ORBÁN JÓZSEF

A rádiófrekvenciás felderítés, védelem és ellentevékenység a rendészetben

Bevezető gondolatok

Az elmúlt három évtizedben a rádiófrekvenciás eszközök meghódították az élet minden területét, melyből a teljesség igénye nélkül említhetjük a mobiltelefon, a vezetéknélküli telefon, a WIFI, a Bluetooth, a műholdas navigációs rendszer (a továbbiakban: GNSS), [1] a terület- és áruvédelmi rendszerek, az okos otthonok RF adattovábbítású érzékelői és vezérlői, valamint a vagyonvédelem RF átjelzésének alkalmazási köreit. Az RF berendezések működésének befolyásolása vagy akár akadályozása egyaránt lehet a honvédelem, a büntetés-végrehajtás, a szakszolgálatok, a terrorelhárítás, a NAV, az Országgyűlési Őrség vagy akár a rend- és határvédelem műveleti tevékenységének része is.

Az RF eszközök használatában rejlő lehetőséget azonban felfedezték a bűnözői körök is, így rendészeti szempontból az illegális alkalmazás megakadályozása újabb feladatot jelent. Az 5G[2] mobiltávközlés még csak kibontakozóban van, de már megjelentek azok az eszközök is, melyek ellehetetlenítik a használatát, meghamisítják a rajta keresztül továbbított adatokat, avagy kémkednek a továbbított információtartalomban. Ez is alátámasztja a fenyegetettség felmérését, a károkozás megelőzését és káros ha-

[1] A GNSS jelentése Globális Navigáció műhold rendszer, amely gyűjtőfogalomként a GPS (USA), Galileo (EU) és a GLONASS (Oroszország) globális műholdas helymeghatározó rendszereket együttesen jelenti.

[2] 2017-ben a 4G alapjain a 3GPP (3rd Generation Partneship Project – 3. generációs Együttműködési Projekt) kidolgozta az 5. generációs (5G) mobilkommunikációt, amely új mobiltávközlési modellek kidolgozását tette lehetővé.
Forrrás: https://www.3gpp.org/release-17
Letöltés ideje: 2022.08.09.

tásainak csökkentését, valamint a veszélytudatosság növelését célzó tanulmányok és intézkedések fontosságát.[3] A nem polgári küldetés-kritikus hálózati kommunikációs rendszerek[4] fejlesztésénél várható, hogy a kiforrott 4G LTE[5] hálózatok eredményeit felhasználó eszközpark beszerzésére kerül sor, így ezek RF sérülékenységi vizsgálata lényeges.[6]

Az alábbi áttekintés előzménye a Büntetés-végrehajtás Országos Parancsnoksága (a továbbiakban: BVOP) és a Nemzeti Média- és Hírközlési Hatóság (a továbbiakban: NMHH) a büntetés-végrehajtási intézményekbe illegálisan becsempészett mobiltelefonokkal elkövetett bűncselekmények megakadályozását célzó folyamatban lévő közös munkája. Az alábbi munka áttekintést ad a nem polgári rádiófelderítés, a rádiófrekvenciás védekezés, továbbá az RF ellentevékenység rendészeti bevezethetőségének kihívásokkal teli lehetőségeiről, az ellentmondásokról és a szabályozás jelen helyzetéről.

Hasonlóképp bemutatja a bűnözői körökben már alkalmazott és jövőbeli potenciális veszélyt jelentő RF módszereket és eszközöket. Ez utóbbit azzal a céllal is, hogy csomag vagy gépjármű átvizsgálásánál, helyszíni szemlénél könnyen felismerhetővé váljanak az eszközök, valamint jelezhető legyen, hogy RF ellentevékenység eszközét használták, vagy szándékozták használni.

---

[3] Marojevic, Vuk – Lichtman, Marc – Raghunandan, Rao – Reed, Jeffrey – Piqueras Jover, Roger: 5G NR Jamming, Spoofing and Sniffing: Threat Assessment and Mitigation.
Forrás: https://www.nitrd.gov/nitrdgroups/images/7/77/5G-NR-Jamming-Vuk-Marojevic.pdf
Letöltés ideje: 2022.08.09.

[4] Az Egységes Digitális Rádiótávközlő Rendszer (EDR) elsődlegesen a készenléti szervezetek (például: rendőrség, mentő, tűzoltóság, katasztrófavédelem) számára készült országos rádiótávközlő rendszer, amely magas rendelkezésre állást biztosít.

[5] 4G – Negyedik generációs mobiltávközlés, LTE – Long Term Evolution, hosszú távú fejlődés.

[6] Marojevic, Vuk – Lichtman, Marc – Raghunandan, Rao – Ha, Sean – Reed, Jeffrey: Performance Analysis of a Mission-Critical Portable LTE System in Targeted RF Interference.
Forrás: https://arxiv.org/ftp/arxiv/papers/1708/1708.06814.pdf
Letöltés ideje: 2022.08.09.

A tanulmány kifejezetten a katonai alkalmazáson kívül álló RF felderítés, védelem és ellentevékenység területét veszi górcső alá.[7] A katonai elektronikai hadviselés és a rajta kívül álló felhasználási területek elhatárolása érdekében a tanulmányban a rádiófrekvenciás (a továbbiakban: RF) felderítés, az RF védekezés és az RF ellentevékenység a nem katonai alkalmazást jelenti. Az RF ellentevékenység olyan cselekmény, melynek során más rádiófrekvenciás berendezésének működését, céloknak megfelelő használatát megzavarják, a kommunikációs csatorna tartalmát megváltoztatják, avagy működésképtelenné teszik. Rendészeti és bűnüldözési aspektusból a vizsgálat tárgya rádiófrekvenciás eszközzel támogatott bűnüldözésre és rádiófrekvenciás eszköz felhasználásával elkövetett bűnelkövetésre osztható fel.

A rádiófrekvenciás felderítés, védelem és ellentevékenység eszközei

A rádiófrekvenciás (RF) eszközök felderítése és működésük megzavarása szinte egyidős a rádiózással. A rádiózavarás első katonai alkalmazását az 1905-ös orosz–japán háborúhoz kötik.[8] A rádiófrekvenciás eszközök felderítése a hírszerzésen és a katonai célokon túl a polgári életben a vízi és légi közlekedésben megoldotta a járművek irány- és helymeghatározását. Ez utóbbi a járművek saját navigációja mellett a földi berendezések esetében segítette a logisztikai és vészhelyzetben a mentési feladatok ellátását. A rádiófrekvenciás eszközökkel megvalósított zavarás,[9] az elektronikai el-

[7] A katonai területen alkalmazott olyan eszközök katonai területen kívüli alkalmazásának az esélye még terrorcselekményeknél is csekély (például az impulzusbomba), nem képezi a tanulmány tárgyát.

[8] Horváth József: Elektronikai hadviselés korunk konfliktusaiban. Honvédségi Szemle 2016/1. szám. 18–26. o.

