kimenő teljesítménnyel elektronikai zavarást végrehajtani.

Ennek érdekében cél volt a projekt keretében kifejleszteni és megépíteni:

- a felderítő (ESM) és a zavaró (ECM) modul vezérlő szoftverét, valamint az állomás önálló működtetését biztosító programot;
- a teljesítményerősítő egységeket és a szükséges tápegységeket;
- a harmonikus szűrőbankot és az antennakapcsoló egységet.

- továbbá a projekt keretében integrálni a szélessávú és monitoring vevőt az adórendszerrel és egy kompakt, gyorsan konfigurálható, kis terepjáróba építhető állomásváltozatot megépíteni. [107]

A projekt végén készített HT28 SAJ Integrált Felderítő és zavaró rendszer „INTERJAM” záró szakmai beszámolóban részletesen bemutatásra került a projekt során végrehajtott valamennyi részfeladat, beleértve ebbe a tevékenység alapját képező, a korszerű felderítési és zavarási technikákra vonatkozó elemzés leírását, vagy a fejlesztés és kivitelezés során tapasztaltakat. A projekt elméleti vizsgálatokat és egy eszköz kifejlesztését és összeállítását foglalta magába. Az előkészítő munka során végrehajtották a felderítési és zavarási technikák vizsgálatát, illetve kidolgozásra került a Felderítés hatékonysági minősítő és a Zavarás hatékonysági minősítő eljárás. Ezen feladatok után következtek az egyes részelemek fejlesztései, mind az adástechnikai, mind az antennarendszer, valamint a vételtechnika vonatkozásában. A különböző egységek ebben az esetben már a szoftverrádió technológián alapuló részelemeket tartalmaztak, melyek a katonai felhasználásnak is megfeleltethető kivitelben kerültek beépítésre. Az egységek fejlesztését és egybeépítését követően végrehajtott tesztelések eredményeit feldolgozták és a rendszer üzemelését biztosító szoftver folyamatos módosításával korrigálták azokat. Az elkészült rendszert a későbbiek folyamán valós megrendelés alapján más rendszerintegrátorok saját rendszerükbe beintegrálták. [161]

A projekt kivitelezése során az állomások alábbi fontosabb képességekkel kerültek kialakításra:

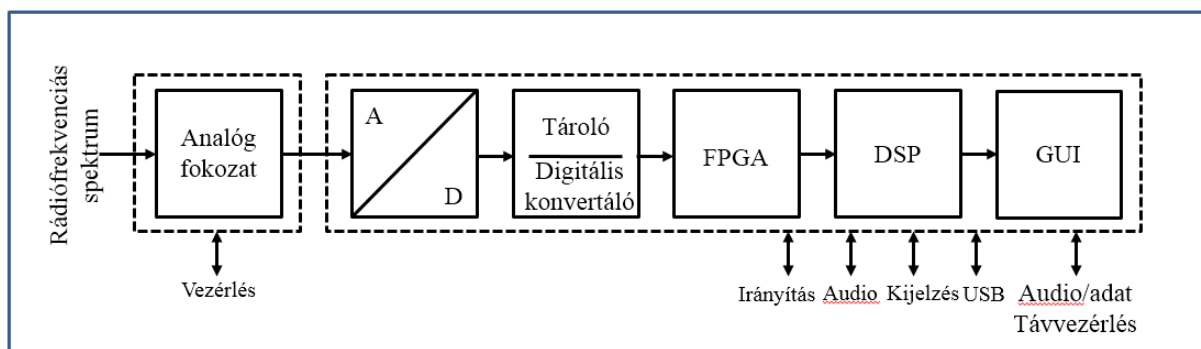
- Elektronikai felderítő állomás
  - 0,09-3000 MHz frekvenciatartomány;
  - helyi vagy távoli rögzítési lehetőség;
  - iránymérési képességekkel bővíthető;
  - helyi vagy távoli vezérlés lehetősége.
- Elektronikai zavaró állomás
  - 100-500 MHz frekvenciatartomány;
  - folyamatos vagy válasz zavar üzemmód;
  - 100 ms válaszüzemi (1ms opció);
  - 1000 W kimenő teljesítmény (a tervezett 800W helyett). [162]

A 2.1. képen látható eszköznél a szoftverrádió technológia alkalmazásának célja az volt, hogy ugyanazon állomást rádiófelderítő-zavaró, radarfelderítő-zavaró, mobil kommunikációt felderítő-zavaró, GPS zavaró feladatban alkalmazhassák, az üzemmódok közötti váltás pedig egy másik szoftver indításával történt. [107]



2.1. kép: Az INTERJAM eszköz labormintája gépjárműbe beépítve. [107] [163]

A kifejlesztett és a komplex rendszerben felhasznált részegységek többségénél a szoftverrádió technológia beépítésre került, melyet a SRS-3000 panorámavevő működésének ismertetésével mutatok be az 2.5. ábrán.



2.5. ábra: Az SRS-3000 panorámavevő jelfeldolgozása.<sup>147</sup>

<sup>147</sup> [164] alapján szerkesztette a szerző.

**A panorámavevő esetében is – mint a szoftverrádiós eszközöknél általánosan – a lényeg, hogy az analóg jelet minél előbb digitalizáljuk és minden további feladatot már a digitális jellel végezzük.** A fenti eszközben az analóg jel az analóg fokozatot követően az A/D átalakítóra (Analog/Digital Converter) kerül, amely a folytonos jelből időben és szintben kvantált jelet állít elő. A digitalizálást követően tároló (FIFO, First In/First Out, azaz a legelőször érkező adat kerül ki először a pufferből) vagy digitális konvertáló (DDC digital down-converter) kerül alkalmazásra, annak függvényében, hogy szélessávú vagy keskenysávú jelfeldolgozásról beszélünk. Az utolsó fokozat a digitális jelfeldolgozás, amely az újraprogramozható hardver elemekben (FPGA<sup>148</sup>, DSP<sup>149</sup>) történik. Az egész vevő a grafikus felhasználói felületen (graphical user interface, röviden GUI) keresztül vezérelhető. A helyi és a távvezérlés a külső csatlakozásokon keresztül biztosítható. [164]

Az INTERJAM projekt keretén belül kifejlesztett egyedi elektronikai felderítő és zavaró eszköz koncepciójának továbbfejlesztésével a következő célkitűzés egy olyan elektronikai hadviselési rendszer felépítése volt, amelynek egy önálló eleme képes lett volna összekapcsolni három-öt felderítő-zavaró rendszerállomást, gyűjteni és feldolgozni az elektronikai felderítési információkat, feladatot szabni az alárendelt állomásoknak, irányítani azok működését, ellenőrizni a végrehajtás hatékonyságát és együttműködni a szomszédos hasonló vezetési szintekkel. [165]

Az elgondolás alapja a Nemzeti Közszolgálati Egyetem jogelődje, a Zrínyi Miklós Nemzetvédelmi Egyetem kutató-oktatói által végzett kutatások eredménye volt, miszerint az **elektronikai hadviselés területén is szükség van az automatizált harcvezetés alkalmazására.** Ennek fontosságát a **napjainkban egyre nagyobb számú, az elektromágneses spektrumot használó eszköz megjelenése támasztja alá.** Az újabb és újabb eszközök felderítése és a szükséges tevékenység – további figyelés, lehallgatás vagy zavarás – elrendelése a kezelők esetében több időt vesz igénybe, mintha ez a tevékenység automatizáltan történne.

**Az automatizált harcvezetés feltételei:**

- **adatbázis, vagy elektronikai harcrend<sup>150</sup>**, amely tartalmazza a valamennyi félre vonatkozó adatot (helyzetinformációk, frekvencialisták, folyamatosan frissített felderítési adatok, stb.);

<sup>148</sup> FPGA, Field Programmable Gate Array – szabadon (felhasználó által) programozható logikai áramkört elem

<sup>149</sup> DSP, Digital Signal Processor – Digitális jelfeldolgozási algoritmusok végrehajtására optimalizált processzor

<sup>150</sup> EOB, Electronic Order of Battle

- **egységes adatstruktúra** a rendszer minden elemében;
- **stabil és megfelelő sávsebességű adatátvitel;**
- **strukturált alhálózatok**, amelyek vezetőmunkahelyei egy központi információs rendszerhez kapcsolódnak. [165; 6. old.]

### **2.2.8. Az SDR koncepció által nyújtott előnyök az MH-ban történő alkalmazásuk bevezetése esetén**

Mint azt már korábban említettem, véleményem szerint az SDR alapú elektronikai hadviselési eszközök alkalmazása nagyon fontos és napjainkban már mindenképpen szükséges képességfejlődést jelentenének az MH vonatkozásában. Annak érdekében, hogy az SDR alapú eszközök alkalmazásával kihasználható előnyök egyértelműen láthatóak legyenek, bemutatok néhány, az EHV századnál jelenleg is megtalálható eszközt.

*Az UP-3/MA ultrarövidhullámú panoráma vevőkészülék biztosítja „a teljes 20-100 MHz frekvenciatartomány egyidejű panorámázását, a frekvenciatartomány öt körzetre való felbontását, a kiválasztott körzet panoráma megfigyelését, a vevőegység távvezérlését az 50 m távolsáig kihelyezhető indikátoregységről, a kiegészítő vevő ráhangolását a lehallgatásra kiválasztott adásra, a teljes 20-100 MHz frekvenciatartományban, vagy azon belül kiválasztott körzetben üzemelő adások vételét és frekvencialépték helyes megjelenítését az indikátor katódsugárcsővén, a belső markerjel generátor által előállított markerjel üttetésével a felderített állomás frekvenciájának pontos meghatározását, a felderített állomás jeleinek AM vagy FM demodulálását és az adás meghallgatását a kiegészítő vevő segítségével, a saját marker helyettesítését a kiegészítő vevő (VU-21) oszcillátorjével, a vevő hangolási frekvenciájának indikálását a frekvenciaegyeztetés céljából.”*[166]

A két részből, vevőből és indikátoregységből álló UP-3MB ultrarövidhullámú panoráma vevőkészülék a 100-520 MHz-es frekvenciatartományban üzemelve „biztosítja a frekvenciatartomány hét körzetre való felbontását, a kiválasztott körzet panoráma megfigyelését, a kiegészítő vevő ráhangolását a lehallgatásra kiválasztott adásra, a teljes 100-520 MHz frekvenciatartományban, vagy azon belül kiválasztott körzetben üzemelő adások vételét és frekvencialépték helyes megjelenítését az indikátor katódsugárcsővén, a felderített állomás jeleinek AM vagy FM demodulálását és az adás meghallgatását, a saját marker helyettesítését a kiegészítő vevő (VU-32) oszcillátorjével, a vevő hangolási frekvenciájának indikálását a frekvenciaegyeztetés céljából.” [167]

Az UP-3/MA ultrarövidhullámú vevőnél említett VU-21M ultrarövidhullámú vevőkészülék rendeltetése a 20-100 MHz-es frekvenciatartományban működő rádióadások

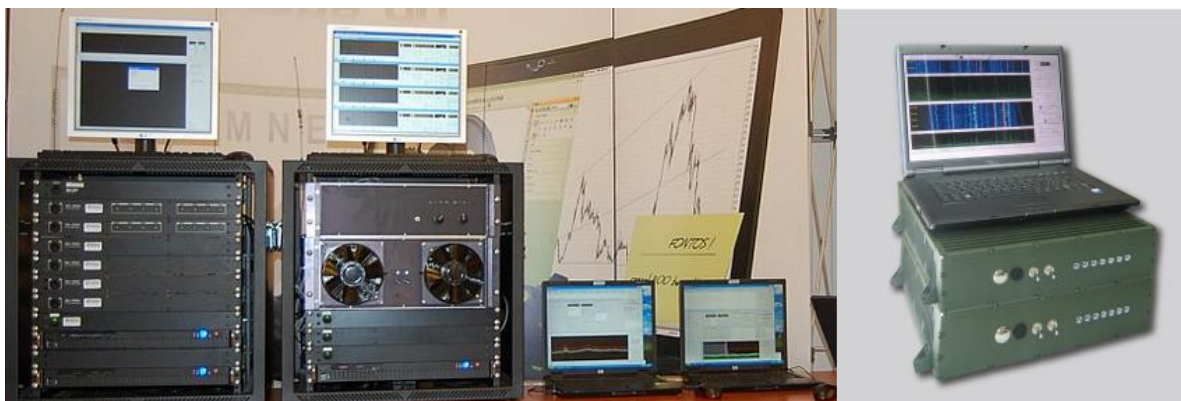
felfedése, információtartalmának megállapítása mellett képes az információtartalom rögzítésére a csatlakoztatott magnetofon segítségével, az IU-6M iránymérő vezénylesére, az iránymérő antenna lehangolására, a panorámavevővel való közös üzemeltetésnél a panorámakép alapján az adó kiválasztására, távíró csatornalebontó egységgel való együttműködésre. [168]

Az UP-3/MB ultrarövidhullámú vevőnél említett VU-32M ultrarövidhullámú vevőkészülék rendeltetése a „100-500 MHz-es frekvenciatartományban működő rádióadások felderítése, lehallgatása az alkalmazott adásmódnak megfelelő beállítás mellett, és a vételi frekvencia kijelzése.” [169]

Az INTERJAM projekt eredményeit, illetve a nyíltan elérhető piaci termékek közül a véletlenszerűen kiválasztott Jordan Electronic Logistics Support Signal Sniper [163] eszköz jellemzőit felhasználva megállapítható, hogy **az SDR alapú eszközök bevezetése az alábbi jellemzőkben, képességekben nyújthat jelentős előnyt, képességfejlődést az MH elektronikai hadviselési képessége vonatkozásában:**

- A frekvenciatartomány vonatkozásában: a bemutatott MH eszközök együtt képesek a 20-520 MHz közötti frekvenciatartomány átfogására. **Napjaink fejlett rendszerei egy eszközben képesek az itt megadott frekvenciatartománynál lényegesen nagyobb frekvenciatartományban üzemelni, az SDR koncepció által biztosított képességek felhasználásával gyorsabb és pontosabb eredményeket biztosítani;**

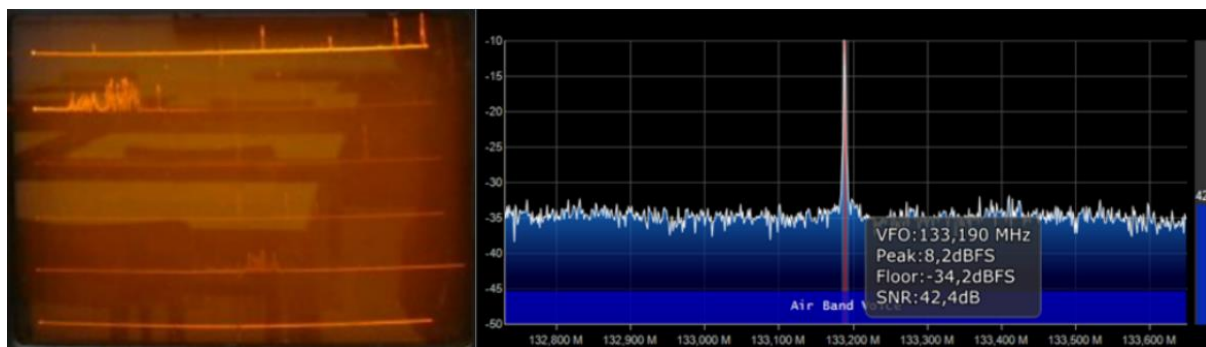
- A napjaink fejlett **eszközeinek beállítása, vezérlése vonatkozásában:** megállapítható, hogy a 2.2. képen látható módon, **számítógépes alapon történik**, amely – a beépített kisebb méretű, nagyobb pontosságú és képességű alkotóelemek felhasználásával – **sokkal finomabb léptékű beállítások** alkalmazását biztosítja;



2.2. kép: Az INTERJAM projekt eszköze és a Signal Sniper kezelőfelülete, valamint kijelzőik. [161] [170]



- A kijelzés vonatkozásában: a fejlett eszközök az eredmények kijelzését a 2.3. képen látható módon, a korábbi **panorámaindikátorok helyett sokkal részletesebb képei megjelenítést nyújtó eszközökön** biztosítják úgy, hogy a különböző jellemzők (megjelenítendő információ változtatása, felbontás módosítása kinagyítással (zoomolás), több információ egy ablakban, stb.) kiválasztása, beállítása sokkal egyszerűbbé, illetve például a **vízesés diagramok alkalmazásával sokkal informatívabbá**, a kezelő által sokkal **jobban értékelhetővé, átláthatóvá** vált;



2.3. kép: UP-3MB ultrarövidhullámú panorámaindikátora [161], illetve egy SDR-vel és a hozzá biztosított szoftverrel készített spektrumkép<sup>151</sup>.

- Az eszköz képességének növelése vonatkozásában: az **SDR koncepció alkalmazásával a további fejlesztési lépcső lehet az elektronikai támogató (felderítő) és az elektronikai zavaró képesség egy eszközbe történő beintegrálása**;
- Megfelelő **informatikai/programozói képesség beintegrálása esetén biztosított az SDR koncepció által nyújtott előnyök kihasználása**, hiszen az MH igényeinek megfelelően kerülhetnek megírásra a programok, amellyel az eszközök működését befolyásolhatjuk;
- Egyéb jellemzők vonatkozásában: mindenképpen meg kell említeni a **fizikai méret és a súly csökkenését**, amely pozitívan befolyásolja a használhatóságot. Emellett **további szolgáltatások** is elérhetőek, így például a felfedett adás információtartalmának rögzítése a számítógép merevlemezére, a felfedett adás visszahallgatása, miközben az SDR alapú eszköz folytatja a meghatározott tevékenységet.

Mindenképpen fontos azt kijelenteni, hogy az **SDR alapú fejlesztésnek, vagy az eszközök/eszközrendszer beszerzésének egyidőben, vagy viszonylag rövid – néhány éves – intervallumban kell megtörténnie** az egységes és kompatibilis rendszer kialakítása

<sup>151</sup> Saját készítésű kép.

érdekében. Lényeges és egyértelműen kijelenthető, hogy az MH érdekeit az szolgálja, hogy **ugyanaz az SDR alapú rendszer kerül alkalmazásra az MH valamennyi érintett alakulatánál, mind a szárazföldi, mind a légierő haderőnem vonatkozásában.** Számos korábbi kutatás foglalkozott az MH érdekében szükséges EHV képesség fejlesztésével, de a tanulmányok alapvetően a szárazföldi haderőnem fejlesztésére fókuszáltak.

Az SDR koncepció számos más előnyt is biztosít az MH elektronikai hadviselési képességének fejlesztésében. Ezek között szerepel például a már többször említett **könnyebb továbbfejlesztési lehetőség**, amely elsődlegesen az üzemeltető szoftver módosítását fogja jelenteni. Magában hordozza a **szükséges módosítások könnyebb végrehajthatóságát, szoftvermódosítások vagy egy új hullámforma megírásával** és az eszközökre történő feltöltésével.

A korábbi elektronikai hadviselési eszközökre az volt jellemző, hogy **vagy elektronikai támogató feladatra vagy elektronikai zavarásra** voltak alkalmazhatóak. Napjainkban egyre több gyártó termékpalettáján jelennek meg olyan eszközök, amelyek a **mindkét feladatra alkalmazhatóak**, természetesen nem egy időben. Ennek **előnyeiről-hátrányairól szintén megoszlanak a vélemények.** Az MH vonatkozásában – **véleményem szerint, figyelembe véve a jelenleg meglévő humán és pénzügyi erőforrások helyzetét – a mindkét feladatot ellátni képes eszközök fejlesztése, beszerzése javasolt.** Ennek oka az, hogy a komplex, mindkét feladatra képes eszköz esetében a gépjárműtechnika nincs duplikálva, az áramellátó illetve az informatikai és kommunikációs eszközök is kisebb mennyiségben szükségesek. Ehhez hozzáadódik még az alacsonyabb kezelő állomány miatt fellépő költségmegtakarítás is. **Véleményem szerint az MH jelenlegi létszámával arányos és a feladatrendszeréhez igazodó elektronikai hadviselési képesség kialakítása, modernizálása úgy célszerű, hogy az elektronikai támogató és a rádiófelderítő képesség harcászati szinten nem kerül szétválasztásra az információszerző eszközök és szervezeti elemek vonatkozásában, hanem csak a feldolgozás során.**

Az elektronikai támogatás és zavarás egy komplexumba integrálásának ötlete már **korábban is megjelent**, azonban kiemelném azt, hogy a korábban ismert méretek itt is jelentősen csökkenthetőek, mivel napjainkban **az SDR technológia jóval kisebb helyigényű megoldást képes nyújtani.** Az is fontos, hogy a korábbi évtizedekben a reakció idő a *„lefogás olyan területein, ahol a kereső – más szóval célfelderítő – eszközök egybe vannak építve a zavaróberendezésekkel”* másodpercekben volt mérhető. [63; 36. oldal] Azonban a közben eltelt 30-35 esztendőben olyan mértékű fejlődésen ment keresztül az elektronikai ipar,

hogy ez a néhány másodperces reagálási idő már nagyságrendekkel kisebb időre csökkent. [80]

Az egy eszköz – két funkció megvalósításának lehetőségét biztosítja a szoftverrádió technológia. **A szoftverrádió technológián alapuló eszközök működését a szoftver határozza meg, annak módosításával az eszköz működése változtatható, természetesen a rendszerelemek paraméterei által biztosított korlátokon belül.** [171] Az ilyen készülékek további elemekkel – például több, különböző frekvenciasávban használható antennával – kiegészítve nagyobb frekvenciatartományban is képesek lehetnek üzemelni, illetve az elektronikai támogató és az elektronikai zavarás funkció egy eszközbe integrálható. [31]

**Korlátként jelentkezik az is, hogy a különböző funkciókra történő átálláshoz (az alkalmazandó szoftver elindítása és betöltése) szükséges idő alatt a rendszer nem alkalmazható. Ez a korlát megszüntethető, amennyiben egy eszközben több SDR kerül beintegrálásra, azonban ez növeli a költségeket.**

Fontos azonban az is, hogy nemcsak a frekvencia, hanem más kisugárzási paraméterek megváltoztatására képes lehet egy ilyen eszköz. Ebben az esetben a működés alapja egy független, tanulni képes „intelligens” elem, amely a mért adatokat összehasonlítja a rendszerben tárolt tudásbázissal<sup>152</sup>, majd a kapott eredmény alapján a rendszer végrehajthatja a meghatározott paraméterváltoztatásokat. [172]

**Véleményem szerint az MH elektronikai hadviselési képességének fejlesztésekor alapvető kritérium az SDR alapú eszközök beszerzése, amely biztosítja a későbbi módosítások, kisebb fejlesztések, illetve az MH érdekében szükséges egyedi módosítások végrehajtását.** Valamennyi dandár szintű katonai szervezetet el kell látni ilyen képességgel, és természetesen, nem szabad elfelejtenünk a légierő alakulatait sem, mivel hatótávolságukkal jelentős képességet biztosítanak. Az SDR alapú eszközök beszerzése azért indokolt, mivel figyelembe a teljes eszközpark egységes platformra történő átcseréléséhez szükséges anyagi forrásigényt, láthatjuk, hogy az jelentős összeget fog felemészteni és nehezen biztosítható újabb fejlesztésre fordítható forrás rövidtávon ismételten. Ebben az esetben azt is figyelembe kell venni, hogy az új eszközök rendszeresítése a személyi/szervezeti rendszer felújításának szükségességét is magában hordozza.

A szárazföldi haderőnem EHV alakulatainak eszközei esetében a nem-SDR technológia alapú és az SDR technológia alapú elektronikai hadviselési eszközök beszerzése

---

<sup>152</sup> Knowledge base.

esetében is felvetődik az a kérdés, hogy a beszerzés alapja a 'kettő funkció – egy eszköz' vagy az 'egy funkció – egy eszköz' elgondolás legyen. Fontos megjegyezni, hogy nem lehet csak és kizárólag egy szempont alapján dönteni, mivel **a technikai megvalósíthatóság kérdése mellett figyelembe kell venni harcászati, gazdasági, szervezeti szempontokat is.** Mint az a korábban bemutatott INTERJAM projekt elemzéséből is látható, a 'kettő funkció – egy eszközben' elgondolás napjaink fejlett technikai környezetében kivitelezhető.

A két elgondolás összehasonlításához az 1. fejezetben már említett, a NATO 2006-2016 közötti időszakra vonatkozó haderőtervezési javaslatot veszem alapul, amely egy dandár elektronikai hadviselési képességét adja meg, de egyben meghatároz egy minimum technikai eszköz darabszámot is az alábbiak szerint

*„- kettő iránymérő alap (minimum három rádió-iránymérő állomás egységes vezénylésével)”,* azaz minimum hat darab technikai eszköz (az egyszerűség miatt hat darab eszközt veszek figyelembe);

- *„rádiótechnikai felderítő képesség meghatározott frekvenciatartományban”,* itt is egy alappal számolva minimum három darab eszköz (az egyszerűség miatt három darab eszközt veszek figyelembe);

- *„kettő kommunikációs mobil zavaróállomás”,* ebben az esetben nincs további megjegyzésem.

A leírtak alapján a fenti javaslat tizenegy darab szaktechnikai eszközt tartalmaz. A javaslatban szereplő értékelő-elemző-zavarást irányító eszköz esetünkben nem képezi a további elemzésem részét, hiszen arra mindkettő esetben szükségünk van.

**A nem-kommunikációs felderítésre meghatározott eszközök esetében véleményem szerint mindenképpen indokolt a zavaró képesség beépítése,** hiszen mint az az 1. fejezetben bemutatott esetekből is látszik, **napjaink konfliktusaiban nagy szerep hárul a légierő eszközeire.** Emiatt egy esetleges konfliktus esetén a szembenálló fél a radarjaink zavarására, pusztítására fog törekedni, melynek hatását nem biztos, hogy teljes mértékben lesz képes a NATINAMDS rendszer kiküszöbölni. Fontos szempontnak tartom azt is **a beszerzési követelmények meghatározása során figyelembe venni, hogy az eszközöknek képesnek kell lenniük a megszerzett információt (a felderített repülőeszközökre vonatkozó adatokat) az MH légvezetési rendszere részére átadni, a Légi Irányító Központtal<sup>153</sup> együttműködni.**

---

<sup>153</sup> Control and Reporting Centre, CRC

A „Kettő funkció – egy eszköz” koncepció esetében nagyobb az egy eszközre jutó beszerzési költség, azonban kevesebb gépjárműtechnika szükséges. A rádiótechnikai felderítés és zavarás egy eszközbe építésével nem merül fel további eszköz igény. Ekkor kisebb a logisztikai és humán erőforrás igény is.

Az „Egy funkció – egy eszköz” koncepció esetében kisebb az egy eszközre jutó beszerzési költség. Ez azonban nem ad reális képet a végső beszerzési árról, hiszen ebben az esetben több eszköz megvásárlása szükséges, a hozzátartozó hordozóeszközzel. A rádiótechnikai zavaró képesség felállítása – a kommunikációs zavarás esetében megadott darabszámot figyelembe véve – további 2 darab eszközt jelent. Ebben **az esetben előnyként** jelentkezik az, hogy megfelelő földrajzi elhelyezés esetén **folyamatban lévő zavarás esetén is folytatható a felderítés.**

Mint már említettem, **javaslom**, hogy mind **a szárazföldi haderőnemnél, mind a légi haderőnemnél egyidőben kerüljön rendszeresítésre SDR alapú elektronikai hadviselési rendszer**, figyelembe véve az adott haderőnemre jellemző speciális igényeket, beleértve ebbe többek között a páncélvédettséget, vagy a repülésbiztonsági szabályokat is. Azt, hogy a fenti kettő változat közül végül melyiket kell előnyben részesíteni, a beszerzés tervezett időpontjában aktuális helyzet figyelembe vételével kell meghatározni.

