

Végvári Zsolt¹ 

A rádióvezérelt improvizált robbanóeszközök elleni védelem

Protection against Radio-Controlled Improvised Explosive Devices

Magyarországon – a szomszédunkban zajló orosz–ukrán, illetve a gázai háború ellenére – az improvizált robbanóeszközök (IED-k) most kevésbé vannak reflektorfényben, mint korábban az afganisztáni és iraki szövetséges megszállás alatt voltak, de ezek továbbra is veszélyes fegyverek. A világ távolabbi részein zajló fegyveres összecsapásokban és az említett két konfliktusban is alkalmazzák őket. Mivel valószínűleg a belátható jövőben is veszélyt jelentenek mind a haderőkre, mind a civil lakosságra, a védekezés ellenük továbbra is kulcsfontosságú. Ez az írás az IED egyik fajtája, a rádió-távvezérelt eszközök elleni védekezés módszereit és lehetőségeit mutatja be.

Kulcsszavak: improvizált robbanóeszköz, IED, rádió-távírányítás, zavarás

In Hungary, with the Russo-Ukrainian war and the war in Gaza, improvised explosive devices (IEDs) are less in the spotlight now than they were during the allied occupation of Afghanistan and Iraq, but they still remained dangerous weapons. They are still used in armed conflicts in remote parts of the world and in these two conflicts too. As they are likely to continue to pose a threat to both military forces and civilians for the foreseeable future, defending against them remains elemental. This article describes the methods and options for countering one type of IED, the radio-remotely controlled device.

Keywords: improvised explosive device, IED, radio remote control, jamming

¹ Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Haditechnikai Tanszék, e-mail: Vegvari.Zsolt@uni-nke.hu

Bevezetés

Az improvizált robbanóeszközök olyan robbanószerkezetek, amelyek nem gyárban, hanem a hadszíntéren megtalálható, jellemzően nem katonai anyagok felhasználásával, ügyes kezű emberek által ad hoc módon összeszerelve készülnek. Az aszimmetrikus hadviselés tipikus fegyverei, a gerillák kedvelt eszközei a nagyobb hagyományos katonai erőt felvonultató reguláris hadseregek ellen, de a terroristák is széles körben alkalmazzák.

Az improvizált robbanóeszközök alkalmazása és típusai

Lényegében a puskapor feltalálása óta megvan a lehetőség improvizált robbanóeszközök alkalmazására, de csak a 20. század első felétől beszélhetünk szignifikáns jelenlétről. Az első, jelentős számban használt IED-nek (*improvised explosive device*) a Molotov-koktél tekinthető. Vietnámban is alkalmaztak úgynevezett Body-trapeket (lényegében aláaknázott holttesteket), de az IED-vel végrehajtott támadások csak a 21. században érték el azt a szintet, hogy napi témává váljanak.² Ennek oka, hogy bizonyos országokban, ahol a reguláris haderő (ha volt ilyen) alulmaradt egy másik fegyveres erővel szemben, de az ellenállásnak megmaradt a bázisa a lakosság körében, akkor a kialakuló gerillamozgalom az internetet használva könnyen és egyszerűen hozzájuthat ahhoz a minimális tudáshoz, ami egy ilyen eszköz építéséhez kell, illetve a globalizált kereskedelem révén maguk a szükséges összetevők is elérhetők. Ezek a feltételek a megelőző időszakban nem álltak fent, ezért volt lényegesen kevesebb ilyen jellegű támadás például a vietnámi háború során.³

A szövetséges megszállást követően csak Afganisztánban 2009-ben 9300 darab, 2010-ben 15200 darab, míg 2011-ben 16500 darab IED-t észleltek és hatástalanítottak.⁴ Ez a fenyegettség a megszállás alatt folyamatosan fennállt, a nem hatástalanított improvizált robbanóeszközök 2011 és 2020 között Irakban és Afganisztánban összesen közel 3000 szövetséges katonát öltek meg, ami a teljes veszteség közel 50%-a. A járulékos civil veszteség ennek legkevesebb a négyszerese volt.⁵

A cikk írásakor nagy intenzitással zajlik az orosz–ukrán háború a szomszédunkban, de itt reguláris haderők csapnak össze, amelyek rendszeresített fegyverzete jóval hatékonyabb bármilyen improvizált eszköznél, így nincsenek igazán rászorulva arra, hogy kisipari módszerekkel hozzanak létre robbanóeszközöket. Mindezzel együtt az orosz támadást követően felröppentek meg nem erősített hírek, hogy a megszállt területeken az orosz erők ilyeneket alkalmaztak.⁶

Az viszont tény, hogy az orosz inváziót megelőző 12 évben az oroszbarát szakadár erők nagyszámú, évente 50–100 IED-támadást hajtottak végre,⁷ amelyek azért kaptak kisebb publi-

² KISS 2009.

³ DARUKA 2014.

⁴ HORVÁTH 2018.

⁵ A Decade of Global IED Harm Reviewed 2020.

⁶ PONNEZHATH 2022.

⁷ VÉGH 2022.

citást, mert elsősorban a Donyeck és Luhanszk régiókra koncentráltak, ahol egyébként szinte napi rendszerességgel voltak hagyományos fegyveres összecsapások is. A támadások többsége nem direkt emberélet ellen irányult, főleg az ukrán fegyveres erők mozgását igyekeztek gátolni.



