

MMXV.

III. ÉVFOLYAM

II. SZÁM

# NEMZETBIZTONSÁGI

# SZEMLE

KÜLÖNLENYOMAT



NEMZETI KÖZSZOLGÁLATI EGYETEM  
NEMZETBIZTONSÁGI INTÉZET  
BUDAPEST

## Nemzetbiztonsági célú rövidhullámú stratégiai COMINT rendszerek elektronikai védelmi megfontolásai

Kovács Róbert

### Absztrakt:

Az 1990-es rendszerváltást követően Magyarországon létrejött demokratikus nemzetbiztonsági szolgálatok struktúrája új keretet adott a magyarországi rádiófelderítő tevékenységnek. A közelmúlt technológiai fejlődése (szélessávú feldolgozás, szoftverrádió technológia, többcsatornás vevőrendszerek) a rövidhullámú felderítésben is új technológiai, szervezési megközelítéseket követelt meg. A stratégiai adatszerző rendszerek egyik legfontosabb jellemzője, hogy az elektronikai védelem eszközeivel hogyan képes az elektronikai támadásokkal szemben fellépni.

A cikk a rövidhullámú sávú adatszerzés sajátosságainak bemutatásával, rövid történeti áttekintést nyújt a jelenlegi magyarországi rádiófelderítés szervezeti rendszerének kialakulásáról és tematikusan vizsgálja a rövidhullámú stratégiai adatszerző rendszer elemeinek (stationer RH központ, stationer és mobil RH szenzorok) lehetséges elektronikai védelmi aspektusait.

**Kulcsszavak:** stratégiai, rádiófelderítés, rövidhullámú, elektronikai védelem, nemzetbiztonság

### Abstract:

After the change of regime in 1990, the new democratic structure of national security services provided a new framework for radio reconnaissance activity in Hungary. The recent technological improvements (wideband processing, software radio technology, multi-channel receiver systems) also required a new technological, organizational approaches in shortwave signal intelligence. The key feature of strategic data gathering systems is how to use the measures of electronic protection to act against electronic attacks.

Based on introducing the particularities of data gathering in HF band, this article is intended to provide short historical overview of the current Hungarian radio reconnaissance formations and thematically examines the potential electronic protection aspects of a strategic shortwave data acquisition system components (stationary HF centers, stationary and mobile HF sensors).

**Keywords:** strategical, SIGINT/COMINT, shortwave-high frequency, electronic protection measures, national security

## Bevezetés

A nemzetbiztonsági célú rövidhullámú sávú stratégiai rádiófelderítő rendszerekben alkalmazható elektronikai védelmi lehetőségek nagymértékben függenek a rendszerek sávspecifikus kialakítási lehetőségeitől, fizikai, technológiai sajátosságaitól. A mai magyarországi nemzetbiztonsági célú adatgyűjtéshez kapcsolódó elektronikai védelmi intézkedések meghatározásához szükséges megvizsgálni a rádiófelderítésnek háttérrel adó hullámtartományi sajátosságokat, a magyarországi szervezeti berendezkedést, valamint a stratégiai rendszerek elemeinek egyedi jellemzőit, melyek befolyásolják az alkalmazható védelmi módszerek körét. A rövidhullámú stratégiai rádiófelderítő rendszerek jellemzői áttekintésének, a főbb rendszerelemek egyedi vizsgálatának célja annak megválaszolása, hogy elektronikai védelmi szempontból ezen rendszerelemek mutatnak-e olyan sajátosságokat, amelyek meghatározók a rendszer egésze szempontjából.

## 1. Rövidhullámú adatszerzés sajátosságai

### 1.1 Hullámterjedés a rövidhullámú sávban

A földfelszíni adó és vevőberendezések között a rádióhullámok alapvetően két fajta módon terjednek. A Föld felszínének közelében, mint felületi vagy talajhullámok illetve a nagyobb magasságokban az ún. térhullámok útján.

A rövidhullámú (3-30 MHz) tartományba eső elektromágneses hullámok terjedésében jelentős szerepe van a Föld légkörének az atmoszférának. Azon belül is a tropopauza<sup>1</sup> felett kb. 10-11 km-es magasságtól kezdődő sztratoszféra valamint az afölötti, hozzávetőleg 80-800 km-es magasságban elhelyezkedő, ionoszférának nevezett tartományoknak. Jelentőségük annak köszönhető, hogy a Nap ultraibolya és korpuszkuláris sugárzásának<sup>2</sup> valamint egyéb sugárzások (pl. kozmikus háttérsugárzás) hatására a semleges gázmolekulák ionizálódnak, ezáltal elektromos vezetőképessegre tesznek szert, így az elektromágneses hullámok ebbe a közegbe érkezve elhajlást szenvednek, ami bizonyos frekvenciatartományban az ionoszférától nagy távolságból szemlélve visszaverődésként (reflexióként) vizsgálható.

Az ionoszféra ionkoncentrációja a magasság, napszak, évszak, naptevékenységek függvényében időben és térben változó tulajdonságot mutat, azonban ezzel együtt vannak bizonyos – reflektálóképesség szempontjából - viszonylag karakterisztikusabb tulajdonságokat mutató tartományai.

---

<sup>1</sup> viszonylag stabil állandó hőmérsékletű átmeneti réteg a troposzféra és sztratoszféra között

<sup>2</sup> részecske sugárzás, napszél

Hullámviszaverő képesség alapján négy ilyen réteget különböztetünk meg, melyek:

- D-réteg (kb. 40-80 km): a Föld Nap által megvilágított oldalán alakul ki, mely így adott földrajzi ponton nappal érvényesül déli maximummal, majd éjszaka megszűnik. Hullámterjedési szempontból alapvetően elnyelő, csillapító tulajdonságokkal bír, elsősorban rövidhullámú sáv alatti (<3 MHz) tartományokban,
- E-réteg vagy Kenelly-Heaviside réteg (kb. 100-160 km): adott földrajzi ponton napfelkelte előtt keletkezik és részben napnyugta után is fennmarad, de lényegesen kisebb elektronkoncentráció mellett. Elegendően nagy elektronsűrűség esetén már képes a rövidhullámú tartomány alsó felébe tartozó hullámok visszatükrözésére,
- F-réteg vagy Appleton-réteg (180-400 km): legnagyobb vastagságú réteg, napnyugta után az elektronkoncentráció csökkenése lényegesen lassabb, mint az alacsonyabb rétegeknél és éjszaka is fennmarad. Minimumát napkeltekor éri el. A nappali intenzív besugárzás hatására az elektronsűrűség magassági maximum értékének két tartománya alakul ki, az alsó 20-300 km-es tartományban az  $F_1$ -réteg, míg a magasabb kb. 400 km tartományban az  $F_2$ -réteg. A rövidhullámú terjedés szempontjából az  $F_2$ -réteg jelentős reflektáló képességet képvisel.

