

XXXII. Országos Tudományos Diákköri Konferencia
Had- és Rendészettudományi Szekció
Gödöllő, 2015. április 15-17.
Szent István Egyetem Gazdaság- és Társadalomtudományi Kar
Nemzeti Közszolgálati Egyetem

A rádió-távvezérlésű improvizált robbanóeszközök zavarásának kérdései

Jelige: Gilgames eposz

Pályamunka lezárásának időpontja: 2014. július

TARTALOMJEGYZÉK

Tartalomjegyzék.....	1.
BEVEZETÉS	2.
1. FEJEZET: AZ IMPROVIZÁLT ROBBANÓESZKÖZÖK ALKALMAZÁSÁNAK TÖRTÉNETI ÁTTEKINTÉSE	6.
1.1. A második világháborútól napjainkig	6.
1.2. Az ellentevékenységek nehézségei	7.
2. FEJEZET: AZ IMPROVIZÁLT ROBBANÓ ESZKÖZÖK KONSTRUKCIÓI, TIPIKUS SZERKEZETI ELEMEINEK JELLEMZÉSE	9.
2.1. Az IED eszközök általános ismertetése	9.
2.2. Az IED eszközök csoportosítása	11.
2.3. Rádió távvezérlésű IED-k	14.
2.4. RCIED-hez használt rádió berendezések általános jellemzői	16.
3. FEJEZET: A RÁDIÓ-TÁVVEZÉRLŐ ESZKÖZÖK ZAVARÁSA.....	19.
3.1. A hatékony rádiózavarás elvi alapjai	19.
3.2. Zavarási módszerek, technológiák	20.
3.3. Zavarás másodlagos következményei	24.
4. FEJEZET: A ZAVARÓ BERENDEZÉSEK NÉHÁNY TÍPUSA	25.
4.1. TMP-Tactical Manpack.....	26.
4.2. A STAR család.....	28.
4.3. SHADOW.	32.
4.4. Cassidian intelligens zavaró berendezés.	35.
ÖSSZEGZÉS.....	41.
IRODALOMJEGYZÉK.....	43.
ÁBRAJEGYZÉK	45.
TÁBLÁZATOK	45.
KÉPEK JEGYZÉKE	46.

BEVEZETÉS

A terrorizmus a modern világban jól ismert, általános fogalom, azonban konkrét definíciói kissé eltérőek lehetnek. Alapvető sajátosságai minden meghatározásban fellelhetők: erőszak alkalmazása, vagy azzal való fenyegetés, félelem és zavarkeltés. A globális terrorizmussal szemben folytatott küzdelemben a hagyományos hadviselés a gerilla hadviseléssel találta szemben magát, ahol a gyengébb, hátrányban lévő fél teljesen más módon veszi fel a harcot az erősebb ellenféllel szemben.

A terroristáknak minősített csoportok, a kormányellenes erők, az ellenállók és lázadók tevékenységének fő célja nem pusztán az emberölés, hanem az általa kiváltott pszichológiai utóhatás. Ide sorolhatók az általuk végrehajtott robbantásos cselekmények, melyek célpontjai általában szimbolikus jelentőségűek, de a hatásuk által okozott elrettentés és médiakampány miatt akár stratégiai befolyással is rendelkezhetnek. [1]

A 20. század második felében elterjedt ún. „aszimmetrikus hadviselés” sajátossága, hogy nem írható le kötött szabályokkal, nincs általánosan elfogadott szisztémája. Az ilyen jellegű háborúban, eltérő hadikultúrájú felek csapnak össze, ami a katonai potenciál eltérésében, haditechnikai és technológiai különbségekben mutatkozik meg. Az aszimmetrikus harc részeként, akár a kis létszámú terrorista csoportok, a nem hagyományos hadviselés lehetőségeit kihasználva, képesek súlyos személyi veszteségeket és anyagi károkat okozni egy sokkal nagyobb és jobban felszerelt katonai egységnek.

A [2]-es irodalmi forrásban a szerző megfogalmazza, hogy 21. század kezdetétől, a bekövetkező konfliktusokban a NATO hadereje, képességei és harceljárásai egyre kevésbé érik el a kívánt stratégiai célt, aminek egyik oka az, hogy az ellenfél kultúrája, fejlettségi foka, az emberi élethez való viszonya és értékrendszere nagyon eltér a nyugati társadalmakétól.

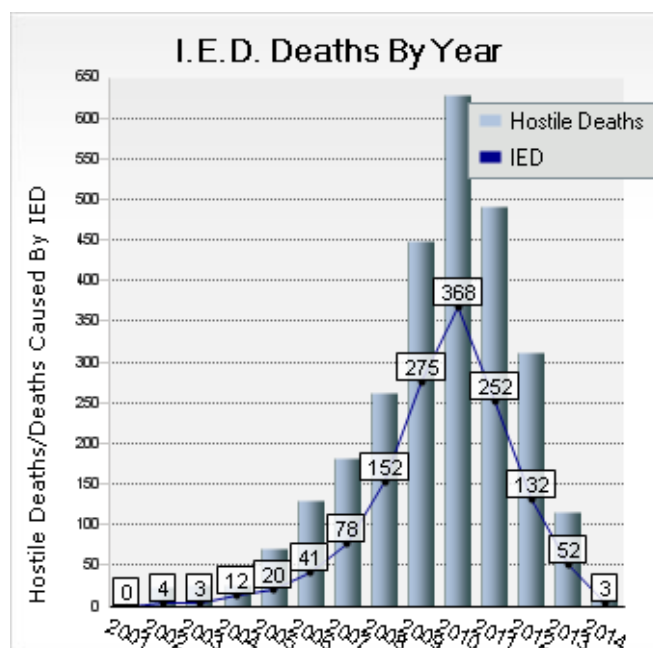
„Az ellenfél azzal, és úgy harcol amivel tud. [...] Véleményem szerint tehát azt látjuk aszimmetrikusnak, ami ellen mi magunk nem tudunk (vagy úgy gondoljuk, hogy nem tudunk) eredményesen küzdeni.” [2]

A 2001. szeptember 11-i merénylet új korszakot nyitott meg a terrorizmus elleni harc történetében. Az Amerikai Egyesült Államok meghirdette a terrorizmus elleni háborút, melynek első lépése terv szerint, az al-Kaida terrorszervezet felszámolása volt, és az általuk

irányított rezsim megbuktatása Afganisztánban. A Nemzetközi Biztonsági Közreműködő Erők (*International Security Assistance Force - ISAF*) 2002-ben kezdte meg működését, eleinte csak a fővárosra, Kabulra korlátozva, majd az ország többi részére is kiterjesztették tevékenységüket, melynek alapvető feladata egy legitim kormányzati rendszer kialakítása és annak megszilárdítása. [3]

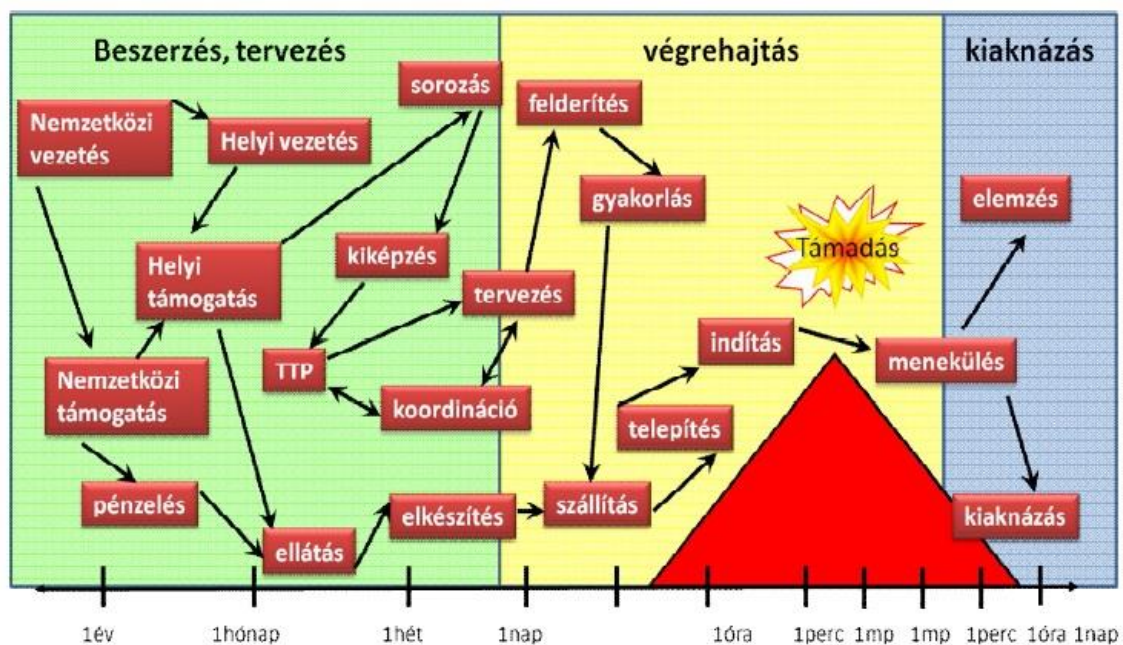
A NATO, fennállásának legnagyobb békefenntartó misszióját vezeti jelenleg is Afganisztánban, ahol a terrorizmust üldözve, nap, mint nap az aszimmetrikus hadviselés által alkalmazott módszerek, új feladatok elé állítják korunk haderőit. Az új módszerek közül, az öngyilkos merénylők és a házi készítésű robbanóeszközök jelentik az egyik legszámottevőbb problémát. Ezeket a robbantásos merényleteket, olyan házilag gyártott eszközökkel hajtják végre, amelyek nagyon egyszerűek is lehetnek, a megépítésükhöz szükséges alkatrészek olcsók és könnyen elérhetőek. Ezek az eszközök óriási veszélyt jelentenek a polgári lakosságra és katonákra egyaránt. Mára globális és maradandó fenyegetésnek tekinthetők.

Habár 2010 óta csökkenő tendenciát mutat (**1. ábra**) az ilyen eszközök által okozott halálestek száma, ami leginkább a koalíciós erők által tett erőfeszítéseknek köszönhető és nem a merénylők csökkenő aktivitásának. A tagországok közös fejlesztései, a NATO felügyelete alatt szervezett tanfolyamok és nemzetközi konferenciák közösen járulnak hozzá küzdelemhez és az ellentevékenység terjesztéséhez.



1. ábra. Az afganisztáni veszteségek és ezen belül az IED-k részesedése

Fontosnak tartom kiemelni, hogy az ellentevékenység nem csupán egyszerű műszaki probléma. Amíg kezdetben az eszköz semlegesítésére, illetve a már bekövetkezett esemény hatásainak csökkentésére koncentrált, addig a mai átfogó megközelítés sokkal szélesebb spektrumot ölel fel. A szemben álló félnek számos tevékenységet kell végrehajtani ahhoz, hogy egy támadást kivitelezhessen: létre kell hoznia egy olyan hálózatot, mely embereket, forrásokat, feladatokat foglal magába. Napjainkban a hangsúly a megelőzésre, így a hálózatellenes műveletekre tevődik át, azaz megpróbálja megakadályozni az ellenfelet már az előállításban és a telepítésben (2. ábra). [4],[5]



2. ábra. Az IED hálózat működése

Az improvizált robbanószervezetek működése és indítása többféle mechanizmussal történhet, melyeket részletesebben a későbbiekben ismertettek. Dolgozatom fő témáját a rádió távvezérlésű alkalmi robbanószervezetek és az ellenük való védekezés adja, különös tekintettel az elektronikai hadviselésre. Ha kudarcot vall a megelőzés, és nem sikerül megakadályozni az ellenfelet a robbanószervezet elhelyezésében a következő lépés megtalálni, és hatástalanítani azt. A rádiózavarás egyfajta „ideiglenes hatástalanítás”, tekintettel arra, hogy megakadályozza a rádió távvezérelt szerkezet felrobbanását anélkül, hogy azt megtalálták volna.

A témával kapcsolatban, korábban két tudományos diákköri pályamunka is született. Kiss Zsolt 2008-as dolgozata hasonló kérdéskört tárgyal a zavarás energetikai viszonyaira kiélezve, valamint több aktív zavaró rendszert is bemutat.

Bodnár István munkájának [7] az alapja, IED készítéséhez használható zsákmányolt eszközök műszaki vizsgálata, ami segítségül szolgál a védekezésre való felkészülésben, különös tekintettel az új frekvenciatartományokban működő eszközökre, amikre az aktív zavarók programozásakor kiemelt figyelmet kell fordítani. Ez a dolgozat egyfajta kiegészítésnek tekinthető, figyelembe véve, hogy miután áttekintést nyújtok az IED eszközök múltjáról, csoportosításáról, a zavarás jellemzőiről, zavaró berendezések bemutatásán keresztül rávilágítok az aktív rendszerek hátrányaira és a jövőt jelentő reaktív zavarókban rejlő lehetőségekre.