### **Összegzés, részkövetkeztetések**

Értekezésem második fejezetében három kérdéskörrel foglalkoztam, ezek a frekvenciagazdálkodás, a szoftverrádió és annak felhasználása a különböző rendszerekben, illetve a Magyar Honvédség EHV rendszereiben történő alkalmazás nyújtotta előnyök vizsgálata voltak.

Az első alfejezetben a frekvenciagazdálkodás jelenlegi helyzetét mutattam be röviden nemzetközi és nemzeti szinten, kiemelve, hogy napjaink polgári és katonai vonatkozásában is egyre jelentősebb és folyamatosan növekszik a frekvenciaspektrum felhasználásán alapuló eszközök száma.

A második alfejezetben a szoftverrádió technológia felhasználását elemeztem az értekezés tekintetében releváns rendszerekben. Bemutattam, hogy a különböző nemzetek milyen irányban indultak el, milyen új szervezeteket hoztak létre. A különböző rendszerek vonatkozásában a technológiai megoldások ismertetésével rámutattam, hogy számos, a katonai alkalmazás szempontjából fontos technikai eszközben/rendszerben már alkalmazásra került a szoftverrádió technológia. Természetesen a technológia felhasználása sokkal szélesebb körű, hiszen beszélhetnénk még a gépjárműiparban, geodéziában,

méréstechnikában, stb. történő felhasználásáról is. Napról napra jelennek meg újabb elgondolások a szoftverrádió felhasználásával kapcsolatban, amelyek a kutatások befejezését követően beépítésre kerülnek. A szoftverrádió technológia a korábban alkalmazott eljárásokhoz képest jelentősen kibővíti a lehetőségeinket, egyrészt az alkalmazható kisugárzási és vételi paraméterek változtathatósága, másrészt pedig az esetleges továbbfejlesztési lehetőségek leegyszerűsítésével, hiszen ugyanazon hardver felhasználható a szoftver módosításával/fejlesztésével. Lényeges azt is kiemelni, hogy a kognitív rádió már egy újabb lépcső a szoftverrádió evolúciójában.

A fentiek alapján az alábbi következtetéseket fogalmazom meg:

1. Napjaink folyamatosan fejlődő elektronikai világában **a hatékony működéshez és fejlesztéshez folyamatosan figyelemmel követni és alkalmazni kell a megjelenő újításokat.** A Magyar Honvédség **elektronikai hadviselési képességének fejlesztésére az SDR alapú technológia alkalmazása megfelelő alapot nyújt**, hasonlóan a más nemzetek hadseregei által végrehajtott fejlesztésekhez.

2. A frekvenciaspektrum felhasználása napjainkban egyre komplexebb feladat, mivel az azon alapuló eszközök száma folyamatosan emelkedik. Ez a komplexitás igaz a Magyar Honvédségre is, így természetesen az elektronikai hadviselésre is. Az **SDR technológia, illetve a technológia által biztosított frekvencia felhasználási eljárások hatékonyságának növelése érdekében szükséges, hogy összhaderőnemi/hadműveleti szinten az EHV szervezeti elem végezze a frekvenciagazdálkodási feladatokat az EHV feladatok/eszközök vonatkozásában, ebbe beleértve az összhaderőnemi korlátozott frekvenciák jegyzékének<sup>154</sup> kezelését is.**

3. Fontos az, hogy az MH esetében **a fejlesztésnek egy időben, vagy nagyon rövid időn belül kell megvalósulnia**, az MH teljes egészére – azaz **mindkettő haderőnemre** – **vonatkoztatva** homogén SDR alapú technikai eszközökkel annak érdekében, hogy a kompatibilitás biztosított legyen.

4. A technikai fejlesztések által **biztosított képességek minél hatékonyabb kihasználása érdekében** vizsgálni kell a **meglévő szervezeti elemek felépítését és a szükséges mértékben módosítani kell azokat, vagy újakat kell létrehozni.**

---

<sup>154</sup> Joint Restricted Frequency List, JRFL.

### 3. A SZOFTVERRÁDIÓ TECHNOLÓGIÁN ALAPULÓ ELEKTRONIKAI HADVISELÉS ESZKÖZRENDSZER ALKALMAZÁSA AZ MH RENDSZERÉBEN

A szoftverrádió technológia alkalmazása számos olyan kérdést vet fel, melyeket a hatékony működtetés érdekében vizsgálni kell. Jelen fejezetben ezen kérdéseket vizsgálom, beleértve az egyik legfontosabb témát, a támadhatóság és védelem kérdéskörét.

#### 3.1. A szoftverrádió technológia alapú EHV eszközzel szemben támasztott követelmények

Az SDR alapú elektronikai hadviselési eszköz számos, a korábban alkalmazott elektronikai eszközök esetében fellépő problémára megoldást nyújthat. Ezek közül legfontosabb a technológia **gyors fejlődésének és az így bekövetkező technikai és eljárásbeli változásoknak mielőbbi lekövetése**. Emellett nem felejtkezhetünk el a frekvenciamenedzsment kérdéséről sem, amelyre **az SDR alapú eszközök adaptív módon** történő alkalmazása megfelelő válasz annak érdekében, hogy a saját erőink tevékenységét segítsük, a szembenálló fél tevékenységét pedig akadályozzuk. Ahhoz, hogy az SDR technológia valamennyi előnyét kihasználjuk, az eszközök és a rendszerek elemeit a lehető legerősebb minimum követelmények kell megállapítanunk.

A követelményeket az egyes elemekre lebontva kell megállapítani, azonban úgy, hogy azok összességében egységet alkossanak és a képesség-ár arány is elfogadható legyen a döntéshozók részére. A követelmények meghatározása érdekében mindenképpen célszerű az 1. fejezetben már röviden bemutatott PRIZMA rendszer működésének és az INTERJAM projekt eredményeinek további elemzése.

A PRIZMA rövidhullámú rádiózavaró berendezés **a teljes kiépítettség állapotában képes lett volna** a rendszerhez tartozó felderítő, iránymérő **állomások távvezérlésére**, az általuk **vett jelek feldolgozására, értékelésére**, az üzemeltetési **parancsok továbbítására és vételére**, a zavaróállomásoknál pedig a zavaró **tár elemek vételére**, a kapott parancsnak megfelelő **zavarás végrehajtására és a végrehajtott feladatok visszajelentésére**. A rendszer a vett adatokat adatbázisban kezelte, a rendszerbe betáplált szempontok szerint csoportosította, listázta. Az összeköttetés rádiórelé csatornán, modemekkel volt biztosítva az alárendelt állomások között, míg a parancsnoki munkahely modemeken keresztül, kábellel csatlakozott a VERA és a FLÓRA állomáshoz. **Kiképzési, gyakoroltatási célból az**

**állomások kábelekkkel is összeköthetőek és műantennával üzemeltethetőek voltak.** A működés fontos alappillére volt az egyes állomásokban beépített parancsnoki számítógép, amely az előljáró állomástól vette és feldolgozta a parancsokat, feladatokat, az alárendelt munkahelyeitől kapott adatokat, vagy a végrehajtott feladatokra vonatkozó jelentéseket. A kapott parancsokban megadott frekvencia, működési szektor és egyéb szempontok alapján vezérelte az adott munkahelyeket. [24; 4. sz. melléklet]

A korábban alkalmazott, továbbá a korábbiakban bemutatott PRIZMA rendszer és INTERJAM projekt képességeinek figyelembevételével, valamint az elvégzett kutatások és a **saját tapasztalataim alapján a stacioner** (pl. országvédelem) és **telepíthető** (pl. országvédelem, békeműveleti feladatok) **elemeket tartalmazó szoftverrádió technológia alapú elektronikai támogató és zavaró rendszer kialakítására az alábbiak szerint teszek javaslatot.**

Alapvetően a kialakítandó rendszerrel szemben támasztandó követelményeket elemzem, az egyes paramétereknél nem határozom meg annak számszerű értékét, mivel az időközben történő kutatások-fejlesztések, illetve az így elérhetővé váló új elemek és képességek jelentős változást okozhatnak az eszköz egyes paramétereiben, és így akár a teljes rendszerben.

**A szoftverrádió technológián alapuló elektronikai támogató és zavaró komplexum rendeltetése:** Az üzemi frekvenciatartományba eső, az előljáró rendszerelem által meghatározott frekvenciatartományban – a kialakítás függvényében – elektronikai támogató és/vagy zavaró feladatok végrehajtása honi vagy más műveleti területen úgy, hogy az SDR technológián alapulva legyen képes reagálni a műveleti környezetben történő változásokra a saját üzemelési paramétereinek rövid idő alatt történő módosításával.

Ezen belül legyen alkalmazható:

- a kommunikációs és nem-kommunikációs rendszerek felderítésére és zavarására a lehető legnagyobb frekvenciatartományban, beleértve a GNSS és a mobiltelefon-rendszer zavarását is;
- a beérkező adatok alapján a szükséges elemzések elvégzésére;
- a nyers vagy elemzett adat továbbítására;



- az érvényben lévő parancsok vagy az előjáró állomástól érkező eseti parancs figyelembe vételével elektronikai zavarás kiváltására az üzemi frekvenciatartományban;
- a rendszer egyes állomásai legyenek képesek autonóm, távvezérelt vagy közvetlen kezelői irányítás alatt üzemelni.

A rendszer egészével és egyes elemeivel szemben támasztott általános követelmények:

- **felhasználóbarát kialakítás, egyszerű kezelhetőség**, különösen a hordozható kivitel esetén;
- legalább **kétféle áramfelvételi lehetőség** az egyes eszközökön (kivéve az egyszeri felhasználású eszközökön);
- legalább **kétféle adatátviteli mód** biztosítása az értékelő-elemző központ vagy a kijelölt vezetőállomás irányába (kivéve az egyszeri felhasználású eszközökön);
- **beépített rendszertesztelési képesség**.<sup>155</sup>

A rendszer részei:

- **értékelő-elemző és zavarást irányító központ**, amely ellátja az elektronikai támogató és zavarási tevékenység vezérlését is;
- **alállomás vagy alállomások hálózata**, amely a stacioner, a mobil, a hordozható vagy az egyszeri felhasználású eszközök kombinációjából kerül összeállításra. Az elrendelt feladat függvényében kerül meghatározásra a valós elemek típusa és száma, azaz a műveleti feladat függvényében skálázható a rendszer elemeinek száma.

A képességek (elvi) megfogalmazása az egyes eszköz/állomás tekintetében:

Kivitel vonatkozásában:

- **egyszeri felhasználású, részképességgel bíró kivitel** (elektronikai támogató, vagy rádiózavaró funkciók egyikével, illetve kisebb frekvenciatartomány átfogása, a kijuttatást még nem gátló méret elérése érdekében);
- **hordozható, részképességgel bíró kivitel** (elektronikai támogató, vagy rádiózavaró funkciók egyikével, illetve kisebb frekvenciatartomány átfogása, a személyi állomány által történő hordozhatóságot még nem gátló méret elérése érdekében);
- **gépjárműbe épített, elektronikai támogató és zavaró funkcióval**;

---

<sup>155</sup> Built-In Test Equipment (BITE)

- **megfelelő méret és energetikai viszony esetén repülőgépre** (elsősorban szállító repülőgép vehető figyelembe), **helikopterre vagy pilóta nélküli repülőgépre felszerelhető változat**;
- **fixen telepített** (konténer, épület) elektronikai támogató és zavaró funkcióval.

**Az egyszeri felhasználású eszközök alkalmazásának célja** a repülő (pilóta által vezetett vagy pilóta nélküli eszközökkel) vagy tüzérségi eszközökkel az alkalmazási helyszínre történő kijuttatást követően történő **elektronikai támogató vagy zavaró feladat** végzése. A tevékenység történhet előre programozott időpontban, előre programozott frekvenciatartományban, vagy mindkét funkciót tartalmazó kivitel esetén a végrehajtott elektronikai támogató tevékenység során felfedett tevékenység esetén autonóm módon történő zavarással. Természetesen azzal számolnunk kell, hogy az eszköz fizikai mérete nagymértékben befolyásolja az egyidőben kijuttatható egyszeri felhasználású zavaróadók számát, a lefogható frekvenciatartományt, illetve rendelkezésre álló üzemidőt.

A **hordozható kivitelű SDR alapú elektronikai hadviselési eszközzel** a kisebb harcászati elemek (rajok, szakaszok, különleges műveleti csoportok) támogatása biztosítható, úgy, hogy **a rendelkezésre álló technikai megoldások függvényében megvalósítható lehet már ebben a méretben az elektronikai támogató és zavaró funkció egy eszközbe történő beintegrálása**. A feladatot úgy kell megoldani azonban, hogy azt egy személy valóban képes legyen szállítani, üzemeltetni. Az egyszeri felhasználású és a hordozható eszközök esetében nem szabad azonban azt sem elfelejteni a tervezés során, hogy az akkumulátorok vonatkozásában is számos fejlesztés van folyamatban, amelyek alkalmazásával egyrészt az üzemidő növelése, másrészt pedig az eszköz tömegének csökkenése érhető el.

A gépjárműbe épített verzióval - annak mobilitása révén - a különböző műveletek, manőverek biztosítása, a harcelyzetekben bekövetkező gyors és éles változások lekövetése valósítható meg, illetve a **napjainkban jellemző aszimmetrikus, illetve hibrid hadviselés esetén biztosítható például a lakott területen folytatott műveletek támogatása**. A hordozó gépjárművel szemben támasztott követelményeket egy későbbi bekezdésben részletesebben is elemzem.

Repülőgépbe, helikopterbe, illetve pilóta nélküli repülőgépbe építhető verzió esetén **nagyobb mobilitással és hatótávolsággal számolhatunk**. Ebben az esetben kiemelt figyelmet kell fordítani az autonóm tápellátásra, illetve az antenna kiépítésre. Figyelembe kell vennünk azt is, hogy **az 1. fejezetben említett LEFOGÓ típuscsaládhoz, vagy a JEWCS**

**konténerekhez hasonló megoldásokkal** is kialakíthatunk elektronikai támogató vagy zavaró képességet.

A földi telepítésű konténerbe vagy épületbe telepíthető verzió elsődlegesen országvédelemre, a saját erők híradó forgalmazásának ellenőrzésére, vagy hosszabb idejű békeműveleti tevékenységre alkalmazható. Véleményem szerint a korábban ismertetett „Egérfogó” rendszer telepítési helyei továbbra is felhasználhatóak az új rendszer kialakítása során például a gyakorlatokon alkalmazott saját híradás ellenőrzésére, annak figyelembe vételével, hogy kiegészítő telepítési helyekre szükség lehet.

Egy – **különböző kivitelű elemeket tartalmazó – rendszer** kialakítása **egy jól skálázható és konfigurálható elektronikai hadviselési képességet biztosít**, amely az adott feladat (konvencionális vagy nem-konvencionális hadviselés, országvédelem vagy békeműveleti tevékenység) jellemzőinek figyelembevételével **rugalmasan átszervezhető**.

Fontos és mindenképpen ki kell hangsúlyozni, hogy a **fenti rendszerek beszerzése, vagy fejlesztése, rövid idő alatt**, egy cég/konzorcium által kell, hogy megvalósuljon annak érdekében, hogy mind a **kettő haderőnem, valamint mindegyik kivitel esetében azonos jellemzőkkel, eljárásokkal, adatátviteli módszerekkel működjön**.

#### A technikai paraméterek vonatkozásában:

Mint az a különböző elektronikai és egyéb használati eszközöknél elvárás, itt is meg kell találni a **megfelelő egyensúlyt a követelmények, a reálisan megvalósítható technikai paraméterek** és az ennek érdekében szükséges **fejlesztési vagy beszerzési költségek között**. Számos technikai paramétert meg kell határozni a tervezés és a kialakítás során. Értekezésemben az alapvető szempontokat emelem ki, azonban a pontos paraméterek meghatározása a tervezés feladata, figyelembe véve a rendelkezésre álló lehetőséget, mind technikai, mind humán, mind pénzügyi tekintetben.

Legfontosabb követelmények:

- üzemeltetés vonatkozásában **elfogadható üzemelési frekvenciatartomány** (hordozható eszközök esetében mind a felderítés, mind a zavarás vonatkozásában minimum 50 MHz – 512 MHz, hordozójárműbe építhető verzió esetén minimum 50 MHz – 2500 MHz) – teljesítmény hordozható eszközök esetében minimum 50 MHz – 512 MHz, hordozójárműbe építhető verzió esetén minimum 50 MHz – 2500 MHz) – **méret viszony kialakítása**, zavarállóság, legalább kétféle adatátviteli mód, stb.;

- **minél tágabb üzemi hőmérséklet** (minimum -20C - +55C), **illetve páratartalom tartomány;**

- az adott eszköztípus esetében a beépíthető elemek függvényében elérhető **legnagyobb mérési pontosság** elérése;

- **térképes megjelenítési lehetőség**, a mérési eredmények összevetése/ellenőrzése matematikai modellek alkalmazásával;

- **vízesés típusú megjelenítés** az elektromágneses spektrum megfigyelése eredményének vizualizációja során;

- **nagymértékű automatizált működés** lehetősége, mind a frekvenciaspektrum megfigyelése, mind a mérési eredmények feldolgozása terén;

- **hordozhatóság és beépíthetőség biztosítása**, annak minden aspektusát figyelembe véve, mint a fizikai méretek, az energetikai viszonyok, a kezelőállomány létszáma, stb.;

- **kompatibilitás biztosítása** a már meglévő vagy beszerzésre tervezett elektronikai, kommunikációs, gépjármű-technikai, stb. eszközökkel;

- **önálló illetve hálózati tápellátás.**

#### Gépjárművel szemben támasztott követelmények:

Mindenképpen fontos megvizsgálni, hogy lehetőség esetén könnyű és nehéz páncéltartó ellátott járművekbe is beépítésre kerülhessenek az SDR alapú elektronikai hadviselési állomások. Ennek oka az, hogy **különböző műveleti területeken (beépített környezet, sivatag, magas hegyi környezet, stb.)** kerülhet alkalmazásra az eszköz, és emiatt más és más követelményeket határoznak meg.

Főbb követelmények:

- **egységes gépjárműpark alkalmazása**, a támogatott alegységekkel lehetőség szerint azonos terepjáró képesség [80; 71. old.];

- **a vonatkozó NATO szabványokban (NATO STANAG) meghatározott előírásoknak történő megfelelés a kompatibilitás és az interoperabilitás érdekében;**

- **a hazai műszaki és környezetvédelmi előírásoknak történő megfelelés;**

- **az elektronikai támogató és zavaró feladatok végrehajtásához szükséges feltételek biztosítotttsága** (például energiaellátás biztosítása, berendezések és antenna hordozása, kommunikációs képesség, stb.). Megoldást jelenthet akár az ISO szabványkonténer felépítményként történő felhasználása, így a hordozójármű váltása esetén kisebb költségekkel kell számolni. Ebben az esetben csak a konténer hordozásának feltételeit kell megteremteni, nincs szükség a technikai eszközök, kábelezések átszerelésére;

- a kijelölt **műveleti helyszínen előírt feltételek** biztosítása, ebbe beleértve a **szükséges terepjáró képesség vagy páncélvédettség meglétét;**

- legyen **szállítható vasúton, vízen vagy levegőben**, rendelkezzen a szükséges rögzítési pontokkal;

- lehetőség szerint a **hazai védelmi ipar bevonásával kerüljön kifejlesztésre** (akár más gyártóval történő együttműködés, vagy licencvásárlás is megfontolandó).

Az egyéb műszaki paraméterek, így a hatótávolság, akadályok leküzdési képesség, szállítható felszerelés súlya, tartalék alkatrészek mennyisége, stb. meghatározása a pályázat kiírásakor szükséges az aktuális eljárásoknak megfelelően.

Az alkalmazható gépjármű esetében számos típus figyelembe vehető, egyaránt találhatunk magyar és külföldi gyártmányt. A megfelelő típus kiválasztásakor **számos szempontot kell figyelembe venni**, így a **különböző veszélyek elleni védelem** biztosítottát, a **maximális hatótávolságot és sebességet, terepjáró képesség mértékét**, de akár az **üzemanyag típusát** is. Fontos, hogy feleljen meg különböző NATO szabványoknak, így például a NATO egységes hajtóanyag koncepcióban (NATO STANAG 4362: Single Fuel Conception) foglaltaknak, a védelmi rendszere a vonatkozó NATO szabvány (NATO STANAG 4569: Protection Levels for Occupants of Armoured Vehicles) szerint kerüljön kialakításra, beleértve nemcsak a páncél-, de az ABV védettséget is. Kerek kialakítás esetén jellemző például a Run-flat rendszer beépítése, a légnyomás állíthatóságának biztosítása. Bár az ilyen típusú eszközöknél kevésbé jellemző a szaktechnika beszerelése miatt fellépő helyhiány következtében, de mindenképpen vizsgálandó kérdés, hogy valamilyen (kollektív) fegyverzettel ellátásra kerüljön-e.

Amennyiben nem konténerbe kerül beépítésre a teljes rendszer, akkor **az egyes eszközök modulszerű vagy úgynevezett rack szekrénybe történő beépítése** szintén nagyban megkönnyítheti a gépjármű típusának váltása esetén szükséges átépítést. Az átépítés lehetőségét azért kell a lehető legegyszerűbben biztosítani, hogy az aktuálisan alkalmazott gépjármű típusa az adott műveleti területen alkalmazott gépjárműparkba illeszkedjen, amely mind az erők védelme, mind a logisztikai ellátás szempontjából fontos.

#### Légi járműre történő be- vagy ráépítés esetén alkalmazandó követelmények:

Mint azt az 1. fejezetben már említettem, a Magyar Néphadsereg időszakában már álltak rendelkezésre légi járműre fejlesztett elektronikai hadviselési eszközök. Napjainkban is számos ország rendelkezik ilyen képességgel, mivel a gépjárművekbe épített eszközrendszereknél nagyobb mobilitást és hatótávolságot biztosít, **azonban beszerzése és**

**rendszerben tartása korántsem jár olyan költséggel**, mint egy dedikáltan elektronikai hadviselési célú repülőgép.

A Magyar Honvédség jelenleg meglévő helikopter képessége nem teszi lehetővé – ahogy az a közelmúltban sem volt kivitelezhető – hogy a meglévő helikopterekből – azok alacsony száma – kijelölésre kerüljön egy kontingens és azok átalakításra kerüljenek elektronikai hadviselési eszközökké. Emellett mindenképpen figyelembe kell venni azt is, hogy a Magyar Honvédség helikopteres képessége a katonai célú alkalmazáson felül katasztrófavédelmi feladatokba is bevonásra kerülhet.

A Magyar Honvédség helikopteres képessége fejlesztésre szorul, melynek során **„korszerű navigációs, kommunikációs, illetve aktív önvédelmi (radar és lézer besugárzásjelző, rakétaindítás-jelző, automatikus zavarótöltet kilövő) rendszerekkel”** [173] rendelkező típus beszerzése szükséges. A megfelelő típus kiválasztása esetén a repülőeszközök az országvédelmi és szövetségi feladatok mellett katasztrófavédelmi, kiemelt védelmi és nemzetgazdasági feladatokba is bevonhatóak lehetnek. Az országvédelmi és szövetségi feladatok között szerepel az elektronikai hadviselés is. [173]

Mind a szállító repülőgépek, mind az elektronikai hadviselési eszköz/konténer hordozására képes pilóta nélküli repülőgépek vonatkozásában is hasonló a helyzet, az MH jelenleg minimális mennyiségben rendelkezik ilyen célra alkalmazható eszközökkel, azaz minél előbb javasolt a már többször betervezett beszerzések végrehajtása. Mind a helikopterek, mind a szállító repülőgépek esetében az SDR alapú elektronikai hadviselési rendszer kialakítását **az 1. fejezetben említett JEWCS konténerekhez hasonló megoldással javasolom**, annak érdekében, hogy a beszerzésre kerülő repülőeszközök minél hatékonyabban kerülhessenek kihasználásra, illetve hordozó eszköz esetleges meghibásodása ne jelentse a képesség elvesztését. Vadászipülőgép és pilóta nélküli repülőgép vonatkozásában a felszerelhető konténerméret határolja be a lehetőségeinket, de **a szoftverrádió technológia alkalmazásával ebben az esetben is fejleszthető ki alkalmazható konténer**.

#### Antennarendszerre vonatkozó követelmények:

A hatékony működés miatt mind az egyszeri felhasználású, mind a hordozható, a repülőeszközre szerelhető, illetve a gépjárműves rendszerek esetében is **a legkritikusabb kérdések az antenna fizikai méretei, illetve hordozható és a gépjárműves rendszerek esetében az antenna telepítéséhez szükséges idő és személyzet létszáma**. Ehhez azt is figyelembe kell venni, hogy **a szoftverrádió technológia alkalmazásával jóval nagyobb frekvenciatartomány fogható át, így különböző antennakészletekre lehet szükségünk**. A

jelenleg forgalomban lévő különböző eszközök esetében a gyártók többféle antennával kísérleteznek az előbb említett jellemzők csökkentése érdekében.

**Ideális esetben** a rendszerhez tartozó antennának széles frekvenciasávot, a műveletben alkalmazott valamennyi frekvenciát, más fogalommal **az érdekeltségi frekvenciatartományt**<sup>156</sup>. **képesnek kellene lennie átfogni.** A gyakorlatban azonban ez nem valósítható meg, bár számos kutatás folyik ennek érdekében. A kialakítás módja, vagy a rendelkezésre álló szállítótér miatt korlátozott helykapacitás azt is kizárja általában, hogy több antennát használjunk úgy, hogy mindegyik antenna egy-egy szűkebb frekvenciatartományban üzemeltethető. Emiatt a rendelkezésre álló antenna egy nagyobb frekvenciatartományban lesz alkalmazható, azonban így a nyereség értéke alacsony lesz. [174]

Az antennák méretének csökkentése vonatkozásában számos különböző fejlesztés van folyamatban napjainkban is. Esetünkben a bonyolultságot az jelenteni, hogy egy eszközbe kell implementálni a rádiójelek vételére és az elektronikai zavarás megvalósítására alkalmazandó antennarendszert, úgy, hogy a jellemzők (irányítottság, antennanyereség, stb.) vonatkozásában a lehető legjobb értékeket érhessük el – beleértve a lehető legnagyobb lefogható frekvenciatartományt is. Fontos szempont azonban az, hogy a fizikai méretek nem léphetnek át egy észszerű határt, hiszen **az EHV eszközt a kiépítésnek megfelelő módon ki kell tudnunk juttatni az alkalmazási helyszínre, a katonának vagy a gépjárműnek/légijárműnek szállítania kell tudni. Eme kritériumok mentén kell kialakítani a megfelelő illesztőegységeket, a hordozó platformot, illetve biztosítani kell a gyors telepítés és bontás lehetőségét is.** Amennyiben a fenti kritériumok teljesülnek, még mindig **kérdéses a költséghatékonyság,** amely mind a fejlesztőket, mind a potenciális vásárlókat egyaránt befolyásolja, **nemcsak a beszerzés, hanem a későbbi karbantartás és esetleges továbbfejlesztés esetében is.**

Az **antennák kialakítása során azt is figyelembe kell venni,** hogy sok esetben a műveleti tempó azt igényli, hogy az **EHV támogatás folyamatos legyen. Az első Öböl-háború során negatív tapasztalat volt az, hogy az EHV egységek nem voltak képesek menetben**<sup>157</sup> **támogatni a szárazföldi csapatokat, hanem meg kellett állniuk, felállítani az antennákat,** majd a csapatok előremozgását figyelembe véve bontani és követni az előrenyomulást. [174; 515. old.]

