*Balajti István**

Korszerű elektronikai harceszközök hatása a rádiólokátor rendszerekre

A tüzérség trónfosztása

Egy Napóleonnak tulajdonított mondás szerint: „A tüzérség a csataterek királynője”. A haditechnika fejlődésével a megvívott csaták sikeres kimenetele tekintetében a tüzérség szerepe jelentősen átalakult és egyre gyakrabban merült fel a kérdés, hogy más haderőnemek és fegyvernemek pl. a légierő, a páncélozott gyalogság vagy a napjainkban népszerű kiberhadviselés átveszi, vagy már át is vette ezt a szerepet. A szerző, nem vitatva a különböző fegyvernemek fontosságát és hatóerejük növekedésében rejlő előnyöket, a siker döntő elemét az együttműködésük szinkronizálásában és pontos valós idejű összehangolásában látja. *„A rádióelektronika terjedésével a REH*[1] *feladata lényegesen megnőtt, tevékenysége kiterjedt a kézifegyverektől a stratégiai atomeszközökig (űrfegyverekig), a katonáktól a hadműveleti-harcászati magasabb egységekig. Aktív vagy passzív eszközeivel és rendszabályival átfogja a hadsereg teljes egészét. Ezért a REH megítélésében új szemléletet és gyakorlatot kell követni.”* [1]

A második világháború idején még elegendő volt, ha a fegyvernemi parancsnokok az „egyeztessük óráinkat” felszólítással zárták a hadművelet megkezdésének eligazítását. Napjainkban a sikerhez már a katonai tevékenységek *mikro-* (10^{-6}), és/vagy *nano-* (10^{-9}) másodperces szintű összehangolása szükséges. Néhány esetben a pontosság ennél nagyságrendekkel nagyobb, pl. a stratégiai titkosítást végző berendezések esetén gyakori követelmény az atomórák pontossága. Ezt az „idillt”, költséghatékonyan csak az elektronikai hadviselés eszközeivel lehet megbontani, a szembenálló (lefogni kívánt erők) fél hatékony együttműködését minimalizálni, illetve az elvárt védelmet biztosítani. Az ehhez szükséges katonai elvárások megvalósításához a szakemberek napjainkra hatékony eszközöket, újfajta eljárásokat dolgoztak ki, amelyek kiegészítik, és a mesterséges intelligencia különböző megvalósítási szintjein „szinkronizálják” a különböző irányokból tervezett elektronikai támadást, valamint a védelmet. A tanulmány röviden áttekinti az elektronikai hadviselés (EHV) közelmúltban fontosnak tartott elemeit, összefoglalja és javaslatokat fogalmaz meg a szerző szerint kiemelten kezelendő kérdéskörökre és kutatási irányokra.

Az elektronikai hadviselés legfontosabb jellemzői

Az USA Védelmi Minisztériuma folyamatosan frissíti a katonai szakterületek elnevezéseit és fogalmait, ugyanakkor a szerző hadmérnöki nézőpontból, egyszerűsítve elemzi a kihívásokat, ahol a régebbi elnevezések és fogalmak ismerete szélesebb körben terjedt el, ezért célszerű a régebbi és az újabb szemléletek „egyesítése”.

Napjainkban az EHV tevékenységeit a közös elektromágneses spektrumhasználat (Electro Magnetic Spectrum Operations – EMSO) 1 MHz-től 1 THz-ig – az optikai és infravörös tartományokat is beleérve – tervezése, koordinálása és kezelése jellemzi. [2] Az EHV kapcsolódó tevékenységek „hagyományos” légi-, tengeri, alacsony műholdpályákról, szárazföldi mobil/fix települési és a megtámadott ellenfélhez viszonyítva közeli, vagy távoli körzetekből is történhetnek. Az EMSO használatának sokszínűségét, kiterjedését és komplexitását szemlélteti az *1. ábra*.

ÖSSZEFOGLALÁS: Az elektronikai hadviselés (EHV) a rádió és a rádiólokátorok elterjedésével, valamint katonai műveletekben történő alkalmazásával a 20. század elején és középső évtizedeiben jelent meg. Megelőzte a kiberhadviselést, amelynek célja egy állam vagy egy szervezet információs rendszereinek stratégiai szintű, katonai célú, szándékos támadása. E tevékenység csak évtizedekkel később, a számítógépek és az internet feltalálása nyomán indult fejlődésnek. Napjainkban vannak átfedések az elektronikai- és a kiberhadviselés között, de kulcsfontosságú különbségek is megfigyelhetők. Míg a kiberhadviselés nem lehet sikeres a jól megtervezett és védett, a globális kibertérrel csak nagyon korlátozott adatkapcsolattal rendelkező katonai rendszerek ellen, addig a korszerű elektronikai harc (EHC) rendszerek behatolhatnak az ilyen típusú „erődítményekbe”. 2017-ben, egy év előkészítés után, indult el a Magyar Honvédség elektronikai hadviselés-fejlesztési programja, amelynek célja a rádióelektronikai felderítő és zavaróképesség megújítása. A Magyar Honvédség modernizációjának sikere alapvetően az újonnan megjelenő műszaki lehetőségek és katonai alkalmazások, szakmai kiszolgálásától és felhasználásától függ.