[9] 11/2011. (XII. 16.) NMHH rendelet a nem polgári célú frekvenciagazdálkodás egyes hatósági eljárásairól 2.§ (1) 12. pontja szerint *„zavar: adás, sugárzás vagy indukció, illetve ezek valamely kombinációja következtében fellépő nem kívánt elektromágneses energiának valamely rádiórendszerben a vételre gyakorolt káros hatása, amely az átvitel, illetve*

lentevékenységnek nevezett művelet sokáig olyan privilegizált haditechnikai tevékenység volt, amely az ellenérdekű fél kommunikációjának megzavarását célozta meg.[10] Az elektronikai ellentevékenység az elektronikai hadviselés[11] részeként található meg a katonai szakszótárban.[12] A polgári felhasználók az ellenérdekű országok műsorszóró adásainak (például Szabad Európa Rádió,[13] BBC) zavarásán keresztül tapasztalhatták meg az ilyen irányú katonai műveleteket. A hazai polgári eszközöket érintő RF zavarás 1942-ben az *„Amerika Hangja"* adás vételének akadályozásával kezdődött.[14]

A katonai szakirodalomban az elektronikai ellentevékenység[15] hármas felosztása használatos: a zavarás (jamming), a pusztítás (neutralization) és a megtévesztés (deception).[16] A nem polgári területen is használható lenne

a vétel minőségének olyan romlásában, az információ olyan torzulásában vagy veszteségében jelentkezik, ami elkerülhető lett volna ezen nem kívánt energia megjelenése nélkül".

[10] Az elektronikai ellentevékenységet megvalósító berendezések az EU haditechnikai eszközlistáján szerepelnek. A velük kapcsolatos minden tevékenység (a tervezéstől az export/importig) a Budapest Főváros Kormányhivatala Kereskedelmi, Haditechnikai, Exportellenőrzési és Nemesfémhitelesítési Főosztály engedélyével lehetséges.
Forrás: https://mkeh.gov.hu/haditechnika/hadiipar/hadiipariteveng
Letöltés ideje: 2022.08.30.

[11] Haig Zsolt – Kovács László – Ványa László – Vass Sándor: Elektronikai hadviselés. Nemzeti Közszolgálati és Tankönyv Kiadó Zrt., 2014. 30–31. o.

[12] Berkáné Danesch Marianne – M. Szabó Miklós – Mező András (szerk.): Katonai terminológiai értelmező szótár. 107.

[13] A Szabad Európa Rádió (SZER) 1951. október 6-án kezdte meg Kelet-Európába irányuló politikai tartalmú adásait.

[14] Horváth László Ferenc: Egy történet Magyari Endréről. A magyar rádiózavarás történetéről.
Forrás: http://www.puskas.hu/lacibacsi/astoryaboutME.pdf
Letöltés ideje: 2022.07.25.

[15] Az európai terminológiában Electronic Couter Measures (ECM), míg a tengerentúlon az Electronic Attack (EA) egyre gyakrabban jelenik meg.

[16] Haig et al. (2014): im. 38.

a felosztás, ugyanakkor csak a zavarás (jamming) és a megtévesztés (leginkább spoofing) ismeretes a gyakorlatban.[17] Jamming esetében a törvénysértés hírközlés szinten, spoofing alkalmazásakor a hírközlési törvény megsértése mellett az informatikai rendszer elleni támadás, a rendszerbe való jogosulatlan belépés tényállása is megvalósul.

A jogszerű felhasználók szemszögéből a rádiófrekvenciás zavarás területe négy szereplős: katonai; nem polgári, de nem katonai; polgári szereplők; valamint mindezek együttes érdekeit védő hatóság. A katonai alkalmazás – beleértve a NATO tevékenységet is – egyszerű kérdéskörnek tekinthető, mivel katonai célokra elkülönített sávokban kommunikálnak és katonai eszközökkel szemben végeznek zavarást is. A hazai katonai gyakorlatok során a polgári célú sávokban ma már nem hajtanak végre RF ellentevékenységet.

A felderítés és a védekezés esetében megkülönböztethetünk passzív és aktív módszereket. A passzív módszer egyik előnye, hogy a másik fél előtt rejtve marad az ellentevékenység teljes folyamata. Az aktív megoldások viszont hatékonyabbak lehetnek. A katonai területen kívül eső ellentevékenység – a jelenleg ismert módszerek alapján – mindig aktív.

[17] Az RF ellentevékenység szinonimájaként szokták említeni a kevésbé pontos, de könnyen kimondható RF zavarást, vagy az angol terminológiát használva a jamming kifejezést. A felosztásból látható, hogy a jamming csak egy körülhatárolható része az RF ellentevékenységnek.

A passzív rádiófelderítés

A passzív rádiófelderítés rádióiránymérőn, a kódolt üzenetváltás visszafejtésén,[18] valamint passzív radaron[19] keresztül lehetséges.

A rádió-iránymérés elvei régóta ismertek. Az egyik a jelerősség maximumát, a másik pedig a doppler frekvencia váltását keresi. A jelerősségen alapuló mérés egyszerű eszközökkel is megvalósítható, ugyanakkor nagyon pontatlan. A doppler iránymérő működése teljesen azonos a közlekedésben akusztikusan megfigyelhető szirénával (például mentőautó), amely közeledéskor magas hangon szól, a távolodás pillanatában pedig mélyebb frekvenciára vált. A doppler rádió-iránymérőnél a szenzor antennáját forgatják meg, amely így a forgatási sugáron hol közeledik, hol pedig távolodik. A jelenség matematikailag jól leírható, és gyakorlati pontossága 1 fok alatt van. Egy szenzor alkalmazásakor irány-, két szenzorral a szenzorokon átvetíthető felület kivételével helymeghatározásra is lehetőség nyílik. A felderítés hatékonyágát és pontosságát a tereptárgyak és az épített környezet rontja. Három vagy több rádió-iránymérő információinak egyesítése már jó helymeghatározást szolgáltat.

A passzív felderítés kézenfekvő lehetősége a rádiófrekvenciás spektrum figyelése. A rádiófrekvenciát kisugárzó eszközök felhasználási módtól függő jellegzetességekkel bírnak, így az adási frekvencia és a spektrum képe utalhat a tevékenységre is.

A hagyományos kommunikációs eszközök – a CB[20] rádiók, 1. ábra – alkalmazását a mobiltelefonok nagy mértékben csökkentették.

---

[18] A rádió-iránymérés és a kódvisszafejtés (e kettőt együttesen rádióelhárításnak nevezték korábban) nem polgári alkalmazása a rendszerváltás előtt tipikusan az állambiztonsági szolgálatok eszköztárát gyarapította. (In: Dobák Imre – Endrődi Ferenc: A magyar rádióelhárítás nemzetközi együttműködésének története (1955–1990). Nemzeti Közszolgálati Egyetem. 2014.) Polgári területen a rádió-iránymérőt a légi járművek helymeghatározására alkalmazták.

[19] A passzív radaron alapuló rádiófelderítés a haditechnikában, az űrkutatásban és a légi közlekedésben kezd teret nyerni. Magas bekerülési költsége és bonyolult telepítése miatt rendészeti alkalmazása belátható időn belül nem várható.

