

Horváth József¹

A REPÜLÉSIRÁNYÍTÁS ELEKTRONIKAI ZAVARÁSA²

A világszerte alkalmazásban lévő kommunikációs, navigációs és egyéb elektronikai rendszerek megkönnyítik életünket, állandó használatuk számunkra már természetes. Fontos kiemelni, hogy ezen rendszerek azonban nem sérthetetlenek, a szakemberek számára könnyen támadhatóak. Cikkemben szeretnék egy áttekintést nyújtani az elektronikai zavaróberendezések repülésirányítással kapcsolatos hatásairól. Röviden bemutatom az elektronikai hadviselést, az elektronikai zavarás alapjait, a jogszabályi környezetet, az alkalmazott eszközöket, majd elemzem a repülés érintett területeit és az elektronikai zavarás elleni védekezést.

ELECTRONIC JAMMING OF THE FLIGHT CONTROL

Throughout the world the used communication, navigation and other electronic systems make our everyday life easier, permanent use of these systems is evident for us. Important to highlight, that these systems are not inviolable, for the experts is easy to attack them. In my article I would like to provide an overview about the effect of the electronic jamming systems in connection with the flight control. I describe briefly the electronic warfare, the basic of the electronic jamming, the legal environment, the jammers, and I analyse the affected area of the flight control and the defense against the electronic jamming.

BEVEZETÉS

Az elektronikai zavarást számos területen alkalmazzák, katonai körökben a legismertebb az improvizált robbanóeszközök elleni harc (közismert angol kifejezéssel Counter-Improvised Explosive Device, C-IED), melynél a robbantás mobiltelefonnal vagy egyéb más, rádiófrekvenciás jel vételére alkalmas eszközzel történő indításának megakadályozása a feladat. A polgári életben a leggyakrabban színházi előadások, értekezletek során megszólaló telefonok elnyomására használják. Egyre több forrásból hallható, hogy ezen eszközök megjelentek az iskolákban is a digitális puskázás megakadályozására, például egy német iskolában „Játékelrontó”-nak elnevezett elektronikai zavaróeszközt használnak erre. [1]

Cikkemben az elektronikai zavarás polgári és katonai repülésirányítás elleni alkalmazásának lehetőségeit elemzem. A cikk egyes részeiben ötvöződnek a katonai definíciók és leírások a polgári életben alkalmazottakkal azért, hogy ezzel is elősegítsem a téma könnyebb feldolgozását mindenki számára.

Fontos kiemelni, hogy amennyiben a zavaróeszközöket a repülésirányítás folyamatának megzavarására használják és a repülést irányító, illetve repülőgépet vezető személyzet nincs kellően felkészítve ilyen helyzetekre, súlyos katasztrófa bekövetkezésével és nagymértékű emberáldozattal számolhatunk.

1 mk. őrnagy, MH ÖHP FEF, horvath0101@gmail.com

2 Lektorálta: Prof. Dr. Haig Zsolt mk. zeds, egyetemi tanár, Nemzeti Közszerződési Egyetem, haig.zsolt@uni-nke.hu



I. ELEKTRONIKAI ZAVARÁS

Elektronikai zavarás

„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. Az elektronikai ellentevékenység az elektronikai hadviselés azon területe, amely magába foglalja az elektromágneses és irányított energiák kisugárzását abból a célból, hogy megakadályozza vagy csökkentse az elektromágneses spektrum ellenség által való hatékony használatát. Az elektronikai ellentevékenység egyik területe az elektronikai zavarás. Az elektronikai zavarás az elektromágneses energia szándékos kisugárzását, visszasugárzását vagy visszaverését jelenti azzal a céllal, hogy megakadályozzuk az ellenség elektronikai eszközeinek vagy rendszereinek hatékony működését.” [2]

Az elektronikai zavarással kapcsolatos jogszabályi környezet Magyarországon

Magyarországon a zavaró eszközök körének meghatározása a polgári és katonai alkalmazás vonatkozásában is a haditechnikai eszközök és szolgáltatások kivételének, behozatalának, transzferjének és tranzitjának engedélyezéséről, valamint a vállalkozások tanúsításáról szóló 160/2011. (VIII. 18.) számú Kormányrendelet alapján történik, ahol a jogalkotó a zavaró eszközök közé az alábbi eszközöket sorolja:

„Jelen pont, engedélyezés alá vonja mindazokat a termékeket, eszközöket, technológiákat, szoftvereket, ezek alkatrészeit, és tartozékait, amelyek ezen rendelet XXVI. fejezet 1., 2. és 3. pontjaiban felsorolt eszközök zavarására, működésük felfüggesztésére, illetve lehetetlenné tételére terveztek, állítottak elő, így különösen:

- a) rádiófrekvenciás zavaró adók;*
- b) vezetékes zavaró adók;*
- c) akusztikus zaj generátorok;*
- d) lézer- vagy infravörös sugárzással működő zavaró adók;*
- e) elektronikai eszközök tönkretételére tervezett, előállított berendezések;*
- f) informatikai eszközök zavarására tervezett, előállított eszközök, szoftverek;*
- g) biztonsági rendszerek zavarására tervezett, előállított eszközök.” [3]*

A fenti rendelet meghatározza, hogy mi tartozik a zavaró eszközök közé, azonban az eszközök használatának módját nem.

Ezzel az elektronikus hírközlésről szóló 2003. évi C. törvény foglalkozik az alábbiak szerint:

„Elektronikus hírközlő berendezést, nagyfrekvenciás berendezést, valamint minden olyan berendezést amely működése közben nagyfrekvenciás jelet vagy mellékhatást kelt, továbbá azokat a villamos vagy elektronikus alkatrészeket tartalmazó berendezéseket (a továbbiakban együtt: villamos vagy elektronikus berendezés), amelyek alkalmasak arra, hogy elektromágneses zavart okozzanak, vagy amelyek működésére ilyen zavar hatással



lehet, úgy kell üzemben tartani, hogy az más, zavarérzékenység szempontjából egyébként megfelelő villamos vagy elektronikus berendezés működésében zavart ne okozzon.” [4]

Elektronikai zavartípusok bemutatása

Elektronikai zavar minden olyan jelenség, amely az adott elektronikai vevőeszközökön a hasznos jel vételét akadályozza vagy teljes mértékben meggátolja, esetünkben radarokra és kommunikációs eszközökre vonatkoztatva. Megkülönböztetünk természetes és mesterséges zavarforrásokat. Természetes zavarforrások például a kozmikus sugárzás, a villám és egyéb légköri jelenségek. Mesterséges eredetű zavarforrás az elektromágneses elven működő készülék üzemszerű, vagy hibás működése során keletkező és a környezetbe kijutó jel. Ilyenek pl. a nagyfeszültségű energetikai hálózat, a rádió és TV adók, nagyáramú kapcsolók, motorok, stb. [5] A dolgozatban az aktív eszközökkel létrehozott elektronikai zavarás hatásai kerülnek elemzésre. [6]

Annak mértékét, hogy az elektronikai zavaró jel és a hasznos jel milyen arányban áll egymással, számos tényező befolyásolja. Ezek között vannak adóoldali jellemzők (pl. adó teljesítménye, adó és vevőkészülék közötti szakaszcsillapítás, stb.), vevőoldali jellemzők (vevőantenna nyeresége az adó és a zavaró felé, stb.) illetve a zavaróoldalra vonatkozó jellemzők (zavaróadó teljesítménye, stb.) Az elektronikai zavarokat hatékonyságuk (amelyet a vétel pontjában az elektronikai zavar és a hasznos jel energiaszintjének aránya alapján határoznak meg) alapján három csoportba sorolják, lehet gyenge, közepes és erős. Ennek meghatározásában van segítségünkre a lefogási tényező. A lefogási tényező a vevőeszközön megjelenő hasznos jel és zavaró jel teljesítményének viszonyát adja meg az alábbiak szerint:

$$K = \frac{P_{\text{zavaró jel}}}{P_{\text{hasznos jel}}} \quad (1)$$

K: lefogási tényező, $P_{\text{zavaró jel}}$: zavaró jel teljesítménye, $P_{\text{hasznos jel}}$: hasznos jel teljesítménye

Amennyiben: $K \gg 1$, a zavarás erős, sikeres;

$K = 1$, a zavarás közepes, a zavart eszköz valószínűleg még elegendő hasznos jelszintet vesz a működéséhez;

$K \ll 1$, a zavarás gyenge, nem hatásos, a zavart eszköz biztosan elegendő hasznos jelszintet vesz a működéséhez.