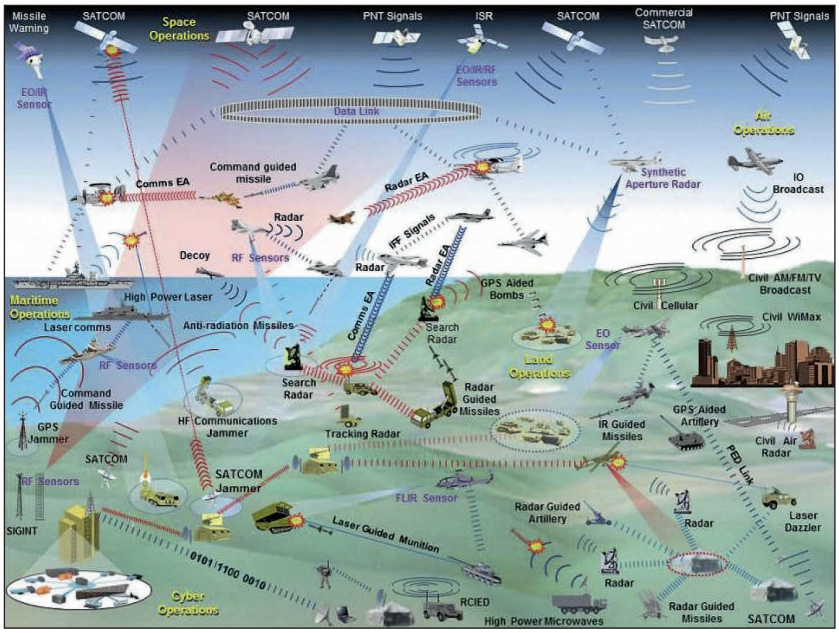
KULCSSZAVAK: elektronikai hadviselés (EHV), kiberhadviselés, rádiólokátor, DRFM (Digitális Rádió Frekvencia Tárolás)

ABSTRACT: Electronics Warfare (EW) emerged in the early and middle decades of the 20th century with the spread of radio and radar and their use in military operations. It therefore predates cyberwarfare (CW), which emerged decades later with the invention and spread of computers and the internet to disrupt the activities of a state or organization, especially the deliberate attacking of information systems for strategic or military purposes. Today, some overlap exists between EW and CW, though there is a key difference between the two. While the CW could not be successful against well defended, designed and separated military systems that have very limited data connection to the global cyberspace, the advance EW systems shall penetrate these types of “Fortifications”. In 2017, after a year preparation, the Hungarian Army’s electronic warfare development program was launched, aimed to renew radio electronic reconnaissance and jamming capability. The success of the Hungarian Army modernization basically depends on the understanding, its professional service and usage of the newly emerging technologies and their military applications in the battlefield.

KEY WORDS: Electronics Warfare (EW), cyberwarfare (CW), radar, DRFM (Digital Radio Frequency Memory)

* Oktató, NKE HHK Katonai Műszaki Doktori Iskola. ORCID: 0000-0003-3566-2904

DOI: 10.23713/HT.55.3.01



1. ábra. Elektronikai hadszíntér – elektromágneses „káosz" környezet [3]
Space Operations – űrben történő tevékenységek; Missile Warning – rakétaindítás jelzése; SATCOM – Satellite Communication – műholdas kommunikáció; National Positioning, Navigation, and Timing (PNT) – nemzeti helymeghatározás, navigáció és időzítés; ISR – Intelligence, Surveillance, and Reconnaissance – hírszerzés, megfigyelés és felderítés; Commercial – kereskedelmi; EO/IR/RF Sensors – Electro-Optical/Infra-Red/Radio-Frequency Sensor – elektrooptikai/infravörös/mikrohullámú érzékelők; Data Link – adatkapcsolat; Air Operations – légi műveletek/tevékenységek: Syntetic Aperture Radar – szintetikus apertúrájú rádiólokátor; IO Broadcast – közlemények továbbítása; Command Guided Missiles – parancsvezérelt rakéták;
Comms EA – Communications Electronic Attack – távközlési eszközök elektronikus támadása; RADAR EA – rádiólokátorok elektronikus támadása; Decoy – csalétek;
IFF Signals – saját/idegen felismerés jelei; Maritime Operations – tengeri műveletek/tevékenységek: Laser Comms – lézeres távközlés/kommunikáció; High Power Laser – nagy teljesítményű lézer; Anti-radiation Missiles – önrávezető rakéták;
Land Operations – szárazföldi műveletek/tevékenységek: GPS Aided Bombs – Global Positioning System – globális helymeghatározással támogatott bombák; GPS Jammer – GPS zavaró; GPS Aided Artillery – GPS támogatású tüzérség; Search Radar – célkereső rádiólokátor; Tracking Radar – útvonalképző rádiólokátor; Leser Guided Minition – lézervezérelt lövedék; Laser Dazzle – lézer álcázás; hőkövető lövedékek;
SATCOM Jammer – SATCOM zavarók; HF Communications Jammer – HF-frekvenciás kommunikációt zavaró; SIGINT – Signals intelligence – rádiófelderítés; FLIR Sensor – hőkamerás érzékelő; civil WiMAX (Worldwide Interoperability for Microwave Access) – polgári hozzáférésű világméretű mikrohullámú inter-operativitás; RCIED (Radio-Controlled Improvised Explosive Device Link) – rádióvezérelt rögtönzött robbanószerkezet-kapcsolat; Civil Cellular – polgári mobiltelefon-rendszerek; Hight Power Microwaves – nagy teljesítményű mikrohullámok; Cyber Operations – kiberhadviselés