[20] Citizen's Band Radio, CB: nyilvános kétirányú személyes kommunikációt lehetővé tevő rádió adó-vevő. Az 1980–90-es években a mobiltelefon helyettesítésére használták. Mára

1. ábra
Egy korszerű CB kézirádió[21]

A CB rádió előnye, hogy a mobiltelefon szolgáltatástól független, így az adóteljesítmény-vevőérzékenység korlátokat figyelembe véve bárhol alkalmazható, de jelentősége egyre kisebb. A CB rádiók helye iránymérréssel meghatározható, a nyílt szöveg miatt könnyen megfigyelhető és lehallgatható.

Technológiailag sokkal korszerűbbek a funkcionálisan a CB rádiók helyére lépő magán mobilrádiók (Private Mobile Radio, PMR[22]),[23] melyek

ez a funkciója megszűnőben van. Átutazók, így különösen kamionok közötti kommunikációban még mindig alkalmazzák. A járművön elhelyezett nagyméretű ostorantenna miatt könnyen azonosítható.

[21] Forrás: https://www.alan-electronics.de/funktechnik/Notfallset-CB-Basic.aspx Letöltés ideje: 2022.08.30.

[22] Sajnálatosan a PMR rövidítést használják a Professional Mobile Radio (például TETRA, DMR, TETRAPOL) és a Private Mobile Radio esetében is.

[23] Recommendation T/R 25-08 (Lecce 1989, revised in Vienna 1999, revised in Utrecht 2005, revised in Brussels 2008). Planning Criteria and Coordination of Frequencies in the Land Mobile Service in the Range 29.7-921 Mhz.

engedélyhez és előfizetéshez nem kötöttek. A PMR-ek a távközlési infrastruktúrától függetlenek, így a mobiltelefon szolgáltatók azonosítási és helymeghatározási kockázatától mentesek.

2. ábra
Motorola Talkabout T82 Extreme Walkie Talkie, PMR-446 készülék-pár[24]

Ezért kedvelt segédeszköz a szervezett bűnözés kiszolgálására és terrorcselekmények végrehajtásához. Megfigyelésük csak rádiófelderítési eszközökkel lehetséges.[25] Kevésbé ismert, hogy léteznek olyan programok – sőt korábbi mobiltelefonoknál[26] beépített tulajdonság volt –, amelyek hálózatfüggetlen közvetlen walkie-talkie szolgáltatást tudnak nyújtani. A felkészített okostelefonok WIFI kapcsolaton keresztül működnek, amikor kellő közelségben tartózkodnak a kommunikációba bevont felek. Bűncselekmények elkövetésénél kedvező kommunikációs eszköznek bizonyulhat. A titkosított kommunikációs csatorna miatt szintén rádiófelderítési eszközök szükségesek a megfigyeléshez.

Forrás: https://docdb.cept.org/download/2710
Letöltés ideje: 2022.08.30.

[24] Forrás: https://www.motorolashop.hu/motorola_pmr446_walkie_talkie
Letöltés ideje: 2022.08.30.

[25] Balog Károly: A digitális PMR-ek szerepe a szervezett bűnözésben és a kiscsoportos direkt kommunikációban. In: Nemzetbiztonsági Szemle 2015/2. szám. 71–89. o.

[26] Pl. Nokia N90

Egy másik figyelemre méltó terület a pilóta nélküli légi járművek felderítése. A drónok helyének meghatározására kétféle, együtt is alkalmazható passzív módszer terjedt el: a rádió-iránymérés (3. ábra) és a pilóta nélküli légijármű és a távpilóta vezérlőegysége közötti kommunikációból a helyadatok kinyerése.

3. ábra
Phantom's PH-DF-6000 iránymérő [27]

Az aktív felderítés

Az aktív felderítésnél a felderítendő eszköz és a felderítő között rádiófrekvenciás interakció lép fel, emiatt a nem kívánatos dekonspiráció esélyével is számolni szükséges. Ez különböző rendvédelmi és biztonsági szervezetek egyidejű párhuzamos megfigyelései és felderítési tevékenysége esetén

[27] Forrás: https://phantom-technologies.com/direction-finder-model-ph-df-6000/
Letöltés ideje: 2022.08 30.

különösen kedvezőtlen lehet. E módszercsaládba tartoznak azok az eszközök, melyekkel az elrejtett – készenléti üzemállapotú (stand-by) vagy kikapcsolt – rádióberendezések, így a mobiltelefonok is felfedezhetők. A felderítés a félvezetők nem lineáris tulajdonságára alapoz. A besugárzott eszköz félvezetőiben a vett rádiófrekvencia többszöröse is megjelenik (felharmonikusok), és kisugárzásra kerül. A felharmonikusok vételén keresztül az eszköz leleplezhető. Hasonlóan aktív eszköz a mobiltelefon bázisállomásának utánzásával működő berendezés. Az ál-mobiltelefon bázisállomás folyamatosan növeli kimenő teljesítményét, s ezzel olyan hatást vált ki a felderítendő mobiltelefonokban, mintha az ál eszköz felé mozognának. Kellő térerősség esetén a roamingnál ismert módon a környezetében levő mobiltelefonok kapcsolatba lépnek az ál bázisállomással, és megadják az azonosításukat szolgáló adatokat. Az adatok megszerzése után az ál bázisállomás lecsökkenti kimenő teljesítményét, s ezzel „visszaengedi" a mobiltelefonokat a korábban használt hálózatra. Az adatok birtokában az előfizető meghatározható. Szem előtt kell tartani viszont, hogy az aktív módszereknél az alkalmazó felfedi magát, így a dekonspiráció kockázata itt is fellép.

Védekezési lehetőségek

A rádiófrekvenciás eszközzel megvalósított lehallgatások ellen a bűnözői és a bűnüldözői oldalon a passzív védekezés a legegyszerűbb megoldás. A fontos megbeszéléseket rádiófrekvenciásan árnyékolt térben – ún. Faraday-kalitkában – folytatják le. Ez törvényes megoldás, továbbá engedélyhez nem kötött, fedett ügynök bevetésénél figyelembe kell venni. A Faraday-kalitka lehetetleníti a rádiómikrofonok, a rádióadó-vevők és a mobiltelefonok használatát. Az aktív védekezési megoldás már az RF ellentevékenység kategóriájába tartozik.

Rádiófrekvenciás ellentevékenység

Elöljáróban megemlíthető, hogy az általánosan alkalmazott egyszerű RF ellentevékenység a kommunikáció szintjénél nagyobb amplitúdójú fehérzaj[28] kisugárzásával a vételi csatornák információit elfedi. A továbbiakban bemutatott képeken szereplő jogellenes eszközök a felismerhetőséget szolgálják.