Itt kell megemlíteni a K_z (az adott üzemmódhoz tartozó előírt arány) fogalmát. A K_z értékét a K értékével összehasonlítva megkapjuk, hogy a zavarás valóban sikeres-e. Ez akkor igaz, amennyiben a K értéke nagyobb, mint K_z értéke. [7]

Elektronikai zavaróeszközök

Az elektronikai zavaróeszközök beszerzése többféle szempont alapján lehetséges, attól függően, hogy hol, milyen célra szeretnénk alkalmazni és milyen pénzügyi keretből gazdálkodhatunk. Ezen ismervek alapján válogathatunk a piacon fellelhető számos gyártó egyszerűbb vagy bonyolultabb technikai megoldásokat is alkalmazó, ezáltal több szolgáltatást nyújtó termékei közül. Az egyszerűbb eszközök általában egy fixen beállított frekvencia zavarására képesek

egy be-kikapcsoló gombbal működtetve, míg a jó minőségű eszközök már több frekvenciatartomány zavarására alkalmasak különböző teljesítményű jelet sugározva.

Az elektronikai zavaróeszközök csoportosítása sokféle szempont alapján lehetséges, a cikkben az alábbi - saját tapasztalataimon alapuló - szempontokat vettem figyelembe:

- felhasználói csoportok szerint:
 - polgári célokra készített;
 - katonai és rendvédelmi erők számára készített eszközök.

A két csoport eszközei között nehéz vizsgálni a különbséget, mivel a katonai és rendvédelmi szervek részére szállított eszközök pontos specifikációja nem kerül nyilvánosságra, azt minden szervezet gondosan őrzi. A lényeges az, hogy ezen eszközök a polgári életben is kapható típusok több szolgáltatást nyújtó vagy stabilabb kivitelben készülő változatai, melyeket a gyártó cég a megrendelő igényei alapján módosít.

A polgári célra készített eszközök az alábbiak szerint tovább csoportosíthatóak:

- hordmód/telepítés módja szerint:
 - kézi;
 - hordozható;



1. ábra Hordozható elektronikai zavaróeszköz egy börtönön belül elhelyezve [8]

- gépjárműbe épített;
- fixen telepített eszközök;



2. ábra Fixen telepített elektronikai zavaróeszköz egy börtön külső falánál [9]

- Hatótávolság szerint:
 - kis hatótávolságú (maximum 10 méter);
 - közepes távolságú (maximum 100 méter);
 - nagy hatótávolságú (100-500 méter);

A hatótávolságot számos körülmény (domborzati viszonyok, építmények) befolyásolja.

- Alkalmazási cél (amely a frekvenciatartományt is meghatározza):
 - rádiótelefon zavaró;
 - GPS zavaró;
 - Bluetooth – Wi-Fi zavaró;
 - videó zavaró (pl. kémkamerák);
 - valamint ezek kombinációja;
- Áramellátás módja szerint:
 - elem vagy akkumulátor;
 - hálózati táplálás;
 - gépjármű tápellátó rendszer (esetleg aggregátor);

Az eszközök áramellátásának módja függ az eszközök méretétől és telepítés módjától. Általánosságban elmondható, hogy az elemről vagy akkumulátorról, illetve a hálózatról történő üzemeltetés a legtöbb esetben biztosított.

Katonai és rendvédelmi erők számára készített eszközök elemzése esetén a fenti csoportosítás további szempontokkal bővíthető, így például az alkalmazási célnál megjelenik a rádiótechnikai eszközök zavarása.

II. ELEKTRONIKAI ZAVARÁS A REPÜLÉSIRÁNYÍTÁSBAN

A repülésirányítás elektronikai zavarással történő támadásának realitása

A repülésirányítás ellen irányuló zavarásokra lehet példákat találni, azonban azt nehéz felbecsülni, hogy mennyire reális egy ilyen jellegű támadás végrehajtása. Emiatt ennek lehetőségét nem szabad figyelmen kívül hagyni és a rendszerek fejlesztése esetén a megfelelő védelmet is biztosítani kell.