---

<sup>156</sup> Signals of Interest, SOIs

<sup>157</sup> On The Move

**Stacioner feladat** – például országvédelem esetén – **jó megoldást jelenthet és egyetértek azzal az elgondolással, hogy több antennakészletet telepítünk egy-egy eszközhöz** különböző helyszíneken és csak magát az eszközt mozgatjuk. [80; 65. old.] Ez nemcsak gazdasági, szakmai-technikai, de az önvédelem szempontjából is előnyös megoldást jelent.

Az elektronikai támogató és zavaró, illetve rádiófelderítő eszközöket fejlesztő és gyártó cégek többféle kivitelű antennával gyártják technikai eszközeiket, ezek között megtalálhatóak a gépjárműre vagy külön utánfutóra applikált, pneumatikus változatok is. Az is egyértelmű, hogy a hordozható verzióhoz rendszeresíthető antennát sokkal kisebb méretben kell elkészíteni, ami azonban jelentősen befolyásolja a lefogható frekvenciatartományt is.

A **gépjárműre vagy külön utánfutóra szerelt antennák összehasonlítása** során megállapítható, hogy természetesen mindkettő változatnak meg vannak a maga előnyei és hátrányai. **A gépjármű tetejére történő ráépítés – az antenna összecusokott állapotában – kisebb mértékben rontja annak terepjáró képességét, mint a külön utánfutóra történő ráépítés, azonban a magasabb súlypont a vezethetőséget negatívan befolyásolja. A külön utánfutóról történő antennarendszer használata mind a könnyebb telepíthetőség, mind az energiaellátás biztosításának megoldásában egyszerűsítheti a fejlesztést és az üzemeltetést.** Természetesen nem szabad elfelejteni, hogy ebben az esetben az utánfutó vonatkozásában is teljesíteni kell a NATO szabványokban, valamint a hazai műszaki és környezetvédelmi előírásokban meghatározott előírásoknak történő megfelelést. A műholdas kommunikációhoz szükséges VSAT<sup>158</sup> berendezésekre is meg kell határozni a szükséges követelményeket, amennyiben azokat alkalmazni tervezzük.

#### Szoftverek vonatkozásában:

**A korszerű rádióelektronikai felderítő eszközöknek keresési, iránymérési, jelanalizálási, kommunikációs és rendszerirányítási feladataik vannak, mindezen feladatokat pedig különböző algoritmusok, szoftverek és adatbázisok alapján hajtják végre.** [103; 62. old.]

Ez alapján könnyen belátható, hogy az egyes eszközök, valamint az egyes eszközök rendszerként történő működtetése során számos különböző funkciójú szoftverre van szükségünk. A hatékony és folyamatos működés érdekében fontos az, hogy a rendszerben üzemeltetett szoftverek kompatibilisek legyenek a Magyar Honvédségben már korábban

---

<sup>158</sup> VSAT, Very Small Aperture Terminal: műholdelérési szolgáltatásokat biztosító infokommunikációs rendszer, amely űrszegmensből (műholdak), földi vezérlő/irányító elemekből és végponti felhasználói terminálokból áll.



alkalmazásba vett szoftverekkel, beszéljünk akár operációs rendszerekről, akár térkép vagy adatbázis-kezelő szoftverekről. A megfelelő méretű kijelzővel készülő eszközök esetében fontos a megfelelő térképes megjelenítés és az ehhez szükséges szoftver is. **A feladatok ezen stádiumában javaslom a mérési eredmények matematikai modellezéssel történő ellenőrzését/összevetését** a minél nagyobb pontosság elérése, és az esetleges hibák kiküszöbölése érdekében. Ez egyúttal további szoftver-, illetve számítási kapacitásigényt is jelent.

#### Kommunikáció – adatforgalom vonatkozásában:

**Az SDR állomás működésével kapcsolatos kommunikációs lehetőségek vizsgálatához elsődlegesen az állomások működéséhez szükséges adattípusok vizsgálata szükséges.** A vizsgált adattípusokat az alábbiakban mutatom be, megkülönböztetve a harcfeladat végrehajtásához közvetlenül és közvetve szükséges adatokat. A harcfeladat végrehajtásához közvetlenül szükséges adatok alatt a különböző üzemmódokkal kapcsolatos információkat, távvezérlési parancsokat értem, míg a harcfeladat végrehajtásához közvetve kapcsolódó adatok alatt többek között az üzemi paraméterekkel (külső-belső hőmérséklet, stb.), őrzés-védelemmel kapcsolatos információkat értem. **Az SDR technológiához kapcsolódó üzemelési paraméterek módosítását az elektronikai támogató és a rádiózavaró üzemmóddal kapcsolatos adatok közé sorolom. Az üzemeltetéssel kapcsolatos adatok között szereplő szoftverfrissítés alatt az eszközre telepített különböző szoftverek frissítését értem.** [171]

**Az SDR alapú EHV eszközök működtetése érdekében szükséges adatok csoportosítása:**

- **Harcfeladattal kapcsolatos adatok:**
  - Elektronikai támogató üzemmóddal kapcsolatos adatok;
  - Rádiózavaró üzemmóddal kapcsolatos adatok;
  - Távvezérlési parancsok;
  - Kezelő által történő üzemeltetéssel kapcsolatos adatok;
- **Üzemeltetéssel kapcsolatos adatok:**
  - Üzemi paraméterek;
  - Őrzés-védelemmel kapcsolatos adatok;
  - Szoftverfrissítés. [171]

**Az SDR alapú elektronikai hadviselési állomások adatokkal történő feltöltése** alapesetben a bázison/központban folyik, majd megtörténik az állomás kitelepítése. A működés közben szerzett vagy generált adatok továbbítása pedig **erről a telepítési helyről történik a központ irányába, az üzemmóddal illetve távvezérléssel kapcsolatos adatok továbbítása pedig a központtól az állomás irányába.** Ezek alapján egyaránt figyelembe kell venni a vezetékes és vezeték nélküli adatátviteli módokat is, amelyek alkalmazását az áthidalandó távolság függvényében választunk meg. Esetünkben **szükség van egy viszonylag kis távolságú adatátvitel megvalósítására,** amelyhez használhatunk **vezetékes vagy kis hatósugarú vezeték nélküli megoldásokat,** míg a **telepített állomással történő kommunikáció esetében már csak a vezeték nélküli megoldásban** gondolkodhatunk. [171]

A bázison történő adatfeltöltés esetén választhatjuk a jól bevált módszereket, amelyeket napjaink elektronikai eszközeinek programozásakor is alkalmazunk, így például:

- **kis távolságú adatátvitel:**
  - vezetékes (pl. USB csatlakozófelület, optikai és egyéb kábelek);
  - Smart Card Loading, (intelligens kártyáról való letöltés) [175];
  - védett, vezeték nélküli:
    - WLAN;
    - Bluetooth.

Ebben az esetben - mivel az adatforgalom honi területen vagy védett térben történik, gyors és zavarmentes végrehajtás lesz a jellemző.

- **nagy hatótávolságú vezeték nélküli átviteli módok:**
  - VSAT műholdas kapcsolat;
  - harcászati internet, amely a polgári felhasználású internethez hasonló működési elven, azaz az internet protokollok (Internet Protocol, IP) kommunikációján alapul;
  - mikrohullámú adatátvitel;
  - egyéb rádiókapcsolat (pl. WIMAX, stb.). [171]

A **kommunikációs lehetőségekkel kapcsolatban javaslom megvizsgálni a** viszonylag új és a rendvédelmi szervezeteknél még kevésbé alkalmazott adattárolási és elérési lehetőséget biztosító megoldást, **a számítási felhőt, amelynek alkalmazásával az elektronikai hadviselési képesség hatékonysága tovább emelhető.**

A számítási felhő vonatkozásában mindenképpen lényeges az, hogy a felhő katonai alkalmazásának lehetőségét több nemzet és a NATO is vizsgálja, esetenként már alkalmazza is. [176]

Jelenleg a felhőrendszerek rendvédelmi alkalmazásával kapcsolatban – érthető módon – **számos biztonsági kérdés még megválaszolatlan.** Biztonsági kockázat, hogy **a felhőszolgáltatók polgári cégek,** hiányoznak a rendvédelmi ágazat részére megfelelő biztonsági eljárásokat meghatározó szabályozók. Kérdéses, hogy hogyan ellenőrizhető a saját adataink kezelésével kapcsolatos tevékenység, **mi történik** abban az esetben, **ha a polgári szolgáltató szándékosan elérhetetlenné teszi a szolgáltatást, vagy valamilyen egyéb oknál fogva válik azzá.** Az Európai Hálózat- és Információbiztonsági Ügynökség<sup>159</sup> (a továbbiakban ENISA) korábban már említett kiadványa ennél jóval több biztonsági kockázatot is felsorol, azonban azok nagy része más rendszerek esetében is fennáll. Ilyen például a **rejtjelkulcsok kompromittálódása, az adatátvitel során történő lehallgatás, vagy a rendszerek elosztott szolgáltatásmegtagadással járó támadásra<sup>160</sup> történő felhasználása,** stb. [177] Az ENISA dokumentumán kívül is elérhető még számos más, a számítási felhőkkel kapcsolatos biztonsági kérdéseket elemző anyag, amelyek nemcsak segítséget nyújthatnak, hanem a lehetséges katonai alkalmazással kapcsolatos kétségeinket növelhetik. A felvetett biztonsági kérdések megválaszolásában sokat segíthet egy, valamilyen nemzetközi – **a katonai alkalmazás vonatkozásában NATO – szervezet által kidolgozott szabványrendszer,** amely alapján a szolgáltatók osztályozni tudnák saját rendszerüket. [178] A fenti problémákat alapvetően kiküszöböli az, ha **az adott szervezet képes saját maga számítási felhő infrastruktúra kiépítésére és üzemeltetésére.**

Ahhoz, hogy a korábban már említett elektronikai hadviselési folyamatok (például tervezés) anyagai vagy adatok a felhőben tárolhatóak legyenek, több technikai és biztonsági kérdést vizsgálni kell. Az első esetben **a felhőbe felvihető folyamatok, illetve adatok körének meghatározása** a feladat. Megfelelő megoldás lehet, hogy **korlátozzuk a számítási felhőbe felvihető folyamatok anyagait például a minősítés alapján.** Így elképzelhető, hogy egy gyakorlat során a számítási felhőt a közös kidolgozói munka helyszínéül alkalmazzuk, azonban egy valós művelet során már nem. Ez nem feltétlenül jó megoldás, azonban a saját állományunk védelme a legfontosabb szempont. A második esetben a megoldás egy **megfelelő szintű titkosítás alkalmazása lehet, azonban fontos, hogy a kulcsmenedzsment**

<sup>159</sup> European Union Agency for Network and Information Security, ENISA

<sup>160</sup> Distributed Denial of Service, DDoS

**nem adható át a felhőszolgáltató részére.** A különböző elemeknek saját maguknak kell kódolni az adatokat és csak azokat lehet feltölteni a felhőbe.

A számítási felhő elektronikai hadviselési vonatkozású alkalmazása azonban számos, további biztonsági kérdést felvet. **A különböző EHV adatok, természetüknél fogva, mindig magasabb minőségűek, mint az „átlag” katonai információk.** Emiatt sokkal szigorúbb feltételeket kell meghatározni, amennyiben azokat a számítási felhőbe szeretnénk feltölteni. [178]

A rendszer telepítési vagy szolgáltatási modell szerinti kiválasztásának egyik legfontosabb szempontja a rendszer és a szolgáltató által biztosított biztonsági szint. A telepítési modell esetében több dokumentumban is a közösségi számítási felhőt jelölték meg a rendvédelmi szervek vonatkozásában, mint lehetséges verzió, **azonban véleményem szerint az elektronikai hadviselési vonatkozású adatok általánosanál magasabb minősítési szintje miatt a Magán számítási felhő (Private cloud) kiválasztása a célszerű.** Ennek oka, hogy a Magán számítási felhő (Private cloud) esetében **a „teljes rendszer kézben tartott, a biztonság itt garantálható a legjobban, meglévő rendszerek, rendszerelemek felhasználhatóak”.** [179]

A szolgáltatási modell kiválasztása sem egyszerű szempont, ebben az esetben is számos szempontot kell elemezni. **Véleményem szerint a Platform, mint szolgáltatás (Cloud Platform as a Service (PaaS)) vagy az Infrastruktúra, mint szolgáltatás (Cloud Infrastructure as a Service (IaaS)) vehető figyelembe,** mivel a fenti megoldások biztosítják a legnagyobb szabadságot a felhasználónak.

### **A számítási felhő alkalmazásának lehetőségei az elektronikai hadviselés vonatkozásában**

Az elektronikai hadviselés vonatkozásában a két legfontosabb alkalmazási lehetőség az alábbi:

- **a különböző helyszínekről (állomások, központok) történő munkavégzés biztosítása,** így lehetővé téve ugyanazon adatbázishoz, munkaanyaghoz, térképréteghez, stb. történő hozzáférést bárhonnán, több felhasználó részére;

- **a különböző állomások, eszközök közötti adatátvitel biztosítására.** [178]

Az első eset a felhő alkalmazásának egyik alapvető szolgáltatása, a rendelkezésre álló erőforrások felhasználásának mértéke az igényeknek megfelelően kerülhet szintezésre. Ebben az esetben **lényeges kérdés a speciális programok biztosíthatósága.** Az elemző, tervező feladatok során előfordulhat, hogy olyan szoftverekre van/lenne szükségünk, amelyek

beszerzése, annak specifikussága miatt nem biztos, hogy gazdaságilag megéri a szolgáltató számára vagy számunkra. [178]

A második esetben a korábban bemutatott adatok rendelkezésre állását tudjuk biztosítani a különböző állomások részére. **Az SDR alapú elektronikai állomások működéséhez szükséges, az adott harcfelelathoz közvetlenül kapcsolódó adatok** (elektronikai támogató és rádiózavaró üzemmód adatai, a távvezérlési parancsok, illetve a kezelő által történő üzemeltetés során felhasználandó adatok), **valamint az üzemeltetéssel kapcsolatos adatok** (az állomás üzemi paramétereinek, őrzés-védelemmel kapcsolatos adatok, valamint a szoftverfrissítés) **elérhetősége érdekében azokat a felhőbe feltöltve biztosíthatjuk, hogy a különböző helyszínen települő állomások az adatokat bármikor elérhessék.** Ennek egyik lehetséges előnye, hogy az adatokhoz történő hozzáférés jól időzíthető, könnyebben illeszthető a harci munkához és a folyamatban lévő műveletekhez. [178]

Mindenképpen meg kell említenünk a számítási felhő katonai alkalmazásával kapcsolatban a „**combat cloud**”<sup>161</sup> fogalmat is. Az alabamai Légierő Parancsnokság és Törzstiszti Akadémia szerint a harci felhő *„egy átfogó hálózat az adatelosztásra és az információ megosztásra a harctéren belül, ahol minden engedélyezett felhasználó, platform vagy csomópont átlátható módon szolgáltatja az alapvető információkat, illetve megkapja azokat, és képes ezt kihasználni a katonai műveletek teljes spektrumában.”*<sup>162</sup> [180] Az orosz hadsereg saját magának alakít ki ilyen képességet 2020-ig úgy, hogy az első ilyen központ már kiépítésre került a Déli Katonai Körzetben, ahova az elcsatolt Krím-félsziget is tartozik. [181]

### 3.2. Az elektronikai hadviselési rendszer beszerzésének, hazai fejlesztésének, gyártásának főbb kérdései

Az elektronikai hadviselési eszközök és rendszerek beszerzése annak specifikussága miatt nem egyszerű kérdés. A **feladat és a megszerzett és értékelt adatok különlegessége** miatt ezen eszközök és rendszerek esetében **nem beszélhetünk egyszerűen a boltok polcairól kiválasztható termékekről**<sup>163</sup>, **de a NATO rendszerén**<sup>164</sup> **belül sem egyszerűen megoldható kérdés.**

<sup>161</sup> Harci felhő

<sup>162</sup> Saját fordítás.

<sup>163</sup> COTS (Commercial Off The Shelf) – a kereskedelemben, a boltok polcain könnyen elérhető megoldások.

<sup>164</sup> NOTS (NATO Off The Shelf) – a NATO dokumentációkban az „N” betű a szűk piaccal rendelkező, speciális igényeket kielégítő termékekre utal.

A védelmi piacon számos cég kínál elektronikai hadviselési eszközöket, azonban **komplex rendszerek már csak kisebb számban érhetőek el**, illetve ahhoz, hogy a Magyar Honvédség érdekeit hatékonyan szolgáló rendszer kerüljön beszerzésre vagy kifejlesztésre, **nagyon egyértelmű és reálisan megvalósítható feltételeket** kell a beszerzési eljárás során meghatározni.

Egy **komplex elektronikai hadviselés rendszer beszerzése** – hasonlóan más, nagy bonyolultságú rendszerekhez, legyen szó radar, repülőgép, tüzérségi, vagy akár egy komplex gép és harcjármű beszerzésről – **számos nehézséget** hordoz magában, **amely nemcsak gazdasági, de technikai, technológiai vonatkozású is lehet**. Egy-egy új rendszer beszerzésénél rendkívül fontos, hogy a már meglévő rendszerrel az új rendszer mennyire kompatibilis, mennyire illeszthetőek egymáshoz. Mindezt annak tükrében kell megvizsgálni, hogy amennyiben **az új rendszer elemeiben különböző időben – esetleg különböző cégtől** – kerül beszerzésre, **felléphetnek különböző kompatibilitási problémák**, amelyek az adott rendszerek hatékony működését negatívan befolyásolják, illetve akár komolyabb működési problémákhoz vezethetnek.

Fontos kérdés az is, hogy a piacon elérhető vagy – a magyar ipar felhasználásával – saját fejlesztésű eszközök, rendszerek kerüljenek beszerzésre. Mindkét változatnak meg vannak a maga előnyei, amelyet a megfelelő szintű döntéshozóknak kell mérlegelniük.

*„Az önálló fejlesztés költsége többszöröse lehet a „kész” megvásárolható rendszerelemeknek. A kereskedelembe kapható szoftverek támogatottsága általában lényegesen jobb, mint az egyedi fejlesztésű rendszereké. Figyelembe kell venni azt is, hogy az önálló fejlesztés lényegesen több időt igényel, mint egy „kész” vett, már többször bizonyított rendszer adaptációja.” [182]*

A fenti összehasonlítással kapcsolatban lényegesnek gondolom, hogy annak ellenére, hogy informatikai beszerzéssel kapcsolatban került összeállításra, az első és harmadik pontjait az elektronikai hadviselési rendszerek beszerzése esetén is figyelembe lehet venni, már meglévő rendszerek beszerzése melletti érvként. A második szempont esetünkben kevésbé vehető figyelembe, **azonban fontos, hogy pont ezen egyedi fejlesztés miatt – mivel javaslatom alapján erre a feladatra a hazai ipar képviselői kerülnének felkérésre – vélelmezhetően gyorsabban reagálnának (pl. rövidebb helyszínrre érkezési idő, rövidebb szállítási idő, stb.) az MH használatában lévő eszközökkel kapcsolatos problémákra.**

Az állami szervezetek és így a Magyar Honvédség által végrehajtott beszerzések jogi alapját a közbeszerzésekről szóló 2011. évi CVIII. törvény képezi. Az értekezésben

javasoltaknak megfelelő elektronikai hadviselési rendszerek beszerzése esetén meghívásos eljárás végrehajtása indokolt, mivel a meghatározásra kerülő feltételek teljesítésére alkalmas ajánlattevők száma kevés.

A következő **rendkívül fontos kérdés a beszerzés során alkalmazandó értékelési szempont rendszer kialakítása.** A szempont egy olyan, a beszerzési folyamat során alkalmazandó és elvárt tulajdonság, amelyet az előkészítés során a szakemberek kiválasztanak, a fontosságának megfelelően súlyoznak, így segítve a döntési folyamatot. [182]

Az elektronikai hadviselési rendszer esetében kiemelt szempont lehet a legfontosabb fizikai paraméterek csoportja, a módosíthatóság, a továbbfejleszthetőség, a más rendszerekkel meglévő kompatibilitás, a modularitás, a karbantartás, a biztonság, dokumentáció és képzés, vagy a beszállító cég által vállalt garancia tartalma. Természetesen fontos szempont a pénzügyi teljesítés rendszere, de a beszállító cég szakmai tapasztalata is.

Az 1.3.2. alfejezetben már bemutattam, hogy korábban több, védelmi célú elektronikai alkatrészt és eszközt gyártó magyar vállalat létezett. Napjainkban is elérhető több védelmi célú fejlesztéssel, vagy a védelmi iparban is alkalmazható eszközöket gyártó cég.

A **Honvédelmi Minisztérium négy hadiipari cég tulajdonosi jogkörét gyakorolja,** ezek a mindegyike rendelkezik **hivatalos NATO beszállítói címmel.** Az egyik legnagyobb és legismertebb ilyen védelmi célú vállalat a HM ARZENÁL Elektromechanikai ZRt., amely különböző fegyverrendszerek szervizelésével, fejlesztésével foglalkozik. A ZRt. által fejlesztett rendszerek között megtalálhatóak különböző radarrendszerek (P-18, P-37, Mistral légvédelmi rakéta rendszer, stb.), illetve további fejlesztések is. [183] A másik három a HM ARMCOM Kommunikációtechnikai ZRt., a HM Elektronikai, Logisztikai és Vagyonkezelő ZRt. és a HM CURRUS Gödöllői Harcjárműtechnikai ZRt.

**Az állami tulajdonú hadiipari cégek és a védelmi eszközök fejlesztésével és gyártásával is foglalkozó üzleti szféra között az együttműködés megvalósulhat,** melyet mutat például a BHE Bonn Hungary Elektronikai Kft., mint konzorcium vezető és a HM ARMCOM Kommunikációtechnikai ZRt. közötti együttműködés. A konzorcium a "Nagy megbízhatóságú, nemzeti biztonsági stratégiai műveletet támogató MIMO adatrádió rendszer kifejlesztése, gyártásának és üzemeltetésének előkészítése hazai platformokon" elnevezésű projektre nyert el támogatást a "Vállalatok K+F tevékenységének támogatása (KFI\_16)" című felhívás keretében. [184]

A hordozó eszközök vonatkozásában kettő magyar gép- és harcjármű termékcsaláddal foglalkozom. Ezek egyike a RÁBA gépjárműcsalád, a másik lehetőség pedig a Komondor könnyű-páncélvédettségű többcélú harcjármű család.

### RÁBA gépjárműcsalád

*„A Rába Jármű Kft. Jármű üzletág nemzetközi partnereivel együtt 2018-ig a Magyar Honvédség kizárólagos terepjárójármű beszállítója. A katonai beszállítás a 2003-ban aláírt szállítási keretszerződésben szereplő öt terepjáróosztály járműveit érinti. A speciális katonai felhasználásra szánt Rába H típusú járműcsalád több mint egy évtizedes fejlesztőmunka eredménye.”*[185] A Kft. nyilatkozata alapján **a gépjárműcsalád egyes elemei képesek megfelelni a modern hadviselési követelményeknek, sokoldalúan felhasználhatóak, szállíthatóak vasúton, repülőgépen és hajón is. Különböző védelmi megoldásokkal kerültek felszerelésre (pl. felderítés elleni védelemmel), de páncélvédelemmel is elláthatóak.**[185]



3.1. kép: H18.206DAE-001 terepjáró bázisjármű. [186]



Főbb jellemzők:

- a járműcsalád kielégíti a NATO interoperabilitás követelményeit;
- a személyzet opcionális páncélvédelme;
- a beépített fő- és részegységek maximális azonossága, különböző célú felépítmények széles választéka;
- optimális logisztikai háttér;
- központi gumiabroncsnyomás-szabályozó rendszer opciós beépítése;
- családellen felépülő három terhelési kategória;
- Hercules C130 típusú repülőgépen való szállíthatóság, illetve a korlátok nélküli vasúti szállítás lehetősége.

#### Komondor könnyű-páncélvédettségű többcélú harcjármű család

A 2015-ben egybeolvadó és attól az időponttól Gamma Műszaki Zártkörű Részvénytársaság néven működő Respirátor Zrt. és a Gamma Zrt. **könnyű-páncélvédettségű harcjármű-család** fejlesztésébe kezdett 2010-ben.

A Nemzeti Fejlesztési Ügynökség (NFÜ) "Vállalati innováció ösztönzése (KMOP 1.1.4-09)" tárgyában meghirdetett pályázatán a Gamma Műszaki Zrt. **"Terepjáró, moduláris ballisztikai védelemmel ellátott ABV-felderítő jármű fejlesztése"** témában támogatást nyert el. A fejlesztés során a Gamma Zrt. kifejlesztett egy „atom-, biológiai-, és vegyi szennyezések mobil felderítésére, analizálására és behatárolására alkalmas komplex rendszert, amely mind a katonai, mind a katasztrófavédelmi alkalmazási igényeknek képes megfelelni és mindez egy magyar tervezésű és gyártású bázisjárműre kerül integrálásra. A most kifejlesztett ABV-felderítő jármű képességeinek jelentős bővülését az tette lehetővé, hogy már az alapjármű tervezésekor figyelembe vételre kerültek az ABV-felderítés speciális igényei is.” [187]



3.2. kép: RDO-3221 KOMONDOR jármű, tetején a Pro Patria Electronics Kft. által forgalmazott PGSR-3i 'Beagle' mozgócél felderítő radarral. [188]

A Zrt. Komondor gépjárműcsaládjában a már említett atom-, biológiai-, és vegyi szennyezések felderítésére alkalmas gépjárművön kívül számos egyéb feladatrendszerre optimalizált típus érhető el.

Ezek közül kiemelnék néhány fontosabbat, ezzel is mutatva a variálhatóságot és a rendelkezésre álló lehetőségeket:

- **mobili vezetési pont;**
- **felderítő jármű;**
- páncélozott sebesültszállító jármű;
- légvédelmi rakéta hordozó és indító jármű;
- műszaki mentő jármű. [187]

A cég rendelkezik képességgel nagyobb teherbírású járművek (6x6), illetve utánfutók gyártására is, melyet a 3.1. ábrán illusztrálunk.



3.1. ábra: A Gamma Zrt. nagy teherbírású járműve (bal oldalon) és beépített utánfutója (jobb oldalon) [189]

A hordozójárművek vonatkozásában természetesen több más, kisebb nagyobb vállalat is bevonásra kerülhet, így például a nagy múltú IKARUS autóbuszgyár, illetve a különböző autómárkák (pl. Suzuki, Audi, Opel, Mercedes) hazánkban települt gyáregységei.

#### A szoftverfejlesztés és tesztelés kérdései:

Amennyiben **saját fejlesztésű eszközökről és rendszerekről** beszélünk, mindenképpen foglalkozni kell a szoftverfejlesztés kérdésével is. Lehetőségünk van különböző cégek **szoftvereinek megvásárlására**, illetve természetesen az eszközzel együtt **saját szoftver is fejleszthető**. Mindkettő megoldásnak meg vannak az előnyei, hátrányai, amelyeket a követelmények meghatározása során gondosan, minden aspektusára kiterjedően vizsgálni kell. **Ezen szempontok között nemcsak a költségek, a fejlesztői támogatás időtartama, a követelményeknek való megfelelés kérdései szerepelnek, de mind a magán, mind az üzleti és a katonai alkalmazásnál is egyre fontosabb szemponttá váló biztonság is.** A biztonság vonatkozásában lényeges, hogy nemcsak a nem szándékos biztonsági problémákkal (pl. fejlesztői hibák) kell számolnunk, hanem például a szándékosan kialakított behatolási pontokkal (pl. back-door), az engedélyünk/tudtunk nélkül beépített szoftverösszetevőkkel (pl. tevékenységünkről jelentő szoftverek beépítve az általunk megrendelt szoftverben) is.