Jelen dolgozat célja:

- rövid történeti áttekintést adni az improvizált robbanóeszközök alkalmazásáról;
- részletesen összefoglalni az improvizált robbanóeszközök konstrukcióit, legfontosabb jellemzőiket;
- elvi alapon bemutatni a rádió-távvezérlő eszközök zavarásának kérdéseit;
- összegyűjteni és bemutatni a ma használatos legújabb (hozzáférhető) hordozható és mobil zavaró berendezéseket, jellemezni működési elvüket, majd végül
- az összefoglalásban felvillantani a további kutatásoknak alapot adó alkalmazási problémákat.

A dolgozatban a hivatkozott irodalmi forrásokat az irodalomjegyzékben, előfordulási sorrendjük szerint rendezett listában, szögletes zárójelben, számmal megjelölve adtam meg.

A képek forrásait a képek jegyzéke tartalmazza.

1. FEJEZET: AZ IMPROVIZÁLT ROBBANÓESZKÖZÖK ALKALMAZÁSÁNAK TÖRTÉNETI ÁTTEKINTÉSE

1.1. A második világháborútól napjainkig

Az improvizált robbanóeszközök (*Improvised Explosive Devices – IED*) nem a 21. század találmányai, már a második világháború időszakában több hadszíntéren is eredményesen alkalmazták. A szakirodalom a Molotov-koktélt tekinti az IED ősenek. Ezeket alapvetően az ellenséges páncélosok ellen alkalmazták: becsapódáskor az üveg összetörik és a palackban lévő folyadék magas hőmérsékleten elégve a járművet felgyújthatja.

Szintén a gerilla hadviselés egyik eszköze a vietnámi háborúban alkalmazott meglepő akna (*booby trap*). Ezeket fel nem robbant lőszerkből, és bombákból állították elő házilagosan, majd rejtve helyezték el őket a terepen, így számtalan gyanútlan katona halálát okozva. Innentől kezdve indultak fejlődésnek, a legkülönbözőbb házilagosan készített robbanóeszközök, melyek napjainkra az aszimmetrikus hadviselésben az elmaradottabb fél egyik legmeghatározóbb fegyverének számít.

Az 1979-es szovjet invázió után, az Egyesült Államok és egyes iszlám államok támogatták a kormányellenes erőket Afganisztánban, aminek következtében rengeteg harckocsi akna és egyéb IED készítésére alkalmas robbanóanyag került az országba. A kezdetekben ezek az eszközök több tízkilónyi robbanóanyagot tartalmaztak, melynek robbanóereje és repeszhatása meglehetősen nagy, de páncéltörő ereje minimális volt. Ezeket az eszközöket az ellenálló erők folyamatosan fejlesztették. Ahogy a robbanóeszközök ereje növekedett, folyamatosan növelni kellett az indításhoz szükséges távolságot is, így jöttek létre a távirányítással működtetett eszközök. [8]

Ahogy az **1. ábra** is mutatja, Afganisztánban, a veszteségek jelentős részét az IED-k okozta halálos áldozatok száma teszi ki.

A helyzet Irakban is hasonló volt, ahol a megszállás alatt 4804 halálesetet könyveltek el a koalíciós erők részéről, aminek több mint 60%-át okozták a nem hagyományos módon előállított robbanószerkezetek.[9]

1.2 Az ellentevékenységi nehézségei

Mint láthatjuk, az improvizált robbanóeszközök alkalmazása világszerte nem újdonság, viszont típusaik sokfélesége már a modern kor hadviselésének jellegét tükrözik: repülő és úszó, távirányítással célba juttatott, rádió-távvezérlésű, többszörösen lépcsőzött és más típusú támadással kombinált IED-k. A veszély abban rejlik, a terroristák által véghezvitt folyamatos újítások és fejlesztések miatt, a merénylők mindig lépéselőnyben vannak, és a saját erőik csak nagy veszteségek árán tudnak alkalmazkodni. A csapatok alkalmazkodásának javulását csak a kulcsfontosságú összetevők (időzítők, elektromos alkatrészek, álcázási módszerek) folyamatos megismerése, nyomon követése segítheti.

További nehézség, hogy a merénylők folyamatosan gyűjtik az információkat az ott állomásozó erők harcászati eljárásairól, technikáiról. Tanulmányozzák az interneten is elérhető nyílt leírásokat, tananyagokat, és igyekeznek kiismerni a koalíciós erők rutin jellegű eljárásait. Így sajnos megtalálják a sebezhető pontokat, kiszámítják a biztonságos távolságokat és azon kívül helyezik el a másodlagos robbanószerkezetet. Az is előfordul, hogy a terroristák videofelvételt készítenek akciójukról, majd gyakorlatilag információs hadviselést folytatva, azt feltöltik az internetre.

Óriási előnyt jelent a merénylők számára az alkalmazási környezet, a terep ismerete, amit ki is tudnak használni. A célpont kiválasztása szintén nagy jelentőséggel bír. Általában olyan célpontot támadnak, ami nagy hírértékű a sajtó számára, például rendőr- és katonatisztek, önkormányzati képviselők, vagy akiknek a feladata a robbanóeszközök hatástalanítása, megsemmisítése, például műszaki felderítő járőrök, tűzszerészek.

A fejlesztések eredményeképp, megjelentek olyan összetett megoldások, ami ellen nagyon körülményes a védekezés. Az is előfordul, hogy a robbantás biztosításához többszörös gyújtást alkalmaznak (vezetékes és rádió-távvezérlésű), így ha valamelyik meghibásodik, a másik módon még mindig működésbe hozható a robbanószerkezet. A másik gyakran felbukkanó megoldás a kombinált gyújtás, amikor a robbanótestre a vezeték juttatja el a jelet, de a vezeték egy vevőre csatlakozik, ami rádió-távvezérléssel működik. Ha a vevőt, a zavaró berendezés hatótávolságán kívülre helyezzük, a zavarás ellenére, a robbanás rádió-távvezérléssel indítható.

A nyugati kultúrában a még oly nagyfokú társadalmi támogatottsággal folytatott katonai akciók veszteségei sem elfogadhatók, de legalábbis nehezen tolerálhatók a társadalom számára. Minden katona sebesülése, vagy halála a kormányok ellenzékei részéről újabb hangos tiltakozást vált ki, jelentős belpolitikai botrányhoz vezethet, aminek eredményeképp megtörténhet az is, hogy kivonják a csapatokat a hadműveleti területről, vagy újabb nemzeti korlátozások, biztonsági intézkedések bevezetésével korlátozzák addigi tevékenységüket.

Az ellentevékenység egyik legfontosabb feladata a megelőzés, hogy felszámolják azt a hálózatot, amely az IED-ket előállítja, elhelyezi, felrobbantja és annak sikerét felhasználja politikai-katonai céljainak elérésére. [10]

Technikai szempontból, amíg a fegyver előállítása és telepítése kifejezetten olcsó, az ellenük való tevékenység során a szükséges rendszabályok bevezetése, alkalmazása, a technikai újítások kidolgozása, bevezetése hatalmas költségeket emészt fel. A vizsgálat tárgyául választott rádió-távvezérlésű improvizált robbanóeszközök elleni harc az elektronikai hadviselés szakterületéhez tartozik. Az elektronikai hadviselés aktív zavaró tevékenységének kezdetei az 1904-1905-ös orosz-japán háborúig nyúlnak vissza, azonban az ezt követő évtizedek nagy háborúi, helyi háborúi és katonai konfliktusai egészen más technikát igényeltek. A „hagyományos” elvek szerint a rádiófelderítés által szolgáltatott céladatokat értékelték, meghatározták a fontosakat, együttműködésben a tűzeszközökkel tervezett pusztítással, kijelölték a zavarással lefogandó célokat.

Az IED-k ellen alkalmazott rádiózavarás már csak abból a szempontból is esetleges, hogy az összes létező és a csapatokra nézve veszélyt jelentő IED-nek csak egy része rádió-távvezérlésű, amiből az következik, hogy a „tökéletesen kivitelezett rádiózavarás” sem képes valamennyi IED működésének akadályozására.

A másik következtetés ebből az, hogy ugyan a rádióelektronikai felderítés (SIGINT) támogatja, adatokkal látja el a zavaró eszközök programjait beállító szakembereket, azonban ezek az adatok a múltból szólnak és lehetséges, hogy a következő IED-t egy addig soha nem használt frekvenciájú eszközzel hozzák működésbe. Ezért kell minél alaposabban megismernünk az IED-k mechanizmusait, alkalmazási elveiket és azokra minél nagyobb valószínűséggel hatékony választ adó megoldásokat találni. A következő fejezet ezért az IED-k technikáinak megismerését, jellemzőinek összefoglalását tartalmazza.

2. FEJEZET: AZ IMPROVIZÁLT ROBBANÓ ESZKÖZÖK KONSTRUKCIÓI, TIPIKUS SZERKEZETI ELEMEINEK JELLEMZÉSE

Az aszimmetrikus hadviselés legelterjedtebb eszköze tehát a házilag készítésű robbanóeszköz, improvizált robbanóeszköz, alkalmi robbanóeszköz, vagy más terminológia szerint az elsődleges megjelenésére utalva, az „útszéli bomba”. Az IED egyik definíciója: *„az improvizált robbanóeszközök olyan rombolóhatású nem nagyüzemi módon előállított bombák, amelyek a romboló vagy halálos hatást egészségre ártalmas anyagokkal, pirotechnikai eszközökkel vagy gyújtóhatású vegyi anyagokkal érik el.”*[8]

Alkalmazásuk egyik célja a személyi állomány és a gépjárművek robbanás okozta pusztítása, de az ott állomásozó, feladatot végrehajtó csapatok demoralizálása, biztonság érzetének csökkentése, az állandó, alattomos fenyegetettség tudatának, a stressz-helyzetnek a fenntartása is kiemelten jelentős hatás. [11]

2.1 Az IED eszközök általános ismertetése

Általánosságban kijelenthető, hogy egy ilyen eszköz előállítása egyszerű is lehet. Házi körülmények között megépíthető, akár a mindennapi életben használt eszközökből, vegyszerekből. Elkészítésükhöz nem szükséges magas műszaki előképzettség, hiszen az interneten is elérhető számos leírás és útmutató az előállításhoz ugyanúgy, mint az alkalmazáshoz. Ebből kifolyólag, szerkezeti felépítésük, technikai színvonaluk és bonyolultságuk csupán a rendelkezésre álló anyagoktól és a készítő kreativitásától függ.

Az IED alapvetően a következő részekeségekből áll:

1. **Robbanóanyag töltet:** erre a célra felhasználhatóak különböző katonai harcanyagok, például tüzérségi lövedékek, rakéták, aknák, vagy a belőlük kinyert robbanóanyagok **(1. kép)**, továbbá a katonai és a polgári robbantás-technikában használt különböző robbanóanyagok, C4, Semtex, stb., illetve a különböző vegyszerekből, házilag előállított robbanóelegyek, mint a műtrágya és a petróleum keveréke, vagy akár a különböző méretű edényekbe töltött és így skálázható hatású járműbenzin.



1. kép. Szerelt harckocsi akna és tüzérségi lövedékek

2. **A gyújtószerkezet:** a robbanótöltet indítására, gyújtására szolgáló szerkezet. Minden olyan harceszköz nélkülözhetetlen alkotóeleme, amelynek robbanótöltete van. Feladata a töltet robbantása, a kívánt pillanatban. Előfordul, hogy katonai vagy a bányászatban is használt detonátorokat alkalmaznak, de a leggyakoribb a harcanyagokból kinyert gyújtók, elektromos indítású gyutacsok beépítése.
3. **Az indító mechanizmus:** feladata, hogy megszakítsa vagy létrehozza az elektromos vagy mechanikus kapcsolatot. A leggyakoribbak azok a mechanikus szerkezetek, amelyek húzásra, teherelvételre, nyomásra, elmozdításra reagálnak, tehát valamilyen fizikai behatásra működtetik a robbanóeszközt. További lehetőség egy időzítő szerkezet beépítése (óramű, elektronikus-, kémiai időzítők) ami a célpont helyzetétől függetlenül, a beállított idő elteltével, önállóan hozza működésbe a robbanóeszközt. A távirányított működésű robbanószerkezetek (*Remote Controlled IED – RCIED*) vezetéken vagy rádió távvezérlésen keresztül kapják meg az indító jelet, aminek a hatására felrobbannak.

Ezekon kívül a szerkezeteknek tartalmazniuk kell még áramforrást, amely célszerűen lehet akár hosszú működési idejű elem, motor-, személygépkocsi- vagy tehergépjármű akkumulátora, vagy a biztonságtechnikai riasztókban használatos zselés áramforrás. A pusztító hatást repeszekkel, üvegcserepekkel, csavarokkal, vasszilánkokkal fokozhatják, melyek elsősorban a személyi sérülések mértékét, súlyosságát növeli.

2.2 Az IED eszközök csoportosítása

A házilag előállított robbanószerkezetek felépítésüket tekintve nagyon változatosak lehetnek, figyelembe véve, hogy az előállításukhoz szükséges anyagok és eszközök tárháza kifogyhatatlan. Mivel nem iparilag kerülnek előállításra, minden IED egyedi darab. Sajnos az elkövetők mindig egy lépéssel előttünk járnak, így ahhoz, hogy alkalmazkodhassunk a terroristák módszereihez, ajánlatos csoportosítani az általuk alkalmazott eszközöket és eljárásokat, hogy ezáltal elősegítsük a védekezési metódus kidolgozását. Jelen dolgozat témáját tekintve, az indítási mód szerinti csoportosítást találtam a legcélszerűbbnek, figyelembe véve, hogy ez szorosan összefügg az eszköz felépítésével, valamint ezen az osztályozáson keresztül lehet a legjobban bemutatni, az általam választott típusban rejlő előnyöket és hátrányokat mind a saját csapatok, mind a terroristák szemszögéből.

