Horváth József

A REPÜLÉS ELEKTRONIKAI ZAVARÁSÁNAK VALÓS ESETEI

Napjainkban számos helyen olvashatunk, hallhatunk a kritikus, vagy létfontosságú infrastruktúrák védelméről. A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény 1-3. sz. mellékletében meghatározott ágazatok közé tartozik a közlekedés, melynek egyik alágazata a légi közlekedés. A légi közlekedés, mint kritikus infrastruktúra, védelmének számos aspektusa van. Fontos az, hogy nemcsak a napjainkban oly gyakori terrorista cselekmények ellen kell felkészülnünk, de a különböző természeti jelenségek, műszaki okok miatti hatások kiküszöbölésére is. Az egyik ilyen műszaki ok lehet a cikk témájául szolgáló elektronikai zavarás. Jelen cikk a repülőterek, mint kritikus infrastruktúrák, védelme az elektronikai zavarás ellen című kutatásom második része. A cikk célja olyan esetek elemzése, melynek során az elektronikai zavarás került alkalmazásra a légi közlekedés valamely eleme ellen, legyen az radarrendszer vagy kommunikációs rendszer. Figyelembe vettem a globális helymeghatározó rendszer zavarását is, amely szintén fontos a repülés vonatkozásában.

Kulcsszavak: *repülőtér, repülésirányítás, elektronikai zavarás, kritikus infrastruktúra*

A KRITIKUS INFRASTRUKTÚRÁK SÉRÜLÉKENYSÉGE, TÁMADHATÓSÁGA

Kritikus infrastruktúrák

Az Amerikai Egyesült Államok 2001. évi terrorellenes törvényében kritikus infrastruktúrának határozták meg *„mindazon fizikai vagy virtuális rendszereket és berendezéseket, amelyek oly létfontosságúak az Amerikai Egyesült Államok számára, hogy azok korlátozása vagy megsemmisülése meggyengítő hatással lenne a nemzetbiztonságra és a nemzetgazdaság biztonságára, a közegészségre, közbiztonságra vagy ezek bármely kombinációjára”* [1]. Az Európai Unió szerint a kritikus infrastruktúrák *„azok a fizikai eszközök, szolgáltatások, információs technológiai létesítmények, hálózatok és vagyontárgyak, melyek megrongálása vagy elpusztítása súlyos hatással lenne az európaiak egészségére, békéjére, biztonságára vagy gazdasági jólétére, illetve az EU és a tagállamok kormányainak hatékony működésére”*. A NATO Felsőszintű Polgári Veszélyhelyzeti Tervezési Bizottságának meghatározása szerint kritikus infrastruktúrák „*azok a létesítmények, szolgáltatások és információs rendszerek, amelyek olyan létfontosságúak a nemzetek számára, hogy működésképtelenné válásuknak vagy megsemmisülésüknek gyengítő hatása lenne a nemzet biztonságára, a nemzetgazdaságra, a közegészségre, a közbiztonságra es a kormány hatékony működésére.”* [2]

Magyarországon a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény 1-3. sz. mellékletében kerültek meghatározásra azon ágazatok és ezen ágazatok alágazatai, amelyek *„valamelyikébe tartozó eszköz, létesítmény vagy rendszer olyan rendszereleme, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához –, és amelynek kiesése e*

feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna" [3]. Mint már említettem korábban, a légi közlekedés a Közlekedés ágazathoz tartozó alágazat.

A különböző kiemelt, kritikus vagy létfontosságúnak nyilvánított objektumok – közöttük repülőterek, erőművek, energetikai vállalatok, illetve kormányzati és vallási épületek – ellen elkövetett támadásokról számos hírt kapunk napjainkban. Fontos azt is kihangsúlyozni, hogy nemcsak a különböző konfliktusok (pl. Irak, Afganisztán stb.) helyszínein történnek ilyen támadások, hanem egyre gyakoribbak már Európában is. A támadások különböző módon kerülnek kivitelezésre, ezek között megtalálhatóak a fizikai támadások – például robbantásos merényletek – de egyre gyakoribb a kibertámadás is. Sajnálatos módon repülőterek és repülőgépek, vonat és metróállomások, illetve szerelvények is ezen kiemelt célpontok között szerepelnek, hiszen egy-egy sikeres támadásnak jelentős médiaértéke lehet, egyrészt a lehetséges áldozatok magas száma, másrészt pedig az okozható gazdasági kár nagy mértéke miatt. Ezen támadási módszereken kívül számos egyéb módszerrel is lehet akadályozni egy repülőtér működését, ezek között valamelyik alrendszer elleni szabotázzsal, illetve a cikk témájául szolgáló elektronikai zavarással.

Az elektronikai hadviselés az utóbbi években, évtizedekben rendkívüli változásokon ment keresztül. Ennek oka, hogy az elektromágneses spektrumot külön műveleti színtérnek ismerik el, új és veszélyes irányított fegyverek jelentek meg, amelyekben jelentős mennyiségű elektronikai elem van jelen, melyek befolyásolják a pontosságát és a halálosságát ezen fegyvereknek [4]. Az elektronikai zavarás az elektronikai hadviselés három funkciója közül az elektronikai ellentevékenységnek egyik eleme. Fontos azt megjegyezni, hogy az elektronikai hadviselés – véleményem szerint – mint a megnevezése is mutatja, alapvetően katonai tevékenység, azonban az elektronikai zavarás alkalmazása az internet világában beszerezhető elektronikai zavaróeszközök tükrében mindenképpen elemzésre váró probléma. Az elektronikai zavarás elméleti megvalósíthatóságával egy korábbi cikkemben már foglalkoztam [5], jelen cikkben a megtörtént események alapján elemzem az alkalmazás módszereit.

Az elektronikai zavarás légi közlekedés elleni alkalmazása történhet szándékosan és nem szándékosan. A cikk későbbi fejezetében mindkettőre számos példát fogok bemutatni. Bár jelenleg a nem szándékos esetek vannak többségben, mindenképpen figyelembe kell venni, mint szándékos támadási lehetőséget is. Ennek oka az, hogy a terrorista szervezetek folyamatosan tanulnak, újabb és újabb támadási metódusokat alkalmaznak, a zavaróeszközök pedig viszonylag kis méretűek és rendkívül könnyen elérhetőek az interneten. Több eszköz telepítése, időszakos, vagy rendszertelen működtetése pedig a telepítési helyek felfedését rendkívül megnehezíti. Az új támadási eljárások között meg kell említeni a 2001. szeptember 11-i támadássorozatot, amely repülőgépek eltérítésével különböző amerikai célpontok – így New York-i Világkereskedelmi Központ[1], a Pentagon és a Fehér Ház – ellen irányult [6]. Továbbá fontos és szintén újszerű támadás volt az iráni ipari létesítmények ellen 2010-ben végrehajtott számítógépes támadás, melynek során a létesítmények számítógépeit a Stuxnet vírussal fertőzték meg. Egy iráni szakértő szerint mintegy 30 ezer számítógép volt érintett az incidensben. A Symantec biztonsági cég szerint a program *„ipari létesítmények irányításának átvételére és adataik külföldre továbbítására is alkalmas"*. Mivel a vírus nem személyes adatok

[1] World Trade Center

megszerzésére vagy levélszemét terjesztésére, hanem komoly védelemmel rendelkező ipari rendszerek feletti irányítás átvételére szolgál, a Kaspersky Lab számítógép-biztonsági cég alapítója szerint *„egy új korszak: a kiberterrorizmus, a kiberfegyverek és a kiberháború korának nyitányáról”* beszélhetünk. [7] Tovább nem szabad elfelejtenünk a drónok bevetését a robbanóanyag célterület felé juttatásának céljából.

