ORBÁN JÓZSEF

RÁDIÓFREKVENCIÁS ELLENTEVÉKENYSÉG A KRIMINALISZTIKÁBAN

1. Bevezetés

A rádiófrekvenciás (RF) eszközök működésének megzavarása szinte egyidős a rádiózással, s első katonai alkalmazását az 1905-ös orosz-japán háborúhoz kötik.[1] Ez az RF ellentevékenységnek nevezett művelet sokáig olyan privilegizált haditechnikai tevékenység volt, amely az ellenérdekű fél kommunikációjának megzavarását célozta meg. Az RF ellentevékenység az elektronikai hadviselés[2] részeként található meg a katonai szakszótárban.[3] A polgári felhasználók az ellenérdekű országok műsorszóró adásainak (pl. Szabad Európa Rádió, BBC stb.) zavarásán keresztül tapasztalhatták meg az ilyen irányú katonai műveleteket. A hazai polgári eszközöket érintő RF zavarás 1942-ben az „Amerika Hangja" adásának vételének akadályozásával kezdődött.[4]

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 (GNSS), 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 egyarán lehet a büntetés-végrehajtás, a szakszolgálatok, a terrorelhárítás, a NAV, az Országgyűlési Őrség, vagy akár a rend- és határvédelem műveleti tevékenységének része is. Az RF ellentevékenységben rejlő lehetőséget azonban felfedezték a bűnözői körök is, így rendészeti szempontból az illegális alkalmazás megakadályozása újabb feladatot jelent.

Az áttekintés apropóját a Büntetés-végrehajtás Országos Parancsnoksága (BVOP) és a Nemzeti Média- és Hírközlési Hatóság (NMHH), a büntetés-végrehajtási intézményekbe illegálisan becsempészett mobiltelefonokkal elkövetett bűncselekmények megakadályozását célzó közös munkája adta. Az alábbi tanulmány szélesebb kitekintéssel rövid összefoglalást ad a nem polgári RF ellentevékenység kihívásokkal teli bevezethetőségének kriminalisztikai lehetőségeiről, az ellentmondásokról és a szabályozás jelen helyzetéről.

---

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

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

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

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

2. Kihívások

Az RF ellentevékenység eszközei és az ezekkel nyújtott szolgáltatások haditechnikai célúnak minősülnek,[5] a berendezések teljes köre szerepel az európai haditechnikai eszközlistán.[6] Mivel az elektronikus ellentevékenység egyes fajtái elektromágneses zavart keltve rontják, vagy lehetetlenítik a polgári rádiófrekvenciás berendezések használatát, ezért a nem katonai felhasználást az Uniós jog tiltja, és felszólítja a tagállamokat, hogy minden lehetséges intézkedést tegyenek meg a jogszerű spektrumfelhasználók érdekében.[7] Az elektronikus hírközlésről szóló törvény (Eht.) az alapelvek között sorolja fel a „rádióspektrum hatékony, szakszerű, a legmodernebb műszaki megoldásokkal, technológiákkal történő káros zavarástól mentes használatának elősegítése" célt.[8] Az Eht. által meghatározott feladatok és kötelezettségek megvalósításáért az NMHH felel. A rádiófrekvencia engedély nélküli, vagy az egyedi engedélyhez nem kötött, ám jogsértő frekvenciahasználat esetén, a tevékenységet okozó eszközöket a Hatóság jogosult lefoglalni vagy zár alá venni.[9]

Összegezve, a rádiófrekvenciás zavarás, így az RF ellentevékenység megakadályozása és megszüntetése az NMHH kötelessége, de kivételes engedély adásának kizárólagos jogosultja is.