A felületi hullámok rövidhullámú tartományú terjedését a földfelszín terep elemei valamint a talaj dielektromos állandója<sup>3</sup> jelentősen befolyásolja, ezáltal maximális hatótávolságuk 100-200 km, amely érték a sáv tartományon belül a frekvencia növelésével rohamosan csökken.

A földfelszínről kisugárzott térhullámok az ionoszféra reflexiós rétegeiről (megfelelő körülmények között) képesek visszaverődve jelentősen nagyobb, több ezer km-es távolságokat megtenni. A rétegek reflektáló képessége függ a frekvenciától és a beesési szögtől. Általánosan szabályként elmondható, hogy reflexió létrejöttéhez a frekvencia és a beesési szög növekedésével egyre nagyobb ionkoncentráció szükséges. Azt a maximális frekvenciaértéket, amely az ionoszféra adott pillanatnyi állapotában, adott beesési szög mellett még képes reflektálni felső üzemi frekvenciának<sup>4</sup> nevezzük. A D-réteg hasonlóan frekvenciafüggő csillapító hatása miatt az adott terjedési körülményekhez tartozik egy ún. alsó üzemi frekvencia<sup>5</sup> is, amely adott bemeneti jel-zaj viszony mellett a vevővel még vehető. A MUF és LUF közötti használható frekvencia ablak folyamatosan változik, értéke néhány MHz- től akár 20 MHz-ig is terjedhet. Tovább

---

<sup>3</sup> dielektromos állandó vagy relatív permittivitás: elektromosan nem vezető anyagok szigetelőképességére jellemző anyagi tulajdonság

<sup>4</sup> Maximum Usable Frequency - MUF

<sup>5</sup> Lowest Usable High Frequency- LUF

bonyolítja a terjedési képet, hogy teljesen dielektromos tulajdonságú talajnál a függőlegesen polarizált hullám a talajról nem verődik vissza, ha a beesési szög eléri az ún. Brewster-szöget. A nem teljesen dielektromos tulajdonságú talajnál a visszaverődési tényezőnek ennél az értéknél minimuma van (pszeudo-Brewster szög). A felület mentén párhuzamosan haladó hullám 180°-os fázistolást szenved, emiatt létezik egy olyan minimális kilövési (elevációs) szög érték (kb. 4-5°), amely alatt a sugárzás a teljes tartományban gyakorlatilag megszűnik.

Bizonyos körülmények között azonban a reflektált hullámok a földfelszínről továbbreflektálódva (többszörös visszaverődés), több ugrással, extrém távolságokat (8-12 ezer km) is képesek áthidalni.

A felületi hullámokkal adott pontból már nem-, a térhullámokkal a reflexiók feltételek (ugrások) miatt még nem elérhető földrajzi tartományokat ún. holtzónáknak nevezünk, amelyek kiterjedése a több száz km-es tartományokat is elérheti.

## 1.2 Rövidhullámú összeköttetések jellemzői

A rövidhullámú sáv előző pontban vázolt szofisztikált terjedési tulajdonságai (soktényezős időbeli-, térbeli- nap-, évszak-, frekvencia-, polarizáció-, napfolt- és naptevékenység függősége) a sáv tartományra jellemző sajátos összeköttetési csatornák kialakítását követeli meg, illetve teszi lehetővé. Az ionoszférikus terjedésnek köszönhetően, térben és időben folyamatosan változó közegben, időben rendkívül ingadozó vételi körülmények között, a térhullámokkal Föld nagyságrendű távolsági összeköttetések valósíthatók meg az alábbi jellemzőkkel:

- 24 órás összeköttetések megvalósításához több frekvencia használata szükséges
- műsorszórások folyamatos biztosítása ütemezett frekvenciaváltást igényel
- az összeköttetések létrehozásához frekvencia tervezés szükséges
- a sáv tartomány sűrű csatorna kiosztású, nagyszámú energia jelenlétével
- az összeköttetések külső zajkörnyezeti feltételei időben és térben folyamatosan változnak
- magas intermodulációs követelmények
- az adásformák tipikus sávszélessége néhány kHz-es tartományú
- néhány helyhez kötött és mobil szolgálat intelligens, kognitív (frekvencia adaptív) rendszereket használ (ALE)<sup>6</sup>
- a legtöbb modulációs sávszélesség meghaladja a korrelációs sávszélességet

---

<sup>6</sup> *Automatic Link Establishment*

A rövidhullámú sávban a Nemzetközi Rádiószabályzat és a Frekvenciák Nemzeti Felosztási Táblázata (FNFT) szerinti besorolásban a következő jelentősebb tipikus szolgálatok üzemelnek:

**Állandóhelyű:**

RH állandóhelyű

A3E (AM) és J3E (SSB) adásmódú CB berendezések

Távírányító, távmérő, távjelző és vagyonvédelmi berendezés

Állandóhelyű mozgó:

külgügyminisztérium, külképviselőtek céljaira, illetve. rendkívüli állapot, szükségállapot, veszélyhelyzet esetén pont-pont típusú összeköttetések adat, beszéd és képátvitelhez

**Állandóhelyű műsorszórás:**

RH rádió-műsorszórás,

Egyoldalsávú RH rádió-műsorszórás

Tengeri mozgó:

Dunai hajózás RH rádiókommunikációs rendszer

Rádiótelefon üzemű hajóállomások

Légi mozgó:

Levegő-föld (A/G) beszédátviteli és adatátviteli összeköttetés elsősorban nemzetközi és nemzeti polgári légiútvonalakon

**Amatőr:**

Rövidhullámú amatőrrádiózás

160 m-es amatőrsáv (1,81-2,0 MHz)

80 m-es amatőrsáv (3,5-3,8 MHz)

40 m-es amatőrsáv (7,0-7,1 MHz)

30 m-es amatőrsáv (10,1-10,15 MHz)

20 m-es amatőrsáv (14,0-14,35 MHz)

17 m-es amatőrsáv (18,068-18,168 MHz)

15 m-es amatőrsáv (21,0-21,45 MHz)

Műholdas rövidhullámú amatőrrádiózás

Fentiekén túlmenően, a sávban egyéb speciális felhasználások (nemzetközi vészfrekvenciák, speciális vivőfrekvenciák, hiteles frekvenciák és órajelek, ember által lakott űrjárművek kutatási és mentési frekvenciája, egyeztetett kutatási és mentési műveletek, kisteljesítményű eszközök /LPD-k/, ISM berendezések valamint kis hatótávolságú induktív eszközök /SRD-k/ is rendszeresítettek.