1. ábra: Egy legalább két halálos áldozattal járó IED-támadás nyomai (2015, Donyeck)

Forrás: *Ukraine Crisis: Burnt-out Shells of Buses Following Attack 2015*

A cikk írásakor szintén zajló gázai konfliktusban dokumentáltan alkalmaz ilyeneket a Hamász, de mivel az izraeli erők csak igen lassan és óvatosan, a tűzéréség és a légerő intenzív alkalmazásával nyomulnak előre, kevés áldozatot szednek ezek a szerkezetek.⁸ Tulajdonképpen az izraeli támadást megelőzően gyakrabban vetettek be ilyen robbanóeszközöket a palesztin ellenállás tagjai,⁹ bár a nem megfelelő képzés hiányában ez gyakran öngyilkos küldetésnek bizonyult.¹⁰

Bár Magyarországon, illetve Európában a figyelem erre a két konfliktusra összpontosul, eközben a világ távolabbi részein továbbra is számos áldozatot szednek az improvizált robbanóeszközök. Egy londoni székhelyű szervezet 2023 első félévében összesen 640 igazolt IED-robbantást dokumentált, ezek során 450 ember halt meg, és további 1000 személy sérült meg súlyosan.¹¹ Ez a szám a vizsgált időszakban robbanás áldozatává vált civil személyek 16%-a, ami – figyelembe véve, hogy ekkor éppen egy több mint 1000 kilométeres frontszakaszon zajlott az orosz–ukrán háború – döbbenetesen nagy. A gázai konfliktus palesztin források szerint több mint 30 000 civil áldozatot követelt már, ami mellett az IED-k által okozott veszteségek eltörpülnek, de az látható, hogy az IED-k által jelentett fenyegetés továbbra is valós.

Az improvizált robbanóeszközöknek számtalan formája ismert, de annyi közös bennük, hogy az eszközökben okozott pusztításon és az élőerő pusztításán túl a média hatására többnyire van egy kognitív dimenzióban kifejtett hatásuk is. Emiatt gyakran választanak a készítők szimbolikus célpontokat. Az IED-k többféle módon is csoportosíthatók, például a célpontjuk szerint:¹²

⁸ PANELLA 2023.

⁹ Improvised Explosive Device IED 2024.

¹⁰ Palestinian Teens Killed in Accidental Blast While Handling Explosives 2023.

¹¹ OVERTON 2023.

¹² KOVÁCS 2012.

- épületek (állami, kormányzati, katonai létesítmények, középületek stb.);
- rendezvények helyszínei (piac, sportcsarnok, kiállítás, átadóünnepség);
- közművek elemei (elektromos hálózat, víz-, gázközműhálózat);
- közlekedési csomópontok, létesítmények.

De az alkalmazó gerillák sokszor nem valamilyen infrastrukturális elemet támadnak, hanem az ellenséges megszálló erők katonáit, a velük együttműködő politikai, gazdasági vezetőket, azok létesítményeit és gyakorta a járműveiket. E támadásoknak erős a szimbolikus jelentőségük, hiszen tényleges katonai veszteségeket okoznak a megszállóknak, miközben nem tesznek jelentős kárt a megszállt terület polgári lakossága által is használt infrastruktúrában, amely gyakran egyébként is szegényes és/vagy sérült.

Az improvizált robbanóeszközök felépítése is egyszerű sémát követ. Van egy burkolat, ami összefogja és jobb esetben álcázza is az eszközt, illetve valamilyen robbanóanyag, amelynek mennyisége a cél és lehetőség függvényében minél több. Ezt – az internetet segítségül hívva – viszonylag szerény vegyészeti tudással is elő lehet állítani például műtrágyából, de háborús területen gyakran használják a fel nem robbant lövedékekben található robbanóanyagot, vagy esetleg a zsákmányolt lőszeres indítótölteteiben található robbanóanyagot, esetleg magát a lőszeret vagy lövedéket.¹³ Ha az IED-t élőerő ellen kívánják alkalmazni, akkor repeszképző anyagokat is el szoktak helyezni a robbanóanyag körül.



2. ábra: 105 mm-es tüzérségi lövedékből kialakított robbanóeszköz és az elhelyezése egy amerikai támaszpont közelében (2005, Afganisztán)

Megjegyzés: az első felvételen jól látható a vezeték elvezetése

Forrás: *Improvised Explosive Devices. TRADOC DCSINT Handbook 2006*

A robbanóanyag fajtájától függően kell egy gyújtószerkezet, ami szintén lehet háborús területen talált katonai gyújtószerkezet, gyutacs, esetleg bányászati detonátor vagy valamilyen házilag előállított gyutacs is. Mindezekon túl már csak egy működtető mechanizmus szükséges. Ez lehet valamilyen időzítő (*time operated IED*), valamilyen, az áldozat által

¹³ Kovács 2012.

működésbe hozott mechanizmus (*victim operated IED*), például mechanikus érzékelő (igen csekély számban, de előfordul passzív infravörös érzékelő használata is) vagy távirányító (*command operated IED*).¹⁴

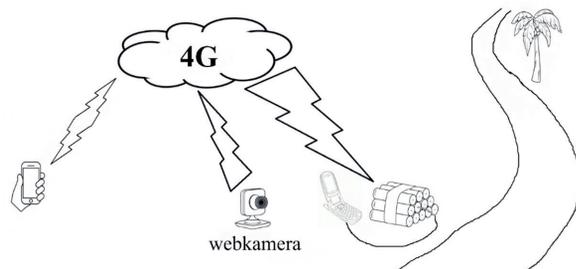
Az első két lehetőséget az elkövetők viszonylag óvatosan alkalmazzák, mert nem garantálható, hogy a választott célpont, és lehetőség szerint csak az semmisüljön meg a robbanásban. Időzítő esetében elfordulhat, hogy a működésbe lépés időpontjában civilek tartózkodnak a közelben, míg a mechanikus (vagy infravörös) érzékelők esetében szintén van arra esély, hogy azt nem az ellenséges katonák, hanem esetleg játszadozó gyerekek hozzák működésbe. Az ilyen, jelentős számú civil áldozattal és minimális vagy semmilyen katonai áldozattal járó robbantások kontraproduktívak a robbantó személy vagy szervezet szempontjából, hiszen csökkenti a lakossági támogatást. Ez utóbbit az elkövetők pedig mindenképpen igyekeznek megtartani, hiszen a robbanóeszközök építését és elhelyezését igen nehéz a lakosság figyelmét elkerülve végezni, az a valóságban többnyire a civilek jelentős részének tudtával és hallgatólagos egyetértésével történik.

