ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉSTERVEZET

DOMJÁN ANDRÁS

KIEMELTEN VÉDETT OBJEKTUMOK KOMPLEX BIZTONSÁGA KÜLÖNÖS TEKINTETTEL A RÁDIÓFREKVENCIÁS SPEKTRUM ELLENŐRZÉSÉRE

Témavezető: Prof. Em. Dr. Berek Lajos

BIZTONSÁGTUDOMÁNYI DOKTORI ISKOLA

Budapest, 2026. 04.06. nap

TARTALOMJEGYZÉK

BEVEZETÉS

Az infokommunikációs fejlesztések vívmányai a mindennapi életünk részévé váltak. A mobiltelefonok, a különböző adatgyűjtő és adatmegosztó berendezéseink, elektronikus használati tárgyaink, szinte a nap minden pillanatában a közvetlen közelünkben üzemelnek. A lakó-, és munkakörnyezetünk digitalizációja következtében, több szintű felhő alapú szolgálatatások és az ezeket magába foglaló úgynevezett kibertér jött létre. Az „okos" eszközeink felépítésével, lakóházaink, közintézményeink, hivatali építményeink, városaink is mind-mind egy egészet képezve „okossá" válnak. Ennek a dinamikus rendszernek a működése során, folyamatos-, szakaszos-, vagy véletlenszerű ütemezéssel, rádiófrekvenciás kommunikáció zajlik az éterben. Ezeket a jeleket megfelelő műszerezettség esetén detektálhatjuk, rögzíthetjük és bizonyos feltételek megléte mellett, akár az adat tartalmukat is megismerhetjük. A vezetéknélküli kommunikáció jellemzően pont-pont vagy pont-multipont kialakításban van jelen körülöttünk a levegőben, amely magában hordozza az illetéktelenek hozzáférésének lehetőségét az elküldött adatokhoz. Napjaink információvédelmének egy meghatározó részét maga a rádiós összeköttetések sérülékenységének vizsgálata és hatékony védelme jelenti. Ebben a rádiófrekvenciás szempontból meglehetősen zsúfolt környezetben kell kialakítani és működtetni a saját, személyes vagy vállalati adatátviteli-, és biztonságtechnikai rendszereinket, a lehető legnagyobb védelmi fokozattal és hatékonysággal.

A technológiai fejlődés hatása megfigyelhető a biztonsági szektornál, azon belül is különösen az alkalmazott eszközökre, rendszerekre gyakorolt változtatások, újítások területén. Az építmények védelme esetében egészen mást jelent egy teljeskörű, úgynevezett komplex biztonsági rendszer kiépítése a klasszikus értelemben vett objektumőrzési feladatoktól eltérően. Jellemzően a nagyvállalati-, vagy kormányzati szinten találkozhatunk ilyen volumenű megoldásokkal a létesítmények esetében, amelyek magukba foglalják a piacon elérhető biztonságtechnikai eszközökön felül, a megfelelő módon felkészített és kiképzett állomány rendelkezésre állását is.

A klasszikus, szenzor- és humánerőforrás-alapú objektumvédelmi rendszerek önmagukban nem képesek kezelni a rádiófrekvenciás környezet dinamikus változásait, különösen a rejtett, nem állandó sugárzással működő eszközök esetében.

Az objektumok biztonságát szavatoló aktív védelmi rendszerek közül kiemelt figyelmet kell fordítani a rádióspektrum ellenőrzésére szolgáló mérőhálózatokra. Az úgynevezett szoftverrádiók (SDR[1]) mindennapjainkban való jelenléte nagymértékben megkönnyíti a biztonsági szektor ezen területének a fejlesztését. Ez a technológia a védelem szempontjából jellemzően nem egy elterjedt, illetve sűrűn alkalmazott módszer hazánkban, ennek ellenére szükséges tüzetesebben megvizsgálni, feltárni a benne rejlő lehetőségeket, előnyöket és adott esetben implementálni a komplex védelmi rendszereinkbe a leghatékonyabb változatokat, a biztonsági szint növelése érdekében.

A TUDOMÁNYOS PROBLÉMA MEGFOGALMAZÁSA

A háborús konfliktusokkal összefüggésben oly sokat emlegetett aszimmetrikus hadviselés során alkalmazott improvizált robbanóeszközök (IED[2]) megjelentek világszerte, nem csak a közvetlenül katonai műveletek által érintett országok területén. Ez a fajta fenyegetettség jelen van a hétköznapjainkban különböző formában annak ellenére, hogy sokszor tudomást se veszünk róla, csak a tudósításokból értesülünk a bekövetkezett robbantásos merényletekről, vagy a bombafenyegetésekről. Hazánk esetében is komoly figyelmet kell fordítani erre a területre, mivel a bűnös célú robbantások lehetőségét sok esetben a robbanóanyaghoz való hozzáférés képessége elősegítheti, valamint ezt a tendenciát a szomszédos országokban bekövetkezett események csak tovább fokozhatják. A „dél-szláv” háborút követően nálunk is megnövekedett kockázatként jelentkezett a volt jugoszláv hadianyagok megjelenése a bűnözői körökben, amelyeket sok esetben az egymás elleni konfliktusok „kezelésére” alkalmaztak. A közelmúltban kezdődött orosz-ukrán háború következtében ismét aktuálissá válik ez a probléma, amelyet kezelni kell, elsősorban mint kiemelt kockázati tényezőt. Jelen esetben az ukrajnai háborús helyzetnek a bűnözői körökben zajló illegális fegyver-, és robbanóanyag kereskedelemre gyakorolt hatása még ismeretlen számunkra. Ennek ellenére a fenyegetettséget komolyan kell venni, és a biztonsági rendszereinket a lehető legjobban felkészíteni a legújabb kihívásokkal szemben.

Az információáramlás következtében a híradások, gyakorlatilag valós időben vagy minimális késleltetéssel mutatják be a robbantásos helyszíneket, illetve az elkövetési

[1] Software-defined radio – szoftver alapú rádió
[2] Improvised Explosive Device – improvizált robbanó eszköz

módokat, sok esetben az alkalmazott szerkezetről is részletes beszámolóval szolgálnak. Ennek a dinamikus információ-megosztó folyamatnak a következménye, hogy bizonyos esetekben akár bátoríthatja is az elkövetőket mivel a bűnös cselekményüknek az „üzenete", szinte azonnal megjelenik a médiában. A terrorizmus alapfegyvereként emlegetett „félelemkeltés", ilyen körülmények között még hatásosabban alkalmazható. A nagy befogadóképességű épületek, vagy akár a kiemelten védett objektumok, intézmények mind-mind elsődleges célpontként kezelendőek, illetve nagyon könnyen azzá válhatnak.

A védelem szempontjából a másik meghatározó terület az információbiztonság, amely átszövi a mindennapi életünket a magánszférától kezdve a munkakörnyezetünkön át, a gazdasági-, politikai-, stratégiai-, vagy akár a hadi ügyekkel összefüggő megbeszélések, döntések helyszíneit is beleértve. Az elmúlt 10 évet tekintve a közéleti és a magánszférában egyaránt meghatározó területet képviselt az információvédelem azon belül is a lehallgatás elleni védelem. Európai uniós szinten ugyanúgy jelen volt ez a probléma, mint a nemzetállamok esetében. Jellemzően ezen események mind-mind valamilyen típusú objektumhoz, építményhez kapcsolódnak, legyen az akár egy magánlakás vagy hivatali épület. A robbantásos merényletekhez hasonlóan, az illegális lehallgatásokból vagy rejtett megfigyelésekből szerzett információk elsődleges megosztási felülete szintén a közmédia, vagy az internet, amelyeken keresztül a kívánt hatásukat a „kiszivárogtatók" a lehető leggyorsabban elérhetik.

Az objektumvédelem tekintetében mindegyik esetben szükség van különböző megelőző intézkedésekre, amelyek közül fokozott figyelmet kell fordítanunk az úgynevezett technikai átvizsgálásra. Ennek célja, hogy a rejtett lehallgató-, vagy improvizált robbanóeszközöket felkutassuk. Ez a gyakorlatban egy olyan tüzetes, mindenre kiterjedő ellenőrzést jelent, amelynek során egy objektum helyiségein felül, az ott elhelyezett műszaki-technikai eszközöket is érinti. A bevezetőben említett vezeték nélküli összeköttetések számában az elmúlt években exponenciális növekedés volt tapasztalható, és a szakemberek véleménye szerint ez a tendencia a közeljövőben még nagyobb mértékben fog emelkedni. A változást az okozza, hogy - részben a szokásainknak köszönhetően - a hétköznapi berendezési tárgyaink szinte mindegyike már valamilyen hálózathoz kötődik, de valójában a mennyiségi mutató ilyen meredeken felfelé ívelő jellegét, a technológiában történt kapcsolatokra épülő fejlesztéseknek tudhatjuk be. Ebből következik, hogy az eseti jelleggel végrehajtott technikai átvizsgálások hatásfoka

nagymértékben lecsökken, ha nem tudjuk folyamatos ellenőrzés alatt tartani a védendő objektumunkat. Továbbá a rendelkezésre álló hálózatok magukba hordozzák a távolról működtetés vagy indítás lehetőségét is a lehallgató és természetesen az improvizált robbanóeszközök esetében egyaránt.

A jelenlegi objektumvédelmi gyakorlatban a lehallgatás elleni védelem és az improvizált robbanóeszközök detektálása elkülönült rendszerként jelenik meg, miközben a technológiai fejlődés következtében ezen fenyegetések egyre inkább azonos rádiófrekvenciás és vezérléstechnikai alapokon nyugszanak, amelyeket a meglévő védelmi rendszerek nem képesek integrált módon kezelni.

A két említett lehetséges kockázati tényező, valós fenyegetést jelent a kiemelten védett objektumainknál, amelyekre mindkét területet érintő biztonságtechnikai megoldást képvisel a rádióspektrum ellenőrző mérőhálózat a detektálás szempontjából. Ez a feladat nem könnyű, és a normál vivőfrekvenciák ellenőrzésén túlmenően, részletesebb vizsgálat is szükséges a beazonosítás elvégzéséhez.

A gyakorlatban ezt a két területet – lehallgatás-, robbantás elleni védelem – egymástól elkülönítve kezeljük, de véleményem szerint, pont a technológiai fejlődés indokolja, hogy a detektálás során egy rendszerként tekintsünk rá a kiemelten védett objektumok esetében.

KUTATÁSI CÉLKITŰZÉSEK

Az objektumvédelem önmagában is meglehetősen összetett és bonyolult rendszert takar, amelyen belül nagyon sokféle szempont szerint valósíthatjuk meg az elérni kívánt biztonsági szintet. Az általam választott vizsgálandó terület ebből a szerteágazó rendszerből -a kormányzati objektumokhoz kapcsolódó - közvetlenül az építményeken belül jelentkező robbantás-, és információvédelmi fenyegetettség kezelésére szolgáló rádiófrekvenciás mérőhálózat szükségességének és hatékonyságának elemzése.
Értekezésemben az improvizált robbanószerkezeteket a civil területeken, „terrorista” jellegű alkalmazásuk alapján vizsgálom, elsődlegesen a detektálhatóságuk szempontjából. A polgári életben, közvetlenül a rendvédelmi - azon belül is - biztonságtechnikai szemszögből közelítem a témakört, amelynek során a merényletekkel kapcsolatban, a kutatásomhoz elsősorban a nyílt sajtóban elérhető adatokat, esettanulmányokat használom.

A katonai célpontok, járművek, táborok elleni támadásokat a kutatásom során közvetetten vizsgálom, a harcászati terminológiában az improvizált robbanóeszközökre alkalmazott kategorizálásokat, összehasonlításként a technikai kialakítások és a végrehajtások taktikai módjai vonatkozásában.

A kiemelten védett objektumok esetében az úgynevezett komplex védelmi rendszer megvalósítása alkalmával, kutatási célként a következőket határoztam meg:

- a kutatásom alapjául elsősorban a polgári célpontok ellen elkövetett merényletek során használt robbanószerkezetek felépítése szolgál, de kitekintésként a háborús területeken alkalmazott változatokat is vizsgálom a technikai fejlődésük szerint;
- a kiemelten védett objektumok esetében, elemzem a lehetséges kockázatokat és meghatározom a fő fenyegetettségi területeket;
- részletesen tanulmányozom a mai modern robbanóeszközök indítási módjait, a felhasznált elektronikai egységek felépítésének vonatkozásában is;
- kiemelt figyelmet fordítok az elektronikus indítású és a rádió-távirányítású eszközök felderíthetőségére, párhuzamot vonva a lehallgató berendezések ezen változataival;
- a lehallgatás elleni védelem esetében a nyílt kereskedelmi forgalomban elérhető technikai eszközök nagyszámú megjelenésével megnövekedett kockázatot vizsgálom;
- a bűnös céllal elkövetett robbantásoknál előforduló szerkezetek evolúciójának elemzésével, kapcsolódási pontot keresek az információvédelem érdekében a rádióspektrum ellenőrzésére telepített mérőhálózatok, a két terület vonatkozásában való alkalmazhatóságára, elsősorban az objektumvédelem területén;
- a megelőzés érdekében alkalmazott rádióspektrum ellenőrző rendszer működésének vizsgálata, a szükséges technikai alapelvek megfogalmazása, a kiemelten védett objektumok esetében;
- kutatási eredményeim által javítani az objektumvédelem területén dolgozó szakemberek felkészültségét, bővíteni ezirányú ismereteiket és ezáltal erősíteni a kiemelten védett objektumok biztonságát.

A TÉMA KUTATÁSÁNAK HIPOTÉZISEI

A technológiai fejlődés következtében a lehallgatás elleni védelem és az elektronikus indítású robbanóeszközök detektálása között olyan vezérléstechnikai és a rádióspektrum analízishez közvetlenül kapcsolódó hasonlóságok azonosíthatók, amelyek indokolttá teszik a két terület integrált, közös detektálási platformon történő vizsgálatát.
Kutatómunkámat, a célkitűzésként megfogalmazott tudományos problémák feldolgozásakor a következő hipotézisek határozták meg:

- az objektumvédelem egy speciális részeként kezelendő feladatkör - amely a rendvédelem tevékenységeivel szorosan összefüggő területéhez tartozik - a kiemelten védett épületek komplex biztonsági rendszereinek tervezése és kiépítése során különös figyelmet kell fordítani a robbantás-, és a lehallgatás elleni védelemre;
- a polgári környezetben a civil célpontok ellen elkövetett terrorista jellegű robbantások során alkalmazott szerkezetek, minden részletére kiterjedő módon történő feldolgozása, kiértékelése és rendszerezése elengedhetetlen az eredményes megelőzés, vagy adott esetben az elkövetők felkutatása érdekében;
- a technológiai fejlődés következtében, az objektumvédelem területén paradigmaváltásra van szükség a szakemberek részéről, a lehallgatás-, és a robbantás elleni védelem tekintetében, a detektálást – az alkalmazott eszközök nagyfokú vezérlés-technikai hasonlósága miatt - közös platformon kell kezelni. A megelőző tevékenységen belül az előtalálásra nagyobb hangsúlyt kell fektetni, mint a robbanás hatásainak kivédésére egy kiemelten védett objektum esetében;
- a megelőzés során, az objektum védelmében dolgozó szakemberek, a napi technológiai fejlettségnek megfelelő kiképzésükön felül, a szintén legmodernebb mérőrendszer megléte és annak professzionális alkalmazásával, működésének rendszeres felülvizsgálatával csak együtt garantálhatják a hatékony védekezést. A felsorolt feltételek fennállása esetén is, folyamatos képzések és fejlesztések szükségesek a „naprakész” komplex biztonsági rendszer fenntartásához.

KUTATÁSI MÓDSZEREK

A kutatási célkitűzésemben felsoroltak megvalósítása érdekében a következő módszereket alkalmaztam:

- az improvizált robbanóeszközök terrorista jellegű alkalmazásáról szóló nyílt, sajtóban megjelent esettanulmányok, tudósítások, mint elsődleges források feldolgozásával, az ott használt indítószerkezetek rendszerezésénél az indukció módszerét;
- a kereskedelmi forgalomban elérhető úgynevezett „SPY" eszközök felépítésének és műszaki leírásainak tanulmányozásánál, a működési törvényszerűségek feltárására az elemzést;
- a releváns szakirodalom, mint másodlagos források feldolgozása során elsősorban az analízis módszerét, az indítási mechanizmusok vizsgálatánál;
- összehasonlítás a különböző alkalmazott taktikai módszereknél, ahol az eltérések és hasonlóságok kerülnek feltárásra;
- tapasztalati (empirikus) módszer alkalmazása a detektáláshoz kapcsolódó mérések során közvetlen és közvetett megfigyelések, továbbá a kapott eredmények szintézissel történő feldolgozása.

Az írott-, és az elektronikus források vonatkozásában primer kategóriába a robbantásos merényleteket közvetlenül bemutató tudósításokat, riportokat, szakértői jelentéseket soroltam. A másodlagosként az ezen eseményeket feldolgozó és elemző tanulmányokat tekintettem. A „publikus" -, és a „dark" – weben egyaránt célirányos kereséseket végeztem az improvizált robbanóeszközök leírásával, felépítésével kapcsolatban, külön elemezve az ott bemutatott szerkezetek, megoldások működőképességét és megvalósíthatóságát. A rádiófrekvenciás mérésekhez kapcsolódó szakirodalom feldolgozásánál, külön figyelmet fordítottam az EMC[3] tárgyköréhez tartozó, úgynevezett elektromágneses zavarok felderítésére, azon belül is elsődlegesen a sugárzott jelek és azok terjedési vizsgálataira.

Az empirikus módszerként, közvetlen méréseket végeztem elsősorban a vevőegységek detektálhatósága vonatkozásában, az alkatelemek elektrofizikai tulajdonságaitól függően, különböző metodikával, amelyek szintén a primer kategóriába sorolhatók.
Ehhez kapcsolódóan másodlagos információforrásként a rádiós egységek gyári műszaki-működési leírásait tekintettem kiindulópontként, amelyek alapján megpróbáltam beazonosítani a „sugárzásra képes" alkatrészeket.

[3] Electromagnetic Compatibility – elektromágneses kompatibilitás

1 OBJEKTUMOK BIZTONSÁGA

Az objektumokról általában, hogy mit nevezünk objektumnak, milyen fajtáit különböztetjük meg a funkcionalitás, elhelyezkedés vagy akár a kialakítását figyelembe véve. A védelem szempontjából hogyan kategorizálhatjuk őket, és ennek megfelelően milyen biztonsági rendszert építünk ki a fenyegetettségtől függően. A kutatásom alapjául szolgáló kiemelten védett objektumok esetében a biztonságtechnikai rendszerek főbb jellemzőit vizsgálom a feltételezett kockázatok figyelembevételével. A hipotéziseim közül az első témakörre vonatkozó megállapításaim ebben a fejezetben kerülnek kidolgozásra.

Tekintettel az Objektumvédelemre, mint kiterjedt és összetett témakörre a kutatásom elsődlegesen annak egy speciális részére, a jogszabályok által „kiemelten védett" kategóriába sorolt területére koncentrálódik. A Biztonságtudomány ezen szűk részéhez az általános fogalmak ismertetésén keresztül jutok el, a területhez tartozó biztonsági rendszerek és intézkedések ide vonatkozó vizsgálatán keresztül.

1.1 Az objektum fogalma

A kifejezés eredetét tekintve, latinul tárgyat jelent, de a hétköznapi szóhasználatban sokféleképpen értelmezhetjük. A kutatásom során az értelmező szótárban főnévként megjelölt épületet, építményt vagy létesítményt használom meghatározásként, amelyet elsődlegesen a biztonság szempontjából vizsgálok.

A teljesség igénye nélkül, az objektum jelentésére csak a magyar nyelv értelmező szótára szerinti változatot ismertetem, amely a következőképpen szól:

„...***objektum*** *[ë] főnév -ot, -a*

*1. (**ritka**, **filozófia**, **választékos**) Tárgy, dolog. Mi az a szülőföld szeretete? Nálam, ahol… a gyermekkorra szorul a szülőföld minden emlékképe, valóban úgy tűnik fel, mint valami objektumnak az emberre gyakorolt hatása. (Móricz Zsigmond)*

*2. (**hivatalos**) Épület, építmény, létesítmény. Az állami gazdaság területén levő objektumok; a telekkönyvben szereplő objektumok. A ház a Boronkay nevén van, erősen megterhelve … s megjegyzem, részemről az alku még a feleségem beleegyezéséhez van kötve, mert ő nem akar egy ilyen nagy objektumba belemenni. (Móricz Zsigmond)*

..." [1]

A biztonságtechnika szemszögéből értelmezve az objektum fogalmát, szinte mindegyik esetben szerepel az épület, építmény vagy a létesítmény megnevezés, és ezzel együtt megjelenik - természetesen a funkcióra utalva - a védelem szükségessége is. [2]

1.1.1 Az objektumokról általában

Az emberiséggel gyakorlatilag együtt fejlődött a különböző korokon keresztül, maga a védelemre vonatkozó igény és ennek megvalósítására az objektumok technikai kivitelezése is. Kezdetben az őskori leletek alapján a barlangok látták el ezt a funkciót, amelyek nagyrészt még a természet által létrehozott képződmények voltak. Esetenként minimális átalakítással, kiegészítéssel rendelkeztek az adott ismereteknek, felszereléseknek megfelelően különböző bővítményekkel ellátva. Helyenként ez a fajta „építkezési mód" olyan szintre fejlődött, hogy nem lehetett elhatárolni hol ér véget a barlang és hol kezdődik az építmény (jellemzően a sziklákba vájt épületek vagy lakóterek sokasága). Ezt követően került sor az épített földsáncok, kőzetbe vájt üregek erősítéssel, majd az építőanyagok felhasználásával az állékonyabb épületek, mint például a kővárak és várfalak felépítésére. Azt, hogy pontosan mi ellen kellett védekezni ez jellemzően egy dinamikus folyamatot jelentett, mert a környezeti hatásokon felül, a külső fenyegetés jellege is formálta az objektumaink kialakítását. Az építményeknek jellemzően egy „külső" támadás elleni védelem volt az egyik elsődleges funkciója, amely már a megközelíthetőségükben is megmutatkozott. A létesítmények ugyanis a természetes akadályokat képező meredek sziklaormok, közvetlen folyók mellé, általában külön falazattal körülvéve, illetve megerősítve épültek. A biztonság szempontjából ezek a megoldások jellemzően a fizikai védelem kategóriájába sorolhatók, amelyek a kor technikai feltételeihez igazodva, bizonyos ideig elégségesnek bizonyultak. A haditechnika fejlődése következtében a várak védelmi jelentősége háttérbe szorult. Az urbanizáció hatására egyre több - funkcióját tekintve kiemelt fontosságú – létesítmény vált a mindennapi életünk részévé. A városok népességének rohamos növekedése, az épületek elhelyezkedésének sűrűsödése, a közlekedési útvonalak kiépítése, mind-mind a lakókörnyezetük egyre zsúfoltabbá válását okozta és okozza napjainkban is. Az épületeink rendeltetésük alapján egyre sokrétűbbé válnak, amelynek következtében egy időben többféle szolgáltatást kell biztosítaniuk a bent tartózkodóknak. A mai modern építmények már nem hasonlítanak se kialakításukban, se a használatuk szempontjából az elődjeikre, sőt sok esetben kifejezetten extrém megoldásokat tartalmaznak mind a megjelenésüket vagy akár a műszaki megvalósításukat tekintve. A legújabb kori

fejlesztéseknek köszönhetően, az úgynevezett „okos” megoldások elterjedésével, már a közvetlen környezetünkből kiindulva, a lakásokon belülről, a házakon át, egész városokat magukba foglaló infokommunikációs hálózatokat hozunk létre, amelyek egy rendszert képeznek. Látható az a mérhetetlen fejlődés, amely alatt a barlangoktól eljutottunk napjaink felhőkarcolóihoz és ezzel mennyire összetett és komplex környezetet alakítottunk ki magunk körül. Az épületek eredeti feladatai között meghatározó szerepet töltött be a „védelmező” jelleg, amely sok esetben mára már háttérbe szorul bizonyos kényelmi szempontok javára. A rendeltetésük alapján határozzuk meg a védelmi fokozatukat és ezek megvalósítására már az építési fázisban bizonyos intézkedéseket szükséges megtenni a kívánt cél elérése érdekében.

Ez a fajta sokféleség, amely az objektumokat jellemzi a funkciójukat, felépítésüket vagy akár az elhelyezkedésüket tekintve, meglehetősen bonyolult védelmi rendszereket igényelnek az általunk meghatározott biztonsági szint elérése érdekében. Nem lehet külön-külön kezelni az építményeket, hanem sok feltételt figyelembe véve, adott esetben csoportokba rendezve, az egymásra gyakorolt hatásokat is számításba kell venni, és így alakítani ki a leghatékonyabb biztonságtechnikai megoldásokat.

1.1.2 Az objektumok funkciója

Az építmények, létesítmények a betöltött szerepük szerint is csoportosíthatók, amely nagyban meghatározza a kialakítás-, és a megvalósítandó védelem módját. A rendeltetésük alapján különböző sorrendiséget is felállíthatunk, de én a kutatásom alapjául az állam működése szempontjából kiemelkedően fontos létesítményeket veszem górcső alá, ezen belül is az államigazgatási, államhatalmi funkciókat betöltő objektumokat.

Az épületek rendeltetését és ez alapján a kialakítás módját, nem választhatjuk el, mivel a két fogalom egymásra hatással van. Célunk, a funkcionalitás hatékonyságának szem előtt tartásával a lehető legbiztonságosabb létesítmények megalkotása.

Az építményeket ezen felül további kategóriákba sorolhatjuk a rendeltetésük szerint, mint például az energia ellátásáért és elosztásáért létesített, az egészségügyi intézmények, kórházak, gazdasági-, oktatási-, vallási-, kereskedelmi-, vendéglátóipari épületek vagy akár a hír-, távközlési létesítmények, illetve a pénzintézetek, továbbá a közösségi közlekedés épített objektumai (pl.: metró alagút). [2]

A szerepüket tekintve nem sorolhatók a kevésbé fontos létesítmények kategóriájába például az egészségügyi vagy az oktatási intézmények az államhatalmi épületekkel

szemben, viszont az elmúlt időszakban, a háborús övezeteken kívüli terrorista-, valamint információszerző jellegű támadások „kedvelt” célpontjai jellemzően az utóbbiak voltak.

