HADMÉRNÖK

X. Évfolyam 1. szám - 2015. március

HORVÁTH József
horvath0101@gmail.com

AZ ELEKTRONIKAI ZAVARÁS NAPJAINKBAN

Absztrakt

Az elektronikai ellentevékenység egyik eleme az elektronikai zavarás. Az elektronikai zavarás a legismertebb terület, mivel a médiában rengeteg információt találhatunk róla. Napjainkban egy hatékony zavarás kivitelezése nem egyszerű a fejlett kommunikációs és radarberendezések miatt. Az elektronikai zavarás új kihívásokkal is szembesült, mivel megjelent az igény az új elektronikai rendszerek (pl. navigáció) zavarására is. Jelen cikkben a szerző bemutatja az elektronikai zavarás fogalmát, bemutat néhány példát a múltból illetve bemutatja a jelenlegi és jövőbeli helyzetet.

The electronic jamming is one of the elements of the electronic warfare. The electronic jamming is the best known EW expression among the people, since there are a lots if information about it in the media. Recently to carry out an effective jamming is not simple, because of the advanced communication and radar systems. The electronic jamming meets new challenges as well, because there is a need for the jamming of the new electronic systems (e.g. navigation). In this paper, the author describes the concept of the electronic jamming, cites several examples from the past and introduces the current and future situation.

Kulcsszavak: *elektronikai hadviselés, elektronikai ellentevékenység, elektronikai támadás, elektronikai zavarás ~ electronic warfare, electronic countermeasures, electronic attack, electronic jamming*

BEVEZETÉS

Az elektronikai hadviselés egyik részterülete az elektronikai ellentevékenység, vagy ahogyan több forrásban is szerepel, elektronikai támadás[1]. A fogalom további 3 részterületre osztható, ezek az elektronikai zavarás, az elektronikai megtévesztés és az elektronikai pusztítás. Az elektronikai hadviselés valamennyi részterülete közül az elektronikai zavarás az, ami a leginkább észlelhető vagy felderíthető, illetve, amiről a hétköznapi emberek is a legtöbb információval rendelkeznek. Sokszor jelennek meg a sajtóban a különböző elektronikai zavaró eszközökről szóló cikkek és képek, illetve számos webáruházban rendelhetünk ilyen eszközt mindenféle engedély nélkül. Fontos tudni, hogy az elektronikai zavaróeszközök a haditechnikai eszközök és szolgáltatások kivitelének, behozatalának, transzferjének és tranzitjának engedélyezéséről, valamint a vállalkozások tanúsításáról szóló 160/2011. (VIII. 18.) számú Kormányrendelet hatálya alá esnek és engedélykötelesek.

Jelen cikk célja bemutatni az elektronikai zavarás helyét, alkalmazásának alapelveit, illetve ismertetni, elemezni a szoftverrádiós technológia támadhatóságát informatikai és elektronikai zavarási szempontok alapján.

AZ ELEKTRONIKAI ZAVARÁS AZ ELEKTRONIKAI HADVISELÉS FOGALOMRENDSZERÉBEN

Mielőtt belemélyednénk az elektronikai zavarás megvalósíthatóságának elemzésébe, fontos, hogy tisztában legyünk a fontosabb alapfogalmakkal.

„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. Területei az elektronikai támogató tevékenység, az elektronikai ellentevékenység és az elektronikai védelem.” [1]

Az elektronikai ellentevékenység három fő területe:

- elektronikai zavarás (Electronic jamming), amely az elektromágneses energia szándékos kisugárzását, visszasugárzását, vagy visszaverését jelenti azzal a céllal, hogy ezáltal megakadályozzuk az ellenség elektronikai eszközeinek vagy rendszereinek hatékony működését;
- elektronikai megtévesztés (Electronic deception), amely az elektromágneses energiának a szándékos kisugárzása, átalakítása, visszasugárzása, elnyelése, vagy visszatükrözése azzal a céllal, hogy megtévessze, félrevezesse, összezavarja, vagy eltérítse az ellenséget, annak elektronikai rendszereit;
- elektronikai pusztítás (Electronic neutralization), amely az elektronikai pusztítás az elektromágneses és egyéb irányított energiák, vagy az önrávezetésű fegyverek alkalmazását jelenti, az ellenség elektronikai eszközeiben és az élőerőben tartós, vagy ideiglenes károkozás céljából. [1]