Az EHV három egymást kiegészítő, valamint egymást részben átfedő területre osztható [4,5]:

- Elektronikai támogató tevékenység (ESM – Electronic Support Measures), a Magyar Honvédség doktrínájának fogalomhasználata szerint elektronikai megfigyelés: a kisugárzott elektromágneses energia felkutatására, elfogására, elemzésére és az adatok, ismeretek gyűjtésére, értékelésére tett intézkedések. Az elektronikai megfigyelés célja az információ kiaknázása a katonai műveletek támogatása érdekében.
- Elektronikai támadás (ECM – Electronic Counter Measures): az elektromágneses spektrum ellenség általi hatékony használatának megelőzésére vagy csökkentésére tett intézkedések.
- Elektronikai védelem (ECCM – Electronic Protection/Counter-Counter Measures): célja az ellenség elektronikai támadásainak és elektronikai felderítésének kiküszöbölése vagy hatékonyságának csökkentése. Alkalmazását behatárolják az eszközök beszerzési és a modernizációs követelményei, pl. információs és adatátviteli csatornák, radarok ECCM performanciái, valamint az azok alkalmazását meghatározó harcászati-hadműveleti követelmények. Ez utóbbiak katonai alkalmazásához – Szun-Ce szavait idézve – szükséges:

o *Stratégia,* taktika nélkül a leglassabb út a győzelemhez.
o *Taktika,* stratégia nélkül csak zaj a vereség előtt. [15]

Magyarországon, az 1980-as években, a Videoton Rádióelektronikai gyáregységében, a Mechanikai Laboratóriumban és a Híradástechnika Szövetkezetben korszerű, felderítő- és zavaró-komplexumokat fejlesztettek hazai és külföldi felhasználók számára. [6] Ezek az eszközök, nemzetközi összehasonlításban is a kor kiemelkedő színvonalán jegyzett integrált elektronikai támogató tevékenység és elektronikai támadás képességekkel rendelkező rádióelektronikai rendszerek voltak. A történelem „fintora", hogy a cseh passzív felderítő- és radarrendszereket napjainkban már a világ élvonalába tartozó termékek között tartják számon, míg a hazai EHV-val kapcsolatos K+F+I (kutatás + fejlesztés + innováció) tevékenység csak most kezd újraéledni. [7] Az újrakezdés legnagyobb problémája, hogy ezek a feladatok felkészült szakembergárdát, egyetemi végzettségű vagy doktori fokozatokkal rendelkező hadmérnökök és parancsnokok alkalmazását követeli meg, akiknek a hazai kiképzése napjainkban igen nehéz feladat.

A témakörre vonatkozó kiemelt figyelem elvárásait, költségeit és a megvalósításra kitűzött határidőket szemléltetik az USA Kongresszusának készült jelentések. A legfrissebb dokumentum a 2019 és 2023 közötti EHV-eszközök kutatás-fejlesztésére és a beszerzésükre vonatkozik. [8] A haditengerészet, a légierő, a szárazföldi csapatok, a DARPA[2] és más kutatóintézetek EHV-eszközök fejlesztésére 5 év alatt 25,8 milliárd dollárt költenek, míg a beszerzésre 22,6 milliárd dollár áll rendelkezésre. A szerző szerint részben az EHV témakörébe tartozik a haditengerészet irreguláris és terrorellenes tevékenysége, mivel kihasználhatja az elektronikai támogató tevékenység nyújtotta előnyöket, és kiterjesztheti az EHV lehetőségeit. [9] A szárazföldi csapatok EHV-feladatait és projektjeit foglalja össze, illetve tekinti át [10] a jelentés. Ezek közül a legfontosabbak a rögtönzött robbanószerkezetek, a drónok és egyéb pilóta nélküli légi eszközök, valamint a kommunikációs és radarrendszerek elleni zavaróadók. (Az eszközök részletesebb áttekintésére egy későbbi tanulmányban kerül sor.) Az USA elektronikai hadviselési képességei közül a haditengerészet és a légierő a legütőképesebb. Háromféle, elsődlegesen elektronikai támadásra készült repülőgéptípussal rendelkeznek, amelyek a Navy EA–18G Growler, (lásd *2. ábra*) az Air Force EC–130H

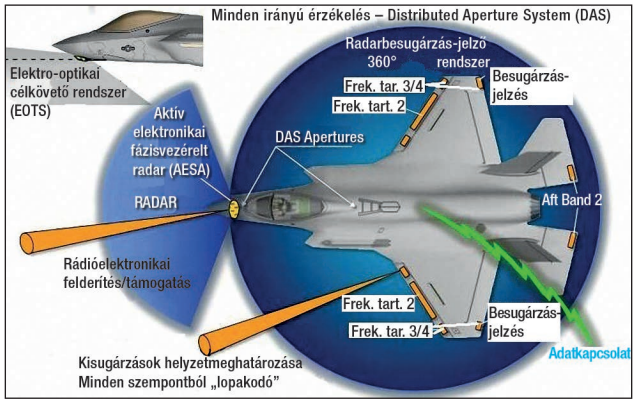
2. ábra. Az elektronikai támadásra optimalizált Navy EA–18G Growler repülőgép [11]

5. ábra. Újgenerációs zavarókonténer [11]

3. ábra. Az Amerikai Egyesült Államok Légierejének EC–37B Compass Call Re-Host repülőgépe [11]