1.1.3 Az objektumok kialakítási módjai

A kialakítás módja szerint, elsősorban a fizikai kiterjedését tekinthetjük a legmeghatározóbbnak, hogy milyen méretű építményről is van szó. Ez alapján a vertikális irányból közelítve, a földszintes kiviteltől kezdve a toronyházakig bezárólag találkozhatunk bármilyen nagyságú épülettel. A horizontális szempontból előfordulhatnak akár több száz kilométeres hosszúságú létesítmények is, mint például az energiaellátási szektorban található nagyfeszültségű villamos távvezetékek, a hozzákapcsolt transzformátor hálózattal. A biztonság szempontjából az egyik legfontosabb rendszernek tekinthetjük a korábban említett publikus közlekedéshez tartozó metróhálózatot, az összes felszíni és a mélyépítéssel kialakított objektumaival együtt.

Az építmények elhelyezkedése alapján beszélhetünk önálló épületekről, iker-, vagy tömbösített változatokról, ahol adott esetben a méretbeli különbségek is jelen vannak. Az építkezéseknél alkalmazott anyagok szerint is csoportosíthatjuk a létesítményeinket, annak tükrében, hogy melyik a meghatározó építőanyag. Az életünk egyéb területeihez hasonlóan itt is megfigyelhető a különböző tervezési és kivitelezési trendek változása, amely alapján minden kornak megvannak a kedvelt építőelemei, napjainkban elég nagy népszerűségnek örvend a látható „natúr” vasbeton szerkezet üveggel, illetve acél felületekkel kombinálva.

Az építőanyagoknak a biztonságtechnika szempontjából elsősorban a fizikai, azon belül is a mechanikai, illetve a statikai jellemzőik dominálnak, amelynek köszönhetően szerves részét képezik a védelmi kialakításoknak. Fontos szerepet játszanak az állékonyságukból kifolyólag, például az építmények robbantás elleni védelmében. Az anyagszerkezeti tulajdonságok szempontjából, a kutatási területemhez kapcsolódó úgynevezett rádiófrekvenciás csillapítási tényező az egyik leglényegesebb jellemző. Ez a gyakorlatban magának az épület különböző szerkezeti összetevőinek, az elektromágneses hullámok terjedésére gyakorolt hatását jelenti, ami általában gyengítő vagy „árnyékoló” következményekkel jár. Információvédelmi szempontból, kifejezetten előnyös jelenségként tekintünk az építőanyagok ezen tulajdonságára. A legtöbb esetben különböző anyagok alkalmazásával, ezen hatások kombinációjával alakítjuk ki a kívánt védelmi szintet. Nem elhanyagolható szempont lehet a rádiófrekvenciás hullámok

verődésének a jelensége, amely elsősorban a sugárzás pontos helyének a meghatározásánál jelentkezik, mint nehezítő tényező.

1.2 Kockázatértékelés

A biztonságtechnika szempontjai szerint megközelítve egy objektum tervezését, ahhoz szerteágazó és komplex ismeretekre van szükség. A biztonságot, mint a legfontosabb feltételt szem előtt tartva, egy alapos elemző-, értékelő munkának kell megelőznie a védelmi rendszer összeállítását. Ennek során a tervezett létesítmény funkcióját, elhelyezkedését, kialakítását, és adott esetben az ott dolgozók, vagy ideiglenesen bent tartózkodók személyét is figyelembe véve, szükséges meghatározni a lehetséges kockázati tényezőket, illetve veszélyforrásokat. Az objektumvédelemhez kapcsolódóan, mint tudományterület különböző szempontjait vizsgálva, azon belül a kutatásom egy nagyon speciális részét foglalja magába a kiemelten védett objektumok esetében.
A biztonságtudomány meghatározó pillérének tekinthetjük a biztonságot, amely már magában is egy állapot jellemzésére szolgáló fogalom. A biztonságot mindig valamilyen veszély vagy kockázati tényező meglétével kölcsönhatásban értelmezhetjük, és az ellene tett intézkedések, kialakított rendszerek együttes hatása hoz létre valamilyen védettségi szintet, a nem kívánt hatások csökkentése érdekében. Ennek a mértéke a védelmi rendszerek komplexitásától és a megfelelő alapossággal elvégzett kockázatelemzéstől függ. [3]
Kutatásom során a védett objektumok jellege miatt, a biztonság fogalmát kiterjesztetten értelmezem, a személy- és vagyonvédelmen felül, az információvédelem megvalósítását is kiemelten, azzal együtt kezelem.

1.2.1 Az értékelés folyamata

A kockázati tényezők és a lehetséges veszélyforrások feltárását követően, egy iterációs folyamat végeredményeként lehet meghatározni a komplex védelmi rendszer összetevőit. Az elemző-értékelő ciklus alatt, a számításba vehető veszélyek összetevőit és azok bekövetkezésekor jelentkező károk várható mértékét egyenként vizsgálva, az elhárítására alkalmas biztonsági alkalmazások költségeivel összehasonlítva kapjuk a legoptimálisabb eredményt. Tekintettel az objektumok jellegére, valamit az ott dolgozó szintén „védett” személyekhez kapcsolódóan, az esetlegesen felmerülő támadási típusok tárháza, meglehetősen széleskörű. Ezek vizsgálatát, előfordulási valószínűségét nem csak külön-

külön, hanem egymással összefüggésben is figyelembe véve - a védelmi rendszerünket lehetőség szerint - ennek megfelelően kell optimalizálni.

A mai modern biztonságtechnikai megoldásoknak már képesnek kell lenni a fenyegetettség dinamikus változását is lekövetni, a terrorizmus és a nemzetközi helyzet alakulásának megfelelően. A komplex védelmi beruházást olyan innovatív módon kell megvalósítani, hogy az a szükséges fejlesztésekre alkalmas tartalékokkal rendelkezzen, és adott esetben a bővíthetőség megoldható legyen a hatékonyabb működés biztosítása mellett. A technikai fejlődés mindennapjainkra gyakorolt hatását mi sem példázza jobban, mint a mobilkommunikáció terén tapasztalható változások, az egymásutáni generációk viszonylag rövid időn belüli megjelenésével (2G, 3G, 4G, 5G, *6G*). Az említett technológiai váltások a mobiltelefónia területén nagyjából 3-5 évente történtek a megjelenésüktől kezdődően, amit a napjainkban alkalmazott rendszer esetében a ’90-es évektől számítunk. A generációs váltások során a főbb rádiós paraméterek is változtak úgy, mint a moduláció, sávszélesség és a vivőfrekvencia. A folyamat részeként a rádiós környezetben történt változások nagymértékben kihatnak az általam kutatott területre, mivel mindkét részt markánsan érintik (robbantás elleni védelem, információvédelem). A kockázat jellegét tekintve, amely lényegében a védett objektumba esetlegesen bejuttatott improvizált robbanószerkezet vagy távirányítású lehallgató berendezés hatékony detektálását jelenti, a védelmi rendszer tervezésénél az említett technológiai változásokat is figyelembe kell venni.

A kiemelten védett objektumok beléptetéshez kapcsolódó átvizsgálások és a folyamatos őrzésével, felügyeletével összefüggő információ-. és robbantás elleni védelemhez kapcsolódó kockázatok rendszerszintű elemzésére, a kutatás során az ok-okozati (Ishikawa[4]-módszert) alkalmaztam. Maga a módszer lehetővé teszi, hogy a komplex védelmi rendszer folyamatában résztvevő technikai-, humán-, szervezeti és természetesen a környezeti tényezők egymásra gyakorolt hatásait strukturált módon, hierarchikus összefüggésben vizsgáljam.

A tényleges diagram a mellékletben található, annak felépítését a következőkben ismertetem.

A klasszikus 6M modellt használtam a rendszer hibáinak feltárására, ahol a központi problémát maga a „hal feje” szimbolizálja, ami egyben a fő kockázati eseményt is jelenti:

[4] Dr. Kaoru Ishikawa (1915-1989) japán professzor, a minőségellenőrzési körök (QC) megalkotója

- A beléptetési és felügyeletei rendszer hiányosságai következtében a védett objektum területére elektronikus indítású robbanóeszköz vagy rejtett lehallgató-megfigyelő eszköz bejuttatása.

Az lehetséges okok közül csoportonként a következő szempontokat vizsgáltam:

I. Technológiai eszközök

Ebbe a kategóriába tartoznak az objektumvédelemben alkalmazott technológiai berendezések és műszaki megoldások kockázatai, amelyek az oda belépők vagy az ott benntartózkodók, illetve az oda beszállítandó tárgyakat átvizsgálni és az épületben üzemelő egyéb technikai eszközök működését hivatottak felügyelni. A kategória alágai:

- Személy-, csomagvizsgáló berendezések képalkotása és felbontása, szoftveres elemzése;
- Behatolásjelző rendszer zónázási hibái;
- Videotechnikai rendszer holtterei, kamerák fényérzékenysége, felügyeleti szoftver hiányosságai;
- RF-monitor rendszer hiánya vagy „lefedettsége” (érzékelési határa);
- Szenzorok elhelyezése nem megfelelő.

II. Humán tényező

A humán összetevőhöz kapcsolódó kockázati elemeket általában a technikai eszközök előtti szempontonként szokás feltüntetni a folyamatban, de én szándékosan módosítottam a sorrenden, mivel a kiemelten védett objektumok esetében jellemzően „másodlagos” tényezőkként tekintenek rá a gyakorlatban. A következő alágak sorolhatók ide:

- Biztonsági személyzet képzettségi szintje;
- IED-, és lehallgató eszközök felépítése ismeretének hiánya;
- Figyelemcsökkenés, monotonitás 24/7 rendszerek felügyelete;
- Protokollok következetlen betartása;
- Jogosultságkezelési hibák;
- Belső fenyegetettség jelenléte (szándékos vagy gondatlan közreműködés).

III. Módszertan és eljárások

Ebbe a kategóriába tartoznak elsősorban a komplex védelmi rendszer működési folyamataihoz kapcsolódó kockázati tényezők, amelyek a következő alágakban vannak felsorolva:

- Beléptetési protokollok hiányai;
- Zónarendszer következetlen alkalmazása;

- Reagálási idők nem definiáltak;
- RF[5]-ellenőrzés, feldolgozás hiánya vagy nem integrált alkalmazása;
- Kizárólag eseti jellegű technikai átvizsgálások;
- Incidenskezelési eljárások hiánya vagy késlekedése.

IV. Környezet

A környezeti hatások, amelyek közvetlenül befolyásolják a rendszer működését, az alábbi alágakba sorolva:

- Nagy személy-, teherforgalom;
- Külső infrastruktúra közelsége;
- Időjárási és fényviszonyok (videotechnikára gyakorolt hatása);
- Zsúfolt rádiófrekvenciás spektrum;
- Épületszerkezeti árnyékolás és verődések.

V. Szervezeti irányítás

A menedzsmenthez köthető okok elsősorban a stratégiai irányítás hiányosságai következtében, úgynevezett rendszerszintű sebezhetőséget generálnak a védelmi rendszerek működésében, a felsorolt alágak szerint:

- Kockázatelemzés hiánya vagy elavultsága;
- Technológiai fejlesztések elmaradása;
- Képzési rendszer hiányosságai;
- Együttműködés hiánya a védelemben résztvevő egységek között;
- Szabványosítás hiánya;
- Auditálás és ellenőrzés hiánya.

VI. Anyag és infrastruktúra

Az infrastruktúra fizikai tulajdonságaihoz kapcsolódó okok, amelyek közvetlenül befolyásolhatják a védett objektumon belüli IED-k, lehallgató eszközök rejthetőségét és működtethetőségét, az alábbi alágak felsorolásában:

- Építőanyagok csillapítása és árnyékoló jellege;
- Gépészeti terek, álmennyezetek, kábelcsatornák;
- Ideiglenes szerkezeti elemek (építés és átalakítás);
- Bútorzat és burkolatok esetében a rejthetőség jellege.

[5] RF - rádiófrekvenciás

1.3 „Védett” objektumok

Az általam vizsgált államhatalmi és államigazgatási létesítmények esetében, a „védett” kategória elsősorban a fenyegetettség elemzésének és a hozzá kapcsolódó biztonság kialakításának az aspektusából származik. Értekezésemben nem kívánok foglalkozni az építészeti értékeket képviselő, úgynevezett műemlék jellegű kategóriával, valamint az „értéktároló” típusú épületekkel, ezeket csak felsorolásként, mint lehetséges osztályozási módot említem. A kutatásom alapjául szolgáló terület közvetlenül, a biztonságtechnika egy meghatározott részére koncentrálódik, amely szorosan kapcsolódik azon objektumokhoz, amelyekben az állam működését meghatározó tevékenység zajlik. Az információvédelem és a robbantás elleni védelem, mint két kiemelten kezelt terület képezi az értekezésem alapját.

Mindkét fenyegetettségi típus komoly figyelmet kell, hogy kapjon az objektumvédelem területén, mivel a hatásukat tekintve, nehezen jósolható a bekövetkező tényleges kár mértéke. Az improvizált robbanóeszközök és a lehallgató berendezések együtt kezelése első ránézésre szokatlannak tűnhet, de figyelembe véve az IED-k evolúcióját, valamint a háborús konfliktusban érintett országokban előforduló eseteket tanulmányozva, közös pontot találhatunk a detektálás területén. Ezt a lehetőségek ki kell használnunk a biztonságtechnika alapelveit szem előtt tartva, hogy a fenyegetettséget a lehető legalacsonyabb szintre tudjuk mérsékelni.

Nagyon sok tanulmány foglalkozik manapság a robbantás elleni védelemmel az objektumok tekintetében, de jellemzően az épületek detonációval szembeni állékonysága vagy a védendő létesítmény robbanóanyaggal való megközelítésének megakadályozása az elsődlegesen vizsgált terület. A robbanóanyagok hatásmechanizmusát tekintve, egy esetleges épületen belül bekövetkező robbantás, a lehető legsúlyosabb következményekkel járó káresemény, mivel a „zárt” térben lejátszódó folyamatok egy speciális helyzetet teremtenek. A háborús övezetektől távoli országokban is előfordulnak terrorista jellegű robbantásos merényletek, amelyeket személyek-, vagy különböző objektumok ellen követnek el. Az elkövetés módja felől megközelítve a cselekményeket, közös motívumokat fedezhetünk fel bennük, mégpedig szinte egytől-egyig előre megtelepítve a helyszínt, a célterületen elrejtve vagy álcázva helyezték el a pokolgépeket. Ennek tükrében fő feladatként, az improvizált robbanószerkezetek bejuttatását kell megakadályozni az épületeinkbe, amennyiben ez nem sikerült, akkor a merényletet

megelőzően szükséges a rejtett IED-k felkutatása, az összes lehetséges biztonságtechnikai berendezésünk és az ehhez kapcsolódó taktikai megoldások alkalmazásának segítségével. Az említett két fontos kockázati tényező meghatározó szerepet tölt be a kormányzati épületek őrzésében a fenyegetettség szempontjából, amelynek elhárításában egy többszintű, összehangolt biztonságtechnikai rendszer képes a feladatának megfelelően eredményesen működni. A védett objektumok vonatkozásában elsősorban a rendeltetésük, valamint a funkciójuk határozza meg a szükséges biztonsági szint elérése érdekében, a komplex védelmi rendszerek kialakítását. A védelem kiépítése során figyelemmel kell lenni arra a fontos tényezőre is, hogy sok esetben bizonyos protokolláris szempontok is dominálhatnak a normál hétköznapi működés mellett, például egy külföldi delegáció beléptetése alkalmával. Az ilyen helyzetekben kerülnek előtérbe a „láthatatlan védelem" eszközei, a különböző szenzorokkal ellátott detektor kapuk, vagy akár a lehallgatás elleni védelemmel rendelkező tárgyalók, és a rádióspektrum ellenőrző rendszerek.

1.3.1 Komplex védelmi rendszer

Egy biztonságtechnikai védelmi rendszer az én véleményem szerint, akkor tekinthető komplexnek, ha az egyes területei egymástól nem csak függetlenül, hanem összehangoltan is képesek működni, adott esetben még átfedés is található a különböző szektorai között. Ez a gyakorlatban azt jelenti, hogy például a beléptetésnél alkalmazott csomagátvizsgálást egymást követően több, különböző elven működő berendezéssel is végrehajtjuk, és az együttes eredményt elemezve hozzuk meg a szükséges döntést. Reptereken és egyéb kielemelten védett létesítményeknél találkozhatunk hasonló megoldásokkal a személyek átvizsgálásánál, ahol a mikrohullámú testszkennert követően egy mágneskaput vagy robbanóanyag detektort is alkalmaznak az alaposabb ellenőrzés végett. [4]

A kutatási témámhoz közvetlenül kapcsolódó tevékenység vonatkozásában, még inkább előtérbe kerül a védelmi rendszerek egymásra hatása, ugyanis szükséges kiterjesztetten kezelni a fenyegetettségre utaló információkat, és azokat egymással összefüggésben, értelmezni. Ezt a folyamatot csak komplex biztonsági implementáción keresztül valósíthatjuk meg, amelynek egyik fontos eleme a megfelelő rugalmassággal rendelkező értékelő-elemző szoftver. Alkalmasnak kell lennie a dinamikusan fejlődő - elsősorban a rádióspektrum tekintetében - környezethez, és a technológiai változásokhoz - a detektálás és a jelanalízis vonatkozásában egyaránt - azok legpontosabb lekövetéséhez. A legújabb

fejlesztésekben egyre többször találkozunk az úgynevezett „tanítható” alkalmazásokkal, amelyek képesek a korábbi mérési eredményeiket is figyelembe véve, együttesen vizsgálni a detektált jeleket. Továbbá csökkenteni kell a biztonságtechnikai rendszereinkben a legnagyobb hibaszázalékot generáló „humánfaktort” és a valós idejű, folyamatos felügyeleti idő kiesését.

1.3.2 Kiemelten védett objektumok

Hazánkban az állam működése szempontjából kiemelkedően fontos létesítményeket külön jogszabályokban foglaltak szerint kell védeni, amelyekben meghatározzák a személy-, és objektumvédelemhez kapcsolódó feladatköröket, azok szükséges tárgyi-, és személyi feltételeit. A felsorolt szempontokon felül nem elhanyagolható az információvédelem tekintetében, az épületben kezelt minősített adatok és az ott keletkező vagy elhangzott egyéb érzékeny információk. A minősített adatkezelés szerves részét képezi a betekintés és megismerés személyi feltételei mellett, az ezekhez közvetlenül kapcsolódó biztonságtechnikai rendszerek, illetve a védendő adatok tárolásának, őrzésének szabályai is, amelyek részletesebb vizsgálatára a kutatásom nem terjed ki.

Az épületeken belül szükséges úgynevezett biztonsági zónákat kijelölni, az oda történő beléptetés rendjét meghatározni, amelyet folyamatos kontroll segítségével ellenőrizni. Ez a rendszer csak akkor képes hatékonyan működni, ha biztonsági személyzeten felül, az ott dolgozók, valamit az oda látogatók is maradéktalanul betartják az előírt szabályokat.

A technológiai fejlődés hatására az infokommunikációs rendszereink és berendezéseink is napról-napra változnak, egyre összetettebbé és szofisztikáltabbá válnak. Ezekre való tekintettel az államirányítási-, központi stratégiai-, gazdasági szervek épületének, ennek megfelelő fejlettségű védelmi rendszerrel kell rendelkeznie. Az objektumvédelemben alkalmazott hagyományos elektronikai védelmi berendezéseken felül, speciális detektáló-, ellenőrző monitor hálózatra van szükség, amely alkalmas ebben a meglehetősen „zsúfolt” rádiófrekvenciás környezetben is hatékonyan észlelni, és adott esetben azonosítani is a veszélyt jelentő elektronikai eszközöket.

Az RF-monitor rendszer kiegészítésére szükség lehet különböző aktív és passzív működésű megoldásokra, mint például a sokak számára ismert rádió-zavaró eszközökre (jammer) vagy a vezeték nélküli átviteli út csillapítását növelő egyéb kialakításokra, úgynevezett Faraday-kalitka jellegű helyiségekre. Tekintettel a munkakörnyezet technikai felszereltségére, az egymással folyamatos kapcsolatban lévő rendszerekre, egy elektromágneses zavarkeltő berendezés használata, meglehetősen „összekuszálná” a

szálakat a napi feladatvégzés alkalmával. A megfelelő rádiófrekvenciás árnyékolás kiépítését sok esetben az épületek belső kialakítása korlátozza, az alkalmazását pedig a protokoll nehezíti.

A korábbi években megvalósított védelmi rendszereink mind technikailag és természetesen az alkalmazott metódusok tekintetében is megújításra szorulnak. A jelenlegi és a közeljövőben várható fejlesztések miatt, napról-napra új kihívásokkal kell megküzdeni a biztonsági rendszereinknek, amelyek a megfelelő fejlesztések nélkül, nem lesznek képesek felvenni a harcot az újonnan megjelenő fenyegetettségekkel szemben. A meghatározott védelmi szint garantálása érdekében szükséges a folyamatos fejlesztés és az állomány képzése, már nem elegendő kizárólag a „fizikai" jelenlét biztosítása egy kiemelten védett objektum tekintetében. Az ismertetett szempontok alapján, egy strukturált biztonságtechnikai rendszer, a megfelelő speciális képzettséggel rendelkező személyzettel képes garantálni hatékony védelmet. [5]

1.3.2.1 Jogszabályi háttér

A védett személyekről és a kijelölt létesítmények védelméről Magyarországon jogszabályban rögzített módon a Rendőrség és a Terrorelhárítási Központ[6] (a továbbiakban TEK) gondoskodik. A jogszabályok konkrétan nevesítik a védendő személyek körét és meghatározzák a védett objektumok őrzési feltételeit. A rendőrségen belül a Készenléti Rendőrség (a továbbiakban KR) Személy- és Objektumvédelmi Igazgatóság, a Terrorelhárítási Központ esetében pedig a Személyvédelmi Igazgatóság feladatkörébe tartozik a jogszabályban felsorolt létesítmények és személyek védelmét biztosítani. A teljesség igénye nélkül ismertetnék néhány ide vonatkozó jogszabályt, amelyek az objektumvédelem szempontjából meghatározzák az adott szervezetek munkáját. Az 1994. évi XXXIV. törvény a Rendőrségről (a továbbiakban Rtv.) I. Fejezetében a feladatok felsorolása között található konkrétan a személy- és objektumvédelemre utaló pont:

„…1. § 6a. védi a jogszabályban meghatározott, Magyarország szempontjából különösen fontos személyek (a továbbiakban: védett személy) életét, testi épségét; őrzi a jogszabályban meghatározott létesítményeket és értékeket (a továbbiakban együtt: személyvédelmi és létesítménybiztosítási feladatok), …" [6]

[6] A Kormány 232/2010. (VIII. 19.) Korm. rendelete a Terrorelhárítási Központról, 22660 MAGYAR KÖZLÖNY, 2010. évi 135. szám.

A megfogalmazás általános módon határozza meg a védelmi tevékenységet, a Magyar Köztársaság érdekei szempontjából „különösen fontos” személyek, és létesítmények vonatkozásában. Az Rtv. V. Fejezetében 46. §-ban találhatunk még a személyvédelemi és létesítménybiztosítási intézkedésekkel összefüggésben egy kicsit konkrétabb feladatszabást. A védett épületekbe való bejutás és az esetleges technikai ellenőrzés lehetőségét biztosítja a rendőrség számára.

A jogszabályi hierarchiát figyelembe véve, az Rtv. -ben nevesített feladatkör végrehajtásának utasítása a 160/1996. kormányrendelet határozza meg a szervezetek számára felsorolás formájában a védelemre jogosultak körét és az őrzési kötelezettséget a kiemelten fontos létesítmények esetében. Az 1996 óta hatályos jogszabály többször is módosításra került, de a legutóbbi 2024. december 17-én megjelent változatában szerepel először nevesítve az információvédelem mint tevékenység, amely a következő módon lett megfogalmazva:

„…c) szükség esetén az Rtv. 46. § (1) bekezdésében foglaltakon túlmenően – indokolt esetben külföldön is – intézkedik a tűzszerészeti, élelmiszer-biztonsági, továbbá a vegyi, biológiai vagy nukleáris veszélyek felderítésére és elhárítására irányuló, valamint az információvédelmi tevékenység végrehajtása érdekében haditechnikai minősítésű eszközöket igénylő ellenőrzés lefolytatására. …” [7]

A kutatásom alapjául szolgáló területhez kapcsolódóan, itt jelenik meg konkrétan az információvédelem érdekében - haditechnikai minősítésű eszközzel – végrehajtott ellenőrzés - technikai átvizsgálás - ami a lehallgatás elleni védelem egyik legfontosabb összetevője.

A biztosítási feladatok során a konkrét tevékenységi körök a rendőrség kijelölt egységei számára a 19/2013. (V. 17.) ORFK[7] utasításban vannak meghatározva. Az utasítás pontokba szedve (1-10-ig) taglalja a II. Fejezetben *„RÉSZLETES RENDELKEZÉS”* – címszó alatt a következőképpen szól:

1. *Tevékenységi körök*
2. *Személy-, lakás-, munkahely-biztosítás, lakókörnyezet-, útvonal-ellenőrzés*
3. *Helyszín-, híradó́-biztosítás, biztonságtechnikai védelem*
4. *Megelőző́-védelem*
5. *Tűzszerész-, technikai, utazás-, egészségügyi biztosítás*

[7] Országos Rendőr-főkapitányság

6. *A KR Személy- és létesítményvédelmi tevékenységével kapcsolatban felmerülő feladatai*
7. *Veszélyeztetettség megállapítása, védelmi fokozatok*
    a) *kiemelt*
    b) *fokozott*
    c) *megerősített*
    d) *alapszintű*
8. *A Személy- és létesítményvédelmi tevekénység végrehajtásában közreműködő rendőri szervek feladatai*
9. *Biztosítási terv*
10. *Létesítményvédelmi feladatok*

A megelőző-védelmi tevékenységgel szorosan összefügg a veszélyeztetettség megállapítása, amelynek alapján meghatározható a szükséges védelmi fokozat. A jogszabály melléklete tartalmazza a különböző védelmi fokozatokhoz alkalmazható biztonsági intézkedések körét. [8]

Napjainkban a kiemelten védett objektumok védelmi rendszereinek tervezésekor vagy a szükséges fejlesztések elvégzése előtt, nagy hangsúly tevődik a nyílt-, illetve a titkosszolgálatok által összegyűjtött és rendszerezett, fenyegetettségre vonatkozó információkra. Ezen adatok birtokában a kockázatanalízis során vizsgálhatjuk az esetleges támadások bekövetkeztében várható kár mértékének nagyságát. Az állam működése számára kiemelkedően fontos létesítmények esetében, sokszor ez a hatás vagy következmény konkrétan nem megállapítható, ezért törekedni kell a biztonsági rendszerek lehető leghatékonyabb kialakítására, a várható veszélyek elhárításával szemben. [5]

A jogszabályi előírásokat tekintve nem szabad figyelmen kívül hagyni a különleges jogrend kihirdetésével összefüggő, esetleges objektumvédelemhez kapcsolódó intézkedéseket. Magyarország Alaptörvényében a különleges jogrenden belül található az 51/A. cikk, amely a terrorveszélyhelyzetre vonatkozik. Ez a cikk egy nagy eséllyel bekövetkező terrortámadás közvetlen lehetőségére vagy ténylegesen megtörtént terrorcselekményre utal, és azzal összefüggésben felhatalmazást ad a Kormány számára, a sarkalatos törvényben meghatározott intézkedések megtételére. A terrorveszéllyel összefüggésben a 1824/2015. (XI. 19.) kormányhatározat szerint, a belügyminiszter meghatározhat különböző fenyegetettségi fokozatokat, amelyeket bizonyos területrészeket érintően vagy Magyarország egészére rendelhet el. A veszélyeztetettség

mértékét egy négylépcsős skálán jelölik a 4-es (alacsony) fokozattól, az 1-es (kritikus) legmagasabb kockázati szintig bezárólag.