Az indítás mód szerint, a következőképpen csoportosíthatjuk:

- **Az áldozat által működésbe hozott IED (*Victim Operated IED - VOIED*)** a célpont tevékenysége hozza működésbe az eszközt, váltja ki a robbanást. Ez egyfajta közvetlen fizikai kontaktust igényel, ami lehet húzás, elmozdítás, nyomás vagy akár teherelvétel, esetleg szeizmikus, mágneses vagy infravörös mozgásérzékelők által észlelt környezeti változás, amit a célszemély megjelenése, mozgása vagy akár az általa kibocsájtott hő váltott ki. Többségében a hatás nyomán egy áramkör záródik, és bekövetkezik a detonáció. **(2. kép)**



2. kép. Áldozat által működésbe hozható, nyomással indítható IED

Nagy előny a terroristák számára, hogy az ilyen típusú eszköz bevetésekor nem szükséges a merénylőnek a helyszínen tartózkodnia, viszont ha a felderítés ellen jól álcázzák, és magára hagyják a szerkezetet, előfordulhat, hogy nem az általuk választott célpont, hanem egy teljesen ártatlan civil személy esik áldozatul. Ennek elkerülésére megoldás lehet, hogy csak közvetlenül a célszemélyek megjelenése előtt élesítik az eszközt.

- **Az időzített IED** (*Time Operated IED - TOIED*) lehetővé teszi készítője számára, hogy a robbanás időpontját előre beállítsa. Ezt a megoldást abban az esetben alkalmazzák, ha pontosan tudják, hogy a célpont mikor közelíti meg a helyszínt. Ebben a konstrukcióban az áramforrás és a gyújtószerkezet közé egy időzítő egységet építenek be, ami lehet egy mechanikus vagy egy elektronikus óramű, például egy régi vekker, de akár egy sütő vagy egy termosztát időkapcsolója. **(3. kép)**

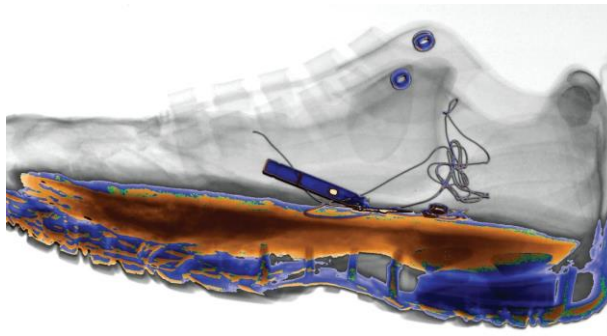


3. kép. Időzítővel ellátott IED

Az elkövető szempontjából itt is előny, hogy nem szükséges a helyszínen tartózkodnia, hátrány, hogy a merénylet sikere legnagyobb részben az időzítésen múlik, így a végeredmény bizonytalanabb, hiszen az áldozat helyzetétől függetlenül bekövetkezik a robbantás.

- **A parancs indítású IED** (*Command Operated IED - COIED*) meghatározó jellemzője, hogy az elkövető által kiadott jelre következik be a robbantás, ami nagyfokú pontosságot tesz lehetővé. A szakirodalom ezen a kategórián belül három különböző típust különböztet meg:

- **az öngyilkos merénylő által indított IED (Suicide Born IED - SBIED)** egy kivételes formája az IED-knek, tekintettel arra, hogy ebben az esetben az elkövető tudatosan, vagy esetleg valamilyen pszicho toxikus szer hatása alatt állva feláldozza önmagát is. A célpontot általában a ruházatukban elrejtett robbanószerkezettel közelítik meg, ami lehet akár cipőbe épített, **(4. kép)** egy övre vagy mellényre rögzítve, sőt ha repülőgépre akarják feljuttatni, az ellenőrzés miatt, akár a bőr alá is bejuttathatják, hogy felcsempészhessék a fedélzetre. [1]



4. kép. Cipőbe rejtett IED röntgenképe

- **A vezetékes indítású IED (Wire Controlled IED - WCIED)** előállítása szintén nem igényel nagy szakértelmet, tekintettel arra, hogy egy egyszerű áramkör segítségével működtethető. A merénylők szempontjából hátrány, hogy a telepítése több időt igényel, mert a vezetéket is külön álcázni kell, valamint az elkövetőnek a helyszín közelében kell tartózkodnia, bizonyosan látótávolságon belül (kb. 100-300 méter). Előnye a rádió távvezérlésű eszközökkel szemben, hogy indítását nem tudják megakadályozni a rádiófrekvenciás zavaró eszközök. **(5. kép)**



5. kép. Vezetékes indítású IED hatástalanítása

- **A rádió távvezérlésű IED** (*Radio Controlled IED - RCIED*) dolgozatom központi eleme, így a következő alfejezetben erre részletesebben kitérek.

Fontosnak tartom kiemelni, hogy a felsorolt kategóriák közül bármelyik kombinálható például egy másodlagos vagy harmadlagos IED alkalmazásával, valamint egyéb más fegyverek támogatásával így egy komplex támadás kerül végrehajtásra. Ez a módszer gyakran az első támadásra reagáló erők vagy mentőcsoportok ellen irányul és gyakran katasztrofális kimenetelű.[2]

2.3. Rádió távvezérlésű IED-k

Az RCIED indítómechanizmusának alapja, hogy az elkövető vezérlésének hatására, a nála lévő adókészülék egy elektromágneses jelet sugároz ki, amely a vevő bemenetén RF jelfeszültségként jelenik meg, a vevő detektálja és feldolgozza a jelet, ami a kimeneten megjelenve működésbe hozza a gyújtó szerkezet áramkörét. Nincs galvanikus fizikai összeköttetés az indító személy (aki az adót vezérli) és az IED között (ami tartalmazza a vevőegységet), hanem az elektromágneses hullámok fénysebességű terjedése teremti meg a kapcsolatot.

Mint ahogy azt az előző fejezetben említettem, a rádió távvezérlésű improvizált robbanóeszközök a parancsindítású IED-k közé sorolhatóak. Nagy előnyük a vezetékes indítású berendezésekkel szemben, hogy álcázásuk kevésbé körülményes, tekintettel arra, hogy a WCIED elektromos vezetéket általában be kell ásni, vagy más módon eltakarni, álcázni. További könnyebbség, hogy az előállításához szükséges eszközök akár a kereskedelmi forgalomban is kaphatóak, különös tekintettel az indító egységre, ami lehet egy mobiltelefon vagy vezeték nélküli csengő, mely a lakosság mindennapi használati eszközeinek körében is elterjedt, így nem kelt feltűnést a beszerzésük.

Mindemellett ez a fajta vezérlés biztosítja azt, hogy nincs szükség helyhez kötött fizikai kapcsolatra az eszköz és az indító személy között, miközben lehetővé teszi a helyzettől függően a merénylő akár folyamatos helyváltogatását, robbantás pillanatának optimálisabb kiválasztását. Ennek feltétele, hogy az indító személy megfigyelés alatt tartsa az IED-t és a célpont helyzetét. [12]

A korszerű rádiótechnikának köszönhetően elméletben nem korlátozott a távolság a gyújtóhely és a robbanóeszköz között, hiszen egy mobiltelefonnal a világ bármely részéről indítható egy RCIED, de ez a megoldás nagyon komoly információs infrastruktúrát igényel. Fejlett kommunikációs hálózatok megléte biztosíthatja az elkövető számára, hogy egy webkamera és internetkapcsolat segítségével akár valós idejű megfigyelés alatt tartsa az eszközt és a célszemélyek, járművek mozgását. Valójában a helyszínen a domborzati és időjárási viszonyok néhány km-re korlátozzák az indítási távolságot. Ilyen messziről már nehézkes lehet beazonosítani az álcázott robbanóeszköz helyét, így annak azonosítására a gyújtóhelyről jól látható jelzést szoktak alkalmazni, ami lehet egy kőrakás vagy fára rögzített színes rongydarab, ami természetesen a célpont számára is feltűnő lehet, így ezeknek a jelzéseknek a felismerése életmentő lehet. [1]

Egy teljes RCIED rendszer a következő elemeket tartalmazza:

- egy rádiófrekvenciás vevő, vagy adó-vevő;
- egy frekvenciában megegyező adó vagy adó-vevő;
- egy kódoló és dekódoló egység (ami csökkenti egy véletlenszerűen bekövetkező akaratlan indításnak a kockázatát);
- áramforrás;
- detonátor;
- robbanóanyag;
- másodlagos áramforrás a vevőben (ez abban az esetben szükséges, ha a vevő kimenete nem elegendő a gyújtó indítására);

A [11]-es irodalmi forrás három kategóriába sorolja az RCIED-ket:

- **kereskedelmi eszköz:** ahogy azt a neve is sugallja, az ilyen típusú rendszer kereskedelmi forgalomban elérhető egységekből áll és nem igényel átalakítást, ahhoz hogy RCIED-ként alkalmazzák, mindössze be kell építeni az áramkörbe. Ezeket a változatokat azok az elkövetők is eredményesen használhatják, akik egyáltalán nem, vagy csak minimális szakképzettséggel rendelkeznek.
- **módosított eszköz:** ezek a típusok szintén széles körben beszerezhetőek, de már igényelnek némi módosítást ahhoz, hogy egy RCIED részét képezzék. Lehetséges módosítás például, egy erősítő, a dekóder vagy egy másodlagos áramforrás beépítése.

- **rendelésre gyártott eszköz:** az ilyen jellegű rendszereket szándékosan azzal a céllal állítják elő, hogy RCIED-ként kerüljön alkalmazásra. Úgy tűnik, hogy ezek a berendezések már úgy épülnek, hogy képesek kihasználni az elektronikai ellentevékenység lefedettségének korlátait és egyre nagyobb számban használnak ilyeneket.

2.4. RCIED-hez használt rádió berendezések általános jellemzői

Azt, hogy az indításhoz szükséges elektromágneses jel eljusson az adóból a vevőbe több tényező is befolyásolja. Ide tartoznak az adó-vevő párosra jellemző paraméterek, mint az eszköz vivőfrekvenciája, hangolható frekvencia tartománya, modulációs módja, az antennanyereségek, a kisugárzott teljesítmény, a vevő érzékenysége, valamint az alkalmazott üzemmód zavartűrő képessége. Az indító jelnek egyes esetekben nagyon bonyolult elektromágneses környezeten kell keresztülhaladnia. A közvetítő közeget befolyásolja az időjárás, a természetes és mesterséges zajok, reflexiók, valamint a szándékos zavarásból eredő negatív befolyásoló tényezők.

A mérénnyelőkkel szemben nagy hátrányt jelent számunkra, hogy nem ismerjük pontosan az általuk alkalmazni kívánt frekvenciát, figyelembe véve hogy az RCIED-hez használható rádió berendezések tárháza rendkívül szerteágazó, ezek az eszközök más-más frekvenciatartományban működnek, eltérő kisugárzott teljesítménnyel. Mivel elsősorban technikai és nem mellesleg anyagi korlátok miatt nem vagyunk képesek az egész frekvenciasávot hatékonyan lefogni, így a korábbi tapasztalatokra építve, a trendek megismerésével biztosíthatjuk csapataink számára a hatékony védekezést.

1. táblázat. Tipikus frekvenciatartományok és szokásos teljesítmények

Eszközfajta	Névleges frekvenciatartomány	Tipikus teljesítmény
mobil telefonok	900/1800/1900 MHz	2 W
CB rádiók	26-28 MHz	0,1-10 W
modell távirányító adók	27, 35, 41,48 MHz	0,1-1 W
gyerekjátékok távirányítói	27, 35, 41,48 MHz	0,01-0,1 W
garázsnyitók, rádiós gépkocsi centrálzárak	435 MHz	0,01 W
vezeték nélküli csengők	435 MHz	0,01 W
riasztórendszerek RF elemei, WLAN eszközök	435, 868, 2400, 4500 MHz	0,1-0,5W

- **mobiltelefonok:** a digitális mobil rádiótelefon rendszerek alapja, a cellás struktúra, ami azt jelenti, hogy a szolgáltatási területet kisebb területekre, azaz cellákra osztják, amelyek egy-egy adó-vevő állomás (bázisállomás) sugárzási körzetét jelentik. Ez a megoldás biztosítja a rendszer számára, hogy a rendelkezésre álló frekvenciákat egymástól kellő távolságban újra felhasználhassák, valamint, hogy a kis teljesítményű mobiltelefonok bárhol elérhessék a rendszert. A rendszer vezérlését a mobil kapcsolóközpont (MSC) biztosítja. Ha egy készülékkel bejelentkezünk egy adott hálózatba, az egy vezérlőcsatornára hangolódik és folyamatosan tartja a kapcsolatot a bázisállomással. Ha hívást indítunk, a rendszer hozzáférési információt küld a vezérlőcsatornán át, a bázisállomáson keresztül az MSC irányába, ami kijelöl egy hangcsatornát, tájékoztatja a készüléket, hogy melyik frekvenciára hangolódjon és létrejön a kapcsolat. A kicsengetési jel hatására a készülék hang-, illetve rezgő jelzést ad a felhasználónak, amit a telefon hangszórójára illetve rezgető motorjára küldött elektromos feszültséggel hoz létre. Ez a feszültség alkalmas lehet egy RCIED indítására. **(6. kép)** Figyelembe véve, hogy az általam leírt kapcsolat ideje eltérő lehet, ez a megoldás nem biztosít a merénylő számára pontos időzítést, sőt egy esetleges téves hívás, vagy egy rendszerüzenet beérkezése, idő előtt működésbe hozhatja a robbanóeszközt.