Compass Call, és az Air Force EC–37B Compass Call Re-Host *(3. ábra)*. A negyedik repülőgéptípus, az F–35 Joint Strike Fighter úgynevezett „megnövelt”, „rendszerbe integrált” képességekkel rendelkezik, amely képességekről csak nagyon kevés tényt hoztak nyilvánosságra *(4. ábra)*. Az EA–18G és az EC–130H kifejezetten elektronikai hadviselési támogató feladatokra épített repülőgépek. Az előbbi kísérő (escort) zavarásra, míg az utóbbi távoli (stand-off) zavarásra alkalmas. Az F–35 azonban más szerepkörbe tervezett repülőgép, de önvédelmi EHV-képességgel rendelkezik. Külső felfüggesztésként használatos az AN/ALQ–99 zavarómodul és az újgenerációs zavaróadó konténer (Next Generation Jammer) *(5. ábra)*, valamint a „miniatűr légi indítású csapda” zavaróadó (Miniature Air Launched Decoy-Jammer). [11] A drága EHV-eszközrendszerek kiegészülnek az elektromágneses spektrum szűk tartományainak figyelésére, és az elfogott jelek modulált visszasugárzására optimalizált berendezésekkel is. Ezek az aránylag olcsó DRFM- (Digital Radio Frequency Memory) eszközök kis tömegük miatt többek között drónok függesztményeként is tömegesen bevethetők.

4. ábra. Az F–35 Joint Strike Fighter elektronikai hadviselésre optimalizált rendszerei [11]



A légtérellenőrzést ellátó radarrendszereket gyakran az integrált légvédelem „szemének” nevezik, amelyet, ha „megvakítanak”, illetve „megtévesztenek”, a harctevékenységek sikere jelentősen befolyásolható. Általánosan elfogadott tény, hogy a rádiólokátorok céltárgydetektálási zónái „fehérzaj” típusú aktív zavarással hatékonyan csökkenthetők. Az előzőekben felsorolt zavaró rendszerek légtérellenőrző radarokra gyakorolt lehetőségeit elképzelt EHV-helyzeteken keresztül szemlélteti az *1. táblázat*. Legyen a zavaradó átlagteljesítménye „szinte jelentéktelen” 1 W, amely adás-vétel kapcsolón keresztül csatlakozik a 10 dBm nyereséggel rendelkező antennához. Ez 10 W effektív kisugárzott teljesítményt (ERP – Effective Radiated Power) jelent a radar frekvenciasávjában. (Az említett példa megfelel egy drónra szerelhető DRFM-eszköz átlagosnak számító teljesítményének.) A zavarás a radar pillanatnyi/üzemi sávszélességében (PS) a leghatékonyabb, mivel ekkor a legnagyobb a zavarás jelteljesítmény-sűrűsége. Ha a radar és a zavaradó pillanatnyi sávszélessége megegyezik pl. 2,5 MHz, akkor ez 4 W/MHz ERP-t jelent a radar „elvakítása” szempontjából. Hamis céltárgyaknak a radar fényalábjában történő szimulálásához azonban, ennek a teljesítménynek az ezredrésze is elegendő, mivel „csak” a radarimpulzust kell visszasugározni. A zavar jelteljesítmény-sűrűsége jelentősen csökken, ha a radar szórt spektrum (SS) üzemmódban képes működni, mivel akkor a zavaradó teljesítménye eloszlik az egész üzemi frekvenciasávban. Pl. legyen: „L”, „S”, és „VHF” sávú radarok esetén az üzemi frekvenciatartomány 200 MHz, 500 MHz és 80 MHz. Ennek következtében, szórt spektrum üzemmódban a zavaradó hatásos teljesítménye az „L” sávban ERP = 0,05 W/MHz, az „S” sávban 0,02 W/MHz, mid a „VHF” sávban 0,125 W/MHz. Az ERP = 10 W fehérzajjal történő zavarás különböző típusú, „L”, „S” és „VHF”-sávú, a rádiólokátorok maximális céltárgydetektálási távolságára gyako-

1. táblázat. Különböző típusú zavarhelyzetek céltárgy-detektálásra gyakorolt hatása*

Szabványos céltárgy / Repülőgéptípus	R_{max} [km] = 300 km, Szabadtér, P_d = 0,8/P_{vl} = 10^{-6}, Zavaradó: ERP = 10 Watt, helyzete = 300/100 km és 10/1 km								
	L (1,3 GHz) BW = 200 MHz			S (3,1 GHz) BW = 500 MHz			VHF (0,18 GHz) BW = 80 MHz		
	–	PS	SS	–	PS	SS	–	PS	SS
RCS = 1 m², Sw1 [km]	300	256/228 57/18	299/292 161/54	300	299/289 149/50	300/299 258/102	300	208/127 41/13	250/166 54/17
Airbus A320 [km]	531	251/301 100/32	529/517 282/94	447	445/432 220/74	447/446 384/150	791	542/329 107/35	657/430 141/46
Saab JAS–39 [km]	393	335/225 75/24	392/384 210/70	332	330/320 165/55	332/331 285/112	530	364/222 72/23	440/290 96/31
SR71/MiG–25 [km]	446	251/129 85/27	445/435 238/80	394	392/380 194/65	394/393 338/133	501	345/210 68/22	416/275 91/29
HyW [km]	224	191/118 43/14	223/218 121/40	171	171/166 86/28	171/171 148/59	300	208/127 41/13	250/166 54/17