A fenti „balesetek” elkerülhetők, ha a robbanóeszközt öngyilkos merénylő viszi a célpont közelébe, ami nyilvánvalóan nem minden merénylő számára vonzó lehetőség, vagy úgy, ha a robbanóeszközt távirányítással hozzák működésbe, akkor, amikor az a célpontban (és lehetőség szerint csak abban) a legnagyobb kárt okozza. A távirányítás legegyszerűbb módja egy vezeték a robbanóeszköz és működtető személy búvóhelye között, de ennek is vannak hátrányai. Ha a vezetéket csak egyszerűen lefektetjük, azt könnyű észrevenni, ha pedig elásuk, akkor az azzal járó földmunka szintén nehezen álcázható, viszonylag könnyen felfedhető. Mindezekon túl a vezeték villamos ellenállása miatt a távirányíthatóság távolsága limitált (törpe egyenfeszültség esetén csupán néhányszor 10 méter), illetve, ha a működtető személy túl messzire van az eszköztől, az megnehezíti a célpont azonosítását is. A túl közel elhelyezkedő merénylő viszont a saját testi épségét kockáztatja, illetve megnehezíti a menekülését is.

A rádióvezérelt improvizált robbanóeszközök és a védelem lehetőségei

A fentiekből látszik, hogy az elkövetők számára a legjobb megoldás a vezeték nélküli távműködtetésű eszközök alkalmazása, vagyis a rádió-távirányítású improvizált robbanóeszközök (RCIED – *radio controlled improvised explosive device*) építése. Ez a megoldás szinte teljesen kizárja az IED nem akaratlagos működtetését, azaz a nem kívánt áldozatokat, miközben kellő távolságot biztosít az operátornak a menekülésre is. Sőt, a rádió-távirányítás egy speciális formája, a mobiltelefonos megoldás, akár azt is lehetővé teszi, hogy a merénylő több 100 km-re legyen a robbantás helyétől, bár, ha a célpont például egy mozgó jármű, akkor figyelembe kell venni a késleltetést is.

¹⁴ Kiss 2009.



3. ábra: A mobilszolgáltatók internetelérésével akár egy másik országból is működtethető az RCIED

Forrás: a szerző szerkesztése

Mivel improvizált eszközről van szó, a távirányító sem erre a célra készült. Bár egy egyszerű rádió adó-vevő elkészítése egyébként nem túl bonyolult, az elkövetők többnyire nem mérnökök vagy technikusok, így azt más készülékekből szerelik ki és alakítják át. Általánosan elterjedt megoldás a mobiltelefonos működtetés, amikor egy mobilkészüléket automatikus hívásfogadásra állítva kötnek az elektronikus gyújtóra. Viszonylag olcsó és egyszerűen kivitelezhető, hiszen bármilyen régi telefon és egy feltöltős SIM-kártya is elégséges hozzá, de mindenképpen stabil mobilszolgáltatásnak kell lennie a robbantás tervezett helyszínén.

Bármilyen más, könnyen beszerezhető rádióeszköz is felhasználható. A teljesség igénye nélkül: garázkapunyító, autóriasztó, vezeték nélküli csengő, walkie-talkie, modellautó-távirányító. A kisebb adóteljesítményű eszközök (például garázkapunyító) néhány 10 méterről, egy komolyabb adóteljesítményű walkie-talkie akár több kilométerről is képes elindítani a robbanóeszközt.

Az IED-ek elterjedése természetesen azt eredményezte, hogy fejlődött az ellenük való védekezés is. A legjobb védelem a megelőzés, vagyis IED-k építésének és telepítésének megakadályozása, illetve a mégis telepített IED-k észlelése és hatástalanítása még a robbantást megelőzően. A híradásokba csak a robbantások kerülnek, de azt azért tudni kell, hogy az IED-k egy jelentős részét időben felfedezik és hatástalanítják. Ehhez komoly felderítőmunka szükséges, illetve jó kapcsolatok ápolása a helyi lakossággal, hiszen ők csaknem biztosan észreveszik, ha a lakóhelyük mellett valaki egy bombát helyez el. Sok más mellett ez a fő oka, hogy a korszerű katonai műveleteknek mindig része a CIMIC,¹⁵ vagyis a helyi lakossággal való együttműködés (*civil-military cooperation*). Meg kell említeni a műszaki csapatokat, akik mentesítik a hadiutakat, és a tűzszerészek áldozatos munkáját is, akik az életük kockáztatásával semlegesítik ezeket a szerkezeteket.

Sajnos minden igyekezet és a lakosság nagyfokú együttműködése esetén sem lehet teljesen kizárni, hogy műveleti területen improvizált robbanóeszközöket helyezzenek el, illetve az elhelyezett eszközök sem mindig deríthetők fel. Ennek megfelelően léteznek egy általános IED elleni védelmi módszer, ami a robbanás hatásainak csökkentésére, kivédésére irányul. Ez független az IED működtetésének módjától, általánosan igaz mindegyik típusra, hogy a már bekövetkezett robbanás következményeit igyekeznek mérsékelni. Személyi védelemről sajnos

¹⁵ Fieldtrip to the Counter-IED Centre 2015.

nem igazán lehet beszélni, mivel egy katona által hordozható felszerelés mérete és tömege nem teszi lehetővé, hogy egy, a közelben bekövetkező robbanás hatásaitól az hatékonyan óvja őt. A műveleti területen jellemzően viselt repeszálló mellény (*plate carrier*) és a sisak ad egy minimális védettséget, de további védőelemek hozzáadására már nincs mód.