**Vásárolt szoftver** alkalmazása mellett szól, hogy **a saját fejlesztésűnél hamarabb integrálható be a rendszerbe, a tesztelések már a forgalmazást megelőzően megtörténtek.** Hátránya, hogy **kevésbé illeszkedik az elvárásainkhoz, az esetleges módosítások/továbbfejlesztések nehezebben kivitelezhetőek.** Mindenképpen lényeges és egyben fontos biztonsági kockázat, hogy az **eszközünk/rendszerünk képessége mások előtt is ismert lesz.** Emellett azt is ki kell emelni, hogy ebben az esetben **a biztonsági rések feltárására és azok megszüntetésére nagy hangsúlyt kell fektetni.**

A saját szoftver kifejlesztésének és az azzal történő üzemelésnek az előnye az, **hogy a felállított fejlesztőcsoport a rendelkezésünkre áll**, az a későbbiekben is összehívható lehet, így jelentős rugalmasságot biztosít a szükséges módosítások és továbbfejlesztések során, illetve mindenképpen **biztonságosabbnak ítéltető**, mintha egy cég fejlesztését vásárolnánk meg. **Hátránya**, hogy egy új szoftver **kifejlesztése, annak tesztelése és a feltárt problémák megszüntetése hosszú időt vesz igénybe.**

A szoftverfejlesztéssel és az azon alapuló informatikai rendszertervezéssel kapcsolatban számos elv létezik, így többek között a Vizesés modell, az Evolúciós modell, a Komponens alapú és újrafelhasználható rendszerfejlesztés, a Spirális fejlesztés és más megoldások.

*„A szoftverfejlesztés életciklusában megjelenő általános feladatok a következők:*

- 1. Követelmények megfogalmazása – funkcionális specifikáció;*
- 2. Rendszertervezés (design) – rendszerterv;*
- 3. Kódolás, testreszabás és tesztelés;*
- 4. Bevezetés.” [190]*

A rendszerfejlesztés egyik legkritikusabb része a **szoftvertesztelés**, amelynek célja, hogy a fejlesztés során ellenőrizzük, hogy a **szoftver valóban meg fog-e felelni a megrendelői elvárásoknak, illetve maga a szoftver megfelel-e a feladatra.** A szaknyelvben ezen eljárást szoftvervalidációnak nevezik, melynek elemei a verifikáció és a validáció. A szoftvervalidáció részeit képezik a szemlék, a felülvizsgálatok a folyamat teljes ideje alatt. A verifikáció célja annak ellenőrzése, hogy a „szoftver megfelel-e a specifikációnak, azaz eleget tesz-e a funkcionális és nem funkcionális követelményeknek”. A validáció célja annak meghatározása, hogy a szoftverrel „teljesül-e a vásárló elvárása, amibe beleértendő olyan nem funkcionális tulajdonságok is, mint a hatékonyság, hibatűrés, erőforrásigény”. [190; 133. o.]

**A szoftvertesztelés feladatai nagyban függenek attól, hogy vásárolt szoftverről, vagy általunk fejlesztett szoftverről van szó.**

Az eszközzel megvásárolt szoftver esetében a tesztelés módja és ideje a **beszerzési eljárás során meghatározott feltételektől függ.** Lehetséges, hogy már a fejlesztés bizonyos fázisaiba is bekapcsolódhatunk, így már akár a folyamat során is felfedhetők lehetnek bizonyos hibák. Vásárolt szoftver esetében a legfontosabb **az átvételi teszt**, de mindenképpen gondolni kell arra is, hogy az üzemeltetést megelőzően, vagy az üzemeltetés során vizsgáljuk

a rendellenes működést a lehetséges biztonsági problémák feltárása érdekében. Fontos, hogy vásárolt eszköz esetében az azzal **együtt szállított program forráskódjának** átadását is tartalmaznia kell a szerződésnek **a későbbi fejleszthetőség/módosíthatóság érdekében.**

**Saját fejlesztésű** szoftver esetében **a tesztelés a fejlesztés egyes lépéseiben már végrehajtható az adott részfeladatra, illetve a fejlesztés végén a teljes programra vonatkozóan.** Így jóval korábban rendelkezünk információval az egyes problémákról, illetve szükség esetén bele is tudunk avatkozni a fejlesztés menetébe. **Saját fejlesztés esetén az alkalmazó a végső tesztelésen is részt vehet, így lerövidítve az átadás idejét.**

A szoftver vizsgálata lehet statikus, vagy dinamikus. A statikus vizsgálat a dokumentumok, tervek, illetve a forráskódok ellenőrzésére terjed ki. **A dinamikus átvizsgálás a tényleges szoftvertesztelés,** melynek során tesztadatok alkalmazásával ellenőrizzük, hogy a szoftver működése megfelelő-e.

A szoftvertesztelés eredményeivel kapcsolatban két fontos fogalom a prioritás és a súlyosság. A prioritás a hiba kijavításának sürgősségét jelenti, míg a súlyosság azt, hogy mekkora a hiba kihatása a működésre. Mindenképpen ismerni kell a definíciók pontos jelentését annak érdekében, hogy a tesztek eredményeit helyesen értelmezzük. Lehet, hogy egy súlyos hiba kijavításának szükségességét hátra sorolják, mivel a hiba bekövetkezésének rendkívül csekély a valószínűsége. [191]

**A fentiek alapján, akár saját fejlesztésű, akár vásárolt szoftverekről beszélünk, mindenképpen célszerű lehet egy saját szoftverfejlesztő – szoftvertesztelő informatikai állomány megléte.**

### **3.3. A szoftverrádió alapú elektronikai hadviselési eszköz és rendszer elleni támadás és a védelem módszerei, kiemelten az informatikai támadások vonatkozásában**

A szoftverrádió alapú eszközök esetében sok dokumentumban csak az előnyöket említik, ezek között felsorolva például a nagyobb hatékonyságú frekvencia felhasználást vagy a könnyebb és gyorsabb továbbfejlesztés lehetőségét. Nem szabad elfelejteni azonban, hogy az előnyök mellett hátránya is van a technológiának, mivel **a szoftverrádió technológia alkalmazása további felderítési/támadási lehetőségeket indukál.** Ezekkel részletesebben az utolsó alfejezetben foglalkozom.

**A lehetséges támadási módok és a várható támadás hatékony elhárításához** szükséges védelmi megoldások kutatása és meghatározása előtt szükséges annak vizsgálata, hogy **eszközünket milyen módszerekkel deríthetik fel a különböző támadási módszerek**

esetében. Ennek vizsgálatához foglalkozom mind a gépjárműbe épített, mind a repülőeszközre szerelt EHV eszközök felderíthetőségével.

A felderítést követően az EHV eszköz/rendszer pusztítása történhet fizikai módon, az úgynevezett „kemény típusú” („Hard Kill”) támadásokkal, illetve az úgynevezett „lágy típusú” („Soft Kill”) támadásokkal. [192] Dolgozatomban nem vizsgálom részletesen a „kemény típusú” támadások kivitelezését, a „lágy típusú” támadások esetében pedig alapvetően az informatikai támadásokra fókuszálok.

### 3.3.1. A hordozójárművek/objektumok felderíthetősége

A katonai gépjárművek és objektumok felderítését korábban főként **optikai, infravörös vagy akusztikai eszközök** alkalmazásával tervezték. Napjainkban **azonban több új**, a katonai felderítésben is alkalmazható lehetőség jelent meg, például a **szintetikus apertúrájú radar**<sup>165</sup> vagy a **lézer alapú távérzékelés**<sup>166</sup>. A szintetikus apertúrájú radar alkalmazásán alapuló felderítés alapja a valósnál többszörösen nagyobb méretű antenna szintetizálása, úgy mintha egy óriási, valós antennával<sup>167</sup> történő mérés történné. A rendszer előnye, hogy nagy pontossággal képes az eltérő radarkeresztmetszettel rendelkező elemek egymástól történő elkülönítésére, például egy haditechnikai eszköz kimutatására az erdőben. [193] A lézer alapú távérzékelés alkalmazásával, sűrű mintavételezés mellett a fakorona és a felszín visszaverődése könnyen elkülöníthető, így a fémeket tartalmazó haditechnikai eszközök könnyen felderíthetőek. [194] Repülőeszköz esetében a különböző földi radarok, illetve légtérellenőrző repülőgépek felderítési távolságát kell figyelembe vennünk.

A hordozó eszközök és objektumok **védelme érdekében különböző festékek, multispektrális álcázások, speciális bevonatok alkalmazását illetve speciális anyagból történő kialakítást** tervezhetjük. Kiemelt figyelmet kell fordítanunk a **jelentős hőkisugárzással vagy hanghatással** járó elemekre. A különböző aerosolok, füstködök felhasználása pontos tervezést igényel, hiszen ezekkel felhívhatjuk a figyelmet az eszköz telepítési helyére, azonban az eszköz veszélyhelyzetben történő kivonása során alkalmazásuk célszerű lehet. A radar alapú felderítés ellen védekezhetünk **elektronikai zavaróeszközök, rádiólokációs álcázás alkalmazásával**. Elektronikai zavarás esetén saját eszközeinket védhetjük, ha azt egy távolabbi platformról, vagy több eszköz bevonásával, azok grafikon

<sup>165</sup> Synthetic Aperture Radar, SAR

<sup>166</sup> Light Detection and Ranging, LIDAR

<sup>167</sup> Real Aperture Radar, RAR

szerinti üzemeltetésével és áttelepítésével hajtjuk végre. A zavarás tervezése során azt is ellenőrizni kell, hogy saját eszközeink képesek-e továbbra is interferenciamentesen üzemelni. **A rádiólokációs álcázás végrehajtását az álcázó eszközök mérete és a rendelkezésre álló szállítókapacitás behatárolja.** A rádiólokációs álcázó eszközök MH-ban történő alkalmazását már említettem az első fejezetben.

### 3.3.2. Az elektromágneses kisugárzás alapján történő felderítés

Az állomás az **üzemszerű működés során kibocsátott elektromágneses kisugárzás alapján is felderíthető.** Ilyen kisugárzással jár az elektronikai zavarás, az elektronikai támogató tevékenység során megszerzett adatok, valamint az üzemeltetéssel kapcsolatos információk továbbítása. Az állomás üzemelése során továbbításra kerülő adatokat a 3.1. fejezetben bemutatam. **Elektronikai zavarási tevékenységünk során a szemben álló fél – természetesen megfelelő technikai háttér megléte esetén – képes eszközünk helyzetének meghatározására és pusztítására, mind a földi, mind a légi eszköz esetén.** Az elektronikai támogató tevékenység során megszerzett adatok, valamint az üzemeltetéssel kapcsolatos információk (pl. távvezérlési parancsok vagy szoftverfrissítés vétele) továbbítása általában **rövid idejű kisugárzást jelent**, így annak felderítése nehezebb feladat. [171]

Az ebbe a kategóriába tartozó támadások között kiemelném az „Alvás megvonás” (sleep deprivation) elnevezésű, az „Alvás megtagadás” (Denial of sleep) típusú támadások közé sorolt módszert is. **A támadás célja, hogy a vezeték nélküli szenzorok folyamatosan „ébren” legyenek, ezzel csökkentve a hasznos működésükre maradó időt.** Ez például a rádiófelderítő és zavaró, egyszeri felhasználású eszközöknél úgy valósítható meg, hogy értéktelen információtartalmú forgalmazással működésre, azaz a forgalmazás hallgatására vagy zavarására kényszerítik az eszközöket, így lemerítve a rendelkezésre álló energiaforrásukat. Egy másik lehetséges módzat, hogy a megtévesztő adás teljesítményének növelésével az elektronikai zavaráshoz szükséges teljesítmény növelésére kényszeríti az eszközünket, így csökkentve a rendelkezésre álló üzemidőt. [195]

**Az EHV eszközök vonatkozásában is több – beépíthető, illetve az üzemeltető által alkalmazható – védelmi megoldás közül választhatunk.** A gyártás során kialakítható a **frekvenciaugratásos képesség** vagy alkalmazhatjuk a már említett **kognitív rádió koncepciót.** Üzemeltetői fogás a „**háborús frekvencia**” kategória kijelölése, melynek célja, hogy békeidőben az eszköz működési frekvenciatartományából adott frekvenciák használatát



tiltjuk, így szükség esetén feloldva a korlátozást a szembenálló fél számára nem ismert frekvenciákat tudunk alkalmazni. A **kisugárzás korlátozás**<sup>168</sup> célja, hogy a kisugárzást a lehető legrövidebb idő alatt hajtsuk végre. Ez magában foglalja a zavarás időszakos megszakítását, a zavart adó kisugárzásának ellenőrzését. A zavarás végrehajtását zavarási grafikon alapján ajánlott végrehajtani, mellyel tervezhetjük elektronikai hadviselési eszközeink telepítési helyeinek már említett változtatását.

### 3.3.3. Informatikai támadás és védelem

Az EHV eszközök esetében is figyelembe kell venni az informatikai támadásokat, melyek napjainkban az egyik leggyakrabban elkövetett és sokszor sokak életét negatívan befolyásoló eseménytípussá váltak. Mivel fontos katonai rendszerekről beszélünk, ezen rendszerek esetében is ki kell alakítani a megfelelő kibervédelmet, amely a kibertérből jelentkező fenyegetések elleni védelmet jelenti, beleértve a saját kibertér képességek megőrzését is. [196]

Véleményem szerint kijelenthető, hogy az **SDR alapú EHV eszközök** esetében is – hasonlóan az általános számítógép–hálózatokhoz – **biztosítania kell a rendszernek a bizalmasság – sértetlenség – rendelkezésre állás feltételrendszer meglétét**. A bizalmasság jelentése az, *„hogy a tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról”*. A sértetlenség arra vonatkozik, hogy *„az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve azt, hogy az az elvárt forrásból származik és ez ellenőrizhető”*, illetve azt, hogy *„az elektronikus információs rendszer eleme rendeltetésének megfelelően használható”*. A rendelkezésre állás azt jelenti, hogy az *„elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak”*. [196]

Az informatikai támadások elkövetése előtt a támadónak szintén meg kell találnia, fel kell derítenie rendszereinket. *„A számítógép–hálózati felderítés szoftveres vagy hardveres úton való behatolást jelent a szembenálló fél számítógépes rendszereibe, illetve hálózataiba, azzal a céllal, hogy hozzáférjünk az adatbázisaiban tárolt adatokhoz, információkhoz, és azokat felderítési céllal hasznosítsuk.”* [197] Azt, hogy ilyen támadás egy többszörösen védett rendszer esetében is kivitelezhető, az iráni ipari létesítmények ellen 2010-ben

---

<sup>168</sup> Emission control, EMCON



végrehajtott számítógépes támadás bizonyítja. A támadás, melynek során az ipari rendszerek feletti irányítás átvételére szolgáló Stuxnet vírus jutott be, mintegy 30 ezer számítógépet érintett. [198]

*„A számítógép–hálózati támadás szoftveres vagy hardveres úton való behatolást jelent a szembenálló fél számítógépes rendszereibe, illetve hálózataiba, azzal a céllal, hogy tönkretessük, módosítsuk, manipuláljuk, vagy hozzáférhetetlenné tegyük az adatbázisaiban tárolt adatokat, információkat, illetve magát a rendszert vagy hálózatot.”* [197; 3. o.]

A sikeres informatikai támadás lehetséges eredményei:

- *„Sérülés (corruption), vagyis az informatikai rendszerben található adatokat a támadónak sikerül megváltoztatnia, vagy törölnie.*
- *Szivárgás (leakage), amikor a támadónak olyan adatokat sikerül megszereznie, amihez nem szabadna hozzáférnie.*
- *Megtágadás (denial), a megtámadott rendszer működése lehetetlenné válik.”*[199]

Az informatikai támadás hatása lehet rövid vagy hosszabbtávú, de okozhatja a rendszer teljes, visszaállíthatatlan összeomlását is.

Esetünkben az informatikai támadások elkövetői az alábbi csoportokból kerülhetnek ki:

- Szemben álló, vagy egyéb, a saját erőinkről adatot gyűjtő regulális hadsereg, irregulális, vagy hírszerző szervezetek.
- Szervezett bűnözők pénzügyi célból.
- Terroristák ideológiai célból.
- Politikai csoportok.
- Ipari kémek.
- Tudásukat tesztelő, vagy már képzett hackerek.

A számítógépes hálózatokra definiált támadási kategóriák egyik lehetséges csoportosítása az alábbi:

- *„Fizikai: a rendszer elemeinek eltulajdonítása.*
- *Gyenge pontok: a rendszer gyenge pontjainak kihasználása engedély nélküli hozzáférés céljára.*
- *Rosszindulatú programok: speciális programkódok rendszerbe juttatása az ott tárolt adatok megsemmisítésének szándékával.*

- **Hozzáférési jogok:** felhasználók hitelesítési adatainak megszerzése és így a rendszer erőforrásainak jogosulatlan felhasználása.
- **Kommunikáció-alapú:** a hálózati hozzáféréseken keresztül végrehajtott támadások (hamisítás, lehallgatás).” [199; 21. old.]

Konkrét védelmi megoldások alkalmazása érdekében az **alább felsorolt biztonsági problémákat kell kiemelten figyelembe vennünk:**

- **Az operációs rendszerek, egyéb programok sebezhetősége**, melyre a gyártók által biztosított hibajavítások megoldást jelenthetnek, azonban azt mindenképpen figyelembe kell venni, hogy **egy-egy ilyen biztonsági rés sok esetben az adott hibát kiaknázó támadás felfedésekor derül ki.** A hibajavítás fejlesztése ezt követően kezdődik meg és kerül kiadásra.

Kritikus lehet a „zero day exploit”, azaz a „**nulladik napi támadás**”, melynek lényege, hogy a szoftverfejlesztőnek nulla napja van egy felfedezett biztonsági rés esetében a hibajavítás kiadására, hogy megszüntesse a felhasználók sérülékenységét. Mindeközben azonban már lehet, hogy mások is felfedezik a biztonsági rést és támadásokat indítanak. [200]

Ebben a körben kell foglalkozni a korábban már említett back-door programok jelentette biztonsági kérdéssel is.

- **Az adatátvitel (vagy a gyártás) során esetlegesen feltelepülő rosszindulatú programok alkalmazása** szintén olyan problémát jelentenek, melyekkel foglalkozni kell. Ebben az esetben fontos, hogy a korábban már említett vezeték nélküli adatátviteli megoldások (infra, Bluetooth, WLAN, stb.) esetében számos olyan támadási megoldás létezik, amely **az adatok védelme mellett további védelmi megoldásokat igényel.**

- **A felhasználói hibák** közé sorolhatóak a személyi állomány nem megfelelő tevékenységéből adódó problémák, melynek során **a felhasználó nem engedélyezett programot telepít**, vagy engedélyezett program telepítése, alkalmazása során **olyan programtevékenységet is engedélyez, melyet nem ért**, így lehetővé teszi a programba rejtett rosszindulatú kódok futtatását. De ide sorolandó az is, hogy **a felhasználók megosztják egymással felhasználónevüket és jelszavukat.** A felhasználók nem megfelelő tevékenysége során az is problémát jelent, hogy egy kívülről támadóval szemben már eleve több információval rendelkeznek a rendszer védelmi képességéről, jogosultságuk szerint képesek lehetnek akár a védelmi rendszer részleges, vagy teljes kikapcsolására.

A fentiekén kívül számos támadási módszer kivitelezhető, ezek között mindenképpen meg kell említeni a **szolgáltatás-megtagadásos támadást**<sup>169</sup> (DoS, Denial of Service), a **felhasználó megtévesztését** (social engineering), **rosszindulatú/kártékony programok telepítését**, illetve a **közbeékelődéses támadást** (Man in the Middle). A fent említett támadási módszerek többsége további támadási fajtákat foglal magában, amely mindegyike külön-külön védelmi megoldás kialakítását teszi szükségessé.

A számítógép–hálózati védelem részeként nemcsak az eszköz, hanem a teljes rendszer esetében végig kell gondolnunk a védelmi lehetőségeket, **komplex informatikai biztonsági rendszert** kialakítva, **felhasználva a passzív és aktív hálózatvédelmi módszereket**.

Valamennyi érintett terület (személyi biztonság, fizikai biztonság, adminisztratív biztonság, elektronikus információbiztonság) esetében vizsgálni kell az aktuális szabályozóknak, a valószínűsíthető támadási lehetőségnek megfelelő védelmi megoldásokat. Kiemelt figyelmet kell fordítanunk az **elektronikus információbiztonság részterületeire** (átviteli biztonság, kompromittáló kisugárzás elleni védelem, rejtjelzési biztonság, számítógép- és hálózati biztonság) annak érdekében, hogy ne csak egy eszközre, hanem a **teljes rendszerre érvényes és valóban alkalmazható biztonsági szabályok és védelmi megoldások** kerüljenek kidolgozásra. Fontos kérdés **a kezelőállomány kiképzése, felkészítése**, a védelemnek erre a területre is ki kell terjednie. [197] [201] Nem szabad azt sem elfelejteni, hogy az egyes eszközök vagy rendszerek különböző műveleti környezetben (pl. békeidőszak, országvédelem, békétámogató művelet, stb.) is alkalmazásra kerülhetnek.

Az elektronikai hadviselési eszközök és rendszerek **komplex informatikai védelmének magában kell foglalnia az adminisztratív védelmet** (pl. informatikai és titokvédelmi szabályzók, stb.), **a fizikai védelmet** (pl. vagyonvédelmi rendszerek alkalmazása, stb.) és a **technikai/logikai védelmi megoldásokat** (valós idejű behatolás-detektálás és elhárítás, rosszindulatú szoftverek elleni védelem, tűzfal, stb.).

### **3.3.4. Az SDR koncepció alkalmazása következtében fellépő új támadási módszerek és az ellenük kialakítandó védelem**

Az előző alponthan említett támadási és védelmi megoldások bármely EHV eszköz vagy rendszer esetében alkalmazhatóak, ahol számítógép vagy számítógépes-hálózat alkalmazásban van, azonban **jelen alfejezetben specifikusan az SDR alapú EHV eszközök**

---

<sup>169</sup> DoS, Denial of Service

**és rendszerek ellen végrehajtható támadások és az ezen támadások ellen alkalmazható védelmi megoldások elemzésével** foglalkozom. A szoftverrádió technológia alkalmazása esetén mindkettő alfejezetben elemzett támadási és védelmi megoldásokkal számolni kell a rendszerünk kialakítása során, mivel az SDR koncepció alkalmazása a támadási lehetőségek számának növekedésével jár.

Az SDR technológiát alkalmazó rendszerek elleni támadások egy lehetséges csoportosítása szerint a támadások lehetnek:

- **A rádió feletti irányítás megszerzése (Radio Control):** ebben a támadási típusban a támadó megpróbálja megszerezni **az irányítást a rádió készlet egy része vagy teljes egésze felett**. Ennek végrehajtása érdekében rosszindulatú szoftvert juttatnak be a rádióba vagy a rádiófrekvenciás interfészen keresztül vagy valamely fizikai kapcsolatán keresztül. Az ilyen támadások célja lehet például a megfelelő működés akadályozása a rendszerbiztonság kompromittálása érdekében. A rosszindulatú szoftver bejuttatásának módja lehet például a puffer túlsordulás vagy a hullámforma letöltés felhasználása, de számolnunk kell azzal is, hogy a rosszindulatú program már a gyártás során is belekerülhet az adott elemekbe (hardver trójai). [202]

- **Megszemélyesítés (Personification):** ebben a támadási módszerben a támadó célja **az SDR megtévesztése, miszerint a behatoló a rádióháló része vagy jogosult belépni abba**. Ez a támadás szolgálhat például hamis, elévült vagy érvénytelen információ rendszerbe történő bevitelére, továbbítására, az SDR működésének megváltoztatására. Ide sorolják például a visszajátszásos támadást (replay attack). [202]

- **Jogtalan adatmódosítás (Unauthorized Data Modification):** ebben a támadásban **a cél a rendszer által továbbított vagy a rendszerben tárolt adatok megváltoztatása**, mellyel a rádiórendszer működése vagy biztonsága csökkenthető. A támadás kivitelezhető például az alkalmazott hullámforma paramétereinek megváltoztatásával, vagy a hardver sérülékenységének kihasználásával. [202]

- **Jogtalan adathozzáférés (Unauthorized Access to Data):** az ilyen támadás során **az érzékeny belső információhoz történő hozzáférés a cél, anélkül hogy módosítanák azt**. Ez különböző rosszindulatú kódok, hardver trójai és eszközklonok alkalmazásával történhet, de ide tartozik a hálózat forgalmának figyelése, az oldalcsatorna támadások, vagy pszichológiai befolyásolás (Social Engineering) is. A hálózati forgalom figyelésének és az

oldalcsatorna támadások célja nemcsak az átvitt információ megszerzése, hanem a különböző rendszerparaméterek kielemezése is, amely egy későbbi támadás alapját szolgálhatja. [202]

- **Szolgáltatás megtagadásos vagy más szakirodalmak alapján túlterheléses támadás (Denial of Service):** ebben a támadásban a cél, hogy **az SDR rendszer elérhetetlenné vagy működésképtelenné váljon.** Az ilyen támadások eszközei a puffer túlsordulás, a hardver trójai, vagy az elektronikai zavarás. [202]

**A fenti támadások többségének lényege, hogy a támadás az EHV eszköz üzemszerű működése során az adatátviteli úton keresztül történő behatolással történik meg,** ezért a **védelmi megoldásokban a felhasználó jogosultságának ellenőrzésére, az adatátviteli utak védelmének biztosítására, illetve az üzemközben vett parancsok (pl. üzemelési paraméterek megváltoztatására vonatkozó parancs, másik hullámforma, stb.) hitelességének ellenőrzésére** kell nagy hangsúlyt fektetni.

Ezen támadások többségében is megoldást nyújt a korábban már említett védelmi megoldások alkalmazása, így egy **komplex informatikai biztonsági rendszer** felépítése. Ennek a rendszernek az alapja az **adminisztratív védelem, a fizikai védelem és a technikai/logikai védelem** elemeinek összehangolt működtetése.

Az előző bekezdésben felsorolt három védelem elemei közül az alábbiakban kiemelek néhány fontos és hatékonyságot növelő megoldást:

- A szoftverek esetében a **gyártói hibajavítások, frissítések folyamatos telepítése.**
- **A felhasználó többszintű azonosítása,** amelynek során felhasználásra kerülnek az adott személy egyedi, **biometrikus jellemzői** (pl. írisz, ujjlenyomat, hang, stb.) is.
- **Kiemelten fontos a letöltésre kerülő parancsok (programok) zárt környezetben (Sandbox) történő futtatása** az alábbi feladatok végrehajtása érdekében:
  - **a küldő állomás autentikálása;**
  - az esetlegesen elrejtett **rosszindulatú programok keresése.**

A biztonságos futtatókörnyezettel (Sandbox) kapcsolatban fontos az, hogy **ebben az esetben is adaptív megoldásokat** kell alkalmaznunk, mivel a **kártékony programok képesek lehetnek annak felismerésére, hogy ilyen környezetben futtatják.** Mindenképpen szem előtt kell tartanunk azonban azt is, hogy a biztonságos futtatókörnyezet alkalmazása során a **letöltés befejezése és kapott feladat/parancs valós végrehajtásának megkezdése közötti időt a lehető legkisebbre kell csökkenteni, azaz megfelelő erőforrást kell biztosítanunk a zárt környezetben történő gyors futtatáshoz és ellenőrzéshez.**

### 3.4. A szoftverrádió technológia alkalmazása esetében javasolt szervezeti változások

Mint már korábban említettem, az MH katonai szervezeteinél jelenleg kettő szervezetszerű elektronikai hadviselési alegység van, ezek az EHV század az MH 24. BGFE-nél, illetve az EHV Támogató Központ az MH 59. SZD RB-nél. Az 1. fejezetben ismertettek alapján megállapítható az, hogy az EHV képesség az MH vonatkozásában képességfejlesztést és létszámnövelést igényel.