6. kép. Mobiltelefonnal indítható IED

- **CB rádiók:** Az indító szerkezet egy adott jelszint átlépése esetén robbantja fel az eszközt, ami azt is jelenti, hogy a rádió vivőfrekvenciáján kisugárzott zavarjel vagy egy szélessávú zavarásból származó véletlenszerű jel is képes kiváltani a működésbe lépést. Ezért célszerű megbizonyosodni arról, hogy az alkalmazni kívánt frekvenciasávot általában nem használják a környéken, valamint a vevő érzékenységeinek küszöbértékét magasabbra állítani.[7]
- **távirányítók:** Működésük alapja, hogy az adóban található enkóder¹ előállít egy elemi impulzusokból álló jelsorozatot. A beállítástól függően az elemi impulzusok "1" vagy "0" értéket vehetnek fel. Ezt a jelsorozatot kisugározza és a vevő az antennán vett jelet demodulálja és a kapott jelsorozatot a dekóderre² vezeti. Abban az esetben, ha a vett jelsorozat bitmintája azonos a vevőn beállított mintával, akkor a kimeneten pl. meghúzza a működtető relét, ami beindítja a detonációt. [7]

A fentiekből jól látható, hogy a rádió-távvezérléshez használatos eszközök köre igen széles palettát ölel fel. A módosításokkal úgy frekvenciában, mint teljesítményben a valószínűleg ismert eszközök paramétereitől jelentősen eltérő példányok építhetők, amik a korábban szerzett tapasztalatainknak ellentmondhatnak, vagyis váratlanul érhet az alkalmazásuk. Emiatt kiemelkedő a jelentősége mind a SIGINT-nek, mind a technikai analízist végző szakértőknek, hiszen elsősorban ők képesek először jelezni a korábbiaktól eltérő jellemzőkkel bíró eszközöket.

A hatékony rádiózavarás létrehozásához szükséges műszaki beállítási feladatok végrehajtására a missziókban külön erre a célra rendszeresített beosztást hoztak létre, aki egyrészt a frekvenciamenedzsment műveleteit, másrészt a zavaróeszközök, áramforrások, antennarendszerek legjobb műszaki állapotáért dolgozik.

Tudni kell ugyanakkor, hogy a rádiózavarás hatékonysága egy sor fizikai folyamattól, adott, megváltoztathatatlan műszaki paramétertől függ, így csodára a legtapasztaltabb szakemberek sem képesek. Ezeket tekintjük át a következő fejezetben.

¹ Az adóoldali kód kialakítására szolgáló digitális áramkör. Beállítása történhet előzetesen gyárilag, kis kapcsolósor (DIP) átkapcsolásával, vagy primitívebb kivitelek esetén a nyomtatott áramkörtől fóliák átvágásával.

² A vevőoldali kód egyeztetést végző áramkör, az enkóder típuspárja, vagy egy univerzális integrált áramkör, amely bekötéstől függően enkóder vagy dekóder feladatot lát el.

3. FEJEZET: A RÁDIÓ-TÁVVEZÉRLŐ ESZKÖZÖK ZAVARÁSA

3.1. Hatékony rádiózavarás elvi alapjai

A rádiófrekvenciás információátvitel alapja az, hogy egy adóállomás elektromágneses energia formájában sugározza ki az információt, ami a vevő bemenetén feszültséget indukál. Ha ezt a jelet a vevő képes detektálni és feldolgozni, az információ megjelenik a kimeneten. A rádiózavarás lényege az, hogy a vevő bemenetén olyan nagyságú zavaró jelet hozunk létre, amely megakadályozza az információ feldolgozását, így meggátolva, hogy a vevő kimenetén megjelenjen a hasznos információ.

Az, hogy a zavaró- és a hasznos jel műszaki paramétereit tekintve milyen viszonyban van a vevő bemenetén egymással, nagyon sok mindentől függ. Tekintettel az elektromágneses környezet bonyolultságára, néhány egyszerűsítést és elhanyagolást alkalmazva, a hatékony zavarás fizikai megvalósításához alapvetően az alábbi befolyásoló tényezőket kell számításba vennünk:

- az összeköttetésben dolgozó „hasznos” jel adójának teljesítménye;
- az adó antennanyeresége a vevő irányában;
- a vevő érzékenysége;
- alkalmazott üzemmód (zavarállóság, jelfeldolgozási eljárás);
- a zavaró berendezés teljesítménye;
- a zavaró állomás antennanyeresége a vevő irányában;
- a zavarandó összeköttetés távolsága és az azon fellépő szakaszcsillapítás;
- a zavaró adó és a lefogandó vevő távolsága, az azon fellépő szakaszcsillapítás;
- hullámterjedést befolyásoló tényezők;
- üzemi frekvencia;
- a zavaró adó által sugárzott zavarjel üzemmódja (moduláció típusa), stb.

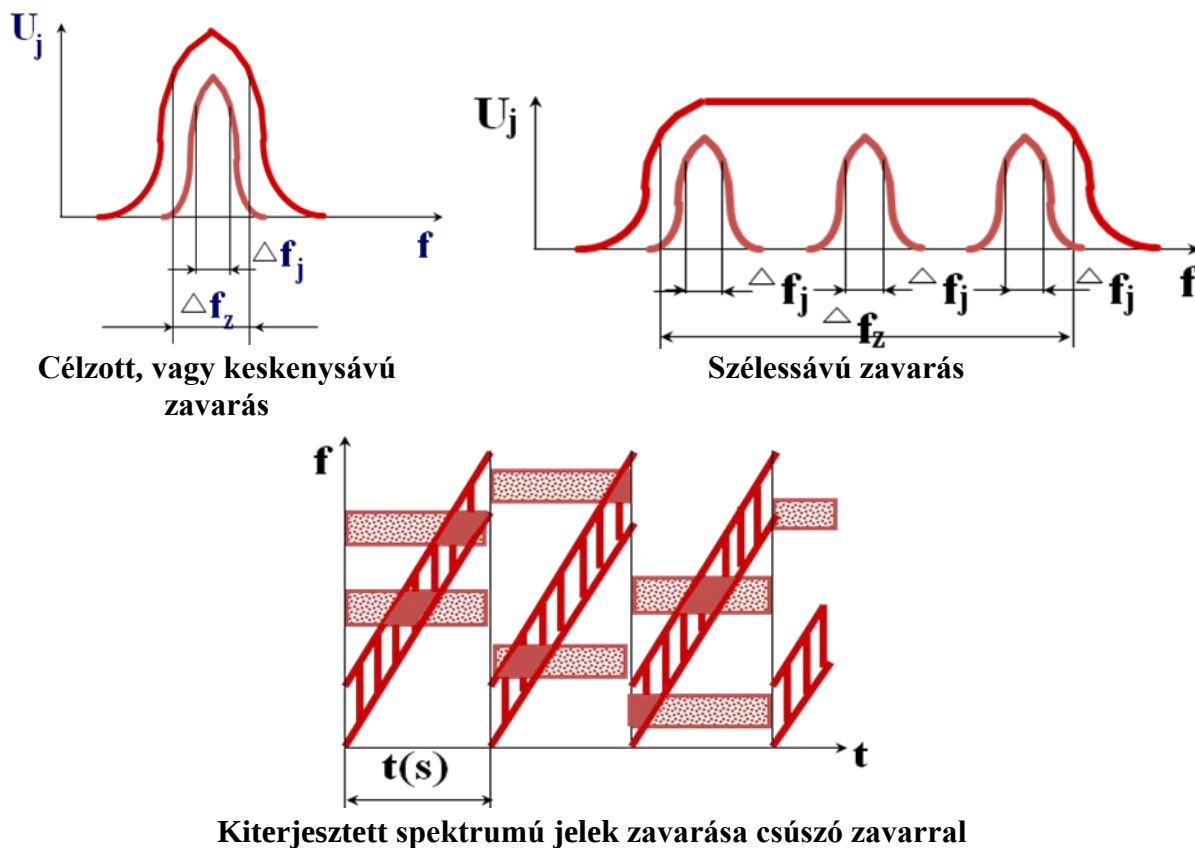
A fentebb leírt paraméterekből számítható a lefogási tényező, ami definíció szerint a lefogás bekövetkezésekor a bemeneten fellépő zavarjel és hasznos jel teljesítményének minimális aránya. Ha a vevő bemenetén nagyobb zavar/jel viszonyt tudunk létrehozni, mint a lefogási tényező, akkor hatékonynak minősül a zavarás. Egy RCIED összeköttetésének zavarásánál eltekinthetünk az antennák irányítottságának figyelembevételétől, mivel nem jellemző az irányított antennák alkalmazása, valamint mivel nem ismerjük a vevő

elhelyezkedését így a zavaráshoz is célszerű körsugárzót alkalmaznunk. [13] Az RCIED zavarásánál ismeretlenek az adó-vevő paraméterek így leginkább a korábbi tapasztalatokra és elemzésekre támaszkodhatunk, amik alapján összeállíthatunk egy adatbázist, amely tartalmazza a mérénylek által leggyakrabban alkalmazott frekvenciákat, teljesítményeket, impulzus paramétereket és ez alapján – kidolgozva a hatékony zavarjeleket – programozhatjuk a zavaró berendezéseket.

3.2. Zavarási módszerek, technológiák

Ahogy azt a korábbiakban bemutattam, rendkívül széleskörű a mérénylek által felhasználható adó-vevő eszközök fajtája, így mondhatni végtelen számú a lehetséges adó-vevő konfiguráció, ebből következik, hogy nagyszámú frekvenciasávot szükséges lefogni a csapatok megóvása érdekében. Ezt a számot tovább növeli az a tény, hogy ezen eszközök jó része több-kevesebb szaktudással elhangolható a névleges gyári frekvenciáról.

Az RCIED-k lefogására alkalmazott zavarási módokat spektrum szerint három csoportra bonthatjuk:



3. ábra. Zavarási módok spektrum szerint

Célzott, vagy keskenysávú zavarás esetén a zavarjelet egy kis frekvenciasávban vagy egy vivőfrekvencián sugározzuk ki, így nagy teljesítménysűrűséget vagyunk képesek előállítani az adott spektrumban. Ebből következik, hogy ezzel a megoldással csak egy eszközt lehetséges zavarni így a szélessávú adásmódot alkalmazó berendezésekkel szemben hatástalan.

Szélessávú zavarás esetén, akár több, a frekvenciatartományban egymás mellett üzemelő eszközt is képesek vagyunk lefogni, de figyelembe véve, hogy a kimenő teljesítmény korlátozott, minél nagyobb frekvenciatartományt akarunk lefogni, annál alacsonyabb lesz a frekvenciaegységre jutó zavarjel teljesítménysűrűsége.

Kiterjesztett spektrumú adásmódok zavarása alatt például a csúszó zavar, valamint a több frekvenciát véletlenszerűen bejáró frekvencia ugratást értjük. Csúszó zavar esetén a szélessávú zavarjel az adott frekvenciatartományban, viszonylag nagy teljesítménysűrűséggel, időben periodikusan átsöpör, ami azzal a következménnyel járhat, hogy a nagy teljesítményszint „leülteti” a vevőkészüléket, vagyis mialatt az automatikus erősítés szabályzó (*Automatic Gain Control - AGC*) megvédi azt a túlvezérlődéstől, így a feléledési időre vételképtelenné is válhat. Ez az ún. AGC zavarás. [11] Frekvencia ugratás esetén pedig diszkrét frekvenciákat váltogatva végezhetnénk a zavarást, de a frekvenciasorrend, vagyis az adójel szekvenciájának ismeret hiányában ez kivitelezhetetlen.