4. ábra
8 sávos nagy teljesítményű (20 W) mobiltelefon és Wifi blokkoló / zavaró (jammer) asztali[29]

A 4. ábrán látható nagy teljesítményű eszköz mobiltelefonok és WIFI zavarására szolgál. Webes áruházban rendelhető, használata jogellenes. A bolt üzemeltetője utal is erre: *„Célunk egy olyan webshop létrehozása volt, mely olyan termékeket forgalmaz, amiket Magyarországon kevés helyen vagy egyáltalán nem vásárolhatóak meg."* Székhelye Romániában, a Bihar

[28] A fehérzaj olyan véletlenszerű RF zaj, melynek teljesítménye a lefedni kívánt RF spektrumban állandó.
[29] Forrás: https://spyonlineshop.com/termek/8-savos-antennas-nagy-teljesitmenyu-15-w-mobiltelefon-es-wi-fi-blokkolo-zavaro-2/
Letöltés ideje: 2022.08.30.

megyei Monospetriben van,[30] melyre az uniós haditechnikai termékekre vonatkozó szabályozás szintén iránymutató.

A forgalmazó termékbemutatója szerint „*benzinkutak, gyárak, bankok, vonatok, buszok, stb. mobil mentesítésére*" alkalmas. Ez alapján a bűnözők fantáziája és segítőik felkészültsége szab határokat a jövő RF bűncselekményeinek.

Az ellentevékenység hatékonyságát a fehérzaj kisugárzásán túlmutató célzott, intelligens akciók javítják. Ugyanakkor mindezek a módszerek már átvezetnek a titkosszolgálati eszközök területére. Ide tartozik az sms üzenetek meghamisítása, a mobiltelefon-hívások manipulálása.

Gépkocsilopások esetében az RF kulcs zárási parancsának megakadályozása vagy a kulcs kódjának másolása lehet az elkövetői módszer.

5. ábra
Gépkocsi távvezérlő blokkoló[31]

[30] Forrás: https://spyonlineshop.com/kapcsolat/
Letöltés ideje: 2022.08.30.
[31] Forrás: https://spyonlineshop.com/termekkategoria/gsm-gps-wifi-blokkolok-jammer/
Letöltés ideje: 2022.08.30.

A gépkocsizárás megakadályozásának bűnüldözői felderítése a közelben elhelyezett rádió-iránymérővel lehetséges, melynek használata nem igényel bírói engedélyt.

A pilóta nélküli légijárművek elleni aktív védekezés egyik módja szintén a fehérzaj kisugárzása.

Egy másik kifinomultabb, drónnal szembeni RF ellentevékenység, amikor a műholdas helymeghatározó rendszer adatait meghamisítják, így a földrajzi koordináták alapján repülő autonóm eszközök nem érnek célba.[32] Még szofisztikáltabb megoldás a kommunikációs rendszer feltörése és a vezérlés átvétele. Ez lehetővé teszi, hogy a járművet egy előre meghatározott helyre irányítsák és tiltsák az újbóli felszállását. Az intelligens ellentevékenység időigényes, ezért megfontolandó olyan védőzóna meghatározása, melynek elérésekor a fehérzajos ellentevékenységet alkalmazzák.

IED-vel[33] vagy drónnal elkövetendő terrorcselekmények megelőzése, továbbá kiemelten fontos személyek, objektumok vagy műveleti terület[34] esetén az RF ellentevékenység kombinált módszere javasolt. Kockázati zónák meghatározásával az RF felderítési, az RF intelligens hatástalanítási, az RF nyers erő, a fizikai megsemmisítési és a fizikai védelmi övezeteket lehet felállítani.

A zavarás megvalósulhat úgy is, hogy az elkövető nincs tisztában cselekménye jogellenességével és az okozott károk mertékével. Ilyennek tekinthető, amikor a WIFI eszközök a meteorológiai radaroknak dedikált

[32] A pilóta nélküli légi járművek azon csoportja, amely RF támogatás nélkül, optikai helyzetmeghatározással repül, az itt tárgyalt módszerekkel nem hatástalanítható. Itt a fizikai védekezés és megsemmisítés megoldásai lehetnek célravezetők.

[33] Házi készítésű robbanó eszközök – Improvised Explosive Device (IED).

[34] Műveleti területnek minősül a helyszíni szemle, továbbá a bűncselekmények elkövetési helye.

5600–5650 MHz RF spektrumot használják.[35] A zavarás kedvezőtlen esetben súlyos felderítési problémát okoz a meteorológiai szolgálatoknak.[36] Megítélésem szerint ebben az esetben a közérdekű üzem működésének gondatlanságból elkövetett megzavarása tényállás[37] is megvalósul.[38]

A Nemzetközi Távközlési Egyesület (ITU)[39] nagy horderejű események RF zavarásának megakadályozásával kapcsolatosan a vendéglátó államra külön kötelezettségeket is ró. A rendezvény helyszínén jelen lévő szolgálattal biztosítani kell az RF zavarmentességet.[40] Az iránymutatás nem tesz különbséget a rossz akaratú és a védelmi szándékú alkalmazás között. Mindebből látható, hogy a rendészeti célú RF ellentevékenység alkalmazásánál számos kihívással kell szembenézni.

Tények és kihívások

A rádiófrekvenciás kommunikációhoz használható spektrum véges és szűkös természeti erőforrás, melynek kezeléséért a Nemzeti Média- és Hírközlési Hatóság felelős.

---

[35] Forrás: https://nmhh.hu/cikk/198443/Meteorologiai_radarokat_zavarhatnak_vezetek_nelkuli_eszkozok
Letöltés ideje: 2022.08.30.

[36] Saltikoff, Elena – Cho, John Y. N. – Tristant, Philippe – Huuskonen, Asko – Allmon, Lynn – Cook, Russell – Becker, Erik – Joe, Paul: The Threat to Weather Radars by Wireless Technology, American Meteorological Society, July 2016. 1159–1167. o.

[37] BTK. 323.§ (5)

[38] Az Országos Meteorológiai Szolgálat adatait a katasztrófavédelemtől a légi közlekedésig sok létfontosságú szolgálat és szolgáltatás használja.

[39] Nemzetközi Távközlési Egyesület – International Telecommunication Union (ITU) – az ENSZ mellett működő szervezet, melynek feladata a nemzetközi távközlési együttműködés segítése.

[40] Report ITU-R SM.2257-3 (06/2015), Spectrum management and monitoring during major events.
Forrás: https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-SM.2257-3-2015-PDF-E.pdf
Letöltés ideje: 2022.08.11.

Az erőforrás optimális felhasználása az NFFF-ben[41] szabályozott, egyes sávok esetében díjfizetéshez kötött, másnak zavart nem okozhat.[42] Aki tehát rádióengedéllyel rendelkezik, elvárja, hogy az a spektrumrész, amiért fizetett, zavartalanul legyen használható. A térítésmentesen használható spektrumtartományok olyan mélyen beépültek a társadalom működésébe, hogy azok zavarása kedvezőtlen gazdasági hatásokat is eredményezhet.

A többi nem polgári szereplő a polgári felhasználók érdekeit sérti akkor, amikor zavarja azok RF eszközhasználatát. A problémakör kihívása az, hogy egy létfontosságú alapszolgáltatás, a kommunikáció hozzáférhetőségét befolyásolhatják. Az RF ellentevékenység – amennyire csak lehetséges – célzott alkalmazású, hogy meghatározott személyek vagy eszközök kommunikációját akadályozzák meg. Annak ellenére, hogy már elektronikusan programozható a fedési területhez szükséges teljesítmény, a zavarás pontos határa nem állítható be, így óhatatlanul nem kívánatos hatásokkal is szembesülhet az alkalmazó.