## **2. A nemzetbiztonsági célú rövidhullámú elektronikai adatgyűjtés magyarországi környezete**

A rövidhullámú stratégiai adatszerző rendszerek elektronikai védelmi lehetőségeinek vizsgálatához szükséges feltérképezni azokat a környezeti változókat, helyi adottságokat, és feltételeket (történelmi adottságok, törvényi környezet, szervezeti struktúra, nemzetközi szerződések földrajzi-geopolitikai adottságok), amelyek keretet adnak egy ilyen rendszer magyarországi működtetésére, illetve meghatározzák az adatgyűjtő rendszer jelenkori elektronikai védelmi lehetőségeit, szükségleteit.

### **2.1 Történelmi előzmények**

Ismereteink szerint a nemzeti alapokon működő katonai hírszerzés és elhárítás Magyarországon már a Habsburg monarchia felbomlását követően a monarchia hadseregének korábbi, hasonló rendeltetésű szervezetének felépítése és szabályai alapján jött létre.

Ennek keretein belül rádiófelderítő tevékenységet először 1918-ban végeztek. A hírszerzési célú tevékenység stratégiai, hadműveleti - majd később a II. világháború során - harcászati szinten folyt a Honvéd Vezérkar Hírszerző- és Elhárító VKF-2 Osztályán.

A II. világháború követően a hírszerzés és elhárítás a Honvédelmi Minisztérium csoportfőnökségek keretében folyt (VI-2. Osztály), majd 1953-tól a MNVK 2. Csoportfőnöksége volt felelős a katonai hírszerzésért.

Ezzel párhuzamosan 1947-től a BM Államrendőrség Államvédelmi Osztályának (ÁVO) megalakulásával, annak keretein belül létrejött egy polgári rádiófelderítő csoport a magyarországi rádióforgalom ellenőrzés személyi és technikai feltételeinek kidolgozására, amely tevékenység 1949-től az akkor létrejövő Államvédelmi Hatóság (ÁVH) operatív technikával foglalkozó II. Főosztályán indult növekedésnek.

Az 1955-ben Moszkvában megrendezett állambiztonsági értekezletet követően az elhárítás a Belügyminisztérium alárendeltségébe került, míg a katonai hírszerzés a Honvédelmi Minisztérium keretein belül folytatta tevékenységét egészen 1990-ig. Ennek megfelelően a magyarországi rövidhullámú rádiófelderítő-rádióelhárító tevékenység is két pilléren érte meg a rendszerváltást.

A demokratikus berendezkedéssel létrejött két polgári – a Nemzetbiztonsági Hivatal (NBH) és az Információs Hivatal (IH) - valamint két katonai – a Katonai Felderítő Hivatal (KFH) és Katonai Biztonsági Hivatal (KBH) - szolgálat szimmetrikussá formálta az elhárítás és hírszerzés polgári és katonai struktúráját.

Az 1996-ban hatályba lépett *a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény (Nbtv.)* ötödik titkosszolgálatként létrehozta az önálló Nemzetbiztonsági Szakszolgálatot (NBSZ), mint a titkos információgyűjtő eszközökkel valamint módszerekkel dolgozó, szolgáltató jellegű operatív-technikai kiszolgáló szakszolgálatot.

Magyarország 1999-es NATO csatlakozásával a rádiófelderítés tevékenysége, mint fogalom, új értelmezési keretrendszerben került elhelyezésre. Illeszkedve a közösségi rendszer *elektronikai hadviselés*<sup>7</sup> fogalomrendszerén belül elfoglalt helyére, az adatforrások (információforrások) NATO-felosztása szerint alapvetően a *rádióelektronikai felderítés*<sup>8</sup> vagy *elektronikai eszközökkel folytatott felderítés és rádiófelderítés*<sup>9</sup>, ezen belül a *rádiófelderítés*<sup>10</sup> vagy *kommunikációs felderítés* valamint a *rádiótechnikai felderítés*<sup>11</sup> vagy *elektronikai eszközök felderítése* fogalmi hármásában nyert értelmezést.

Az Nbtv. 2010. évi módosítását követően az NBH jogutódja az Alkotmányvédelmi Hivatal (AH) és NBSZ belügyminiszteri, míg az IH külügyminiszteri irányítás alá került. További változás történt 2012-ben, amikor is a KFH-t és KBH-t egy közös szolgálatba vonták össze Katonai Nemzetbiztonsági Szolgálat- (KNBSZ) néven, továbbá az IH-t KÜM-ből Miniszterelnökség alá rendelték. A változtatások ellenére is a magyar titkosszolgálati rádiófelderítő tevékenység (katonai hírszerzés,<sup>12</sup> polgári technikai hírszerzés<sup>13</sup>, valamint hírközlő hálózatok kommunikáció ellenőrzése<sup>14</sup>) továbbra is megtartotta több pilléres struktúráját.

## 2.2 Titkos információgyűjtés és titkos adatszerzés jogszabályi környezete Magyarországon

A titkos információgyűjtés jelenlegi kereteit – a nemzetbiztonsági szolgálatok vonatkozásában az Nbtv. szabályozza, amely az Információs Hivatalt, az Alkotmányvédelmi Hivatalt, a Katonai Nemzetbiztonsági Szolgálatot valamint a Nem-

---

<sup>7</sup> *Electronic Warfare - EW*

<sup>8</sup> *Signal Intelligence - SIGINT*

<sup>9</sup> Kobilka István: *Nemzetbiztonsági alapismeretek, Nemzeti Közszolgálati Egyetem, Budapest, 2013. p.127.]*-ben a szerző a „rádiófelderítés” kifejezést a COMINT mellett a SIGINT vonatkozásában is értelmezi

<sup>10</sup> *Communication Intelligence - COMINT*

<sup>11</sup> *Electronic Intelligence - ELINT*

<sup>12</sup> *Katonai Nemzetbiztonsági Hivatal honlapja, Forrás:*

<http://www.honvedelem.hu/szervezet/knbsz> (Letöltve:2015.05.24.)

<sup>13</sup> *Információs Hivatal honlapja, Forrás: [http://www.ih.gov.hu/hivatal\\_hirszerzes.shtml](http://www.ih.gov.hu/hivatal_hirszerzes.shtml)* (Letöltve:2015.05.24.)