A korszerű zavaró berendezések ezeket a módszereket képesek együttesen is alkalmazni. A zavaró jel kiváltása szerint három zavarási módot különböztethetünk meg:

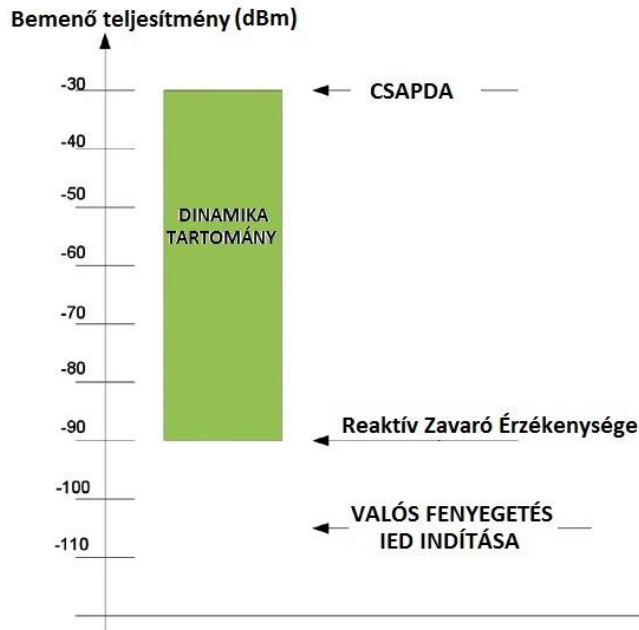
- **aktív:** a hagyományos megközelítése az RCIED zavarásnak a folytonos nagyteljesítményű zavarás. A zavarás jellemzői előre rögzítettek, mint a frekvencia, a sáv szélesség, és a kisugárzott teljesítmény, így a zavaró folyamatosan sugároz a beállított paraméterekkel. Az aktív zavarókba beprogramozható egy vagy több keskenysávú jel vagy akár a vivőfrekvencia zavarása is (célzott zavarás), valamint ez ötvözhető nagyobb frekvenciatartomány folyamatos lefogásával (szélessávú zavarás). Az angol szakirodalom „*barrage-jamming*”-nek nevezi azt a megoldást, amikor az aktív zavaró az összes elérhető teljesítményt kisugározza egy időben, minden beállított frekvencián, a másik megoldás pedig az ún. „*sweep jamming*” ami alatt a korábban bemutatott csúszó zavarást értjük. Mindkét megoldás nagy teljesítményigényű és kevésbé hatékony, hiszen folyamatosan zavar olyan frekvenciákat is, amik az adott

pillanatban nem jelentek veszélyt, azonban eredményes a kisteljesítményű jelek zavarásában, amiket nehéz észlelni. Ez a zavarási eljárás előzetes felderítési adatok alapján összeállított frekvencialista alapján működik, de a valós elektronikai környezethez, az abban a pillanatban működő rendszerekhez vajmi kevés köze van, mivel az ilyen zavaró berendezések vevőkészülékkel nem rendelkeznek.

- **reaktív:** biztosítja, hogy a zavaró kizárólag akkor sugározzon, ha fenyegetettséget észlel. Az aktív módszertől eltérően a zavaró berendezés egy széles frekvenciatartományban működő vevőegységgel is rendelkezik, amely folyamatosan tapogatja le a spektrumot, és ha sugárzást észlel, előállít egy célzott válaszzavar jelet, így a teljesítményt a potenciális fenyegetésekre összpontosítja. Ez a megoldás nagyobb hatékonysággal foghatja le a nagyteljesítményű, keskenysávú jeleket tekintettel arra, hogy a kimenő teljesítményt eleinte csupán néhány frekvenciára fókuszálja. A hatásos zavarás megvalósulásához itt is ugyanazoknak a feltételeknek kell teljesülni, amiket korábban bemutattam, azzal a különbséggel, hogy egy reaktív zavaró esetében már számításba kell vennünk a zavaró távolságát az adótól, valamint a jelfeldolgozási időt.

Ez a megoldás is számos problémát hordoz magában. Tekintettel arra, hogy a reaktív zavaró mozgás közben egy folyamatosan változó elektromágneses környezetben halad, korlátozni kell a bejövő jel dinamika tartományát. A [14] forrásban megjelölt példában az AGC feladata szabályozni a bejövő jel erősítését. Ez egyfajta sebezhetőséget hordoz magában azáltal, hogy terroristák alkalmazhatnak egy nagyteljesítményű sugárzó berendezést csapdaként, ami csökkenti a reaktív zavaró berendezés vevőjének érzékenységet (növeli a minimális detektálható jelerősséget) így kisebb teljesítménnyel indíthatnak egy RCIED-t anélkül, hogy azt a reaktív zavaró észlelné. **(3. ábra)**

További lehetőség az ismert működő berendezések „maszkolása”, vagyis ezen kisugárzásokra nem indítunk zavarási folyamatot. Ezek az adások helyi polgári, baráti katonai, vagy harmadik fél megkímélendő összeköttetéseiben dolgozhatnak, ugyanakkor ezek leállása esetén zavarás kiváltása nélkül hozhatók működésbe az RCIED-k. Ennek a veszélye annál inkább fennáll, minél jobban megismerhető a reaktív zavaró berendezések működési algoritmusai.



4. ábra. A reaktív zavaró berendezés elvének sebezhetősége

Hasonló probléma lép fel, amikor a zavaró berendezés sűrűn lakott területen belül üzemel. A lakosság által használt elektronikai berendezések telítésbe vihetik a vevőt, így az is előfordulhat, hogy a potenciális fenyegetést nem érzékeli.[14]

Ezekre a problémákra lehetne megoldás egy „vegyes” üzemű zavaró berendezés kifejlesztése, ami ötvözi az aktív és reaktív zavarók előnyeit.

- **vegyes:** a zavaró folyamatosan sugároz egy kis teljesítményű, szélessávú zavaró jelet előre programozott frekvenciatartományokban, így biztosítva egy minimális biztonsági „buborékot”, valamint ezzel egy időben, elemzi a spektrumot és a reaktív zavaróhoz hasonlóan válaszzavarást hoz létre a potenciális fenyegetésekre. Így a végső eredmény az egyszerű aktív zavarókénál nagyobb zavarási hatótávolság biztosítása. Ebben az esetben az elsődleges probléma az, hogy el kell kerülni, hogy az aktív modul telítésbe vigye, a reaktív egység vevőjét. Elméletben ez egy folyamatos „kapcsolgató” technológiával lenne megvalósítható: az aktív modult ki kell kapcsolni amíg a reaktív dolgozik, és viszont. [14]

3.3. A zavarás másodlagos következményei

A rádióelektronikai zavarás egyik legjelentősebb negatív „mellékhatása” lehet, hogy a baráti erők rádiófrekvenciás eszközeit (rádió, mobiltelefon, reaktív zavaró) is zavarjuk. Ez abból következik, hogy gyakran ezek az eszközök ugyanabban a sávban működnek, mint amire a zavaró berendezéseket beprogramoztuk. Egy zavaró berendezéssel is ellátott alegység környezetében nagy valószínűséggel léphet fel interferencia, ami abból is következhet, hogy különböző, de egymásra ható frekvenciákon történik kisugárzás, ami már két adó esetén is bekövetkezhet, de alapvetően ott jelent ez problémát, ahol viszonylag kis területen több rádiófrekvenciás eszközt egy időben működtetnek. Ez a jelenség már egy zavaró adó esetében is megakadályozhatja vagy korlátozhatja a saját csapatok kommunikációját.

Az egyik lehetséges ilyen eset, amikor egy saját zavaró olyan frekvencián sugároz, ami szerepel a veszélyeztetett frekvenciák listáján, valamint egy szövetséges katonai alegység is ezt a tartományt használja kommunikációra. Láthatóan a legegyszerűbb megoldás, az lenne, hogy amint nyilvánvalóvá válik az interferencia, vagy a zavaró állomás programozója vagy a kommunikációs rendszer kezelője frekvenciát vált. Azonban ez a megoldás több nehézségbe is ütközik: tekintettel arra, hogy az adott frekvencia rajta van a fenyegetettségi listán, létfontosságú a lefogása a csapatok megóvása szempontjából, de nem kizárt az sem, hogy ugyanez a sáv feltétlenül szükséges a kommunikáció biztosításához. További problémát okozhat, amikor egy előre beprogramozott aktív zavaró, egy olyan sávot is zavar, amire érzékeny egy reaktív zavaró, így egymás közelében, a reaktív eszköz egy olyan tartományban is sugározni fog, ami nem jelent fenyegetést.

A harmadik lehetséges nem kívánt hatás akkor következhet be, amikor két reaktív berendezés találkozik és kölcsönösen zavarják egymást, vagyis az egyik zavaró adó jelét, egy másik reaktív eszköz vevője veszi és kidolgozza rá a zavaró jelet, majd ez visszafelé is megismétlődik. Ez az ún. „ping-pong effektus”. Ezekre a problémára alapvető megoldás az elektromágneses kompatibilitási (EMC) rendszabályok kidolgozása és betartása. Ennek a részét képezi egy egységes frekvencia-egyezmény kidolgozása, ami tartalmazza azokat a frekvenciákat, amiken a baráti erők elektronikai berendezései üzemelnek, így nem szabad zavarni. Tehát az ésszerű megoldás az lenne, ha a reaktív zavarót úgy programozzuk be, hogy ismerje a saját csapatok kisugárzásait és ne reagáljon azokra. Természetesen ez nem oldja meg a többi problémát, ami az elektromágneses jelek összegződéséből, felharmonikusok megjelenéséből ered. [15]

4. FEJEZET: A ZAVARÓ BERENDEZÉSEK NÉHÁNY TÍPUSA

Ahogy azt a korábbiakban említettem, az IED támadások harcászati jelentősége válik lassan a legkevésbé fontossá, sokkal nagyobb hangsúlyt kap a polgári lakosságra és azon keresztül a katona-politikai döntéshozókra kifejtett lélektani hatása. Ezzel természetesen a merénylők is tisztában vannak, így egyre aggasztóbb az előállítás és az alkalmazás kifinomultsága. Az IED-k csoportosítása, ami a védelmi tevékenységek meghatározásához szükséges, még egy ésszerű vezérelv alapján is sokrétű, a felhasznált eszközök, a telepítés valamint az indítás módja szerinti komplexitás miatt. Ahogy ellenfél gyorsan és hatásosan alkalmazkodik a mi mentesítési-semlegesítési módszereinkhez, nekünk is új megoldásokat kell alkalmaznunk.

Amíg a fegyver előállítása és telepítése kifejezetten olcsó, és mindössze egyes részfeladatok igényelnek némi szakértelmet, az ellenük folyó tevékenység során technikai újítások tömkelege jelenik meg. Haditechnikai vállalatok sora, óriási költségvetéssel dolgozik egyre korszerűbb és hatékonyabb zavarók fejlesztésén. Dolgozatomban a teljesség igénye nélkül mutatok be RCIED ellen kifejlesztett zavaró berendezéseket, figyelembe véve, hogy a katonai szervek részére szállított eszközök pontos technikai paraméterei nem nyilvánosak.

Az előzőekben ismertettem, hogy a különböző zavarási megoldások milyen előnyöket és hátrányokat hordoznak magukban, a továbbiakban pedig a [14] forrás nyomán bemutatom, hogy a legújabb fejlesztésű zavaróknak milyen követelményeknek kell megfelelniük:

- nagy sáv szélesség lefoglalása;
- nagy hatósugarú lefedettség (egyesített használata az aktív és reaktív zavaróknak);
- rugalmas a zavarandó frekvenciák közötti váltásban, tehát szükség esetén könnyen átprogramozható legyen akár műveleti területen is;
- képes legyen rögzíteni az elektromágneses spektrumban zajló eseményeket;
- biztosítható legyen az elektromágneses kompatibilitás az egyéb fedélzeti berendezésekkel, kommunikációs eszközökkel;
- optimalizálni kell a kisugárzott teljesítményt;
- alacsony költségigényű legyen, melynek egyik feltétele lehet, hogy a gépjárműbe épített zavaró berendezés átalakítható legyen a gyalogos katona által hordozható háti zavaró berendezéssé.

Ezek a kihívások nem csupán technológiai akadályokat jelentenek, a legtöbb ország gazdasági körülményei megkövetelik a védelmi kiadások minimalizálását, így költséghatékony megoldásokra kell törekedni, ami miatt szükséges az együttműködés a fejlesztő vállalatok között.

4.1. TMP- Tactical Manpack

A TMP (**5. ábra**) egy korszerű, háton szállítható, rádiófrekvenciás zavaróeszköz. Fő alkalmazási területe a nem hagyományos módon előállított, távvezérelt robbanóeszközök elleni védelem biztosítása az erők megóvása érdekében. Akkumulátorról működtethető, számítógép által vezérelt, szélessávú zavaró berendezés, amely a digitális jelfeldolgozó processzor és a mikroprocesszor-vezérelt digitális hangolású szintézerek segítségével biztosítja, a szoftverbázisú zavarójelek sokaságának előállítását.



5. ábra. A TMP 0512 egység kialakítása

A zavarójel előállítása szempontjából az aktív eszközök csoportjába tartozik. A feladatra vonatkozó paramétereket és a zavarójel-formákat közvetlenül egy számítógépről lehet feltölteni. A Feladatkonfiguráló Fájlok tartalmazzák a zavarási módokat, a célfrekvenciákat és más egyéb paramétereket, amiket Feladatszerkesztő (*Mission Editor*) program segítségével

lehet előállítani. A kész fájlokat a Feltöltőprogram (*Fill Gun manager*) segítségével lehet feltölteni a zavaróeszközökbe. (6. ábra.)