Járművek esetében már van racionalitása az IED elleni védelem kialakításának. A harcjárművekre vonatkozóan az Allied Engineering Publication¹⁶ 55-ön (AEP55) alapuló NATO STANAG 4569 definiál védelmi szinteket. Ez adott védelmi szintekhez meghatározza azt a lövedéktípust, amely még nem képes átütni, továbbá, hogy egy 155 mm-es repeszromboló gránát repeszai hány méterről nem képesek átütni a páncélt. A szabvány tartalmaz aknák elleni védelmet is, ahol a brizáns robbanóanyag tömege a meghatározó. Az adott szintnek megfelelő páncélt az alábbi robbanóanyag-mennyiségek detonációja esetén véd:

- Level 1: kézigránát;
- Level 2: 6 kg (2a – kerekek lánctalpak alatt vagy 2b – jármű padlólemeze alatt);
- Level 3a és b: 8 kg;
- Level 4a és felett: 10 kg.

Az IED-k elleni védelem még nem került bele a szabványba, de a nem megfelelő védelem okozta halálesetek nyomán az amerikai hadsereg már 2006 elején elindította az úgynevezett MRAP-programot.¹⁷ Az MRAP-járművek – elsősorban az IED-k által leginkább veszélyeztetett könnyű harcjárművek – esetében a tervezéskor már fokozott mértékben vették figyelembe az IED-k hatásait. A haspáncél jellemzően „V” kialakítású, ami a detonáció energiáját a jármű két oldalán elvezeti, illetve a függesztett ülések megakadályozzák a személyzet lábsérüléseit. A leginkább konvoj kíséretre specializált járművek felismerhetők a viszonylag magas felépítésükről. Az IED-k elleni védelem ára sajnos az irányíthatóságot negatívan befolyásoló magasabb súlypont.¹⁸



4. ábra: Irakban a magyar katonák által is használt Navistar International MaxxPro Plus MRAP jármű (2013, Erbil)

Forrás: Hungarian Army Receive 12 MRAP Armoured Vehicles MaxxPro Plus from United States 2013

¹⁶ Szövetséges Műszaki Kiadvány.

¹⁷ *Mine-Resistant Ambush Protected* – kb. aknavédett és meglepetéstámadástól védett.

¹⁸ GÁVAY 2014.

A létesítmények IED elleni védelme elvben még egyszerűbb, hiszen lehetőség van falak, kerítések és egyéb védművek, például vasbeton merevítések építésére, ugyanakkor a gyakorlatban az adott terület sajátosságai, a pénzügyi és műszaki lehetőségek nagyban befolyásolják a tényleges megvalósítást.¹⁹

Az RCIED-ek elleni zavarásos védelem

Kimondottan az RCIED-ek elleni védekezésnek van egy más esetekben nem használható módja is, ez a zavarás (*jamming*). Ilyenkor nem tudjuk biztosan, hogy az érintett területen van-e RCIED, de feltételezzük, hogy lehet, ezért azokat a frekvenciasávokat, amelyeket a robbanóeszközök építői jellemzően használnak, egy nagy teljesítményű zavarjellel elnyomjuk, így megakadályozva a RCIED adója által sugárzott jel észlelését a vételi oldalon. A kereskedelmi forgalomban elérhető rádióeszközök sugárzási teljesítménye korlátozott, ráadásul a rádiójel erőssége a távolság négyzetével arányos módon csökken. Feltételezve, hogy egyébként is közelebb vagyunk az RCIED vevőjéhez, mint a robbantó, egy kellően nagy teljesítményű zavaróadóval (*jammer*) gond nélkül „túl lehet kiabálni” a RCIED adóját, megakadályozva a detonációt. Mivel az elkövetők ritkán rendelkeznek egy rádióberendezés megépítéséhez szükséges műszaki ismeretekkel és anyagokkal, az esetek csaknem 100%-ában üzletben kapható rádióeszközöket használnak fel. A jellemzően használt frekvenciasávokat az 1. táblázat tartalmazza.

1. táblázat: RCIED-eszközökhöz gyakran használt rádióberendezések

Frekvencia	Jellemző eszköz	Jellemző adóteljesítmény	Jellemző hatótávolság	Megjegyzés
25–28 MHz	CB-rádió	0,1–4 W	több km	több sávban
27, 35, 41 és 48 MHz	gyermekjáték, távirányítók	0,1 W	100 m	
27, 35, 41 és 48 MHz	modell-távirányítók	1 W	km	
136–174 MHz	ipari eszközök	1–5 W	km	több sávban, COTS-eszközként ²⁰
139–170 MHz	játékkontroller	1 W	100 m	több sávban
308–345 MHz	garázsnyitók, riasztók, vezeték nélküli csengők	0,1 W	10–100 m	több sávban
435 MHz	WLAN-rendszerek	0,1–1 W	km	jellemzően irányított antennával
446 MHz	walkie-talkie	0,5 W	km	
900 MHz	GSM	1–2 W	cellafüggő	
1800, 1900 MHz	GSM	1–2 W	cellafüggő	
2100 MHz	3G (UMTS)	1–2 W	cellafüggő	
2400 MHz	WLAN-rendszerek	1–2 W	km	jellemzően irányított antennával
2600 MHz	4G (LTE)	1–2 W	cellafüggő	
700, 3500 MHz, 26 GHz	5G	1–2 W	cellafüggő	