A Honvédelmi Minisztérium Haderőtervezési Főosztály, Haderőtervezési és Modernizációs Osztálya 2007-ben egy lövészdandár felderítő támogatására megtervezett ISTAR zászlóaljban a HUMINT század, a kettő felderítő század mellett egy elektronikai hadviselés századdal számolt. [92] Korábban már említettem az MH-ban jelenleg kettő lövész és egy különleges rendeltetésű dandár, illetve egy felderítő ezred van, melyek esetében EHV képesség biztosítása indokolt. A légierő vonatkozásában javaslom figyelembe venni az MH 59. SZD RB-t és az MH 86. Szolnok Helikopterbázist.

A korábban tett javaslataim megvalósítása esetén, miszerint **az SDR alapú EHV eszközök alkalmazása megfelelő alapot nyújt a fejlesztések végrehajtásához**, a jelenleg meglévő **EHV képességhez képest jelentős szervezeti változással** kell számolni. A korábban említett katonai szervezeteknél kialakítandó EHV alegységek felépítésének, funkciójának vizsgálata nem része a dolgozatomnak, ebben a fejezetben az **SDR technológia nyújtotta előnyök kihasználásához szükséges szervezeti elemekkel foglalkozom**.

Véleményem szerint **az SDR technológia alapú EHV rendszerekben történő alkalmazásával** az alábbi új feladatrendszerekkel kell számolni:

- **Frekvenciagazdálkodással kapcsolatos feladatok:**

Korábban már említettem, hogy a Magyar Honvédség érdekében a frekvenciagazdálkodással kapcsolatos feladatokat az MH BHD frekvenciagazdálkodási szervezete végzi. **Az elektromágneses spektrum telítettsége miatt a spektrum használatára vonatkozó szabályzók betartása, a szoftverrádió technológia alkalmazásából eredő rugalmasság biztosítása, valamint a saját EHV elemeink hatékony működéséhez szükséges összhaderőnemi korlátozott frekvenciák jegyzékének<sup>170</sup> folyamatos pontosítása rendkívül fontos feladat.** Az aktuális frekvenciaadatokkal történő feladatvégrehajtás alapja a dandár szintű szervezeteknél lévő és a hadműveleti/összhaderőnemi szinten kialakított EHV elem, illetve az MH-ban rendelkezésre

---

<sup>170</sup> Joint Restricted Frequency List, JRFL.

álló egyéb eszközök (radareszközök, különböző felderítő platformok, stb.) által biztosított információ hálózatban történő kezelése, feldolgozása, így növelve a lefedhető távolságot és megszerzett információk több forrásból történő megerősítését.

- **Informatikai/kibervédelmi feladatok:**

A 2.2.8. alfejezetben már említettem, hogy az SDR alapú fejlesztésnek, vagy az SDR alapú eszközök/eszközrendszer beszerzésének nagyon rövid időtartamon belül kell végbe mennie az egységes és kompatibilis rendszer kialakítása érdekében, mind a szárazföldi, mind a légi haderőnem vonatkozásában. A kialakításra kerülő EHV szervezeti elemeket úgy kell megtervezni, hogy a szárazföldi és a légi haderőnem specifikus jellemzőit figyelembe kell venni. **A szoftverrádió technológia felhasználása miatt informatikai képességet javaslok kialakítani az EHV elemekben.**

A frekvenciagazdálkodási és informatikai feladatok EHV elemekhez történő beintegrálásával az elektronikai hadviselési szakfeladatok hatékony végrehajtása magasabb szintre emelhető, mivel figyelembe kell vennünk azt, hogy *„az új módszereknek köszönhetően az információhiány helyett most a „túl sok adat kora” köszöntött be, ami egészen más feldolgozási, értékelési módszerek, eljárások megalkotását követeli meg”*. [161]

A fenti feladatok hatékony végrehajtása érdekében az **összhaderőnemi/hadműveleti szinten**, valamint a létrehozásra kerülő **EHV alegységeknél** az alábbi szervezeti módosításokat javaslom:

- Összhaderőnemi/hadműveleti szinten a frekvenciagazdálkodási, valamint az informatikai feladatok végrehajtása, valamint a többi EHV elem közötti koordináció érdekében Elektronikai Hadviselési Koordinációs Részleg<sup>171</sup> felállítása és állandó jelleggel történő üzemeltetése. Az **informatikai feladatok** ellátására **egy nagyobb létszámú informatikai elem kialakítását javaslom**, melynek feladataira a későbbiekben teszek javaslatot.

- **Harcászati szinten frekvenciagazdálkodási feladatkör és informatikai feladatkör létrehozása az EHV alegységek értékelő-elemző és zavarást irányító központjaiban.** Az informatikai feladatok ellátására harcászati szinten 1-2 fő informatikai szakember biztosítását javaslom.

---

<sup>171</sup> Electronic Warfare Coordination Cell - EWCC

**Az összhaderőnemi/hadműveleti szinten kialakítandó informatikai elem feladataiként az alábbiakat határozom meg:**

- **A szoftvertesztelési feladatok végrehajtása** fejlesztőtől/gyártótól történő szoftverbeszerzés esetén.
- Az MH fejlesztőtől/gyártótól való függetlenségének biztosítása az eszköz/rendszer későbbi fejlesztése során a programozói képességgel.
- **Kibervédelem biztosítása.**
- Az eszközök működési paraméterei változtatásához kapcsolódó programozói feladatok végrehajtása, az adott műveleti terület elektronikai helyzetére történő reagáló képesség biztosítása érdekében.
- Az interferencia elkerülése érdekében a saját elektronikai kisugárzó eszközeinkkel kompatibilis működtetési feltételek kialakításához kapcsolódó programozói feladatok végrehajtása.
- **Az adatbázisok kezelése**, a hadszíntérre jellemző specifikumok alapján a szükséges módosítások végrehajtása az adatbázison.

A harcászati szinten feladatot végrehajtó informatikai állomány az első kettő feladatban csak részlegesen vesz részt, alapvető feladatuk az utolsó négy pontban felsorolt tevékenység végrehajtása.

A fejlesztőtől/gyártótól történő szoftverbeszerzés esetén fellépő szoftvertesztelési feladatokat a 3.2. alfejezetben már elemeztem. Ebben az esetben fontos, hogy a szoftvertesztelést az MH állománya a fejlesztés minél korábbi fázisában megkezdhesse. Lényeges az is, hogy hatékony tesztelés alapja az, hogy a felhasználó EHV állományunk és az informatikai szakállományunk között nagyon szoros, állandó munkakapcsolat legyen. Mindenképpen ki kell emelni, hogy a magyar védelmi ipar által történő saját eszköz/rendszer kifejlesztéséhez szükséges informatikai képesség biztosítása nem ezen elem feladata, arra külön munkacsoport felállítása indokolt. Természetesen ez nem zárja ki azt, hogy szakmai javaslataival segítse a fejlesztést.

Az MH fejlesztőtől/gyártótól való függetlenségének biztosíthatóságának alapja, hogy a rendszer működtetéséhez szükséges program forráskódja rendelkezésre álljon, az az eszköz/rendszer leszállításakor átadásra kerüljön. Azt, hogy a későbbi továbbfejlesztés, módosítás során a rendelkezésre álló/kialakított informatikai elem képessége/mérete



ellegendő-e, azt a továbbfejlesztés, módosítás elvárt/szükséges mértéke fogja meghatározni. Lehetséges az is, hogy külön munkacsoport felállítása válik indokolttá, melynek tevékenységét informatikai elemünk szakmai javaslataival segíti.

**A kibervédelem biztosítása** és a Magyar Honvédség kibervédelme vonatkozásában mindenképpen meg kell említeni a **Honvédelmi Ágazati Elektronikus Információbiztonsági Eseménykezelő Központot (HÁEI-BEK)**, amelynek *„rendeltetése a honvédelmi célú informatikai rendszerek biztonságának támogatása, a rendszerek működése során bekövetkező biztonsági események ágazati szintű kezelése, a sérülékenység vizsgálatok végrehajtása és a fenyegetettségek kezelése.”* [203] A hadműveleti szintű EHV Koordinációs Részlegnek az informatikai tevékenység vonatkozásában a fenti szervezettel együtt kell működnie, az informatikai biztonsági környezetet velük együttműködésben kell kialakítani.

Az informatikai elem kibervédelmi feladatai közé véleményem szerint az alábbi speciális tevékenységek tartozhatnak:

- **Megelőzés**, melynek célja a folyamatos helyzet értékelés végrehajtása, elemzések, jelentések készítése, javaslattevés a feltárt hibák elhárítására.

- **Biztonsági események kezelése, támadások elhárítása.**

A megelőzés tovább bontható az alább felsorolt feladatokra, speciális tevékenységekre. A tesztek, elemzések során a támadás egy-egy támadási metódus önálló, vagy több metódus egyidejű végrehajtásán alapulhat. Az elemzés pontos célját időben, a megfelelő szakemberek bevonásával kell meghatározni a hatékony végrehajtás és az implementálható javaslatok kialakíthatósága érdekében.

- **Etikus hackelés**, melynek célja a rendszer gyengeségeinek, támadható sérülékenységeinek felderítése.

- **Penetrációs teszt** végrehajtása, amely egy tervezett, minden részterület (szoftverek, konfigurálás, felhasználói tevékenység, stb.) ellenőrzésére kiterjedő folyamat. Az ellenőrzés eredménye, illetve a feltárt hiányosságok megszüntetésére tett javaslatok képezik az alapját a további megelőző tevékenységnek.

- **„Hadijáték”** (War game) a katonai művelettervezésből is jól ismert, az informatikai/kibervédelmi feladatok közé beemelt tevékenység, melynek célja egy megtervezett biztonsági eseményre történő reagálás megfigyelése, dokumentálása, majd az állomány tevékenységének utólagos elemzése és javaslatok megtétele. [204]

Az eszközök **működési paramétereinek változtatásához**, illetve az interferencia elkerülése érdekében **a saját elektronikai kisugárzó eszközeinkkel kompatibilis működtetési feltételek kialakításához** kapcsolódó programozói feladatok végrehajtása az összhaderőnemi/hadműveleti és a harcászati szinten egymással koordináltan kell, hogy végrehajtásra kerüljön. Ennek érdekében a legcélravezetőbb megoldás, ha a változtatások a magasabb szinten kerülnek végrehajtásra, majd onnan továbbításra az alárendelt szint felé.

Az **adatbázisok kezelése**, a hadszíntérre jellemző specifikumok alapján a szükséges módosítások **adatbázison történő végrehajtása** nem az adatbázisban tárolt információ módosítását jelenti, mivel az információ módosítása az EHV szakállomány feladata. Az adatbázis módosítása ebben az értelemben az *”adatbázis sémájának módosítását jelenti, esetünkben például újabb adatkategória megjeleníttetését az adatbázisban.* Fontos az, hogy ezen változtatások végrehajtása csak az adatbázisért felelősként kijelölt szervezeti elem (pl. elektronikai hadviselési koordinációs részleg, magasabb szintű elektronikai hadviselési szervezet, stb.) jóváhagyásával történhessen meg.” [171; 109. o.] Ezen feladatok a kialakítandó informatikai elem feladatai között kell, hogy szerepeljenek.

### **Összegzés, részkövetkeztetések**

Értekezésem harmadik fejezetében a szoftverrádió technológián alapuló elektronikai hadviselési eszköz Magyar Honvédségben történő alkalmazhatóságát, az SDR technológián alapuló EHV eszközök rendszerbe szervezésének kérdéseit vizsgáltam, ebbe beleértve az ilyen típusú eszközöket tartalmazó rendszerek elleni támadás lehetőségeit, valamint a védelmi megoldásokat.

Az első alfejezetben a szoftverrádió technológia alapú **EHV eszközzel szemben támasztandó perspektivikus követelmények meghatározását végeztem el**, figyelembe véve egy teljes rendszer kialakításához szükséges valamennyi aspektust, így többek között a hordozóeszközökre, antennarendszerre, adatátviteli megoldásokra, stb..

A második alfejezetben az **elektronikai hadviselési rendszer beszerzésének, hazai fejlesztésének, gyártásának főbb kérdéseit elemeztem**, figyelembe véve a kettő lehetséges beszerzési lehetőség, azaz a saját fejlesztés, illetve az erre a szakterületre specializálódott gyártó már kifejlesztett termékének megvásárlása közötti előnyöket és hátrányokat.

A harmadik alfejezetben **a szoftverrádió alapú elektronikai hadviselési eszköz és rendszer elleni támadások és az ismertetett támadások elleni védelmi megoldásokat vizsgáltam**, kiemelten **az informatikai támadások** tekintetében. Fontosnak tartom

megemlíteni, hogy az informatikai megoldások alkalmazásával egy újabb, rendkívül széleskörűen alkalmazott támadási módszer is megjelenhet az elektronikai hadviselési eszközök ellen. A lehetséges támadási metódusok elemzése megfelelő segítséget nyújthat a védelmi megoldások kidolgozása során. **Kiemelten vizsgáltam a szoftverrádió technológia sajátosságából eredő támadási lehetőségeket, illetve tettem javaslatot ezen támadási lehetőségek kiküszöbölésére.**

A negyedik alfejezetben a szoftverrádió technológián alapuló elektronikai hadviselési eszközök rendszerbe szervezésének szervezeti kérdéseit vizsgáltam, melynek során elemeztem korábbi feladatokat és a különböző szervezeti elemekkel kapcsolatban korábban tett javaslatokat. Az értekezésben megjelenített eredmények, valamint az alfejezetben végrehajtott elemzések alapján javaslatot tettem **az összhaderőnemi/hadműveleti szinten kialakítandó, állandóan működő, az elektronikai hadviselési feladatokat koordináló szervezet felállítására**, illetve a frekvenciagazdálkodási és az informatikai/programozói képesség kialakítására.

A fentiek alapján az alábbi következtetéseket fogalmazom meg:

1. A **szoftverrádió technológia** a Magyar Honvédség elektronikai hadviselési képességének fejlesztésében **fontos és state-of-the-art megoldást jelenthet**, azonban a szükséges eszközök kifejlesztése/kiválasztása, alkalmazásuk bevezetése **rendkívül gondos tervezést igényel**.

2. A szoftverrádió technológia alkalmazása különböző, **korábban nem alkalmazott adatátviteli és adattárolási módszerek bevezetését indokolja, teszi lehetővé**.

3. Magyarországon **rendelkezésre áll egy SDR koncepció alapú elektronikai hadviselési rendszer kifejlesztésére képes védelmi ipari háttér**. Az említett védelmi ipari háttér bevonása érdekében a követelményeket nagyon pontosan meg kell határozni.

4. A **fejlett elektronikai hadviselési képesség** a szembenálló fél elektromágneses spektrumban történő manőverezését nagymértékben képes akadályozni, saját erőink tevékenységét pedig hatékonyan támogatni. Emiatt az elektronikai hadviselési eszközök és rendszerek **a szembenálló felek célpont listáin kiemelt fontossággal szerepelnek**. Emiatt továbbra is **fontos kérdés az EHV eszközök támadhatósága és a lehetséges védelmi megoldások**, melyek között a szoftverrádiós technológia alkalmazása miatt már **az informatikai jellegű támadásokkal is számolnunk kell**.

5. A meglévő katonai szervezetek figyelembevételével javasolt elektronikai hadviselési alegységek kialakítása napjaink hadviselésének megfelelő elektronikai hadviselési

képességet biztosít, amely mind országvédelmi, mind békeműveleti tevékenység esetén hatékony támogathatja a kijelölt műveleti feladatok végrehajtását. A korábbi időszakban is alkalmazott értékelő-elemző és zavarást irányító központban **az SDR koncepció előnyeinek felhasználása érdekében informatikai/programozói képesség kialakítása indokolt.**

## Összegzett következtetések

Napjaink konfliktusainak elemzése során számos esetben olvashatunk az elektronikai hadviselés alkalmazásáról, mind a szárazföldi erők, mind a légierő által végrehajtott tevékenység során. **Az elektronikai hadviselés szerepe** a technikai eszközök fejlődése, az elektromágneses spektrum alkalmazásán alapuló eszközök számának növekedése miatt **továbbra is megkérdőjelezhetetlen**. Sok esetben szerepeltetik, mint hatásnövelő, hatásfokozó eszköz vagy képesség, melynek fejlesztésére a különböző nemzetek jelentős erőforrásokat fordítanak és az elért eredményeket, az újonnan kifejlesztett technikai eszközöket alkalmazzák is a folyamatban lévő konfliktusokban. **Fontos azt is kihangsúlyozni, hogy az elektronikai hadviselési eszközök** birtoklása nemcsak a nagy nemzetek számára elérhető lehetőség, hanem az erőforrások megfelelő felhasználásával a kisebb országok hadseregei számára is **biztosítható és biztosítandó képesség**.

Az is lényeges, hogy **az elektronikai hadviselési képesség is skálázható**. Sok esetben csak kimondottan **önvédelmi célú képességről** beszélhetünk, ilyen a rádió-távírányítású improvizált robbanóeszközök elleni kis hatótávolságú zavaróeszközök birtoklása és alkalmazása. Ez jóval kisebb anyagi erőforrást igényel, míg például a **kimondottan támadó célú elektronikai zavaróképesség** – beleértve a több eszközből álló komplex rendszert – kiépítése/beszerzése már jóval nagyobb anyagi és humán erőforrást igényel. Ennél is **nagyobb költség** lehet – beleértve a hordozó repülőeszköz beszerzésének és üzemeltetésének költségét is – **a szembenálló fél légvédelmének elnyomására képes zavarókonténerek üzemeltetése**, de ebben az esetben azt is figyelembe kell venni, hogy véleményem szerint ez a képesség már csak a nagyobb – megfelelő méretű légierővel és erőforrással rendelkező – államok részére érhető el. A Magyar Honvédség részére véleményem szerint a fent említett három példa közötti szintnek megfelelő elektronikai hadviselési képesség fenntartása indokolt.

Mindenképpen fontos azt is megjegyezni, hogy az elektronikai hadviselési képesség birtoklása nemcsak a hadseregek privilégiuma, annak részelemeit – így például az elektronikai zavarást – a különböző polgári és rendvédelmi szervezetek is alkalmazzák. Ilyen szervezetek lehetnek például a büntetés-végrehajtási szervezetek, vagy a különböző konfliktusok helyszínein dolgozó őrzés-védelmi, logisztikai vagy segélyfeladatokat végző cégek, ügynökségek. A feladatok hatékony végrehajtását nagyban segítheti az egyazon

feladatban résztvevő különböző szervezetek közötti tapasztalatok, információk megosztása. Ez alatt azt értem, hogy **egy adott műveleti területen dolgozó, különböző vezetési/irányítási rendszerbe tartozó szervezetek különböző információkkal rendelkezhetnek**, melyek nem biztos, hogy eljutnak a másik végrehajtó szervezethez. **A végrehajtók közötti tapasztalat/információ megosztás ezt a hibát küszöböli ki.**

Az értekezés első fejezetében áttekintettem az elektronikai hadviselés alkalmazását befolyásoló változásokat, ebbe beleértve mind a biztonságpolitikai helyzet változásának, mind a technikai fejlődés hatásait. **Megállapítottam, hogy a biztonságpolitikai változások, a különböző politikai, gazdasági és katonai szervezetek tevékenysége, a napjainkban, Európában elkövetett terrortámadások Magyarország biztonsági helyzetére – és így a Magyar Honvédség feladataira is – kihatással vannak.** A Magyar Honvédség feladatait a különböző műveleti helyszíneken különböző képességekkel – köztük az elektronikai hadviseléssel lehet – biztosítani, támogatni. A hatékony elektronikai hadviselési támogatás alapvető feltétele a kor színvonalának megfelelő technikai színvonalú eszközpark. Megvizsgáltam a Magyar Honvédség elektronikai hadviselési és rádiófelderítő képességének változását, a vizsgált időszakban javasolt/végrehajtott fejlesztések eredményeit. **Alátámasztottam, hogy a jövőben is fontos szerep hárul az elektronikai hadviselésre a különböző konfliktusokban és a különböző hadviselési módokban (szimmetrikus, aszimmetrikus, hibrid), illetve a vizsgált nemzetek jelentős forrást fordítanak erre a területre.** Vizsgáltam a korábbi, hazai, az elektronikai eszközök gyártására képes iparágak leépülését, illetve a Honvédelmi Minisztérium által kezdeményezett hadiipari fejlesztési kezdeményezéseket.

A második fejezetben a szoftverrádió technológia elterjedését és a különböző elektronikai rendszerekben történő alkalmazását vizsgáltam. **Megállapítottam, hogy az SDR technológia mind az elektronikai hadviselési rendszerekben, mind az elektronikai hadviselés alkalmazásával befolyásolható rendszerekben felhasználásra került.** Lényeges, hogy számos fejlesztés, kutatás van folyamatban a további előnyök kihasználása érdekében. Kiemelt figyelmet fordítottam a magyar INTERJAM projekt eredményeinek vizsgálatára. Vizsgáltam a Magyar Honvédségben jelenleg meglévő és a szoftverrádió technológia alkalmazásával elérhető elektronikai hadviselési képességek közötti különbséget. **Javaslatot tettem a szoftverrádió technológia alapú elektronikai hadviselési eszközök beszerzésére.**

A harmadik fejezetben vizsgáltam a szoftverrádió technológián alapuló elektronikai hadviselési eszközzel és rendszerrel szemben támasztandó perspektivikus követelményeket, a beszerzésével/fejlesztésével kapcsolatban figyelembe veendő szempontokat, illetve az SDR alapú elektronikai hadviselési rendszer felderíthetőségét és az azok ellen történő védelem lehetőségeit. **Megállapítottam, hogy a szoftverrádió technológián alapuló elektronikai hadviselési eszközök esetében szükséges a védelmi megoldások kiterjesztése az informatikai védelmi megoldásokra is, illetve azt, hogy a fenti megoldások szervezeti változásokat is generálnak mind harcászati, mind hadműveleti/összhaderőnemi szinten.** Ennek érdekében javaslatot tettem a szükséges elektronikai hadviselési/informatikai állomány biztosítására, illetve szervezeti elem felállítására, valamint ezen elemek feladataira.

## **Új tudományos eredmények**

**1. Elemezve a Magyar Honvédség elektronikai hadviselésének fejlesztésére tett korábbi javaslatokat, valamint a szoftverrádió technológia alkalmazásában rejlő előnyöket, javaslatot tettem a Magyar Honvédség elektronikai hadviselési képességének szoftverrádió technológián alapuló fejlesztésére.**

**2. Meghatároztam a szoftverrádió technológia alapú elektronikai hadviselési eszközökkel/rendszerrel szemben támasztandó követelményeket a Magyar Honvédség elektronikai hadviselési képessége vonatkozásában.**

**3. A szoftverrádió technológián alapuló elektronikai hadviselési eszköz/rendszer elleni támadási módszerek elemzésével javaslatot tettem a védelem megtervezése során figyelembe veendő szempontokra, kiemelten az informatikai terület vonatkozásában.**

**4. A hadműveleti/összhaderőnemi szintű, illetve a harcászati szintű értékelő-elemző és zavarást irányító központokban frekvenciagazdálkodási feladatkör, valamint informatikai/programozói képesség kialakítására tettem javaslatot az SDR koncepció által nyújtott előnyök kihasználása, az SDR alapú EHV eszközök működési paramétereinek – az adott műveleti környezethez – illeszkedő gyors változtathatósága, valamint az informatikai jellegű támadások megelőzése és elhárítása érdekében.**

**5. Hadműveleti/összhaderőnemi szinten Elektronikai Hadviselési Koordinációs Részleg felállítására és állandó jelleggel történő üzemeltetésére tettem javaslatot a Magyar Honvédség szoftverrádió technológia alapú elektronikai hadviselési képességének kihasználása érdekében.**



## Ajánlások

1. Értekezésemet, kutatási eredményeimet javaslom felhasználni a Magyar Honvédség elektronikai hadviselési képességének fejlesztése tervezésekor.
2. Az értekezést javaslom felhasználni a Magyar Honvédség harcászati, hadműveleti és stratégiai szintjén szolgálatot teljesítő tiszti és főtiszti állomány oktatása, ismeretszint fenntartása során, mivel az ismeretek fejlesztése a szakmai tevékenység színvonalának minél magasabb szinten történő tartása miatt az egyik legfontosabb feladat.
3. Javaslom felhasználni a katonai oktatásban, ebbe beleértve az MH Altiszti Akadémia és a Nemzeti Közsolgálati Egyetem Rádióelektronikai felderítő és elektronikai hadviselés specializációjú képzéseit, az Egyetem esetében mind alap, mind mesterképzésen.
4. Javaslom alkalmazni forrásirodalomként vagy a kapcsolódó tantárgyak ajánlott irodalmaként, mivel az elektronikai hadviselés vonatkozásában – mint témája és fontossága miatt érzékeny szakterület esetében – kevés kutatható szakanyag áll rendelkezésre.
5. Javaslom az egyes fejezetek következtetéseit további tudományos vizsgálatok, kutatások alapjaként felhasználni, akár elektronikai hadviselési, akár rádióelektronikai felderítő vagy más szakterületek vonatkozásában.