A közelmúltban a COVID-19 hatására kialakult pandémiás helyzetben szükség volt a különleges jogrendben meghatározott „Veszélyhelyzet" elrendelésére, amelynek során egészségügyi-biztonsági intézkedések kerültek bevezetésre az objektumokkal összefüggésben. Az állam működése szempontjából kiemelkedően fontos létesítmények folyamatos működésének fenntartása érdekében, különböző technikai kiegészítéseket kellett alkalmazni az objektumvédelem területén. A normál beléptetési protokollt bővíteni kellett, az esetlegesen fertőzött személyek kiszűrése érdekében a testhőmérséklet mérésére alkalmas berendezések telepítésével. A feladat kivitelezésére sok esetben hőkamerákat alkalmaztak. A különleges jogrend meghosszabbítása jelenleg is tart a járvány elmúltával az orosz-ukrán háború miatt az Alaptörvény 53. cikke alapján „háborús veszélyhelyzet" – címén.

1.3.2.2 Szervezeti változások

A személy- és objektumvédelem alapjait meghatározó normákból látható, hogy azok a '90-es évekből származnak, amely szempont még nem jelent önmagában kockázatot, de kihatással van bizonyos mértékig a végrehajtó szervezetek munkájára. Ez idő alatt különböző szervezeti átalakítások zajlottak a rendőrségen belül, amelyek következtében bizonyos feladatkörök átmozgatásával vagy adott esetben létrehozásával, illetve megszüntetésével jártak. Az általam kutatott terület közvetlenül nem érinti a szervezeti változásokat, illetve változtatásokat, azokat pusztán a védelmi rendszerek fejlesztése és adott esetben újra tervezése szempontjából tekintem relevánsnak. A területet érintően a 2010-től kezdődően voltak a legmarkánsabb változtatások, amely során létrehozták a terrorizmus elleni szervezetet a Terrorelhárítási Központot, melynek feladatkörében külön nevesítve lett bizonyos közjogi méltóságok (Köztársasági Elnök, Miniszterelnök) védelme, továbbá egyéb személyvédelmi tevékenységek. Ez idő alatt zajlott a Köztársasági Őrezred megszüntetésének folyamata, ami 2012. július 01-fejeződött be a KR Személy- és Objektumvédelmi Igazgatóság jogutódlásával a feladatköröket illetően. 2013. január 01-vel megalakult az Országgyűlési Őrség, amelynek szintén szerepel a kiemelten védett objektumok és a jogszabályban nevesített személyek védelme a feladatkörében. [9]

A védett személyek tekintetében is volt némi variálás ugyanis 2015. április 01-től a Köztársasági Elnök védelme átkerült a KR-en belül újonnan megalakult Köztársasági

Elnöki Őrség feladatkörébe, és ezzel egy időben a legfőbb ügyész személybiztosítása a TEK-hez lett delegálva. 2018-ban a 160/1996. kormányrendelet ismételt módosítása következtében a védelemre jogosultak körébe bekerült a külgazdasági és külügyminiszter személye is, szintén a terrorelhárító szerv feladataként meghatározva. 2022 nyarától kezdődően, ismételt változtatásra került sor, a Köztársasági Elnök személyének védelmével kapcsolatban, ugyanis a tevékenység újra visszakerült TEK feladatkörébe. [10]

1.3.2.3 Változásoknak a védelmi rendszerekre gyakorolt hatásáról

A személy- és létesítményvédelemhez kapcsolódó jogszabályok csak egyfajta keretet biztosítanak a végrehajtó szervezetek számára, de a technikai paraméterekre vonatkozólag nem találtam konkrét meghatározásokat vagy rendszertechnikai irányelveket. Az információvédelem egyik fő részének tekinthető minősített adatok védelmét és kezelését, több szintű jogszabályrendszer biztosítja, amelyben az alkalmazott adatátviteli rendszereken felül, az objektumok védelmét is ellátó biztonságtechnikai rendszerek is szabályozásra kerültek. Ezzel szemben a személy- és objektumvédelem területén, sok esetben ezeket a fogalmakat külön kezelik. A minősített adatkezelésre egyfajta statikus módon tekintenek, amely szerint a jogszabályban rögzített módon, úgynevezett kompromittáló kisugárzástól mentes helyiségeket alakítanak ki, viszont a védett személyek vonatkozásában, például a közvetlen munkakörnyezetük, vagy a közlekedési eszközeik esetében, már nem mindig ennyire szabályozott a rendszer. A létesítményekben és az adott biztosítandó helyszíneken gyakorlatilag a végrehajtást végző szervezeti elemek technikai felkészültsége, valamint biztonságtechnikai berendezésekkel való ellátottsága a meghatározó. Ebből pedig egyenesen következik, hogy az alkalmazott technikai eszközök fejlettsége nagyban befolyásolja az adott védelmi fokozatnak megfelelően kiépített rendszer hatásosságát. A biztosításokban részvevő szervezetekre való tekintettel, bizonyosfajta „szabványosításra” lenne szükség, a közös helyszíneken való együttes feladatvégrehajtás gördülékenyebbé tétele végett. A szervezetek vonatkozásában történt relatív gyakori változtatások, megítélésem szerint nem minden esetben szolgálták a komplex védelmi rendszerek megvalósításának lehetőségét. Ez elsődlegesen a nem egységes rendelkezésre álló technikai eszközpark vagy adott esetben az eltérő szemléletmódból adódik. Emiatt szükség lenne egy olyan technikai fórum létrehozására a személyvédelmi szervezetek részvételével, amelynek

elsődleges feladata egy egységes védelmi koncepció kidolgozása a létesítménybiztosításhoz kapcsolódóan.

1.4 Kormányzati objektumokat ért támadások

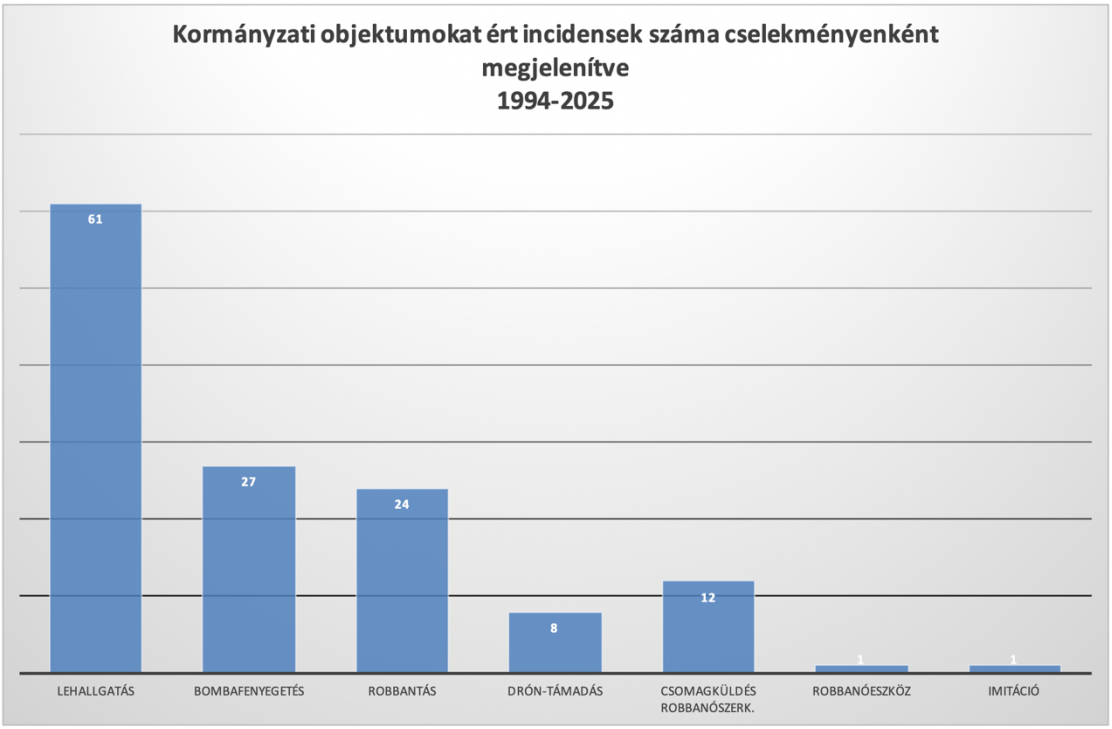
A kiemelten védett létesítményekhez kapcsolódó incidensek vonatkozásában, a nyílt sajtóban is megjelent eseteket vizsgáltam, hogy arányaiban milyen típusú támadások tekinthetők jellemzőnek. A teljesség igénye nélkül, közvetlenül a kutatásom témaköreként meghatározott RF-monitor hálózat, mint a komplex biztonsági rendszer egyik fő eleme alkalmazhatóságának szempontjai szerint választottam, a robbantás-, és a lehallgatás elleni védelmet érintő eseményeket.

A következő diagram szemlélteti összegezve a különböző módokon jelentkező incidenseket, az előfordulási arányaikban. A robbanószerkezetekhez köthető támadások többféle bontásban szerepelnek a kimutatás szerint, amelyek elsősorban a detektálhatóság szempontjait figyelembe véve lettek külön kezelve. A tényleges robbantások bekövetkezését követően, az objektumok esetében egyfajta helyszíni szemle végrehajtása során előkerült bizonyítékok utaltak az alkalmazott improvizált robbanóeszközök felépítésére.

Az imitációk alatt a relatív alkalmatlan IED-re vonatkozó előfordulásokat mutatja, amelyek bizonyos esetben a robbanóanyag nélkül, vagy azt pirotechnikai anyaggal helyettesítve kerültek alkalmazásra.

A rejtett eszközökkel végrehajtott információszerzés, közismert néven a lehallgatás, az objektumok vonatkozásában kvázi támadásnak tekinthető, mivel jellemzően közvetlenül nem az építményre azok berendezéseire, illetve az ott tartózkodókra hat. A következmények az esetek többségében csak később jelentkeznek, amikor a megszerzett - főként védett - információ nyilvánosságra kerül, vagy arra jogosulatlan birtokába jut és azt „ártó szándékkal” felhasználja.

A hétköznapi használatban, a nagy számban megjelent drónok, az elkövetkezendő időszakban mérhető fenyegetettséget képeznek majd a személy-, és az objektumvédelem területén egyaránt.



1**. kimutatás diagram** A sajtóban megjelent kormányzati objektumokat ért incidensek alakulása meghatározott cselekmények szerint összegezve[8]

A végrehajtott robbantások nagy részénél a rendelkezésre álló (publikált) adatok alapján, nem lehetett egyértelműen azonosítani azt a pontot az események bekövetkezése során, amikor minden kétséget kizáróan detektálható lett volna előre a merénylet. Ezen adatok feltüntetésével elsődlegesen a fenyegetettség jelenlétére szeretném felhívni a figyelmet, mivel egy esetleges robbantás bekövetkezése a hatásmechanizmusát tekintve, komoly következményekkel járhat a kiemelten védett létesítmények esetében a funkciójuktól függetlenül.

A bombafenyegetésekre vonatkozó elkövetések a teljesség igénye nélkül lettek jelezve, mivel ezen fajta cselekményeknél nem feltételen kap nyilvánosságot minden egyes eset, viszont a védelem szempontjából ezekre kiemelt figyelmet kell fordítani.

Az imitációk esetében is elsősorban a probléma jelenlétére kívánom felhívni a figyelmet, mivel a relatív alkalmatlan eszközökkel végrehajtott bűncselekmények ugyan olyan végrehajtásra kényszerítik a rendvédelmi-, illetve az objektumvédelmi egységeket, mintha tényleges pokolgépek lennének. Bűnügyi szempontból vizsgálva az ilyen eseteket külön figyelmet kell fordítani arra a tényre, hogy egy imitáció alkalmazása akár „főpróbája” is lehet egy későbbi valós merényletnek. Az alkalmazott biztonsági

[8] A nyílt sajtóban megjelent események alapján szerkesztette a szerző.

intézkedések nagy része ugyanis teljes mértékben felmérhetők és kielemezhetők egy ilyen jellegű fenyegetés végrehajtásakor.

A fenyegetettség kezelésében nagy segítséget jelenthet a beléptetéshez kapcsolódó ellenőrzések, azok műszaki felszereltsége, illetve az eseti jelleggel megfelelő műszerezettséggel végrehajtott technikai átvizsgálások.

Az utóbbi két fenyegetettséget - a kiemelten védett objektumok vonatkozásában - vizsgálva, teljes mértékben alkalmasak az adott típusú létesítményekben történő munkavégzés megzavarására. Magyarországon az ilyen jellegű elkövetésekre külön nevesített jogszabályok lettek megalkotva, amelyek különböző büntetési tételeket helyeznek kilátásba a fenyegetőzőkkel szemben.

1.4.1 A védett létesítmények működésének megzavarása

A magyar Büntető Törvénykönyvnek (a továbbiakban Btk.) alapesetben két szakasza nevesíti a telefonban elhangzó „klasszikus" értelemben vett robbantással való fenyegetést, a betelefonáló által közölt: *„Bomba fog robbanni az .... épületben!"*. Az ilyen típusú fenyegetések mögött, jellemzően nincs valódi szándék a robbantás elkövetésére, ennek ellenére mégis alkalmas a köznyugalom vagy az adott objektum működésének a megzavarására. Az említett esetekben az objektum jellegétől függ, hogy melyik tányállás valósul meg, a cselekmény ez alapján ütköztethető a Btk. 323.§ *Közérdekű üzem működésének megzavarása* vagy a Btk. 338.§ *Közveszéllyel fenyegetés* tényállás valamelyikével. A Btk. XXX. Fejezetében a közbiztonság elleni bűncselekmények között szerepel a 323-as szakasz, amely a következőképpen fogalmazza meg a cselekményt alapesetben:

„(1) Aki közérdekű üzem működését jelentős mértékben megzavarja, bűntett miatt egy évtől öt évig terjedő szabadságvesztéssel büntetendő."[9]

A XXII. fejezetben a köznyugalom elleni bűncselekmények között található a 338-as szakasz, amely például egy bevásárlóközpontba történő, robbantással fenyegető telefonálás esetén, az elkövetővel szemben alkalmazható.

„(1) Aki a köznyugalom megzavarására alkalmas olyan valótlan tényt állít, híresztel, vagy azt a látszatot kelti, hogy közveszéllyel járó esemény bekövetkezése fenyeget, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő."[10]

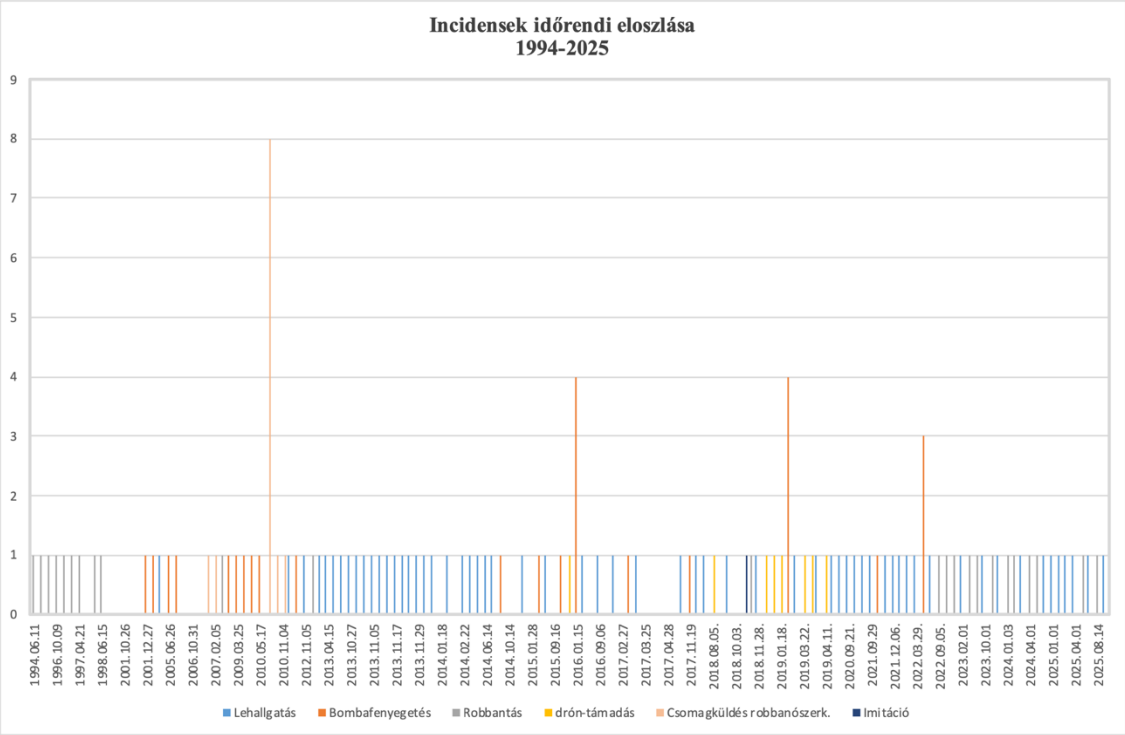
[9] Btk. 323.§ Közérdekű üzem működésének megzavarása
[10] Btk. 338.§ Közveszéllyel fenyegetés

A robbantással való fenyegetés a Büntető Törvénykönyv megfogalmazása szerint, már a puszta tény közlésével is megvalósul, mivel önmagában alkalmas a köznyugalom megzavarására. A közérdekű üzemet érintő fenyegetés esetében pedig, annak működésére gyakorolt hatása révén válik súlyosabban büntetendő cselekménnyé.

Mindkét szakasz esetében a robbantással való fenyegetés hatására keletkező kár vagy okozott zavar mértékétől függ a büntetési tétel, ami jól tükrözi az intézkedési kényszert, hogy ezekben a helyzetekben is végre kell hajtani a teljes kiürítési protokollt a biztonság érdekében a védelem résztvevőinek. Az ilyen szituációk mindig komoly dilemmát jelentenek a védett létesítmények biztonsági vezetőinek annak ellenére, hogy különböző vizsgálatokat végeznek a beléptetéshez vagy a beszállításhoz a személyek és a csomagok vonatkozásában.

Az internet elterjedésével a hálózaton használt népszerű csevegő vagy üzenetközvetítő alkalmazásokon keresztül, egyre többször juttatják a fenyegetéseket a védett objektumok őrzőinek, illetve üzemeltetőinek vagy akár a hatóságok tudtára. Az ilyen jellegű, félelmet keltő üzenetek visszakövetése, a feladó személyazonosságának megállapítása komoly IT-s felkészültséget igényel, és bizonyos esetekben együttműködést a külföldi érdekeltségű szerverek üzemeltetőivel. A tartalmát tekintve (robbantással fenyegetés) az ilyen jellegű cselekményeket is valós kockázatként kell kezelni, amelyeket megfelelő szakértelemmel szükséges lereagálni.

A következő diagram a vizsgált fenyegetettségek időrendi felsorolása látható az elkövetéshez kapcsolódó dátumok megjelölésével. A megjelenített eseményeknek az előfordulásuk szempontjából van jelentősége. A célom elsődlegesen az volt, hogy bemutassam a típusok szerinti megjelenések viszonylagos állandóságát, a kisebb nagyobb besűrűsödésektől függetlenül.



2. kimutatás diagram A sajtóban megjelent incidensek dátum szerinti eloszlása[11]

Az időskálán jól kivehető módon bizonyos fajta állandóság tapasztalható a bombafenyegetések és a lehallgatásokhoz kapcsolódó eseményekkel kapcsolatban, amelyekről a nyílt sajtóban is megjelentek cikkek. A kétféle fenyegetettséget az elemzés szempontjából némileg külön kell kezelni, mivel a lehallgatás viszonylatában jelentős fokú látenciával számolhatunk, azokról nem minden incidens tekintetében kerül ki valós információ a médiába vagy adott esetben csak jóval később számolnak be róla. Ennek a folyamatnak egyik eklatáns példájának tekinthető a „Snowden ügy”. 2013-ban a volt NSA[12] ügynök „kitálalt” a nemzetbiztonsági szolgálatuk tevékenységével és ezzel egyidőben az alkalmazott technikai eszközeik egy részének leírásait a sajtóban közzé tette. [11] Emiatt látható egyfajta kezdő pontként az időskálán, a lehallgatások viszonylag sűrű előfordulása. Ezt követően sorra jelentek meg a leleplező cikkek, hogy „Ki?, Hol?, és Kit?” figyelt meg, illetve hallgatott le. Ez a folyamat rávilágít arra a tényre, hogy a „lehallgatás”, mint tevékenység jelen van a mindennapjainkban a politikában, a hadászatban, a gazdasági területen ugyanúgy akár bizonyos esetekben a magánszféránkat érintően is. A diagram kezdeti szakaszán jól látható módon nem szerepelnek lehallgatásra vonatkozó esemény bejegyzések, de a sajtóban sorra jelentek meg a ’90-es évek második

[11] A nyílt sajtóban megjelent események alapján, dátum szerinti bontásban szerkesztette a szerző.
[12] National Security Agency – Nemzetbiztonsági Ügynökség, az Amerikai Egyesült Államok rádióelektronikai, jelhírszerzéssel foglalkozó (SIGINT) hírszerző szervezete

felében feltételezett ilyen cselekményekre utaló adtok. 2003-ban megjelent Guardian cikke szerint, EU-s politikusokat hallgattak le Brüsszelben az irodáikban, tolmácsfülkékben és magában az Európai Unió Tanácsának és a Tanács Főtitkárságának helyet adó Justus Lipsius nevű épület esetében pedig felmerült, hogy már az építése során „megtelepítésre" került. [12] Az említett szituációk egyértelműsítik, hogy az információ megszerzéséhez fűződő érdekek és igények olyan mértékben jelen vannak a politikai-, hadi-, gazdasági területeken, amelyet nem lehet megelőző intézkedések nélkül kezelni. Ez a helyzet véleményem szerint az objektumvédelem területén bizonyos szempontból szemléletbeli váltásra kell, hogy sarkallja a biztonsági szektorban dolgozó szakembereket.

A jelenleg is zajló orosz-ukrán háború során kiszivárgott minősített információk szerint, az amerikai hírszerző szolgálatok gyakorlatilag folyamatosan lehallgatták a szemben álló felek mellett, a szövetségeseik közül, Izraelt és Dél-Koreát. [13]

Ez a tevékenység gyakorlatilag örök időktől, politikai-, háborús helyzettől, illetve egyéb meggyőződéstől függetlenül mindig velünk van, az egymással szemben vagy azonos táborokban álló nemzetektől eltekintve.

1.5 A védelem kialakításának módjai

Az előzőekben ismertetett fenyegetettségekkel kapcsolatban a megfelelő védelem kialakításához a Biztonságtechnika alapjait figyelembe véve az információbiztonság irányából közelítem meg a szükséges rendszer összeállítását. Sorra veszem a biztonságtechnika alapján kialakítandó védelmi elemeket és mindegyiknél kihangsúlyozom a hatékony védekezéshez elengedhetetlen szempontok figyelembevételét. Első lépésként a „Védelem" és a „Biztonság" fogalomkörét szeretném tisztázni a Biztonságtechnika alapján.

A hétköznapi életünk során gyakran találkozunk a biztonság fogalomkörével különböző irányokból megközelítve. A teljesség igénye nélkül megemlítem elsősorban a biztonságtechnikához közvetlenül kapcsolódó fogalmakat, mint a közbiztonság, a fizikai biztonság, a személy-, vagyonbiztonság, az információbiztonság, amelyekre jellemzően önmagukban is fontos tényezőként tekinthetünk. A biztonság kifejezés alapvetően egy állapotra utal, amelynél szinte minden esetben meghatározható a veszélyeztető tényező vagy tényezők összessége. Ezek alapján kapjuk a korábban felsorolt fogalmakat, amelyekben konkrétan szerepel, hogy a „védett" állapot milyen behatásokkal szemben

valósul meg. Tehát a biztonság megvalósítása érdekében az összes kockázati tényezőt fel kell tárnunk, hogy tudjuk mi ellen védekezzünk és ehhez milyen biztonságtechnikai berendezésekre, illetve szervezeti kialakításokra lesz szükségünk. [2]

Az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Kar, Személy- és Vagyonbiztonság című tankönyvében, a következő módon van definiálva a biztonság fogalma:

„A biztonság személyek és szervezetek azon állapota, melyet, a létüket, illetve rendeltetésszerű működésüket veszélyeztető szándékos jogellenes magatartások és az azokkal szemben alkalmazott védelmi erőforrások együtthatása határoz meg." [14]

A fogalom meghatározásából egyértelműen azonosítható az összefüggés a biztonság, mint állapot és az azt létrehozó védelmi intézkedésekkel kapcsolatban. A két fogalom egymással dinamikus egységben lévő aktív rendszert képez, ahol a védelmi megoldások kialakításánál kiemelt figyelmet kell fordítani a technológiai fejlődésre reagálni képes tartalékok képzésére, adott esetben a fejlesztéseket biztosító implementációk előzetes beépítésére. Ennek a kölcsönhatásnak az alapjául szolgáló fogalmat és annak létrejöttéből kialakult állapotot a következő módon összegezte Egon Bahr[13] német biztonságpolitikai szakértő: *„A biztonság a múltban abszolút, a jelenben relatív, a jövőben kiszámíthatatlan."*. A három idősíkhoz külön-külön kapcsolódó állapothatározó jól szemlélteti a biztonság viszonylagosságát az idézett mondatban is. Abszolút biztonságról kizárólag múlt időben beszélhetünk, amikor is kétséget kizáróan megállapíthatjuk az összes ismert kockázati tényező ellenére, hogy nem történt „támadás". Az információvédelemhez kapcsolódóan ez akár éveket jelenhet, és akkor is csak vélelmezhető, hogy nem történt információszivárgás.