<sup>14</sup> *Nemzetbiztonsági Szakszolgálat honlapja. Forrás: <http://www.nbsz.gov.hu/?mid=28>* (Letöltve:2015.05.24.)



zetbiztonsági Szakszolgálatot (együtt: nemzetbiztonsági szolgálatok) nevesíti meg a tevékenység folytatására jogosult szervezetekként. A törvény értelmében a nemzetbiztonsági szolgálatok feladataik teljesítése érdekében titkos információgyűjtést folytathatnak, melyhez speciális eszközöket és módszereket alkalmazhatnak. Ezen szolgálatok főbb feladatai a következők:

**A Katonai Nemzetbiztonsági Szolgálat:**

- hírszerző, elhárító, védelmi és ellenőrzési feladatok elvégzésével, a nyílt és a titkos információgyűjtés eszközzel működési területén elősegíti Magyarország nemzetbiztonsági érdekeinek érvényesítését, ezáltal közreműködik az ország függetlenségének és törvényes rendjének védelmében;
- megszerzi, elemzi és továbbítja a kormányzati döntésekhez szükséges, a külföldi eredetű, a biztonságpolitika katonai elemét érintő katonapolitikai, hadiipari és katonai információkat;
- biztosítja a Honvéd Vezérkar hadászati-hadműveleti tervező munkájához szükséges információkat, működteti Magyarország katonai felderítő rendszerét.

**Az Információs Hivatal:**

- megszerzi, elemzi, értékeli és továbbítja a kormányzati döntésekhez szükséges, a külföldre vonatkozó, illetőleg külföldi eredetű, a nemzetbiztonsága érdekében hasznosítható információkat.

**Az Alkotmányvédelmi Hivatal:**

- felderíti és elhárítja a Magyarország függetlenségét, politikai, gazdasági, védelmi vagy más fontos érdekét sértő vagy veszélyeztető külföldi titkosszolgálati és Magyarország törvényes rendjének törvénytelen eszközökkel történő megváltoztatására vagy megzavarására irányuló leplezett törekvéseket és tevékenységet.

**A Nemzetbiztonsági Szakszolgálat:**

- a jogszabályok keretei között a titkos információgyűjtés, illetve a titkos adatszerzés eszközeivel és módszereivel – írásbeli megkeresésre – szolgáltatást végez a titkos információgyűjtésre, illetve a titkos adatszerzésre feljogosított szervek titkos információgyűjtő, valamint titkos adatszerző tevékenységéhez;

- a törvény által titkos információgyűjtésre, valamint titkos adatszerzésre feljogosított szervek igényei alapján biztosítja az e tevékenységhez szükséges különleges technikai eszközöket és anyagokat;
- technikai felderítés keretében hírközlő hálózaton folytatott kommunikáció tartalmának megismerését és rögzítését végzi;
- bizonyos eseteket kivéve, a titkos információgyűjtés eszközeit és módszereit saját kezdeményezésre nem alkalmazhatja.

A rádiófelderítés/rádióellenőrzés - mint titkos információgyűjtő és titkos adatszerző tevékenység – megvalósításához a nemzetbiztonsági szolgálatok:

- a nemzetbiztonsági jelleg leplezésével információt gyűjthetnek;
- az információgyűjtést elősegítő információs rendszereket hozhatnak létre és alkalmazhatnak;
- hírközlési rendszerekből és egyéb adattároló eszközökből információkat gyűjthetnek;
- elektronikus hírközlési szolgáltatás útján továbbított kommunikáció tartalmát megismerhetik, az észlelteket technikai eszközzel rögzíthetik;
- számítástechnikai eszköz vagy rendszer útján továbbított, vagy azon tárolt adatokat megismerhetik és azok tartalmát technikai eszközzel rögzíthetik, továbbá felhasználhatják.

Fontos megjegyezni, hogy az Nbtv. alapján a polgári és a katonai titkosszolgálatok a fentiek szerinti „alanyi” joggal élhetnek a titkos információgyűjtés lehetőségével.

Emellett az egyéb ágazati törvények alapján feljogosított további öt szervezet- a Rendőrség<sup>15</sup>, a Nemzeti Védelmi Szolgálat<sup>16</sup>, a Terrorrelhárítási Központ<sup>17</sup>, a Nemzeti Adó- és Vámhivatal<sup>18</sup> valamint az Ügyészség<sup>19</sup> - tevékenységi körükhöz kapcsolódó nyomozati cselekmények körében- szintén élhetnek a titkos információgyűjtés és titkos adatszerzés eszközével, azonban ezek az esetek a stratégiai jellegű rövidhullámú felderítés és adatszerzés vonatkozásában – jellegüknél fogva- nem képeznek súlyponti szerepet.

Az NBSZ szolgáltatásai a másik három nemzetbiztonsági szolgálat részére „teljeskörűen” hozzáférhetőek és elérhetőek. Tekintettel arra, hogy bár az NBSZ koncentrált titkos információgyűjtő és titkos adatszerző technikai eszköz rend-

---

<sup>15</sup> a Rendőrségről szóló 1994. évi XXIV. törvény alapján

<sup>16</sup> a Rendőrségről szóló 1994. évi XXIV. törvény alapján

<sup>17</sup> a Rendőrségről szóló 1994. évi XXIV. törvény alapján

<sup>18</sup> a Nemzeti Adó- és Vámhivatalról szóló 2010. évi CXXII. törvény alapján

<sup>19</sup> az ügyészségről szóló 2011. évi CLXIII. törvény alapján

szer kapacitással bír, a nemzetbiztonsági szolgálatok saját eszközeiket is – a törvényi keretek korlátai között - felhasznál(hat)ják feladataik végrehajtása során.

Magyarországon a nemzetbiztonsági szolgálatok közül az Információs Hivatal és a Nemzetbiztonsági Szakszolgálat rádiófelderítést, a Katonai Nemzetbiztonsági Szolgálat pedig rádióelektronikai felderítést hajt végre törvényi felhatalmazás alapján.

A nemzetbiztonsági célú, rövidhullámú sáv tartományú, magyarországi rádiófelderítés szempontjából az 1.1. fejezetben ismertetett jellemzőkkel bíró hullámterjedés elsősorban a nagy távolságban található (külföldi) rövidhullámú rádióforrások jeleinek vételét, rádiólokációs helymeghatározását és a sáv tartományban üzemelő pont-pont vagy pont- több pont jellegű kommunikációs összeköttetési rendszerek felderítését és rádióellenőrzését teszi lehetővé, illetve ellenőrzésének ad keretet.

### **3. Stratégiai rövidhullámú COMINT rendszerek elektronikai védelmi lehetőségei**

#### **3.1. Az elektronikai védelemről általában**

A rövidhullámú stratégiai információgyűjtő és adatszerző rendszerek elektronikai védelmi képességének vizsgálatához szükséges áttekinteni az elektronikai védelem fogalmkörét, a harcászati elektronikai konfliktusban elfoglalt szerepét és területeit.