Fontos azonban az is, hogy az elektronikai zavarást és az interferenciát ne tévesszük össze. Interferencia okozta baleset történhetett 2000. január 07-én, a svájci Kloten repülőtér mellett, amikor a Zürich–Drezda menetrendszerinti járat a felszállást követően indokolatlan jobb fordulatot tett, majd a következő ilyen fordulónál meredek süllyedésbe kezdett. A személyzet nem tudott korrigálni, a 3 fő személyzet és a 7 fő utas meghalt. A vizsgálat szerint valószínűsíthetően egy utas tiltott mobilhasználata okozhatott zavart a repülőgép fedélzeti rendszerében [8].

Repülőterek, repülésirányítás sérülékenysége, támadhatósága

Amikor a repülőterek és repülésirányítás sérülékenységét vizsgáljuk, számos természetes és mesterséges okot lehet felsorolni. Az Európai Uniós Hálózat- és Információbiztonsági Ügynökség[2] a repülőterek működését befolyásoló veszélyeket öt csoportba sorolta. Ezen csoportok az alábbiak:

- emberi hibák, melyek lehetnek:
  - konfigurációs hibák;
  - felhasználói hibák;
  - hardware elvesztése;
  - irányelvek, előírások figyelmen kívül hagyása.
- harmadik fél által okozott hibák, melyek lehetnek:
  - internet szolgáltatói hiba;
  - felhő szolgáltatói hiba;
  - közmű szolgáltatói hiba (gáz, villany, víz);
  - távoli karbantartást végző szolgáltató hibája;
  - biztonsági auditálást végző szolgáltató hibája;
- - rosszindulatú tevékenységek, melyek lehetnek:
  - túlterheléses támadás (Denial of Service (DoS));
  - szoftverhiba kiaknázása;
  - jogok/jogosultságok nem megfelelő használata;
  - hálózati behatolás/támadás;
  - pszichológiai támadás (social engineering);
  - lehallgatás eszközökkel;
  - fizikai hozzáférés;
  - rosszindulatú szoftverek az informatikai eszközökön (beleértve a személyzet és az utasok eszközeit is;
  - fizikai támadás a repülőtér elemei ellen;
- rendszerhibák, melyek lehetnek:
  - eszköz vagy rendszer hibája, vagy helytelen működése;
  - kommunikációs linkek hibája vagy zavara;

[2] European Union Agency For Network And Information Security, ENISA

- eszközök elemeinek hibája, vagy helytelen működése;
- a fő ellátás hibája vagy zavara;
- energiaellátás hibája vagy zavara;
- hardware vagy szoftverhiba;

✈ egyéb okok, melyek lehetnek:

- természeti jelenségek: földrengés, áradás, napkitörés, vulkáni tevékenység, űrhulladék és meteorit;
- ipari eredetű: nukleáris baleset, ipari tevékenység, veszélyes kémiai incidensek;
- egyéb: járványok, tűz [9].

Az ICAO a szándékos támadási metódusokat az alábbiak szerint azonosította:

✈ *„civil légijármű tömegpusztító fegyverként történő felhasználása;*
✈ *öngyilkos merényletek a levegőben és a földi létesítményekben;*
✈ *elektronikus támadások: rádió adóvevő készülékek és egyéb eszközök alkalmazása annak érdekében, hogy azokkal megzavarják, interferenciába lépjenek a földi vagy légi navigációs, irányító, ellenőrző rendszerekkel;*
✈ *számítógépes támadások, melyek blokkolják, vagy megváltoztatják a légi kommunikációt;*
✈ *vegyi-, biológiai támadások utasok ellen, nukleáris és egyéb radioaktív anyagokkal való visszaélés, valamint*
✈ *légvédelmi rakétákkal történő támadás repülőgépek ellen.”*[10]

1. ábra Az Eyjafjöll izlandi vulkán 2010. évi kitöréséből származó hamufelhő által megtett út[3]

A természeti okok egyik napjainkban többször is hallható típusa a vulkáni hamu okozta probléma. A vulkáni hamu esetében fontos az is, hogy hamu mennyisége a kitörés időtartamától, terjedése pedig a az időjárási körülményektől nagy mértékben függ. A hamu a terjedés és a

[3] Szerkesztette a szerző.

mennyiség függvényében a vulkántól távolabb lévő repülőterek működését is negatívan befolyásolhatja. Az Eyjafjöll izlandi vulkán 2010. évi kitöréséből származó hamufelhő miatt számos európai repülőtér ideiglenesen bezárásra került, egy napra Magyarországon is légtérzárat rendeltek el. Az 1. számú ábrán látható, hogy a hamufelhő a müncheni repülőtérig kb. 2570 km, Budapestig pedig kb. 2940 km utat tett meg [11].

Támadási módszerek

Amikor a repülés elleni támadásokról beszélünk, általában a repülőtéren lévő utasok, a repülőtéri infrastruktúra, illetve a repülőgépek elleni támadásokról beszélhetünk. Ezen támadások többféle módon kivitelezhetőek, sajnálatos módon számos incidens történt már napjainkig.

Ernszt Ildikó A Nemzetközi légiközlekedés védelme című könyvében a légi terrorizmussal kapcsolatban az alábbi cselekményeket határozta meg, mint elkövetési módokat:

- *„repülőgép eltérítés;*
- *repülőterek elleni támadás;*
- *repülőgépek felrobbantása;*
- *repülőterek kiszolgáló területei elleni támadások;*
- *repülőgépek lelövése;*
- *egyéb, gépek ellen elkövetett bűncselekmények, incidensek, szabotázs akciók."* [12]

A következő alpontokban a napjainkra legjellemzőbb három támadási módszerrel foglalkozom, ezek a fizikai támadás, a kibertámadás és az elektronikai zavarás.

Fizikai támadás

A támadások során különböző típusú fegyvereket alkalmaztak, lőfegyvereket, robbanóeszközöket, de előfordult késsel végrehajtott támadás is. Azaz ezen esetekben nem az infrastruktúra, hanem az ott tartózkodó emberek voltak a célpontok, a repülőtéri infrastruktúrában bekövetkezett károk másodlagos károk voltak.

l972. május 30-án az izraeli Lod repülőterén a Népi Front Palesztina Felszabadításáért[4] nevű palesztin szervezethez rendkívül közel álló terrorista csoport tagjai gépfegyverekkel és kézigránátokkal felszerelkezve támadtak rá várakozókra, megölve 26 embert, további nyolcvanat megsebesítve. 1975. december 29-én New York LaGuardia repterén történ nagy erejű robbanás, 11 ember meghalt, 74-en pedig súlyosan megsérültek. A nyomozás során nem sikerült megtalálni sem az elkövetőket, sem a támadás okát. Ebben az esetben bizonyított, hogy a halottak és sérültek többségét nem a detonáció, hanem a közeli szekrények szétrepülő törmelékei okozták. A robbanás során a plafonról egy a 3×5 méteres vasbeton elem is leszakadt. 1982. augusztus 7-én az Ankarától 28 kilométerre északkeletre található Esenboğa nemzetközi repülőtéren a Titkos Örmény Hadsereg Örményország Felszabadítására[5] nevű terrorszervezet tagjai robbantottak bombát és nyitottak tüzet az ott lévő emberekre, közülük megölve kilenc, megsebesítve hetvenkettő embert. 1983. július 25-én az Orly repülőtéren hajtott végre robbantást az ASALA, amiben nyolcan meghaltak, ötvenöten megsérültek. Az elkövető elmondása szerint a repülőgépet szerette volna felrobbantani, ám a pokolgép korán lépett működésbe. 1985. december 27-én

[4] Popular Front for the Liberation of Palestine, PFLP
[5] Armenian Secret Army for the Liberation of Armenia, ASALA

reggel Bécsben és Rómában történt támadás. A római Fiumicino nemzetközi repülőtéren négy arab fegyveres nyitott tüzet és dobott kézigránátokat a várakozó utasokra, megölve 16, megsebesítve 99 embert. A Bécs-Schwechat-i nemzetközi repülőtéren három arab terrorista kézigránátokkal megölt kettő és megsebesített 39 embert [13].