6. ábra. A TMP programozási eljárása

Ez az eszköz két, egymást kiegészítő egységből áll:

- TMP 0512- a 25-512 MHz frekvenciasáv lefogására;
- TMP 0512EB- a GSM 900, GSM 1800 és a GSM 1900 csatornák lefedésére.

Külső kinézetük és a kezelés tekintetében a két egység azonos, mindössze az általuk átfogott frekvenciatartomány és ebből kifolyólag az antennák eltérőek.

A TMP adómodulja maximum 10W kimenő teljesítmény leadására képes. Az antennák közvetlenül az eszközön is elhelyezhetők, de gépjárművön való üzemeltetés esetén, egy RF kábellel a gépjármű tetején elhelyezett antennához is csatlakoztatható. Az eszközök üzemeltethetők akkumulátorról és adapteren keresztül 24 V-os fedélzeti hálózatról. [16]

A programozási eljárásból adódóan, láthatjuk, hogy a felderítés során összegyűjtött információkból készült adatbázis alapján határozhatóak meg az eszköz számára, a szükséges lefogandó frekvenciatartományok. Habár viszonylag sok zavarási paraméter beállítható (frekvencia, sáv szélesség, teljesítmény, söprési idő, védett kommunikációs ablakok stb.), gyakorlatilag az eszköz teljesen független az elektromágneses helyzettől, nem a valós körülményekre reagál.

4.2. A STAR család

A STAR család [17] öt féle aktív zavaró berendezést foglal magába: STAR V, STAR Light 3, STAR Light 6, STAR Manpack and STAR Manpack C. Mindegyik zavaró átalakítható a megrendelő igényeinek megfelelően.

A **STAR V-t (8. kép)** az EOD³ csapatok, valamint gépjárművek és konvojok RCIED elleni védelmére fejlesztették ki. Az ún. multi-sweep zavarási módot alkalmazva, képes egy időben csúszó zavarást biztosítani több, előre beprogramozott frekvenciatartományban. Lehetőség van, tartományonként kettő, védett, „kommunikációs ablak” beállítására. A rendszer tartalmaz 8 szélessávú adót, 3 aluláteresztő szűrőt, 1 antenna közösítőt, 6 körsugárzó antennát **(7. kép)** és 8 szélessávú digitális adót.



7. kép. A STAR V antennái

Alapvetően nyolc beprogramozott alsávban üzemel 20 MHz és 2,5 GHz között. A STAR V adóteljesítménye 20 és 200 W között változik (az alsávoktól függően) de a

³ Explosive Ordnance Disposal

maximális kimentő teljesítménye 740 W. A zavaró rendelkezik TCP-IP, RS 485 és USB csatlakozófelülettel, továbbá 22 és 30V közötti feszültséggel üzemel.



8. kép. STAR V zavaró berendezés

A **STAR Light 3 (9. kép)** elsősorban páncélozott harcjárművek oltalmazására fejlesztették ki. Fel van szerelve 4 szélessávú erősítővel, 4 adóval és 3 körsugárzó antennával. Ebben az esetben is a 4 modulra külön-külön két védett frekvencia állítható be a kommunikáció biztosításához. A lefogható tartományok és a hozzájuk tartozó kimenő teljesítmények a következők: VHF - 50W, UHF - 100W, GSM - 25W, DCS - 25W.

A rendszert ellátták egy RS-485 és egy LAN Ethernet csatlakozó felülettel, aminek a segítségével programozhatók a zavarni kívánt frekvencia tartományok és beállíthatók más technikai paraméterek. Az operátor a külső panelről is vezérelheti a berendezést, de csak a ki/be kapcsolást, és külön a modulok üzemelését. A rendszer egyenárammal működik, 22 - 30V között. Beépíthető nem-légkondicionált járművek csomagtartójába, mint például az Iveco LMV, MRAP Dingo stb.



9. kép. STAR Light 3 zavaró berendezés

A **STAR Light 6 (10. kép)** is elsősorban gépjárművek RCIED elleni védelmét szolgálja. Az előző két egységhez hasonlóan, ez is digitális multi-sweep zavarási módot alkalmaz, így több kijelölt frekvenciatartományban képes zavaró jeleket biztosítani párhuzamosan. A zavaró egység moduláris felépítésű, 6 szélessávú adót tartalmaz, 5 körsugárzó antennát, 6 adó, aluláteresztő és összegző modult. Frekvencia alsávok: 25-100 MHz; 100-176 MHz; 176-512 MHz; 925-960 MHz; 1.805-1.880 MHz; 2.110-2.170 MHz.

A STAR light 6 kimenő teljesítménye 150 W, de ez lehetőség szerint növelhető 225 W-ra. A zavaró a külső panelről vezérelhető. Az alrendszerek ki/be kapcsolása mellett, a kimenő teljesítményük is változtatható.



10. kép. STAR Light 6 zavaró berendezés

A **STAR Manpack (11. kép)** a TMP-hez hasonlóan egy háton szállítható zavaró eszköz, a kis létszámú alegységek, tűzszerészek, különleges műveleti alegységek és konvojok megóvására. Ez a digitális multi-sweep technológiával működő eszköz 4 modulból épül fel, minden modulhoz külön tartozik egy antenna, így a zavaró több eltérő frekvenciatartományban is üzemel: VHF és UHF tartományban valamint mikrohullámon is, így képes zavarni a tipikus kommunikációs csatornákat, mint például a GSM sávokat és a Wi-Fi-t. A maximális kimenő teljesítménye 80 W.



11. kép. STAR Manpack zavaró berendezés

A **STAR Manpack C** egy nagyobb teljesítményű, átalakított változata a STAR Manpack rendszernek. A kimenő teljesítménye 100 W.

4.3. SHADOW

A SHADOW család [18] szintén, a fegyveres erők számára tervezett zavaró berendezések csoportja. Ezek már a reaktív eszközök kategóriájába sorolhatók, így alkalmasak a rádiófrekvenciás jelek monitorozására. Az „intelligens” zavaró technológia segítségével optimálisan kihasználható a berendezések kapacitása; a vétel után osztályozza és azonosítja a vett jeleket és csak a potenciális fenyegetésekre reagál. A Shadow technológia feldolgoz minden RF jelet ami RCIED indítására alkalmas és egy időben akár 2000 fenyegetést is képes lefogni, valamint különösen hatékony a mobilkészülékek zavarásában. A három eszközből álló együttesből, kettő RCIED zavarására, egy pedig ezen túlmutatva az ellenséges kommunikáció zavarására alkalmas. [19]

Mindegyik eszköz több típusú gépjárműre is felépíthető. Üzemeltethetők a fedélzeti-, vagy más váltóáramú generátorról. Továbbá kritikus létesítmények, térségek védelmére telepíthető, beltéri és kültéri használatra egyaránt.

A **Black Shadow (11. kép)** egy intelligens, aktív/reaktív zavaró berendezés, amely 20 MHz-től 2,5 GHz-ig üzemel, de lehetőség szerint az átfogott frekvenciatartomány kibővíthető 6 GHz-ig vagy 18 GHz-ig. Alapvetően két hűtőberendezéssel ellátott, rázkódásmentesre építetett modulból áll: az egyik a vevő-, jelfeldolgozó-, és adó modul, a másik a teljesítmény erősítő.



12. kép. Black Shadow zavaró berendezés

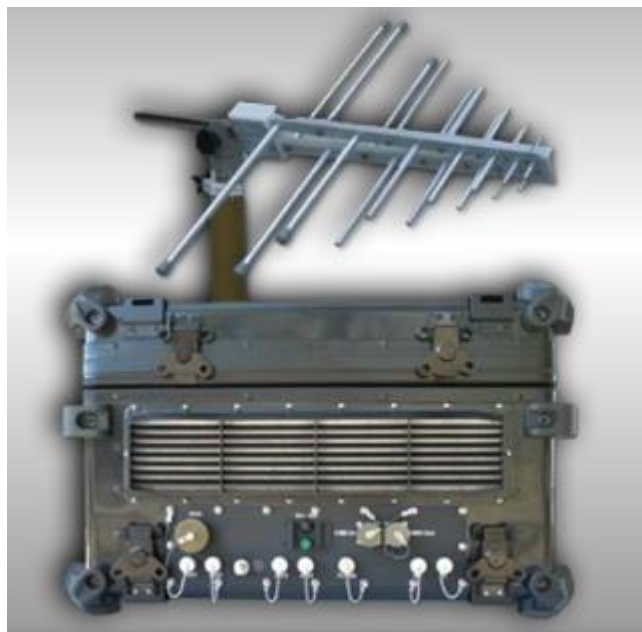
Elsődleges célja a konvojok védelme, valamint egyéb nagy hatótávolságú zavarás például nagy kiterjedésű területek RCIED elleni oltalmazása. A gyártó állítása szerint 100 m sugarú körben a Black Shadow 2000 fenyegetésre képes reagálni egy időben.

A **Raid Shadow (13. kép)**, egy könnyű, reaktív, automatikus zavaró berendezés, szintén 20 MHz-től 2,5 GHz-ig terjedő frekvenciaátfogással, amely tovább bővíthető. Ez egy kisebb tömegű (22 kg-os, hátizsákra méretezett) változata a Black Shadow rendszernek, amely számos lehetőséget biztosít a megelőzésre. Többféle, szabadon programozható zavarást tesz lehetővé, mindig az adott feladat során megcélzott kommunikációhoz igazodva. Lényegében különleges műveleti egységek, tűzszerészek, és kis területek, például ellenőrző-áteresztő pontok védelmére fejlesztették ki.



13. kép. Raid Shadow zavaró berendezés

A **Comjam Shadow (14. kép)** egy harcászati, nagytávolságú, kommunikációs zavaróeszköz, amely vészjelző és iránymérő funkcióval is rendelkezik. Az előző két berendezéssel megegyező frekvenciatartományban üzemel. A gyártó állítása szerint az iránymérő 5°-os pontossággal, a zavaró több mint 1 km-es hatótávolságon belül hatékony. A reaktív üzemet figyelembe véve, csak akkor sugároz, ha az ellenséges kommunikáció éppen aktív.



14. kép. Comjam Shadow zavaró berendezés

Ezek a reaktív berendezések már egy újabb generációt képviselnek az RCIED elleni küzdelemben. A felderítési adatokból származó információk, amik alapján a veszélyes frekvenciákat tartalmazó adatbázisokat összeállítják, az idő elteltével elévülnek. Habár folyamatosan frissítik az adatbázisokat, ezek általában statisztikákra épülnek, így egy kivételes eset, egy - a korábbiakhoz képest - új frekvencián üzemelő adó-vevő berendezés megjelenése is – amit nem fog le az aktív eszköz - emberi életetekbe kerülhet. Az előre programozott zavarási paraméterek és a valós elektromágneses környezet között lévő szakadékot hidalja át a reaktív zavarást biztosító technológia. Természetesen ez sem 100%-os

megoldás, hiszen a távolságokból adódó futási idő, valamint a válaszkésleltetési idő⁴ jelentősen befolyásolja a hatékonyságot.

4.4. Cassidian intelligens zavaró berendezés

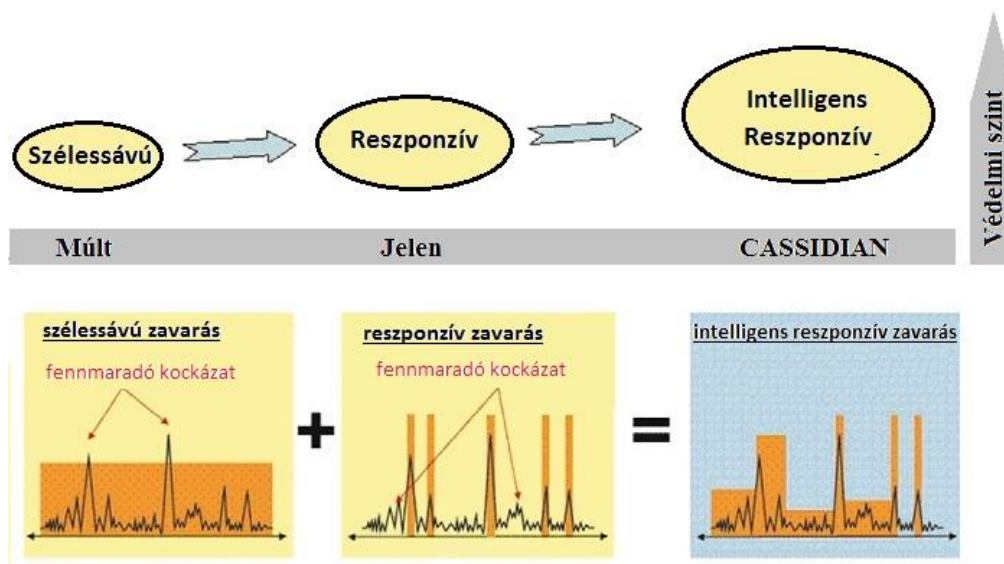
Ez az új fejlesztésű zavaró berendezés 20 MHz-től 6 GHz-ig érzékeli és elemzi a rádiófrekvenciás jeleket, majd egy valós idejű zavarójelet sugároz ki, az észlelt frekvencián, ami meggátolja az összeköttetést az indító személy adója és a robbanóeszköz vevője között. A sikeres lefogáshoz értelemszerűen, mint minden reaktív zavaró berendezésnél, itt is elsődleges szempont a térbeli elhelyezkedés, figyelembe véve, hogy a zavarónak vennie kell a merénylő adója által kisugárzott indító jelet.