Az elektronikai védelem, mint az elektronikai hadviselés szerves eleme, alapvető rendeltetése az elektromágneses spektrum saját csapatok részéről történő hatékony használatának biztosítása. Mindezt az ellenséges fél elektronikai támogatása és elektronikai ellentevékenysége ellenében szükséges véghezvinnie. Hasonlóképpen, a saját rendszerek, csapatok nem szándékos elektronikai zavaró tevékenységének kiküszöbölése, illetve leküzdése is e védelmi tevékenység feladatát képezi. Olyan aktív és passzív műveletek, módszerek vagy tevékenységi előírások, rendszabályok alkalmazását jelenti, amelyek célja az ellenség felderítő és elektronikai ellentevékenységi hatékonyságának csökkentése, ellehetetlenítése.

A passzív elektronikai védelem azon intézkedéseket tartalmazza, amelyek az ellenség által nem detektálhatóak, így azok főleg taktikai, módszertani és eljárásrendi megfontolásokat tartalmaznak, beleértve a védelmi pajzsok alkalmazását.

Az aktív elektronikai védelem érzékelhető az ellenség által és a védelmet valamilyen speciális berendezés vagy egy adott elektronikai berendezés speciális működtetési módjának alkalmazásával biztosítja.

Az elektronikai védelmi tevékenységek három fő területben csoportosíthatók. Első csoportba azok az intézkedések, aktív tevékenységek tartoznak, amelyek a saját eszközök, rendszerek elektronikai felderítését célzottan megakadályozzák.

lyozni. Az elektronikai felderítő tevékenységen olyan információszerezést megcélzó tevékenységet értünk, amely az infokommunikációs rendszerekben tárolt vagy azokban továbbított adatokhoz való hozzáférést, azok felhasználását célozza meg, másrésztől a hatékony támadás elősegítéséhez szükséges célinformációk megszerzését foglalja magában. Az elektronikai felderítésnek számos területe létezik, idetartoznak a különböző sáv tartományokra kiterjedő műszeres felderítés<sup>20</sup> különböző szakágai, a képi felderítés<sup>21</sup> valamint a rádióelektronikai felderítés<sup>22</sup>. A felderítés elleni védelem fogalmán belül megkülönböztethetők az elektronikai álcázást biztosító tevékenységek valamint az elektromágneses kisugárzások csökkentését, megakadályozását célzó tevékenységek.

Másik nagy területe az elektronikai védelemnek az elektronikai ellentevékenység (zavarás) elleni védelem, amely körébe a szándékos és nem szándékos zavarok elleni tevékenységek valamint az elektronikai pusztítás elleni védelmet célzó tevékenységek tartoznak.

Harmadik csoportba sorolható az elektronikai ellenőrzés témaköre. Ide olyan technikai és szervezési rendszabályok összessége tartozik, amely feladata a saját eszközenszer elektronikai védelmi állapotának folyamatos vizsgálata, a védelmi intézkedések, rendszabályok betartásának és hatékonyságának nyomon követése, a saját rendszer ellenség szempontjából történő vizsgálata, tesztelése.

A három nagy terület a módszer, jelleg, tartomány alapján számos részterületekre bontható<sup>23</sup>, melyek alapján lehetséges egy adott objektum/rendszer elektronikai védelmi lehetőségének vizsgálata.

### **3.2 Rövidhullámú stratégiai adatszerző rendszerek elektronikai védelmi áruó jegyei**

Az elektronikai védelmen belül az elektronikai felderítés elleni tevékenység hatékony tervezéséhez szükséges megvizsgálni a védendő rendszereink azon tulajdonságait (áruó jegyeit), amelyek az ellenség felderítő tevékenysége szempontjából jelentőséggel bírnak. Az áruó jegyek ismeretében kidolgozható a védelmi eljárás vagy az adott objektumra vonatkozó felderítés elleni rendszabályok összessége.

Stratégiai adatszerző rendszerek esetében áruó jegyeknek a rendszer elemeinek, technikai eszközeinek működésére jellemző olyan sajátosságait, jellegzetességeit értjük, amelyek az ellenség számára lehetővé teszik, hogy elemzésükkel a rendszer elemei felderíthetővé váljanak. A rendszer elemeinek mozgására, összetartozására, csoportosítására utaló jellemzőket hadműveleti-harcászati áruó jelekként azonosítjuk, míg az eszközenszer védettségére, zavarállóságára, ren-

---

<sup>20</sup> *Measurement and signature intelligence - MASINT*

<sup>21</sup> *Imagery Intelligence - IMINT*

<sup>22</sup> *Signal Intelligence - SIGINT*

<sup>23</sup> *lásd 4.2, 4.3. és 4.4 fejezetek*

deltetésére, típusára, hovatartozására vonatkozó jegyeket technikai jegyekként tartjuk nyilván:

Adatszerző rendszerek hadműveleti-harcászati áruló jelek:

- épületek/objektumok mennyisége;
- épületek/objektumok földrajzi elhelyezkedése;
- épületek/objektumok nagysága;
- épületek/objektumok külső megjelenési formája;
- épületek/objektumok egymáshoz viszonyított elhelyezkedése;
- épületek/objektumok körleteinek mérete.

Adatszerző rendszerek technikai jellegű áruló jelek:

- a kibocsátott és visszavert jelek
  - térbeli alakja (irányítottság, méretek);
  - belső struktúrája (vivőfrekvencia, modulációs mód, modulációs tartalom, moduláció minősége);
  - a sugárzó eszközök;
  - üzemi frekvenciája;
  - frekvencia stabilitása;
  - frekvencia váltogatása (zavarás hatására);
  - harmonikus sugárzása;
  - sávon kívüli sugárzása;
  - vivőelnyomása;
- az antenna berendezések
  - külső geometriai méretei (alak, felépítés);
  - iránykarakterisztikák;
  - a tér figyelési módja (forgatás, lengetés);
- az információ továbbítás
  - módja (adásmód, üzemmód);
  - sáv szélesség jellemzők;
  - egyidejű csatornák száma;
  - időosztásos csatornák képzése.

Az áruló jelek ismeretében teljes kép alkotható a védendő rendszerről és kidolgozhatók azok az eljárások, rendszabályok, amelyek megakadályozzák vagy csökkentik az ellenség vagy saját eszközeink rendszerünk zavartatására irányuló képességét.

A rövidhullámú adatszerzés szempontjából fontos megemlíteni, hogy a nemzetbiztonsági célú tevékenység passzív rádiófelderítő eszközökkel valósul meg. A szenzorok és központ közötti – a megszerzett adatok továbbítására vagy az adatszerzés irányítására szolgáló – összeköttetések – pl. rádiós megvalósítás esetén tartalmazhatnak aktív elemeket. Passzív rendszerelemek esetén a fenti felsoro-

lásból a kibocsátott és visszavert jelek valamint a sugárzó eszközök jellemzői, mint áruló jelek nem rendelkeznek relevanciával.