A műholdas helymeghatározó rendszer (GNSS) zavarása[43] az egyik legtöbb vitát kiváltó ellentevékenységi kérdéskör, mivel a zavarmentes működésnek a közlekedésben és a mezőgazdaságban alapvető szerepe van. Emellett a GNSS kulcsszerepet játszó referencia időt szolgáltat a pénzforgalmi, az időszinkronizált gyártási tevékenységekhez, valamint a folyamatirányítási rendszerekhez is. Így a kellő körültekintés nélküli zavarása jelentős károkat eredményezhet. Hasonlóképp kritikus a mobiltelefonok zavarása. Mikor merülhet fel az RF ellentevékenység szükségessége? A lista igen hosszú lenne, ezért csak néhány eset felsorolására szorítkozom. Házi

[41] 7/2015. (XI. 13.) NMHH rendelet a nemzeti frekvenciafelosztásról, valamint a frekvenciasávok felhasználási szabályairól (NFFF)

[42] 7/2015. (XI. 13.) NMHH rendelet, 7. § (4) *„Egy adott rádiószolgálat számára felosztott frekvenciasávban egy rádióalkalmazás állomása úgy üzemelhet, hogy nem okoz káros zavarást az állomás számára egyedi engedélyben biztosított frekvenciasáv szélességét figyelembe véve a közvetlenül szomszédos frekvenciasávokban felosztott rádiószolgálatok rádióalkalmazásainak."*

[43] Ványa László: Műholdas helymeghatározó rendszerek elektronikai hadviselési kérdései. Repüléstudományi közlemények, XXVIII. évfolyam, 2016., 145–151.

készítésű robbanó eszközök távműködtetésének[44,45,46] távvezérelt jármű segítségével[47] elkövetetett bűn- vagy terrorcselekményeknek,[48,49] pilóta nélküli légi járművek kiemelt fontosságú létesítmények feletti illegális repüléseinek megakadályozása, vagy olyan rendőrségi operatív művelet, ahol a bűnözői körök kommunikációját kell ellehetetleníteni. Fontossága és komplexitása miatt ide sorolhatjuk diplomáciai küldöttségek vagy valamilyen szempontból fontos konvojok védelmét is.

A Hatóság ellentmondásos helyzetét jelenti, hogy egyszerre kellene feltétel nélkül garantálnia az RF spektrum zavarmentességét és biztosítani az RF ellentevékenység lehetőségét.

A világon minden hírközlési hatóság szembesül a problémával, de a dilemmák miatt még senkinek sem sikerült kételyek nélküli megoldást találni. A modus operandi technológiai fejlődés nyújtotta lehetőségeinek bővülése miatt a bűnüldözés és a hírközlési hatóságok közös kiútkeresésének új dimenzióit kell megnyitni.

---

[44] Kovács Zoltán: Az improvizált robbanóeszközök főbb típusai. Műszaki Katonai Közlöny, XXII. évfolyam, 2012. 2. szám, 37–52.

[45] Gulyás Attila: The Radio Controlled Improvised Explosive Device (RCIED) threat in Afghanistan. AARMS Vol. 12, No. 1 (2013) 9–23.

[46] Kovács Tibor – Csurgó Attila: Az improvizált robbanószerkezetek elleni védekezés irányai napjaink műveleti környezetében. Műszaki Katonai Közlöny, 31. évfolyam, 2021. 2. szám, 111–125.

[47] Amennyiben egy gépjárművet az IED csomagolásaként vagy tárolására használják, úgy a terminológia Vehicle-borne IED (VBIED).

[48] Ilyen elhíresült terrorcselekményként tartják számon az 1991. december 23-án a Ferihegyi gyorsforgalmi úton elkövetett robbantási akciót, amit az NSZK-ban működő Vörös Hadsereg Frakció (RAF) tagok követtek el. A merénylet célpontjaként tekintett busz négy utasa könnyebben megsérült, ugyanakkor a kísérő jármű rendőr utasai súlyos sérülést szenvedtek.

[49] Nacen, Kanpur: Improvised Explosive Devices (IED).
Forrás: https://nacin.gov.in/resources/file/e-books/E-book%20No.02%20on%20Programme%20Global%20Shield.pdf
Letöltés ideje: 2022.08.11.

Szabályozási helyzetkép

A rádiófrekvenciás felderítés, az irány- és helymeghatározás, a rádiófrekvenciás spektrum figyelése – ide nem számítva a megszerzett információ jogellenes felhasználását – nem tiltott. A passzív RF védelem legtöbb fajtája hasonlóképp nem tilos, bár itt a részletek ismerete is szükséges, mellyel kapcsolatosan két példa is említhető. A CB rádiónak dedikált sáv nyilvános, ezért rendészeti megfigyelése és lehallgatása nem igényel külön engedélyt.[50]

A mobiltelefonok megfigyelésére, lehallgatására viszont csak a szükséges törvényességi garanciák megszerzése mellett van lehetőség.[51] Ugyanakkor jelenleg az RF ellentevékenység minden fajtája tilos, mivel az más jogait közvetlenül sérti.

A további vizsgálódást elősegíti az NMHH spektrumgazdálkodási szerepének rövid áttekintése. Az elektronikus hírközlésről szóló törvényben (Eht.) meghatározott feladatok és kötelezettségek megvalósításáért az NMHH felel.[52] Az NMHH az elektronikus hírközlés és a rádiófrekvenciás spektrumgazdálkodás területén a Ksztv. alapján jogalkotó hatáskörrel, rendeletalkotási jogkörrel is felruházva látja el az RF spektrumgazdálkodás polgári és nem polgári hatósági feladatait.[53] A spektrumhasználatot szabályozó, a nemzeti frekvenciafelosztásról, valamint a frekvenciafelhasználás szabályairól szóló rendelet[54] webes felületű megjelenítését és az adatok

[50] 1994. évi XXXIV. törvény a rendőrségről [Rtv.] 66.§ (1) c) pontja *„személyt, lakást, egyéb helyiséget, bekerített helyet, nyilvános vagy a közönség részére nyitva álló helyet, illetve járművet titokban megfigyelhet, a történtekről információt gyűjthet, valamint az észlelteket technikai eszközzel rögzítheti”*.

[51] Rtv. 70.§ (1) „Bírói engedélyhez kötött eszköz”, 70.§ (2) e) információs rendszer titkos megfigyelése.

[52] 2003. évi C. törvény az elektronikus hírközlésről (Eht.)

[53] 2010. évi XLIII. törvény a központi államigazgatási szervekről, valamint a Kormány tagjai és az államtitkárok jogállásáról. (Ksztv.) 1.§ (3) a) pontja.