Ahol: BW: sávszélesség, PS: pillanatnyi sávszélesség, SS: szórt spektrum/a radar üzemi sávszélessége, Airbus A320 RCS= (L: 10 m², S: 5 m², VHF: 50 m²), *Saab JAS–39 RCS=* (L: 3 m², S: 1,5 m², VHF: 10 m²), *SR71/MiG–25 RCS=* (L: 5 m², S: 3 m², VHF: 8 m²), *HyW RCS=* (L: 0,3 m², S: 0,1 m², VHF: 1 m²)

* A szerző radaregyenleten alapuló, Blake chart számításokkal készült saját táblázata a Haditechnika 2021/1. szám 6. oldalán megjelent 2. táblázat továbbfejlesztése.

rolt hatását szemlélteti az 1. táblázat. A zavaradó 300 km, 100 km, 10 km és 1 km távolságra található a radartól. Természetesen a vizsgált radarok műszaki paraméterei olyanok, hogy zavarmentes környezetben, a „szabvány céltárgyat", amelynek hatásos radarkeresztmetszete (RCS) = 1 m², a céltárgy-fluktuáció típusa: Sw1) azonos távolságon, 300 km-en detektálják, azonos céltárgydetektálás minőségi elvárásokkal (P_d,P_{vl}) és 20,5 dB veszteséggel**.** A táblázatban szerepelnek a „szabvány céltárgy" mellett más valós céltárgyak legnagyobb hatásos radarkeresztmetszettel mérhető maximális, oldalról megvilágított céltárgydetektálási lehetőségei. (Ennek kb. a tizede a RCS, ha a valós céltárgy elölről kerül besugárzásra.) Az áttekintés elősegítéséhez hasonlítsuk össze a „szabvány céltárgy" céltárgydetektálási sajátosságait a hiperszonikus fegyverek (HyW) hasonló lehetőségeivel. Zavarmentes környezetben az „L", az „S" és a „VHF"-sávban üzemelő radarok a „szabvány céltárgy"-at 300 km távolságon detektálhatják, míg ugyanezek a radarok a hiperszonikus fegyvereket csak 224, 171, és 300 km-en. Ha célzott zavarást (PS) alkalmazunk a radarok ellen, 300 km, 100 km, 10 km és 1 km távolságról a „szabvány céltárgy" detektálhatósága: 256, 228, 57 és 18 km, míg a HyW detektálhatósága: 191, 118, 43 és 14 km az „L" sávban. Szórt spektrumban (SS) történő zavarás esetén ezek az értékek: 299, 292, 161 és 54 km, míg a hiperszonikus fegyverek detektálhatósága: 223, 218, 121 és 40 km. Az „S" és „VHF" sávra vonatkozó értékek már könnyen értelmezhetők.

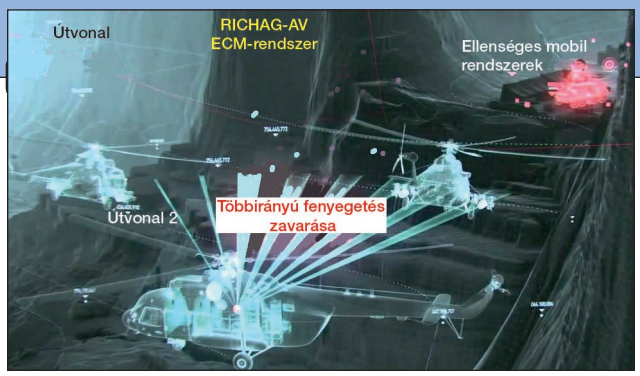
A rádióelektronikai zavarás hatékonysága három csoportba sorolható: *erős, közepes* és *gyenge*. [4] Az 1. táblázatban jól látható, hogy egy drónra szerelhető kis teljesítményű zavaradó 10 km-es távolságon belül közepes és/vagy erős szinten képes csökkenteni a radarok céltárgydetektálási tereit. Ugyanakkor az újgenerációs, korszerű zavarókonténerek vagy egyéb mobil platformok 50 W/MHz, 100 W/MHz, esetleg a 200 W/MHz zavarójel-teljesítménysűrűséggel is jellemezhetők. Ezek az eszközök már 100, 300 km távolságról, esetleg alacsony műholdpályákról is hatékonyak. Ennek következtében a jelenleg üzemben lévő radarok céltárgydetektálási terei annyira lecsökkenthetők, hogy nem képesek az elvárt repülőgéptípusokat detektálni, útvonalba fogni, az útvonalakat fenntartani, és mint céltárgyakat azonosítani. További problémát okoz a különböző zavarási eljárások, módszerek vegyes alkalmazása.

A különböző hatékonysági mutatók értékelésére számos tanulmánykötet készült. Ugyanakkor hadmérnöki-harcászati szempontból felmerül a kérdés, hogy valóban csak ezek a kategóriák léteznek, vagy léteznek ennél korszerűbb rádióelektronikai zavarási módszerek, eljárások is. Gondoljunk például az aktív „lopakodó" technológiát alkalmazó repülőgépekre, amelyek jól láthatók a rádiólokátorokkal, de a radarimpulzus manipulálásával „eltűnhetnek", ha ez a cél. Ezért folyamatosan vizsgálnunk kell azokat a lehetőségeket, új vagy újszerű műszaki megoldásokat és alkalmazási módszereket, amelyek során a zavarás tényét az ellenséges elektronikai eszközök (pl. radarok, információs csatornák stb.) nem, vagy csak nehezen észlelhetik.