[1] Electronic attack, EA

AZ ELEKTRONIKAI ZAVARÁSRÓL ÁLTALÁBAN

Elektronikai zavar minden olyan jelenség, amely az adott elektronikai vevőeszközökön a hasznos jel vételét akadályozza vagy teljes mértékben meggátolja. A zavarok osztályozásának egyik lehetséges módja:

1. mesterséges:
    a) szándékos:
        - sugárzási jellemzők szerint:
            - folyamatos;
            - impulzus;
        - spektrum szerint:
            - célzott;
            - szélessávú;
            - csúszó;
        - hatékonyság szerint:
            - gyenge;
            - közepes;
            - erős;
        - hatásjellemzők szerint:
            - álcázó;
            - imitáló;
        - létesítési mód szerint:
            - aktív;
            - passzív;
    b) nem szándékos:
        - ipari;
        - áramköri;
        - kölcsönös;
2. természetes:
    c) atmoszférikus;
    d) kozmikus;
    e) elektrosztatikus; [1]

Az elektronikai hadviselés részét képező elektronikai zavarás mesterséges, szándékos zavarokkal hozható létre.

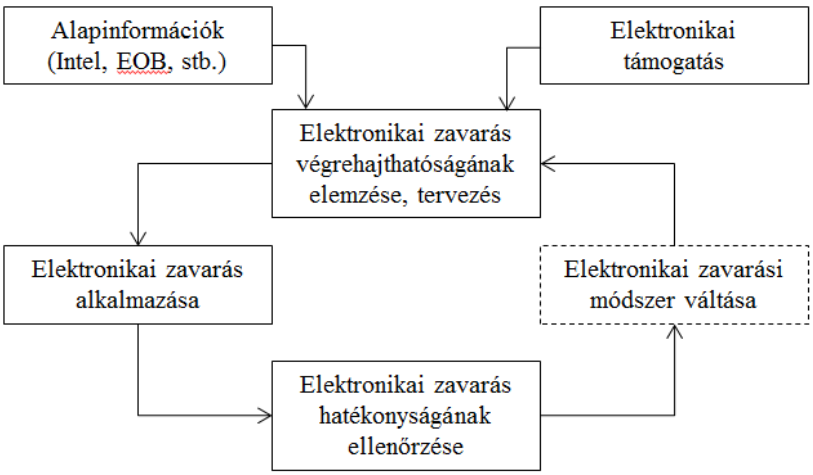
A rádióeszközök lefogása akkor hatékony, ha a vevő bemenetén nagyobb zavar/jel viszonyt tudunk létrehozni, mint K*zmin*. A K*zmin*, a lefogási tényező a lefogás bekövetkezésekor a bemeneten fellépő zavarjel és hasznos jel teljesítményének minimális aránya. Minél kisebb ez az arányszám, annál könnyebb energetikailag a hatékony zavarást létrehozni.

$$K_{zmin} = \frac{P_z}{P_j}$$

Lefogási zóna az a terület vagy térrész, ahol K > Kz *min*, le nem fogott zóna, ahol K < Kz *min*, és a kettő terület közötti határon a K = Kz *min*. [1]

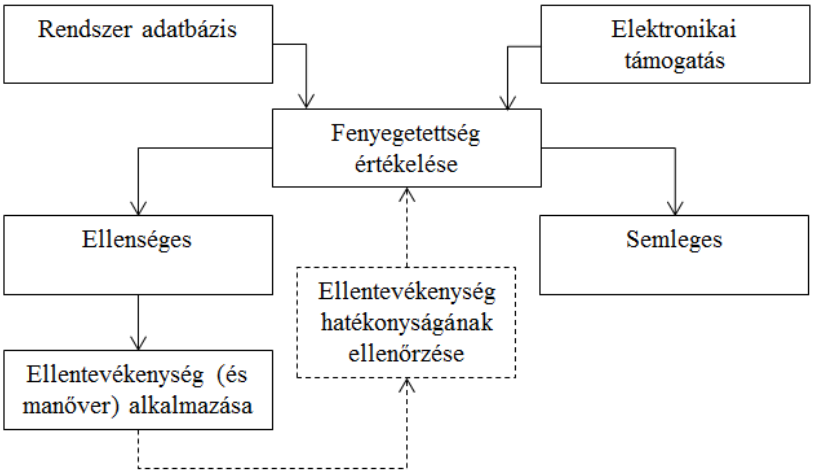
Az elektronikai zavarás végrehajtásával kapcsolatban véleményem szerint különbséget kell tenni a tervezett (védelmi vagy támadó célú) és az „önvédelmi” célú elektronikai zavarás között. Az 1. sz. ábrán látható a tervezett elektronikai zavarás folyamata. A tervezett elektronikai