A robbantás elleni-, információvédelmi szempontoknak - általam kiemelten kezelendő fenyegetettség - is megfelelő védelmi rendszer kialakításához, a bemutatásra kerülő területek együttes megléte szükséges a relatív biztonság eléréséhez.

A következő pontokban ismertetem a létesítménybiztosításhoz kapcsolódó védelmi rendszerek kiépítése során kiemelt figyelmet igénylő főbb pontokat.

1.5.1 Építőipari beruházások védelme

A biztonságtechnikai rendszerek kiépítésének igénye fő szabály szerint a kiemelten védett létesítmények esetében, már a tervezési fázisban megfogalmazódik. A védendő objektum

[13] Egon Bahr (1922-2015.) német újságíró, politikus, író, német gazdasági együttműködés miniszter 1974-1976.

tervezett helye és a körülötte található épített környezet már önmagában meghatározó lehet a különböző védőtávolságok és a fizikai megközelíthetőség szempontjai szerint.
A kiépítésre kerülő védelmi berendezések paraméterezését jellemzően az objektum funkciója és ezzel szoros összefüggésben a várható kockázati tényezők befolyásolják. A tervezés során külön figyelmet kell fordítani a biztonsági rendszerek azon részére, amelyeket az építkezés megkezdésétől kezdve kell működtetni, és ez által folyamatosan kontroll alatt tartva a teljes kivitelezésig az ott folyó munkálatokat. [15]
Normál esetben egy nagyobb volumenű építkezés védelme érdekében kiépített biztonságtechnikai rendszer fő feladataként, az építési területre történő be-, kiléptetés kontrolljaként definiálható. Az építőanyagok beszállítása és az egyéb anyagmozgatások mellett, a személyforgalom (területen dolgozók) kezelése, megfelelő módon való dokumentálása. Ez a feladat már önmagában egy viszonylag bonyolult védelmi rendszer telepítését igényli, a meghatározott biztonsági szint elérése érdekében. Tekintettel a védendő értékek változatosságára és mennyiségére, meglehetősen nagy terhet ró az építkezések biztosításában résztvevőkre. A biztosítás alatt jelen megfogalmazásomban, a védelmi berendezések és intézkedések összességét értem. Ezekben a folyamatokban jelentős szerep hárul a biztonságtechnikai rendszeren belül az úgynevezett humán faktorra. Az eredményesség szempontjából meghatározó lehet az őrzésben részvevők előképzettsége, valamint folyamatos képzése. [16]
Az általam vizsgált veszélyeztetettség szempontjából elengedhetetlen a szakképzett személyzet által végzett kontroll tevékenység. Ez magába foglalja a földmunkákhoz kapcsolódó szakaszos tűzszerészeti átvizsgálásokat, valamint az épületszerkezeti kialakításoknál, bizonyos időközönként a robbanóanyag detektálást. Az építkezés utolsó fázisában – jellemzően a belsőépítészeti kialakítások végzésekor – nagyon fontos a visszatérő jelleggel végrehajtott tűzszerészeti ellenőrzés.
A védendő épületek felújításakor, átalakításakor szintén megfelelő hangsúlyt kell fektetni a folyamatos, szakképzett személyzet általi kontroll megvalósítására. Az ilyen esetekben fokozottabb figyelmet illeti elsősorban a lehallgatás elleni védelmi intézkedéseket, valamint átvizsgálásokat, de ennek ellenére nem szabad elhanyagolni az improvizált robbanószerkezetek okozta fenyegetettséget sem.
Az építkezésre vonatkozó MABISZ előírások, valamint ezen időszakra kiadott működési biztonsági szabályzatban foglaltak vizsgálata nem tartozik a kutatásom területéhez, ezért ezek konkrét tartalmára kizárólag a védelemmel összefüggésben teszek említést.

1.5.2 Fizikai védelem

Az információvédelem szempontjából a 90/2010. Kormányrendelet[14] alapján kell az objektumokban kialakítani a minősített adatok kezeléséhez szükséges helyiségeket és egyéb védelmi megoldásokat. A rendelet V. és VI. Fejezetében kerültek meghatározásra a fizikai biztonságra vonatkozó előírások, amelyek a különböző minősítésű adatokkal történő munkavégzés helyszíneire fogalmazza meg a kialakítások technikai feltételeit. A biztonsági rendszer megvalósításának alapelve, hogy egymásra épülő elemekből kell összeállítani, amely külső-, közbenső-, és belső részekből áll. A hármas tagozódás külső elemét a védendő terület határainak biztosítását ellátó technikai megoldások jelentik. A különböző paraméterekkel rendelkező falazat, födém és padlózat mellett, kiegészítő rácsszerkezetek kerülnek elhelyezésre a nyílászárók esetében. Minden egyes szerkezeti elemre vonatkozóan külön mechanikai, statikai és biztonságtechnikai paraméterek lettek meghatározva, amelyekkel az adott termékeknek vagy építőelemeknek rendelkezniük kell. Különböző vastagságú téglafalazattal egyenértékű szilárdságú térelválasztó és térelhatároló elemeket írnak elő, a minősített adat fokozatától függően a helyiségek kialakítása során. Ugyanezen kategóriák határozzák meg a biztonsági ajtók, rácsszerkezetek áttörésgátlását vagy az ablakok áttörésbiztos fokozatát.

Az ismertetett fizikai jellemzők elsősorban a minősített adatokhoz való közvetlen hozzáférést hivatottak megakadályozni, adott esetben gátolni, de a robbantás-, és lehallgatás elleni védelemben csak közvetetten játszanak szerepet. Az objektumon belül a védett zónák kialakítása és azok kategóriákba sorolása a hozzájuk tartozó belépési jogosultságokkal, nagymértékben elősegítik a hatékony védekezést az IED-k és egyéb információszivárgást lehetővé tevő eszközök bejuttatásának lehetősége ellen.

A kormányrendelet külön fejezetben foglalkozik az úgynevezett személyi feltételekkel, amelyek elsősorban a védendő adatokkal dolgozókra vonatkozó előírásokat tartalmazza. Az alkalmazottak számára személyi biztonsági tanúsítványt kell kiállítani, amely lehetővé teszi részükre a minősített adatok jogszabályi keretek közötti megismerését és kezelését. Ezt a folyamatot a védelmi rendszeren belül egyfajta szűrőnek tekinthetjük, ami elengedhetetlen az esetleges személyi kockázatok előzetes felderítésében. A korábban bemutatott fejezetben az építőipari beruházások esetében is javasolt az előzetes szűréseket elvégezni kiterjesztetten, a munkálatokban részvevő dolgozókra is.

[14] 90/2010. (III. 26.) Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről

A fizikai védelem részét képező, az épületek megközelítését megakadályozó, a szerkezetét megerősítő építészeti megoldásokat jelen dolgozatomban nem vizsgálom.
A következő részben a fizikai védelem kiegészítésére alkalmazott technikai rendszerek ismertetésére kerül sor a kutatási célomhoz igazodva, hogy azok milyen hatással vannak az információvédelemre és a robbantás elleni védelemre együttesen. A cél érdekében milyen jellegű változtatásokra, illetve kiegészítésekre van szükség ezeken a területeken.

1.5.3 Elektronikai védelem

A kormányrendeletben meghatározott elemeken felül, mint a cím is jelzi, az elektronikai védelem egy speciális szempontból történő használatát ismertetem. A kutatásomhoz kapcsolódó területként kiterjesztett módon kezelem, nem csak a biztonságtechnikai értelemben ide tartozó rendszereket vizsgálom, hanem a beléptetéshez közvetlenül kapcsolódó berendezések információ-, robbantás elleni védelmével összefüggésben, azok hatékonyságát is.
A kiindulási feltételek között meghatározó szerepet játszanak napjaink elektromos és elektronikus berendezései, valamint ezek rendszerei. A védett környezet kialakítása érdekében, a védelmi rendszerünk rendelkezésre álló detektáló képességeit, kivétel nélkül ki kell terjeszteni az objektumba bekerülő összes elektronikai szerkezetre, függetlenül azok alkalmazási jellegétől. Enélkül nem lehet garantálni az épület robbantás elleni és információvédelmi biztonságát a kívánt szinten. A feladat végrehajtása meglehetősen összetett ellenőrzési és szervezési tevékenységet foglal magába a beléptetési rendszer működtetése és a biztonsági átvizsgálások összehangolása területén.
A tűzjelző rendszerek részletes bemutatásától eltekintek, a teljesség igénye nélkül azokat csak felületesen, a kutatásomhoz közvetetten kapcsolódó szempontok szerint elemzem.

1.5.3.1 Behatolásjelző-, beléptető rendszer

A biztonságtechnika területén jól ismert rendszerek az objektumvédelem egyik alapvető elektronikai védelmi alrendszerét képezik, melyeknek elsődleges feladata az illetéktelen behatolás, jogosulatlan jelenlét, továbbá az épületszerkezetek megbontásának észlelése és jelzése. A rendszer jellemzően különböző érzékelők – mozgásérzékelők, infravörös sorompók, nyitás- és törésérzékelők – úgynevezett strukturális hálózatából, valamint a hozzájuk kapcsolódó egyéb jelző- és vezérlőegységekből áll.
A biztonságtechnika klasszikus értelmezésében a behatolásjelző rendszer funkciója elsősorban a fizikai védelem támogatására, annak kiegészítésére korlátozódik. A kutatásom szempontjából azonban indokolt ezen rendszerek kiterjesztett szerepének

vizsgálata, különös tekintettel a robbantás elleni védelem és az információvédelem területére gyakorolt közvetlen és közvetett hatásaikra.

A behatolásjelző rendszer szerepe elsősorban a felderítés és megelőzés fázisában releváns, mivel az improvizált robbanóeszköz közvetlenül a célterületre történő bejuttatása és elhelyezését követően, a lehető legrövidebb időn belüli reagálással biztosíthatja a hatékony védelmet. Ennek megfelelően gyakorlatilag az előkészítő cselekmények időbeni felismerésében nyújt, hatható segítséget számunkra. A mozgásérzékelők és infrakapuk által biztosított védendő terület, amely különböző zónákra osztva és közvetlen felügyelettel ellátva képes garantálni, hogy a nem rendeltetésszerű használat, vagy az adott térrészen való jogosulatlan, illetve munkaidőn kívüli mozgást, a megszokottól eltérő tevékenységek azonosítását időben észlelhessük. A zónák megfelelő kialakításával, különösen azon térrészekre, ahol az improvizált robbanóeszközök elhelyezése potenciálisan megvalósítható, kiemelt figyelmet fordíthatunk.

A nyitás-, és törésérzékelők különösen fontos szerepet kapnak a komplex védelmi rendszer kialakításában az által, hogy jelzik az épületszerkezetek, különböző burkolatok (álmennyezet, álpadló) továbbá a vízszintes vagy függőleges úgynevezett strangok megbontását, megnyitását. Ezek a helyek különösen alkalmasak lehetnek a rejtett megfigyelő eszközök vagy IED-k elhelyezésére, ezért kiemelt figyelmet kell fordítani a megközelítésük időbeni észlelésére.

Az információvédelem szempontjából a behatolásjelző rendszer szerepe elsősorban a rejtett lehallgató berendezések elhelyezésének vagy telepítésének, továbbá az ilyen jellegű tevékenység előkészítésére irányuló tevékenységek időbeni feltárásában nyújthat megfelelő segítséget. Az IED-k esetében a korai felismerésben nyújtott segítséghez hasonlóan, az információvédelem területén is alkalmazható az épületszerkezetek, burkolatok védelmén túl, az elektromos hálózathoz vagy az adatátviteli infrastruktúrához való hozzáférés, illetve a védett helyiségben történő jogosulatlan tartózkodás detektálására. A rendszer biztosította eseményrögzítés kiindulási pontnak tekinthető a kiemelten védett objektumok időszakos technikai átvizsgálásához, az esetleges kockázatok lehetőségének korai felismerésére. Az információvédelmi incidensek, adatszivárgások megakadályozása szempontjából különösen fontos a rögzített adatok hatékony értelmezése, mivel a tényleges károkozás és az információszerző tevékenység felismerése között akár jelentős késedelem (látencia) állhat fenn.

A behatolásjelző rendszerek az információvédelem és a robbantás elleni védelem területén azt kiegészítő, egyfajta megelőző támogató egységként és nem önálló védelmi eszközként járulnak hozzá a kiemelten védett objektumok biztonságához.
Az objektumokba történő belépéshez közvetlenül kapcsolódó biztonsági tevékenység kiemelt részét képező az úgynevezett átvizsgáláshoz köthető detektor berendezéseket ismertetem a kutatásom témaköréhez igazítva. Itt a csomagröntgenek, robbanóanyag detektor-, fémdetektor-, félvezetődetektor-, mikrohullám-tartományú kapuk szerepét említem, amelyekkel közvetlenül vagy adott esetben alkatrészek formájában lehetünk képesek felismerni a kockázatot jelentő eszközöket. Ezen a ponton jutnak leginkább szerephez a működtetést végző személyzet képzettsége, gyakorlata és a munkáját közvetlenül segítő speciális szoftverek vagy a napjainkban egyre inkább elterjedő mesterséges intelligencia alapú megoldások. Ez meglehetősen összetett és bonyolult feladatot jelent a beléptetést végző személyzet számára, ezért szükséges a naprakész oktatási anyagok és a folyamatos képzések biztosítása. A beléptetési vagy adott esetben a beszállítási pontokon kell a felsorolt detektor berendezésekkel beazonosítani a potenciálisan veszélyt jelentő eszközöket, illetve azok összetevő alkatrészeit. Ebben az esetben elengedhetetlen a célzatos elektronikai-, elektrotechnikai és katonai ismertetekben való jártasság megléte a hatékony munkavégzéshez. Jelenleg ezen a ponton van a legnagyobb bizonytalanság a rendszerben, mivel a humán faktor okozza a detektálási láncban a hiba jelentős részét. A kiértékelő-, és feldolgozó szoftverek jelenthetik a hatékonyság növelését, valamit a folyamatos továbbképzések és az ismeretek naprakész szinten tartása együttesen garantálhatja kockázatok csökkentését.

1.5.3.2 Videotechnikai rendszer (kamera, hőkamera)

Az objektumvédelemhez tartozó elektronikai védelem területén a videotechnikai rendszerek jelentik az úgynevezett eseménykövető és bizonyítási funkciót ellátó dokumentáló egységét. Elsődleges rendeltetésük az objektum területén belüli, valamint a közvetlen közelében zajló események vizuális megfigyelése, ellenőrzése, továbbá a rendellenességekhez kapcsolódó döntéstámogatás biztosítása. A rendszer tipikusan fix és mozgatható (PTZ[15]) kamerákból és hozzá kapcsolódó képfeldolgozó egységekből tevődik össze, valamint ezek közvetlen részét képező megjelenítést és elemzést végző szoftveres környezetből.

[15] Pan-Tilt-Zoom – forgatás, döntés, nagyítás

A kutatásom szempontjából azt vizsgáltam, hogy a videotechnikai rendszer milyen mértékben járul hozzá a robbantás elleni védelemhez, valamint az információvédelmi fenyegetések kezeléséhez, a komplex biztonsági rendszer részeként alkalmazva.
A bűnös célú robbantásos cselekmények előkészítése során számos olyan tevékenységi elem jelenik meg az előkészületek során, amelyek jó eséllyel vizuálisan érzékelhetők. A kamerarendszerek ezért jelentős szerepet töltenek be az ilyen jellegű cselekmények időbeni felismerésében, az ezekhez köthető gyanús magatartásformák dokumentálásában. A kamerarendszerek alkalmazása lehető teszi számunkra a védett objektum területén a szokatlan mozgások és viselkedési minták azonosítását, a csomagok, illetve egyéb tárgyak felügyelet nélküli hátrahagyásának észlelését. A kialakított zónahálózat kiegészítésére, az ott telepített mozgásérzékelő egységek jelzéseinek pontos értelmezéséhez nyújtanak hathatós és gyors segítséget. A korlátozott látási viszonyok között a hőkamerák jelentenek pontosabb és értékelhetőbb képet az adott térrészekről vagy adott esetben a felügyelet nélküli tárgyakról. A tárgyak hőképén látható disszipált hő jelenléte akár figyelmeztető, pozitív jelzés is lehet az őrség számára.
Az információvédelmi incidensek szempontjából a telepített kamerarendszerek elsősorban a rejtett eszközök telepítésével, karbantartásával vagy kivonásával kapcsolatban szolgáltathatnak információt. Tehát a megelőzés és az utólagos rekonstruálhatóság szempontjából tölthetnek be kiemelt szerepet. További lehetőséget biztosítanak a védett helyiségekhez kapcsolódó hozzáférések folyamatos felügyeletére, a jogosulatlan belépések azonosítására, az adott területen végzett tevékenységek utólagos elemzésére. A korábban említett technikai ellenőrzések végrehajtásának időszerűségében is fontos szerepet játszik a kamerarendszer által detektál jogosulatlan vagy ellenőrizetlen jelenlétek száma, az adott objektumrészre vonatkozólag. Egy esetleges információvédelmi incidenst követően a rejtett lehallgató-, megfigyelő eszköz felkutatásában, az elkövető személyének azonosításában jelenhet segítséget.

1.5.3.3 Tűzjelző rendszer

Az elektronikus tűzjelző rendszert a kutatásom témáját figyelembe véve a komplex biztonsági rendszer részeként, de elsősorban biztonságtechnikai összetevőként kezeltem, amely közvetlenül nem kapcsolódik az általam vizsgált területekhez. A védett objektumok vonatkozásában egy esetleges támadás vagy bombafenyegetéshez kapcsolódó épületkiürítés során kezelhetjük kockázatként a tűzjelző rendszer szabotálását egy provokált működtetés következtében. A kiemelten védett létesítmények esetében a

rendelkezésre álló reagáló személyzet, illetve a kiépített videotechnikai rendszer következtében a korábban említett kockázat mértéke nagymértékben csökkenthető, a gyakorlatban elhanyagolható.

A tűzjelző rendszerrel kapcsolatban egyetlen aspektusból kell behatóbban foglalkozni, amennyiben vezetéknélküli rendszerösszetevőt tartalmaz pl.: 433MHz vagy 868MHz működési frekvenciájú elemeket. Adott esetben a detektálás során jelenthet „hamis pozitív" jelzést, de erre a 3. fejezetben részletesen kitérek.

1.5.4 Információvédelem

Az információvédelem szempontjából a korábban ismertetett elektronikai rendszerek a mai gyakorlat szerint attól elkülönült területként szerepelnek, melyek elsősorban a beléptetésben vagy az objektumon belüli jogosultágok kezelésében segítik a védelem munkáját. A kiemelten védett objektumok információvédelmi követelményrendszere Magyarországon két fő jogszabályi rendszerhez kapcsolódik, egyrészt a nemzeti minősített adat védelméről szóló szabályozás (minősített adat védelméről szóló törvény, a továbbiakban: Mavtv.), másrészt a nemzetközi kötelezettséghez, így kiemelten a NATO/EU-besorolású információk védelméhez tartozó biztonsági irányelvek. Az információvédelemhez közvetlenül kapcsolódó jogszabályi háttérből kizárólag a lehallgatás elleni védelemre utaló részekre koncentrálok, a minősített adatkezeléssel és tárolással csak említés szintjén foglalkozom, azok nem képezik a kutatásom közvetlen területét. Az említett jogszabályokban egyetlen fogalom szerepel a védett tárgyalások helyszínét biztosító épületrészekre: „lehallgatásmentes". Ez önmagában elég tágan értelmezhető keretrendszert jelent, viszont technikai szempontból megközelítve, meglehetősen bonyolult védelmi megoldások kiépítését követeli meg. A fogalom a biztonságtechnika és a védelem szempontjából jogi-technikai értelemben nem abszolút állapotot, hanem kockázatcsökkentett, meghatározott követelményeknek megfelelő védelmi szintet jelöl. Ez az állapot a biztonság szempontjából relatív fogalom, mivel a rejtett információszerzési tevékenységhez egy meglehetősen dinamikusan fejlődő infokommunikációs háttér is kapcsolódik, és nem utolsó sorban az ilyen jellegű cselekmények következménye sok esetben látenciában marad. Azaz jellemzően nincs közvetlen visszajelzés rejtett lehallgatóeszköz használatáról, úgynevezett információszivárgási csatornák megjelenéséről. A gyakorlati szempontból való megközelítése a védendő információ kijutásának lehetőségével összefüggésben, elkülöníthetünk aktív-, és passzív információszivárgási csatornákat. A két mód

elhatárolásának a feltétele, hogy az „aktív” jelző konkrét információszerző tevékenység céljából, hozzá kapcsolódó lehallgató-, megfigyelő eszköz alkalmazását feltételezi. A másik kategóriába elsődlegesen az úgynevezett kompromittáló kisugárzásokat sorolhatjuk, amelyek alapvetően nem megfelelő működtetés, működés vagy felhasználás következtében teszik lehetővé az információ kijutását a védett térrészről.

A klasszikus értelemben vett információvédelem azon részét, amely a kutatásom fő területét képezi, elsősorban a technikai védelmi megoldások jelentik. Itt külön -külön elemzem a védelem passzív és aktív összetevőit annak érdekében, hogy jobban áttekinthető legyen a közvetlen kapcsolat a két terület fontosságát illetően a komplex védelmi rendszer kialakítása során.

1.5.4.1 RF (rádiófrekvencia) védelem

A rádiófrekvenciás szempontból két nagy területre lehet osztani a védelmi megoldásokat, amelyek elsősorban a rádióhullámok terjedésével vagy adott esetben annak csillapításával, valamit érzékelésével összefüggő tevékenységek a módjukból adódóan aktív vagy passzív jellegűek.

Az aktív védelmi megoldások egyik kiemelt részét képezi, az általam vizsgált rádiófrekvenciás-monitor rendszer, amelynek részletes bemutatására a III. Fejezetben kerül sor. Az RF-monitor rendszer fontos kiegészítésének tekinthető - annak szerves részét képező - úgynevezett technikai átvizsgálások (TSCM[16]), amelyek meghatározott rendszerességgel kerülnek végrehajtásra a védett objektum kijelölt helyiségeiben.

Kvázi aktív védelmi megoldásnak tekinthetjük a rádiófrekvenciás zavarásokat is, amelyek további két alterületre bonthatók, a hangtartományban végrehajtott általában fehérzaj jellegű jelek sugárzására és a vezeték nélküli kommunikáció csatornáinak a blokkolására, amit a köznyelv jammelésnek (JAMMER[17]) nevez. Ezek a technikai megoldások az improvizált robbanóeszközök elleni harcból kerültek át az információvédelmi tevékenységhez, véleményem szerint vitatható a hatékonyságuk ezen a területen.

A következő résznek a passzív védelmi megoldásokat tekinthetjük, amelyek elsősorban a fizikai hatásukból adódóan jelentenek segítséget a megfelelő biztonsági szint elérése érdekében. Ezen fizikai hatások közül a csillapítás az egyik legjelentősebb következménye a megfelelő építőanyagok alkalmazásának és a célirányos szakszerű

[16] Technical Surveillance Counter Measures – technikai elhárítás
[17] JAMMER – rádiófrekvenciás zavaró eszköz

kivitelezésnek az építés vagy átalakítás során. Ezen munkafolyamatok során, minden részletére kiterjedően folyamatos és közvetlen felügyeletet kell biztosítani az előre „megtelepítések” elkerülése végett.
Fontos megjegyezni, hogy a lehallgatás elleni védelem alapkövét jelenti egy jól definiált rádiófrekvenciás spektrum figyelő rendszer, a megfelelően módon kialakított helyiséggel, a hozzá kapcsolódó passzív és aktív védelmi megoldásokkal együtt.

1.5.4.2 Félvezetődetektor-rendszerek

Alapvetően a különböző rezsim szabályok és előírások annyit érnek, amennyit önként betartanak belőlük az emberek, illetve képesek vagyunk betartatni velük. A kiemelten védett objektumok esetében is fel kell készülni. az ilyen jellegű mulasztásokra, és ezzel szemben a védekezés egyik leghatékonyabb eszköze a felderítést tekintve, a félvezetődetektor rendszer (NLJD[18]). Legfőbb jellemzője ennek a rendszernek, hogy az esetlegesen inaktív lehallgató berendezéseket is képes detektálni, ami megkönnyíti a védett térrészbe történő eszközbejuttatás felderítését a beléptetések során.

1.5.4.3 Kitekintés

A védett objektumok ellen elkövetett támadások között szerepelnek a lehallgatásokhoz, illetve a robbantásos merényletekhez kapcsolódó események, amelyek közül szeretném kiemelni az Egyesült Államok moszkvai nagykövetség épületének a visszabontását (1982) és a brüsszeli Justus Lipsiusban (Európai Tanács épülete 2002-2017) talált lehallgatóberendezések eseteit.
A ’80-as évek elején a hidegháborút követő időszakban kezdték Moszkvában építeni az új amerikai nagykövetség épületét egy előzetesen megkötött viszonossági szerződés keretében. Kezdetben nem fektettek túl nagy hangsúlyt az építkezéssel összefüggésben az információvédelemre. A gyakorlatban ez azt jelentette, hogy helyi munkaerővel és ott gyártott építőelemekkel dolgoztak, minimális felügyelet mellett. A tervezett befejezést megelőzően az amerikaiaknak időközben a tudomására jutott, hogy az épület számos helyen megtelepítésre került a KGB által. Ennek következtében az utólagos vizsgálatok kimutatták, hogy szinte nem volt olyan építőeleme, illetve helyisége az objektumnak, ami ne lett volna „bepoloskázva”. Ezen körülmények következtében az építkezést leállították és a nagykövetség épülete közel 20 évig befejezetlen maradt. Végül a „Top Hat” – projekt keretein belül a központi épület utolsó két szintjét visszabontották és a maradék hat

[18] Non-Linear Junction Detector – félvezető detektor

emeletre még újabb négy szintet emelve fejezték be az építményt, saját munkaerővel és anyagokból. [17]

A második eset az Európai Unió egyik meghatározó központi épületéhez kapcsolódik, amely funkcióját tekintve az Európai Tanács tevékenységének adott otthont 2017-ig. Az EU Minisztertanácsának épületében több vezető európai országot érintően találtak professzionális lehallgatóberendezéseket. A szakértői vizsgálatok nem tudták egyértelműen meghatározni, hogy „Kihez?" köthetők az információszerző eszközök, de egy olyan vélemény is napvilágot látott, amely szerint az objektum építésekor kerülhettek telepítésre az adott helyiségekbe. További információk szivárogtak ki azzal kapcsolatban, hogy az épület telefonvonalait is lehallgatták. Az említett incidensekre egy rutinszerű technikai átvizsgálás során derült fény. [12]

Mindkét eset jól példázza, hogy az információvédelem ezen területén - a kiemelten védett objektumok tekintetében - elengedhetetlen a folyamatos felügyelet biztosítása az építési-, és átalakítási munkálatok összes fázisában a hasonló helyzetek elkerülése végett.