A rádiófrekvenciás kommunikációhoz használható spektrum véges és szűkös természeti erőforrás. Az erőforrás optimális felhasználása szabályozott, egyes sávok esetében díjfizetéshez kötött. Aki tehát rádióengedéllyel rendelkezik elvárja, hogy azt zavartatás mentesen használhassa, így a neki fel nem róható szolgáltatási zavarok esetén kártérítésre tarthat igényt. A térítésmentesen használható spektrumtartományok olyan mélyen beépültek a társadalom működésébe, hogy azok zavarása kedvezőtlen gazdasági hatásokat is eredményezhetne. Az egyik legfontosabb ilyen terület a műholdas helymeghatározó rendszer (GNSS), melynek 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.

Az RF ellentevékenység olyan cselekmény, melynek során más rádiófrekvenciás berendezésének működését, céloknak megfelelő használatát megzavarják, a kommunikációs csatorna tartalmát megváltoztatják, avagy működésképtelenné teszik. Az RF ellentevékenység szinonimájaként szokták említeni a kevésbé pontos, de könnyen kimondható RF zavarást, vagy az angol terminológiát használva a jamming kifejezést.

A jogszerű felhasználók szemszögéből a probléma 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

[5] 2005. évi CIX. törvény a haditechnikai termékek gyártásának és a haditechnikai szolgáltatások nyújtásának engedélyezéséről

[6] 156/2017. (VI. 16.) Korm. rendelet a haditechnikai tevékenység engedélyezésének és a vállalkozások tanúsításának részletes szabályairól ML11 fejezet a) pontja

[7] 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.o.

[8] 2003. évi C. törvény az elektronikus hírközlésről (Eht.), 2.§. n) pontja

[9] Eht. 50.§.

végeznek zavarást is. A hazai katonai gyakorlatok során a polgári célú sávokban ma már nem hajtanak végre RF ellentevékenységet.

A többi nem polgári szereplő a polgári felhasználók érdekeit sérti akkor, amikor zavarják 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.

Mikor merülhet fel az RF ellentevékenység szükségessége? A lista igen hosszú lenne, ezért csak néhány felsorolására szorítkozom. Házi készítésű robbanó eszközök távműködtetésének, a pilóta nélküli légijárművek kiemelt fontosságú létesítmények feletti illegális repüléseinek megakadályozása, vagy olyan rendőrségi operatív művelet, ahol a bűnözői körök kommunikációját kell lehetetleníteni. Fontossága és komplexitása miatt ide sorolhatjuk küldöttségek, vagy valamilyen szempontból fontos konvojok védelmét is.

Azt jelenti a Hatóság ellentmondásos helyzete, hogy egyszerre kellene feltétel nélkül garantálni 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 kiút keresésének új dimenzióit kell megnyitni.

3. A rádiófrekvenciás ellentevékenység eszközeivel elkövetett bűncselekmények

A rádiófrekvenciás alkalmazásoknál tipikus az eszközök működése alapján a passzív és aktív felosztás. Bár a passzív RF ellentevékenységnek kicsi a jelentősége, mégis érdemes megemlíteni az áruvédelmi RFID eszközök hatástalanítására szánt, és egyes külföldi internetes áruházakban beszerezhető, bolti lopásokhoz használható árnyékoló tasakokat és lopókat.

Kriminalisztikai szempontból tényleges jelentősége az aktív eszközöknek van. 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[10] felkészültségtől függően beléphetnek a CCTV rendszerbe, vagy megzavarhatják annak működését. Az eredményes rendszerfeltörést követően meg tudják határozni a vagyonvédelmi rendszer videó részének 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 videómegfigyelő rendszer a kamera zavarását, mint szabotázst érzékelni tudja, így az a vagyonvédelmi rendszerbe integrálva riasztással jelzi a

[10] Az árucikk EMAG webshopján keresztül megrendelhető. 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_9c4ef229a400c214fdd6acf635fdee1676951eeb85ced9a45f00845ad5ee82f1_1659210600&scenario_ID=52 (Letöltés ideje: 2022.07.30.)

rendellenességet. Ugyanakkor a felkészült elkövető nem csak a kamerát, hanem a riasztórendszer mobiltelefonos átjelző rendszerét is némítani 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 kell beavatkozni, 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. Ezt követően a jármű nyomonkövethetősége megszűnik, olyan helyre szállítható, ahol a védelmi rendszer véglegesen kiiktatható.