zavarást alkalmazzuk, amennyiben a műveletek, a célmeghatározás/céltervezés[2] vagy az információs műveletek[3] tervezése során előre azonosított vagy a feladatok végrehajtása során felfedett elektronikai kisugárzó eszköz ellen tevékenykedünk. Lényeges, hogy az elektronikai hadviselési erők nem tevékenykednek önállóan. Feladatukat az „Átfogó műveletttervezési direktíva”[4] alapján kialakított, és a parancsnok által elfogadott cselekvési vázlatból készített hadműveleti tervben/parancsban foglaltak szerint hajtják végre. Amennyiben a célpont adatok már korábban rendelkezésre álltak, az elektronikai tervezés során már vizsgáltuk a zavarás lehetőségét, és amennyiben az lehetséges, a feladat a műveletek tervezése/végrehajtása során elrendelésre kerül. Fontos kihangsúlyozni, hogy a korábbi, manuális, papíralapú tervezést már felváltotta a korszerű informatikai és térinformatikai rendszereket alkalmazó tervezés, amellyel a korábbi időigényes folyamat jelentősen lerövidült. Ismeretlen kisugárzó eszköz esetében a zavarás lehetőségének vizsgálatát a felfedés pillanatában meg kell kezdeni és a célpontot az érvényben lévő direktíváknak vagy az elöljárói feladatszabásnak megfelelően kell kezelni. A tervezett elektronikai zavarás esetében a hatékonyság ellenőrzésének is fontos szerepe van, illetve időnk is van annak végrehajtására. Ezzel szemben egy repülőgép önvédelmi elektronikai hadviselési rendszere – például a JAS 39 Gripent figyelembe véve – a tárolt adatok alapján beazonosítja a veszélyforrás jellegét (ellenséges vagy semleges) és figyelmezteti a pilótát vagy a rendszer beállításától függően akár meg is kezdi az elektronikai ellentevékenységet. Itt szándékosan az ellentevékenység szót használom, mivel nemcsak zavarásról, hanem elektronikai megtévesztésről is (dipóltöltetek vagy infracsapdák kivetése) beszélünk. Fontos az is, hogy ebben az esetben csupán néhány másodperce van például a pilótának, akinek az elektronikai ellentevékenységgel egy időben már meg kell kezdeni a kitérő manővereket is. Ebben az esetben a zavarás hatékonysága ellenőrzésének létjogosultsága minimális, hiszen amennyiben a kitérő manőver sikeres volt, valószínűleg folytatódik a támadás. Az alábbi ábrák bemutatják a kettő folyamat közötti hasonlóságot és különbséget.



1. ábra. A tervezett - védelmi vagy támadó célú - elektronikai zavarás ellentevékenység alkalmazásának folyamata

[2] Targeting, AAP-6 (2011)
[3] Information operations, INFOOPS
[4] Comprehensive Operations Planning Directive, COPD



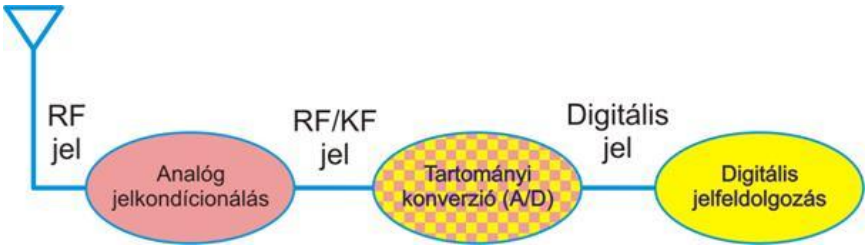
2. ábra. Az „önvédelmi” célú elektronikai ellentevékenység alkalmazásának folyamata

ELEKTRONIKAI ZAVARÁS NAPJAINK KIHÍVÁSAIVAL SZEMBEN

Az elektronikai zavarás napjaink fejlett technológiája miatt számos kihívással szembesül. A zavarandó kommunikációs és rádiólokációs eszközök egyre fejlettebbek, zavarállóságuk is egyre magasabb. Ezen kívül igényként jelent meg más rendszerek elterjedésével azok zavarása is, így például a navigációs rendszerek, infra vagy lézereszközök zavarása.