1.6 Következtetések

A kutatásom alapjául szolgáló objektumok esetében azok védelmi funkcióját tekinthetjük a legfontosabb szempontnak, az ehhez szükséges kritériumoknak teljes egészében meg kell, hogy feleljen a telepíteni kívánt biztonságtechnikai rendszerünk. A feladat maradéktalanul történő végrehajtásához, már a tervezési fázisban együtt kell dolgozni a biztonságtechnikai-, építészeti-, és építő szakembereknek, mivel kizárólag ezen területek összehangolt együttműködésével valósítható meg a komplex védelmi rendszer.

A feldolgozott incidenseken felül, a kormányzati objektumokat ért robbantással való fenyegetésekhez viszonyítva hatványozott számban fordultak elő hasonló cselekmények az iskolák, repülő-járatok, bevásárló központok, vasútállomások ellen szerte a világban, amelyek kisebb nagyobb mértékben bénították meg a mindennapi életet, és ezzel nem kevés anyagi és egyéb terhet róva a hatóságokra, illetve a lakosságra.

A defenzív védelem megvalósításának szükségessége elengedhetetlen, amely különösen igaz az épületen belüli - mint zárt térben bekövetkező robbanás pusztító következményeit figyelembe véve - mert ennek kivédésére tervezett megoldások hatásfoka, nagyon sok tényező együttes hatásától függ. Emiatt az objektumok védelmi rendszereinek egyik kiemelt feladataként, minden esetben meg kell tudni előznie vagy akadályoznia, hogy az épület belső tereiben tudjanak rejtett robbanószerkezetet elhelyezni.

Az információszerzéshez kapcsolódó lehallgatás elleni védelem kialakítása, a másik megoldandó fő feladatunk a kiemelten védett objektumok esetében, mivel a következmények késleltetett vagy bizonyos helyzetekben látens tulajdonsága miatt, csak valós időben tudunk ellene megfelelő hatékonysággal küzdeni.
E két fő feladat hatékony megvalósítása érdekében, elengedhetetlen a kiemelten védett objektumok biztonsági rendszereként, egy rádiófrekvenciás monitor hálózatot telepíteni a védendő épületbe. A történelemből hozott példák alapján, a VIP objektumok építése-, felújítása-, valamint az említett RF monitor rendszer kialakításának, illetve az építési munkálatainak teljes időtartama alatt szükséges a kontroll fenntartása. A problémafeltáró diagramból jól kivehető a megoldandó feladat összetettsége, és a résztvevő elemek egymásra hatása, továbbá csak az együttes jelenlétük képes garantálni a kitűzött célt. A humán faktor szakmai felkészültsége ugyanúgy nélkülözhetetlen a rendszer működtetéséhez, mint a legmodernebb technológia megléte.

A komplex védelmi rendszer kialakítása és az összetevő elemeinek megfelelő módon való összehangolása szükséges a kiemelten védett objektumok széleskörű biztonságának megvalósítása érdekében. A védelmi rendszer technikai összetevőit bemutatva egyértelművé válik, hogy az egymással összefüggésben lévő biztonsági berendezések működtetésért felelős kollégáknak meghatározó szerepe van a megelőzés szempontjából, a szaktudásuk, tapasztalatuk, továbbá a hatékony együttműködésük által.
A „lehallgatásmentes” környezet megvalósítása a kiemelten védett objektumok esetében a bemutatott védelmi mechanizmusok és rendszerösszetevők kiépítése által - azok eredményeként - tekinthető a fogalom egzakt módon meghatározottnak. Ezek alapján a következő módon fogalmazhatjuk meg az elérendő célunkat:

Akkor tekinthetünk „lehallgatásmentes” -nek egy tárgyalót-, helyiséget-, vagy adott esetben objektumot, ha - az üzemeltetési állapotát is figyelembe véve - a minősített vagy érzékeny információ jogosulatlan megszerzésének kockázata a szervezeti-, fizikai-, elektronikai-, és eljárásrendi védelmi intézkedések együttes alkalmazásával, igazolható módon csökkentett. Továbbá a folyamatos kontroll és felügyelet, valamint az időszakos validációs mechanizmusok biztosítottak, annak az állapotnak a fenntartása érdekében.

Az I. fejezethez kapcsolódó forráselemzés 2025. augusztusában zárult le.

A kutatási célkitűzéseim közül az I-es számú hipotézist fejtettem ki ebben a fejezetben.

A fejezethez kapcsolódó eredményeket a következőkben felsorolt publikációimban osztottam meg:

- A kiemelten védett objektumok biztonsága a fenyegetettség tükrében [HADMÉRNÖK, XII. Évfolyam 3. szám – 2017. szeptember]
- Építőipari beruházások biztosítása, kiemelten védett objektumok esetén, különös tekintettel a fenyegetettségre [Műszaki Katonai Közlöny, XXVIII. évfolyam, 2018. 3. szám]

2 TERRORISTA CÉLBÓL ALKALMAZOTT IMPROVIZÁLT ROBBANÓESZKÖZÖK

A szakirodalomban az aszimmetrikus hadviselés egyik leghatékonyabb elemeként említik az improvizált robbanószerkezetek alkalmazását a polgári-, és természetesen a háborús környezetben egyaránt. A bűnös célú robbantások során szinte minden esetben a médiának meghatározó szerepe van az események bemutatásában és nemkülönben a kommentálásában. A terrorizmus alapcéljának tekintett félelemkeltés a lakosság és bizonyos helyzetekben a katonaság legszélesebb köreiben, a sajtón keresztül valósítható meg a leghatékonyabban. A folyamat gyorsaságát fokozzák napjaink infokommunikációs rendszerei, ugyanis manapság szinte mindenki rendelkezik kamerás mobiltelefonnal, amely lehetőséget biztosít akár valós időben tájékoztatni az eseményekről, illetve azok következményeiről. A polgári életben és természetesen a kiemelten védett objektumok esetében is, a legsúlyosabb támadásnak tekinthetjük a terror jellegű cselekményeket, azon belül is a robbantással elkövetett merényleteket. Az ilyen típusú objektumok elleni sikeres támadások nemcsak fizikai károkat okoznak, hanem súlyosan sértik az állam működőképességébe és a biztonságba vetett bizalmat is. Alapvetően egyetlen incidens is elegendő lehet ahhoz, hogy stratégiai döntéshozatali mechanizmusokat bénítson meg, vagy akár társadalmi destabilizációs folyamatokat indítson el az állami intézmény elleni támadás végrehajtása következtében. A kockázat mértékét nagy arányban növeli, hogy az elkövetők célja az esetek jelentős részében nem kizárólag a pusztítás, hanem jóval inkább a pszichikai hatás elérése, vagyis a félelemkeltés a lehető legszélesebb körben és ezekkel egyidőben természetesen a legnagyobb médiafigyelem kiváltása.

Az objektumvédelem területén ezért komoly figyelmet kell fordítani a robbantás elleni védelemre, ami magába foglalja az épületek detonációval szembeni állékonyságát, valamint a repeszvédelmet is. A statikai és mechanikai védelmi megoldásokon mellet, a leglényegesebb szempontnak viszont a robbanószerkezetek épületbe történő bejuttatásának a megakadályozását kell tekinteni. Ennek a folyamatnak az első lépcsőfoka a beléptetési pontokon történő személy- és csomagátvizsgálás, illetve az áruszállításra használt teherportán történő rakomány ellenőrzése. Az alapos és kontrollált beléptetési folyamat ellenére szükséges a rendszeres objektumon belüli átvizsgálás végzése előre meghatározott szempontok szerint, valamint a rádióspektrum folyamatos ellenőrzése.

A hipotéziseim közül a második és harmadik témakörre vonatkozó megállapításaim ebben a fejezetben kerülnek kidolgozásra.

2.1 A terrorcselekmény fogalma

Az objektumvédelem speciális területét illetően, a kiemelten védett objektumokhoz közvetlenül kapcsolódó jogi következményeket ismertetem, amelyek elsősorban az improvizált robbanóanyagok bűnös célból történő alkalmazásaihoz vagy annak használatának a fenyegetésével társulnak. A robbanóanyagok terrorista jellegű felhasználása a közvetlen fizikai hatásokon túlmenően - kormányzati épületeket érintően - előre megjósolhatatlan következményekkel bírnak.

A Btk. 314. §-ba ütköző terrorcselekmény közvetlen jogi tárgya az államok, az állami szervek, nemzetközi szervezetek kényszermentes cselekvőségéhez fűződő társadalmi érdek, valamint a lakosság háborítatlan életfeltételei, továbbá a személyek szabadsága és az anyagi javak sértetlensége biztosítása. [18]

A bűncselekménynek öt alapesete van, melyek különböző elkövetési magatartásokkal valósíthatók meg.

Az első alapesetet megvalósító elkövetési magatartások azonosak a Btk. 314. § (4) bekezdésében meghatározott bűncselekmények – többek között a közérdekű üzem működésének megzavarása – elkövetési magatartásaival. Ezek a lényegében eszköz jellegű bűncselekmények akkor válnak terrorcselekménnyé, ha ún. terrorista célzatúak lesznek. [18]

Ez a célzat az, amely a terrorcselekményt többek között a közérdekű üzem működésének megzavarásától elhatárolja, ezért az alaki halmazatuk csupán látszólagos. A lehetséges célzatok a következők: állami szerv, más állam vagy nemzetközi szervezet arra kényszerítése, hogy valamit tegyen, ne tegyen, vagy eltűrjön, lakosságot megfélemlítse, más állam alkotmányos, társadalmi vagy gazdasági rendjét megváltoztassa vagy megzavarja, illetve nemzetközi szervezet működését megzavarja. [18]

A Btk. 316. §-ba ütköző alapeset a terrorcselekmény elkövetésével való fenyegetés is. Idetartozik minden olyan tevékenység, amelynek révén az elkövető azt a szándékát juttatja kifejezésre, hogy terrorcselekményt kíván megvalósítani. Mindig támadó jellegű, az elkövető a megfenyegetettet a saját akaratát kiszolgáló eszközzé kívánja tenni akként, hogy annak más választása ne legyen, mint az elkövető akaratának feltétlen teljesítése. [18]

Tekintettel a cselekmény következményeire a terrorizmust, mint elkövetési magatartást a világ minden táján elítélik és a legszigorúbb módon büntetik. Hatása jellemzően túlnyúlik a tényleges cselekményén, ami elsősorban a félelemkeltésen keresztül valósul meg.
A Btk. adott szakaszaiban megfogalmazott célok elérése érdekében az improvizált robbanószerkezetek meglehetősen hatékony eszköznek tekinthetők, mivel sok esetben a közvetlen hatásuk sem jósolható, nem beszélve az egyéb következményeiről.

2.1.1 Az IED-k történeti fejlődése és terrorista célú alkalmazása

Az improvizált robbanóeszközök fejlődéstörténete szorosan összefonódik a gerillahadviselés, a politikai erőszak, és a terrorizmus modern formáinak kialakulásával. Az IED-k olyan nem konvencionális fegyverek, amelyek elsődlegesen nem a reguláris erők arzenáljában jelentek meg, hanem a gyengébb technikai vagy katonai kapacitásokkal rendelkező csoportok eszköztárát gazdagították, lehetővé téve a szimmetrikus erőviszonyok megbontását.
Az IED-k fejlődését vizsgálva megállapítható, hogy azok gyakorlatilag a lőpor, majd azt követően a robbanóanyagok kifejlesztésével, szinte egy időben jelentek meg. Az első ilyen jellegű alkalmazásról a Jin dinasztia[19] idején keletkezett legenda, egy bizonyos Iron Li nevű rókavadász módszerét említi, amelyben már megjelenik a kemény burkolat (porcelán) is, kifejezetten a támadás eredményességének fokozása céljából. [18] A történelem során a későbbiekben is többször előkerülnek jellemzően az uralkodók elleni robbantásos merényletek alkalmával. Az első, technikai szempontból is modernnek nevezett változatok a II. világháborúban jelentek meg.
A 20. század második felében az IED-ek alkalmazása főként az európai szeparatista és nemzeti-felszabadító mozgalmak által terjedt el. Az Észak-Írországban működő Irish Republican Army[20] (IRA) az 1970-es évektől kezdve rendszeresen alkalmazott időzített vagy rádió-távirányítású robbanószerkezeteket a brit katonai és rendőri járművek ellen, valamint politikai célpontok megsemmisítésére. Az európai országok esetében a legjelentősebb szerep az IRA-nak mondható, amelynek 1970-től 2005-ig tartó aktív időszakában, mindösszesen 19000 improvizált robbanószerkezettel elkövetett cselekmény tulajdonítható. Ők kezdték alkalmazni a hosszú idejű késleltetésű indítási módokat, ezt a módszert vetették be a brightoni Grand Hotelben, amelyet 3 hetes

[19] i.sz. 265-420 - Acosta, Oscar. "American Firearms Gun History"
[20] Irish Republican Army – Ír Köztársaásgi Hadsereg

időzítéssel hoztak működésbe a brit miniszterelnök ellen. A szerkezet érdekessége volt, hogy egy videórögzítő időzítő egységét használták fel a robbanás idejének a beállítására. A terrorszervezet fő startégiája között szerepelt, hogy a merényletek során a lehető legkevesebb vétlen civil, illetve saját embere sérüljön vagy haljon meg. Ezért a lehető legpontosabb működtetési módokat kezdték alkalmazni, mint a távvezérelt vagy különböző elektronikus szerkezeteket. Ők vetették be először a mobiltelefonos indítási módot, amelyet később feladtak, mert megbízhatatlannak tartottak. Az IRA meghatározó volt a robbantások elkövetésének taktikai kidolgozásában, majd a megszerzett tapasztalatokat megosztotta több terrorszervezetnek is (ETA[21], PLO[22],FARC[23]), képzés keretein belül. Ennek hatására a későbbiekben megjelentek az IRA által korábban alkalmazott IED szerkezeti kialakítások, mint például a vakuáramkörrel indított detonáció, 2005-ben Baszrában brit katonák ellen követtek el robbantásos merényletet. A ’90-es évek elején kezdte el alkalmazni az ammónium-nitrát alapú robbanóanyagokat, amelyeket később a közel-keleti háborúkban az al-Kaida is rendszeresen használt

Hasonló módszereket alkalmazott a spanyolországi ETA, amely a baszk függetlenségi törekvések nyomán hajtott végre robbantásos merényleteket, többnyire járműbe rejtett bombák formájában.

A terrorszervezetekkel összefüggésben nem szabad megfeledkezni a nemzetközi kapcsolataik következtében jelentkező tapasztalatmegosztásról sem, ami elsődlegesen kiképzési tevékenység formájában vagy akár konkrét merényletek elkövetésében jelentek meg. Ennek a folyamatnak az eredményeként az IRA kiképzői a palesztin terrorszervezet tagjait is képezte, így a Hamász és a Palesztin Iszlám Dzsihád az 1980-as évektől kezdve egyre komplexebb robbanóeszközöket fejlesztettek ki az izraeli katonai járművek, határőrégi ellenőrzõpontok és polgári létesítmények ellen. Ezek a tapasztalatok jelentős mértékben hozzájárultak az IED-taktikák professzionalizálódásához, amelyeket később transznacionális kapcsolatrendszerek és kiképzőtáborok által továbbadtak más fegyveres csoportoknak is. [19]

A 2000-es évek elején bekövetkező afganisztáni és iraki intervenciók katalizálták az IED-ek robbanásszerű elterjedését. A helyi gerillacsoportok, mint a talibánok vagy az Al-Kaida Irakban (később az Iszlám Állam elődje), gyorsan adaptálták a technikát,

[21] Euskadi ta Askatasuna
[22] Palestine Liberation Organization
[23] Fuerzas Armadas Revolucionarias de Colombia

közönséges alkatrészekből – gázpalack, műholdas telefon, RC-jeladó, infrakapcsoló – építettek komoly pusztítóerővel rendelkező robbanószerkezeteket. Az európai terrorszervezetek által korábban használt tudást és technikákat sok esetben az áttelepült, radikalizálódott volt harcosok és oktatók juttatták el a közel-keleti hadszínterekre, ahol kiképzőtáborokban rendszerszintű oktatás folyt. [20] Az iraki, majd azt követően az afganisztáni hadszíntereken egyre elterjedtebben kezdték alkalmazni a különféle elektronikus vezérlésű pokolgépeket. Jól megfigyelhető a háborús övezetekben az a fajta dinamikus kölcsönhatás, amely az improvizált robbanóeszközök újonnan megjelenő változatai és az azokra kifejlesztett taktikai elemek között található. Ebben az akció-reakció elveit követő folyamatban a szerkezeti kialakítások sok esetben az aktuálisan alkalmazott tűzszerész tevékenységet is figyelembe véve lettek megkonstruálva. A hatástalanítási metódus részeként alkalmazott jammer-ek kiiktatására kezdték átalakítani a táv vezérelt IED-ket, amelynek eredményeként megjelentek a spider-ek. Az RC-IED[24] vevőegységét távolabb helyezték el a robbanószerkezettől, általában vezetékes megoldással (néhány 10m-es távolság). Ez az „elhúzás” biztosította pokolgép számára, hogy a hatástalanítást végző tűzszerész által működtetett zavaró berendezés ne tudja megakadályozni a robbantást.

Az egyszerűbb kialakítású elektromos indítású szerkezetek esetén is megjelentek az élesítő kapcsolók, a véletlen elműködtetés megakadályozására, a táv vezérelt IED-nél ezt a funkciót jellemzően DTMF[25] kódolással valósították meg, mivel ez a technika használható volt már az analóg kézirádiók esetén is.

Ezt követően világszerte a különböző terrorszervezeteken kívül, már a magányos elkövetők is elkezdték előszeretettel alkalmazni a megfelelő hatékonysága miatt, a saját céljaik elérése végett. Az elmúlt időszakban a legtöbb esetben a megszálló katonai erők ellenében, vagy az országukban regnáló politikai hatalom, illetve kormány befolyásolására hajtottak végre robbantásos merényleteket.

A kutatásom céljául választott témakör az objektumvédelem meglehetősen összetett rendszerén belül, annak egy nagyon speciális részét érinti, ahol az improvizált robbanóeszközök esetleges felbukkanásának kockázatával kiemelten kell foglalkozni.

[24] Radio Controlled Improvised Explosive Device – rádióvezérlésű improvizált robbanószerkezet

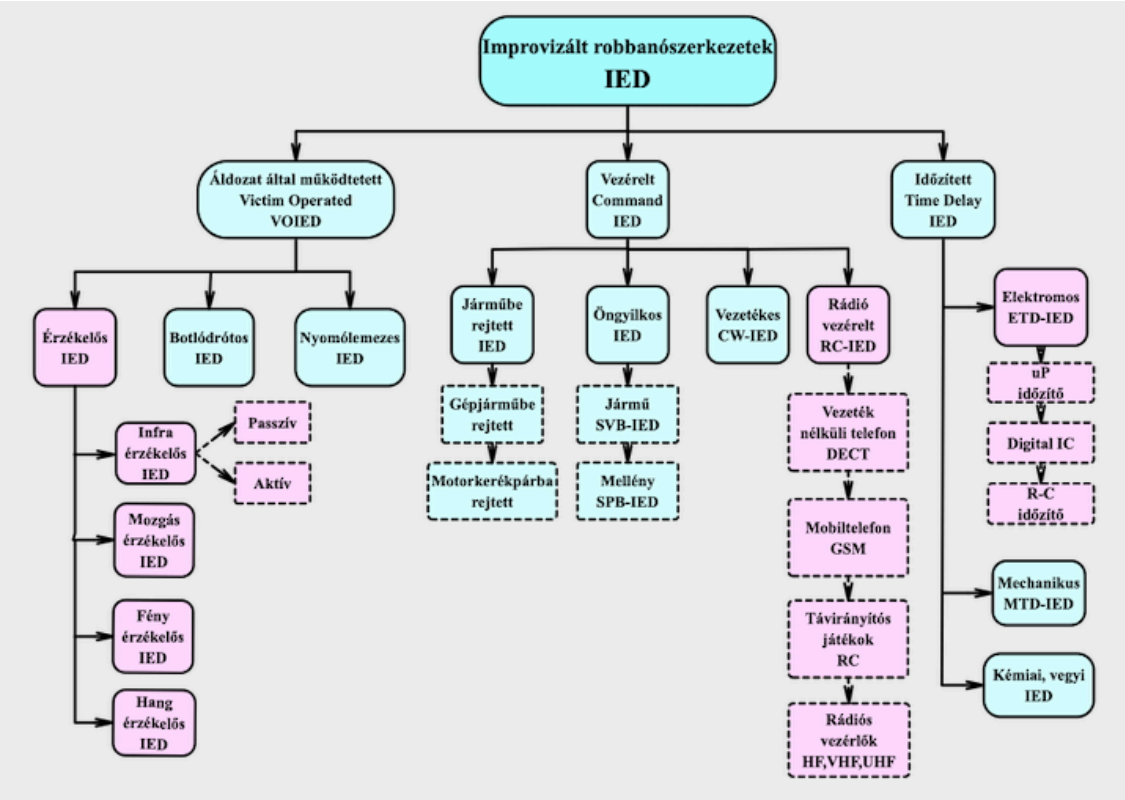
[25] Dual-Tone Multi-Frequency - kéthangú többfrekvenciás jelzés

A következő pontokban röviden összefoglalom az IED felépítését, azok főbb részeit, kihangsúlyozva azon tulajdonságaikat, amelyek lehetővé teszik vagy növelik az időben történő megtalálás esélyét.

2.2 Improvizált robbanóeszközök főbb jellemzői

Az emberi elme nyújtotta variációs lehetőségek tárháza gyakorlatilag végtelennek tekinthető az IED-k megjelenése és az alkalmazott robbanóanyagok kombinációjában. Alapvetően a pokolgépek kialakítása nagyban függ a készítő technikai felkészültségtől, műszaki ismereteitől, az elérhető alkatrészektől, a rendelkezésre álló robbanószerektől és nem utolsó sorban magától az alkalmazás jellegétől. Ezek együttesen fogják meghatározni az improvizált robbanószerkezetek felépítését és a működtetés módját.
A következő pontokban sorra veszem az általános felépítésből kiindulva az elektronikus indítású IED-k főbb szerkezeti egységeit - kiemelve azon típusokat - amelyek alkalmazása jellemzően az urbanizációs környezetben valószínűsíthető.
Kitekintésként szeretném ismertetni az Egyesült Nemzetek Aknaellenes Szolgálatának (UNMAS[26]) az improvizált robbanószerkezetekről szóló lexikonja alapján, az IED-k indítási módjait összefoglaló egyszerűsített struktúráját. A szemléltetés célja, hogy kiemeljem a különböző típusú működtetések esetében, mindegyik robbanószerkezetben megtalálhatók az elektronikus elven üzemelő részegységek.

[26] United Nations Mine Action Service



3. ábra IED-k működtetés szerinti csoportosítása[27]

Az ábrán rózsaszínnel jelöltem azokat az indítási módokat, amelyeknél egyértelműen található olyan elektronikai alkatrész az IED működtető egységében, amely lehetővé teszi számunkra az elektromágneses sugárzáson keresztüli detektálás lehetőségét.

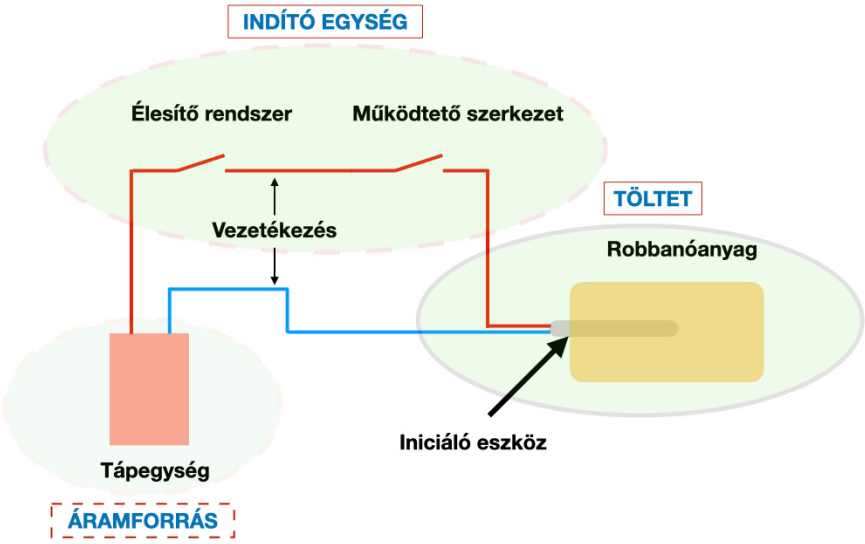
A nevezett kategóriából elsődlegesen az úgynevezett elektronikus és vezeték nélküli indítási módokat ismertetem. Ezek közül is jellemzően, mint legelterjedtebben alkalmazott eljárásokat a rádiófrekvenciás vezérléseket emelem ki. A távvezérelt kategóriába sorolhatók az optikai összeköttetéseken alapuló távirányítók is, mint például a különböző infrás játékok vagy maga a TV távirányítására szolgáló eszközök. Az improvizált robbanószerkezetek között mégsem terjedt el, valószínűleg a IR vezérlés hatósugara miatt, amely a megfelelő működés feltételeként optikai rálátást és maximum néhány 10 m-es távolságot képes áthidalni. Ettől függetlenül nem szabad figyelmen kívül hagyni, mint lehetséges megoldási módot.

2.2.1 IED-k általános felépítése

A következő ábrán az elektromos IED-k általános felépítését ismertetem, amelyek főbb egységei jellemzően mindig megtalálhatóak a robbanószerkezetekben. A klasszikus improvizált robbanóeszközök legfőbb egységei:

[27] United Nations Mine Action Service - Improvised Explosive Device Lexicon (pp. 20-22.) alapján

- áramforrás;
- indító-, működtető egység;
- töltet (adott esetben iniciáló egység)
- burkolat vagy repeszképző anyag.



4. ábra Improvizált robbanószerkezet elvi felépítése

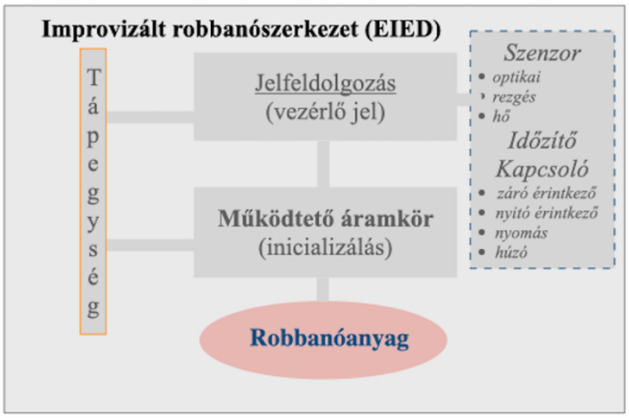
Az ismertetett felépítést figyelembe véve, a kutatásom elsődlegesen az IED-k működtetéséhez kapcsolódó részegységeit érintette, különös tekintettel azok kialakítására szolgáló elemeire, amelyek nagymértékben hozzájárulhatnak a megfelelő időben történő felfedésükhöz.