A pilóta nélküli légijárművek csempészési, drogszállítási és betörés előtti felderítési használata már ismert. Az kevésbé, hogy mások drónrepülésének megakadályozása is felkerült a bűnözői eszközlistára. Mindezek miatt sajnálatos az a tény, hogy hazai és Uniós forrásokból is még mindig elérhetők az elektronikus piactéren a jogellenes célra használható eszközök.[11][12]

4. A rádiófrekvenciás ellentevékenység szerepe a bűnüldözésben

A mobiltelefonok zavarása demokratikus berendezkedésű országokban tiltott nem csak 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 hívható, 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 bonyolultabb, mivel a fehérzajjal működő nyers erőre alapozott egyszerű eszközök nem használhatók. Megoldásként olyan eszközök alkalmazhatók, 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 rádióirányméréssel meghatározva sikeres tettenéréssel bizonyítható volt az autószerelő műhelynek látszó bűnszervezet tevékenysége.

A drogfutárként alkalmazott pilótanélküli légijármű 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 légijármű kommunikációs rendszerébe való belépéssel az útvonali pozíció- és képanyagok

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

[12] A hirdetést 2022. 07. 28-án Budapesten adták fel.
https://www.jofogas.hu/magyarorszag?q=wifi%20zavar%C3%B3#channel=main_page_free_text (Letöltés ideje: 2022.07.30.)

megszerzése, amely viszont speciális eszközöket és jól előkészített taktikai lépéseket igényel.

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

Bűnmegelőzést támogató intézkedés lehet az RF ellentevékenység eszközforgalmazói elleni szigorú rendészeti fellépés. Mivel az RF ellentevékenység felhasználási célú berendezések az Unió haditechnikai eszközlistáján szerepelnek,[13] ezért azok kimerítik a haditechnikai termékkel vagy szolgáltatással visszaélés fogalmát.[14]

5. Nemzetközi kitekintés

Az ausztrál büntetés-végrehajtási intézményekben nem megengedett a mobiltelefonok 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[15] az Új Dél Wales állam Lithgow és Goulburn fegyintézeteiben a mobiltelefon használatát zavaró eszköz alkalmazását.[16] A kísérletet követően az eszköz 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.[17]

Az Egyesült Államokban a RF ellentevékenység szigorú megítélés alá esik.[18] 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 GPS blokkolókat – továbbá mindazon berendezések, melyek a vezetéknélküli infokommunikáció működését károsan befolyásolják,[19] 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.[20] Az engedély nélküli működtetésért, a jogellenes eszköz

[13] 1236/2005/EK rendelet III. mellékletében meghatározott áru.
[14] Btk. 329.§. (1). a) pontja.
[15] Forrás: https://www.legislation.gov.au/Details/F2015L01662/Download (Letöltés ideje:2022.07.25.)
[16] 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.)
[17] https://www.legislation.gov.au/Details/F2018L01185/Download (Letöltés ideje: 2022.07.25.)
[18] Forrás: https://www.fcc.gov/general/jammer-enforcement (Letöltés ideje: 2022.07.25.)
[19] Forrás: https://www.fcc.gov/document/fcc-fines-florida-driver-48k-jamming-communications (Letöltés ideje: 2022.07.25.)
[20] Forrás: https://docs.fcc.gov/public/attachments/FCC-14-55A1.pdf (Letöltés ideje:2022.07.25.)

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.

6. Összefoglalás

Az ellentmondások feloldása és a megfelelő kivételeket teremtő szabályozást követően RF ellentevékenység a bűnüldözés szolgálatába állítható. A jogellenes forgalmazókkal, a birtoklókkal és a felhasználókkal szemben hatékony és koordinált fellépés az elkövetők mozgásterét bizonyosan csökkenti. Megítélésem szerint ennek jogi háttere már rendelkezésre áll.