A már említett Orly repülőtéren 1975–2017. között hat támadást követtek el, amelyek számos áldozatot és sérültet követeltek. A támadások közül három alkalommal palesztinok támadtak izraeli repülőgépet vagy csoportot. A legutolsó támadás során, a tunéziai származású, de francia állampolgárságú elkövetőt lelőtték, más nem sérült meg az incidensben [14][15].

A repülőgépek és repülőterek ellen elkövetett támadások közül mindenképpen meg kell említeni a 2001. szeptember 11-i, az Amerikai Egyesült Államok ellen elkövetett repülőgép eltérítéses támadást, melynek során több repülőgép eltérítésével amerikai célpontokat terveztek támadni. 2016. márciusában Brüsszelben kettő robbantás történt a repülőtéren, egy pedig az egyik metróállomáson, a három támadás során megölve mintegy 30 embert. Ugyanezen év júniusában az isztambuli repülőtéren 3 terrorista lövöldözött, majd felrobbantotta magát megölve 42 és megsebesítve 239 embert. Szintén ebben a hónapban számítógépes támadás érte a varsói Chopin repülőtér egyik alrendszerét. 2017. márciusában az Orly-i repülőtéren történt pisztolyos támadás során csak az elkövető halt meg. A fentieken kívül számos más helyen és módon is követtek el támadásokat. Ezekben a támadásokban alapvetően a minél nagyobb emberi áldozat volt a cél, nem az infrastruktúra elleni támadás. Azonban a támadások során – elsődlegesen a robbantásos merényletek során – természetesen sérült repülőtéri infrastruktúra is. A fentieken kívül számos támadás történt még a világ különböző repülőterein, vagy azok közvetlen közelében. 2011. január 24-én Moszkvában, a Domogyedovói repülőtéren öngyilkos merénylet során 37 ember vesztette életét. 2012. július 18-án Bulgáriában, a burgaszi repülőtéren egy buszon robbantotta fel magát az elkövető, megölve hat embert. 2016. június 28-án az isztambuli Atatürk repülőtér bejáratánál történt merénylet. Ennek a merényletnek 45 halottja volt, annak ellenére, hogy a repülőtérre nem tudtak bejutni, a biztonsági szervezetek feltartóztatták őket [16].

Mint a fenti példák is mutatják, számos támadás történt eddig és várhatóan fog még történni a jövőben is a repülőterek ellen. Ezen tragikus események során jelentős emberáldozatokkal kell számolnunk. Az emberáldozatok miatt nagy hírértéke van ezen támadásoknak, illetve a lakosságban is komoly nyomokat hagy, jelentősen csökkentve a biztonságérzetünket. Gazdasági hatásként jelentkezik, hogy az emberek csökkent biztonságérzete miatt csökken az utasforgalom is.

Kibertámadás

Napjainkban a repülőtereken – hasonlóan az élet más területeihez – egyre növekvő mértékű az informatikai eszközök és rendszerek alkalmazása. Emiatt sajnálatos módon egyre nagyobb figyelmet kell szentelnünk a hackertámadások elleni védelemre a repülőterek vonatkozásában is. Az alábbiakban az eddig ismertté vált hackertámadások közül mutatok be néhányat.

1. Belgium, Brüsszel, Zaventem nemzetközi repülőtér elleni hackertámadás (2016.)

2016. március 22-én, órákkal az előző pontban említett, számos emberáldozatot követő öngyilkos robbantásos merénylet után egy Pittsburgh-i tinédzser hackertámadást indított a repülőtér weboldala ellen. A nyomozás szerint nem terrorista szándék vezérelte a fiatal tettét [17].

2. Lengyelország, Varsó, Chopin repülőtér elleni hackertámadás (2016.)

2016 júniusában a varsói Chopin repülőtéren a repülőgépek földi kiszolgálását támogató informatikai rendszert kibertámadás érte. A kibertámadás miatt 10 járatot kellett törölni, ami mintegy 1400 utast érintett [18].

3. Vietnám, Ho Si Minh-város - Son Nhat és Hanoi - Noi Bai repülőterek elleni hackertámadás (2016.)

2016 júliusában mintegy 100 repülőgép menetrendjét befolyásolta a Ho Si Minh-városban található Son Nhat és a Hanoi-ban található Noi Bai repülőterek elleni hackertámadás. A támadások során a repülőterek üzemeltetésében kritikus rendszerelemekhez nem fértek hozzá a hackerek, csak a repülőgépek indulását és érkezését mutató kijelzők váltak használhatatlanná, illetve a „check-in" rendszer működésképtelensége miatti manuális jegykezelés eredményeképpen alakultak ki járatkésések [19].

4. Ukrajna, Kijev, Boryspil nemzetközi repülőtér elleni hackertámadás (2017.)

2017. júniusában Ukrajna számos állami szervezete mellett hackertámadás ért egy dániai hajózási vállalatot és több orosz energiaszektor több vállalatát. Ukrajnában kormányzati szervek, az ukrán Nemzeti Bank és más nemzeti hitelintézetek, az ukrán Posta, a Csernobil zárt zóna, valamint a Kijevben található Boryspil nemzetközi repülőtér is a célpontok között szerepelt. Ebben az esetben azonban nem a repülőtér kritikus elemeinek működése került akadályoztatásra, hanem „csak" a hivatalos weboldal vált elérhetetlenné és repülőgépek indulását és érkezését mutató kijelzők nem működtek [20].

5. A fedélzeti rendszer támadása a repülés során.

Számos forrásban olvasható, hogy a repülőgép rendszerébe történő behatolásra történtek már próbálkozások. Az egyik ilyen esettel kapcsolatban a Boeing kijelentette, hogy a repülőgép utasainak szórakoztatására kialakított rendszer független a repülőgép repülési és navigációs rendszereitől, azaz hamisak azon kijelentések, hogy azon keresztül támadhatóak a létfontosságú rendszerek. Mindenképpen fontos tény azonban az, hogy az IoActive – amely egy különböző védelmi megoldásokkal foglalkozó cég és amely képes volt egy autó számítógépes rendszerét menetközben feltörni – szintén olyan figyelmeztetést adott ki, miszerint egy ilyen támadás sikeresen kivitelezhető [21][22].