## Témakörből készült publikációim

Szerkesztett könyvben fejezet:

1. Horváth József: Drón, Drón, Drón ... Repüléstudományi Szemelvények 2017. 9-30. oldal  
ISBN 978-615-5764-80-6 <http://www.repulestudomany.hu/kiadvanyok/RepSzem-2017.pdf>

Lektorált folyóiratban megjelent cikkek:

1. Horváth József: A repülés elektronikai zavarásának valós esetei. Repüléstudományi közlemények, XXX. Évfolyam, 2018. 2. szám, 7-24. oldal, ISSN 1789-770X URL: [http://www.repulestudomany.hu/index\\_rtk.html](http://www.repulestudomany.hu/index_rtk.html)
2. József Horváth: Software Defined Radio concept in wireless solutions. Hadmérnök, XIII. Évfolyam 1. szám – 2018. március, 261-269. oldal, ISSN 1788-1919 URL: [http://www.hadmernok.hu/181\\_20\\_horvath.pdf](http://www.hadmernok.hu/181_20_horvath.pdf)
3. Az A2/AD környezet és az elektronikai hadviselés. Sereg Szemle. XV. évfolyam, 2. szám, 2017. április - június, pp.: 188-198., HU ISSN: 2060-3924 URL: [http://www.honvedelem.hu/container/files/attachments/66630/2017\\_2-seregszemle-internetre.pdf](http://www.honvedelem.hu/container/files/attachments/66630/2017_2-seregszemle-internetre.pdf)
4. Horváth József alezredes: Elektronikai hadviselés a felhőben. Sereg Szemle. XV. évfolyam, 1. szám, 2017. január–március., pp.: 124-131., HU ISSN: 2060-3924 URL: [http://www.honvedelem.hu/container/files/attachments/65846/2017\\_1-seregszemle-internet.pdf](http://www.honvedelem.hu/container/files/attachments/65846/2017_1-seregszemle-internet.pdf)
5. Lt. Col. József Horváth: „The Battle of Wizards”: The Future of Electronic Warfare. Defence Review, Special Issue 2016/I., Volume 144., pp.: 173-179., ISSN 2060-1506 URL: <http://www.honvedelem.hu/cikk/58745>
6. Horváth József alezredes: A szoftverrádió alapú elektronikai hadviselési eszközök elleni támadás formái és a védekezés lehetőségei. Sereg Szemle, XIV. évfolyam 1. szám, 2016. január-február, 76-85. oldal, ISSN 2060-3924 URL: [http://www.honvedelem.hu/container/files/attachments/57646/2016\\_1\\_seregszemle\\_internet.pdf](http://www.honvedelem.hu/container/files/attachments/57646/2016_1_seregszemle_internet.pdf)
7. Horváth József alezredes: Elektronikai hadviselés korunk konfliktusaiban. Honvédségi Szemle, 144. évfolyam, 2016/I. szám, 18-26. oldal, ISSN 2060-1506 URL: [http://www.honvedelem.hu/container/files/attachments/55138/hsz\\_2016-1..pdf](http://www.honvedelem.hu/container/files/attachments/55138/hsz_2016-1..pdf)

8. Horváth József alezredes: A szoftverrádió technológián alapuló elektronikai hadviselési eszköz hatékony működéséhez szükséges adatok biztosításának vizsgálata. Sereg Szemle, XIII. évfolyam 2-3. szám, 2015. április-szeptember, 103-114. oldal, ISSN 2060-3924 URL:  
[http://www.honvedelem.hu/container/files/attachments/54566/seregszemle\\_2015\\_2-3szam.pdf](http://www.honvedelem.hu/container/files/attachments/54566/seregszemle_2015_2-3szam.pdf)
9. Horváth József: Software Defined Radio concept in different systems. Hadmérnök, X. Évfolyam 3. szám, 2015. szeptember, 193-202. oldal, ISSN 1788-1919 URL:  
[http://www.hadmernok.hu/153\\_15\\_horvathj.php](http://www.hadmernok.hu/153_15_horvathj.php)
10. Horváth József alezredes: Térinformatika alkalmazása az elektronikai hadviselésben. Sereg Szemle, XIII. évfolyam 1. szám, 2015. január–március, 78-86. oldal, ISSN 2060-3924 URL:  
[http://www.honvedelem.hu/container/files/attachments/51470/seregszemle\\_2015\\_1.pdf](http://www.honvedelem.hu/container/files/attachments/51470/seregszemle_2015_1.pdf)
11. Horváth József: Az elektronikai zavarás napjainkban. Hadmérnök, X. Évfolyam 1. szám, 2015. március, 183-192. oldal, ISSN 1788-1919 URL:  
[http://www.hadmernok.hu/151\\_18\\_horvathj.pdf](http://www.hadmernok.hu/151_18_horvathj.pdf)
12. Horváth József őrnagy: Az elektronikai hadviselés szervezése a Magyar Honvédségben. Sereg Szemle, XII. évfolyam 3. szám, 2014. július-szeptember, 59-70. oldal, ISSN 2060-3924 URL:  
[http://www.honvedelem.hu/container/files/attachments/48923/2014\\_3sz\\_seregszemle.pdf](http://www.honvedelem.hu/container/files/attachments/48923/2014_3sz_seregszemle.pdf)
13. Horváth József: Elektronikai hadviselés a Magyar Honvédségben. Hadmérnök, IX. Évfolyam 1. szám, 2014. március, 175-186. oldal, ISSN 1788-1919 URL:  
[http://www.hadmernok.hu/141\\_17\\_horvathj.pdf](http://www.hadmernok.hu/141_17_horvathj.pdf)
14. Horváth József: SIGINT repülőgépek. Repüléstudományi közlemények, XXVI. Évfolyam, 2014. 2. szám, 388-399. oldal, ISSN 1789-770X URL:  
[http://www.repulestudomany.hu/kulonszamok/2014\\_cikkek/2014-2-31-0113\\_Horvath\\_Jozsef.pdf](http://www.repulestudomany.hu/kulonszamok/2014_cikkek/2014-2-31-0113_Horvath_Jozsef.pdf)
15. Horváth József mk. őrnagy: Katonai megtévesztés. Sereg Szemle, XII. évfolyam 1. szám, 2014. január – március, 163-174. oldal, ISSN 2060-3924 URL:  
<http://www.honvedelem.hu/container/files/attachments/46172/seregsz2014-1-jav.pdf>
16. Horváth József: A repülésirányítás elektronikai zavarása. Repüléstudományi közlemények, XXV. Évfolyam 2013. 2. szám, 278-288. oldal, ISSN 1789-770X URL:  
[http://www.repulestudomany.hu/kulonszamok/2013\\_cikkek/2013-2-20-Horvath\\_Jozsef.pdf](http://www.repulestudomany.hu/kulonszamok/2013_cikkek/2013-2-20-Horvath_Jozsef.pdf)

17. József Horváth: JAS 39 Gripen in air operations. Repüléstudományi közlemények, XXV. Évfolyam 2013. 2. szám, 394-404. oldal, ISSN 1789-770X URL: [http://www.repulestudomany.hu/kulonszamok/2013\\_cikkek/2013-2-30-Jozsef\\_Horvath.pdf](http://www.repulestudomany.hu/kulonszamok/2013_cikkek/2013-2-30-Jozsef_Horvath.pdf)

## **Köszönetnyilvánítás**

Tanulmányaimat és kutatásaimat a PhD doktori fokozat megszerzése érdekében a Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskolában, a Védelmi elektronika, informatika és kommunikáció kutatási területen folytattam 2013 – 2018 között.

Mindenekelőtt köszönettel tartozom témavezetőmnek, Prof. Dr. Ványa László okl. mk. ezredes úrnak, aki számtalan hasznos tanáccsal indított el pályámon a képzés elején.

Köszönöm az opponenseknek, Prof. Dr. Makkay Imre ny. mk. ezredes és Dr. habil Wühl Tibor uraknak, és mindazoknak, akik felhívták figyelmemet a hibáimra, mellyel sokat segítettek a doktori értekezésem javításában.

Köszönöm családomnak is, akik ezen időszak alatt és mindenkor mellettem álltak, támogatásukról mindvégig biztosítottak.

## Hivatkozott irodalom

- [1.] Greg Goebel: The Wizard War: WW2 & The Origins Of Radar. URL: <http://vc.airvectors.net/ttwiz.html> Letöltve: 2017.09.20.
- [2.] Porkoláb Imre alezredes: A különleges műveleti erők szerepe az aszimmetrikus kihívásokból adódó katonai feladatok tükrében, különös tekintettel a nemzetközi terrorizmus elleni küzdelemre. PhD értekezés. ZMNE. 2009. URL: [http://archiv.uni-nke.hu/downloads/konyvtar/digitgy/phd/2009/porkolab\\_imre.pdf](http://archiv.uni-nke.hu/downloads/konyvtar/digitgy/phd/2009/porkolab_imre.pdf) Letöltve: 2017.06.20
- [3.] Magyar Távirati Iroda: Csak két európai NATO-tagország teljesíti a 2 százalékos védelmi költségvetési célt. URL: [http://www.honvedelem.hu/cikk/61895\\_csak\\_ket\\_europai\\_nato-tagorszag\\_teljesiti\\_a\\_2\\_szazalekos\\_vedelmi\\_koltsegvetsesi\\_celt](http://www.honvedelem.hu/cikk/61895_csak_ket_europai_nato-tagorszag_teljesiti_a_2_szazalekos_vedelmi_koltsegvetsesi_celt) Letöltve: 2017.09.27.
- [4.] Magyar Távirati Iroda: Csak öt NATO-tag teljesíti, amit vállalt. URL: <https://vs.hu/kozelet/osszes/csak-ot-nato-tag-teljesiti-amit-vallalt-0704> Letöltve: 2017.09.27.
- [5.] Magyar Távirati Iroda: Magyarország tartja vállalását a NATO felé. URL: <http://www.origo.hu/itthon/20170216-magyarorszag-vilagos-tervvel-rendelkezik-a-vedelmi-koltsegvetes-teljesitesere-vonatkozuan.html> Letöltve: 2017. 09.27.
- [6.] Wilhelm Theuretsbacher: NATO-Übung: Flugsicherung in halb Europa lahmgelegt. URL: <https://kurier.at/chronik/oesterreich/nato-uebung-flugsicherung-in-halb-europa-lahmgelegt/69.226.057> Pápai Csaba: HM: nem mi bénítottuk meg az európai légi forgalmat. URL: <https://vs.hu/kozelet/osszes/hm-nem-mi-benitottuk-meg-az-europai-legi-forgalmat-0608> Letöltve: 2017.09.27.
- [7.] Horváth József: A repülésirányítás elektronikai zavarása. Repüléstudományi közlemények, XXV. Évfolyam 2013. 2. szám, 278-288. oldal, ISSN 1789-770X Online: [http://www.repulestudomany.hu/kulonszamok/2013\\_cikkek/2013-2-20-Horvath\\_Jozsef.pdf](http://www.repulestudomany.hu/kulonszamok/2013_cikkek/2013-2-20-Horvath_Jozsef.pdf) Letöltve: 2018.07.27.
- [8.] Index.hu: Magyarországi NATO-gyakorlat miatt állt az osztrák légiirányítás. URL: [http://index.hu/kulfold/2014/06/08/magyarorszagi\\_nato-gyakorlat\\_miatt\\_allt\\_az\\_osztrak\\_legiiranyitas/](http://index.hu/kulfold/2014/06/08/magyarorszagi_nato-gyakorlat_miatt_allt_az_osztrak_legiiranyitas/) Letöltve: 2017.09.15.
- [9.] Air Traffic Management, Issue I 2015., 6 o. URL: <http://www.airtrafficmanagement.net/> Letöltve: 2015.11.15.
- [10.] Lt. Col. József Horváth: „The Battle of Wizards”: The Future of Electronic Warfare. Defence Review, Special Issue 2016/I., Volume 144., pp.: 173-179., ISSN 2060-1506 Online: <http://www.honvedelem.hu/cikk/58745> Letöltve: 2018.07.27.
- [11.] Az Észak-atlanti Szerződés, Washington DC, 1949. április 4. URL: [https://www.nato.int/cps/en/natohq/official\\_texts\\_17120.htm?selectedLocale=hu](https://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=hu) Letöltve: 2018. 01.04.
- [12.] Magyar Honvédség Összhaderőnemi Műveleti Doktrína (MH ÖMD, Ált/38) (2013) 1. kiadás, p. 1-8.

- [13.] Magyar Távirati Iroda: Új biztonsági és katonai stratégia készül. URL: <http://www.kormany.hu/hu/honvedelmi-miniszterium/hirek/uj-biztonsagi-es-katonai-strategia-keszul> Letöltve ideje: 2017.07.17.
- [14.] Magyarország Alaptörvénye. URL: [https://net.jogtar.hu/jr/gen/hjegy\\_doc.cgi?docid=A1100425.ATV](https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1100425.ATV) Letöltve: 2017.04.03.
- [15.] A Kormány 1035/2012. (II. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról. URL: [http://2010-2014.kormany.hu/download/f/49/70000/1035\\_2012\\_korm\\_határozat.pdf](http://2010-2014.kormany.hu/download/f/49/70000/1035_2012_korm_határozat.pdf) Letöltve ideje: 2017.05.03.
- [16.] Magyarország Nemzeti Katonai Stratégiája, 1656/2012. (XII. 20.) Korm. határozat URL: [http://www.kormany.hu/download/a/40/00000/nemzeti\\_katonai\\_strategia.pdf](http://www.kormany.hu/download/a/40/00000/nemzeti_katonai_strategia.pdf) Letöltve ideje: 2017.05.03.
- [17.] Kelemen Roland: A kibertámadás minősülhet-e fegyveres támadásnak? URL: <https://jogaszvilag.hu/rovatok/szakma/a-kibertamadas-minosulhet-e-fegyveres-tamadasnak> Letöltve: 2017.07.18.
- [18.] A Honvéd Vezérkar főnökének 5/2015. (HK 2.) HVKF intézkedése a V4 EU Harccsoportban részt vevő Magyar Honvédség V4 EU Harccsoport ideiglenes katonai szervezet megalakításával és felkészítésével kapcsolatos katonai szakmai feladatok előkészítéséről és végrehajtásáról. URL: <http://www.kozlonyok.hu/kozlonyok/Kozlonyok/13/PDF/2015/2.pdf> Letöltve: 2017. 05.01.
- [19.] Sudár István: Az ukrán válság összefoglalása. URL: [http://azatlasz.hu/2014/07/az\\_ukran\\_valsak\\_osszefoglalasa](http://azatlasz.hu/2014/07/az_ukran_valsak_osszefoglalasa) Letöltve: 2018. 01. 05.
- [20.] Kis-Benedek József: Az Iszlám Kalifátus és a globális dzsihád új tendenciái, Hadtudomány 2014/3–4., 22-33. o. URL: [http://real.mtak.hu/19065/1/2014\\_3\\_4\\_2.pdf](http://real.mtak.hu/19065/1/2014_3_4_2.pdf) Letöltve: 2017.02.02.
- [21.] Magyar Távirati Iroda: Világszerte több a fegyveres konfliktus és a válság. URL: <http://nepszava.hu/cikk/1011937-vilagszerte-tobb-a-fegyveres-konfliktus-es-a-valsag> Letöltve: 2017.05.21.
- [22.] Kiss Álmos Péter: Generációk a hadviselésben – a negyedik generáció. Hadtudományi szemle. 2009/2. 10 - 18. o. URL: [http://archiv.uni-nke.hu/downloads/kutatas/folyoiratok/hadtudomanyi\\_szemle/szamok/2009/2009\\_2/2009\\_2\\_hm\\_kiss\\_almos\\_10\\_18.pdf](http://archiv.uni-nke.hu/downloads/kutatas/folyoiratok/hadtudomanyi_szemle/szamok/2009/2009_2/2009_2_hm_kiss_almos_10_18.pdf) Letöltve: 2017.02.02.
- [23.] Porkoláb Imre: Hibrid hadviselés: új hadviselési forma, vagy régi ismerős? Hadtudomány. 2015/3–4. 37. o. URL: [http://mhht.eu/hadtudomany/2015/3\\_4/2015\\_3\\_4\\_5.pdf](http://mhht.eu/hadtudomany/2015/3_4/2015_3_4_5.pdf) Letöltve: 2017.02.02.
- [24.] Ványa László mk. alezredes: Az elektronikai hadviselés eszközeinek, rendszereinek és vezetésének korszerűsítése az új kihívások tükrében, különös tekintettel az elektronikai ellentevékenységre. Doktori (PhD) értekezés. Zrínyi Miklós Nemzetvédelmi Egyetem. Budapest. 2001. URL: [http://archiv.uni-nke.hu/downloads/konyvtar/digitgy/phd/2003/vanya\\_laszlo.pdf](http://archiv.uni-nke.hu/downloads/konyvtar/digitgy/phd/2003/vanya_laszlo.pdf) Letöltve: 2017.05.15.

- [25.] David L. Adamy: EW against a new generation of threats. Egyesült Királyság. Artech House kiadó. 2015. 1-2. old. ISBN 13: 978-1-60807-869-1
- [26.] Haig Zsolt: A gépesített hadosztály elektronikai harca. Akadémiai közlemények 211. sz. 1996. ISSN 1218-5507. 63. o.
- [27.] Pál Péter: A légierő csapásmérő képessége az 1991-es Öböl-háborúban. Repüléstudományi közlemények, 2006. 2. szám. URL: [http://www.repulestudomany.hu/kulonszamok/2006\\_cikkek/pal\\_peter.pdf](http://www.repulestudomany.hu/kulonszamok/2006_cikkek/pal_peter.pdf) Letöltve: 2017.01.21.
- [28.] Horváth József: SIGINT repülőgépek. Repüléstudományi közlemények, XXVI. évfolyam, 2014. 2. szám, 392. o. HU ISSN 1789-770X URL: [http://www.repulestudomany.hu/kulonszamok/2014\\_cikkek/2014-2-31-0113\\_Horvath\\_Jozsef.pdf](http://www.repulestudomany.hu/kulonszamok/2014_cikkek/2014-2-31-0113_Horvath_Jozsef.pdf) Letöltve: 2017.01.21.
- [29.] Wentz, Larry, Lessons From Bosnia: The IFOR Experience, IV. Intelligence Operations. URL: <http://www.fas.org/irp/ops/smo/docs/ifor/bosch04.htm> Letöltve: 2014.02.01.
- [30.] Horváth József őrnagy: Az elektronikai hadviselés szervezése a Magyar Honvédségben. Seregszemle, XII. évfolyam 3. szám - 2014. július-szeptember, 68. o. ISSN 1788-1919 URL: [http://www.honvedelem.hu/container/files/attachments/48923/2014\\_3sz\\_seregszemle.pdf](http://www.honvedelem.hu/container/files/attachments/48923/2014_3sz_seregszemle.pdf) Letöltve: 2017.05.20.
- [31.] Horváth József: Elektronikai hadviselés a Magyar Honvédségben. Hadmérnök, IX. Évfolyam 1. szám - 2014. március; 179. o. ISSN 1788-1919 URL: [http://www.hadmernok.hu/141\\_17\\_horvathj.pdf](http://www.hadmernok.hu/141_17_horvathj.pdf) Letöltve: 2017.05.20.
- [32.] Brad Lendon: North Korea jamming South's air traffic navigation. URL: <http://news.blogs.cnn.com/2012/05/03/reports-north-korea-jamming-souths-air-traffic-navigation/> Letöltve: 2017.05.21.
- [33.] David Cenciotti: U.S. F-22 EW-enabled sensor-rich stealth aircraft have escorted Jordanian F-16s during air strikes on ISIS. URL: <http://theaviationist.com/2015/02/10/f-22-escorted-rjaf-jets/> Letöltve: 2017.05.21.
- [34.] AFP Hírugynökség: U.S. says strikes hit ISIS garrison, 'electronic warfare', URL: <http://english.alarabiya.net/en/News/middle-east/2014/12/01/U-S-says-strikes-hit-ISIS-garrison-electronic-warfare-.html> Letöltve: 2017.05.21.
- [35.] David Stupples: How Syria is becoming a test zone for electronic warfare. URL: <http://edition.cnn.com/2015/10/09/opinions/syria-electronic-warfare-russia-nato/> Letöltve: 2017.05.21.
- [36.] Eli Lake: Ukraine Asked U.S. for Tech to Counter Russia's Jet-Killers, URL: <http://www.thedailybeast.com/articles/2014/07/23/exclusive-ukraine-asked-u-s-for-tech-to-counter-russia-s-jet-killers.html#> Letöltve: 2017.05.18.
- [37.] Andy Eckardt: Army Commander Ben Hodges, Ukraine Crisis Needs More Than Weapons, 05.02.2015. URL: <http://www.nbcnews.com/storyline/ukraine-crisis/army-commander-ben-hodges-ukraine-crisis-needs-more-weapons-n300856> Letöltve: 2017.05.21.
- [38.] Russian electronic warfare station discovered in Donbas, says Tymchuk URL: <https://www.unian.info/society/1029285-russian-electronic-warfare-station-discovered-in-donbas-says-tymchuk.html> Letöltve: 2017.05.18.



- [39.] Rumi Zoltán ezredes: A területekhez való hozzáférés, illetve a hozzáférést gátló műveletek. Honvédségi Szemle 2017/3, 143. évfolyam, ISSN 2060-1506 2015/6. 30-31. o. URL: [http://www.honvedelem.hu/container/files/attachments/54257/hsz\\_6.pdf](http://www.honvedelem.hu/container/files/attachments/54257/hsz_6.pdf) Letöltve: 2017. 06.20.
- [40.] Lieutenant Colonel Andreas Schmidt (DEU AF, JAPCC): Countering Anti-Access/Area Denial. URL: <https://www.japcc.org/countering-anti-access-area-denial-future-capability-requirements-nato/> Letöltve: 2017.06.30.
- [41.] Dave Majumdar: Can America Crush Russia's A2/AD 'Bubbles'? URL: <http://nationalinterest.org/blog/the-buzz/can-america-crush-russias-a2-ad-bubbles-16791> Letöltve: 2016.06.29.
- [42.] Tomasz Smura: Russian Anti-Access Area Denial (A2AD) capabilities - implications for NATO, Pulaski Policy Papers, ISSN 2080-8852 Warsaw, URL: [https://pulaski.pl/wp-content/uploads/2015/02/Pulaski\\_Policy\\_Paper\\_No\\_29\\_16\\_EN.pdf](https://pulaski.pl/wp-content/uploads/2015/02/Pulaski_Policy_Paper_No_29_16_EN.pdf) Letöltve: 2016.11.27.
- [43.] Jonathan Wade: Russia's A2/AD in Crimea. <http://thesentinel.ca/russias-a2ad-crimea/> Letöltve: 2017.06.18.
- [44.] Csányi Benedek: Oroszország és a változó Arktisz. Kül-Világ, VII. évfolyam, 2010/2–3. 81-97. o. ISSN 1785-5284 URL: <http://www.kulvilag.hu/2010/0203/csanyi.pdf> Letöltve: 2017.05.18.
- [45.] Eszterhai Viktor: Új világrend küszöbén: A hatalmi erőegyensúly átalakulása Délkelet-Ázsiában, játékelméleti megközelítésben. <http://www.geopolitika.hu/hu/2017/03/08/uj-vilagrend-kuszoben-a-hatalmi-eroegyensuly-atalakulasa-delkelet-azsiaban-jatekelmeleti-megkozelitesben/> Letöltve: 2017. 06. 24.
- [46.] Szerző nélkül: Aranyárban tankolhatunk, ha lezárják a Hormuzi-szorost. <http://vilag.transindex.ro/?cikk=16383> Letöltve: 2017. 06. 24.
- [47.] Horváth József: Az A2/AD környezet és az elektronikai hadviselés. Sereg Szemle. XV. évfolyam, 2. szám, 2017. április - június, 188-198. o. HU ISSN: 2060-3924 URL: [http://www.honvedelem.hu/container/files/attachments/66630/2017\\_2-seregszemle-inernetre.pdf](http://www.honvedelem.hu/container/files/attachments/66630/2017_2-seregszemle-inernetre.pdf) Letöltve: 2018.01.05.
- [48.] Pozderka Zoltán: Az információs műveletek helye és szerepe a művelettervezésben. Hadtudomány 2016/Különszám. 131-141. old. ISSN 1588-0605 [http://mhtt.eu/hadtudomany/2016/2016kulonszam/ht2016\\_kulonszam\\_133-143.pdf](http://mhtt.eu/hadtudomany/2016/2016kulonszam/ht2016_kulonszam_133-143.pdf)
- [49.] Bárány Zoltán ezredes: A hadműveleti szinten végrehajtott művelettervezés folyamata Honvédségi Szemle 142. évfolyam 2. szám 2014. március, pp: 52-67 ISSN 2060-1506
- [50.] AAP-6, NATO glossary of terms and definitions.
- [51.] Magyar Honvédség Összhaderőnemi Elektronikai Hadviselés Doktrína, 2. kiadás, 2015. 2-2
- [52.] Dr. Haig Zsolt alezredes – Dr. Várhegyi István nyá. ezredes: A vezetési hadviselés alapjai. Budapest: 2000., ZMNE, Egyetemi jegyzet. 104. o.

- [53.] Frunze Katonai Akadémia Szerzői Kollektívája: A rádióelektronikai harc az összefegyvernemi harcban és a hadsereg műveleteiben. 1972. Honvédelmi Minisztérium, Szovjetunió. Fordította: Dr. Bokor Imre mk. alez., - Németh Pál alez. 3. o.
- [54.] Harry Foster: The Joint Stealth Task Force, JFQ 72, 1st Quarter 2014 URL: [http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-72/jfq-72\\_47-53\\_Foster.pdf?ver=2014-03-13-152410-190](http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-72/jfq-72_47-53_Foster.pdf?ver=2014-03-13-152410-190) Letöltve: 2017.01.21.
- [55.] Haig Zsolt – Kovács László – Ványa László – Vass Sándor: Elektronikai hadviselés. Budapest, 2014., ISBN 978-615-5305-87-0
- [56.] HQ Supreme Allied Commander Transformation, Defence Planning Policy and Analysis Branch: Technology Trends Survey, Version 3, 2015.02., a szerző fordítása.
- [57.] Michael R. Frater-Michael Ryan: Eelectronic warfare for the Digitized Battlefield. Artech house, Boston, 2001. Preface. ISBN 1-58053-271-3
- [58.] Haig Zsolt őrnagy: A gépesített hadosztály elektronikai harcának megtervezése, megszervezése és vezetése, különös tekintettel az elektronikai helyzetértékelés korszerű módszereire, Doktori (PhD) értekezés, Zrínyi Miklós Katonai Akadémia. Budapest, 1996. 6-7. oldal
- [59.] The Alliance's Strategic Concept, 55. bekezdés URL: [http://www.nato.int/cps/en/natolive/official\\_texts\\_27433.htm?selectedLocale=en](http://www.nato.int/cps/en/natolive/official_texts_27433.htm?selectedLocale=en) Letöltve: 2017.01.12.
- [60.] Supreme Allied Commander Transformation: Framework for Future Alliance Operations. August 2015. URL: <http://www.act.nato.int/images/stories/media/doclibrary/ffao-2015.pdf> Letöltve: 2017.01.12.
- [61.] NATO Smart Defence. URL: [http://www.nato.int/cps/en/natohq/topics\\_84268.htm](http://www.nato.int/cps/en/natohq/topics_84268.htm) Letöltve: 2017.01.12.
- [62.] NATO, Press & Media Office: Defence Expenditures of NATO Countries (2008-2015). URL: [http://www.nato.int/cps/en/natohq/news\\_127537.htm](http://www.nato.int/cps/en/natohq/news_127537.htm) Letöltve: 2017.01.12.
- [63.] Csatári Sándor ezredes: A rádióelektronikai harc helyzete és továbbfejlesztésének fő iránya a Magyar Néphadseregben. Doktori értekezés. 1984. I. fejezet (I. kötet).
- [64.] Chandler Harris: Electronic Warfare Spending Rises in 2013 Budget Request. URL: <http://news.clearancejobs.com/2012/03/15/electronic-warfare-spending-rises-in-2013-budget-request/> Letöltve: 2013.10.13.
- [65.] United States Department of Defense, Fiscal Year 2014 Budget Request. URL: [http://comptroller.defense.gov/defbudget/fy2014/FY2014\\_Budget\\_Request\\_Overview\\_Book.pdf](http://comptroller.defense.gov/defbudget/fy2014/FY2014_Budget_Request_Overview_Book.pdf) Letöltve: 2013.10.18.
- [66.] Sydney J. Freedberg Jr.: Army's Electronic Warfare Cupboard Is Bare: No Jammer Until 2023. URL: <http://breakingdefense.com/2015/07/armys-electronic-warfare-cupboard-is-bare-no-jammer-until-2023/> Letöltve: 2017.01.22.
- [67.] Intelligence Resource Program, Prophet. URL: <http://www.fas.org/irp/program/collect/prophet.htm> Letöltve: 2017.01.22.