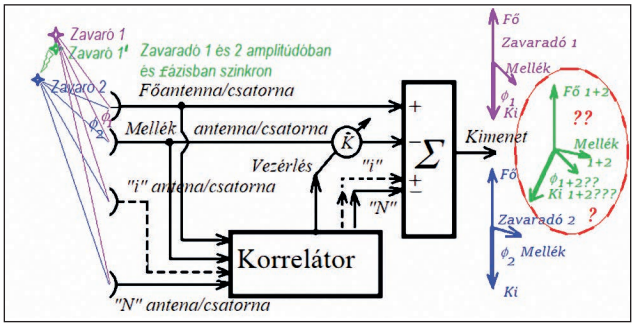
Az EHV-rendszerek fejlesztési irányai

Az aktív fázisvezérelt antennákkal (lásd az AESA jelölést a *4. ábrán*) felszerelt repülőeszközök és konténerek napjainkban – a feladatok és a zavarási, megtévesztési lehetőségek hatékony alkalmazásának érdekében – már digitális adatkapcsolatban állnak egymással. Az aktív zavarás lehetőségeivel kapcsolatos előzőleg ismertetett sajátosságokból következik, hogy az ESM a több irányból érkező fenyegetéseket időben detektálja, elemzi, és a veszélyt felismerve ellenintézkedésekkel csökkenti azok hatását. A folyamat részletesebb elemzését mutatja a *6. ábra*, ahol elektronikai támadás alkalmazással semlegesítik az ellenség több irányból, azonos időben megjelenő fenyegetéseit.

Az EHV fejlődésének következő (a rádiólokátor felbontóképességén belüli) szintje az egymással időben szinkronban lévő, „pontszerű" elektronikai támadórendszerek (pl. a *7. ábrán* jelölt „Zavaradó 1" és „Zavaradó 2" platformok) „RF-jeleinek" amplitúdó- és fázisában való szinkronizálása.



6. ábra. Több irányból érkező, különböző típusú fenyegetések elleni EHV-válasz [12]

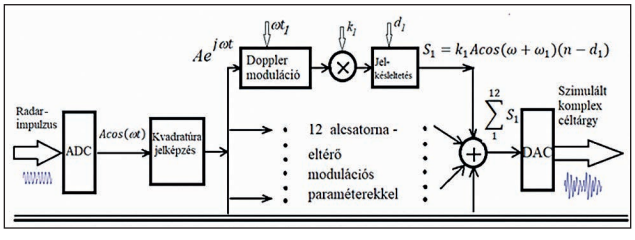


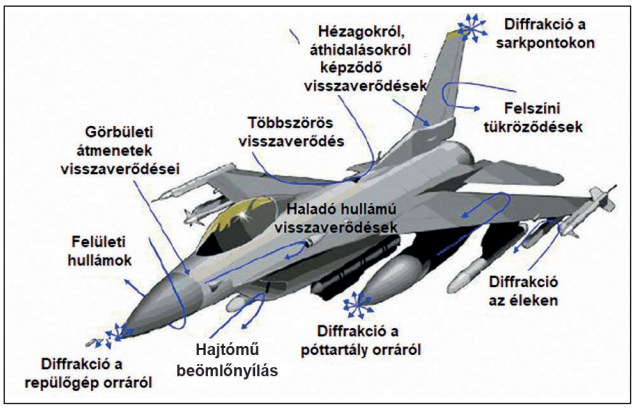
7. ábra. A térbeli aktív zavarszűrés elve [13]

Ez utóbbi esetben (a rádiólokátor felbontóképességénél jelentősen nagyobb) pontszerű elektronikai támadás már „térben kiterjesztett", a rádiólokátorok mérési szabadságfokát meghaladó zavarási lehetőségekkel rendelkezhet. Ezt szemlélteti a *7. ábra,* ahol a „Zavaradó 1" (lila) és „Zavaradó 2" (kék) hagyományosan „pontszerű" a radar zavarvédelmi rendszerei számára. Ezért a fő és segédcsatornákra érkező jelek fázisfutási különbsége „Korrelátorral" pontosan mérhető, és a zavarójelek teljesítménye a beérkezési szög és jelfeszültség ismeretében, adaptív vezérléssel (K) jelentősen csökkenthető. Természetesen csak abban az esetben, ha a radar segédcsatornáinak száma több mint a zavaróadók száma. Például 2 db, a radar számára nagy kitöltési tényezővel rendelkező „pontszerű" zavaradó jeleit, 3 db segédcsatornás rendszer már hatásosan kompenzálhatja; lásd a „Zavaradó 1" (lila) és „Zavaradó 2" (kék) „pontszerű" helyzetet szemléltető vektorokat a 7. ábrán. Ugyanez a védelmi rendszer már hatástalan a „térben kiterjesztett" „Zavaradó 1" (zöld) és „Zavaradó 2" (kék) amplitúdóban és fázisban szinkronizált zavarása esetén. Ezt szemlélteti a 7. ábra utolsó vektordiagramja, ahol a „Korrelátor" által képzett vektorok nem helyesek, hiszen azt a zavaróadók manipulálják. A probléma kiküszöbölésére növelni kell a radarok térbeli mérési szabadságfokát. Erre nyújtanak lehetőséget a multistatikus radarrendszerek.