[54] 7/2015. (XI. 13.) NMHH rendelet a nemzeti frekvenciafelosztásról, valamint a frekvenciasávok felhasználási szabályairól. (NFFF)

igény szerinti szűrését a Spektrumgazdálkodást Támogató Információs Rendszer (STIR) biztosítja.[55]

Az RF ellentevékenység eszközei és az ezekkel nyújtott szolgáltatások haditechnikai célúnak minősülnek,[56] a berendezések teljes köre szerepel az európai haditechnikai eszközlistán.[57] Mivel az elektronikus ellentevékenység egyes fajtái elektromágneses zavart keltve rontják vagy lehetetlenítik el a polgári rádiófrekvenciás berendezések használatát, ezért a nem katonai felhasználást az uniós jog tiltja,[58] és felszólítja a tagállamokat, hogy minden lehetséges intézkedést tegyenek meg a jogszerű spektrumfelhasználók érdekében.[59] Az Eht. az alapelvek között sorolja fel a *„rádióspektrum hatékony, szakszerű, a legmodernebb műszaki megoldásokkal, technológiákkal történő káros zavarástól mentes használatának elősegítése”* célt.[60] A rádiófrekvencia engedély nélküli, vagy az egyedi engedélyhez nem kötött, ám jogsértő frekvenciahasználat esetén a zavarást okozó eszközöket a Hatóság jogosult lefoglalni vagy zár alá venni.[61] Emiatt a rádiófrekvenciás zavarás, így az RF ellentevékenység megakadályozása és megszüntetése az NMHH kötelessége,[62] de kivételes engedély adásának kizárólagos jogosultja is. A 11/2011. (XII. 16.) NMHH rendelet 19.§ (2) a) pontja szerint

[55] Forrás: https://stir.nmhh.hu/publicview/
[56] 2005. évi CIX. törvény a haditechnikai termékek gyártásának és a haditechnikai szolgáltatások nyújtásának engedélyezéséről (Httv.)
[57] 156/2017. (VI. 16.) Korm. rendelet a haditechnikai tevékenység engedélyezésének és a vállalkozások tanúsításának részletes szabályairól ML11 fejezet a) pontja
[58] Az uniós megközelítés elgondolkodtató. Analógiát keresve megjegyezhető, hogy hasonló ahhoz, amikor a bankok védelmét csak fegyver nélküli élőerővel biztosítanák, miközben a bankrablók használhatnák fegyvereiket.
[59] Az Európai Parlament és a Tanács 2014/53/EU Irányelve (2014. április 16.) a rádióberendezések forgalmazására vonatkozó tagállami jogszabályok harmonizációjáról és az 1999/5/EK irányelv hatályon kívül helyezéséről, HL. L153/62–106.
[60] Eht. 2.§. n) pontja
[61] Eht. 50.§.
[62] 7/2017. (VII. 28.) NMHH rendelet a nem polgári célú frekvenciagazdálkodás körébe tartozó rádióberendezésekről (Berendezés rendelet)

„Tilos a rádióállomással (…) más rádióállomás üzemét szándékosan zavarni”.[63] A kivételek átlátható szabályozása megkívánja a rendelet módosítását, amely folyamatban van. A módosítási tervezet szerint RF ellentevékenységre alkalmas eszköz jogszerű birtokosa és használója csak nem polgári szervezet lehet.[64]

A 12/2011. (XII. 16.) NMHH rendelet 2.§ tételes meghatározása szerint a nem polgári célú rádióspektrum-gazdálkodás körébe az alább felsorolt szervezetek tartoznak:

„a) honvédség,
b) nemzetbiztonsági szolgálatok,
c) a rendőrség belső bűnmegelőzési és bűnfelderítési feladatokat ellátó szerve,
d) terrorizmust elhárító szerv,
e) általános rendőrségi feladatokat ellátó szerv,
f) hivatásos katasztrófavédelmi szerv,
g) büntetés-végrehajtási szervezet,
h) Nemzeti Adó- és Vámhivatal vám- és nyomozóhatósági feladatokat ellátó szervei,
i) zártcélú rendészeti hálózat, a K-600/KTIR Hírközlési és Informatikai Rendszer és az egységes digitális rádiótávközlő rendszer vonatkozásában a kormányzati célú hírközlési szolgáltató,
j) fővárosi és megyei védelmi bizottságok,
k) Országgyűlési Őrség” [65]

A rendeletben felsorolt szervezetek az ország biztonságát és védelmét, így a társadalom érdekét szolgálják. Erre alapozható az a megkülönböztető

[63] A 11/2011. (XII. 16.) NMHH rendelet a nem polgári célú frekvenciagazdálkodás egyes hatósági eljárásairól
[64] Forrás: Balogh János NMHH Védelmi és Rendészeti Frekvenciagazdálkodási Főosztály
[65] 12/2011. (XII. 16.) NMHH rendelet a nem polgári célú frekvenciagazdálkodás rendjéről, valamint a nem polgári célú frekvenciagazdálkodás körébe tartozó szervezetekről

szemlélet, amely nem szolgál profitorientált, vagy csak egyéni civil érdekeket. Hiányérzetet kelt, hogy a kritikus infrastruktúrákat üzemeltető szervezetek, így az energia, a víz, a szennyvíz és a közlekedés hiányzik a felsorolásból. Ami viszont óvatosságra int, hogy a kritikus infrastruktúrákra alapozott kivételek képzésénél könnyen megjelenhetnek azok a piaci szereplők, amelyek létfontosságú rendszerelemek üzemeltetésében alvállalkozók. Mindezeket figyelemmel kell követni a folyamatban lévő rendeletalkotás során. Az aktuális helyzetben az RF ellentevékenység eszközeinek tervezése, kivitelezése, forgalomba hozatala és kereskedelme a versenyszféra vállalkozásainak kezében van. Ennek feloldása a belföldi piac esetében a megrendelő nem polgári szervezet megbízó és felhatalmazó okirata alapján lenne lehetséges. A tervezet szerint az engedélyeztetés első lépése a szervezet és az RF eszköz nem polgári nyilvántartásba vétele az RF kompetenciákkal bíró NMHH Hivatalánál. A második lépés a haditechnikai eszközlistán szereplő és Hivatalnál regisztrációval rendelkező berendezés engedélyeztetése[66] a Budapest Főváros Kormányhivatala Kereskedelmi, Haditechnikai, Exportellenőrzési és Nemesfémhitelesítési Főosztály Exportellenőrzési Osztály Haditechnikai Osztályánál.[67] Harmadik lépésben a termék forgalomba hozhatóságát a kérelemben szereplő paraméterek validálásával az NMHH engedélyezi. A vázolt folyamat megvalósításához a 156/2017. (VI. 16.) Korm. rendelet, a 12/2011. (XII. 16.) NMHH rendelet és a 11/2011. (XII. 16.) NMHH rendelet[68] harmonizált módosítása szükséges.

A rádiófrekvenciás eszközökkel elkövetett bűncselekmények

A rádiófrekvenciás alkalmazásoknál tipikus az eszközök működése alapján a passzív és aktív felosztás. Bár a passzív RF ellentevékenységnek kicsi a

[66] Httv. 2.§, 3.§ és 4.§ bekezdései szerint.
[67] 156/2017. (VI. 16.) Korm. rendelet a haditechnikai tevékenység engedélyezésének és a vállalkozások tanúsításának részletes szabályairól
[68] 11/2011. (XII. 16.) NMHH rendelet a nem polgári célú frekvenciagazdálkodás egyes hatósági eljárásairól

jelentősége, mégis érdemes megemlíteni az áruvédelmi RFID[69] eszközök hatástalanítására szánt, és egyes külföldi internetes áruházakban beszerezhető, bolti lopásokhoz használható árnyékoló tasakokat.