- [68.] Andrea Shalal: Pentagon sets up panel to study electronic warfare requirements. URL: <http://www.reuters.com/article/us-usa-military-electronicwarfare-idUSKBN0MD1PX20150318> Letöltve: 2017.06.20.
- [69.] How Good Is Russian Electronic Warfare? URL: 12.01.2016. <https://russiandefpolicy.wordpress.com/2015/10/27/how-good-is-russian-electronic-warfare-part-i/> Letöltve: 2017.06.20.
- [70.] John Keller: New Russian directed-energy weapon could complicate U.S. military strategic planning. 05.02.2016. URL: <http://www.militaryaerospace.com/articles/2015/07/directed-energy-weapon.html> Letöltve: 2017.06.20.
- [71.] Roman Dzsereljkó: Az orosz „Gamma-SZ1” rádiólokátor állomás. Fordította: Hajnal István őrnagy, szerkesztette: Somogyi Péter alezredes. URL: <http://raketaezred.hu/index.php/hirek/friss-hirek/796-gamma-sugarzo> Letöltve: 2017.06.20.
- [72.] John Costello: China Finally Centralizes Its Space, Cyber, Information Forces. URL: <http://thediplomat.com/2016/01/china-finally-its-centralizes-space-cyber-information-forces/> Letöltve: 2016.11.20.
- [73.] Ward Carroll: China's Cyber Forces. URL: <http://defensetech.org/2008/05/08/chinas-cyber-forces/> Letöltve: 2016.11.20.
- [74.] Jeffrey Lin-P.W. Singer: China Builds Its Own 'Wild Weasel' To Suppress Air Defenses. URL: <http://www.popsci.com/china-builds-its-own-wild-weasel-to-suppress-air-defenses> Letöltve: 2016.11.20.
- [75.] Congressional Research Service Reports: Network Centric Operations: Background and Oversight Issues for Congress. URL: <https://fas.org/sgp/crs/natsec/RL32411.pdf> Letöltve: 2016.11.20.
- [76.] NATO's merry-go-round electronic surveillance in the Black Sea. URL: <https://www.rt.com/news/163484-nato-black-sea-eavesdropping/> Letöltve: 2017.02.08.
- [77.] David Stupples: How Syria is becoming a test zone for electronic warfare. URL: <http://edition.cnn.com/2015/10/09/opinions/syria-electronic-warfare-russia-nato/> Letöltve: 2017.02.08.
- [78.] U.S. says strikes hit ISIS garrison, 'electronic warfare'. URL: <http://english.alarabiya.net/en/News/middle-east/2014/12/01/U-S-says-strikes-hit-ISIS-garrison-electronic-warfare-.html> Letöltve: 2017.02.08.
- [79.] Makk László mk. vezérőrnagy: A haderő átalakítása a hidegháború utáni korszak biztonsági kihívásainak tükrében. Zrínyi Miklós Nemzetvédelmi Egyetem. Doktori értekezés. 2008. URL: [http://archiv.uni-nke.hu/downloads/konyvtar/digitgy/phd/2008/makk\\_laszlo.pdf](http://archiv.uni-nke.hu/downloads/konyvtar/digitgy/phd/2008/makk_laszlo.pdf) Letöltés ideje: 2017.05.10.
- [80.] Sztvórecz András ezredes: A szárazföldi haderőnem elektronikai harc szakcsapatainak technikai és szervezeti korszerűsítése. Budapest, 1993. Zrínyi Miklós Nemzetvédelmi Egyetem. Kandidátusi értekezés. 9. o.
- [81.] Balogh Péter: A magyar katonai rádiófelderítés története. Rendvédelem-történeti Füzetek XXIII. évf. (2013) 31-34. szám. 15-16. o. URL:

- [http://epa.oszk.hu/02100/02176/00014/pdf/EPA02176\\_rendvedelem\\_31-34\\_015-026.pdf](http://epa.oszk.hu/02100/02176/00014/pdf/EPA02176_rendvedelem_31-34_015-026.pdf) Letöltve: 2016.05.15. HU-ISSN 1216-6774
- [82.] Hekli László alezredes: A harcászati és a hadművelleti rádióelektronikai felderítés története. Felderítő Szemle 2004/3. ISSN 1588-242X, 109-152. o.
- [83.] Szűcs László: Lehallgatásból önálló fegyvernem. URL: <http://www.honvedelem.hu/cikk/13362> Letöltve: 2016.10.18.
- [84.] Ványa László: Az elektronikai hadviselési csapatok: hogyan tovább? Hadtudomány, 2001.02.05. ISSN 1215-4121 Forrás: <http://www.zmne.hu/kulso/mhht/hadtudomany/2001/2/05/chapter1.htm> letöltve: 2013.10.13.
- [85.] Bozsóki Attila: Az elektronikai harc gyakorlatok kiképzési tapasztalatai, együttműködés lehetőségei a légierő csapataival. Repüléstudományi konferencia 2012, XXIV. évfolyam, 2012. 2. szám, 7-32. oldal, ISSN 1789-770X
- [86.] Vass Sándor százados: A Magyar Honvédségben az elektronikai harc — ezen belül az elektronikus védelem — számítógépekkel biztosított tervezése, különös tekintettel az elektromágneses kompatibilitás kérdéseire. Zrínyi Miklós Nemzetvédelmi Egyetem. Kandidátusi értekezés. 1995. 52., 57. oldal
- [87.] Magyar Honvédség 78. Gróf Pálffy Miklós Elektronikai harc század évkönyve, 1985-1995., Győr
- [88.] Pados László mérnök-alezredes: A rádióelektronikai harc helye, szerepe és feladatai a csapatrepülők harctevékenységében. Kandidátusi értekezés. MN Légyvédelmi és Repülő Parancsnokság. 1988. 51-52. o.
- [89.] Ványa László: Helikopterek elektronikai hadviselési alkalmazásai a 90-es évekig. Repüléstudományi közlemények. URL: [http://www.repulestudomany.hu/folyoirat/2017\\_2/2017-2-05-0371\\_Vanya\\_Laszlo.pdf](http://www.repulestudomany.hu/folyoirat/2017_2/2017-2-05-0371_Vanya_Laszlo.pdf) Letöltve: 2017.10.07. ISSN 1789-770X 65-72. oldal
- [90.] Sárý Zoltán: Repülő pingpongasztal, Aranysas, 2015. június, URL: [http://www.aranysas.hu/archivum\\_1506.php](http://www.aranysas.hu/archivum_1506.php) 50-54. oldal
- [91.] A Magyar Honvédség 5. Bocskai István Lövész dandár története II. 2004–2008., Debrecen: 2009. Magyar Honvédség, ISBN 978-963-06-4151-7
- [92.] Balogh Péter: A Magyar Honvédség ISTAR (ISR) képességei, a fejlesztés lehetséges irányai, különös tekintettel az elektronikai hadviselésre. Hadmérnök, VII. Évfolyam 4. szám - 2012. december, 75-94. oldal, ISSN 1788-1919 URL: [http://hadmernok.hu/2012\\_4\\_balogh.pdf](http://hadmernok.hu/2012_4_balogh.pdf) Letöltve: 2017. 05.14.
- [93.] Varga Zoltán őrnagy: Az elektronikai hadviselés helyzete a Magyar Honvédségben, alkalmazásának lehetőségei műveleti területen. Nemzeti Közzolgálati Egyetem, HHK, Diplomamunka. 2013.
- [94.] HVK Felderítő csoportfőnökség. URL: <http://www.honvedelem.hu/szervezet/hvkfelderito> Letöltve: 2017.09.29.
- [95.] MH Összhaderőnemi Parancsnokság. URL: [http://www.honvedelem.hu/szervezet/mh\\_ohp](http://www.honvedelem.hu/szervezet/mh_ohp) Letöltve: 2017.09.29.
- [96.] Antal Ferenc: Átkelés és álcázás. URL: <http://www.honvedelem.hu/cikk/40053> Letöltve: 2013.10.13.

- [97.] Domján László vezérőrnagy: A Magyar Honvédség PRT szerepvállalás előkészítése, a misszió főbb eseményei a nemzeti vezetés szemszögéből. Sereg Szemle, 2013.05.28., 26-40. o., ISSN: 2060-3924 URL: <http://www.honvedelem.hu/container/files/attachments/43461/seregszemle-kulonszam-internet.pdf> Letöltve: 2017. 01.25.
- [98.] Miskolczi József okl. mk. alezredes: A Magyar Honvédség elektronikai hadviselési erői és eszközei, alkalmazásuk lehetőségei. KFH Felderítő Szemle, VI. évfolyam, különszám. 2007.02. ISSN 1588-242X 145. o. URL: <http://knbsz.gov.hu/hu/letoltes/fsz/2007-konferencia.pdf> Letöltve: 2017.02.20.
- [99.] Halász András mérnök alezredes: Az összefegyvernemi hadművelet rádióellentevékenységeinek korszerű technikai eszközei. Kandidátusi disszertáció. Zrínyi Miklós Katonai Akadémia. 1963. 2. o.
- [100.] Bokor Imre mérnök alezredes: Az összefegyvernemi hadsereg rádióelektronikai harcának fejlődése a rádió elektronikai eszközök és rendszerek korszerűsítésének függvényében. Doktori értekezés. Zrínyi Miklós Katonai Akadémia. 1982. 3. o.
- [101.] Pacsay Tomassich Orsolya: A visegrádi együttműködés és regionális biztonság. Zrínyi Miklós Nemzetvédelmi Egyetem. Doktori értekezés. 2006. 34. o. URL: [http://archiv.uni-nke.hu/downloads/konyvtar/digitgy/phd/2007/pacsay-tomassich\\_orsolya.pdf](http://archiv.uni-nke.hu/downloads/konyvtar/digitgy/phd/2007/pacsay-tomassich_orsolya.pdf) Letöltés ideje: 2017.04.15.
- [102.] Király György alezredes: A szárazföldi összefegyvernemi hadsereg főcsapásának irányába támadó gépesített lövész (harcocsi) hadosztály rádióelektronikai harcának tervezése, szervezése és vezetése. Kandidátusi értekezés. MN Rádióelektronikai Főnökség. 1982. 14-15. o.
- [103.] Kovács László mk. őrnagy: Az elektronikai felderítés korszerű eszközei, eljárásai és azok alkalmazhatósága a Magyar Honvédségben. Doktori (PhD) értekezés. Zrínyi Miklós Nemzetvédelmi Egyetem. Budapest 2003. 46. o. URL: [http://archiv.uni-nke.hu/downloads/konyvtar/digitgy/phd/2004/kovacs\\_laszlo.pdf](http://archiv.uni-nke.hu/downloads/konyvtar/digitgy/phd/2004/kovacs_laszlo.pdf) Letöltve: 2017.06.10.
- [104.] Gácsér Zoltán mk. őrnagy: A katona harci képességét növelő korszerű, hálózatba integrált egyéni felszerelésrendszerének kialakítási lehetőségei a Magyar Honvédségben, Doktori (PhD) értekezés. Zrínyi Miklós Nemzetvédelmi Egyetem. Budapest, 2003. URL: [http://archiv.uni-nke.hu/downloads/konyvtar/digitgy/phd/2008/gacser\\_zoltan.pdf](http://archiv.uni-nke.hu/downloads/konyvtar/digitgy/phd/2008/gacser_zoltan.pdf) Letöltve: 2017.06.10.
- [105.] Gerlits Péter ny. mk. alezredes: Elhalt fejlesztések. URL: <http://www.hadmer0.atw.hu/> Letöltve: 2017. 07.20.
- [106.] Dékány István – Szőnyi István: A magyar katonai rádiófelderítés története. Zrínyi kiadó, Budapest, 2009. ISBN 978-963-327-465-1
- [107.] Dr. Ványa László: Az INTERJAM projekt első éve. URL: [http://archiv.uni-nke.hu/downloads/bsz/bszemle2008/4/04\\_Vanya\\_Laszlo.pdf](http://archiv.uni-nke.hu/downloads/bsz/bszemle2008/4/04_Vanya_Laszlo.pdf) Letöltve: 2018.06.01.
- [108.] Lázár Tibor: A BHG emlékére (Horváth Gyula - Kozma Gyula, a Rádiótechnika Évkönyve 1997 számában megjelent cikke alapján). URL: [http://lazarbibi.hu/index.php?option=com\\_content&view=article&id=55:a-bhg-emlekere&catid=22&Itemid=123](http://lazarbibi.hu/index.php?option=com_content&view=article&id=55:a-bhg-emlekere&catid=22&Itemid=123) Letöltve: 2017.07.15.

- [109.] Intel Security, (2015) McAfee Labs, Threats Predictions 2016. URL: <http://www.mcafee.com/us/resources/reports/rp-threats-predictions-2016.pdf> Letöltve: 2017.05.20.
- [110.] Központi Statisztikai Hivatal kimutatás: Háztartások info-kommunikációs eszközellátottsága és egyéni használat jellemzői (2005–). URL: [http://www.ksh.hu/docs/hun/xstadat/xstadat\\_eves/i\\_oni006.html](http://www.ksh.hu/docs/hun/xstadat/xstadat_eves/i_oni006.html) Letöltve: 2017.05.20.
- [111.] MH vitéz Szurmay Sándor Budapest Helyőrség Dandár. URL: <http://www.honvedelem.hu/szervezet/Szurmay> Letöltve: 2017.04.10.
- [112.] 7/2015. Nemzeti Média és Hírközlési Hatóság rendelete a nemzeti frekvenciafelosztásról, valamint a frekvenciasávok felhasználási szabályairól URL: [https://net.jogtar.hu/jr/gen/hjegy\\_doc.cgi?docid=a1500007.nmh](https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1500007.nmh) Letöltve: 2017.04.10.
- [113.] Nemzeti Média és Hírközlési Hatóság: A NATO Nemzeti Rádiófrekvencia Hivatal (NARFA) nemzeti hatósági feladatai. URL: [http://nmhh.hu/cikk/1657/a\\_nato\\_nemzeti\\_radiofrekvencia\\_hivatal\\_narfa\\_nemzeti\\_hatosagi\\_feladatai](http://nmhh.hu/cikk/1657/a_nato_nemzeti_radiofrekvencia_hivatal_narfa_nemzeti_hatosagi_feladatai) Letöltve: 2017.10.16.
- [114.] Di Pu – Alexander M. Wyglinski: Digital Communication systems engineering with Software-Defined Radio. Artech House 2013. 207-209. old. ISBN-13: 978-1-60807-525-6
- [115.] Paul Burns: Software Defined Radio for 3G. Artech House 2003. Norwood. 31. old. ISBN 1-58053-347-7
- [116.] Wireless Innovation Forum: What is Software Defined Radio? URL: [http://www.wirelessinnovation.org/index.php?option=com\\_content&view=article&id=63:Introduction\\_to\\_SDR&catid=19:site-content&Itemid=77](http://www.wirelessinnovation.org/index.php?option=com_content&view=article&id=63:Introduction_to_SDR&catid=19:site-content&Itemid=77) Letöltve: 2017.06.10.
- [117.] Hóka Miklós mk. alezredes: A Magyar Honvédség harcászati rádiórendszerének kialakítási lehetőségei egyes NATO-tagországok rádiórendszereinek vizsgálata tükrében. Doktori (PhD) értekezés. Zrínyi Miklós Nemzetvédelmi Egyetem. Budapest, 2005. 24. o. URL: [http://archiv.uni-nke.hu/downloads/konyvtar/digitgy/phd/2005/hoka\\_miklos.pdf](http://archiv.uni-nke.hu/downloads/konyvtar/digitgy/phd/2005/hoka_miklos.pdf) Letöltve: 2017.06.20.
- [118.] Wireless Innovation Forum: Software Defined Radio - Rate of Adoption. URL: [http://www.wirelessinnovation.org/sdr\\_rate\\_of\\_adoption](http://www.wirelessinnovation.org/sdr_rate_of_adoption) Letöltve: 2017.06.10.
- [119.] Fürjes János Norbert mk. őrnagy: Kis és közepes sebességű digitális adatátviteli rendszerek automatikus analízisének és dekódolásának lehetőségei. Doktori (PhD) értekezés. Zrínyi Miklós Nemzetvédelmi Egyetem. Budapest. 2010. URL: [http://archiv.uni-nke.hu/downloads/konyvtar/digitgy/phd/2011/furjes\\_janos.pdf](http://archiv.uni-nke.hu/downloads/konyvtar/digitgy/phd/2011/furjes_janos.pdf) Letöltve: 2017.06.20.
- [120.] Fürjes János: Nagy sávszélességű jelfeldolgozás kihívásai. Hadmérnök. 2007. november 27. ISSN 1788-1919 URL: [http://hadmernok.hu/kulonszamok/robothadviseles7/furjes\\_rw7.html](http://hadmernok.hu/kulonszamok/robothadviseles7/furjes_rw7.html) Letöltve: 2017.06.16.
- [121.] Szabó Géza: Analóg jelek digitális feldolgozása és továbbítása. Budapesti Műszaki és Gazdaságtudományi Egyetem, Jegyzet. 2001.



- [122.] Dr. Hrivnák István: Digitális-Analóg (D/A) és Analóg-Digitális (A/D) átalakítók. Budapesti Műszaki és Gazdaságtudományi Egyetem, Jegyzet. 32. oldal
- [123.] Fürjes János: Korszerű rádiófelderítés kihívásai az információs műveletekben. Hadmérnök. 2008. június. ISSN 1788-1919 URL: [http://hadmernok.hu/archivum/2008/2/2008\\_2\\_furjes.pdf](http://hadmernok.hu/archivum/2008/2/2008_2_furjes.pdf) Letöltve: 2017.11.12.
- [124.] Karika Róbert: Újrakonfiguráló algoritmusok tervezése és implementálása szoftverrádiós rendszerek hatékonyságának növelésére. Budapesti Műszaki és Gazdaságtudományi Egyetem. Diplomadolgozat. Budapest, 2006.
- [125.] Wireless Innovation Forum: Defining Cognitive Radio (CR) and Dynamic Spectrum Access (DS Ultimate Software Radio (USR)A). URL: [http://www.wirelessinnovation.org/Defining\\_CR\\_and\\_DSA](http://www.wirelessinnovation.org/Defining_CR_and_DSA) Letöltve: 2017.04.15.
- [126.] Wireless Innovation Forum: Cognitive radio concept architecture. URL: [http://www.wirelessinnovation.org/cognitive\\_radio\\_architecture](http://www.wirelessinnovation.org/cognitive_radio_architecture) Letöltve: 2017.04.15.
- [127.] Attila Gulyás: Enable command and control (C2) for Special Operation Forces through SDR applications. AARMS Vol. 8, No. 1 (2009) pp. 35–52 URL: <http://www.zmne.hu/aarms/docs/Volume8/Issue1/pdf/05guly.pdf> Letöltve: 2017.10.11.
- [128.] Hóka Miklós: A csúcstechnológia alkalmazása a hadszíntéren. Katonai Biztonsági Hivatal Szakmai Szemle. 2006. 2. szám. 73. oldal. ISSN: 1785-1181
- [129.] Walter Tuttlebee: Software Defined Radio (Enabling Technologies). John Wiley & Sons Ltd. Chichester, West Sussex, UK. 2002. ISBN 0-470-84318-7.
- [130.] John Keller: SDR and cognitive radio: the new horizons of military communications. URL: <http://www.militaryaerospace.com/articles/print/volume-22/issue-10/special-report/sdr-and-cognitive-radio-the-new.html> Letöltve: 2017.05.10.
- [131.] Jack Browne: Sampling SDRs For Tactical Applications. URL: <http://defenseelectronicsmag.com/systems-amp-subsystems/sampling-sdrs-tactical-applications> Letöltve: 2017.02.12.
- [132.] German Armed Forces commissions Rohde & Schwarz to develop SDR base unit. URL: [https://www.rohde-schwarz.com/us/news-press/press-room/press-releases-detailpages/rohde-schwarz-equips-the-german-federal-armed-forces-with-state-of-the-art-software-defined-radio-systems-press\\_releases\\_detailpage\\_229356-452548.html](https://www.rohde-schwarz.com/us/news-press/press-room/press-releases-detailpages/rohde-schwarz-equips-the-german-federal-armed-forces-with-state-of-the-art-software-defined-radio-systems-press_releases_detailpage_229356-452548.html) Letöltve: 2017.09.25.
- [133.] Defense World.net: Software Defined Radios For Russian Armed Forces [http://www.defenseworld.net/news/11325/Software\\_Defined\\_Radios\\_For\\_Russian\\_Armed\\_Forces](http://www.defenseworld.net/news/11325/Software_Defined_Radios_For_Russian_Armed_Forces) Letöltve: 2017.09.25.
- [134.] Adam Baddeley: Finland Lays Foundation for National Software-Defined Radio. URL: <http://www.afcea.org/content/?q=node/223> Letöltve: 2017.02.01.
- [135.] 1298/2017. (VI. 2.) Korm. határozat a Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program megvalósításáról. URL: [https://net.jogtar.hu/jr/gen/hjegy\\_doc.cgi?docid=A17H1298.KOR&timeshift=ffffff4&txtreferer=00000001.TXT](https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A17H1298.KOR&timeshift=ffffff4&txtreferer=00000001.TXT) Letöltve: 2017.10.14.

- [136.] Adrian Graham: Communications, Radar and Electronic Warfare. 2011. John Wiley & Son Ltd. Chichester, West Sussex, UK. ISBN 978-0-470-68871-7.
- [137.] Richard A. Poisel: Electronic warfare receivers and receiving systems. Egyesült Királyság. Artech House kiadó. 2014. 621. old. ISBN 13: 978-1-60807-847-1
- [138.] Karl Rothammel: Antennakönyv. 3. bővített, javított kiadás. Műszaki könyvkiadó, Budapest, 1977. ISBN: 963 10 0762 6
- [139.] FM 6-02.53 Tactical Radio Operations, 2009 Augusztus, Headquarters, Department of the Army
- [140.] Károly Krisztián főhadnagy: Globális műholdas navigációs rendszerek alkalmazási lehetőségei katonai és polgári célú flotta- és erőkövetési rendszerekben (1.). Honvédségi Szemle 2018/1. Vezetés, felkészítés. pp. 83-97. HU ISSN 2060-1506
- [141.] U.S. government: What is GPS? URL: <http://www.gps.gov/systems/gps/> Letöltve: 2017.03.15.
- [142.] U.S. government: GPS modernization. URL: <http://www.gps.gov/systems/gps/modernization/> Letöltve: 2017.03.15.
- [143.] Information and Analysis Center for Positioning, Navigation and Timing: GLONASS history URL: <http://glonass-iac.ru/en/guide/index.php> Letöltve: 2017.03.15.
- [144.] European Space Agency: What is Galileo? URL: [http://download.esa.int/docs/Galileo\\_IOV\\_Launch/Galileo\\_factsheet\\_2012.pdf](http://download.esa.int/docs/Galileo_IOV_Launch/Galileo_factsheet_2012.pdf) Letöltve: 2017.03.15.
- [145.] BeiDou System Introduction. URL: <http://en.beidou.gov.cn/introduction.html> Letöltve: 2017.03.15.
- [146.] Galileo Constellation Information. URL: <https://www.gsc-europa.eu/system-status/constellation-information> Letöltve: 2017.03.15.
- [147.] Beidou 3 (Compass Navigation Satellite System). URL: <http://spaceflight101.com/spacecraft/beidou-3/> Letöltve: 2017.03.15.
- [148.] Galileo: Galileo signal tracked by Rockwell Collins S-SDR receiver. URL: <http://galileognss.eu/galileo-signal-tracked-by-rockwell-collins-s-sdr-receiver/> Letöltve: 2017.03.15.
- [149.] Islam Alyafawi: Real-time localization using Software Defined Radio. Dolgozat. Berni Egyetem, Filozófia és természettudományi Intézet. 2015. URL: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.697.3237&rep=rep1&type=pdf> Letöltve: 2017.09.05.
- [150.] Software Defined Radio for Mobile Radio Networks. URL: [www3.alcatel-lucent.com](http://www3.alcatel-lucent.com) Letöltve: 2017.02.20.
- [151.] Jobbágy Szabolcs: WLAN hálózatról röviden. Hadmérnök, IV. Évfolyam 2. szám - 2009. június. p 303. [http://hadmernok.hu/2009\\_2\\_jobbagy.pdf](http://hadmernok.hu/2009_2_jobbagy.pdf)
- [152.] Nagy Dániel: Szórt spektrumú adatátvitel, a WIFI és a WIMAX megvalósításában. Hadmérnök, XI. Évfolyam 3. szám - 2016. szeptember, 191.-203. o. URL: [http://hadmernok.hu/163\\_15\\_nagy.pdf](http://hadmernok.hu/163_15_nagy.pdf) Letöltve: 2017.08.14.



- [153.] Doug Richardson: An illustrated guide to the techniques and equipment of electronic warfare. Salamander Books Ltd. 1996. UK, London, 10. o. ISBN 0 86101 266 8
- [154.] Radartutorial, Book 2. URL: <http://www.radartutorial.eu/druck/Book2.pdf> Letöltve: 2017.08.14.
- [155.] Balajti István: Az iker VHF radar stratégiai jelentősége a modern légvédelemben, Hadmérnök, VI. Évfolyam 4. szám - 2011. december. 140-153. o. URL: [http://hadmernok.hu/2011\\_4\\_balajti1.pdf](http://hadmernok.hu/2011_4_balajti1.pdf) Letöltve: 2017.06.18.
- [156.] Dr. Kurucz István - Kiss Tibor: A RAT-31DL radarok logisztikai biztosításának megvalósítása. Katonai logisztika. 2014. 22. évf. 2. sz. 32-74. o. URL: [http://epa.oszk.hu/02700/02735/00078/pdf/EPA02735\\_katonai\\_logisztika\\_2014\\_2\\_032-074.pdf](http://epa.oszk.hu/02700/02735/00078/pdf/EPA02735_katonai_logisztika_2014_2_032-074.pdf) Letöltve: 2017.06.18.
- [157.] Ferenczy Gábor, Szűcs Péter, Balog Károly: Rádiólokáció alapjai. Bolyai János Katonai Műszaki Főiskola. Főiskolai jegyzet. Budapest, 1988. 45. o.
- [158.] Gajendra Kumar: A Nexus between Radar System and Software Defined Radio to provide High-speed Communication System. URL: [http://www.mistralsolutions.com/newsletter/Jan12/Technical%20Paper\\_Mistral.pdf](http://www.mistralsolutions.com/newsletter/Jan12/Technical%20Paper_Mistral.pdf) Letöltve: 2017.06.18.
- [159.] W. G. Cheaw, Y. K. Chan, and V. C. KooW. G. Cheaw, Y. K. Chan, and V. C. Koo: Design of a Digital Synthetic Aperture Radar. URL: <https://piers.org/piersproceedings/download.php?file> Letöltve: 2017.06.18.
- [160.] Andrea Stockman, Niklas Glavmo: Software Development For a Radar Application Based on SDR Technology. URL: <http://publications.lib.chalmers.se/records/fulltext/200534/200534.pdf> Letöltve: 2017.06.18.
- [161.] Dr. Eged Bertalan: Integrált elektronikai felderítő és zavaró rendszer fejlesztése, rövid nevén, az Interjam projektzáró a Nemzetvédelmi Egyetemen. Előadás. 2010.09.30., Zrínyi Miklós Nemzetvédelmi Egyetem Bolyai terem.
- [162.] Dr. Eged Bertalan: Elektronikai hadviselési és felderítő rendszerek integrációja korszerű digitális - és szoftver rádió technológiával. IV. Évfolyam 2. szám. 2009. június. 269-283. o. URL: [http://hadmernok.hu/2009\\_2\\_eged.pdf](http://hadmernok.hu/2009_2_eged.pdf) Letöltve: 2017.05.10.
- [163.] Dr. Eged Bertalan: HT28 SAJ Integrált Felderítő és zavaró rendszer „INTERJAM” záró szakmai beszámoló. URL: <https://www.slideshare.net/beged/ht28-sajintrov20> Letöltve: 2017.09.10.
- [164.] SAGAX Kft.: SRS-3000 HF/VHF Wideband Search and Intercept Receiver datasheet.
- [165.] Dr. Eged Bertalan: Rádióelektronikai védelmi, hadviselési és harcvezetési rendszer. URL: <https://www.slideshare.net/beged/sagax-ew-projekt-intro> Letöltve: 2017.09.10.
- [166.] Prof. Dr. Ványa László okl. mk. ezredes, PhD: UP-3MA ultrarövidhullámú panoráma vevőkészülék. Típusismeret előadás.
- [167.] Prof. Dr. Ványa László okl. mk. ezredes, PhD: UP-3MB ultrarövidhullámú panoráma vevőkészülék. Típusismeret előadás.