Elektronikai zavarás

Az alábbi esetek elemzéseiben az elektronikai zavarás repülőterek vagy repüléssel kapcsolatos tevékenységek elleni alkalmazását mutatom be. Ezen példák a különböző incidensek jellemző esetei:

- elektronikai zavarás szándékos alkalmazása a polgári rendszerek ellen;
- az elektronikai zavarás szándékos alkalmazása katonai vagy más rendvédelmi feladatok során, mellyel nem szándékosan, de negatívan befolyásolták a polgári rendszerek működését;
- polgári személy által használt elektronikai zavaró eszköz negatív hatása a polgári rendszerekre.

A példák között bemutatok egy olyan esetet is, amely közvetve kapcsolódik az elektronikai hadviseléshez, azonban a kiváltó ok egy technikai meghibásodás volt.

Mint említettem, ezen esetek csak mintaként bemutatott incidensek, ezeknél jóval nagyobb számú, valamilyen zavaráshoz kötődő eseményről érhető el leírás a különböző adatbázisokban. Az amerikai kormányzat, az amerikai repülési szervezetek és cégek, valamint a repülésben dolgozó személyek (pilóták, légiirányítók stb.) által üzemeltett, 1976-ban létrehozott Légi közlekedési Biztonsági Jelentési Rendszer[6] adatbázisában 2018. 01. 27-én a „jamming" kereső szó alkalmazásával 141 találatot kaptam, melyekből a legelső egy 1989. januári, a legutóbbi pedig egy 2017. októberi bejegyzés volt. Az eredményként kapott találatok közül nem mindegyik kapcsolódik az elektronikai zavaráshoz, van, amelyik esetében ismeretlen a kiváltó ok, illetve található olyan is, amelyek esetében két, egyéb rendszer közötti interferencia volt a probléma. A már említett első esetnél a bejelentést adó pilóta a Texas államban található Corpus Christi nemzetközi repülőtérnél észlelte a LORAN (Long Range Aid to Navigation, Távoli navigációs segítség) rendszer megbízhatatlanságát. A jelentésben rögzítette, hogy saját nyomozásának eredménye szerint az amerikai Kábítószer-ellenes Hivatal (Drug Enforcement Administration, DEA) alkalmazta az elektronikai zavarást annak érdekében, hogy az alacsonyan repülő kábítószer kereskedők repülését akadályozza. 2017-ben öt alkalommal rögzítettek elektronikai zavarással kapcsolatos esetet, melyek közül:

- három esetben egyértelműen GPS[7] zavarásról szól a jelentés;
- egy esetben GPS zavarásról/kiesésről szól a jelentés;
- egy esetben radarzavarást említenek a szöveges leírásban, azonban a végső következtetésben már GPS zavarás szerepel [24].

1. Haditengerészet zavarta San Diego elektronikai rendszereit (2007.)

2. ábra Az elektronikai zavarás helyszínei a San Diegói incidens vonatkozásában[8]

[6] Aviation Safety Reporting System, ASRS

[7] Az amerikai fejlesztésű globális műholdas helymeghatározó rendszer elnevezése, Navigation System with Timing and Ranging Global Positioning System, NAVSTAR GPS

[8] Szerkesztette a szerző.

2007 januárjában számos szervezet és a lakosság furcsa jelenségeket tapasztalt San Diegóban. A repülőtér repülésirányítói nem tudták a repülőgépek mozgását követni, a közeli Haditengerészeti Egészségügyi Központban nem működtek a vészhelyzeti személyhívók, melyeket az ügyeletes orvosok értesítésére alkalmaztak. ezen felül nem működött a kikötő közlekedés irányító rendszere, a mobiltelefonokon nem volt térerő, és az emberek nem tudtak pénzt felvenni a bankjegykiadó automatákból. A fenti jelenségeket mintegy kettő órán keresztül észlelték. Három napig tartott, míg sikerült megtalálni a probléma okát. A fenti időszakban a kettő hadihajó gyakorlatot hajtott végre, melynek során a rádiójeleket zavarták. Emellett nem szándékosan, de zavarták a GPS[9] jeleket is a város nagy részében [25][26].

2. Kaminonsofőr zavarta a newark-i Liberty nemzetközi repülőtér működését (2009.)

2009-ben a Newark-ban (New Jersey állam) található Liberty nemzetközi repülőtéren a mérnökök azt tapasztalták, hogy időnként a globális műholdas helymeghatározási rendszerek (a továbbiakban GNSS[10]) jeleinek vétele akadályozva van. Két hónapig tartott, mire a Szövetségi Repülésügyi Hivatal[11] szakembereinek sikerült megoldania a problémát: egy kamionsofőrnek, aki naponta a repülőtér közelében közlekedett, egy olcsó GNSS zavaróeszköz volt a birtokában. A célja a zavaróeszköz alkalmazásával az volt, hogy a főnöke ne legyen képes nyomon követni a mozgását [27].

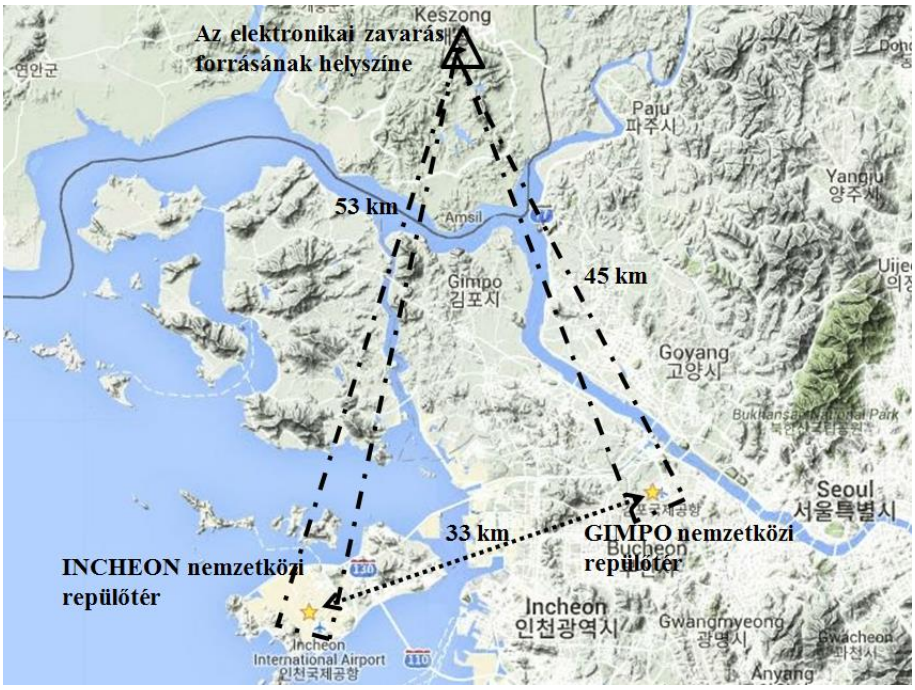
3. Újabb kaminonsofőr zavarta a newark-i Liberty nemzetközi repülőtér működését (2012.)

2012 augusztusában hasonló incidens játszódott le ugyanezen repülőtér vonatkozásában. Ebben az esetben már a zavarbejelentés másnapján bemérték a kamionsofőrt, aki szintén a munkaadója elől akart elrejtőzni a zavaró eszköz alkalmazásával. Miután a Szövetségi Hivatal szakemberei beazonosították és elfogták, 32.000 dolláros büntetést kapott, illetve állásából is elbocsátották. [28] A hivatkozott cikk szerzője visszautal a 2009-ben történt incidensre, így bár nagyon hasonló a két esemény, kizárható, hogy egyazon esetről van szó.