Nem szándékosan a repülésirányítás ellen irányult annak a gépjárművezetőnek a tevékenysége,



aki egy olcsó zavarókészüléket vásárolt magának – feltehetően rádiótelefonok zavarására – és azt üzemeltette az utazásai során. Azonban amikor a napi útjai során elhaladt a New Jersey-ben lévő Newark repülőtér közelében, eszközével zavarta a repülőtér GPS vevőit. [10]

Napjainkban azonban nemcsak egyedi felhasználók által használt eszközökkel történt zavarásról lehet információt találni, függetlenül attól, hogy az ilyen feladatra alkalmazható eszközök ára, mérete egyre kisebb és az interneten számos helyről beszerezhetőek. Több olyan példa is található, amely azt bizonyítja, hogy az ilyen tevékenységet magasabb szinten elfogadják vagy legalábbis nem tesznek meg minden szükséges lépést annak megszüntetésére.

2012. április 28 és május 6. között ötszáznál is több Dél-Koreába tartó vagy onnan induló repülőgép, valamint 120 hajó is jelezte, hogy GPS készüléke nem volt használható, a jel erősség nulla szintű volt. Dél-Korea állítása szerint a zavaró kisugárzás Észak-Korea egyik határmenti városából történt. Az ilyen jellegű tevékenység emberi életet veszélyeztet közvetlenül. Ez a példa mutatja be valójában azt, hogy mire lehet képes egy ilyen támadás. Amennyiben ezt egy kritikus helyen alkalmazzák, pl. egy szorosban vagy sekély medrű vizeken történő közlekedést gátolják ezzel, nagyon rövid idő alatt jelentős problémát okozhatnak. [11]

Repülésirányítás zavarásának lehetőségei

Az elektronikai zavarás alkalmazásának egyik legnagyobb veszélyt rejtő lehetősége, amennyiben a repülésirányításban alkalmazott frekvenciák ellen használják. Nemcsak az áldozatok valószínűsíthetően magas száma, hanem a támadás által a hozzátartozókra és a közvéleményre kifejtett pszichológiai hatása miatt is.

A repülésirányítás vonatkozásában a kommunikációs rendszerek (irányítótorony – repülőgép személyzet vagy két repülőgép személyzete között), valamint a rádiólokációs rendszerek (földi telepítésű illetve a repülőgépen telepített) vannak veszélyben. A rádiólokációs rendszerek olyan frekvenciatartományokban működnek, amelyek zavarása az interneten beszerezhető egyszerűbb eszközökkel nehezen valósítható meg.

A kommunikációs célú rendszerek elemzésénél fontos, hogy repülőterek által használt frekvenciák megtalálhatóak nyílt forrásokban, mint az a 3. ábrán is látható. A probléma az, hogy hiába titkosított az ezen frekvenciákon folytatott kommunikáció a nagyobb repülőterek esetében, az elektronikai zavarás szempontjából hamar kiismerhetőek a legfontosabb jellemzők.



| Azonosító | Hívójel | Frekvencia |
|-----------|--------------------|------------|
| LHCC | Budapest Control | 133.200 |
| LOVV | Wien Radar | 134.350 |
| LJLA | Ljubljana Radar | 135.275 |
| LDZO | Zagreb Center | 129.650 |
| LYBA | Beograd Center | 135.350 |
| LRBB | Bucharest Radar | 122.025 |
| UKLV | Lvov Center | 128.000 |
| LZBB | Bratislava Control | 134.725 |

| TMA | Magassági határ | Légtér | Irányító | Frekvencia |
|----------|-----------------|--------|----------|---------------------|
| Budapest | 2000 | FL195 | C | LHBP_APP 129.700 |
| Wien | 5500 | FL245 | C | LOWW_APP 128.200 |
| Kosice | 1000 | 9500 | D | LZKZ_APP 119.850 |

3. ábra TMA irányítói frekvenciák és a területi irányító központok elnevezései és frekvenciái [12]

A radarrendszerek rövid elemzéséhez példaként a HungaroControl rendszerét ismertetem, ahol a légiforgalmi irányítók a Magyar Automated and Integrated Air Traffic Control System (a továbbiakban MATIAS) elnevezésű légi navigációs rendszerrel dolgoznak.