Napjainkban a kommunikációs eszközök körében jelentős fejlesztések történtek. Megjelentek a kiterjesztett spektrumú adásmódok. Egyre több hadseregben kerül alkalmazásra a szoftverrádió technológia, illetve sok gyártó már foglalkozik kognitív rádióval kapcsolatos fejlesztésekkel is.

A szoftverrádió elve szerint a szoftveresen módosítható paraméterek (pl. frekvenciasáv, hullámforma /modulációs mód/, teljesítmény) változtatásával ugyanaz az eszköz különböző rádióalkalmazásokra vehető igénybe. Az alábbi képen egy digitális vevő felépítése látható, melyben a digitális jelfeldolgozás újraprogramozható hardver elemekkel (FPGA[5]/EPLD[6]), vagy digitális jelfeldolgozó processzorral történik. [2] [3]



3. ábra. Egy digitális vevő általános felépítése [3]

A Harris cég már az 1980-as évek végétől alkalmazza a szoftverrádió technológiát a rádiócsaládjaiban, így a jelenleg a piacon lévő Falcon II and Falcon III rádiócsaládban is. A Rockwell Collins a gyártója az első repülőeszközökön is alkalmazható SDR alapú eszköznek. Természetesen az SDR technológia megtalálható a Rohde & Schwarz, a Thales Communications és más katonai beszállító cégek termékpalettájának eszközeiben is. Arra is találhatunk példát, hogy az egyes országok hadseregei egy adott céggel együttműködve saját szoftverrádiós rendszert fejlesztenek ki. Ilyen például a finn nemzeti SDR program, melynek alapvető követelménye volt, hogy a nagy intenzitású vagy békefenntartó műveletekben történő hatékony alkalmazhatóság mellett a rendszer biztosítsa a katonai, a katasztrófavédelmi és a

[5] Field-programmable gate array, a felhasználás helyén programozható logikai kapumátrix.
[6] Erasable Programmable Logic Device, törölhető programozható logikai eszköz.

nem-kormányzati szervezetek közötti interoperabilitást. A német hadsereg a Rohde & Schwarz céggel szerződött le egy, a követelményeknek megfelelő SDR kifejlesztésére. [4] [5] [6]

Az SDR technológia kiaknázása alig kezdődött meg, már is megjelent egy még fejlettebb szolgáltatást biztosító eszköz, a kognitív rádió. Számos megfogalmazás létezik már a kognitív rádióra, melynek alapgondolata az, hogy az eszköz legyen képes a spektrum figyelésére, a szabad csatornák meghatározására, és szükség esetén a nem használt csatornára történő átváltás lehető leggyorsabb véghezvitelére, így biztosítva az amúgy is zsúfolt frekvenciaspektrum lehető leggazdaságosabb kihasználását. További elgondolásként jelent meg, hogy egy-egy eszköz legyen képes a mért adatok más eszközökkel történő megosztására is. Ez a szoftverrádió elgondolás továbbfejlesztett változata, amelyben az újraprogramozható képesség mellett beépítésre kerül egy független, tanulni képes „intelligens" elem, amely a mért adatokat összehasonlítja a rendszerben tárolt tudásbázissal[7], majd a rendszer végrehajtja a paraméterváltoztatásokat. Fontos az is, hogy alig kezdődött meg a technológia kidolgozása, máris vannak kísérletek annak elektronikai zavarása és a zavarása ellen történő védekezés vonatkozásában. [2] [7] [8]

Mint a fenti példákból látható, jelentős fejlesztésekkel kell felvenni a küzdelmet az elektronikai hadviselési berendezéseknek. Az elektronikai hadviselés területén is lehetséges alternatíva a szoftverrádió technológia alkalmazása, számos egyéb szempont figyelembe vételével. Az alábbi képen a Kerberos cég szoftverrádió alapú elektronikai hadviselési platformja látható, amely képes az adott frekvenciaspektrum megfigyelésére és elektronikai zavarás kivitelezésére is.