4. Észak-Korea zavarja Dél-Korea légi navigációját (2012.)

Dél-Korea Szárazföldi, Szállítási és Tengerészeti Minisztériumának[12] bejelentése alapján 2012. április 28-ától Észak-Korea több alkalommal zavarta a navigációhoz szükséges GNSS jeleket, amellyel több, mint 250 repülőgép repülését, navigációját nehezítette meg. Az incidensben érintve voltak a Dél-Korea, Japán és Thaiföld légitársaságai, de például a FedEx vállalat is. A repülőgépek a dél-koreai Incheon és Gimpo repülőterekről szálltak fel, vagy szálltak le oda. A zavarás ellenére a repülőgépek képesek voltak baleset nélkül folytatni útjukat. A dél-koreai bejelentésben az elektronikai zavarás forrásának helyszíneként a 3. sz. ábrán jelölt Kaesong területet adták meg [29].

[9] Ebben az esetben vélelmezhetően valóban a NAVSTAR GPS zavarása történt.
[10] A globális helymeghatározó rendszerek esetében gyűjtőnévként általában a GPS megnevezést alkalmazzák, amely azonban az amerikai fejlesztésű rendszer (Navigation System with Timing and Ranging Global Positioning System, NAVSTAR GPS) neve. A globális helymeghatározó rendszer neve helyesen alkalmazva Global Navigation Satellite Systems (GNSS). A négy legnagyobb GNSS rendszer az amerikai NAVSTAR GPS, az orosz GLONASS, az Európai Unió által fejlesztett GALILEO és a kínai COMPASS
[11] Federal Aviation Authority
[12] South Korea's Land, Transport and Maritime Affairs Ministry



3. ábra Az elektronikai zavarás helyszínei az észak-koreai és dél-koreai incidens esetében[13]

5. NATO elektronikai hadviselés gyakorlat (2014.)

A NATO Integrált Lég- és Rakétavédelmi Rendszer[14] (a továbbiakban NATINAMDS) részét képező országokban évente kerül megrendezésre a NATO által biztosított Elektronikai Hadviselési Integrációs Program (NATO Electronic Warfare Integration Program, a továbbiakban NEWFIP) elnevezésű többnemzeti elektronikai hadviselési gyakorlat. A gyakorlat célja a NATINAMDS részét képező államok részére elektronikai zavarási környezetet képezni annak érdekében, hogy a szükséges elektronikai ellentevékenységi eljárásokat begyakorolják. A Magyar Honvédség ezen gyakorlaton történő részvételének aktív szervezője vagyok 2012. év óta. A Magyar Honvédség alakulatai közül a feladatban érintettek az MH 12. Arrabona Légvédelmi Rakétaezred, az MH 54. Veszprém Radarezred, az MH Légi Vezetési és Irányítási Központ és az MH 59. Szentgyörgyi Dezső Repülőbázis.

A Magyar Honvédség gyakorlaton résztvevő haditechnikai eszközei ellen az elektronikai zavarást a NATO szerződött partnerei, a COBHAM Aviation és a NATO JEWCS (Joint Electronic Warfare Core Staff) saját technikai eszközeivel biztosítja.

A COBHAM Aviation egy számos – repüléssel kapcsolatos – szolgáltatást nyújtó vállalat, amely Dassault Falcon 20 repülőgéppel képes az elektronikai hadviselési képzések kivitelezésére. A repülőgéppel és a gépre szerelt konténerekkel (úgynevezett POD-okkal) képesek radarzavarást, kommunikációs zavarást biztosítani és – különböző hatásos radar keresztmetszetet[15] biztosító vontatott céllal – hamis célokat imitálni [30].

[13] Szerkesztette a szerző.
[14] NATO Integrated Air and Missile Defence, NATINAMDS
[15] Radar Cross Section, RCS

1. kép Zavarókonténer a Dassault Falcon 20 repülőgép szárnya alatt [30]

A JEWCS a NATO részére elektronikai hadviselés tapasztalatot, támogatást és kiképzést nyújt gyakorlatok és műveletek alatt. Mint a 2. számú képen látható, a JEWCS repülőgépre függeszthető zavarókonténerekkel, szimulátorokkal, önjáró és vontatható zavaróeszközökkel rendelkezik [31].

2. kép A JEWCS elektronikai hadviselési technikai eszközei [16] [31]

A fenti eszközökkel mindkettő szervezet képes a repülőgépek fedélzeti és a légtérellenőrzés földre telepített radarjainak, valamint a pilóta és a légiirányító közötti kommunikáció zavarására.

2014. június 05-én és 10-én számos, a különböző forrásokban eltérő – de minden esetben több tízes nagyságrendű – számú repülőgép tűnt el az ausztriai, a cseh, a szlovák és dél-német repülésirányítás kijelzőiről. A repülőgépek és utasaik az elérhető nyilatkozatok alapján nem voltak veszélyben, a repülőgépek és a repülésirányítás között a rádión keresztüli kommunikáció minden esetben zavartalan maradt. A 2014. június 05-i technikai probléma ideje alatt Magyarországon folyamatban volt a NEWFIP gyakorlat, emiatt számos helyen felvetődött annak gyanúja, hogy ezt a problémát a folyamatban lévő elektronikai hadviselés gyakorlat okozta. A vádat kérdésessé tette azonban, hogy a második hibajelenség időpontjára már befejeződött ez a gyakorlat [32][33][34].

[16] A repülőgép nem a JEWCS eszközrendszer része.

Természetesen számos vizsgálat indult az ügyben, és mint kiderült, nem az elektronikai hadviselés gyakorlat volt a probléma okozója. A problémát Patrick Ky, az Európai Repülésbiztonsági Ügynökség[17] vezérigazgatója által adott nyilatkozat szerint egy, a többszörösen átfedett radarrendszer egyik radarján végzett teszt okozta [35].

6. Svéd repülésirányítás zavarása (2015.)

2015. november 04-én Svédország a repülésirányítási rendszerében támadást érzékelt, egyes források szerint orosz állami hackertámadás érte három repülőterüket. Más források szerint nemcsak repülőterek, hanem több más célpont mellett például Svédország legnagyobb energetikai vállalata is támadást szenvedett. A támadások kivitelezése az Oroszországi Föderáció Fegyveres Erői Vezérkarának Felderítő Főcsoportfőnökségéhez[18] köthető. A támadás eredményeképpen a légiirányítók képtelenek voltak használni számítógépes rendszerüket, emiatt számos helyközi és nemzetközi repülőjárat törlésre került. A támadás tényéről – annak ellenére, hogy nem NATO tagállam – Svédország tájékoztatta a NATO-t és a szomszédos államokat, Norvégiát és Dániát. A probléma lehetséges okaként a Svéd Polgári Repülési Ügynökség az ebben az időszakban tapasztalt napkitörést jelölte meg. Más források viszont azt vélelmezik, hogy Oroszország a napkitörés időpontját – mintegy pajzsként – felhasználva elektronikai hadviselési képességét tesztelte valós célokon. Annak oka, hogy a valószínűsíthetően kibertámadás mellett felmerült az elektronikai hadviselési eszközök lehetséges alkalmazása is, mint kiváltó ok, az az, hogy ebben az időszakban orosz elektronikai hadviselési tevékenységet is tapasztaltak a környező országok. Ez az elektronikai hadviselési tevékenység kommunikációs zavarást is magában foglalt, melynek forrását – egy viszonylag új és nagy rádiótornyot – Kalinyingrádban azonosították [36][37].