15. kép. A Cassidian intelligens zavaró berendezése egy terepjáróba beépítve

A fejlesztő vállalat állítása szerint ez a többrendeltetésű zavaró berendezés egy olyan rendkívül gyors, intelligens, válaszzavaró technológiát használ, ami lényegesen megnöveli az állomány védetségét a RCIED-kel szemben, mert olyan valós idejű zavarjelet sugároz ki, ami pontosan illeszkedik a zavarandó jel frekvenciájára. Ez egy olyan új generációs digitális vevő- és jelfeldolgozó egységnek köszönhető, ami biztosítja, hogy a lefogás egy ezredmásodpercen belül megvalósuljon.

⁴ Jammer Response Time - a „hasznos jel” vételétől a zavarjel kisugárzásáig eltelt idő, ami magába foglalja a jel frekvenciájának és modulációjának meghatározását, a zavarjel kialakítását és kisugárzását



7. ábra. A zavarási megoldások fejlődése

Alapvető követelmény egy modern zavaró berendezéssel szemben, hogy a folyamatos zavarás mellett, működjön a csapatok közti kommunikáció. Habár a korábbi rendszerekben is volt lehetőség a programozás során úgynevezett „kommunikációs ablakokat” létrehozni, ezek általában veszélyesen szélesek voltak. Ezzel szemben ez a reaktív rendszer lehetővé teszi a felhasználó számára, hogy a kommunikációra használatos sáv a zavaró működési frekvenciatartományán belül legyen.[20]

Ezen felül a saját csapatok elektronikai eszközeinek zavarásának a kiküszöbölésére, olyan módon alakították ki a rendszert, hogy ne okozzon interferenciát más zavarók közelében. Ezt úgy oldották meg, hogy működés közben periodikusan ismétlődő időközönként vevő üzemmódra kapcsol, és azon a sávon, ahol interferenciát észlel proaktív zavarási módra vált; ha megszűnik a zavar, pár μ s-on belül visszaáll a rezponzív működés.

Az egész rendszer központi egysége az ún. Vevő Működtető Egység (*Receiver Exciter Unit – REU*) ami a legkorszerűbb FPGA⁵ technológiát használva, biztosítani tudja a hatékony működéshez szükséges sebességet.

⁵ FPGA – (Field Programmable Gate Array) Szabadon programozható logikai egység, amely szabadon összeköthető és átkonfigurálható logikai kapukat tartalmaz igen nagy számban.

REU legfontosabb műszaki paraméterei:

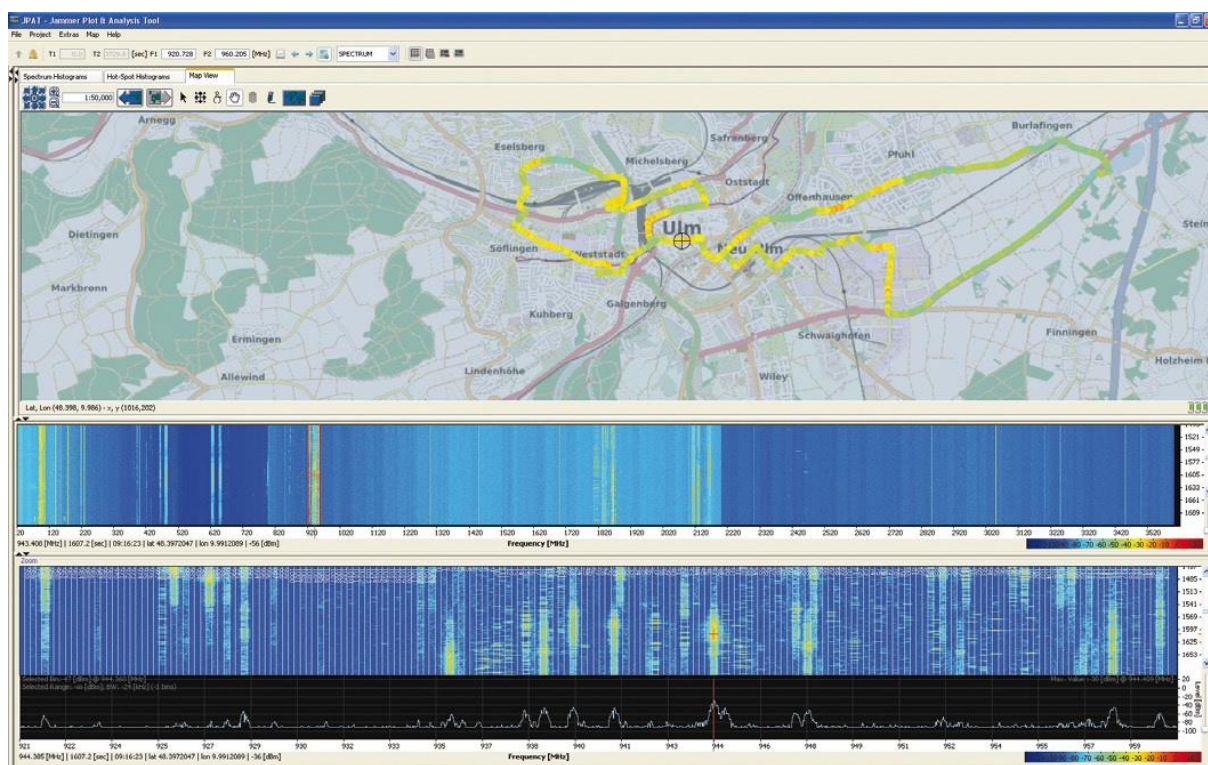
- frekvencia átfogás:
 - 20 MHz – 3,6 GHz, de opcionálisan kiterjeszthető 6 GHz-ig;
 - 1 GHz-es sávszélesség letapogatása egy időben (6 csatornán, egyenként 170 MHz-es sávszélességgel);
 - minden csatorna áthangolható/változtatható működés közben;
 - több REU összekötésével, egy időben nagyobb frekvenciaátfogás biztosítható.
- fenyegetettség észlelés:
 - analízis sebessége 9 GHz/s;
 - érzékel és azonosít 350 millió potenciális fenyegetést másodpercenként.

A zavaró berendezés képes 500.000 potenciális fenyegetésre reagálni másodpercenként. Amíg a kisugárzott teljesítménye megközelíti a 400 W-ot, a felvett teljesítmény csupán kb. 750 W (maximum 1 kW). Ezzel szemben egy hagyományos zavaró berendezésnek akár 10 kW is lehet a felvett teljesítménye.

Ennek a berendezésnek az alapvető feladata, a járművek védelme az út mentén elhelyezett rádió-távvezérlésű robbanóeszközökkel szemben, ezért körsugárzó antennával van felszerelve, hogy minden irányból védettséget biztosítson. Ezen kívül a hatástalanítás néha megköveteli, hogy a tűzszerész katona gyalogszerrel közelítse meg a robbanószerkezetet így az ő feladatát is támogatják a járműbe beépített zavaró berendezéssel, és egy irányított antenna segítségével. Ugyanez a konstrukció támogatja a járőr feladatot végrehajtó személyi állomány oltalmazását ellenséges területen, az általuk hordozott, kisteljesítményű háti zavaróeszköz kiegészítésére.

Mindezekon felül ez a berendezés képes rádióelektronikai felderítést végezni. A vevő képességei lehetővé teszik, hogy miközben reaktív zavaró módban üzemel, rögzíti a környezetében a rádiófrekvenciás jeleket, ezáltal rádiótechnikai felderítési információt biztosítva a saját csapatok számára (*Electronic Intelligence - ELINT*), valamint biztonságos körülmények között, ha nincs a jármű rádió-távvezérlésű robbanóeszköz fenyegetésének kitéve és a reaktív üzemmód kikapcsolt állapotban van, rádiófelderítésre (*Communication Intelligence - COMINT*) is alkalmas.

A rádiótechnikai felderítési információk vétele, és rögzítése nem csökkenti a védelem szintjét, az alapvető funkciójával párhuzamosan képes rögzíteni a teljes, általa átfogott spektrumban megjelenő jeleket, az időponttal és a helyzetre vonatkozó információkkal együtt. Nem igényel egyéb kiegészítő berendezést, az idő és a NAVSTAR GPS-ből származó helyzeti információk elérhetők a beépített számítógépből. Ezek az információk több szempontból is hasznosak lehetnek. A folyamatos adatrögzítésnek köszönhetően, „fekete doboz” funkciókat is ellát, továbbá a művelet befejezése után visszaellenőrizhetőek a megtett út alatt rögzített spektrum információk, aminek a későbbi elemzése során megállapítható, hogy milyen eszközök üzemeltek a jármű közelében. **(16. kép.)** Ezen adatok alapján frissíthető a veszélyes frekvenciákat tartalmazó lista, valamint hozzájárul az ellenség elektronikai harcrendjének feltérképezéséhez. Egy sikertelen RCIED támadást követően, a merénylők nagy valószínűséggel, megváltoztatják az összeköttetés paramétereit, más rádiófrekvenciás csatornát fognak alkalmazni, így a folyamatos információgyűjtés és elemzés létfontosságú.



16. kép. CASSIDIAN's Jammer Plot and Analysis Tool (JPAT)

Ha a platform biztonságos helyen van, és nincs szükség az RCIED elleni védelemre, az úgynevezett SMARTscout **(17. kép.)** kibővítéssel, képes az eszköz COMINT feladatokat is

ellátni. Minimális hardver kiegészítéssel, egy lappal felszerelve egy interaktív vagy egy teljesen automata rádiófelderítő funkció is elérhető. Interaktív működés közben az operátor, a számítógépes szoftver segítségével, kereshet és elemezhet rádiófrekvenciás jeleket, ezzel szemben, automata működés közben a rendszer önállóan gyűjti az információt, így az operátornak csak begyűjtött adatok feldolgozásával kell foglalkoznia. Mindkét üzemmód a következő folyamatokat foglalja magába:

- keresés;
- észlelés;
- moduláció felismerése;
- demoduláció;
- protokoll felismerése;
- dekódolás;
- tartalom kinyerése.



17. kép. SMARTscout rendszervázlata

Alapvetően a rendszer a következő adatszerzési módokra képes:

- felfedés, amelynek célja az új elektronikai objektumok, ezen keresztül az ellenség megjelenő elektronikai rendszerei működésének feltérképezése;
- figyelés, amelynek alapvető módszere az ellenőrzés. Az ellenőrzést az objektum fontossági fokának megfelelően, a korábban szerzett adatokkal összevetve, a változások regisztrálásával és azoknak a kiértékelőkhöz való továbbításával végzik. A különbség, hogy míg a felfedés gyakorlatilag nulla adatokkal indul, addig itt a nagymennyiségű, korábban szerzett – felfedési, figyelési – adathalmazt is kezelni kell.
- lehallgatás, amely alapvetően a jelfelderítés (SIGINT) módszere, amely az átviendő információ tartalmának, a telemetria folyamatok eredményeinek megszerzésére irányuló tevékenység. A lehallgatás az adatforrás folyamatos, megszakítás nélküli figyelését, ellenőrzését igényli. [21]

Természetesen az ellenséges kommunikáció zavarása is megoldható a Cassidian Intelligens Reszponzív Zavaró Rendszerrel, de ebben az esetben már célszerű irányított antennákat alkalmazni.[22]

ÖSSZEGZÉS

„Ez egy olyan harc, vagy háború mely különbözik minden korábbi fegyveres küzdelemtől, mert olyan ellenség ellen folyik, amely nem látható. Ez az ellenség általában nem rendelkezik sem saját országgal, sem saját kormánnyal. Nincs szervezett katonai ereje, nem visel egyenruhát, egyetlen kormánynak sem felel a tetteiért. Nem tart be egyetlen nemzetközi szerződést sem, s lehet, hogy épp mellénk ül egy buszon az a személy, mely ezt az eszmét képviseli.”[23]

Amíg megszállást követő években az Afganisztánban állomásozó nemzetközi erők nem voltak felkészülve, ilyen új, gyorsan fejlődő fenyegetésre, mint az IED támadások, ma már gyakorlatilag a legtöbb gépjármű, jelentősen páncélozott, fel van szerelve különböző zavaró berendezésekkel **(18. kép)**, így a legnagyobb veszélyben az ún. „lágy célok”, a kevésbé páncélozott járművek, gyalogos katonák és civilek vannak, valamint komplex támadás esetén a kikerkező mentőcsoporthoz és tűzszerészek.



18. kép. Oshkos M-ATV

Az improvizált robbanóeszközök ellen tett hazai és nemzetközi erőfeszítések azt mutatják, hogy ezek továbbra is nagymértékű fenyegetést jelentenek a válságkövetek térségeiben feladatot végrehajtó katonák, és a civil lakosság számára egyaránt. A probléma sokrétű és a teljes körű megoldására nincs lehetőség. Az RCIED-k elleni küzdelemben, habár nem 100%-os, de továbbra is a leghatékonyabb megoldás a rádiójelek zavarása. A reaktív

zavarók új nemzedéke, az elődeihez képest nem csak a rádióelektronikai zavarásban mutatott előrelépést, hanem a rádió-távvezérlésű robbanószerkezetek elhárításával foglalkozó szervezetek számára biztosít felderítési információt. Ez segítségül szolgálhat a zavaró berendezések és eljárások optimalizálásához, ezzel is nagymértékben hozzájárulva az erők és eszközök megóvásához.