Ez a rendszer minden szükséges információt elektronikusan biztosít a légiforgalmi irányítók számára. Rossz látási viszonyok esetén a rendszer részét képező radarberendezések nyújtanak segítséget munkájukhoz, amelyekkel minden, a repülőtér felelősségi területén lévő légi jármű mozgása követhető, legyen az földön vagy levegőben. [13]

„Magyarországon az ellenőrzött légtérben – a többszörös radarfedés követelménye miatt – három helyen működik polgári légtérelenőrző radar. Budapest-Ferihegyen egy közelkörzeti (TAR) radar-komplexum található, amely passzív elsődleges („primer”) és nagy pontosságú, szabványos aktív másodlagos („szekunder”) radarberendezésekből áll. Kőrishelyen és Püspök-ladány mellett egy-egy nagy hatótávolságú primer és szabványos szekunder (MSR) radarberendezés működik. A primer és a szekunder radarantennák azonos tengelyre kerültek felszerelésre, ezért szinkronizáltan együtt forognak, adatfeldolgozó berendezéseik pedig duplikáltak. A „primer” radarok passzív rendszerek, a légi jármű pontos helykoordinátáit (távolságát és oldalszögét) mérik. A „monopulse” másodlagos berendezések a légi járművek fedélzetén elhelyezett válaszjel-adó lekérdezésével az azonosító kódot, a gép által mért magasságot és nagy pontosságú helykoordinátákat küldenek a feldolgozó rendszereknek. Mindhárom radarállomás duplikált radaradat-feldolgozó egységgel rendelkezik, és a feldolgozott információkat nagysebességű modemes és mikrohullámú vonalon keresztül továbbítja az irányító központnak.” [14]

A fenti leírásból kivehető, hogy számos technikai meghibásodás ellen védett a repülésirányítás rendszere és ez valamilyen szinten biztosít zavarás elleni védelmet is, azonban nem elsődlegesen erre a problémára fókuszálnak.

A zavarás megvalósítása

A polgári és katonai repülésirányítással kapcsolatos elektronikai zavarás lehetőségének bemutatására a Magyar Honvédség eszközeinek bevonásával évente megtartott NEWFIP³ keretén belüli gyakorlat tapasztalatait használom fel. Ezen elemzéssel kettő célom van. Egyrészt bemutatom, hogy a NATO erőknél rendelkezésre állnak a hatékony elektronikai zavaráshoz szükséges eszközök, másrészt pedig azt mutatom be, hogy szükséges a polgári és katonai repülésirányítás zavarását vizsgálni, mivel az a megfelelő eszköz birtokában bárki által végrehajtható.

A Magyar Honvédség NATINADS⁴ feladatba bevont erői részvételével megrendezésre kerülő elektronikai hadviselési gyakorlaton az elektronikus zavarást repülőgépekre szerelt zavaró konténerekkel, úgynevezett POD-okkal biztosítják (4. ábra), melyek az előzetes egyeztetések alapján kerültek felprogramozásra. A zavaró POD-ok többféle típusú elektronikus zavar generálására képesek, ezen különböző zavarok radarkijelzőkön látható hatásainak néhány példája a 5. ábrán látható. [15]



4. ábra COBHAM Aviation repülőgépe és a szárny alá függesztett zavarókonténer (POD) [16]



5. ábra Aktív zajzavar, aszinkron és szinkron válaszipulzus-zavar az SzT-68U/M⁵ képernyőjén [17]

A megfelelő paraméterek ismeretében lehetséges a POD-ok beprogramozása hatásos zavarásra, és ha nem is teljes mértékben fogják le a céleszközöket, a kezelők munkáját képesek bonyolulttá tenni.

A fenti példából jól látható, hogy amennyiben a szándék meg van erre, a repülésirányítás rendszere is zavarható, a zavaráshoz szükséges rendszerek megszerezhetőek. Fontos az is, hogy a zavaróeszközök helyének meghatározása egy ilyen tevékenységre felkészületlen szervezetnél esélytelen.