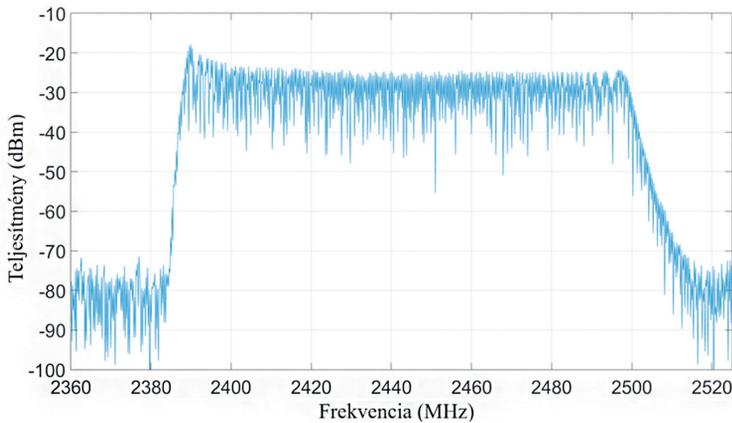
Forrás: Rádióalkalmazási táblázat 2009 alapján a szerző szerkesztése

¹⁹ KOVÁCS 2013.

²⁰ *Commercial On The Self* – polcról levehető kereskedelmi termék.

A jammer tehát egy olyan rádióadó, amely nagy teljesítményű zavarjelet sugároz, az adott frekvencián megbénítva a kommunikációt. Egyszerű lenne a helyzet, ha ismernénk azt a frekvenciát, ahol RCIED működtetésére számítani lehet, csupán erre a frekvenciára kellene hangolni a jammert, és készen is lennénk. Sajnos azonban a fenti frekvenciák bármelyikén lehet számítani RCIED-támadásra, így valamennyit zavarni kellene. Ezt úgy oldják meg, hogy a jammer a teljes kijelölt spektrumban „végigseper” a frekvenciákon. Persze nem analóg módon, hanem időosztásos belépéssel (*time division multiple access* – TDMA). Vagyis a jammer elkezd sugározni a spektrum legalsó frekvenciáján, de csak néhány μs -ig, majd átlép a következő frekvenciára, ami pont akkora távolságra van az elsőtől, ami egy tipikus kommunikációs csatorna sávzélessége. Itt is eltölt néhány μs -ot, majd továbblép a következő frekvenciára és így tovább. Amikor végigért a kijelölt sávon, akkor kezdi előlről, így folyamatosan lefoglalja a teljes, zavarásra kijelölt frekvenciatartományt.

Ez elméletben nagyon szép, de mivel a rádiófrekvenciás energia létrejöttéhez is egy véges idő szükséges, nem azt fogjuk látni a spektrumban, hogy a példának okáért 10 W-os jammer egy 10 W-nak megfelelő (40 dBm) zajfüggőnyt hoz létre a zavart sávban, hanem egy annál szignifikánsan alacsonyabb szintű zajfüggőny jön létre. Tulajdonképpen az adó teljesítményét „szétkenjük” a spektrumban.



5. ábra: 2,4 GHz-es wifisávban működő jammer spektrumképe

Forrás: ROMERO et al. 2018

Néhány évtizeddel ezelőtt még komoly problémát okoztak volna a hagyományos rezgőköröket alkalmazó rádióeszközök, itt ugyanis a rezgőkör elemeinek (tekercs, kondenzátor) módosításával egyszerű mód volt a működési frekvencia megváltoztatására. Szerencsére a korszerű kompakt rádióeszközök már digitális frekvenciaszintézert alkalmaznak, így ezek működési frekvenciája csak szoftveres úton és csak az áramkör gyártója által meghatározott tartományon belül lehetséges. Ez azt jelenti, hogy minimális az esély arra, hogy az elkövetők olyan rádióeszközhöz jussanak, ami a táblázatban foglalt sávoktól eltérő tartományban működik, vagyis jól behatárolhatók azok a spektrumrészek, ahol RCIED működtetésével kell számolni.

Fontos megjegyezni, hogy a legtöbb, az 1. számú táblázatban található eszköz úgynevezett „mozgó” rádióberendezés, vagyis mivel az ellenállomás helyét nem tudjuk pontosan, mind az adó-, mind a vevőkészülék antennája horizontálisan körsugárzó (az adó a tér minden irányába egyforma teljesítménnyel sugároz, a vevő a tér minden irányából egyformán érzékeny). Az esetek többségében ez egy egyszerű botantennát jelent. Ennek magassága viszont hatással van az áthidalható távolságra. A jobban álcázható, kisebb antennák értelemszerűen kisebb áthidalható távolságot eredményeznek.

Az antennák vonatkozásában különösen veszélyesek az ipari WLAN-eszközök, amelyeket például egy egymástól közúttal elválasztott két telephely összeköttetésére használnak. Itt a két állomás helye fix, ezért irányított antennákat használnak, vagyis a rádiófrekvenciás teljesítményt (és az érzékenységet) az ellenállomás irányában nyalábbá formálják, így többszörösére emelve az áthidalható távolságot. Szerencsére az irányított karakterisztikájú antennák, mint például a parabola, nehezen álcázhatók, illetve az irány pontos beállításához már átviteltechnikai ismeretek is szükségesek.

Az antennák elhelyezkedése egyébként is igen fontos. A több 100 MHz-es és az a feletti frekvenciatartományban a rádióhullámok terjedése a fényéhez hasonló, az összeköttetés elvben optikai rálátást igényel. A rádióhullámok azonban a különféle természetes és mesterséges tereptárgyokról visszaverődnek, és az azonos forrásból induló, de különféle utakon terjedő hullámok egymással találkozáskor interferálódhatnak, vagyis hatással vannak egymásra, és a fázistól függően erősítik vagy gyengítik egymást. Ennek megfelelően a vett jel erőssége akár néhány m²-en belül is jelentős eltéréseket mutathat.