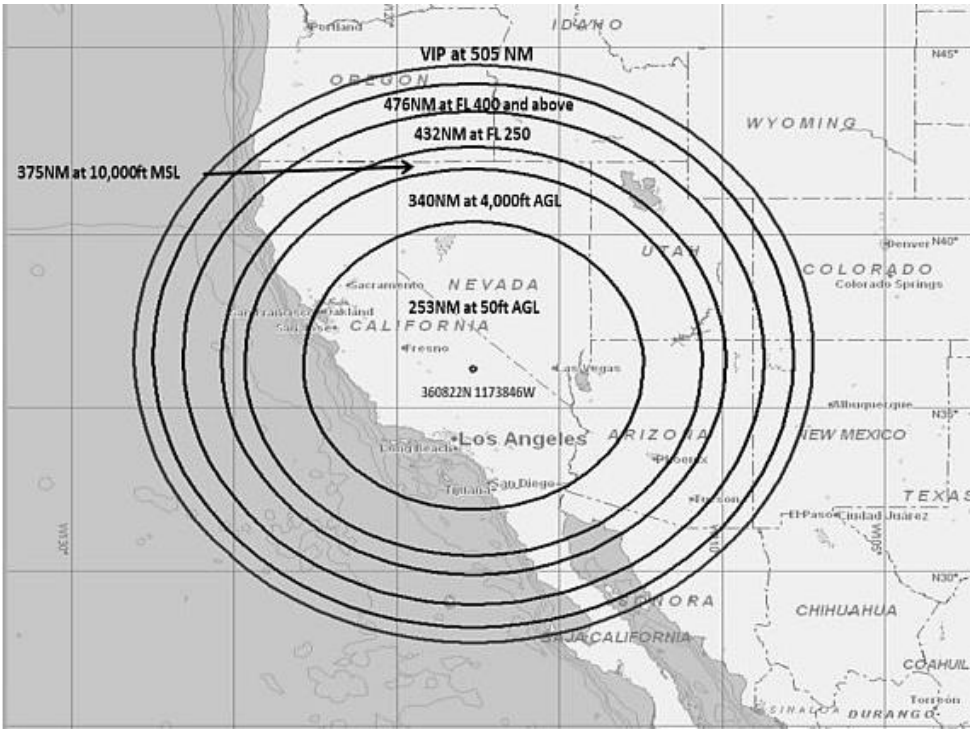
4. ábra Az elektronikai zavarás helyszínei a svédországi incidens esetében [19]

A 4. számú ábrán a helyszínek közötti távolságot szemléltetem, mely alapján látható, hogy a korábban ismert elektronikai hadviselési eszközök hatótávolságát jóval meghaladó távolságokról van szó. Fontos azonban azt is megjegyezni, hogy napjainkban Oroszország vonatkozásában számos új haditechnikai fejlesztés került rendszeresítésre.

[17] European Aviation Safety Agency, EASA
[18] Glavnoje razvedivatyelnoje upravlenyije, GRU
[19] Szerkesztette a szerző.

7. USA, Kalifornia, katonai elektronikai zavarási teszt (2016.)

A repülőterek és a repülés vonatkozásában mindenképpen fontosnak tartok megemlíteni egy, az amerikai hadsereg által tervezett elektronikai zavarási feladatot, amelynek hatása az előzetes elgondolás alapján Kalifornia egészére kiterjedt volna, az oregoni határtól egészen a mexikói határig. A zavarás során a globális helymeghatározó rendszert tervezték zavarni, melynek repülésre kifejtett hatása az 5. számú ábrán látható. A repülőgépek pilótáinak tájékoztatása érdekében kiadtak egy NOTAM[20] közleményt, amelyben az ábrán látható adatokkal megadták, hogy a zavaró eszköz telepítésének helyétől milyen távolságban és milyen magasságig kell számolni esetleges pontatlansággal, vagy teljes mértékű használhatatlansággal [38].



5. ábra Az elektronikai zavarás várható hatása a különböző magasságokban és távolságokban (tengeri mérföldben és lábban megadva)[21] [38]

Azonban a feladat során nemcsak a repülés volt az egyetlen érintett terület. A tervezés során figyelembe kellett venni, hogy minden eszköz, rendszer vagy jármű, amely a globális helymeghatározó rendszer jelét felhasználja, az elektronikai zavarás hatása alá kerülhet. Problémaként jelentkezett, hogy ennek figyelembe vételével oly mértékűvé vált az érintett eszközök száma, hogy nehezen lehetett volna biztonsággal kijelenteni, hogy a feladat végrehajtása nem fog balesettel járni, esetleg emberi áldozatot követelni. Valószínűsíthetően az amerikai Repülőgép-tulajdonosok és Pilóták Szövetsége által támasztott kifogások miatt a tesztelést a végrehajtás előtt törölte a hadsereg[22] [38][39].

[20] Notice to airman, NOTAM: bármely légiforgalmi berendezés, szolgálat, eljárás létesítéséről, állapotáról, változásáról vagy veszély fennállásáról szóló értesítés, amelynek idejében való ismerete elengedhetetlenül szükséges a repülésben érdekelt személyzet részére.
[21] Tengeri mérföld = Nautical mile, NM. 1 NM = 1852 m. Láb = feet, ft. 1 ft = 30,48 cm. AGL: above ground level, földfelszín felett.
[22] Aircraft Owners and Pilots Association, APOA

8. Egyiptom, Kairó nemzetközi repülőtér forgalmának zavarása (2016.)

2016. május 24-én Egyiptom kiadott egy NOTAM közleményt a kairói repülőtért használó repülőgépek pilótái számára, miszerint ismeretlen forrású zavaróeszközből zavarást észleltek Kairó repülőterén. Emiatt a pilótákat figyelmeztették arra is, hogy folyamatosan figyeljék a NOTAM közleményeket [40].

9. Hong kong-i repülésirányítás zavarása (2017.)

2017. áprilisában az indonéziai elnök, Joko Widodo hong kong-i látogatása során a biztonsági intézkedések részét képezte a rádió-távirányítású improvizált robbanóeszközök[23] ellen alkalmazott elektronikai zavaróeszköz, az úgynevezett jammer alkalmazása. A zavaróeszköz a 3. számú képen látható rendőrautóban volt elhelyezve, antennái a gépjármű tetején láthatóak [41].

3. kép Hong kong-i rendőrautó, tetején az antennákkal [41]

Az elektronikai zavaróeszköz működtetése során azonban zavarás érte a repülésirányítás frekvenciáit. A polgári repülésirányítás nyilatkozata szerint időszakosan észleltek interferenciát, melyet bejelentettek a Kommunikációs Hivatalnak. A Hivatal egy kivizsgálócsoportot a helyszínre küldött, azonban sem a zavarforrást, sem annak helyét nem tudták behatárolni. Kormányzati források szerint a repülésirányítás folyamatosan képes volt a feladatait ellátni, a repülőgépek és utasaik nem voltak veszélyben [41].

[23] RCIED, Radio controlled improvised Explosive Device

AZ „OKOS REPÜLŐTÉR” SÉRÜLÉKENYSÉGE, TÁMADHATÓSÁGA

Napjaink egyik kulcsfontosságú kutatási területe a fenntartható fejlődés, az élhetőbb környezet kialakítását célul kitűző „okos város”[24] koncepció. *„Az okos vagy élhetőbb városon olyan települést értünk, amely a rendelkezésre álló technológiai lehetőségeket (elsősorban az információs és kommunikációs technológiát) innovatív módon használja fel, elősegítve ezzel egy jobb, diverzifikáltabb és fenntarthatóbb városi környezet kialakítását.”* Az okos városok egyik fontos eleme a Közlekedés [42].