4. ábra. KER-314 Elektronikai hadviselési állomás [9]

Azt, hogy mennyire nem esélytelen az elektronikai zavarás még ilyen fejlett technikai környezetben sem, mutatja az is, hogy a szoftverrádió technológia sem érinthetetlen. Az SDR technológián alapuló eszközök elleni támadások többféleképpen csoportosíthatóak. Egyik lehetséges módszer szerint 5 csoportba osztják, ezek az irányítás megszerzése8,

[7] Knowledge base. A szerző fordítása.
[8] Radio control.

megszemélyesítés[9], jogtalan adatmódosítás[10], jogtalan hozzáférés az adathoz[11] és a szolgáltatás megtagadás[12]. [10]

Az irányítás megszerzése esetében a cél, hogy az ellenség megszerezze az irányítást a rádió egy része vagy egésze felett. Ez elérhető rosszindulatú programok SDR rendszerbe való bejuttatásával, rádiófrekvenciás úton vagy közvetlenül az eszközhöz kapcsolódva. Ezen rosszindulatú program működésének célja, hogy az SDR rendszer összteljesítményét rontsa, az átviteli jellemzők lerontásával és az adatvesztés mértékének növelésével. A megszemélyesítés célja, hogy elhitessük az SDR rendszerrel, hogy a mi eszközünk az adott rádióhálóhoz tartozik és jogosult belépni a hálóba. Lényeges, hogy számos rádiórendszer alapból rendelkezik GPS vevő rendszerrel, emiatt fontos megemlíteni az ezen támadási csoportba sorolt GPS spoofing támadást. A GPS spoofing lényege, hogy egy hamis adatot tartalmazó jellel elfedjük a valódi jelet a GPS vevő számára, ennek hatására a vevő rossz pozíciót mutat a felhasználónak. Ilyen jellegű támadásnak főleg a polgári felhasználók eszközei vannak kitéve, a katonai eszközök már védettek ezen támadási forma ellen. A jogtalan adatmódosítás esetében a cél az SDR rendszer által továbbított vagy az azon tárolt adatok megváltoztatása annak érdekében, hogy a rendszert használhatatlanná tegyük, akár a biztonság, akár az üzemképesség vonatkozásában. Ebbe a csoportba soroljuk a hullámforma jellemzőinek megváltoztatását vagy az adott hardverre kifejlesztett trójai programmal történő hardvermódosítások végrehajtását. Az adatokhoz történő jogtalan hozzáférés esetében az adatokhoz való hozzáférés és annak megszerzése a cél, nem pedig azok módosítása. Ebben az esetben például rosszindulatú programok segítségével elérhetjük a rendszerben tárolt érzékeny adatokat. Ebbe a támadási csoportba tartozik a hálózati forgalom figyelése illetve a felhasználók hiszékenységén alapuló social engineering is. A szolgáltatás megtagadás támadás esetében a cél az SDR rendszer elérhetetlenné vagy üzemképtelenné tétele. Ilyen támadások szintén végrehajthatóak rosszindulatú programokkal, de ide soroljuk a túlterheléses támadásokat illetve az elektronikai zavarást is. [10] [11]

A korábbi, nem SDR alapú eszközök esetében a támadás lehetséges formája az eszköz pusztítását vagy az elektronikai zavarás alkalmazását jelentette. Az elektronikai zavarás megvalósítása azonban korunk rádióelektronikai eszközeivel szemben bonyolult feladatot jelent. Az adaptív eszközök megjelenése, a kiterjesztett spektrumú rendszerek alkalmazása az elektronikai zavaró eszközök fejlesztőit jelentős kihívások elé állították.