A következőkben röviden bemutatom az elektronikus indítású improvizált robbanóeszközök elvi felépítését, különös tekintettel azon alkatrészeire, amelyek lehetővé teszik a működtetést megelőző detektálás lehetőségét.

2.2.1.1 Elektronikai indítású improvizált robbanó eszközök

A 4. ábrán egy elektronikus indítású IED főbb részei - a működés szempontjából lényeges elemeit elkülönítve - a logikai kapcsolatot feltüntetve láthatóak. Az ilyen indítási módú robbanószerkezetek esetében kiemelt figyelmet kell fordítani az egyes összetevők elektronikai tulajdonságaira, azok közvetlen környezetre gyakorolt hatásaira. A bekapcsolt állapotban lévő elektronikai alkatrészek és szerkezeti elemek a működésükből fakadóan bizonyos mennyiségű hőt bocsátanak ki a közvetlen környezetükbe. Ennek a hatásnak a detektálására jellemzően a technikai vagy tűzszerészeti átvizsgálások

alkalmával van lehetőségünk, mivel egy irodai környezetben a folyamatos hőkamerával történő ellenőrzés megvalósítása nem kivitelezhető. Ezért van szükségünk egy olyan 24/7 spektrum-felügyeleti rendszerre, amely viszonylag hatékonyan képes detektálni az objektumon belüli kockázatot jelentő eszközöket. Az elektronikai berendezések által kisugárzott elektromágneses hullámok érzékelésével, és megfelelő módon történő elemzésével, hatékonyan deríthetjük fel a védett térrészekre esetlegesen bekerült elektronikus indítású IED-ket.



5. ábra Elektronikus indítású robbanószerkezet

Az 5.ábrán a részegységek megnevezésével kívánom bemutatni azokat a speciális funkciókat ellátó összetevőket, amelyek külön-külön rájuk jellemző módon „hagynak nyomot" a közvetlen környezetükben.

Jelfeldolgozó áramkör

Az egység fő feladata, hogy a különböző érzékelőktől bejövő jeleket a működtető áramkör számára értelmezhető formátumúra alakítsa. Az „élesítést" követően gyakorlatilag ezek a perifériák (szenzorok) fogják indítani az improvizált robbanószerkezetet.

A szenzorok közül jellemzően azok jöhetnek szóba, amelyek az áldozat vagy a célpont hatására, annak közvetlen közelében valamilyen indító jelet képesek generálni. Ilyen például a passzív vagy aktív infraérzékelők, ezek általában a mozgás hatására aktiválódnak. A különböző fényérzékelők - látható-, és nem látható tartományban működők - az elmozdulás-, és hang érzékelők. Az imént felsoroltak elsődlegesen az áldozat jelenlétéhez, annak közvetlen ráhatására lépnek működésbe. Az aktív infra kapukat általában vizuális módszerekkel van lehetőségünk még detektálni. A háborús

övezetekben a C-IED[28] tevékenységnek köszönhetően, egyre inkább elterjedtek közvetlenül a hatástalanítást végző tűzszerészek elleni szerkezeti megoldások, mint a röntgen vagy a rádiófrekvenciás sugárzásérzékelőkkel „felokosított" pokolgépek. A szenzortechnológia integráltsága miatt, egyre megbízhatóbb működésű vezérléseket lehet összeállítani, az elérhető dokumentációk pedig a kevésbé képzett készítő számára is garantálják a hibamentes áramkörök megépítésének a lehetőségét.

A fentebb ismertetett indítási módok közül az idő késleltetést tekinthetjük a „legpontatlanabb" végrehajtási megoldásnak bizonyos szempontból, mivel a célpont megfelelő közelsége szükséges a detonáció pillanatában, a kívánt hatás elérése érdekében. A kivitelezési megoldások szerint az időzítő áramkör a legkülönfélébb összeállítású lehet. Az egyszerűbb úgynevezett rövid késleltetésű R-C tagokkal megoldott analóg változatoktól kezdve, a digitális technológiából ismert számlálókkal összeállított vagy a napjainkban használt mikrokontrollerekkel megvalósított hosszú idejű „várakozásra" képes típusokig bezárólag. Itt már napok, esetleg hetek vagy akár hónapokról beszélhetünk a tervezett indítási időpontot tekintve. Külön megemlíteném a hétköznapi használati tárgyak nyújtotta lehetőségeket is, mint például a digitális ébresztőórák, háztartási berendezések időmérő egységei vagy akár a mobiltelefon ébresztő funkciója generálta indító jel - kiegészítve néhány alkatrésszel - felhasználása az improvizált robbanószerkezet elműködtetéséhez.

A mozgásérzékelsős szenzorokhoz szorosan kapcsolódó jelenséget sikerült észlelni az IED-k érzékelő egységeinek vizsgálata során, mégpedig egy PIR[29]-rel szerelt improvizált imitációs eszköz mobil röntgenezése alkalmával. Az eszközt egy faládába rejtve próbáltuk felderíteni átvilágítással, ekkor a röntgenimpulzusok hatására működésbe lépett az indító áramkör. A kísérletet egymás után többször is elvágeztük, de egyértelműen nem volt megállapítható, hogy a PIR szenzort vitték-e telítésbe az Rtg. sugarak vagy az elektronikájára voltak hatással.

Működtető áramkör

Az indító vagy más néven működtető rész fő feladata a robbanóanyag detonációjának beindítása. A pokolgép célhelyen való telepítőjét védi az úgynevezett élesítő kapcsoló, ami a véletlen működtetést akadályozza meg, ennek aktiválását követően a vezérlő jel

[28] Counter-Improvised Explosive Device – Improvizált robbanószerkezet elhárítás
[29] passzív infra mozgásérzékelő

hatására a töltet felrobban. Az indítóegység működési mechanizmusa alapján lehet kategorizálni az improvizált robbanóeszközöket.

Hosszú az út a kezdeti kínai, szó szerint úgynevezett „dobós" robbanószerkezetektől, a napjainkban sok esetben a hétköznapi használati eszközeink köréből kikerülő elektronikai berendezésekkel vezérelt IED-k megjelenéséig technikai fejlődés szempontjából is.

A félvezető technológia elterjedésével a szimpla kapcsolós indítási módoktól eltérően, további lehetőségekkel bővült a működtető áramkörök kialakítása, egyfelől a méret szempontjából is jelentős csökkenés tapasztalható. A félvezető alkatrészek további fejlődésével, integráltságuk növekedésével a működési variációk újabb aktiválási módokat biztosítanak a bűnös szerkezetek készítői számára. Megjelennek a mikrokontrollerek, amelyek tovább csökkentik a kiegészítő alkatrészek számát és egyben összetettebb és pontosabb indítási megoldásokat tesznek lehetővé.

A mikrokontrollerek (MCU[30]-k) a modern elektronikai rendszerek alapvető komponensei, amelyek nagyfrekvenciás digitális működésükből adódóan jelentős elektromágneses zavarkibocsátással (EMI[31]) járhatnak. Bár teljesítményük általában alacsony, a gyors kapcsolási tranziensek és a magas integráltság miatt az általuk generált zavarok kritikus hatással lehetnek a környezetükben található elektronikai egységek működésére. [21] Az EMI kialakulásának alapja a digitális kapcsolási folyamatok során fellépő nagy meredekségű feszültség- és áramváltozás (dV/dt és dI/dt). Ezek a tranziensek a parazita induktivitások és kapacitások révén elektromágneses tér kialakulását eredményezik, amely vezetett és sugárzott zavar formájában jelenik meg. [22] A jelenség különösen a közeltérben domináns, ahol az induktív és kapacitív csatolás meghatározó szerepet játszik.

A mikrokontrollerek egyik legjelentősebb zavarforrása a rendszerórajel. Az órajel tipikusan nagyfrekvenciájú, négyszögjel alakú feszültség, amely rendkívül gazdag harmonikus spektrummal rendelkezik. Bár az alapfrekvencia gyakran néhány tíz vagy száz megahertzes tartományba esik, a meredek felfutásiidők következtében a spektrum jelentős komponenseket tartalmaz akár a gigahertzes tartományig is. Az órajel nemcsak a mikrokontroller belső működését határozza meg, hanem a nyomtatott áramköri lapon (PCB[32]) vezetett struktúrák révén sugárzott zavarként is megjelenhet.

Az említett hatásokat kell tudnunk detektálni a technikai átvizsgálásaink során.

[30] Microcontroller Unit - Mikrokontroller
[31] Elektromágneses interferencia
[32] Printed Circuit Board – nyomtatott áramköri lap

Áramforrás

Az elektromos működtetésű IED számára a villamos energiát a tápegység biztosítja. Ez lehet valamilyen villamos hálózatra kapcsolt változattól kezdve, a különböző elektromos töltést tároló képességű berendezésekig bezárólag bármilyen megoldás. A tápegységekkel kapcsolatban a leglényegesebb kritérium, a megfelelő energiatároló képesség az IED élesítésétől kezdve az inicializáláshoz szükséges impulzus leadásáig. Az alkalmazott alkatrészek a következők lehetnek:

- *akkumulátorok*

A gépjárművekben található normál kivitelű akkuktól kezdve az ipari berendezésekben vagy a háztartásokban fellelhető változatokig minden típus előfordulhat, a helyi sajátosságoktól függően. Az alkalmazott fajtát sok esetben a tervezett felhasználás jellege szabja meg, annak rejtési lehetőségei, a töltöttségének megőrzési képessége.

- *elemek*

A normál szárazelemek a féltartós, illetve tartós típusok is előfordulhatnak, a kapocsfeszültségtől függően soros vagy párhuzamos kapcsolással összekötve. A legújabb fejlesztéseknek köszönhetően megjelent a Lítium és az ezüst-oxid mint kapacitástároló anyag, amelynek következtében sokkal nagyobb kapacitású és élettartamú elemek kerültek a kereskedelmi forgalomba.

- *nagy kapacitású kondenzátorok*

Az elektromos töltés megtartásának az ideje miatt, a kondenzátorok önmagukban történő alkalmazásának a lehetősége meglehetősen korlátozott. A II. világháborúban ennek ellenére, a németek már használtak ilyen elven működő légibomba-gyújtókat, illetve mi magyarok is (El. AZ-50-5, 36M, 40M) [23]. Az IED-hez szükséges elektromos energia biztosítására napjainkban a fotótechnikában használatos extranagy kapacitások jöhetnek szóba az alkalmazás szempontjából.

- *induktív berendezések*

Az indukció alapján működő gyújtószerkezetek közös jellemzője, hogy valamilyen mozgási energia - adott esetben egy mozdítás - szükséges az elektromos áram előállításához. A II. világháborúban a szembenálló felek, szinte kivétel nélkül alkalmaztak mágneses indukció elvén működő gyújtókat a légibombákban (38M, AV-524M, e. AZ-66) [23]. Ezek a fluxusváltozásra épülő szerkezetek még a mai napig megőrizték működőképességüket, mivel a bennük található ferromágneses anyagok „öregedése” meglehetősen hosszú folyamat.

A civil területeken alkalmazott IED-k esetén a rendszer bonyolultsága miatt nem preferált technikának számít, de pont a házi készítésű jelleg nem zárja ki adott esetben a megjelenését.

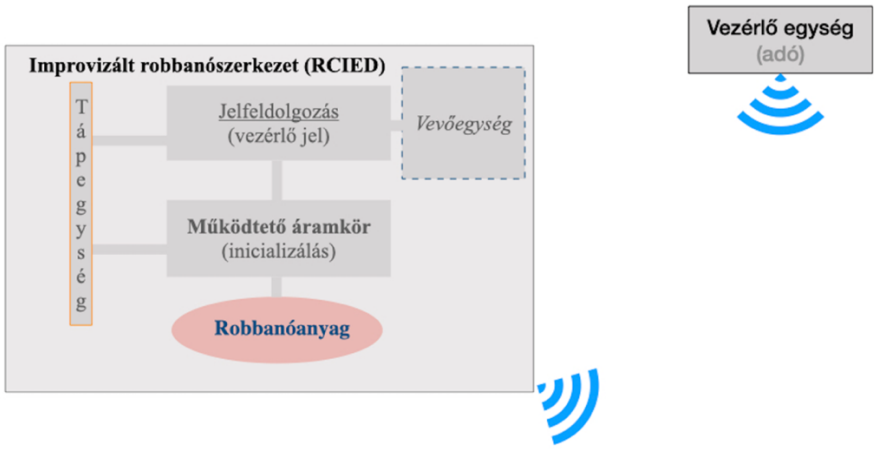
A felsorolt energiatároló egységekhez az esetek többségében különböző feszültségátalakító alkatrészek is társulnak, mivel az elektronikai áramköreink jellemzően eltérő feszültség szinteken üzemelnek, amit kompenzálnunk kell.

A DC–DC konverterek a modern elektronikai rendszerek alapvető energiaátalakító egységei, amelyek különböző feszültségszintek közötti hatékony átalakítást tesznek lehetővé. Működésük kapcsolóüzemű elven alapul, amely magas hatásfokot biztosít, ugyanakkor jelentős elektromágneses zavarforrásként is viselkedhet.

A konverterek működése során a félvezető alapú alkatrészek periodikusan kapcsolnak, amely jelenség hasonlóan a mikrokontrollerekhez, nagy meredekségű feszültség- és áramváltozásokat eredményez. Ezek a tranziensek kölcsönhatásba lépnek az áramkör elkerülhetetlen parazita elemeivel, így az alaplap vezetősávjainak induktivitásával és a csomópontok közötti kapacitásokkal. Ennek következtében nagyfrekvenciás parazita jelek keletkeznek, amelyek a konverter elektromágneses viselkedésének meghatározó tényezői. Az egyik legjelentősebb jelenség a kapcsolási csomópontokon megfigyelhető feszültséglengés (ringing). Ez a jelenség tipikusan a parazita induktivitás és kapacitás által alkotott rezonáns kör eredménye, amely a felfutási él után csillapodó oszcilláció formájában jelenik meg. A lengés frekvenciája és amplitúdója az áramkör fizikai kialakításától függ, és jelentős szélessávú EMI forrást képez. [24]

2.2.1.2 Rádióvezérlésű IED (RCIED) fő részei

A következő ábrán a rádiótávirányítású improvizált robbanószerkezetek elvi felépítését szemléltetem - kiemelve azon fő elemeit - amelyek a működésükből fakadóan egyértelmű jelzéssel szolgálhatnak az átvizsgálások során. Alapvetően az ilyen típusú IED-knél nem a vezetéknélküli kommunikáció érzékelésén alapuló előtalálás lehetőségét vizsgáltam, hanem a működtetést megelőző úgynevezett „rejtett-élesített helyzetű” robbanószerkezetek időbeni detektálását közvetlenül vagy közvetett módon.



6. ábra Rádióvezérlésű robbanószerkezet elvi felépítése

Az elvi ábrán külön jelöltem a távirányításhoz szükséges vevőegységet, amelyre a kutatásom során a legtöbb figyelmet fordítottam. Méréseket végeztem közvetlenül a vevő közelében és attól meghatározott távolságokban, abból a célból, hogy szemléltetni tudjam a környezetünkben található egyéb elektronikai eszközök jelenléte mellett is detektálható a bekapcsolt vevőegység.

A rádiófrekvenciás összeköttetésen alapuló berendezések mindegyike előfordulhat az indítóegység részeként. A VHF[33] és UHF[34] tartományú kézirádiók ugyanúgy, mint a vezeték nélküli asztali telefonok (DECT[35]), kapucsengők vagy a garázskapu nyitók, valamint a gépjárművek riasztóegységei. Megjelentek a távvezérelt relé panelek, amelyek már kész indítási megoldásokat garantálnak.

A távoli indítás kialakításával összefüggésben meg kell említeni a publikus hálózatokat (makró környezet). Azok kiépítettsége a lefedettség megvalósítása, az alkalmazott technológiák, a hálózathoz való hozzáférés lehetősége, mint az előfizetői szabályok, nagy mértékben befolyásolják a mobilhálózat IED-k indítására való felhasználását. Az így megvalósított indítási mód lehetővé teszi akár az internet hálózaton keresztül megfigyelt és végrehajtott merénylet kivitelezését is.

A bemutatott fő részeket megfelelően kialakítva és csatlakoztatva egymáshoz egy valóban hatékony és mérhetetlen pusztító hatású robbanószerkezetet kapunk. Ennek a hatásnak az egyik legmeghatározóbb szempontja az a tény, hogy zárt térben hozzuk lére

[33] Very High Frequency - 30-300MHz frekvencia tartomány (magyar megfelelője URH – ultra rövid hullám)
[34] Ultra High Frequency – 300-3000MHz frekvencia tartomány
[35] Digital Enhanced Cordless Telecommunications - Digitálisan Továbbfejlesztett Vezeték Nélküli Távközlés

a robbanást, amelynek következtében a sérülés és a rombolás mértéke jóval nagyobb, mintha szabad térben következett volna be.

2.3 Detektálás alapelvei

A kutatásom során vizsgált elektronikus indítási módokat az IED-k felderítéséhez kapcsolódóan azért is tartom fontos szempontnak, mivel az urbanizációs környezetben – figyelembe véve az egyéb infokommunikációs technológiákat – elsősorban ilyen típusú improvizált robbanószerkezetek megjelenésére lehet számítani, szemben az egyszerűbb mechanikus kivitelűekkel, mint pl.: a botlódrótos vagy a vegyi késleltetésű megoldások. A detektálások során jellemzően a fizikai-, kémia-, valamint az elektronikai tulajdonságokhoz kapcsolódó vizsgálatokat kell előtérbe helyezni.

Az elektronikus-, és a rádiótávirányítású improvizált robbanóeszközök főbb részegységeinek általános bemutatása mellett, ismertetem a különböző fizikai és kémiai paraméterekhez kapcsolódó detektálási módszereket is.

A rejtett robbanóeszközök felkutatása érdekében a vezetett jelek vizsgálatának a lehetőségét sem szabad kizárni, ugyanis az épületek vezetékhálózata egyfajta antenna rendszernek tekinthető, amely képes lehet a közvetlen közelében elhelyezett rádiós szempontból sugárzó berendezések detektálására.

Az elektromos indítású improvizált robbanószerkezetek működtető köreire alapvetően az jellemző, hogy viszonylag egyszerűbb kialakításúak, amelyek lehetnek egyaránt kereskedelemben elérhető termékek vagy a készítője által megkonstruált áramkörök. Az egyik meghatározó közös tulajdonság bennük a detektálhatóság szempontjából, hogy mindkét konstrukció az esetek többségében nem tartalmaz szűrőket, illetve egyéb parazita sugárzást csökkentő egységeket.

2.3.1 kémiai tulajdonságok alapján működő detekciós megoldások

A robbanóanyagok felkutatásában kiemelkedő jelentőséggel bírnak azok a technológiák, amelyek a vegyületek kémiai tulajdonságaira, különösen az illékony komponensek kipárolgására (volatilizációjára) alapozzák működésüket. A robbanóanyagok – például a trinitro-toluol (TNT), pentaeritrit-tetranitrát (PETN), vagy a ciklonit (RDX) – jellemzően rendkívül alacsony koncentrációban, de mérhetően jelen vannak a környező levegőben, különösen a tárolás, szállítás vagy egy esetleges rejtés során, annak közvetlen közelségében.

A kipárolgáson alapuló detekció lényege, hogy speciális érzékelők (pl. elektronegatív affinitású anyagok, félvezető szenzorok, vagy ionmozgásos spektrométerek – IMS[36]) segítségével azonosítják a robbanóanyag gőzfázisában jelenlévő molekulákat. Az IMS technológia különösen elterjedt a repülőtéri biztonsági rendszerekben, mivel gyors, megbízható és hordozható megoldást kínál. Az érzékelők típusa és szenzitivitása meghatározza a detektálhatóság alsó határát, amely általában a részecskekoncentráció néhány pikogramm/m³ szintjéig is terjedhet. [25]

A lézerfényes vizsgálatok (Laser-Induced Breakdown Spectroscopy – LIBS, valamint a Raman-spektroszkópia) az elmúlt években egyre nagyobb figyelmet kaptak a nem-kontakt, távoli detekciós módszerek körében. A lézerspektroszkópiai eljárások előnye, hogy akár több méteres távolságból is képesek a célanyagon vagy annak környezetében lévő mikroszkopikus maradványok – például robbanóanyag-nyomok – elemzésére. A Raman-spektroszkópia különösen érzékeny a molekulák rezgési módjaira, így a robbanóanyagok egyedi spektroszkópiai „ujjlenyomatát" azonosíthatja. [26]

Az ezen eljárások által nyert adatok mesterséges intelligencia alapú feldolgozása és adatbankhoz való illesztése jelentősen javíthatja a megelőző biztonságtechnikai felderítések hatékonyságát. A beléptetési pontokon történő preventív jellegű alkalmazásukon felül, természetesen a tűzszerészeti átvizsgálásoknál vagy előtalált IED esetében, a feltételezett robbanóanyagok fajtájának meghatározásához nyújthatnak hatékony segítséget.

2.3.1.1 Az IED-k esetében alkalmazott robbanóanyagok

A háborús övezetektől eltérően a normál polgári életben az IED-ben használt robbanóanyagot tekintve a tényleges házi készítés dominál, mivel a katonai robbanó-, szerkezetekhez, szerekhez körülményesebb a hozzáférés. Esetenként mégis előfordul, hogy az elkövetés során szabvány katonai robbanóanyag kerül alkalmazásra, ami általában a szervezett bűnözői körökhöz köthető. Napjaink háborúiban a helyi terrorszervezetek előszeretettel használják fel az UXO[37]-ból kiszerelt nagy hatóerejű katonai robbanóanyagokat. Magyarország esetében a korszerű katonai robbanóanyagok ilyen formájú „beszerzése" csak a közelmúltban lezajlott dél-szláv háborúkhoz volt köthető, viszont a II. Világháborúban fel nem robbant légibombák és tűzérségi lövedékek

[36] Ion mobility spectrometry - ionmozgásos spektrométer
[37] Unexploded ordnance – fel nem robbant bomba

még mindig lehetőséget teremthetnek. A jelenleg zajló orosz-ukrán háború a jövőre nézve további kiemelt kockázatokat jelenthet az illegális robbanóanyagok beszerzését illetően.
A házi készítésű robbanóanyagok közül kiemelném a nemzetközi szakirodalomban a „sátán anyjának" nevezett TATP[38]-t. Ez egy rendkívül instabil, érzékeny és ez által veszélyes anyag, a kísérletezőik közül sokan még az előállítása vagy a szállítása során megsérülnek. Előszeretettel használják a civil területeken elsősorban személyek elleni merényletekhez, a könnyű iniciálhatósága miatt. A detonáció kiváltásához elégséges lehet egy kisméretű villanykörte izzószálának gyújtóhatása vagy külön áramkörrel létrehozott elektromos szikra. A töltet nagysága a merénylet célpontjától és a bombakészítő tapasztalatától függően változhat, de a robbanás mechanizmusából adódóan meglehetősen bonyolult előre pontosan kiszámolni a pusztítás mértékét. A „civil" életben jellemzően a csőbombák tölteteként előszeretettel alkalmazzák a feketelőport, amely a viszonylag könnyű beszerezhetősége és előállíthatósága miatt kedvelt.

2.3.2 Elektromágneses zavarok és összeférhetőség alapjai (EMI[39]-EMC)

A modern elektronikai rendszerek növekvő integráltsága és kapcsolási sebessége miatt az EMI/EMC kérdésköre kiemelt jelentőségűvé vált mind az ipari, és természetesen a fogyasztói alkalmazásokban egyaránt.
EMI-nek tekintünk minden olyan nem kívánt elektromágneses energiát, amely egy elektronikus rendszer működését kedvezőtlenül befolyásolja. Az elektromágneses összeférhetőség ezzel szemben annak képessége, hogy egy berendezés megfelelően működjön saját elektromágneses környezetében anélkül, hogy más rendszereket zavarna. EMI/EMC mérések szerint létezik egy úgynevezett „bűnös" vagy másnéven zavaró jeleket sugárzó áramkör vagy áramköri rész. Az esetek többségében az ilyen típusú részegységek a normál működésük során sugároznak - a közelükben található egyéb berendezések számára - elektromágneses interferenciát okozó rádióhullámokat. [21] Ez a zavaró hatás függhet a jel erősségétől vagy a frekvenciájától, valamint az egymáshoz viszonyított távolságtól. Az ipari gyártástechnológiáknál szabvány írja elő, hogy a különböző elektronikus berendezéseket milyen jellegű vizsgálatoknak kell alávetni annak érdekében, hogy megállapítható legyen az elektromágneses sugárzás-, és azzal szembeni ellenállóképesség mértéke. A vizsgálat során mérik az elektromágneses sugárzást az elektronikai berendezések közvetlen közelében és meghatározott távolságra, egy erre a

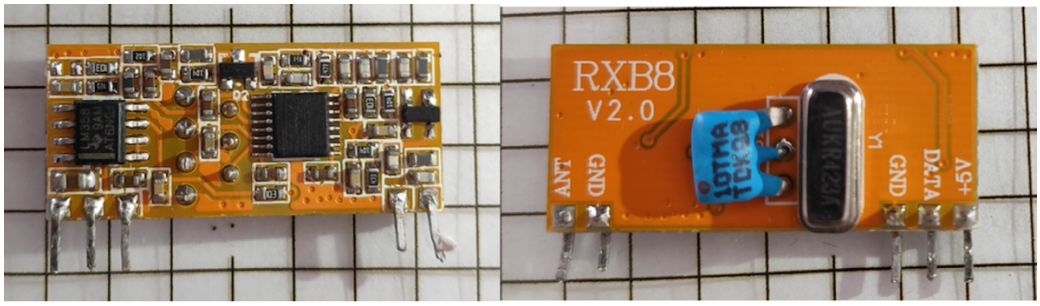
[38] Triaceton-triperoxid
[39] Electromagnetic Interference - elektromágneses zavar

célra kialakított környezetben, a külső zavarok kizárása mellett. Ezeket a speciális helyiségeket nevezzük EMC kamráknak.
Az EMI/EMC összetartozó folyamatnak a vizsgálatára kidolgozott szabványrendszer és vizsgálati módszerekhez kapcsolódó mérési metodikákat tekintem alapjául a kutatásom során az általam választott vevőmodul, vizsgálatai esetében is. Ezen mérések és szimulációk végrehajtása alatt, az elsődleges célom nem a szabvány szerinti megfelelősség vizsgálata, hanem az alapkoncepció bizonyítása, mely szerint az IED-k elektronikus működtető áramkörei elektormágneses sugárzást bocsátanak ki. További kitűzött célom, hogy ezt a jelenséget megfelelő módon szemléltessem.
Ez a tény alapozza meg az elektromágneses sugárzás mérése és elemzése alapján történő detektálás lehetőségét, amely nagy segítséget jelent a technikai átvizsgálások és a tűzszerész ellenőrzések során az objektumvédelem területén.