Ahhoz, hogy a zavarójel a terület minden pontján biztosan erősebb legyen az RCIED adójának jelétől, meg kell oldani, hogy se az interferencia, se a különféle tereptárgyak árnyékoló hatása ne okozza azt, hogy a zavarójel „árnyékba” kerüljön. Ennek érdekében a jammerek több antennát is használnak ugyanannak a sávnak a besugárzására. Azok a jammerek, amelyek széles frekvenciatartományban képesek zavarni, egyébként is több rádiófrekvenciás végerősítőt tartalmaznak, mivel az erősítők csak viszonylag szűk tartományban képesek lineáris karakterisztikát nyújtani. Az eltérő hullámhosszokon tapasztalható eltérő hullámterjedés miatt a végfokozatokhoz különböző antennarendszerek is tartoznak.



6. ábra: Gépkocsira szerelt és kézi RCIED-zavarókészülék

Forrás: Supply of RCIED Vehicle Jammers to U.N. [é. n.]; Integrated Electronic Defense Technology System [é. n.]

A kézi zavaróeszközök esetében az antennák lehetséges elhelyezése a készülék méreteitől fogva nagyjából adott, de gép- és harcjárművek esetében több lehetőség is van. A 6. ábrán látható személygépkocsik esetében a karosszérián körben elhelyezve nyújtanak a legjobb lefedettséget az antennák, ám ez zavarná a sofőr kilátását, így maradt a tető. Harcjárműveknél is megfontolandó a tornyon történő elhelyezés, hiszen ez sem a kilátást, sem a fedélzeti fegyverek alkalmazását nem befolyásolja, ám a páncéltest jelentős árnyékoló hatása miatt közvetlenül a jármű mellett holtterek alakulhatnak ki. Részben ennek kompenzálására, illetve mivel az áramforrás tömege itt nem releváns, a járműfedélzeti jammerek általában egy nagyságrenddel nagyobb teljesítményűek a kézi eszközöknél. Sok esetben ugyanazok a típusok, csak egy rádiófrekvenciás teljesítményerősítővel kiegészítve, és a saját akkumulátor, illetve antennák helyett a jármű fedélzeti villamos rendszerét és külön antennákat használnak.

Fontos megjegyezni, hogy a rádióhullámok terjedési sajátosságai miatt még az adott RCIED-eszköz adóteljesítményénél jóval erősebb jammerek sem garantálnak 100%-os védettséget, így a laikus követelménytámasztók által gyakran használt „oltalmazási hatósugár” nem értelmezhető. Annyi azonban bizonyos, hogy minél nagyobb sávban „kenjük szét” a zavarójelet, annál kisebb az esély a sikeres zavarásra. Miközben a zavaró az adott frekvenciatartományt pásztázza, csak néhány ms-ot vagy μ s-ot tartózkodik egy-egy csatornán, mielőtt továbbugrik a következőre. Minél nagyobb a sáv, annál kisebb az egy-egy csatorna zavarására rendelkezésre álló idő. Mivel a zavaróteljesítmény felépüléséhez is szükséges egy véges idő, nagy zavarni kívánt sáv esetében nő az esélye annak, hogy egy-egy (az RCIED felhasználója szempontjából) hasznos jel átcsúszik a zavarfüggönyön, és beindítja a detonációt.

A szakértők komoly matematikai apparátust vonultatnak fel annak érdekében, hogy a véges adóteljesítmény több csatornán történő elosztása esetén is biztosítsák statisztikailag a leginkább hatékony jellefogást.²¹ Sőt az egyes, az RCIED-ek építésére gyakorta használt sávokban a jellemző, illetve a hatóságilag megengedett modulációs eljárásokhoz adott esetben más-más jelformálási stratégiát alkalmaznak.²²

Ezek a komplex matematikai számításokon alapuló eljárások némileg javítják a jammerek hatékonyságát, de összességében nem adnak arra megoldást, hogy a nagyobb átfogni kívánt sáv esetében csökken az elérhető zavarójel erőssége. Elvben lehetséges a különféle zavarni kívánt sávokra külön-külön rádiófrekvenciás adókat használni, de ezek többszöröznék, mind a jammer méretét, mind az áramfogyasztását, így a valóságban általában csupán egy végfokozatot építenek be a 25–450 MHz tartományhoz és egyet-egyét a különféle mobilfrekvenciákhoz.

Műveleti területen (Irak, Afganisztán) igen hatékony megoldás volt a felderítés. Ez az említett országok esetében annyit jelentett, hogy számba vették az adott régióban aktuálisan elérhető rádióberendezéseket, amit praktikusán úgy valósítottak meg, hogy a szövetséges erők ügynökei hetente elmentek a helyi bazárba, ahol felvásároltak egy-egy példányt minden kapható távirányítású autóból, garázsnyitóból és hasonló működésű egyszerű eszközökből, majd azok adófrekvenciáit felderítési információként megosztották a csapatokkal.

²¹ LEBL–MILEUSNIĆ–RADIVOJEVIĆ 2020.

²² LEBL–MILEUSNIĆ–RADIVOJEVIĆ 2020.

A csapatoknál aztán a jammerekbe egy úgynevezett *mission file*-t töltöttek fel, ami úgy vezérelte a jammert, hogy csak a felderítési adatok alapján kockázatos frekvenciákra koncentrált az adóteljesítményt, a technikailag egyébként lehetséges, de a mérénylők számára aktuálisan nem elérhető frekvenciákat pedig egyszerűen kihagyta. Annak érdekében, hogy az esetleg több régióban is áthaladó konvojkíséretnek biztonsága maximális legyen, a jammerek némelyikébe több *mission file* is feltölthető, amit a megfelelő időben a kezelő vált át.