Példaként alapul véve a frekvenciaugratásos illetve a kognitív rendszereket, láthatjuk, hogy a rádiófrekvenciás jel kisugárzása egy adott frekvencián csak a benntartózkodási ideig tart. Ezután egy korábban meghatározott metódus alapján mind az adó, mind a vevő szinkronban áthangol egy másik frekvenciára. Alapvetően a frekvenciák egy adott frekvenciakészletből kerülnek kiválasztásra, azonban a kognitív rendszerek esetében ez bonyolultabbá válhat, hiszen a rendszer önmaga figyeli a szabad, nem zavart frekvenciákat és a vevővel egyeztetett metódus alapján, akár a korábban meghatározott metódustól eltérően is képes lehet a frekvenciaváltások végrehajtására. Emiatt egyre nehezebb feladattá válhat a hatékony elektronikai zavarás megvalósítása, pedig annak egyéb, korábban már említett jellemzőit még nem is vetettük vizsgálat alá.

Véleményem szerint az SDR technológián alapuló rádióelektronikai eszközök elektronikai zavarásának végrehajtása nem tér el a korábbi rendszereknél alkalmazott módszerektől és eszközöktől. Az elektronikai zavarás tervezése során ideális esetben, az adott eszközt már békeidőben felfedve és megfigyelve, ismerhetjük számos jellemzőjét, azonban figyelembe kell

[9] Personification: megszemélyesítés, azaz annak elhitetése, hogy a behatoló a rendszer egyik eleme. A szerző fordítása.
[10] Unauthorized data modification.
[11] Unauthorized access to data.
[12] Denial of service.

venni azt, hogy a rendelkezésre álló frekvenciakészletnek csak adott része kerül alkalmazásra békeidőben. Ennek figyelembe vételével alapvetően a szélessávú zavarás végrehajtása tűnik megfelelő megoldásnak, azonban ebben az esetben ellenőriznünk kell a kialakítható spektrális teljesítménysűrűség megfelelőségét a zavarni kívánt eszköz vonatkozásában. Ennek érdekében természetesen a lehető legközelebb kell juttatni a zavaróeszközt a zavarni kívánt eszközhöz, ami megoldható pl. egyszeri felhasználású zavaróadók vagy szenzorzavarók telepítésével. Ezen eszközök képesek lehetnek továbbá a zavarás adott időben történő megkezdésére vagy annak megszakítására, a frekvenciatartomány figyelésére és amennyiben, az adott frekvencián tevékenységet észlel, a zavarás újraindítására. Ez egyrészt a zavaróeszköz működési időtartamának növelésére, illetve a szembenálló fél általi felfedés elleni védelemre is szolgál.

ELEKTRONIKAI ZAVARÁS HELYZETE A MAGYAR HONVÉDSÉGBEN

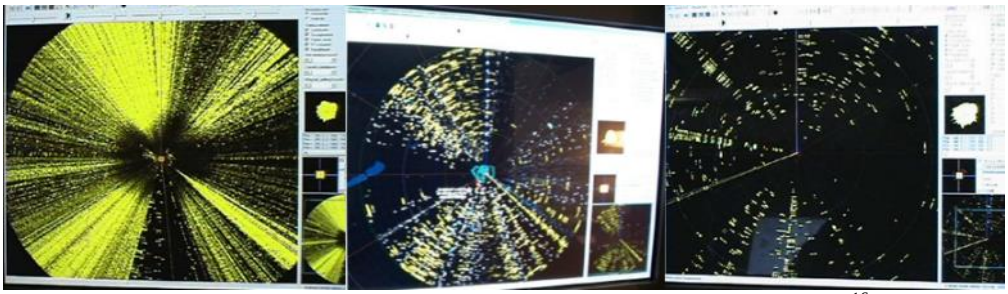
Az MH jelenleg meglévő elektronikai hadviselési képességének bemutatásával már számos cikkíró foglalkozott. Emiatt én csak egy rövid összefoglalást teszek.

Az MH-ban EHV szaktechnikával rendelkező alakulatok közül általában kettő alakulatot szoktak kiemelni. Ezek az MH 5. Bocskai István Lövészdandár kötelékében lévő MH 5/24 Bornemissza Gergely Felderítő Zászlóalj Elektronikai Hadviselés százada illetve az MH 59. Szentgyörgyi Dezső Repülőbázis Elektronikai Hadviselési Támogató Központja.