³ NATO Electronic Warfare Integration Program

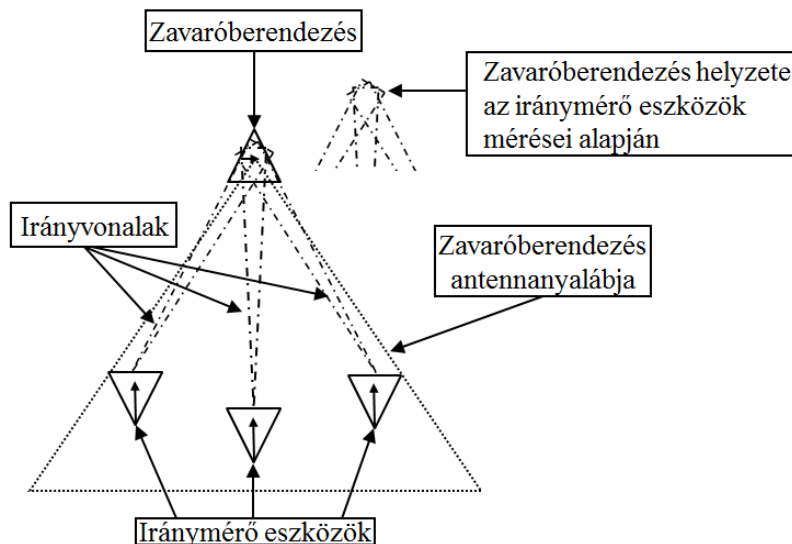
⁴ NATO Integrated Air Defence System

⁵ SzT-68U/M – Közepes hatótávolságú „D-F” sávú radarállomás

Védekezési lehetőségek az elektronikai zavarás ellen

A védekezési lehetőségek egyik lehetséges megoldása az, hogy az elektronikai zavarás észlelésekor a zavarást kibocsátó eszköz megtalálására koncentrálnunk és ehhez szükséges eszközt szerzünk be vagy olyan céget alkalmazunk, amely rendelkezik ilyen eszközzel. A nemzeti frekvenciafelosztás megállapításáról szóló 15/2012. (XII. 29.) Nemzeti Média és Hírközlési Hatóság rendelet 2 §. határozza meg a rádió-iránymérés fogalmát az alábbiak szerint: „olyan rádiómeghatározás, amely a rádióhullámok vételét használja fel valamely állomás vagy tárgy irányának meghatározására. Rádiómeghatározás: valamely tárgy helyének, sebességének vagy más jellemzőinek meghatározása, vagy az ezekre vonatkozó adatok megszerzése a rádióhullámok terjedési sajátosságainak segítségével” [18].

Figyelembe kell venni azt is, hogy a zavaróeszköz pontos helyének meghatározásához 3 felderítő/iránymérő eszköz alkalmazása szükséges, így a háromszögelés módszerével nagy pontossággal meghatározható a zavaróadó helye. Az országok hadseregei számára alapvető fontosságúak ezen eszközök, azonban már a polgári életben is elérhetőek olyan cégek, melyek rendelkeznek ilyen feladatra alkalmas eszközökkel. A 6. ábrán látható, hogy a 3 felderítő/iránymérő eszköz által generált, a zavaróadó felé mutató irányvonal - amelyek azt mutatják meg, hogy a felderítő/iránymérő eszközök a saját helyzetükhöz képest hol érzékelik a zavarás eredőpontját - metszéspontja adja meg a zavaróadó települési helyét. [19], [20]



6. ábra Rádióiránymérés elvi vázlata⁶

Lehetőség van az észlelt zavar jelentésére a Nemzeti Média és Hírközlési Hatóság felé, amelynek illetékes szerve az alábbiak szerint végzi tevékenységét:

„17.1.3.2. Rádióellenőrző és zavarvizsgálati osztály

a. Működteti a mérőszolgálat mobil mérőrendszerekből álló rádióellenőrző és zavarvizsgáló integrált rendszerét.

⁶ Saját szerkesztésű ábra.