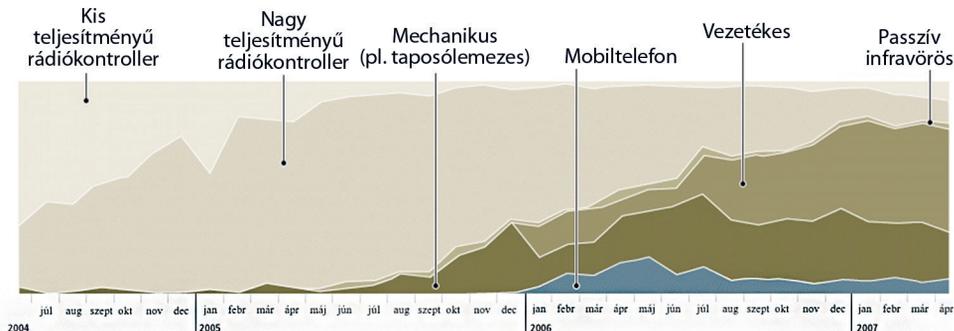
Irakban és Afganisztánban a 2000-es évek elejétől számos szövetséges haderő (köztük a magyar) alkalmazta a TMP 0512 és TMP 0512 EB típusú kézi jammereket. Ez 25–512 MHz tartományban, illetve az EB változat 880–960 és az 1710–1990 MHz-es mobilfrekvenciákon is működik. 10 W-os teljesítményével alapvetően egy kézi eszközről van szó, egy akkumulátorfeltöltéssel körülbelül 3–4 órát képes üzemelni. Többféle antenna is alkalmazható hozzá, és négy frekvenciakonfiguráció (*mission file*) tölthető a memóriájába.



7. ábra: TMP 0512 EB típusú kézi jammer
Forrás: LEBL–MILEUSNIĆ–RADIVOJEVIĆ 2020

A zavarásos RCIED-védelem hatékonysága és korlátai

Az látható, hogy a RCIED-ek ellen alkalmazott jammerek nem tartoznak az igazán szofisztikált eszközök közé. Az alkalmazott technológia alapvetően nem túl bonyolult, a használt berendezések meglehetősen robusztusak. Ugyanakkor az aktuális felderítési adatoknak megfelelően konfigurált frekvenciabeállítások mellett a főbb alkalmazási területeken (Irak, Afganisztán) meglehetősen hatékonynak bizonyultak. A 8. számú ábra jól mutatja, hogy az iraki megszállás kezdeti időszakában a leleplezett IED-k csaknem 100%-a rádió-távírányítású szerkezet volt. Később a jammerek széles körű alkalmazása nyomán aztán ezek aránya nagyjából 25%-ra esett vissza, miközben az észlelt eszközök száma érdemben nem változott.



8. ábra: Az iraki misszió első éveiben észlelt IED-ek indítási módjainak változása

Forrás: a Defense Technical Information Centre jelentései alapján a szerző szerkesztése

Tehát az RCIED-ek elleni rádiózavarásos védekezés igen hatásos lehet, ugyanakkor ez egy idő után kontraproduktívá válhat, hiszen a merénylők más megoldások felé fordulnak, amelyeket esetleg nehezebb időben észlelni. A jammert alkalmazó célpontok sem tudják, hogy sikerrel védtek ki egy támadást. Maga a robbanóeszköz ilyenkor az esetek többségében intakt, azaz sértetlen, érintetlen marad, így a merénylőnek semmi egyéb dolga nincs, mint várni egy újabb – esetleg védtelen – célpontra.

Maguk az improvizált robbanóeszközök a gerillahadviselés (kevésbé eufemisztikusan a terror) eszközei, így konvencionális hadviselés esetén kisebb a jelentőségük. A gerillák többnyire jelentős technológiai hátrányban vannak, de egy korszerű haderő, amelynek van elektronikus harci képessége, ki tudná használni azt, hogy a jammerek kisugárzása alapján igen könnyen nyomon lehetne követni az ellenséges csapatmozgásokat. Mivel a jammerek aktív energiakisugárzással működnek, jelentős mennyiségű villamos energiát is igényelnek. Ha kézi eszközként alkalmazzák, akkor az eszköz és az akkumulátorok tömege érezhetően növeli a csapat által málházott eszközök tömegét, ami negatív hatással van a mozgékonyagra. Ha egy nagyobb gyalogos csoport csak egy vagy két ilyen eszközzel rendelkezik, akkor azoknak a jammer köré csoportosulva kell a feladatukat végrehajtani, így viszont más eszközökkel könnyebben támadhatók.

Harcjárművön alkalmazva az eszköz tömege kevésbé problémás, de a felszerelés nem egyszerű, hiszen az antennák elhelyezéséhez át kell fúrni a páncéltestet és ugyan kisebb mértékben, de az energiaigény azért itt is probléma. A járművek hajtóműve által meghajtott generátor az esetek többségében gond nélkül ellátja a jammert is, de álló helyzetben az hamar lemerítheti az akkumulátort, mozgásképtelenné téve a járművet. Az ISAF-misszióra felkészített magyar BTR-80-as harcjárműveket ennek megfelelően nemcsak jammerrel, de egy második fedélzeti akkumulátorral is felszerelték.²³

²³ A PK-4 pc. kódú készlet beépítési és rendszertechnikai terve 2007.

Az orosz–ukrán háború és a gázai konfliktus árnyékában az IED-ek jelenleg nincsenek az európai figyelem fókuszában, de a fenyegetés megmaradt. A világ számos területén az improvizált robbanóeszközök jelenleg is szedik az áldozataikat mivel igen hatékony, ugyanakkor viszonylag olcsó eszközök, és ahol nem használnak tömegesen jammereket, ott a korábban tárgyalt okok miatt a rádió-távírányítású megoldások dominálnak. Sajnos nem zárható ki, hogy missziós szerepvállalás során a Magyar Honvédség ismét olyan helyzetbe kerül, amikor ezek az eszközök reális veszélyt jelentenek a katonáinkra, így az ellenük való védekezés továbbra sem hanyagolható.