### **3.3. Stratégiai rövidhullámú ellenőrző központok elektronikai védelmi lehetőségei**

Egy stratégiai COMINT központ nagyon hasonlatos vizsgálati feltételeket mutat egy egyéb, hétköznapibb funkcionalitású felhasználással, mint például, vállalati számítógép központ vagy általános informatikai rendszerek központi elemeinek elhelyezése.

Az elektronikai védelmi módszerek jelentős köre a stratégiai COMINT központ általános (irodai) jellegű környezetben (épület, akár lakott, urbánus terület) történő elhelyezhetőség miatt békeidőben nem értelmezhető a központ esetében. A jelentősebbeket említve nem értelmezhetők a vizsgálatban a hidroakusztikai-, akusztikai felderítés elleni rejtés módszerei, a szándékos zavarok elleni védelem zavar hatékonyság csökkentő azon eljárásai, amelyek alapvetően duplex összeköttetések (elsősorban híradó) védelmi eszközeiként hatékonyak. Specialitásuk miatt nem értelmezhetőek továbbá a rádiólokációs- és rádiórelé rendszereknél alkalmazható zavarvédelmi eljárások és szervezési- illetve technikai módszerek sem. Hasonlóképpen kívül esnek a vizsgálhatóság körén azok az eljárások, amelyek valamilyen módon az eszközrendszer elemeinek térben és/vagy időben történő elkülönítésével operálnak, illetve amelyek az ellenség azonnali megsemmisítésén alapszanak (nemzetbiztonsági rendszer, békeidejű használati feltételek).

A központ teljesen passzív (csak jelfeldolgozás folyik, nincs kisugárzott kommunikációja) jellege valamint általános épületben elhelyezhetősége (nincs külső, felismerhető azonosíthatósági jegye, épület nagyságrendű helyigény) értelmezhetőek, azonban nem vagy csak nagyon korlátozottan alkalmazhatóak az elektronikai rejtés aktív elemei, az optikai rejtés álcahalós- vagy fényforrás manipulációs módszerei, a rádiólokációs felderítés elleni rejtés valamint a rádió- és rádiótechnikai felderítés elleni tevékenység egyes aktív elemei. Általánosságban kijelenthető, hogy stratégiai központok esetében még békeidőn kívül sem alkalmazhatóak az objektum különböző hullámtartományú (látható fény, lézer, infravörös) rejtését csak korlátozott ideig biztosítani képes füst- és köd generáló eszközök. Ez utóbbiak elsősorban kisebb objektumok, tárgyak, mobil eszközök harcászati szinten, konfliktus közepette történő védelme során lehetnek hatékonyak. Külön kockázati tényezőként említhető az elektromágneses impulzusok elleni védelem korlátozottsága, mivel az impulzus nagyságára vonatkozó ismeretek hiánya nem teszi lehetővé a szükséges védelmi módszer és eszköz optimális meghatározását. A központ elhelyezését biztosító objektum (épület) vonatkozásában – technológiai szempontból - lehetőség van elektromágneses árnyékolás (pl. falakon fémadalékos bevonatok vagy a központ teljeskörű, Faraday-kalicka

elvű, fémlémezzel történő burkolása) alkalmazására. Ezek a módszerek információbiztonsági kisugárzási (TEMPEST)<sup>24</sup> szempontból az elektromágneses hullámok vonatkozásában az előírt - mintegy 100 dB értékű- csillapítást képesek biztosítani, azonban az elektromágneses impulzusok elleni védelmi képességük nem ismert.

A központ objektumának védelmére hatékonyan alkalmazhatók az elektronikai álcázás területén a külső megjelenési jegyek elkerülése, az akusztikai álcázás, valamint az elektromágneses árnyékolás eszközrendszere. Urbánus környezetben történő elhelyezéssel a műholdas felderítést kivéve jól alkalmazhatók a környezeti elemek, objektumok védő-, árnyékoló tulajdonságán alapuló rejtési lehetőségek, míg a műholdas felderítés ellen biztonságos védelmet egy más kockázati megközelítésű, földfelszín alatti központ kialakítás biztosíthat. A rendszabály alapú megközelítések jelentős mértékben alkalmazhatóak a szándékos és nem szándékos kisugárzások elleni védelem területén is. A zavar eredetének és hovatartozásának meghatározásával, a vevőrendszer lehetőségekhez képesti finomhangolásával, elektromágneses kompatibilitási szabvány előírásoknak megfelelő vagy azokon esetleg akár túlmutató jellemzőkkel rendelkező eszközök fejlesztésével és alkalmazásával biztosíthatók a zavarvédelem feltételei. Elektronikai tisztítás elleni védelem területén a stratégiai központ esetében szintén széles körben alkalmazhatók mindazon technológiai eszközök, alkatrészek (pl.: szikraközök, árnyékoló anyagok, túlfeszültség levezetők, nemlineáris feszültségvédelmi elemek, stb.), amelyek képesek megakadályozni a nagy energiájú rádiófrekvenciás források sugárzott jeleinek objektumba való bejutását.

### **3.4. Stacioner telepítésű rövidhullámú ellenőrző szenzorok elektronikai védelmi lehetőségei**

A szenzorok feladata a sáv tartományban található adások, forgalmazások vétele, a sugárforrás helyzetének iránymérése, valamint a vett jelek további feldolgozásra történő továbbítása valamilyen csatornán (rádiós, vezetékes, optikai) a központhoz. A vett jelek az antennákról vagy diszkrét vevőkre kerülnek vagy teljessávú digitalizálást követően jutnak a feldolgozó központba. A szenzorok emiatt alapvetően különböző polarizációjú szélessávú- vagy keskenysávú vevőantennából, iránymérő antenná(k)ból vagy antennarendszerekből állnak.

A rövidhullámú stacioner telepítésű szenzorok sajátossága, hogy a térszelekтивitás biztosítása céljából a gyakorlatban több típusú és elrendezésű antennából álló antennamezővel rendelkeznek. A sáv tartomány 10-től 100 méterig terjedő hullámhosszából adódóan az antennák fizikai mérete általában jelentős, egyes esetekben a több tíz méteres terjedelmet is eléri. Méretükből adódóan

---

<sup>24</sup> Az amerikai Nemzeti Biztonsági Ügynökség (NSA - National Security Agency) által specifikált, az információ szivárgását gátló normarendszer

jelentős méretű, (általában fém) tartóoszlop és feszítő rendszer kialakítását igénylik. Az antennák elkülönítésének figyelembevételével kialakított antennamező területe a néhány négyzetkilométert is elérheti. Az antennamező elemeitől a rádiófrekvenciás jelek (a talpponti digitalizálást kivéve) kábeleken jutnak be a konténerben vagy kisebb épületben elhelyezett vevőkhöz, melyek hangolása, programozása távvezérelt módon az akár több száz kilométerre található stacioner felderítő központból történik.