- b. Ellenőrzi és felügyeli, saját feladatkörében, valamint a Frekvencia- és azonosítógazdálkodási főosztály felkérésére a polgári rádió-berendezések, rádióállomások és hálózatok engedélynek való megfelelését.*
- c. A KFGH kezdeményezésére elvégzi a nem polgári célú frekvenciagazdálkodásnak a rádiózavar elhárítással, az ellenőrzéssel, a rádiómegfigyeléssel és az adatszolgáltatással kapcsolatos hatósági tevékenységeinek ellátásához szükséges rádió-mérőszolgálati feladatokat.*
- d. Ellenőrzi az üzemben tartott rádióberendezéseket, rádióállomásokat és hálózatokat. Méri és ellenőrzi a műsorszóró szolgáltatás műszaki, minőségi, ellátottsági jellemzőit.*
- e. Méri és ellenőrzi a mobil-szélessávú szolgáltatás műszaki, minőségi és ellátottsági jellemzőit.*
- f. Felderíti és behatárolja az engedély nélküli rádióadásokat. Kivizsgálja a műsorvételi és a rádió-hálózatok közötti zavarokat és intézkedik azok elhárítására.*
- g. EMC méréseket végez a rádiószolgálatok zavarmentes működése érdekében.*
- h. A zavarelhárítás érdekében lefolytatja a törvényben meghatározott hatósági eljárásokat.*
- i. Felkérésre összehangolt méréseket végez a nemzetközi zavarok kivizsgálására és részt vesz rádióellenőrző programok végrehajtásában.” [21]*

A repülésirányítás rendszere támadhatóságának elemzésekor két terület került bemutatásra. Az első a gép/gépek és a torony közötti kommunikáció volt. Ennek zavarása esetén a rendszer kiváltása nehezen valósítható meg, erre alkalmazzák a katonai körökben „chattermark” eljárást, melynek lényege az előzetesen megbeszélte frekvenciák folyamatos változtatása. [22], [23]

A radarrendszerek zavarás esetén történő kiváltása, helyettesítése már könnyebben megválaszolható kérdésnek tűnik, mivel a jelenleg alkalmazott radarok már több frekvencián üzemelnek, megfelelő módon kiépített tartalékrendszerekkel és beépített zavarászűrő berendezésekkel rendelkeznek, azaz hatásos zavarásuk nehéz. Alternatív megoldás lehet az is, hogy a polgári rendszerek zavarása esetén a katonai repülésirányító szolgálat is képes a repülőgépek pontos helyzetének meghatározására, illetve további feladatokban történő segítségnyújtásra.

ÖSSZEGZÉS

A cikk témájául egy, a repülés iránt érdeklődők számára kevésbé látható témát választottam. Ráműtattam arra, hogy a polgári és katonai repülésirányítás elektronikai zavaróeszközökkel történő zavarása megfelelő mérnöki ismeret birtokában végrehajtható, és sajnálatos módon az eszközök beszerzése sem jelent akadályt, hiszen számos internetes oldalon is elérhetőek. A NEWFIP keretén belül szervezett gyakorlat ismertetésével bemutattam, hogy a NATO erők számára a polgári és katonai repülésirányítás zavarásához szükséges eszközök rendelkezésre állnak. Ki kell emelni azt is, hogy az elektronikai zavarás ilyen jellegű alkalmazása leghatásosabban a technikailag kevésbé fejlett helyeken tervezhető, mivel ebben az esetben nem állnak rendelkezésre tartalék rendszerek. Itt olyan területek is szóba jöhetnek például, ahol magyar katonák is teljesítenek szolgálatot (Afganisztán stb). A téma azért is fontos, mert a terrorizmus elleni harc átítatja mindennapjainkat, azonban kijelenthető, hogy szerencsére az elektronikai

zavarás ilyen jellegű felhasználására még nem volt példa és remélhetően nem is lesz.

Az elektronikai zavarás elleni védekezés első lépéseként véleményem szerint a felelős szervezeteknek fokozott figyelmet kell fordítaniuk az elektronikai zavaróeszközök interneten keresztül, jelenleg ellenőrizetlen kereskedelmére. Az elektronikai zavarás hatásainak minimalizálása érdekében pedig nagy hangsúlyt kell fektetni a megelőzésre, ami esetünkben a személyi állomány felkészítését, a már meglévő rendszerek esetében a tartalékrendszerek kialakítását jelenti illetve fontos a védelmi lehetőségek beépítése már a tervezés megfelelő fázisaiban.