A következőkben ismertetem a kutatásom alapjául szolgáló vevőmodul főbb tulajdonságait, majd a bemutatott mérésekkel szemléltetem a fentebb felsorolt jelenségeket. Azért választottam az RXB8-as jelű vevőmodult a vizsgálataim alapjául, mert a viszonylag egyszerű felépítése ellenére is tartalmazza azt a fő működési módot megvalósító egységet, amely az ilyen típusú rádiós modulokban kivétel nélkül megtalálható. Napjaink rádiótávirányítású eszközeinek alapjait képezik a hasonló felépítésű vevőegységek, amelyek szinte kivétel nélkül az úgynevezett szabad (ISM[40]) frekvenciasávokban üzemelnek. Ezek az egyszerű rádiós modulok nagysorozatszámú tömeggyártásban készülnek a távol keleten, és látható módon kihagyták a megfelelősségi vizsgálatok közül a fentebb említett EMI méréseket. A könnyen beszerezhetőségük olcsó áruk, nagyban hozzájárult a széles körben való elterjedésükhöz. A robbantásokról készült hazai és külföldi összefoglaló tanulmányokban is hasonló távirányításos berendezésekből, mint pl.: garázskapunyitók, átjelzők, vezetéknélküli kapcsolók kiszerelt rádiós moduljaik kerültek felhasználásra, az indító egységek összeállításánál. Ezért a vizsgálataim alapjául kifejezetten az ilyen típusú vevőegységekre koncentráltam.
A konkrét mérési feladatokat a 433MHz-es RXB8-V2 jelzésű rádiós modulhoz kapcsolódóan végeztem el. Maga az eszköz egy szuperheterodin elven működő rádió vevőegység, ami az amplitúdómodulációhoz tartozó, úgynevezett amplitúdó billentyűzést használja és a hatókörét tekintve, közel 300m-ről képes érzékelni a működtető jelet. A döntésemet, hogy ezt a modult választottam tovább erősítette a detektálással kapcsolatos

[40] Industrial Science Medical – ipari tudományos orvosi (433MHz, 868MHz, 2400MHz, 5400MHz)

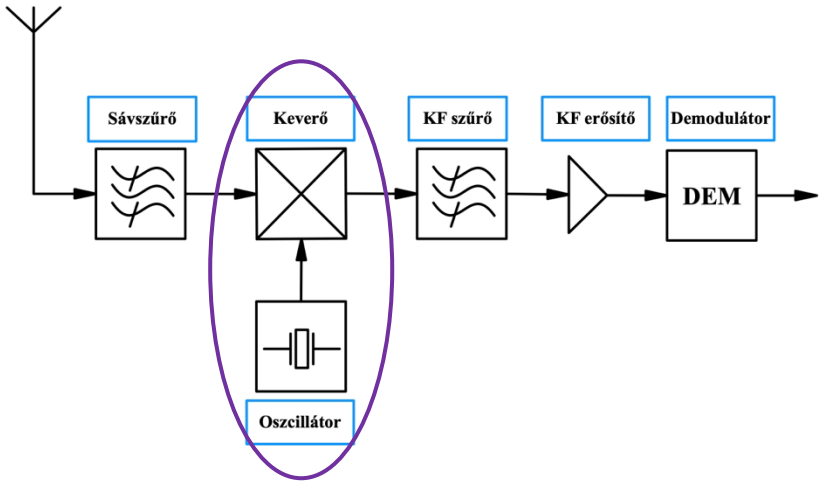
szemléltetés komplexebb lehetősége. Jól beazonosítható magán az eszközön a parazita jelek forrása és távolabbról is hatékonyan detektálható a bekapcsolt állapotú vevő.
A következő ábrán látható a rádiósmodul nagyított fényképe, amely gyakorlatilag ebben a kialakításában néhány kiegészítő alkatrész segítségével, alkalmas lehet egy közel 300m-ről működtethető RC-IED összeállítására.



7. ábra RXB8 vevőmodul

A vevőmodul egy kétoldalas nyomtatott áramköri lapon (NYÁK) felületszerelt módon kialakított áramkör. A NYÁK egyik oldalán a 423MHz-es fémtokozott kristály és egy 10,7MHz-es középfrekvenciás szűrő látható, a szabadon lévő földelt vezetőfóliával. A panel másik oldalán a rádiófrekvenciás jeleket feldolgozó-értelmező áramköri elemek helyezkednek el. Gyakorlatilag a felsorolt alkatrészek együttes egymásra hatása hozza létre az elektromágneses sugárzást az eszköz környezetében.

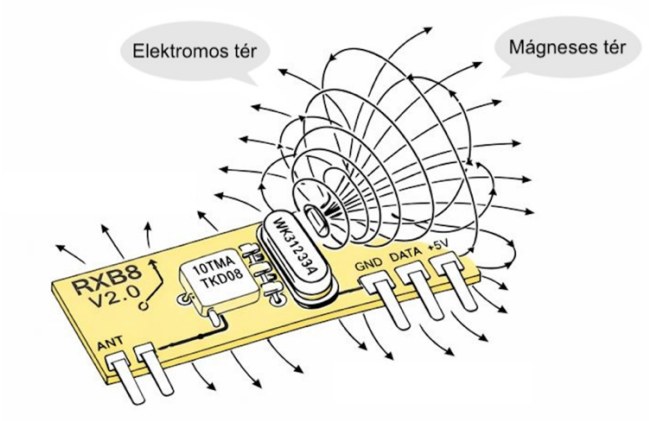
A következő ábrán szemléltetem a vevőmodulok szinte mindegyikében megtalálható elv blokkdiagramját, ez maga szuperheterodin-elv. Működését tekintve ez egy szorzó áramkör, ami tulajdonképpen trigonometrikus függvényeken hajt végre matematikai műveleteket, majd a eredményt formálva kapjuk a kimeneten a demodulált jelet.



8. ábra Szuperheterodin vevő elvi felépítése

A 8-as számú ábrán bekarikázott részt tekinthetjük az áramkör rádiós szempontból a „legaktívabb” helyének, mivel ott a vevőmodul működési frekvenciájához közeli értékű kvarckristályt tartalmazó rezgőkör található. A keverő fokozatban a vivő-, és az oszcillátor frekvenciája kerül összeszorzásra, ez által megjelenik a kettő különbsége is, ami általában a soron következő részegység - középfrekvencia - tartományába eső érték. Ebből adódik, hogy a helyi oszcillátor a venni kívánt frekvencia közeli értékén rezeg (sugároz).

A jelenség szemléltetésére a következő ábra segítségével történik.



9. ábra Áramkörök elektromágneses sugárzása

A 9. számú ábrán látható az áramkör kristályoszcillátorának közvetlen környezetében létrejövő elektromos-, és mágneses terek bemutatása, egymásra merőleges vektorjainak elhelyezkedése a térben. A valóságban természetesen ennél jóval összetettebb a helyzet az erőtereket illetően, ugyanis a kialakulás jellege és a távolság nagyban befolyásolja az elektromágneses hullámok tényleges helyzetét.

A gyakorlati tapasztalat szerint a gyártók törekednek a nemkívánatos, úgynevezett parazita RF összetevők sugárzásának a csökkentésére, de a legnagyobb igyekezetük ellenére mindig mérhető valamilyen szintű jel a távolság függvényében.

A következő pontokban ismertetem a távolság és a hozzá kapcsolódó erőterek értelmezését az EMI/EMC vonatkozásában.

2.3.2.1 Közeltér-távoltér

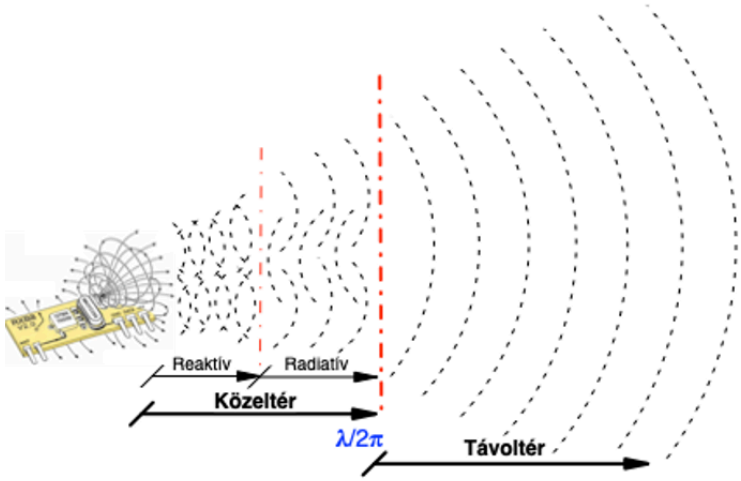
A közeltér-távoltér értelmezésében alapvetően kétféle álláspont létezik a szakmai körökben, én a kutatásomhoz kapcsolódóan az egyszerűsített számítási módot ($\lambda/2\pi$) használtam, mivel számomra elsődlegesen az elv és annak következményeinek az ismertetése a cél.

A közeltér további két részre bonható:

- reaktív (nem-sugárzó) közeltér
- sugárzó (Fresnel) közeltér

A sugárzó antenna (elektromágneses hullámokat kibocsájtó elektronikai alkatrész) közvetlen közelében található az úgynevezett reaktív zóna, amely elsősorban az adott térrészben megjelenő hullámok tulajdonságait határozza meg. Ebben a távolságban az elektromos és mágneses terek nincsenek fázisban és a sok esetben a térerősségük is nagymértékben eltér egymástól.

A következő ábrán látható a közeltér-távoltér szemléltetésre, azon belül is a sugárzási zónák feltételezett határait jelölő EMC szerinti értelmezés.



10. ábra Közeltér-távoltér

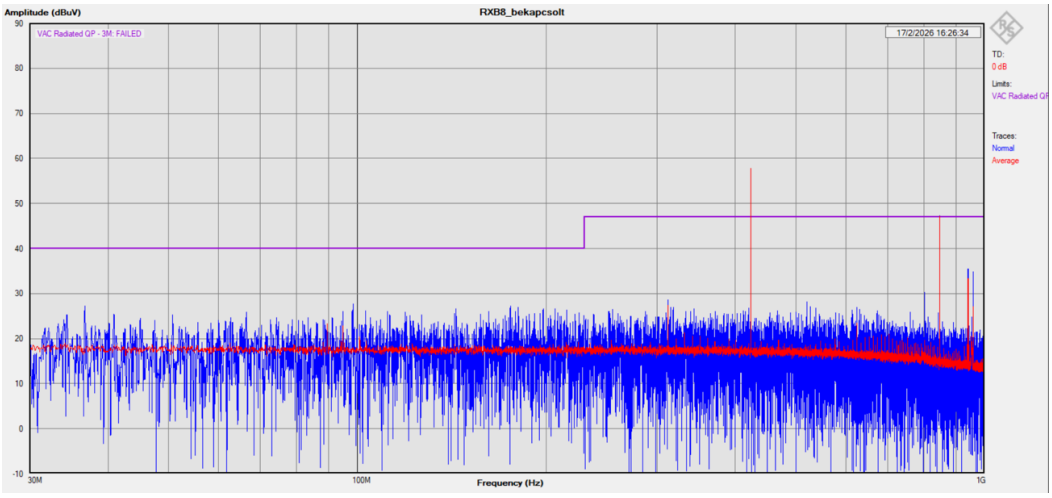
A közel-távoltér elmélete határozza meg, hogy az adott hullámhosszúságú elektromágneses hullámok, milyen módon tudnak kapcsolódni (csatolódni) a környezetükben található egyéb elektronikai alkatrészekhez, valamint a közvetítő közeghez (levegő). Az úgynevezett közeltéri kisugárzást nagyban befolyásolja az elektronikai berendezés felépítése és szerkezete és a közvetlen környezete, valamint annak anyaga, ezek együttesen határozzák meg az elektromágneses hullámok jellemzőit. A hullámforrástól távolodva az egyik legfontosabb tulajdonsága változik meg az elektromágneses sugárzásnak, mégpedig az úgynevezett tér-, jellege alakul át síkhullám formává, amely azután a távolsággal fordított arányban azzal közel négyzetes mértékben csökkenő térerősséget eredményez. [21]

A közeltér-távoltér elmélete mind a kisugárzás és természetesen a hozzákapcsolódó detektálás esetében is meghatározó törvényszerűség. Az elektronikai berendezések, valamint az érzékelő antennák esetében is fontos, hogy milyen frekvenciájú hullámok keletkeznek az adott szerkezet működése során, és azokat a jeleket hogyan tudjuk detektálni.

Az ipari gyakorlatban az EMI/EMC vizsgálatok részeként létezik egy úgynevezett előzetes megfelelősségi mérés (precomplience test), amelynek során közeltéri szondákkal próbálják detektálni az esetlegesen jelen lévő parazita jeleket. A vizsgálandó elektronikai berendezés méreteitől függően, közeltéri szondák (E-, H-mérőfejek) segítségével lehet a sugárzás helyét meghatározni, hogy kiindulásként az adott jel egy konkrét alkatrészből, vezetékből vagy akár több elem egymásra hatásából származik. A mérés alapján lehetséges a sugárzás kiváltó okának a meghatározása is, hogy az gyors feszültség-, vagy áramváltozásból keletkezik.

2.3.2.2 RXB8 modul EMI vizsgálata közeltérben

A következő ábrán egy általam a vevőmodul közelében elvégzett megfelelősségi mérés eredménye látható. A spektrum vizsgálatával azt kívántam bemutatni, hogy a szuperheterodin elvű elektronikai berendezés, milyen parazitajeleket sugároz a közvetlen közelében. A mérés során egy Rohde & Schwarz RTO2024 -es digitális oszcilloszkópot és a hozzákapcsolt HZ-15 közeltéri szondát alkalmaztam. A külső rádióspektrum zavaró hatásának csökkentése végett, a modult a mérőszondával együtt beburkoltam egy szénszálas földelt szövettel. Az árnyékolás hatására gyakorlatilag tisztán a modul által kisugárzott jeleket tudtam detektálni, amelyek jól látható módon, megjelenítésre kerültek a műszer kijelzőjén.

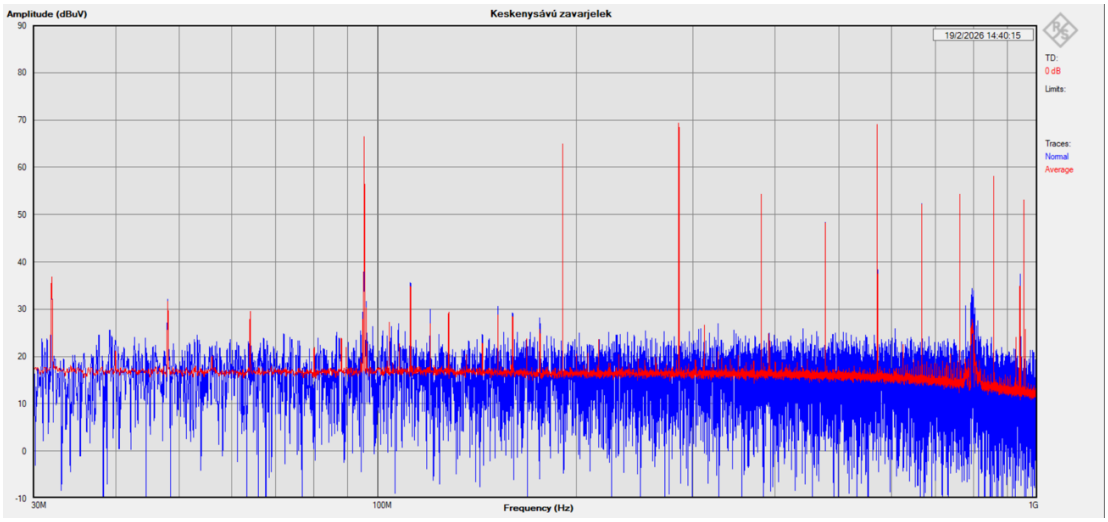


11. ábra Megfelelősségi mérés RTO oszcilloszkóppal

A 11-es számú ábrán az úgynevezett megfelelősségi mérés eredménye, amely szerint két helyen is átlépte a sugárzott frekvencia a beállított küszöbértéket az adott spektrumtartományban. A határérték a műszerben alapbeállításként a 30MHz-1000MHz-ig terjedő sugárzott zavarjelekhez van igazítva, amit ebben az esetben a 423MHz és a 847MHz frekvencia értékeknél az oszcilloszkóp „nem megfelelt” minősítéssel jelzett.
Ez alapján megállapítható, hogy az adott RXB8-as jelű vevőmodul 423MHz-es sugároz a közeltérben (a 847MHz-es összetevő feltételezhetően a sugárzott frekvencia felharmonikusaként jelent meg az éterben).
Az ismertetett mérés során tapasztalt jelenség teszi lehetővé számunkra, hogy valós körülmények során is képesek legyünk detektálni adott esetben egy rádiótávirányítású improvizált robbanószerkezet működtető egységét.
A következő pontokban bemutatom a zavarjelek spektrumban való megjelenésük különböző formáit, a jelek sávszélességekre vonatkozó jellemzőik szerint.

2.3.2.3 Keskenysávú zavarjelek

A keletkezésük elsősorban a digitális áramkörökhöz kapcsolódik, ahol jellemzően diszkrét frekvenciaösszetevőket különböztethetünk meg a spektrumban. Ezek általában az órajelekhez köthető alapharmonikus frekvenciaként és annak különböző felharmonikus elemeiként azonosíthatók, csökkenő amplitúdóval.
A következő ábrán egy keskenysávú zavarjeleket kibocsátó elektronikus áramkör spektrumképe látható.

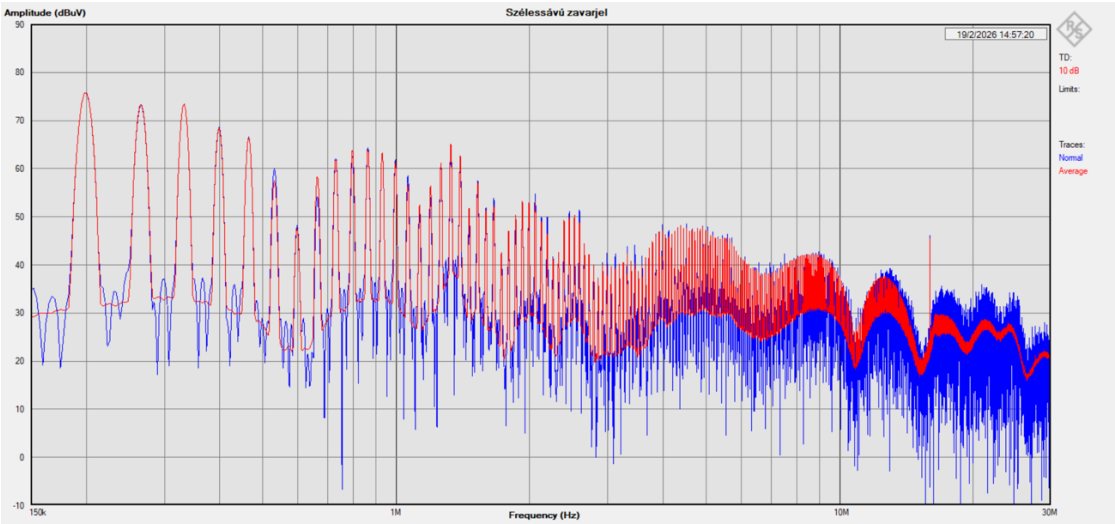


12. ábra Keskenysávú zavarjelek

Az ábrán jól kivehető az úgynevezett „vonalas” spektrum, ami a diszkrét frekvenciaértékek FFT[41]-t követő jellegzetes ismertetőjegye. Az ilyen típusú jelek relatív jól detektálhatóak, nagyszámú mintavételezéssel egyedi azonosításra is lehetőségünk van a kibocsátó eszközre vonatkozólag.

2.3.2.4 Szélessávú zavarjelek

A szélessávú zavarjelek kialakulásának módjai elsősorban a rezonancia jelenséghez köthetők, amely a nagyáramú változások és a digitális áramkörökben létrejövő úgynevezett „csengő” effektus miatt, a spektrumban alakít ki jellegzetes mintákat. További kiváltó hatás lehet még a parazita oszcilláció következtében kialakuló kiszélesedett jelsorozat, amely keletkezésének pontos meghatározására és mérésére kizárólag a közeltérben van mód.



13. ábra Szélessávú zavarjelek spektrumképe

A szélessávú zavarjelek esetében a spektrumkép alapján egyértelműen nem határozhatók meg diszkrét frekvenciaösszetevők, jellemzően széles „hegycsúcs” formájú képek láthatók az adott spektrumtartományban. Egyedi azonosításra csak a spektrum szélesebb tartományban történő értelmezésével lehetséges, kevésbé pontos mértékben, mint a korábban bemutatott diszkrét értékek esetében.

[41] Fast Fourier Transform – gyors Fourier-transzformáció

2.4 Imitációk, bombafenyegetések

A valós IED-k esetleges megjelenése mellett nem szabad megfeledkezni a robbanóanyag nélküli vagy adott esetben csak pirotechnikai elegyet tartalmazó szerkezetekről, az úgynevezett imitációkról. Az ilyen jellegű, robbanószerkezetnek álcázott eszközök, a kiemelten védett objektumok biztonsági rendszereit érintően, hasonló reagálást igényelnek, mint a valós helyzetekben.

Jogi szempontból a cselekmények elhatárolása a konkrét tények és következmények megállapítására az események bekövetkezését követően kerül sor, a robbantással fenyegetés elhangzásakor még nem rendelkezünk mindenre kiterjedő információval. A Büntető Törvénykönyv külön nevesíti a hétköznapi értelemben „bombafenyegetésként" kezelt, általában telefonon közölt fenyegetéseket.

A Btk. 338. §-ba ütköző közveszéllyel fenyegetés közvetlen jogi tárgya a zavart keltő híresztelésektől mentes társadalmi együttélés, a zavartalan köznyugalom. Az követi el, aki a köznyugalom megzavarására alkalmas olyan valótlan tényt állít, híresztel, vagy azt a látszatot kelti, hogy közveszéllyel járó esemény bekövetkezése fenyeget. [27]

A terrorcselekménnyel fenyegetés és a közveszéllyel fenyegetés alaki halmazata kizárt.

A Btk. 316. §-ban meghatározott cselekmény speciális bűncselekmény a 338. §-ban meghatározott közveszéllyel fenyegetés tényállásához képest. Közös vonásuk, hogy mindkettő olyan bűncselekmény elkövetésével fenyeget, amely általában nyugtalanságot kelt, ám ameddig a 338. § szerinti fenyegetés kimondottan közveszéllyel járó esemény bekövetkezését állítja valótlanul, addig a terrorcselekmény kilátásba helyezése magában foglalhatja a közveszély következményét is. Tehát amíg a terrorcselekmény fenyegetés elkövetésénél az elkövető általában nem üres fenyegetést használ, hanem komolyan gondolja annak megvalósítását, addig a közveszéllyel fenyegetés megvalósulása tudatosan valótlan tény állításával történik. [27]

A Kúria Bfv.545/2021/7. számú precedensképes határozata alapján nyilvánvalóan elhatárolja egymástól a két bűncselekményt az, hogy a közveszéllyel fenyegetés elkövetési magatartása a közveszély bekövetkezésének valótlan tényállítása (híresztelése, látszatának keltése). Ehhez képest a terrorcselekmény elkövetésével fenyegetés konkrét, speciális kényszerítési célzatot feltételező fenyegetés. A terhelt a jogesetben nem csupán állította, híresztelte, vagy annak látszatát keltette, hogy (tőle függetlenül) közveszéllyel járó esemény bekövetkezése fenyeget, hanem maga helyezte kilátásba, hogy - követelésének nem teljesítése esetén - azt meg fogja valósítani. [27]

A bűncselekménynek nem tényállási eleme az, hogy az elkövetőnek objektíve lehetősége legyen az általa kilátásba helyezett fenyegetés beváltására. A terrorcselekmény elkövetésével fenyegetés bűntette a Btk. 314. § (4) bekezdésében felsorolt bűncselekménynek a törvényben írt célzattal való kilátásba helyezése esetén csak akkor nem valósulhat meg, ha annak valóra váltása magából fenyegetésből kitűnően objektíve nem lehetséges. A megfenyegetett nem vállalhatja annak kockázatát, hogy az akár valószínűtlennek tűnő, de nem objektíve kizárt fenyegetést figyelmen kívül hagyja vagy további tájékozódástól, későbbi történéstől tegye függővé a reakcióját. Ekként tehát az ilyen - a magából a közlésből kitűnően nem objektíve kizárt - fenyegetés alkalmas a komoly félelem kiváltására és így a terhelt terhére rótt bűncselekmény szükséges tényállási elemének megfelel. [28]

A Kúria döntéséből is egyértelműen látható, hogy az objektíve nem kizárható fenyegetések esetében nincs mérlegelési jogköre a megfenyegetett objektum vezetőjének, mindenképp intézkedésre kötelezett.

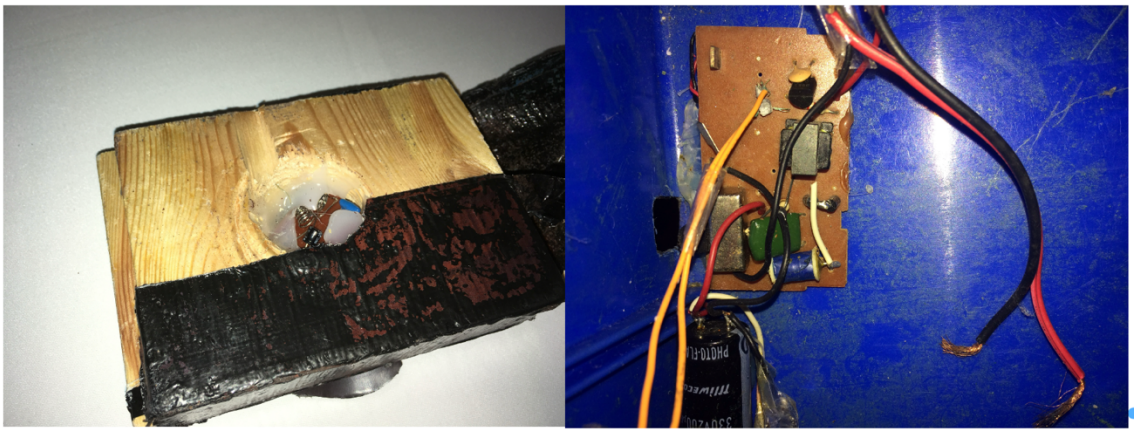
Sok esetben a bombafenyegetések alkalmával történik meg az első tűzszerész jellegű átvizsgálás is az adott objektumban. A megfelelően kialakított komplex védelmi rendszer megléte esetén is, amennyiben sikerül detektálni az adott robbanóeszköznek álcázott szerkezetet a fenyegetést megelőzően, vagy röviddel azt követően, csak teljes vizsgálattal állapítható meg annak imitáció jellege. Ugyanis a működtető részegységek kialakítása és azok környezetre gyakorolt hatása független a tényleges „munkát” végző anyagtól, azaz a robbanóanyag típusától.