Felhasznált irodalom

- A Decade of Global IED Harm Reviewed (2020). *ReliefWeb*, 2020. október 15. Online: <https://reliefweb.int/report/world/decade-global-ied-harm-reviewed>
- A PK-4 pc. kódú készlet beépítési és rendszerteknikai terve (2007). ArmCom Zrt.
- DARUKA Norbert (2014): A bűnös célú/terror jellegű robbantások és az ellenük való védekezés lehetőségei, különös tekintettel a tűzserézs feladatok ellátására. PhD-disszertáció. Nemzeti Közsolgálati Egyetem Katonai Műszaki Doktori Iskola Online: <https://doi.org/10.17625/NKE.2014.032>
- Fieldtrip to the Counter-IED Centre (2015). *Civil-Military Cooperation Centre of Excellence*, 2015. június 3. Online: <https://www.cimic-coe.org/news/fieldtrip-to-the-counter-ied-centre/>
- GÁVAY György (2014): Az IED eszközök által jelentett veszély a járművekre és az ellenük való védekezés lehetőségei. *Műszaki Katonai Közlöny*, 24(1), 60–71.
- HORVÁTH Tibor (2018): Rögtönzött robbanótestek hatástalanításának (C-IED) veszélyhelyzetei, kezelésük lehetőségei. *Műszaki Katonai Közlöny*, 28(2), 103–107. Online: <https://folyoirat.ludovika.hu/index.php/mkk/article/view/1629>
- Hungarian Army Receive 12 MRAP Armoured Vehicles MaxxPro Plus from United States (2013). *Army Recognition*, 2013. december 9. Online: <https://armyrecognition.com/news/army-news/army-news-2013/hungary-9-december-2013-news-uk>
- Improvised Explosive Device IED (2024). *The Times of Israel*, 2024. Online: <https://www.timesofisrael.com/topic/improvised-explosive-device-ied/>
- Improvised Explosive Devices. TRADOC DCSINT Handbook* (2006). TRADOC.
- Integrated Electronic Defense Technology System* [é. n.]. Online: <https://www.shoghicom.com/>
- Joint Improvised Explosive Device Defeat Organization* [é. n.]. Online: <https://apps.dtic.mil/sti/citations/ADA502251>
- KISS Zsolt (2009): A missziókban szolgálókat fenyegető rádió-távvezérlésű bombák és az ellenük való védekezés kérdései. *Hadmérnök*, 4(2), 41–56.
- KOVÁCS Zoltán (2012): Az improvizált robbanóeszközök főbb típusai. *Műszaki Katonai Közlöny*, 22(2), 103–107.
- KOVÁCS Zoltán (2013): Katonai objektumok IED elleni védelmének lehetséges technikai megoldásai. *Műszaki Katonai Közlöny*, 23(2), 114–121.
- LEBL, Aleksandar – MILEUSNIĆ, Mladen – RADIVOJEVIĆ, Jovan (2020): Combined and Comb RCIED Activation Messages Jamming: Two Different Strategies with Similar Names. *Scientific Technical Review*, 70(1), 21–28. Online: <https://doi.org/10.5937/str2001021L>
- OVERTON, Iain (2023): Report on Improvised Explosive Device (IED) Incidents for January – June 2023 (2023). AOAV, 2023. július 13. Online: <https://aoav.org.uk/2023/report-on-improvised-explosive-device-ied-incidents-for-january-june-2023>

- Palestinian Teens Killed in Accidental Blast While Handling Explosives (2023). *The Times of Israel*, 2023. június 21. Online: <https://www.timesofisrael.com/palestinian-teens-killed-in-accidental-blast-while-handling-explosives/>
- PANELLA, Chris (2023): Captured Hamas Weapons Hint That If Israeli Forces Invade Gaza, They Could Face a Deadly Improvised Bomb That US Troops Feared in Iraq. *Business Insider*, 2023. október 19. Online: <https://www.businessinsider.com/captured-hamas-weapons-israel-face-efp-ieds-terrified-us-iraq-2023-10>
- PONNEZHATH, Maria (2022): Russian Forces Continue to Use IEDs to Inflict Casualties, Says UK Intelligence. *Reuters*, 2022. április 9. Online: <https://www.reuters.com/world/europe/russian-forces-continue-use-ieds-inflict-casualties-says-uk-intelligence-2022-04-09/>
- Rádióalkalmazási táblázat (2009). Online: https://nmhh.hu/dokumentum/324/radioalkalmazasi_tablazat.pdf
- ROMERO, Grecia et al. (2018): Mitigation Technique to Reduce the Wi-Fi Susceptibility to Jamming Signals. In *2018 2nd URSI Atlantic Radio Science Meeting (AT-RASC)*. Gran Canaria: IEEE, 1–3. Online: <https://doi.org/10.23919/URSI-AT-RASC.2018.8471439>
- Supply of RCIED Vehicle Jammers to U.N [é. n.]. Online: <http://jamkor.co.kr/supply-rcied-vehicle-jammers-u-n/>
- Ukraine Crisis: Burnt-out Shells of Buses Following Attack (2015). *BBC News*, 2015. február 11. Online: <https://www.bbc.com/news/av/world-europe-31407058>
- VÉGH Krisztián (2022): Az improvizált robbanószerkezetek alkalmazása a hibrid hadviselés során: az orosz–ukrán konfliktus. *Műszaki Katonai Közlöny*, 32(2), 5–23. Online: <https://doi.org/10.32562/mkk.2022.2.1>