FELHASZNÁLT IRODALOM

- [1] Zavaróeszköz az elektronikus puskázás ellen. (2007. 09. 25.) url: http://www.sg.hu/cikkek/55098/zavaroeszkoz_az_elektronikus_puskazas_ellen (2012. 10. 07.)
- [2] Dr. Haig Zsolt alezredes – Dr. Várhegyi István nyá. ezredes: A vezetési hadviselés alapjai. ZMNE, Egyetemi jegyzet, Budapest, 2000.
- [3] 160/2011. (VIII. 18.) számú, a haditechnikai eszközök és szolgáltatások kivitelének, behozatalának, transzferjének és tranzitjának engedélyezéséről, valamint a vállalkozások tanúsításáról szóló Kormány rendelet, XXVI. fejezet 4. pont.
- [4] Az elektronikus hírközlésről szóló 2003. évi C. törvény, 56. § (1) bekezdés.
- [5] Szűcs László: Mérési segédlet RF zavarkibocsátás és zavarérzékenység méréshez. Budapesti Műszaki és Gazdaságtudományi Egyetem, 2011.
- [6] Dr. Haig Zsolt alezredes – Dr. Várhegyi István nyá. ezredes: A vezetési hadviselés alapjai. ZMNE, Egyetemi jegyzet, Budapest, 2000.
- [7] Dr. Ványa László: A pilóta nélküli repülőket fedélzetén alkalmazott zavaró berendezések és a zavarhatékony-ság kérdései. Repüléstudományi közlemények. 2006. 2. szám
- [8] Jammers for prisons. url: <http://www.magnumtelecom.com/Pages/gb/jail.html> (2012. 10. 07.)
- [9] Jammers for prisons. url: <http://www.magnumtelecom.com/Pages/gb/jail.html> (2012. 10. 07.)
- [10] No jam tomorrow. (2011. 03. 11.) url: <http://www.economist.com/node/18304246> (2012. 10. 12.)
- [11] Nagy Balázs András: Kiberháborúba készül Korea? (2012. 05. 12.) url: http://www.mobilityport.hu/hirek/20120512/kiberhaboruba_keszul_korea/ (2012. 10. 12.)
- [12] Kósa Gergely: LHBP APP/CTR kézikönyv. url: http://www.iva.hu/wp-content/uploads/2010/02/ivaohu_atc2.pdf (2012. 10. 13.)
- [13] Hungarocontrol: Technikai háttér. url: <http://iranyitokepzes.hungarocontrol.hu/az-iranyitok-feladata/technikai-hatter> (2012. 10. 07.)
- [14] Hungarocontrol: Radarkorszerűsítés. url: http://www.hungarocontrol.hu/radarkorszerusites?_subid=1 (2012. 10. 07.)
- [15] Bozsóki Attila: A légvédelmi rakétacsapatok Elektronikai hadviselési felkészítésének tapasztalatai a 2005. évi NATO gyakorlat alapján url: http://portal.zmne.hu/download/bjkmk/bsz/bszemle2009/2/08_bozsoki.pdf (2012. 10. 12.)
- [16] NEWFIP 2012 Iron Guard 3 (2012. 06. 21.) url: http://www.jetfly.hu/rovaatok/legter/mh59/galeria/newfip_2012_iron_guard_3/ (2013. 02. 26.)
- [17] Bozsóki Attila: A légvédelmi rakétacsapatok Elektronikai hadviselési felkészítésének tapasztalatai a 2005. évi NATO gyakorlat alapján Bolyai szemle. 2009. XVIII. évf. 2. szám.
- [18] A nemzeti frekvenciafelosztás megállapításáról szóló 15/2012. (XII. 29.) NMHH rendelet
- [19] A nemzeti frekvenciafelosztás megállapításáról szóló 15/2012. (XII. 29.) NMHH rendelet
- [20] Fent Marianne: A rádióiránymérés formaváltozásai hazánkban a rádiótechnika fejlődésének tükrében. 2011. url: http://www.ardf.hu/arc/2010/docs/rim_diplm.pdf (2013. 02. 26.)
- [21] SzMSz a Rádióellenőrző és zavarvizsgáló osztályról. url: <http://nmhh.hu/tart/szervezet/156> (2012. 10. 12.)
- [22] Joint Publication 3-13.1 Electronic Warfare (2007. 01. 25.) url: [http://www.bits.de/NRANEU/others/jp-doctrine/jp3_13_1\(07\).pdf](http://www.bits.de/NRANEU/others/jp-doctrine/jp3_13_1(07).pdf) (2013. 01. 25.)
- [23] Zord Gábor: Aminek van értelme: NEWFIP 09. (2009.11.08) url: http://legiero.blog.hu/2009/11/08/aminek_van_ertelme_newip_09 (2013. 01. 25.)