Az okos repülőtér elgondolás szerint a légi közlekedésben résztvevők számára egy minél komplexebb, időben pontos, akár távolról is elérhető szolgáltatási láncot terveznek kialakítani. A Cisco Internet Business Solutions Group (IBSG) a repülőterekkel kapcsolatba öt okos szolgáltatást különböztetett meg az okos repülőterekkel kapcsolatban, melyek működtetése jelentős előnyöket hordoz mind a szolgáltatók, mind az ügyfelek részére. Az öt okos szolgáltatás az alábbi:

- okos szállítási és parkolási szolgáltatások. Az utazó részére valós idejű szolgáltatásként, GNSS adatok felhasználásával útvonalat, parkolási lehetőséget ajánl;
- okos kiskereskedelmi, vendéglátó és szórakoztatási szolgáltatások. A cél a kiskereskedelmi szolgáltatások optimalizálása, a sorok minimalizálása, amely az utazó részére személyre szabott javaslatokkal elősegíthető. Emellett természetesen megjelenhetnek személyre vagy úticélra szabott reklámok is;
- okos munkahely szolgáltatások. Ezen esetben a különböző mobil felszerelések rádiófrekvenciás azonosítással (Radio Freqvency Identification, RFID) történő nyomon követése történne meg;
- okos repülőtér folyamatok. Hely-alapú szolgáltatások, RFID alapú csomagazonosítás, sor nélküli check-in megvalósítása;
- okos üzleti szolgáltatások. A repülőtér tulajdonosa/üzemeltetője és repülőtéren jelenlévő üzleti partnerek közötti információ megosztásról van szó a hatékonyabb üzemelés érdekében (pl. közlekedés és létesítmény menedzsment, logisztikai és veszélyhelyzeti ellátás, biztonsági szolgálat) [43].

Mivel az okos fejlesztések egyik legfontosabb alapja a rendelkezésre álló információk, események azonnali megosztása a rendelkezésre álló kommunikációs csatornákon, így szándékosság esetén kiemelten fontos célpont, vagy nem szándékos cselekmény esetén jelentős probléma forrása lehet a különböző vezeték nélküli kommunikációs megoldások elektronikai zavarása. Összegezve kijelenthető, hogy az okos repülőtér működése és az ott lévő utasok biztonságérzete negatívan befolyásolható az elektronikai zavaró eszközökkel, amennyiben azok több alkalmazás frekvenciasávját lefogják. Így a zavarandó frekvenciatartományok között szerepelnek a GSM, a Wi-Fi, a Bluetooth és természetesen a GNSS sávok.

[24] Smart city

ÖSSZEFOGLALÁS

Jelen cikkemben a légi közlekedés elektronikai zavarásának megtörtént eseteit kutattam és vizsgáltam. Megállapítható, hogy számos eset történt már eddig is. Bár az évi egy-két eset nem tűnik nagy számnak, azonban ha hozzátesszük, hogy egy-egy utasszállító repülőgép 100-300 utas szállítására képes, egy szerencsétlen esetben jelentős katasztrófával nézhetünk szembe. Azt is hozzá kell tennünk, hogy ebben az esetben még nem számoltunk a földön is lehetséges áldozatok számával. Néhány esetben pedig egyidőben több légijármű is az elektronikai zavarás hatása alatt lehetett.

Fontos az, hogy a kritikus, vagy létfontosságú infrastruktúrák védelme nemcsak a terrorizmus elleni védelmet foglalja magába, hanem a különböző természetes és más események hatása elleni védelmet. Ezen események közé kell sorolnunk az elektronikai zavarást is. A cikkben bemutatott legtöbb esemény az elektronikai zavaró eszközök nem megfelelő alkalmazásából ered. Az ilyen jellegű problémák elkerülését a jelenleg rendelkezésre álló technikai lehetőségek és eszközök alkalmazása biztosíthatja számunkra.

Mint a példákból is látható, jelenleg még nem fordult elő terrorista célú alkalmazása, azonban annak jövőbeli esélyét nem szabad kizárnunk az eszközök könnyű beszerezhetősége, könnyű alkalmazhatósága, és egyszerű kezelhetősége miatt.

FELHASZNÁLT IRODALOM

[1] Bonnyai Tünde: A kritikus infrastruktúra védelem elemzése a lakosságfelkészítés tükrében. Nemzeti Közszolgálati Egyetem. Doktori (PhD) Értekezés. 2014. 19-20. old.

[2] Mógor Judit, Földi László, Solymosi József: Lépések a kritikus infrastruktúra védelmének magyarországi szabályozása felé. Hadmérnök. III. Évfolyam 4. szám - 2008. december. ISSN 1788-1919. 16-17. o. url: http://hadmernok.hu/archivum/2008/4/2008_4_mogor.pdf

[3] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. URL: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1200166.tv Letöltés ideje: 2017.09.27.

[4] David L. Adamy: EW against a new generation of threats. Egyesült Királyság. Artech House kiadó. 2015. ISBN 13: 978-1-60807-869-1

[5] Horváth József: A repülésirányítás elektronikai zavarása. Repüléstudományi közlemények, XXV. Évfolyam 2013. 2. szám, 278-288. oldal, ISSN 1789-770X url: http://www.repulestudomany.hu/kulonszamok/2013_cikkek/2013-2-20-Horvath_Jozsef.pdf

[6] Tarján G. Gábor: A terrorizmus. Rendőrtiszti Főiskola. 2007. ISBN 978-963-9543-74-4 url: http://rtk.uninke.hu/downloads/tanszekek/tarstud/tema/terrorizmus_ma.pdf

[7] Honvedelem.hu: Iránt kibertámadás érte. url: http://www.honvedelem.hu/cikk/22112/irant-kibertamadas-erte

[8] Szabó Miklós: Polgári repülőbalesetek és –katasztrófák fekete könyve, 1990-2002. SYCA kiadó, Budapest, 2002. ISBN 9638626240

[9] European Union Agency For Network And Information Security, ENISA (Európai Uniós Hálózat- és Információbiztonsági Ügynökség): Securing Smart Airports. 2016. december. 17. o. ISBN 978-92-9204-185-4 doi: 10.2824/865081 url: https://www.enisa.europa.eu/publications/securing-smart-airports

[10] Ernszt Ildikó: A Nemzetközi légiközlekedés védelme. Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar. Budapest. 2010. HU ISSN 1787-0607, ISBN 978-963-9808-23-2, 167. o.

[11] MNO.hu: Teljes légtérzárat rendeltek el hazánkban. url: https://mno.hu/migr/teljes_legterzarat_rendeltek_el_hazankban__kepriport_-230435

[12] Forrás 9., 25. o.