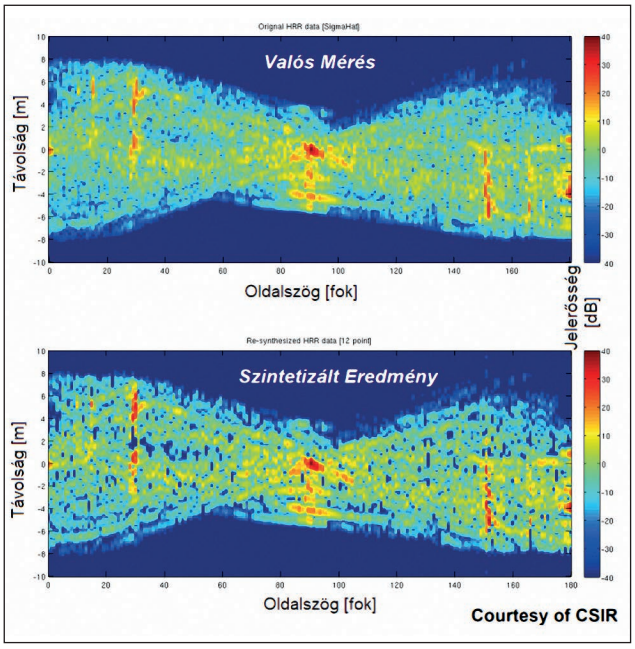
A szerző szerint az elektronikai támadás legjelentősebb, és – szakszerű alkalmazás esetén – a leghatékonyabb, illetve a radarok és kommunikációs csomópontok számára a legveszélyesebb műszaki megoldása, a DRFM-eszközök széles körű alkalmazása. A DRFM általános felépítését szemlélteti a *8. ábra,* míg a berendezés a *11. ábrán* látható.

8. ábra. A DRFM működésének elve [14]



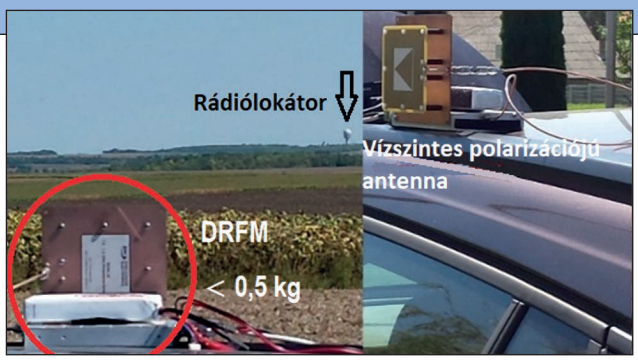


9. ábra. A radarimpulzus céltárgyról való visszaverődésének komplexitása [12]



10. ábra. A céltárgyról visszaverődött, mért, és a DRFM-eszköz által képzett radarjel [14]

Az antenna által vett radarimpulzus sávszűrés, -erősítés és analóg-digitális átalakítás (ADC) után digitális jelfeldolgozásra kerül. Ez minden esetben tartalmazza a „Kvadratúra jelképzést", a „Doppler-modulációt", a sávkiterjesztést „k_1", a „Jelkésleltetést", a radar számára szükséges céljel távolsági elhelyezését, valamint a digitális jelfolyam analóggá alakítását, erősítését, az adás-/vétel-kapcsoló után az antennára érkező jelnek a radar irányába történő visszasugárzását. DRFM-módszerekkel megoldható a napjainkban gyorsan terjedő képalkotó radarok visszavert jeleinek manipulálása. Ebben az esetben a DRFM-eszköz a szimulált komplex céltárgy több, pl. „12 alcsatorna" eltérő modulációs paramétereit állítja be oly módon, hogy az a képalkotó radar mérési pontosságával összemérhető. Ezek között található a céltárgy mikro-Doppler-jeleit moduláló csatornajel. A megoldandó feladat komplexitását szemlélteti a 9. ábra, amely a képalkotó radarok számára fontos céltárgy-visszaverődéseket szemlélteti. Ezek a visszaverődések egyszerűbb esetekben a visszavert jel átlagjelteljesítményét leíró eloszlásfüggvények, pl. Marcum-, Swerling-modellekkel jellemezhetők. A képalkotás hitelességéhez azonban a részleteket pontosan azonosító, a jel hullámterjedési és



11. ábra. Magyar gyártmányú DRFM-eszköz
(Fotó: Balajti István, 2016)

polarizációs tulajdonságait frekvenciatartományonként a megvilágítási szög függvényében tartalmazó mérési eredmények szükségesek. A *10. ábra* a megvalósítási lehetőségek eredményességét mutatja. Az ábra felső része a képalkotó radarral mért valós eredményeket szemlélteti, míg az alatta lévő „csak" egy DRFM által létrehozott manipuláció. A különbségek kiértékeléséhez már mesterséges intelligencia alkalmazása szükséges. A 11. ábra mérés közben mutat egy magyar gyártmányú DRFM-eszközt.

Pontos adatok nem állnak rendelkezésre, de feltételezhető, hogy a DRFM-eszközök beépíthetők a ún. újgenerációs zavaradó konténerekbe, valamint a miniatűr légi indítású csapdákba is. Ismerve a 10. ábrán bemutatott DRFM-radarjel modulálás hatékonyságát a nagy felbontású „visszavert" radarjel-előállítás területen, joggal feltételezhető az elektronikai támadás alkalmazási területeinek bővülése. Ezért békében is fel kell készülni az olyan helyzetekre, ahol csak néhány fontos céltárgy „hiányzik" a teljes és azonosított légi helyzet környezetéből. Ugyanakkor krízis- és háborús helyzetekben a megtévesztéseknek jelentős hatása lehet a légi helyzet megítélésére, hiszen *„közepes" és „erős"* zavarviszonyok között a radarok számára szinkronban repülő hamis kötelékek imitálhatók a fő támadási irányok, csapatmozgások leplezésére.