Kriminalisztikai szempontból tényleges jelentősége az aktív eszközöknek van. A mobiltelefonnal közvetlenül elkövetett bűncselekmények közül kiemelkedő számban a csalások figyelhetők meg. A börtönökbe becsempészett telefonok az időben bővelkedő fogvatartottaknak egyszerre jelentenek időtöltést és pénzszerzési lehetőséget.

A könnyű, akár házilagos telepíthetőség miatt a sokak által alkalmazott vezetéknélküli WIFI kameramegoldások új lehetőséget adtak a bűnözők kezébe. A bűncselekmény előkészítő szakaszában az elkövető vagy tettestársai felderítik a terepet. WIFI kamera szemrevételezéses vagy műszeres azonosításakor [70] felkészültségtől függően beléphetnek a CCTV rendszerbe, vagy megzavarhatják annak működését. Az eredményes rendszerfeltörést követően meg tudják határozni a vagyonvédelmi rendszer videorészének gyenge pontjait, így például a vakfoltokat, a felbontást, ami a későbbi azonosíthatóságot befolyásolja. A nyers erő RF alkalmazása a kamerák információátvitelét gátolja. Ezek a tevékenységek megalapozzák a kiber bűncselekmény elkövetésének tényállását is. Kellő körültekintéssel kialakított videomegfigyelő rendszer a kamera zavarását, mint szabotázst érzékelni tudja, így az a vagyonvédelmi rendszerbe integrálva riasztással jelzi a rendellenességet. Ugyanakkor a felkészült elkövető nem csak a kamerát, hanem a riasztórendszer mobiltelefonos átjelző rendszerét is némítani

[69] Az RFID (Radio Frequency IDentification) az árucikk rádiófrekvenciás azonosítását biztosítja. Az RFID technológia lényege, hogy a termékhez köthető információkat, adatokat az azonosító pontokon (kapukon) egy rádióhullámokkal kommunikáló rendszeren keresztül közvetítik. A passzív védelem ezt a kommunikációt, így az áru mozgásának nyomon követését akadályozza meg.

[70] Az árucikk EMAG webshopján keresztül megrendelhető.
Forrás: https://www.emag.hu/mini-akkus-lehallgato-es-megfigyelo-szett-vezetek-nelkuli-gsm-kamera-riaszto-00083336-a9/pd/DT51X2BBM/?ref=other_customers_viewed-_go_2_1&provider=rec&recid=rec_52_9c4ef229a400c214fdd6acf635fdee1676951eeb8-5ced9a45f00845ad5ee82f1_1659210600&scenario_ID=52
Letöltés ideje: 2022.07.30.

tudja. A komplex RF ellentevékenység taktikájával az elkövető teljeskörű álcalehetőséget kap.

Másik előkészületi módszer lehet a véletlenszerű RF vaklárma generálás, ami miatt előbb-utóbb kikapcsolják a vagyonvédelmi rendszert, vagy figyelmen kívül hagyják a riasztást.

A gépjárművek feltörésénél az RF kulcsok működésébe avatkoznak be, amely a zárási funkció megakadályozásával vagy a nyitási kód megszerzésével lehetséges. Az első művelethez használt eszköz az elektronikában járatlanok számára is egyszerűen beszerezhető egyes internetes áruházakból. A gépkocsilopások esetén az elkövetőnek két RF védelmi pontot kell semlegesíteni: a helymeghatározást és a mobiltelefonos riasztást. Ezután a jármű nyomon követhetősége megszűnik, és olyan helyre szállítható, ahol a védelmi rendszer véglegesen kiiktatható.

A pilóta nélküli légi járművek (UA) csempészési, drogszállítási és betörés előtti terepfelderítési használata már ismert. A drogszállító UA akár a 10. emeleti lakásba is leszállítja az anyagot, majd „nyom nélkül" elhagyja az elkövetés helyét. Belátható, hogy a tettenérés komoly technikai apparátust igényel, s az elkövető lebukásának csekély az esélye.

A büntetés-végrehajtási intézmények nemzetközi gyakorlatában már évek óta kihívást jelent az illegális dolgok beszállítása a létesítmények területére. Az egyik probléma az RF felderítés, a másik pedig a védekezés. A hatályos szabályozás katonai felhasználási területen kívül nem teszi lehetővé a zavarást. A fegyveres védelemnél a fegyverhasználat jogalapja kérdéses.

A problémakör másik vetülete, amely már kevésbé jutott el a köztudatba, hogy mások drónrepülésének megakadályozása is felkerült a bűnözői eszközlistára. Mindezek miatt sajnálatos az a tény, hogy még mindig elérhetők hazai és uniós forrásokból egyaránt az elektronikus piactéren a jogellenes célra használható eszközök.[71,72]

---

[71] Forrás: https://www.emag.hu/gps-blokkolo-gps-jammer-gps-zavaro-1-antennas-008/pd/DDPV3YMBM/
Letöltés ideje: 2022.07.30.

[72] A hirdetést 2022.07.28-án Budapesten adták fel.

A rádiófrekvenciás ellentevékenység szerepe a bűnüldözésben

A mobiltelefonok zavarása demokratikus berendezkedésű országokban tiltott nem csak a polgári, hanem az állami alkalmazásban is. Ugyanakkor a börtönökbe csempészett mobiltelefonok használata a bűnözés melegágya. Magyarországon számos tényező eredőjeként a büntetés-végrehajtási intézményekben engedélyezett a különleges feltételek alapján egyedileg gyártott mobiltelefonok használata. E készülékekről csak a családtagok és az ügyvéd hívhatók, így bűncselekmény elkövetésére kevéssé alkalmas. Ezért fordulhat elő az a helyzet, hogy nálunk is megéri mobiltelefont becsempészni a börtönökbe azoknak, akik az eszközzel bűncselekményt kívánnak elkövetni. A védekezés ezért is bonyolult, mivel a fehérzajjal működő nyers erőre alapozott egyszerű eszközök nem használhatók. Megoldásként olyan berendezések használata javasolt, melyek intelligens módon kiszűrik az illegális felhasználókat, és csak azokkal szemben alkalmaznak RF ellentevékenységet.

Egy, a mobiltelefonos autóriasztók blokkolásával a lopott autók szétszerelésére szakosodott bűnszervezet leleplezésében az NMHH jelentős segítséget nyújtott a rendőrségi operatív egységeknek. Az elkövetők RF ellentevékenységének helyét rádióiránymméréssel meghatározva, sikeres tettenéréssel bizonyítható volt az autószerelő műhelynek látszó bűnszervezet tevékenysége.