Ennek megfelelően elektronikai védelmi szempontból a szenzornak négy funkcionális eleme különböztethető meg, melyek:

- vételi antennák, iránymérő antennák a tartószerkezettel;
- antennák és konténer(épület) közötti összeköttetés (rádiófrekvenciás kábel, optikai kábel, elektromos tápkábel) ;
- konténer(épület) az elhelyezett vételi eszközökkel;
- összeköttetési csatorna a szenzor konténer(épület) és stacioner felderítő központ között (rádiós, vezetékes, optikai) .

A rövidhullámú stacioner szenzorok földrajzi elhelyezése rádióvédelmi szempontból alacsony háttérzajú, ipari létesítményektől mentes, általában természeti környezetben lehetséges, ezáltal városi-, nagyvárosi telepítésük nem ideális. A vételi viszonyokat pozitívan befolyásolja az antenna talajszerkezete, nedvességtartalma, ezért gyakori a rövidhullámú szenzorok lápos, ingoványos, esetleg mocsaras területeken történő kialakítása.

A stacioner adatszerző központhoz képest a jelentős számosságú, méretű és kiterjedtségű antennarendszerrel és vevőeszközzel rendelkező stacioner szenzorok elektronikai védelmi szempontból érzékenyebb képet mutatnak.

A nem értelmezhető védelmi módok nagyrészt hasonlóságot mutatnak a stacioner adatszerző központ jellemzőivel. Ugyanakkor, kiemelhető azonban néhány elem, amelyek a szenzoroknál értelmet nyernek, illetve valamilyen mértékben alkalmazhatók. Ilyenek például a elektromágneses árnyékolás alkalmazása, ami zavarutáni szempontból szükséges pl. a konténer(épület) esetében, azonban az antennák, mint elektromágneses jelátalakító eszközök esetében semmilyen formában nem alkalmazható illetve funkcionalitásában gátolná az antennák működését. Míg a központoknál nem értelmezhető az ellenség által zavarással lefogott elektronikai eszközök helyettesítése, addig a „vadonban”, nagy területen telepített stacioner szenzor esetében az elektronikai eszközök széttelepítése bizonyos korlátok között értelmet nyerhet. Tekintettel, hogy a szenzor rendelkezik valamilyen szintű vételi eszközzel, ezeknél – ha nem is rádiólokációs berendezéseknél használt értelemben – értelmezhető és elméletileg alkalmazhatók a vevő eszköz minőségi mutatóira vonatkozó javítási módszerek (pl.: szelektivitás, dinamikataromány, antenna oldalnyaláb jellemzőinek javítása). Hasonlóképpen, a nem szándékos zavarok védelmi lehetőségeként használhatóvá válnak az elektronikai eszközök üzemi szektorainak kisugárzási és vételi



viszonyok alapján történő elosztása, csoportosítása is. Ez utóbbi az elektronikai ellenőrzés területén, az előírások betartásának területén, valamint a mért EM jellemzők műszaki normákkal történő összehasonlítása esetében is különbözőséget mutat az adatszervező központokhoz képest.

A nagyméretű vételi elemek (antennák, tartószerkezetek) jelenléte miatt, elektronikai rejtés tekintetében - mint passzív módszer - jelentőséghez jut az eszközök áruló jeleinek megszüntetése és rádiólokátor zavarása, azonban a méretek miatt esetenként csak korlátozott mértékben kivitelezhetők és hatékonyságuk is kérdőjeles. A kiterjedt antenna méretek miatt az optikai rejtés területén is nagyobb kihívásokkal szembesülünk és a terep rejtő tulajdonságai is kevésbé használhatók ki.

A szenzorok esetében kulcsponthoz tartozik a központtal magvalósított összeköttetési csatorna fajtája. Rádióösszeköttetés esetén aktív elem lép a képbe, ami felderíthetőség területén emeli a kockázati tényezőt és kiszélesíti a szükséges elektronikai védelmi módszerek körét. Minden tényezőt figyelembe véve a talpponti digitalizálás és optikai kábeles összeköttetések alkalmazása nagymértékben növeli a felderítő rendszer zavarvédeltségét.

### **3.5. Mobil telepítésű rövidhullámú ellenőrző szenzorok elektronikai védelmi lehetőségei**

A mobil telepítésű szenzorok feladatai azonosak a stacioner kivitelű állomásokéval, azonban alkalmazási módjuk, eszközrendszerük eltér attól. Legfontosabb sajátosságuk, hogy önjáróak, gyorsan telepíthetőek, elsőrendű alkalmazási sajátosságuk a mozgékonyosságuk. Ebből adódóan valamilyen terepjáró képességű hordozó jármű felépítménye biztosít helyet a vevő eszközöknek.

Az antennák a felépítményen fixen vagy a telepített gépjármű közelében önálló telepítéssel kerülnek elhelyezésre. Az egység saját tápellátással kell rendelkezzen, ami a gépjármű saját generátoráról vagy az az mellett működtetett vontatható áramforrásról üzemel.

A mobilan telepíthető antennák mérete jelentősen kisebb a stacioner állomáshoz képest. Eltérően a stacioner állomástól a mobil állomások nem rendelkeznek kiterjedt antennaparkkal, az egyszerre üzemeltetett iránymérő vagy vételi antennák száma a néhány darabot éri el. A korlátozott, de célzott felhasználás sajátossága, hogy alkalmazásában, kivitelében, méretében, felhasználásának jellegében, felderítési célpontként nagy hasonlóságot mutat az egyéb harcászati eszközökkel (harckocsi, szállítójármű, stb.). Ebből a tulajdonságaiból adódóan az elektronikai védelmi aspektusai is jelentősen elmozdulnak a harctéri mobil szárazföldi egységek jegyeinek irányába.

Kritikus eleme a szenzornak, hogy mobilitásából adódóan összeköttetése a stacioner központtal – egyedi eseteket leszámítva - kizárólag rádiós úton valósul meg.