A szárazföldi haderőnemhez tartozó EHV század fejlesztésére vonatkozóan számos elgondolás létezik. Ezekben szinte minden esetben közös jellemző, hogy a NATO ISTAR elgondolását veszi alapul. Az ISTAR (Intelligence, Surveillance, Target Acquisition and Reconnaissance) az Egységes Felderítő Információgyűjtő Rendszer nevéből képzett mozaikszó, amely központi koordinációval integrálja a felderítő, megfigyelő és célfelderítő eszközöket a felderítés folyamatába. [1]

Az MH 59. Szentgyörgyi Dezső Repülőbázis Elektronikai Hadviselési Támogató Központ esetében most maga a JAS-39 Gripen repülőgép a fontos. A repülőgép önvédelmi célú elektronikai hadviselési rendszerének egyik fontos feladata az ellentevékenység végrehajtása, amely megvalósulhat elektronikai zavarással, illetve dipól vagy infratöltetek kivetésével. [12]

A Magyar Honvédség légierő haderőneméhez tartozó, a NATINAMDS[13] feladatba bevont erői bevonásával évente kerül megrendezésre a NEWFIP[14] elektronikai hadviselési gyakorlat. Az elektronikai zavarást a NATO partner JEWCS[15] repülőgépre szerelhető zavaró konténereivel vagy az általuk üzemeltetett zavaró gépjárművel biztosítják. A gyakorlaton a Gripen repülőgép pilótái, a légi irányítás és a radarállomások személyi állománya gyakorol elektronikai zavarási környezetben. A zavaróeszközök által generált zavarok néhány példája az alábbi ábrán látható. [13]



5. ábra. Aktív zajzavar, aszinkron és szinkron válaszimpulzus-zavar az SzT–68U/M[16] képernyőjén [13]

[13] NATO Integrated Air and Missile Defence System, NATO Integrált Lég- és Rakétavédelmi Rendszer
[14] NATO Electronic Warfare Integration Program
[15] NATO Joint Electronic Warfare Core Staff, JEWCS
[16] SzT-68U/M – Közepes hatótávolságú „D–F" sávú radarállomás.

A Magyar Honvédségnél rendszeresített elektronikai hadviselési eszközök fejlesztésére megfelelő alternatíva az SDR alapú eszközök beszerzése vagy esetleg saját fejlesztése. A saját fejlesztés gondolata semmiképpen nem elvetendő, hiszen már volt korábban is ilyen kezdeményezés, az „Interjam" nevű Integrált elektronikai felderítő és zavaró rendszer fejlesztése. Továbbá elérhetőek olyan magyarországi, tapasztalattal rendelkező cégek, amelyek jelenleg is katonai alkalmazásokkal kapcsolatos fejlesztéseket végeznek. Akár beszerzésről, akár saját fejlesztésről beszélünk, mindenképpen rendszerben kell gondolkodni, nem egy-egy eszköz beszerzésében. Csak és kizárólag így lehetséges annak biztosítása, hogy a jelenleg tapasztalható nehéz gazdasági helyzetben elérhető technikai színvonal emelkedést évekkel, évtizeddel később is ki lehessen használni. Sok gyártó a felderítő és zavaró képesség egy eszközbe történő integrálás irányába indult el, ebben az esetben azonban nagyon fontos a megfelelő irányítás, az elektronikai felderítő és zavarási feladatok közötti egyértelmű és gyors priorizálás rendszerének kialakítása. A rendszernek biztosítania kell a távvezérelhetőséget, egyes elemei lehetnek stabil telepítésűek (pl. az országvédelemre tervezettek), azonban egyes elemeinek mobilnak kell lenniük, megfelelő páncélozottságú hordozóeszközzel. Azt is figyelembe kell venni, hogy a zavaróadók a bekapcsolásuk pillanatától a szembenálló fél célpontlistájára kerülnek. Az önvédelem biztosítása érdekében emiatt települési helyüket folyamatosan változtatniuk kell, ami máris követelményként állítja fel a gyors telepíthetőséget és a hordozóeszköz megfelelő terepjáró képességét is. Továbbá ki kell alakítani egy adatviteli rendszert is, amelyhez megfelelő műholdkapcsolat is szükséges lehet.