- [168.] Prof. Dr. Ványa László okl. mk. ezredes, PhD: VU-21M ultrarövidhullámú vevőkészülék. Típusismeret előadás.
- [169.] Prof. Dr. Ványa László okl. mk. ezredes, PhD: VU-32M ultrarövidhullámú vevőkészülék. Típusismeret előadás.
- [170.] Jordan Electronic Logistics Support: Signal Sniper adatlap. URL: [http://www.jels-tech.com/images/pdf/signal\\_sniper.pdf](http://www.jels-tech.com/images/pdf/signal_sniper.pdf) Letöltve: 2017.11.08.
- [171.] Horváth József: A szoftverrádió technológián alapuló elektronikai hadviselési eszköz hatékony működéséhez szükséges adatok biztosításának vizsgálata. Seregszemle. XIV. évfolyam, 1. szám, 2016. január–február 76-85. o. ISSN: 2060-3924 URL: [http://www.honvedelem.hu/container/files/attachments/57646/2016\\_1\\_seregszemle\\_internet.pdf](http://www.honvedelem.hu/container/files/attachments/57646/2016_1_seregszemle_internet.pdf) Letöltve: 2017.04.18.
- [172.] Charles Clancy, Joe Hecker, Erich Stuntebeck, Tim O'Shea: Applications of machine learning to cognitive radio networks. URL: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.145.2762&rep=rep1&type=pdf> Letöltve: 2017. 05.10.
- [173.] Nagy László: A Magyar Honvédség helikopter-képesség fejlesztés műszaki és üzemben tartási kérdései. Repüléstudományi közlemények. URL: [http://www.repulestudomany.hu/folyoirat/2017\\_2/2017-2-01-0370\\_Nagy\\_Laszlo.pdf](http://www.repulestudomany.hu/folyoirat/2017_2/2017-2-01-0370_Nagy_Laszlo.pdf) Letöltve: 2017.10.07. ISSN 1789-770X 50. oldal
- [174.] Richard A. Poisel: Antenna systems and electronic warfare applications. Egyesült Királyság. Artech House kiadó. 2012. 1. old. ISBN 13: 978-1-60807-484-6
- [175.] Balogh Károly Szoftver rádiók a kommunikációs felderítésben, Repüléstudományi közlemények, 2003/2. szám. URL: [http://www.repulestudomany.hu/kulonszamok/2003\\_cikkek/balogh\\_karoly.pdf](http://www.repulestudomany.hu/kulonszamok/2003_cikkek/balogh_karoly.pdf) Letöltve: 2017.09.22.
- [176.] Aaron Mehta: For NATO, a Cloudy Future. URL: <http://www.defensenews.com/story/defense/air-space/isr/2015/05/23/nato-combat-cloud-future-mercier-shaffer-interoperable-f35-typhoon-rafale-network/70893364/> Letöltve: 2017.10.18.
- [177.] National Institute of Standards and Technology: The NIST Definition of Cloud Computing. Special Publication 800-145. URL: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf> Letöltve: 2017.08.05.
- [178.] Horváth József alezredes: Elektronikai hadviselés a felhőben. Sereg Szemle. XV. évfolyam, 1. szám, 2017. január–március., 124-131.o., HU ISSN: 2060-3924 URL: [http://www.honvedelem.hu/container/files/attachments/65846/2017\\_1-seregszemle-internet.pdf](http://www.honvedelem.hu/container/files/attachments/65846/2017_1-seregszemle-internet.pdf) Letöltve: 2017.11.05.
- [179.] Kovács Zoltán: Az infokommunikációs rendszerek nemzetbiztonsági kihívásai, 15. oldal. Doktori (PhD) értekezés. Nemzeti Közszolgálati Egyetem. 2015. URL: [http://archiv.uni-nke.hu/feltoltes/uni-nke.hu/konyvtar/digitgy/phd/2015/kovacs\\_zoltan\\_2015.pdf](http://archiv.uni-nke.hu/feltoltes/uni-nke.hu/konyvtar/digitgy/phd/2015/kovacs_zoltan_2015.pdf) Letöltés ideje: 2017.07.10.
- [180.] Aaron Kiser, Maj. - Jacob Hess, Maj. - El Mostafa Bouhafa, Maj. - Shawn Williams, DIA.: The Combat Cloud, enabling multi-domain command and control

- across the range of military operations. Maxwell Air Force Base, Alabama, 2017.  
Március URL: [www.dtic.mil/get-tr-doc/pdf?AD=AD1042210](http://www.dtic.mil/get-tr-doc/pdf?AD=AD1042210) Letöltve: 2017.08.10.
- [181.] Patrick Tucker: Russia, Too, Is Building a Giant War Cloud. URL: <https://www.defenseone.com/technology/2018/06/russia-too-building-giant-war-cloud/148822/> Letöltve: 2017.08.10.
- [182.] Michelberger Pál: Honvédelmi célú informatikai rendszerelemek kiválasztása és bevezetése. 2005. Budapest. Zrínyi Miklós Nemzetvédelmi Egyetem. Doktori értekezés. 11. o. URL: [http://archiv.uni-nke.hu/downloads/konyvtar/digitgy/phd/2005/michelberger\\_pal.pdf](http://archiv.uni-nke.hu/downloads/konyvtar/digitgy/phd/2005/michelberger_pal.pdf) Letöltés ideje: 2017.06.15.
- [183.] HM ARZENÁL Elektromechanikai ZRt.: Védelmi ipari tevékenység. URL: <http://www.hmarzenal.hu/vedelmi-ipar/vedelmi-ipari-tevekenyseg.html> Letöltve: 2018.01.19.
- [184.] BHE Bonn Hungary Elektronikai Kft.: „KFI\_16-1-2016-0254, nagy megbízhatóságú, nemzeti biztonsági stratégiai műveletet támogató MIMO adatrádió rendszer kifejlesztése, gyártásának és üzemeltetésének előkészítése hazai platformokon” URL: <http://www.bhe-mw.eu/tender> Letöltve: 2018.01.19.
- [185.] Rába Jármű Kft. URL: <http://www.raba.hu/jarmu/> Letöltve: 2017.09.20.
- [186.] Rába Jármű Kft. URL: [http://www.raba.hu/jarmu/katonai\\_jarmugyartas.html](http://www.raba.hu/jarmu/katonai_jarmugyartas.html) Letöltve: 2017.09.20.
- [187.] Gamma Műszaki ZRt. URL: <http://gammatech.hu/index.php?module=news&lang=hun&newsid=7> Letöltve: 2017.09.20.
- [188.] Gamma Műszaki Zrt. URL: [http://respirator.hu/img/komondor\\_photogallery/index.php](http://respirator.hu/img/komondor_photogallery/index.php) Letöltve: 2017.09.20.
- [189.] Gamma Műszaki ZRt. <http://www.respirator.hu/?lang=hun&mnuGrp=mnuGalery&module=galery&site=gal1> Letöltve: 2017.09.20.
- [190.] Ficsor Lajos - Krizsán Zoltán - Dr. Mileff Péter: Szoftverfejlesztés. 2011, Miskolci Egyetem, Általános Informatikai Tanszék, 15. old.
- [191.] Fehér Krisztián: Szoftvertesztelési alapismeretek. BBS-INFO kiadó, Budapest, 2016. ISBN 978-615-5477-31-7
- [192.] Haig Zsolt - Várhegyi István A cybertér és a cyberhadviselés értelmezése. Hadtudomány 2008/Elektronikus szám. 2. old.
- [193.] Lovas Tamás – Berényi Attila: Távérzékelés jegyzet, BME, Budapest, 2011. URL: [http://www.fmt.bme.hu/fmt/oktatas/feltoltesek/BMEEOFTMK08/taverzekeles\\_msc\\_jegyzet.pdf](http://www.fmt.bme.hu/fmt/oktatas/feltoltesek/BMEEOFTMK08/taverzekeles_msc_jegyzet.pdf) Letöltve: 2017.07.20.
- [194.] Verőné Wojtaszek Malgorzata: Fotointerpretáció és távérzékelés 3., A lézer alapú távérzékelés. URL: [http://www.tankonyvtar.hu/hu/tartalom/tamop425/0027\\_FOI3/ch01s07.html](http://www.tankonyvtar.hu/hu/tartalom/tamop425/0027_FOI3/ch01s07.html) Letöltve: 2017.07.20.

- [195.] Erol Gelenbe - Yasin Murat Kadioglu: Battery Attacks on Sensors. URL: [https://san.ee.ic.ac.uk/publications/Security\\_WS%2718\\_ymk.pdf](https://san.ee.ic.ac.uk/publications/Security_WS%2718_ymk.pdf) Letöltve: 2017.06.20.
- [196.] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról. URL: <https://net.jogtar.hu/jogszabaly?docid=a1300050.tv> Letöltve: 2018.08.24.
- [197.] Dr. Haig Zsolt mk. alezredes: Számítógép–hálózati hadviselés rendszere az információs műveletekben. Bolyai szemle. 2006/I. 3. old. URL: [http://archiv.uni-nke.hu/downloads/bsz/bszemle2006/1/06\\_Haig\\_Zsolt.pdf](http://archiv.uni-nke.hu/downloads/bsz/bszemle2006/1/06_Haig_Zsolt.pdf) Letöltve: 2018.06.10.
- [198.] Magyar Távirati Iroda: Iránt kibertámadás érte. URL: <http://www.honvedelem.hu/cikk/22112/irant-kibertamadas-erte> Letöltve: 2017.09.15.
- [199.] Gyányi Sándor: Túlerheléses informatikai támadási módszerek és a velük szemben alkalmazható védelem. Doktori (PhD) értekezés. Nemzeti Közszerológati Egyetem. Budapest. 2011. 21. old. URL: [http://archiv.uni-nke.hu/downloads/konyvtar/digitgy/phd/2012/gyanyi\\_sandor.pdf](http://archiv.uni-nke.hu/downloads/konyvtar/digitgy/phd/2012/gyanyi_sandor.pdf) Letöltés ideje: 2017.07.15.
- [200.] Norton Symantec: How do Zero-Day Vulnerabilities work. URL: <https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html> Letöltve: 2018.08.10.
- [201.] Horváth József alezredes: A szoftverrádió alapú elektronikai hadviselési eszközök elleni támadás formái és a védekezés lehetőségei. Sereg Szemle, XIV. évfolyam 1. szám, 2016. január-február, 76-85. oldal, ISSN 2060-3924 URL: [http://www.honvedelem.hu/container/files/attachments/57646/2016\\_1\\_seregszemle\\_internet.pdf](http://www.honvedelem.hu/container/files/attachments/57646/2016_1_seregszemle_internet.pdf) Letöltve: 2017.09.05.
- [202.] David Fernandes CruzMoura - Fabricio Alves Barbosa da Silva - Juraci Ferreira Galdino: Case Studies of Attacks over AdaptiveModulation Based Tactical Software Defined Radios. Hindawi Publishing Corporation. Journal of Computer Networks and Communications. 2012. Article ID 703642. doi:10.1155/2012/703642 URL: <https://www.hindawi.com/journals/jcnc/2012/703642/> Letöltve: 2017.08.22.
- [203.] Munk Sándor: Kiberbiztonsági eseménykezelő szervezetek rendeltetése, feladatai. Hadmérnök. XIII. Évfolyam 3. szám – 2018. június. 434. o. ISSN 1788-1919 URL: [http://www.hadmernok.hu/182\\_30\\_munk.pdf](http://www.hadmernok.hu/182_30_munk.pdf) Letöltve: 2018.08.15.
- [204.] Black Cell Kft., Informatikai Biztonsági Egység, Szolgáltatások. URL: <https://blackcell.hu/szolgáltatások/offenziv-szolgáltatások/> Letöltve: 2018.09.14.

## Rövidítések jegyzéke

|         |                                                                                                                                                                                                                                                       |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AGS     | Alliance Ground Surveillance, Szövetségi Felszínellenőrzési Rendszer                                                                                                                                                                                  |
| AM      | Amplitúdómoduláció                                                                                                                                                                                                                                    |
| AOPG    | Air Operational Planning Group, légierő tervezőcsoport                                                                                                                                                                                                |
| ASIC    | Application-Specific Integrated Circuit, alkalmazás specifikus integrált áramkör                                                                                                                                                                      |
| BHG     | Beloianisz Híradástechnikai Gyár                                                                                                                                                                                                                      |
| BITE    | Built-In Test Equipment, beépített tesztrendszer                                                                                                                                                                                                      |
| BPSK    | Binary Phase Shift Keying, kétállapotú fázisbillentyűzéses moduláció                                                                                                                                                                                  |
| C-RCIED | Counter Radio Controlled Improvised Explosive Devices, Vezeték nélküli robbanóanyagok elleni zavaróeszköz                                                                                                                                             |
| C4ISR   | Command, Control, Communications, Computer, Intelligence, Surveillance, Reconnaissance, Vezetési, Irányítási, Hírközlési, Számítógépes, Hírszerző, Megfigyelő és Felderítő rendszerek információit egyesítő integrált híradó és informatikai rendszer |
| CDMA    | Code Division Multiple Acces, kódosztásos többszörös hozzáférése moduláció                                                                                                                                                                            |
| COMINT  | Communication Intelligence, kommunikációs felderítés                                                                                                                                                                                                  |
| COTS    | Commercial-off-the-shelf, boltok polcáról levehető (alkatrészek, eszközök)                                                                                                                                                                            |
| CRC     | Control and Reporting Centre, Légi Irányító Központ                                                                                                                                                                                                   |
| CVSD    | Continuously variable slope delta, folyamatosan változó meredekségű delta modulációjú hangkódolás                                                                                                                                                     |
| DA      | Direct Actions, közvetlen műveletek                                                                                                                                                                                                                   |
| DDoS    | Distributed Denial of Service, elosztott szolgáltatásmegtagadással járó informatikai támadás                                                                                                                                                          |
| DDS     | Direct Digital Syntheser - magas órajelből kisebb frekvenciájú komponensek szintetizálására alkalmazott áramköri elem, amely analóg kimenő jelet biztosít a kimenetén.                                                                                |
| DoS     | Denial of Service, szolgáltatás-megtagadásos támadás                                                                                                                                                                                                  |
| DSSS    | Direct Sequence Spread Spectrum, közvetlen sorrendű, szórt spektrumú moduláció                                                                                                                                                                        |
| DSP     | Digital Signal Processor, Digitális jelfeldolgozási algoritmusok végrehajtására optimalizált processzor                                                                                                                                               |

|       |                                                                                                        |
|-------|--------------------------------------------------------------------------------------------------------|
| EA    | Electronic Attack, elektronikai támadás                                                                |
| ED    | Electronic Defence, elektronikai védelem                                                               |
| ED    | Electronic Deception, elektronikai megtévesztés                                                        |
| EDGE  | Enhanced Data GSM Environment, GSM rendszer csomagkapcsolt adatátviteli megoldásának továbbfejlesztése |
| EHV   | Elektronikai hadviselés                                                                                |
| ERP   | Effective Radiated Power, tényleges kisugárzott teljesítmény                                           |
| EJ    | Electronic Jamming, elektronikai zavarás                                                               |
| ELINT | Electronic Intelligence, nem-kommunikációs felderítés                                                  |
| EMB   | Electromagnetic Battle Staff, Elektromágneses Tevékenységet Koordináló Törzs                           |
| EMC   | Electromagnetic compatibility, elektromágneses kompatibilitás                                          |
| EMI   | Electromagnetic interference, elektromágneses zavaró hatás                                             |
| EMCON | Emission control, kisugárzás korlátozás                                                                |
| EN    | Electronic Neutralisation, elektronikai pusztítás                                                      |
| ENISA | European Network and Information Security Agency, Európai Hálózat- és Információbiztonsági Ügynökség   |
| ENSZ  | Egyesült Nemzetek Szövetsége, United Nations, UN                                                       |
| ES    | Electronic Surveillance, elektronikai megfigyelés                                                      |
| EU    | European Union, Európai Unió                                                                           |
| EOB   | Electronic Order of Battle, elektronikai harcrend                                                      |
| EWCC  | Electronic Warfare Coordination Cell, Elektronikai Hadviselési Koordinációs Részleg                    |
| FHSS  | Frequency Hopping Spread Spectrum, frekvenciaugratásos, szórt spektrumú moduláció                      |
| FMV   | Finommechanikai Vállalat                                                                               |
| FM    | Frekvenciamoduláció                                                                                    |
| FPGA  | Field Programmable Gate Array – szabadon (felhasználó által) programozható logikai áramkörü elem       |
| GDP   | Gross Domestic Product, bruttó hazai termék                                                            |
| GNSS  | Global Navigation Satellite Systems, globális helymeghatározó műholdas rendszer                        |
| GUI   | Graphical User Interface, grafikus felhasználói felület                                                |
| GPRS  | General Packet Radio Service, Általános csomagkapcsolt rádiószolgáltatás                               |

|              |                                                                                                              |
|--------------|--------------------------------------------------------------------------------------------------------------|
| GPS          | Navigation System with Timing and Ranging Global Positioning System, NAVSTAR GPS                             |
| GSM          | Global System for Mobile Communications, több sávban működő sávban működő páneurópai kommunikációs szabvány  |
| HÁEI-BEK     | Honvédelmi Ágazati Elektronikus Információbiztonsági Eseménykezelő Központ                                   |
| HARM         | High-speed Anti-Radiation Missile, nagy sebességű radarromboló rakéta                                        |
| HMMWV        | High Mobility Multipurpose Wheeled Vehicle, nagy mozgékonyágú többcélú kerekes jármű                         |
| HSCSD        | High Speed Circuit Switched Data, nagy sebességű vonalkapcsolt adatátvitel                                   |
| IED          | Imitative Electronic Deception - imitációs elektronikai megtévesztés                                         |
| IEEE         | Institute of Electrical and Electronic Engineers, Villamos- és Elektronikai Mérnökök Intézete                |
| IEWCS        | Intelligence and Electronic Warfare Common Sensor, Egyesített Felderítő és Elektronikai Hadviselési Rendszer |
| IFF          | Identification Friend or Foe, idegen-barát felismerő                                                         |
| INEW         | Integrated Network-Electronic Warfare, Hálózatalapú elektronikai hadviselés                                  |
| INFOOPS      | Information Operations, információs műveletek                                                                |
| INTERJAM     | Integrált elektronikai felderítő és zavaró rendszer                                                          |
| ISIS vagy IS | Islamic State of Iraq and Syria, Iraki és Szíriai Iszlám Állam, röviden Iszlám Állam                         |
| ISR          | Ideal Software Radio, Ideális szoftverrádió                                                                  |
| ITU          | International Telecommunication Union, Nemzetközi Távközlési Egyesület                                       |
| JEWCS        | Joint Electronic Warfare Core Staff, Összhaderőnemi Elektronikai hadviselés törzs                            |
| JIEDDO       | Joint IED Defeat Organization, Összhaderőnemi IED Elleni Szervezet                                           |
| JOC          | Joint Operational Centre, hadműveleti központ                                                                |
| JOPG         | Joint Operational Planning Group, JOPG                                                                       |
| JTRS         | Joint Tactical Radio System, összhaderőnemi harcászati rádiórendszer                                         |
| LAN          | Local Area Network, Helyi Hálózat                                                                            |
| LIDAR        | Light Detection and Ranging, lézer alapú távérzékelés                                                        |
| LoS          | Line of Sight, rálátás                                                                                       |

|           |                                                                                                                                  |
|-----------|----------------------------------------------------------------------------------------------------------------------------------|
| LOPG      | Land Operational Planning Group, szárazföldi tervezőcsoport                                                                      |
| LPI       | Low Probability of Intercept, kis valószínűséggel felderíthető adásmód                                                           |
| M3TR      | Multiband, Multimode, Multirole Tactical Radio, Többsávos, több üzemmódú és többcélú harcászati rádió                            |
| MA        | Military Assistance, katonai segítségnyújtás                                                                                     |
| MED       | Manipulative Electronic Deception – manipulációs elektronikai megtévesztés                                                       |
| MH PRT    | Magyar Honvédség Tartományi Újjáépítési Csoport                                                                                  |
| MN        | Magyar Néphadsereg                                                                                                               |
| MoU       | Memorandum of Understanding, Egyetértési szerződés                                                                               |
| NATO      | North Atlantic Treaty Organisation, Észak-atlanti Szerződés Szervezete                                                           |
| NATINAMDS | NATO Integrated Air and Missile Defence, NATO Integrált Lég- és Rakétavédelmi Rendszer                                           |
| NATO SACT | NATO Supreme Allied Commander Transformation, NATO Szövetséges Legfelsőbb Átalakítási Parancsnokság                              |
| NEDB      | NATO Emitter Database, NATO kisugárzó eszközök adatbázisa                                                                        |
| NEWFIP    | NATO Electronic Warfare Integration Programme, NATO Elektronikai Hadviselési Integrációs Program                                 |
| NIST      | National Institute of Standards and Technology, Amerikai Nemzeti Szabványügyi és Technológiai Intézet                            |
| NOTS      | NATO Off The Shelf, a NATO dokumentációkban az „N” betű a szűk piaccal rendelkező, speciális igényeket kielégítő termékekre utal |
| NRL       | Naval Research Laboratory, Haditengerészeti Kutatólaboratórium                                                                   |
| OFDM      | Orthogonal Frequency Division Multiplexing, ortogonális frekvenciaosztásos multiplexálás                                         |
| OFDMA     | Orthogonal Frequency Division Multiple Access                                                                                    |
| OPORD     | Operation order, műveleti parancs                                                                                                |
| OTM       | On The Move, menetben/mozgásban (manőver alatt)                                                                                  |
| ÖMTCS     | összhaderőnemi művelettervező csoport, Joint Operational Planning Group, JOPG                                                    |
| PNT       | Positioning, Navigation, Timing, pozíció, navigáció, pontos idő                                                                  |
| QPSK      | Quadrature Phase-Shift Keying, 4 állapotú fázisbilleltűzéses moduláció                                                           |
| RAP       | Recognised Air Picture, azonosított légihelyzet-kép                                                                              |
| RELEK     | Rádióelektronikai Ellenőrző Központ                                                                                              |



|          |                                                                                                                          |
|----------|--------------------------------------------------------------------------------------------------------------------------|
| RC-IED   | Radio controlled improvised Explosive Device, vezeték-nélküli robbanóanyag                                               |
| SA       | Situational awareness, harcászati helyzetismeret                                                                         |
| SAR      | Synthetic Aperture Radar, szintetikus apertúrájú radar                                                                   |
| SCR      | Software Controlled Radio, Szoftver kontrollált rádió                                                                    |
| SDR      | Software Defined Radio, Szoftver vezérelt rádió                                                                          |
| SEAD     | Suppression of Enemy Air Defence, ellenséges légvédelem lefogása                                                         |
| SED      | Simulative Electronic Deception – szimulációs elektronikai megtévesztés                                                  |
| SEWOC    | SIGINT and Electronic Warfare Coordination Cell, Rádióelektronikai Felderítő és Elektronikai Hadviselés Műveleti Központ |
| SIGINT   | Signal Intelligence, rádióelektronikai felderítés                                                                        |
| SINCGARS | Single-Channel Ground and Airborne Radio System                                                                          |
| SLA      | Service Level Agreement, szolgáltatási szint szerződés                                                                   |
| SOI      | Signals of Interest,                                                                                                     |
| SOPG     | Special Operational Planning Group, különleges műveleti tervezőcsoport                                                   |
| SR       | Special Reconnaissance, különleges felderítés                                                                            |
| SSB      | Single Side Band modulation, egy oldalsávós moduláció                                                                    |
| S-SDR    | Secure Software Defined Radio,                                                                                           |
| SUAV     | Small Unmanned Aerial Vehicle, kisméretű pilóta nélküli légi jármű                                                       |
| TRADOC   | U.S. Army Training and Doctrine Command, Amerikai Szárazföldi Haderő Kiképzési és Doktrínális Parancsnokság              |
| UAV      | Unmanned Aerial Vehicle, pilóta nélküli repülő járművek                                                                  |
| UGS      | Unattended Ground Sensors, felügyelet nélküli földi szenzorok                                                            |
| UGV      | Unattended Ground Vehicles, felügyelet nélküli földi járművek                                                            |
| UMTS     | Universal Mobile Telecommunications System, harmadik generációs (3G) mobil adat- és hang-átvitelt biztosító rendszer     |
| USR      | Ultimate Software Radio, Végző szoftverrádió                                                                             |
| TÁKI     | Távközlési Kutató Intézet                                                                                                |
| TTPs     | Tactics, Technics and Procedures, Taktikák, Technikák és Eljárások                                                       |
| VSAT     | Very Small Aperture Terminal, műholdelérési szolgáltatásokat biztosító infokommunikációs rendszer                        |
| VSZ      | Varsói Szerződés                                                                                                         |
| WDL      | Waveform Description Language, hullámforma leíró nyelv                                                                   |
| WLAN     | Wireless Local Area Network, Vezeték nélküli helyi kiterjedésű hálózat                                                   |



## ÁBRÁK JEGYZÉKE

|                                                                                                                     |         |
|---------------------------------------------------------------------------------------------------------------------|---------|
| 1.1. ábra: NATO államok védelmi kiadásai.....                                                                       | 31. o.  |
| 1.2. ábra: Az MN első rádiófelderítő századának felépítése. ....                                                    | 37. o.  |
| 1.3. ábra: Az EHV század felépítése az eszközök vonatkozásában. ....                                                | 40. o.  |
| 2.1. ábra: Háztartások mobil-előfizetéseinek száma, valamint mobil szélessávú internet előfizetéseinek aránya. .... | 54. o.  |
| 2.2. ábra: A szoftver-vezérlésű rádió egy csatornájának blokkvázlata. ....                                          | 58. o.  |
| 2.3. ábra: A hibrid helymeghatározó rendszer tesztkörnyezetének felépítése. ....                                    | 74. o.  |
| 2.4. ábra: Okos antenna rendszer SDR rádióval.....                                                                  | 79. o.  |
| 2.5. ábra: Az SRS-3000 panorámavevő jelfeldolgozása. ....                                                           | 83. o.  |
| 3.1. ábra: A Gamma Zrt. nagy teherbírású járműve és beépített utánfutója. ....                                      | 120. o. |

## Képek jegyzéke

|                                                                                                                                                              |         |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| 1.1. kép: Orosz eredetű elektronikai hadviselési állomás Donbass területén.....                                                                              | 20. o.  |
| 1.2. kép: Magyar jelzésű HMMWV beépített elektronikai zavaróeszközének antennái az MH PRT táborában.....                                                     | 43. o.  |
| 1.3. kép: Interjam zavaró állomás labormintája. ....                                                                                                         | 48. o.  |
| 2.1. kép: Az INTERJAM eszköz labormintája gépjárműbe beépítve.. ....                                                                                         | 78. o.  |
| 2.2. kép: Az INTERJAM projekt eszköze és a Signal Sniper kezelőfelülete, valamint kijelzőik.....                                                             | 86. o.  |
| 2.3. kép: UP-3MB ultrarövidhullámú panorámaindikátora, az INTERJAM SRS-3000 panorámavevő, valamint a Signal Sniper által biztosított képi megjelenítés. .... | 89. o.  |
| 3.1. kép: H18.206DAE-001 terepjáró bázisjármű.....                                                                                                           | 110. o. |
| 3.2. kép: RDO-3221 KOMONDOR jármű, tetején a Pro Patria Electronics Kft. által forgalmazott PGSR-3i ‘Beagle’ mozgócél felderítő radarral.....                | 111. o. |

**Táblázatok jegyzéke**

2.1. táblázat: Globális helymeghatározó rendszerek alapadatai a 2018. 08. 24-i helyzetnek megfelelően ..... 73. o.