Az elektronikai álcázás szükségességével párhuzamosan a mobil szenzor esetében megjelennek a különböző hullámtartományokban (optikai, lézer, infravörös) alkalmazható terep, napszak, optikai forma kihasználását alkalmazó álcázási lehetőségek és előtérbe kerülhetnek a passzív elektronikai rejtés elemei, mint a lokátor zavarás, elektrooptikai felderítés elleni álcázás és akusztikai álcázás szükségessége is. A gépjármű felépítmény anyagi tulajdonságai szükségessé teszik a mágneses mérésen alapuló felderítés elleni rejtés és a rádiólokációs felderítés elleni rejtés módszereinek alkalmazását. A stacioner szenzorhoz képest jelentős különbség mutatkozik a szándékos és nem szándékos zavarok elleni védelem alkalmazásában. A füst- és ködkibocsátó eszköz alkalmazása békeidőben nem rendelkezik relevanciával, azonban a mobil eszközök esetében, konfliktus időszakában kiemelt jelentőséggel bírhatnak.

Mobil állomás esetében a zavarvédelem érdekében az átjátszó állomás, az antenna helyzetének megváltoztatása, esetleges tartalék mobil egység alkalmazása is lehetőség. A központi egységgel való kapcsolattartásban helye és szerepe is lehet olyan, bonyolultabb modulációs módok alkalmazásának, melyek az információt továbbító elektronikai eszközök manőverező képességének kihasználásán alapulnak. Az elektromágneses kompatibilitás (EMC) biztosításában - tartalék egység rendelkezésre állása esetén - alkalmas módszer lehet az elektronikai eszközök széttelepítésének alkalmazása is.

## Összegzés

A nemzetbiztonsági célú rövidhullámú stratégiai rádiófelderítés elektronikai védelmi lehetőségeinek vizsgálatához bemutatásra kerültek a rövidhullámú sávú rádióellenőrző tevékenység sajátosságai.

A nemzetbiztonsági célú rádiófelderítés magyarországi szervezeti evolúciójának eredményeként a SIGINT/COMINT tevékenység ma egy olyan szervezeti keretrendszerben működik, amelyben a komplex stratégiai adatgyűjtés nem, csak az egyes szervezetek (IH, KNBSZ, NBSZ) törvényi feladatkörébe illeszkedő rádiófelderítő és rádiótechnikai felderítő tevékenységek vannak jelen.

A rövidhullámú stratégiai adatszerző központ esetében a mai technológiai és infrastrukturális jellemzők (informatikai alapú jelfeldolgozás, tényleges rádióvédteli eszköz nem funkcionál a központban, elhelyezése gyakorlatilag „bárhol”, irodaépületben is lehet sajátos külső jegyek nélkül, illetve a helyhez kötöttség) az elektronikai védelmi aspektusokat jelentősen leszűkítik.

A stacioner szenzorok, bár szintén helyhez kötött kivitelezésűek, de telepítésük a központtal ellentétben kifejezetten nem urbanus környezetben ideális. A szenzor telepítési környezete, kiterjedt méretű és terjedelmű vevő és iránymérő antennarendszere, valamint tényleges rádióvétel jelenléte ez esetben is sajátos elektronikai védelmi lehetőségeket enged meg, illetve tesz szükségessé.

A mobil szenzorok méretükben, kivitelükben, alkalmazásuk jellegében elektronikai védelmi szempontból nagyon hasonlatos kezelést igényelnek az egyéb harcászati jellegű csapategységekkel.

Fontos megjegyezni, hogy míg a stratégiai központ önmagában alkalmazásakor rendelkezésre állnak hatékony álcázási, rejtési lehetőségek, a helyzet nagymértékben megváltozik, amennyiben a feldolgozó központhoz – annak közvetlen közelében - rövidhullámú vételi és iránymérő antennák, kiterjedtebb antenna rendszerek csatlakoznak.

Összességében megállapítható, hogy a stratégiai felderítő rendszer elemeinek tematikus elektronikai védelmi vizsgálatával megállapíthatóvá váltak az egyes elemeknél alkalmazható, vagy kevésbé hatékony védelmi intézkedések köre.

A vizsgálat eredményeként létrejött táblázatos áttekintés lehetőséget biztosít egy adott létező vagy még tervezés alatt álló rövidhullámú stratégiai adatszerező rendszer elektronikai védelmi lehetőségeinek vizsgálatára, illetve további kutatás alapján egy elektronikai védelmi követelményrendszer megalkotására.

#### Felhasznált Irodalom:

- A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény.
- A polgári célra használható frekvenciasávok felhasználási szabályainak megállapításáról szóló 2/2013. (I. 7.) NMHH rendelet.
- Balajti I. – Vass S.: Elektronikai védelem. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, J-1435. 2000. p. 9
- Dobák Imre: A nemzetbiztonság általános elmélete, Nemzeti Közszolgálati Egyetem, 2014. p.252.
- Frater M. – Ryan M.: Communications Electronic Warfare and the Digitised Battlefield, 2001. [http://army.gov.au/Our-future/LWSC/Our-publications/Working-Papers/~media/Files/Our%20future/LWSC%20Publications/WP/pdfs/wp116-Comms%20EW%20and%20Digitised%20Battlefield\\_Michael%20Frater\\_Michael%20Ryan.pdf](http://army.gov.au/Our-future/LWSC/Our-publications/Working-Papers/~/media/Files/Our%20future/LWSC%20Publications/WP/pdfs/wp116-Comms%20EW%20and%20Digitised%20Battlefield_Michael%20Frater_Michael%20Ryan.pdf) (Letöltve: 2015.05.24)
- Haig Zsolt: Információ társadalom biztonság, NKE Szolgáltató Kft., p.143. ISBN 978-615-5527-08-1
- Haig Zsolt-Kovács László-Ványa László-Vass Sándor: Elektronikai hadviselés, Nemzeti Közszolgálati Egyetem, Budapest, 2014. ISBN 978-615-5305-87-0
- Haig Zsolt-Várhegyi István: A cybertér és a cyberhadviselés értelmezése, Hadtudomány, 2008. elektronikus lapszám [http://www.zmne.hu/kulso/mhht/hadtudomany/2008\\_e\\_2.pdf](http://www.zmne.hu/kulso/mhht/hadtudomany/2008_e_2.pdf) (Letöltve: 2015.05.24.)

- Kobilka István: Nemzetbiztonsági alapismeretek, Nemzeti Közsolgálati Egyetem, Budapest, 2013. p.127. ISBN 978-615-5344-32-9
- Magyar Honvédség Összhaderőnemi elektronikai hadviselés doktrína. Honvédelmi Minisztérium, Honvéd Vezérkar, Felderítő Csoportfőnökség, Budapest, 2004.
- Molnár Béla, Turi-Kovács Attila: Rádió hullámterjedés és hálózattervezés, Közlekedés- és
- Nemzetbiztonsági Szakszolgálat honlapja  
<http://www.nbsz.gov.hu/?mid=28>
- Postaügyi Minisztérium, Budapest, 1969.
- Rothammel Karl: Antenna könyv, Műszaki Könyvkiadó, Budapest, 1977.