A gépjárművek távműködtetésű zárását akadályozó eszköz felderítése hordozható iránymérő rendszerrel leginkább akkor lehetséges, ha az elkövetők sorozatosan ugyanott követik el cselekményeiket. A GNSS helymeghatározás zavarása olyan mértékben megnövekedett, hogy az amerikai védelmi kutatók a zavaró eszközök 200 méter pontosságú felderítésére alkalmas műholdas rendszert fejlesztettek ki. Most még csak katonai felhaszná-

Forrás: https://www.jofogas.hu/magyarorszag?q=wifi%20zavar%C3%B3#channel=main_page_free_text
Letöltés ideje: 2022.07.30.

lásáról adtak szűkszavú tájékoztatást. A rendszer rendészeti vagy határvédelmi hozzáférhetősége esetén lehetőség nyílhat helymeghatározás zavarásával történő bűncselekmények rövid időn belüli jelzésére.

A drogfutárként alkalmazott pilóta nélküli légi jármű a megrendelő által megjelölt helyre, emberi kontaktus nélkül szállíthatja le az „anyagot", így a tettenérés vagy annak bizonyítása kihívásokat jelent. Megoldást jelenthet a pilóta nélküli légi jármű kommunikációs rendszerébe való belépéssel az útvonali pozíció és képanyagok megszerzése, ami viszont speciális eszközöket és jól előkészített taktikai lépéseket igényel.

Bűnmegelőzést támogató intézkedés lehet az RF ellentevékenység eszközforgalmazói elleni szigorú rendészeti fellépés. Mivel az RF ellentevékenység felhasználási célú berendezések az Unió haditechnikai eszközlistáján szerepelnek,[73] ezért azok kimerítik a haditechnikai termékkel vagy szolgáltatással visszaélés fogalmát.[74]

Nemzetközi jogeset – kitekintés

Az ausztrál büntetés-végrehajtási intézményekben nem megengedett a mobiltelefon birtoklása, mivel segítségével bűncselekményt vagy szökést szervezhetnek, de akár a tanúkat is megfélemlíthetik. 2013-ban az Ausztrál Kommunikációs és Média Hatóság (Australian Communications and Media Authority, ACMA) kivételt képezve kísérleti jelleggel engedélyezte[75] Új Dél Wales állam Lithgow és Goulburn fegyintézeteiben a mobiltelefon használatát zavaró eszköz alkalmazását.[76] A kísérletet követően az eszköz

[73] A 1236/2005/EK rendelet III. mellékletében meghatározott áru.
[74] Btk. 329.§. (1). a) pontja
[75] Forrás: https://www.legislation.gov.au/Details/F2015L01662/Download
Letöltés ideje: 2022.07.25.
[76] Radiocommunications (Field Trial by Corrective Services NSW of PMTS Jamming Devices at Lithgow Correctional Centre) Exemption Determination 2015 Radiocommunications Act. 1992.
Forrás: https://www.legislation.gov.au/Details/F2015L01662
Letöltés ideje: 2022.07.25.

használhatóságát társadalmi vitára bocsátották, amit 2018. július 6-án zártak le. A kivételt képező szabályozás 2018. november 1-től 2021. november 26-ig volt hatályban.[77]

Az Egyesült Államokban a RF ellentevékenység szigorú megítélés alá esik.[78] Ilyen eszköz alkalmazása illegális, mivel megakadályozhatja a segélyhívó szolgálatok elérését is. A szövetségi törvénykezés jogellenesnek tekinti az USA teljes területén mindezen eszközök gyártását, importját, marketingjét, forgalmazását és működtetését. A tiltás hatálya alá esnek a műholdas kommunikáció megzavarására alkalmas eszközök – beleértve a GPS blokkolókat –, továbbá mindazon berendezések, melyek a vezeték nélküli infokommunikáció működését károsan befolyásolják,[79] különösen akkor, ha a szándékos zavarás (jamming) érinti a 911-es segélyhívó vonalat. A Szövetségi Hírközlési Bizottság 2016. május 25-i közleményében tájékoztatást adott ki, hogy pénzbüntetést szabott ki a Florida állambeli Jason R. Humphreyre, aki a rendőrség kommunikációját megzavarta. Az indoklásban a büntetési tételek megállapítása is figyelemre méltó, mivel az eljáró hatóság közösségre veszélyesnek minősítette a cselekményt.[80] Az engedély nélküli működtetésért, a jogellenes eszköz használatáért és a más rádiófrekvenciás eszköz működésének megzavarásáért halmazatban eseményenként 16 000 USD büntetést állapított meg az eljáró hatóság. A három bizonyított eset alapján szabták ki a példaértékűnek számító 48 000 USD pénzbeli szankciót.

[77] https://www.legislation.gov.au/Details/F2018L01185/Download
Letöltés ideje: 2022.07.25.
[78] Forrás: https://www.fcc.gov/general/jammer-enforcement
Letöltés ideje: 2022.07.25.
[79] Forrás: https://www.fcc.gov/document/fcc-fines-florida-driver-48k-jamming-communications
Letöltés ideje: 2022.07.25.
[80] Forrás: https://docs.fcc.gov/public/attachments/FCC-14-55A1.pdf
Letöltés ideje:2022.07.25.

Összefoglalás

A rádiófrekvenciás (RF) eszközökkel elkövetett bűncselekmények száma és változatossága növekvő tendenciát mutat. Ezen okból az RF felderítés és védelem alkalmazása iránti igény növekedése érzékelhető a bűnüldözésben, ámbár a lehetőségektől jelentősen elmarad a tényleges alkalmazás. Az RF eszközök működésének szándékos zavarása – az RF ellentevékenység – katonai körön kívül jogellenes, így a bűnüldözés és a büntetés-végrehajtás számára is. Ugyanakkor a jelenlegi gyakorlatban a bűnelkövetők, akik az autólopástól a betörésig segédeszközként alkalmazzák, ténylegesen csak tettenérés esetén szembesülhetnek szankciókkal. Tényekre alapozva megállapítható, hogy a kérdéskörben érintett szervezetek az ellentétes elvárások vagy a kellő ismeretek hiánya miatt nem tudják a társadalom számára optimális eredményeket szolgáltatni. A tanulmány interdiszciplináris megközelítéssel a rádiófrekvenciás rendészeti problémakör kihívásaival, az útkereséssel és a lehetséges válaszokkal foglalkozik.

A tanulmány ismerteti a rádiófrekvenciás felderítés a főbb módszereit, kockázatait, melyek egyaránt segíthetik a bűnözőket és a bűnüldözőket. A rendészeti célú RF ellentevékenység törvényességi háttere még nem kimunkált, ugyanakkor a törekvések megvalósulása az európai élvonalba tartozik. Az eszközök jogellenes forgalmazóival, a birtoklóival és a felhasználóival szemben a hatékony és koordinált fellépés az elkövetők mozgásterét bizonyosan csökkenti. Megítélésem szerint a jogellenes birtoklás és használat szabályozási háttere már rendelkezésre áll, a rendészeti és az eljárási gyakorlat azonban még hiányos. Ezzel szemben a rend- és határvédelmi, a büntetés-végrehajtási területen az RF ellentevékenység jogszerű alkalmazásának törvényi háttere még nem kidolgozott.

A szabályozásban rejlő ellentmondások feloldása és a megfelelő kivételeket megteremtő módosítást követően az RF ellentevékenység a bűnüldözés szolgálatába állítható.