Összegzés

A tanulmány érzékeltette, hogy a korszerű EHV-alkalmazások napjaink légvédelmi rendszerei számára komoly kihívásokat jelentenek. Az elektronikai támadások a meglévő légtérellenőrző radarrendszerek eddig elvárt képességeit jelentősen meghaladó lehetőségekkel és harcászati-hadműveleti alkalmazásokkal rendelkezhetnek. Megállapítható, hogy a kiberhadviselés által kifejlesztett és alkalmazott védelem lehetőségei rendkívüli mértékben beszűkülnek, mivel *a harctéri katonai rendszerek szinte teljesen izoláltak a polgári számítógépes hálózatoktól*. Ugyanakkor a katonai rendszerekben alkalmazott technológia és a döntéselőkészítő rendszerek automatizálása ahhoz vezetett, hogy a folyamatok ismeretének mélységében az elektronikai támadásrendszereinek hatékonysága rendkívüli mértékben megnőtt. Ezért alkalmazásuk elkerülhetetlen az elszigetelt katonai rendszerek leküzdéséhez. Az elektronikai támadás hatékony alkalmazását mindenekelőtt a békében is teljes hatékonysággal üzemeltetett elektronikai támogató tevékenység – ezen belül a rádiófelderítés – határozza meg, ezért ennek az EHV-területnek a fejlesztése elsődlegesen fontos.

Hivatkozott irodalom

[1] Csatári Sándor. *A rádióelektronikai harc helyzete és továbbfejlesztésének fő iránya a Magyar Néphadseregben* Doktori értekezés, 1984. II. kötet 108. o.;

[2] Department of Defense. *Joint Publication 3-13.1, Electronic Warfare*, 2012 02.08, p. I-15, letöltés: 2021. 01. 06. https://www.globalsecurity.org/military/library/policy/dod/joint/jp3_13_1_2012.pdf és https://publicintelligence.net/jcs-ew/;

[3] Malte von Spreckelsen. *Electronic Warfare – The Forgotten Discipline*, Joint Air Power Competence Centre, 2020, letöltés: 2020.10.05. https://www.japcc.org/electronic-warfare-the-forgotten-discipline/;

[4] Haig Zsolt, Kovács László, Ványa László, Vass Sándor. *Elektronikai hadviselés*, Nemzeti Közszolgálati Egyetem, 2014.;

[5] Horváth József. „Elektronikai hadviselés a Magyar Honvédségben" Hadmérnök IX. évfolyam 1. szám (2014. március), letöltés: 2020.09.20. http://hadmernok.hu/141_17_horvathj.pdf;

[6] Gerlits Péter. „Elhalt fejlesztések" lazarbibi.blog.hu Letöltés: 2020.09.20. https://lazarbibi.blog.hu/2016/10/15/elhalt_fejlesztesek;

[7] Horváth József Sándor. *A Magyar Honvédség Elektronikai Hadviselési Képességének Fejlesztése Szoftverrádiók Alkalmazásával*, Doktori Értekezés Tézisfüzete, Bp.: NKE Műszaki Doktori Iskola, 2018. Letöltés: 2020.09.20. https://www.uni-nke.hu/document/uni-nke-hu/horvath_jozsef_sandor_tezisfuzet_2018.pdf;

[8] J. R. Hoehn. *U.S. Military Electronic Warfare Program Funding: Background and Issues for Congress*, Congressional Research Service, Updated April 16, 2020;

[9] J. R. Hoehn. *Navy Irregular Warfare and Counterterrorism Operations: Background and Issues for Congress*, Congressional Research Service, Updated December 17, 2019.;

[10] J. R. Hoehn. *Ground Electronic Warfare: Background and Issues for Congress*, Congressional Research Service, Updated September 17, 2019;

[11] J. R. Hoehn. U.S. Airborne Electronic Attack Programs: Background and Issues for Congress, Congressional Research Service, Updated May 14, 2019;

[12] A. De Martino. *Introduction to Modern EW Systems*, Artech House, 2018;

[13] I. Balajti. „Air Defense System Operation in the EW Space: Understanding where radar system capability exists within Electromagnetic Spectrum Operations (EMSO) for the military" *Military Radar*, London, 27-29 August 2019, https://www.defenceiq.com/events-militaryradar/speakers/istvan-balajti;

[14] R. S. Andrews. *Digital Radio Frequency Memory Technology & Techniques for EW*, http://tangentlink.com/wp-content/uploads/2014/03/7.-Digital-Radio-Frequency-Memory-Technology-Techniques-for-EW-Robert-Andrews.pdf;

[15] Szun-Ce. A hadviselés törvényei. Fordította: Tőkei Ferenc https://mek.oszk.hu/01300/01345/01345.htm#terv, letöltés: 2021.01.10.

Jegyzetek

1 REH – Rádióelektronikai harc (napjainkra: elektronikai harc – EHC; tágabb értelmezésben: elektronikai hadviselés – EHV)

2 Defense Advanced Research Projects Agency (www.darpa.mil) az Amerikai Egyesült Államok Védelmi Minisztériumának kutatási és fejlesztési ügynöksége, amely a korszerű katonai technológiák fejlesztéséért felelős.