A téma további kutatása is indokolt, mivel a rezponzív zavarokat előállító berendezések gyorsaságán, a felderített és veszélyesnek minősített adásra megjelenő válasz gyorsaságán igen sok múlik. A probléma műszaki alapját az elektromágneses hullámok véges terjedési sebessége jelenti. A térben 1 μ s alatt 300 m-t tesz meg a hullám, vagyis pl. 3 km-hez 10 μ s-ra van szükség. Ha az RCIED-t egy olyan vevőkészülék vezérli, amely reakcióideje tegyük fel éppen ennyi, akkor mire az adó jele a távvezérlőtől a zavaróállomás vevőjébe eljut, abban feldolgozásra kerül, majd a kisugárzott zavarjel tegyük fel szintén 3 km úton 10 μ s alatt teszi meg a vevőig terjedő utat, a robbanás régen bekövetkezett.

Ha egy bonyolultabb, 10-12 bites kódolón kb. 1 ms ideig tart a kódszó előállítása és értelemszerűen a dekódolása is, a geometriai távolságokból adódó futási idő elenyésző lesz, a rezponzív zavaró berendezés hatékonyan lehet képes akadályozni a vételt.

Ebből a két gondolatból nem az új fejlesztésű eszközök iránti bizalmunkat kívántam kétségbe vonni, hanem azt hangsúlyozni, hogy esetenként a hamis biztonságérzet komoly veszélybe sodorhatja az alkalmazókat. Meg kell vizsgálni a konkrét műszaki paramétereket és jobb, ha tisztában vagyunk a korlátainkkal, mint ha oktanul felelősöket keresünk a fizikailag megváltoztathatatlan korlátok miatt bekövetkező események után.

„Nem az akadályoz meg bennünket a sikerben, amit nem tudunk, hanem az, amit rosszul tudunk. (Josh Billings)”

IRODALOMJEGYZÉK

- [1] Dr. Kovács Zoltán: Az improvizált robbanóeszközök főbb típusai
Műszaki Katonai Közlöny, XXII. évf. 2. szám, p.37-52. ISSN 1219-4166
- [2] Lőrincz Gábor: Válasz az aszimmetrikus fenyegetésre. C-IED képességépítés a Magyar Honvédségben rövid és középtávon. Honvédségi Szemle, 142. évfolyam, 2. szám, p.39-51. ISSN 1216-7436
- [3] Szűcs László: Krétától Afganisztánig
<http://www.honvedelem.hu/cikk/40804> (2014.04.18.)
- [4] AJP-3.15(B) Szövetséges Összhaderőnemi Doktrína a Nem Hagyományos Módon Előállított és Alkalmazott Eszközök Elleni Tevékenységekhez. 2012. május
- [5] Schmidt Imre: A nem hagyományos módon előállított és alkalmazott robbanóeszközök elleni tevékenység és az erők megóvása összefüggése. , Hadtudomány, 2012 elektronikus szám
http://mhht.eu/hadtudomany/2012_e_Schmidt_Imre.pdf (2014.04.18.)
- [6] Kiss Zsolt: A missziókban szolgálókat fenyegető rádió-távvezérlésű bombák és az ellenük való védekezés kérdései. Hadmérnök, IV. évf. 2. szám, p. 41-56. ISSN 1788-1919
- [7] Bodnár István honvéd tisztjelölt: Zsákmányolt IED részegységek műszaki vizsgálata és a zavarásuk kérdései. Szakdolgozat, NKE Budapest, 2013.
- [8] Makk László- Hajdú László: Az improvizált robbanóeszközök alkalmazásáról.
Új Honvédségi Szemle, LXI. évf. 3. szám, p. 5-21. ISSN 1216-7436
- [9] Operation Iraqi Freedom - Iraqi Deaths
<http://icasualties.org/Iraq/IraqiDeaths.aspx> (2014.04.18.)
- [10] Mező András: A rögtönzött robbanószerkezetek elhárításáról. Honvédségi Szemle, 63.évf., 1.szám, p. 17-19. ISSN: 1216-7436
- [11] Dr. Ványa László: Pilóta nélküli repülőgépek és földi eszközök rádió-távírányítású alkalmi robbanótestek (RCIED) elleni harcban. Repüléstudományi Konferencia 2008. április 11. http://www.szrfk.hu/rtk/kulonszamok/2008_cikkek/Vanya_Laszlo.pdf (2014.04.18.)
- [12] Guidelines for interservice electronic warfare (EW) support to explosive ordnance to explosive disposal (EOD) operations on multinational deployments
Study 2607 EOD Volume 2, 2010. február.

[13] Dr. Ványa László: Rádióösszeköttetések aktív zavarásának elve, energetikai viszonyok számvetése, időparaméterek. EHV berendezések rendszertana III. oktatóanyag. NKE HHK IEH Tanszék.

[14] Eduardo Serantes: RF Jammers: Advanced military technologies in homeland security Counter-IED Report, Autumn/Winter 2013. p. 69-74.

[15] Dr. Franco Fiore - Agata Szydelko: Remotely Controlled IED jamming and radio frequency spectrum challenges: fratricide jamming and interoperability among NATO and coalition forces. Counter-IED Report, 2013 Spring/Summer. p.75-78.

[16] TMP Házilag készítésű távvezérelt robbanóeszközök elleni hordozható szélessávú zavaróberendezés, Műszaki leírás, kezelési karbantartási és tárolási utasítás Carinex Ipari, Kereskedelmi és Szolgáltató Kft. 2011

[17] Protection RCIED Modular Jammer Family
http://www.idexuae.ae/exhibitorlibrary/1524/star_urc_2.pdf (2014.04.18.)

[18] Amesys-Shadow
<http://www.shadow.amesys.fr/> (2014.04.18.)

[19] Bull launches Shadow: a signal jamming system - unique in the world - designed to prevent attacks from remote-controlled improvised explosive devices.
http://www.wcm.bull.com/internet/pr/new_rend.jsp?DocId=640945&lang=en (2014.04.15.)

[20] Dr. Torben Brack, Dr. Hubert Piontek: Smart responsive jamming for military vehicle and convoy protection againsts RCIED attacks. Counter-IED Report, Summer 2012. p. 15-19.

[21] Dr. Ványa László: A rádióelektronikai felderítés, iránymérés, helymeghatározás ppt EHV berendezések rendszertana III. oktatóanyag. NKE HHK IEH Tanszék.

[22] Jürgen Geerkens, Dr. Hubert Piontek: Smart Responsive Jamming goes COMINT: Distributed mobile EW sensors for current and future operational theatres. Counter IED Report, Spring/Summer 2013. p. 79-83.

[23] Daruka Norbert: Bűnös célú robbanószerkezetek alkalmazásának és hatástalanításának sajátosságai. Műszaki Katonai Közlöny, XXII. évfolyam, 2012 különszám p.26-34.
ISSN 1219-4166

ÁBRAJEGYZÉK

1. ábra. Az afganisztáni veszteségek és ezen belül az IED-k részesedése
<http://icasualties.org/oef/> (2014.04.14.)

2. ábra. Az IED hálózat működése
Schmidt Imre - A nem hagyományos módon előállított és alkalmazott robbanóeszközök elleni tevékenység és az erők megóvása összefüggése, Hadtudomány, 2012 elektronikus szám, p. 8. http://mhht.eu/hadtudomany/2012/2012_elektronikus/2012_e_Schmidt_Imre.pdf (2014.04.24.)

3. ábra. Zavarási módok spektrum szerint
Elektronikai ellentevékenység, Dr. Haig Zsolt, oktatóanyag

4. ábra. A reaktív zavaró berendezés elvének sebezhetősége
RF Jammers: Advanced military technologies in homeland security
Eduardo Serantes, Counter-IED Report, Autumn/Winter 2013, p. 72.

5. ábra. A TMP 0512 egység kialakítása
TMP Házilag készítésű távvezérelt robbanóeszközök elleni hordozható szélessávú zavaróberendezés, Műszaki leírás, Carinex Ipari, Kereskedelmi és Szolgáltató Kft. 2011 kezelési karbantartási és tárolási utasítás p. 6.

6. ábra. A TMP programozási eljárása.
Richard Edwards, TMP System Overview ppt.

7. ábra. A zavarási megoldások fejlődése
Jürgen Geerkens, Dr. Hubert Piontek: Smart Responsive Jamming goes COMINT: Distributed mobile EW sensors for current and future operational theatres.
Counter IED Report, Spring/Summer 2013, p. 79.

TÁBLÁZATOK

1. táblázat. Tipikus frekvenciatartományok és szokásos teljesítmények
Kiss Zsolt: A missziókban szolgálókat fenyegető rádió-távvezérlésű bombák és az ellenük való védekezés kérdései, Tudományos Diákköri Pályamunka 2008. ZMNE, Kutató Könyvtár, p. 18.

KÉPEK JEGYZÉKE

1. kép. Szerelt harckocsi akna és tüzérségi lövedékek

http://en.wikipedia.org/wiki/File:IED_Baghdad_from_munitions.jpg (2014.04.14.)

2. kép. Áldozat által működésbe hozott, nyomással indítható IED

<http://www.kateholt.com/galleries/editorial/afghanistan-vi> (2014.04.14.)

3. kép. Időzítővel ellátott IED

<http://3.bp.blogspot.com/->

[1sPa9MbhcU0/TV3Q_O_xKrI/AAAAAAAAADg4/3tmUqkEYp1Q/s1600/ied4.jpg](http://3.bp.blogspot.com/-1sPa9MbhcU0/TV3Q_O_xKrI/AAAAAAAAADg4/3tmUqkEYp1Q/s1600/ied4.jpg) (2014.04.14.)

4. kép. Cipőbe rejtett IED röntgenképe

<http://www.nato.hr/galerije/nato-i-borba-protiv-terorizma---ien-ied> (2014.04.14.)

5. kép. Vezetékes indítású IED hatástalanítása

<http://www.popularairsoft.com/wired-magazine-defeating-ieds> (2014.04.14.)

6. kép. Mobiltelefonnal indítható IED

<http://kk.org/streetuse/2006/08/>

7. kép. A STAR V antennái

Protection RCIED Modular Jammer Family

http://www.idexuae.ae/exhibitorlibrary/1524/star_urc_2.pdf (2014.04.16.)

8. kép. STAR V zavaró berendezés

<https://janes.ihs.com/CustomPages/Janes/DisplayPage.aspx?DocType=Reference&ItemId=++1594662&Pubabbrev=JC4IL> (2014.04.16.)

9. kép. STAR Light 3 zavaró berendezés

<https://janes.ihs.com/CustomPages/Janes/DisplayPage.aspx?DocType=Reference&ItemId=++1594662&Pubabbrev=JC4IL> (2014.04.16.)

10. kép. STAR Light 6 zavaró berendezés

<https://janes.ihs.com/CustomPages/Janes/DisplayPage.aspx?DocType=Reference&ItemId=++1594662&Pubabbrev=JC4IL> (2014.04.16.)

11. kép. STAR Manpack zavaró berendezés

<https://janes.ihs.com/CustomPages/Janes/DisplayPage.aspx?DocType=Reference&ItemId=++1594662&Pubabbrev=JC4IL> (2014.04.16.)

12. kép. Black Shadow zavaró berendezés
<http://www.shadow.amesys.fr/> (2014.04.18.)

13. kép. Raid Shadow zavaró berendezés
<http://news.bull.com/bulldirect/2012/11/01/bull-unveils-raid-shadow-the-new-lightweight-and-compact-smart-reactive-signal-jammer-and-extends-its-range-of-jamming-solutions/>
(2014.04.16.)

14. kép. Comjam Shadow zavaró berendezés
<http://www.shadow.amesys.fr/> (2014.04.18.)

15. kép. A Cassidian intelligens zavaró berendezése egy terepjáróba beépítve
Jürgen Geerkens, Dr. Hubert Piontek: Smart Responsive Jamming goes COMINT: Distributed mobile EW sensors for current and future operational theatres. Counter IED Report, Spring/Summer 2013, p. 79.

16. kép. CASSIDIAN's Jammer Plot and Analysis Tool (JPAT)
Jürgen Geerkens, Dr. Hubert Piontek: Smart Responsive Jamming goes COMINT: Distributed mobile EW sensors for current and future operational theatres. Counter IED Report, Spring/Summer 2013, p. 81.

17. kép. SMARTscout rendszervázlata
Jürgen Geerkens, Dr. Hubert Piontek: Smart Responsive Jamming goes COMINT: Distributed mobile EW sensors for current and future operational theatres. Counter IED Report, Spring/Summer 2013, p. 82.

18. kép. Oshkos M-ATV
<http://arma3game.ru/wp-content/uploads/2013/04/oshkosh-m-atv-2.jpg> (2014.04.18.)