KÖVETKEZTETÉSEK

A hatékony elektronikai zavarás feltétele egy fejlett, a kor kihívásainak megfelelni képes eszköz és az ezen eszközökből kialakított rendszer. A tapasztalatok alapján elmondható, hogy ez is egy macska-egér harc, a különböző (kommunikációs, rádiótechnikai, stb.) eszközök fejlődése magában hordozza az azt zavaró eszközök fejlődését és viszont. A Magyar Honvédség számára is szükséges a fejlett elektronikai hadviselési eszközök és az ezekből felépített rendszer megléte, melyhez az SDR technológia megfelelő alapot szolgáltat.

A bemutatott példákból látható, hogy a szoftverrádiós technológia előnyei mellett hátrány is jelentkezik. Ez a hátrány esetünkben a nagyobb sebezhetőség, ami a régebbi eszközökhöz képest jelentős rizikófaktort jelent. Az új típusú, informatikai jellegű fenyegetettség által okozott hibajelenségek felismerésére és elhárítására, illetve az okozott károk megszüntetésére a kezelőállományt fel kell készíteni.

Az informatikai jellegű támadási lehetőségek megjelenése mellett továbbra is számolnunk kell a korábban is alkalmazott támadási lehetőségekkel, a cikk vonatkozásában az elektronikai zavarással. Az elektronikai zavarás végrehajtására a korábban alkalmazott metódusok megfelelőek, természetesen az aktuális hadműveleti helyzetnek megfelelően kiválasztva azokat.

Felhasznált irodalom

[1] Haig Zsolt – Kovács László – Ványa László – Vass Sándor: Elektronikai hadviselés. Budapest, 2014., p. 271. ISBN 978-615-5305-87-0

[2] Bajó József: A nem polgári célú frekvenciagazdálkodás hatékonyságának korlátai, a gazdálkodási hatékonyság fokozásának lehetőségei. Doktori (PhD) értekezés. Budapest, 2006.

[3] Fürjes János: Nagy sávszélességű jelfeldolgozás kihívásai. Hadmérnök, 2007. november 27. ISSN 1788-1919

[4] Jack Browne: Sampling SDRs For Tactical Applications Forrás: http://defenseelectronicsmag.com/systems-amp-subsystems/sampling-sdrs-tactical-applications letöltve: 2014.02.01.

[5] Adam Baddeley: Finland Lays Foundation for National Software-Defined Radio Forrás: http://www.afcea.org/content/?q=node/223 letöltve: 2014.02.01.

[6] German Armed Forces commissions Rohde & Schwarz to develop SDR base unit. Forrás: http://www.rohde-schwarz.us/en/news_events/press/press_releases/press-German_Armed_Forces_commissions_Rohde_%26_Schwarz_to_develop_SDR_base_unit.html letöltve: 2014.02.01.

[7] Charles Clancy, Joe Hecker, Erich Stuntebeck, Tim O'Shea: Applications of machine learning to cognitive radio networks. Forrás: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.145.2762&rep=rep1&type=pdf letöltve: 2014. 05.10.

[8] Beibei Wang, Yongle Wu, K. J. Ray Liu, Fellow, T. Charles Clancy: An Anti-Jamming Stochastic Game for Cognitive Radio Networks. Forrás: http://www.cspl.umd.edu/beibei/Wang_JSAC_draft.pdf letöltve: 2014. 05.10.

[9] KER-314 Electronic Warfare Platform. Forrás: http://www.kerberosinc.com/files/ker314.pdf letöltve: 2014.02.01.

[10] David Fernandes CruzMoura, Fabricio Alves Barbosa da Silva, Juraci Ferreira Galdino: Case Studies of Attacks over AdaptiveModulation Based Tactical Software Defined Radios. Journal of Computer Networks and Communications, Volume 2012. Forrás: http://www.hindawi.com/journals/jcnc/2012/703642/ letöltve: 2014.02.01.

[11] Dr. Haig Zsolt: Az információs társadalom információbiztonsága. Egyetemi jegyzet 2009. Budapest, ZMNE.

[12] Dr. Kovács László: A JAS 39 GRIPEN elektronikai hadviselési képességei. Forrás: http://www.szrfk.hu/rtk/kulonszamok/2006_cikkek/kovacs_laszlo.pdf Letöltve: 2014. 05.10.

[13] Bozsóki Attila: A légvédelmi rakétacsapatok Elektronikai hadviselési felkészítésének tapasztalatai a 2005. évi NATO gyakorlat alapján. Bolyai szemle, 2009. 02. pp: 105-130.