[13] Mult-kor.hu: Öt híres reptéri terrortámadás. url: http://mult-kor.hu/ot-hires-repteri-terrortamadas-20160322?pIdx=1

[14] Origo.hu: Hat terrortámadás a párizsi Orly repülőtéren. url: http://www.origo.hu/nagyvilag/20170318-hat-terrortamadas-a-parizsi-orly-repuloteren.html

[15] Origo.hu: Itt a biztonsági kamera felvétele az Orly repülőtéren történt támadásról. url: http://www.origo.hu/nagyvilag/20170321-itt-biztonsagi-kamera-felvetele-a-parizsi-orly-repuloteri-tamadasrol.html
[16] Hirado.hu: Az elmúlt 13 év súlyos, európai terrorcselekményeinek összefoglalója. url: http://www.hirado.hu/2017/03/22/az-elmult-13-ev-sulyos-europai-terrorcselekmenyeinek-osszefoglaloja-kepekkel/
[17] Robert Abel: Pittsburgh teen launched cyberattacks on Belgium airport after ISIS attacks. url: https://www.scmagazine.com/child-hacker-admits-to-launching-cyberattacks-on-brussels-airport-after-isis-bombing/article/637387/
[18] Kristóf Csaba: Kibertámadás miatt bénult meg a repülőtér. url: https://biztonsagportal.hu/kibertamadas-miatt-benult-meg-a-repuloter.html
[19] ThanhNienNews.com: More than 100 flight delayed due to cyber-attacks at Vietnam's airports. url: http://www.thanhniennews.com/society/more-than-100-flight-delayed-due-to-cyberattacks-at-vietnams-airports-64772.html
[20] Lizzie Dearden: Ukraine cyber attack: chaos as national bank, state power provider and airport hit by hackers. url: http://www.independent.co.uk/news/world/europe/ukraine-cyber-attack-hackers-national-bank-state-power-company-airport-rozenko-pavlo-cabinet-a7810471.html
[21] Evan Perez: FBI: Hacker claimed to have taken over flight's engine controls. url: http://edition.cnn.com/2015/05/17/us/fbi-hacker-flight-computer-systems/index.html (2017.12.06.)
[22] Tamlin Magee: Is it possible to hack a plane? url: https://www.techworld.com/security/is-it-possible-hack-plane-3644970/
[23] Aviation Safety Reporting System. url: https://asrs.arc.nasa.gov/search/database.html
[24] Jeff Coffed: The Threat of GPS Jamming. url: http://gpsworld.com/wp-content/uploads/2014/02/ThreatOfGPSJamming_FEB14.pdf
[25] David Hambling: GPS chaos: how a $30 box can jam your life. url: https://www.newscientist.com/article/dn20202-gps-chaos-how-a-30-box-can-jam-your-life/
[26] Yukon Palmer: Navy accidentally jammed gps system in San Diego. url: HTTPS://FIELDLOGIX.COM/NEWS/NAVY-ACCIDENTALLY-JAMMED-GPS-SYSTEM-IN-SAN-DIEGO/
[27] Economist.com: No jam tomorrow. url: http://www.economist.com/node/18304246
[28] Glen Gibbons: FCC fines operator of gps jammer that affected Newark Airport ground-based augmentation system. url: http://www.insidegnss.com/node/3676
[29] Brad Lendon: North Korea jamming South's air traffic navigation. url: http://news.blogs.cnn.com/2012/05/03/reports-north-korea-jamming-souths-air-traffic-navigation/
[30] Cobham Aviation hivatalos weboldala. url: http://www.cobhamaviationservices.com/what-we-do/operational-readiness-training/
[31] NATO Joint Electronic Warfare Core Staff (JEWCS) bemutató. url: https://www2.warwick.ac.uk/fac/soc/pais/people/aldrich/vigilant/lectures/gchq/20080904_nr_jewcs_transformation_brief_muxfeldt_unclas_old.pdf
[32] Wilhelm Theuretsbacher: NATO-Übung: Flugsicherung in halb europa lahmgelegt. url: https://kurier.at/chronik/oesterreich/nato-uebung-flugsicherung-in-halb-europa-lahmgelegt/69.226.057
[33] Matthew Day: 13 planes vanish from radars over Europe. url: http://www.telegraph.co.uk/news/worldnews/europe/austria/10898385/13-planes
[34] Wilhelm Theuretsbacher: Wieder störangriff auf flugsicherung. url: HTTP://KURIER.AT/CHRONIK/OESTERREICH/AUSTRO-CONTROL-WIEDER-STOERANGRIFF-AUF-FLUGSICHERUNG
[35] Air Traffic Management, Issue I 2015., 6 o. url: http://www.airtrafficmanagement.net/ (2016.11.10.)
[36] Is there electronic warfare behind the block of Swedish air traffic control systems? url: http://securityaffairs.co/wordpress/46278/cyber-warfare-2/swedish-air-traffic-control-systems.html
[37] Kjetil Stormark: Sweden issued cyber attack alert. url: https://www.aldrimer.no/sweden-issued-cyber-attack-alert-as-its-air-traffic-reeled/
[38] John Keller: Military GPS jammer tests could knock out satellite navigation to much of West Coast. url: http://www.militaryaerospace.com/articles/2016/06/gps-jammer-satellite-navigation.html

[39] Elizabeth A. Tennyson: NAVY cancels planned GPS outage in Southern California. url: https://www.aopa.org/news-and-media/all-news/2016/june/08/navy-cancels-planned-gps-outage-in-southern-california
[40] Declan Selleck: GPS jamming at Cairo. url: http://flightservicebureau.org/gps-jamming-at-cairo/
[41] Kris Cheng: Police accused of jamming air traffic control radio with anti-explosive van during Indonesian president's visit. url: https://www.hongkongfp.com/2017/05/02/police-accused-jamming-air-traffic-control-radio-anti-explosive-van-indonesian-presidents-visit/
[42] MTA Regionális Kutatások Központja: „Smart cities" tanulmány. Győr, 2011. ISBN 978-963-08-1739-4, 6. o.
[43] Dr. Amir Fattah - Howard Lock - William Buller - Shaun Kirby: Smart Airports: Transforming Passenger Experience To Thrive in the New Economy. 2-3 o. Cisco Internet Business Solutions Group (IBSG) 2009. július. url: https://www.cisco.com/c/dam/en_us/about/ac79/docs/pov/Passenger_Exp_POV_0720aFINAL.pdf

THE ELECTRONIC JAMMING OF THE AVIATION

Nowadays we can read or hear a lot about the critical infrastructures. In the 1-3 Annex of the 2012 CLXVI Act, dealing with the identification, designation and protection of critical systems and facilities, we can find the transport as a sector, and the aviation as sub-sector of the transport. The aviation, as critical infrastructure, has several aspect regarding to the needed defence. Not only against the so common terrorism, but we have to prepare to to eliminate the effects of various natural phenomena, technical reasons as well. One of these technical reasons can be the electronic jamming. This article is the second part of my study about the defence of the aviation, as critical infrastructure, against the electronic jamming. The aim of this article is to introduce and analyze cases, where electronic jamming has been used against any element of aviation, whether it be a radar system or a communication system. I have also taken into account the jamming of the global navigational satellite system, which is also important in terms of aviation.

Keywords: *airport, electronic jamming, critical infrastructure*

Horváth József (MSc) doktorjelölt Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola horvath0101@gmail.com orcid.org/0000-0002-2743-3522	Horváth József (MSc) PhD Aspirant National University of Public Service Doctoral School of Military Engineering horvath0101@gmail.com orcid.org/0000-0002-2743-3522

„Az Emberi Erőforrások Minisztériuma ÚNKP-17-3-IV-NKE-16 kódszámú Új Nemzeti Kiválóság Programjának támogatásával készült"

http://www.repulestudomany.hu/folyoirat/2018_2/2018-2-01-0441_Horvath_Jozsef.pdf