Az imitációk kialakításukat tekintve a legkülönfélébbek lehetnek, hasonló módon, mint a valós IED-k, a készítőjének fantáziája, technikai képzettsége és a rendelkezésre álló alapanyagok szabhatnak határt.

Bűnügyi szempontból az imitációk bizonyos helyzetekben egyfajta gyakorló és próbaeszköznek vagy adott esetben prototípusnak tekinthetők, de ennek ellenére a nyomozóhatóságok nem vehetik félvállról az ilyen jellegű eszközökkel „kísérletezgetőket”.

Technikai szempontból az imitációk esetében az RF-tartományban detektált jelek alapján történő elhatárolás lehetősége korlátozott, az IED relatív alkalmassága csak további ellenőrzésekkel igazolható. Ennek ellenére a detektálás szempontjából mindenképp eredményesnek tekinthető a rendszerünk, ha egy relatív alkalmas működtető egységgel szerelt IED-imitációt is képesek vagyunk azonosítani a védett területünkön belül.

A következő kép baloldalán egy tényleges imitáció látható, amelyet egy nemzetközi konferencia alkalmával használtak fel, a biztonsági beléptetéshez kapcsolódó technikai átvizsgálás folyamatának a tesztelésére. A jobb oldalon egy vakuáramkör látható, amelyet egy műanyagdobozba, áramforrással összekötve találtak egy házkutatás során a tetjén egy „Robbanásveszély” matricával.



14. ábra Imitáció vs. relatív alkalmas eszköz

A fa lambéria darabba mart köralakú üregbe, egy régi típusú NYÁK darabkáját, melegragasztóval rögzítették, és ezt az egészet egy szék alján, több rétegben ragasztószalaggal bevonva helyezték el. A műanyagdobozba szerelt vakuáramkör mellet, egy D-típusú elemtartó (4db-os) feltöltött cellákkal, továbbá az áramkör ki volt egészítve egy billenőkapcsolóval is, feltehetően az „élesítő” funkció miatt.

Valójában egyik eszközt sem nevezhetjük tényleges imitációnak, viszont a működőképes vakuáramkör relatív alkalmas működtető-indító egységnek tekinthető, amely képes lehet iniciálni bizonyos érzékenyebb robbanóanyagokat.

A következő pontban az infokommunikációs hálózatok folyamatos fejlődése és a hozzá kapcsolódó úgynevezett okos környezet szenzortechnológiájának rohamos ütemben történő kiépülése okán, szeretném a robbantás-, és lehallgatás elleni védelem számára jelentő kihívásokat röviden összefoglalni.

2.5 Legújabb kori kihívások

Az új trendek a kommunikációs-technológiában átalakítják a hétköznapi életünket, lecserélődnek a korábban megszokott elektronikai berendezéseink és megváltozik a

hozzájuk fűződő kapcsolatunk, minőségben és mennyiségben egyaránt. Az IoT[42]-s technológia megjelenésének hatására a kommunikáció, eszköz és eszköz (M2M[43]) között is zajlik tőlünk függetlenül. Ez a fajta környezeti átalakulás - a használatban való elterjedés - maximum lassítható, de megakadályozni nem lehet. A közvetlen környezetünket gyakorlatilag elárasztják az infokommunikációs berendezések megszámlálhatatlan sokasága. Ennek hatására a rádióspektrum zsúfoltsága kihívások elé állítja a vezetéknélküli eszközök felderítésére szolgáló eszközeinket és rendszereinket egyaránt. További kockázatokat hordoz magába a mindenhol rendelkezésre álló vezetéknélküli hálózatok jelenléte, amelyek közvetlenül is lehetőséget kínálhatnak a távolról történő rejtett megfigyelések-, robbantások elkövetésére.

A smart[44] technológián felül további kihívásokkal kell számolni az objektumvédelem területén, mégpedig az úgynevezett vezető nélküli légijárművek UAV[45]-k elterjedése következtében. A napjainkban zajló háborúk bizonyították a drón-technológia hatékonyságát a hadászat területén, de emellett fokozatosan a hétköznapi életünk részévé is válik, gondoljuk csak a csomagkézbesítés, gyógyszerküldés, vagy akár a személyszállításhoz kapcsolódó kísérletekre. A bűnös célból történő alkalmazásukhoz tartozik a büntetésvégrehajtási intézetekbe való csempész tevékenység vagy esetlegesen a létesítmények, illetve kritikus infrastruktúrák elleni támadások végrehajtása.

Ne feledkezzünk meg a terrorista jellegű támadásokhoz kapcsolódó kockázatokról sem, ugyanis konkrét védett személy elleni alkalmazások is történtek már a világ több pontján is. A venezuelai Maduro elnök ellen 2018-ban, Caracasban két robbanóanyaggal szerelt drónnal hajtottak végre sikertelen merényletet, míg 2019-ben egy jemeni katonai díszszemlén, több magas rangú főtisztet megölve követtek el dróntámadást. [29] [30]

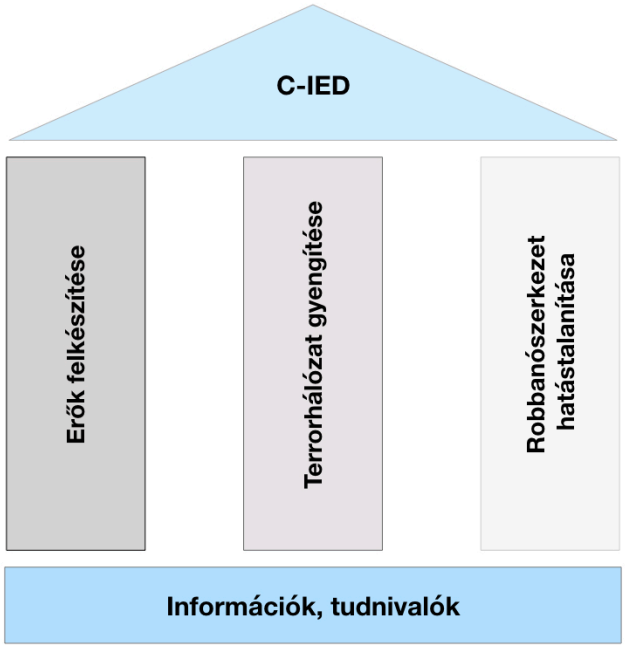
A kutatásomhoz kapcsolódóan a drón-technológiával összefüggésben, nem kívánok részletesebben foglalkozni tekintettel a dolgozatom terjedelmére, a következő fejezetben csak utalok rá a rádiófrekvenciás monitorhálózatok funkciói bemutatása során.

A következő pontban az improvizált robbanóanyagok elleni harc részeként a kutatásomhoz kapcsolódóan, a kiemelten védett objektumok biztonságának növelése érdekében, milyen további intézkedések növelhetik a védelmi szintet.

[42] Internet of Things – internethez kapcsolódó eszközök
[43] Machinet o machine – gép-gép közötti kapcsolat
[44] smart – okos, intelligens
[45] Unmanned Aerial Vehicle – pilóta nélküli légijármű

2.6 C-IED az objektumvédelemhez kapcsolódóan

C-IED NATO alapján szerkesztett védekezési pillérek alkalmazhatóságának a vizsgálata a kiemelten védett objektumok komplex védelmi rendszerei esetében, különös tekintettel a technikai-detektáló berendezések alkalmazhatóságára. Az improvizált robbanóeszközök elleni harc összefoglaló ábrájából – általánosságban – jól láthatóak a főbb elvek, amelyek közül az első és a harmadik pillér, valamit az alapként megjelölt információk kiemelt fontossággal bírnak a kutatásom témáját illetően.



15. ábra Improvizált robbanószerkezetek elleni védelem alappillérei[46]

Az improvizált robbanószerkezetek elleni harc alapját az információk és speciális ismeretek beszerzése képezi. Napjainkban a C-IED alapja, amelyet a legfontosabb taktikai elemként kell kezelni - a terrorizmus határokon átívelő jellege következtében – nemzetközi együttműködésre és összefogásra van szükség az eredményes harc érdekében. A nemzeti hírszerző szolgálatok részéről viszont feltétel nélkül, egységesen kell fellépni a jelenséggel szemben. Az terrorszervezetekkel és a potenciális lehetséges elkövető személyekkel kapcsolatos információk megosztása a valós kockázatanalízis alapját kell képezze, a kiemelten védett objektumok biztonsági rendszereinek tervezése és kiépítése során. A robbantásos merényletek megakadályozására szolgáló intézkedések

[46] Commanders' and Staff Handbook for Countering Improvised Explosive Devices (5000 TSX 0170/TT-7579/Ser: NU0462), p. 7, Figure 1. alapján

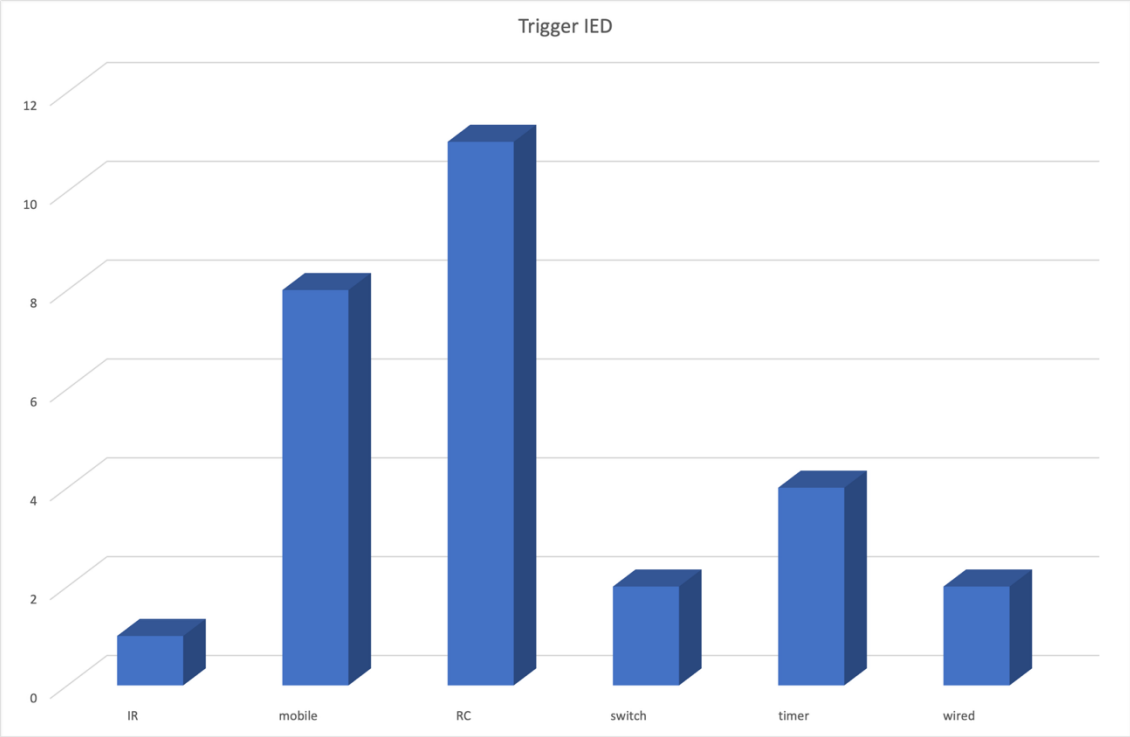
folyamatában az információszerzés az egyik legfontosabb feladat, amely nem véletlenül helyezkedik el a tevékenység alapjaként az ábrázolásban.

2.6.1 Az internet hatása az IED-k esetében

Az internethez való hozzáférés elterjedése magával hozta annak árnyoldalát, a bűnös célú robbantások esetében is. A világhálón tömegével jelentek meg az improvizált robbanószerkezetek megépítéshez segítséget nyújtó komplett útmutatók, videók, amelyek alapján azok könnyedén összeállíthatókká váltak, műszaki előképzettség nélkül is.

A kutatásomhoz kapcsolódóan vizsgálatot végeztem az egyik legnépszerűbb videómegosztó hírportálon (YouTube), a nyílt módon elérhető „oktató" jellegű előadások között. Elemezve azok tartalmát, hogy milyen típusú indítási módot mutatnak be, továbbá milyen jellegű robbanóanyagot vagy pirotechnikai elegyet alkalmaznak. Sok esetben további linkek megadásával a bemutatott szerkezet, valamint indító áramkörének a kapcsolási rajza is megosztásra került magyarázattal kiegészítve.

A következő ábrán láthatók a különböző indítási módok előfordulási arányai, az általam megtekintett videók alapján.



16. ábra IED indítási módok / YouTube videók

A vizsgált videók alapján megállapítható, hogy arányukat tekintve a vezeték nélküli megoldások összeségében többször szerepelnek a megosztott felvételeken. Ez az arány is jól példázza, hogy a rádióösszeköttetéseken alapuló megoldások a népszerűségük miatt,

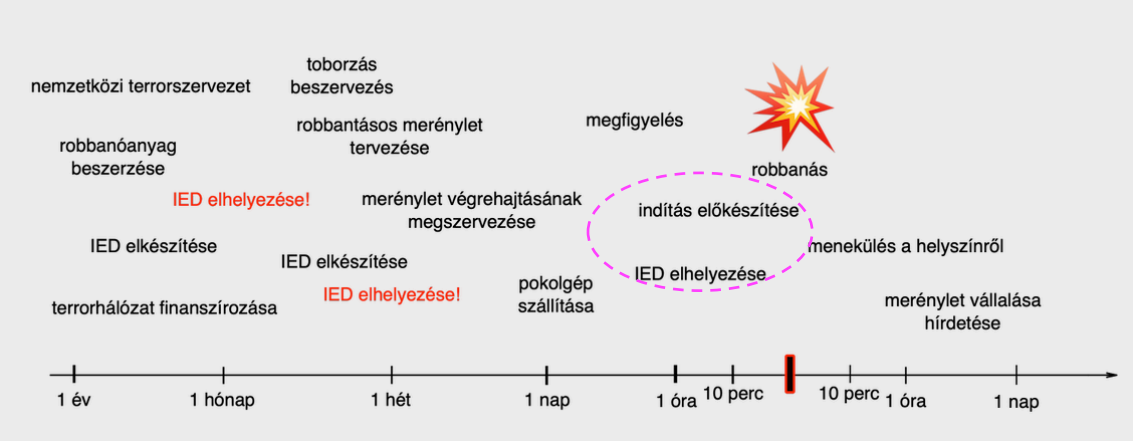
adott esetben magasabb kockázatot képviselnek egy esetleges robbantásos merénylet megtervezése során.

A YouTube-on 2008-2026 között jelentős mennyiségű improvizált robbanóeszköz készítését bemutató videó volt elérhető. Egy 2019-as jelentés szerint miden nap 300000 olyan videó található a YouTube-on, amely lépésről lépésre mutatja be a bombák, csőbombák összeállítását. A 2013-as bostoni maraton merénylői is innét merítettek ihletet a bombáik elkészítéséhez.

A YouTube 2017-től szigorúbb fellépést kezdett az ilyen tartalmak ellen. 2017 nyarán a platform gyakorlatilag háborút hirdetett az erőszakot vagy a bombakészítés fogásait bemutató videók ellen. A mesterséges intelligencia segítségével az év végére a videók 83%-át sikerült kiszűrni a korábbi 8%-os arányhoz képest. Nemzetközi együttműködéssel – mintegy 40 civil szervezet bevonásával – több mint egy millió ilyen terrorizmust elősegítő videót nézettek végig a szűrő algoritmusokkal a tiltás érvényesítése érdekében. Ennek ellenére számos videó továbbra is elérhető maradt vagy újra felkerült, különösen álcázott formában pl.: „filmtrükk” vagy „oktatási cél” megjelölésével.

2.6.2 Az IED „életútja” az időskálán

Az improvizált robbanószerkezettel elkövetett merénylet időskálán való ábrázolása látható a következő grafikonon. A különböző cselekmények lépésenként vannak feltüntetve a hozzá kapcsolódó szervezeti elemekkel és az időben való elhelyezkedés megjelölésével. A C-IED tevékenység során a feltüntetett folyamatokat kell felderíteni, és lehetőség szerint az adott pontokon a szükséges intézkedések során megakadályozni a tervezett bűnös cselekmény megvalósítását.



17. ábra Az IED "életútjának" időskálán való ábrázolása[47]

[47] ALLIED JOINT DOCTRINE FOR COUNTERING – IMPROVISED EXPLOSIVE DEVICES AJP-3.15 (A) MARCH 2011 Section II. Figure 1.1-alapján

A 16-os ábrán az időskálán pirossal jelöltem az IED-k lehetséges elhelyezésének az idejét a tervezett cselekményhez viszonyítva. A korábban elkövetett esetek alapján a létesítmények elleni támadások során jellemzően több nappal vagy akár héttel előbb telepítésre kerültek robbanószerkezetek. A kiemelten védett objektum komplex védelmi rendszerének a skálán feltüntetett becsült időtartam áll rendelkezésére, hogy a megfelelő biztonsági berendezései és intézkedései segítségével megakadályozhassa a robbantás bekövetkezését. Ezen időtartam során, gyakorlatilag bármely ponton megtörténhet a detektálás - akár a közvetlen bejuttatás alkalmával - a beléptetéskor kiszűrésre kerül a „gyanús" szerkezet. A legfőbb célunk a biztonság szempontjából, hogy ez minél hamarabb megtörténjen. A szaggatott vonallal bekeretezett időtartományban van utoljára esélyünk megakadályozni a bűnös célú robbantást. A rendelkezésre álló idő meglehetősen kevés, ebben a helyzetben a rádiófrekvenciás monitor-rendszer nagy segítséget jelenthet bombakutatás során.

Az IED-k esetében az épületen belüli robbantás elleni védelem kialakításának lehetőségeivel - tekintettel a kutatásom speciális területére - részleteiben nem foglalkozom. Egy esetleges bekövetkezett robbantás során a detonáció hatásainak csökkentése érdekében alkalmazott falakat borító burkolatok jelentőségéről teszek említést, amelyek a detonáció sebességének a csökkentésében, illetve a hullámok összegződésének megakadályozásában jelenthetnek segítséget. Amennyiben a detonáció csökkentése érdekében kerül sor valamilyen falborítás kiépítésére, szükséges lehet a rédiófrekvenciás csillapítás növelése végett, további speciális burkolat beszerelésére is.

A harmadik pillérként feltüntetett „Robbanószerkezet hatástalanítása" halmazba sorolható a tűzszerészátvizsgálás is, mint az egyik legfontosabb tevékenység az objektumokat ért bombafenyegetések során. A következő pontban ennek a taktikai elemnek az általam vizsgált szempontok szerinti összefoglalását mutatom be.

2.6.3 Tűzszerészátvizsgálás a védett objektumok esetében

Az improvizált robbanószerkezetek felépítése teszi lehetővé, hogy adott esetben az átvizsgálási folyamat ellenére, mégis be lehet juttatni a védett területekre. A főbb részeit külön-külön akár alkatelemeiként, szétszerelt állapotban gyakorlatilag „észrevétlenül" csempészhetők át a beléptetési pontokon. Az ilyen módon előkészített robbantásos merényletek megakadályozásának egyetlen módja, ha az elműködtetést megelőzően a tűzszerészátvizsgálás során előtalálásra kerülnek.

A jelenleg alkalmazott végrehajtási mód a kiemelten védett objektumok vonatkozásában, a bombafenyegetések során az úgynevezett tűzszerészeti átvizsgálás vagy bombakutatói tevékenység. Mindkét esetben meghatározott feltételeknek kell megfelelni elsődlegesen képzettség szempontjából. Az oktatás bizonyos típusú eszközismeretre épül, valamint a robbanóanyagok főbb tulajdonságai mellett azok hatásainak bemutatására. A gyakorlati rész általában a fizikai kutatást foglalja magába, amelyet jellemzően átvizsgáló tükör és lámpa segítségével hajtanak végre. A kutatási tevékenységéhez kapcsolódó műszerek tekintetében a csomagröntgen, esetleg a robbanóanyag detektorok használatának ismerete szerepel a képzésben. Az elektronikai egységek jelenlétének a detektálása - a disszipált hő érzékelésén, az elektromágneses hullámok mérésén vagy a P-N átmenetek azonosításán keresztül - alapvetően nem képezi az oktatás részét. A kézi műszeres ellenőrzések viszonylag csekély alkalmazása a tűzszerészeti átvizsgálások alkalmával, véleményem szerint az objektumvédelemhez kapcsolódóan komoly kockázatot hordoz magában.

2.7 Következtetések

Az improvizált robbanóeszközök esetleges alkalmazása a kiemelten védett objektumok elleni merényletek során, nagy valószínűséggel elektronikus, azon belül is vezeték nélküli indítószerkezetek használatát feltételezhetjük. A rendelkezésre álló „építőelemek” és az alkalmazásukra jellemző nagyobb szabadságfok, tovább erősítik az RC-IED-re eső választását valószínűségét, egy bűnös célú robbantás tervezésekor.

Az elektronikai berendezések környezetükre gyakorolt hatásuk miatt, sok esetben egyszerűbben detektálhatók, mint a kémiai tulajdonságok alapján történő ellenőrzés, amely alapvetően a robbanóanyagok összetevőit tekinti a riasztás kiváltó oknak. Az improvizált robbanóeszközöknél előszeretettel alkalmaznak úgynevezett házi készítésű robbanóanyagokat, amelyeket jellemzően a háztartási vegyszereink között található összetevőkből, némi kémiai ismeret birtokában előállíthatók.

A mai zsúfolt infokommunikációs környezetünkben a klasszikus értelemben vett robbantás elleni védelem - a kiemelten védett objektumok esetében - már magába hordozza a pokolgépes merényletek kockázatát, mivel az előzetesen alkalmazott biztonsági átvizsgálásoknak jellemzően nem része a rádióspektrum ellenőrzése. Az RF-

mérések alapvetően nem képezik a tűzszerészeti vizsgálatoknál, vagy adott esetben elhagyott csomagok-, táskák ellenőrzésénél a szerkezet tényleges működésének a megállapításához az alkalmazott technikát.
A jövőre nézve ezen tevékenység az egyik meghatározó részét kell hogy képezze a komplex objektumvédelemnek a mindennapokban vagy a bombafenyegetésekhez kapcsolódó átvizsgálások alkalmával.

A fejezethez tartozó forráselemzés 2026. január 30-án zárult le.

A kutatási célkitűzéseim közül az II és III-ss számú hipotézist fejtettem ki ebben a fejezetben.

A II. fejezethez kapcsolódó kutatási eredményeimet a következő publikációimban tettem közzé:

- Kiemelten védett objektumok robbantás elleni védelmének kiegészítése a biztonsági szint növelése érdekében [Műszaki Katonai Közlöny, XXIX. évfolyam, 1. szám – 2019. március]
- A spektrum-monitor rendszerek jelentősége az objektumvédelem területén [Biztonságtudományi Szemle, 2021, III. évf. 1. szám]
- "EVOLUTION" OF IMPROVISED EXPLOSIVE DEVICES (IED) IN THE LIGHT OF TECHNICAL DEVELOPMENT [Műszaki Katonai Közlöny, 32. évfolyam (2022) 1. szám 49–61.]

3 A RÁDIÓSPEKTRUM ELLENŐRZÉSE A TECHNIKAI ÁTVIZSGÁLÁS SORÁN

A rádióspektrum az elektromágneses spektrum azon tartománya, amely a rádiófrekvenciás hullámokat foglalja magába, és amelyet az adatátvitel, kommunikáció és számos elektronikus alkalmazás használnak – vezetéknélküli - átviteli módként. A nemzetközi szakirodalomban az RF-spektrum kifejezést elsősorban a 3 Hz és 300GHz közötti frekvenciatartományra alkalmazzák, amelybe beletartoznak a hosszúhullámú, középhullámú, rövidhullámú, ultrarövidhullámú, mikrohullámú és milliméteres sávok is. [31]

A hétköznapi szóhasználatban az RF-spektrum kifejezés alatt többnyire azokat a frekvenciasávokat értjük, amelyeket rádió-, és televízióadásra, mobilkommunikációra, wifi-re, Bluetooth-ra, radar-, és navigációs rendszerekre, valamint különféle ipari, tudományos és orvosi (ISM) alkalmazásokra használnak. Az RF-spektrum szabályozása nemzetközi (ITU[48]) és nemzeti szinten (NMHH[49]) történik, tekintettel annak véges természetére és egyre növekvő használatára. A folyamatosan bővülő sávszélesség igény miatt, a frekvenciaspektrumhoz való hozzáférés jogosultságát, szigorú szabályozással kezelik nemzeti és nemzetközi szinten egyaránt. Magyarországon a Nemzeti Média- és Hírközlési Hatóság feladatkörébe tartozik a frekvencia igények kezelése, az engedélyben foglalt paraméterek betartatása, továbbá az RF-spektrumban jelentkező zavarjelenségek felderítése.

A rádióspektrum három alapvető jellemzője, amely meghatározza annak felhasználhatóságát:

- Frekvencia (a kommunikációs csatorna kapacitását, hatótávolságát és áthatólóképességét befolyásolja);
- Sávszélesség (az átvihető adatmennyiséget határozza meg);
- Moduláció (lehetővé teszi az információ hatékony kódolását, továbbítását és dekódolását).

A rádióspektrum alkalmazásának jellemzője továbbá a spektrális sűrűség, amely arra utal, hogy az adott frekvenciatartományon belül milyen mértékben használják ki az átvitelre alkalmas frekvenciasávokat. A spektrum-felügyelet és monitorozás kulcsfontosságú a

[48] International Telecommunication Union - Nemzetközi Távközlési Egyesület
[49] Nemzeti Média- és Hírközlési Hatóság

nem kívánt interferenciák kiszűréséhez, a jogosulatlan vagy nemkívánatos jelek észleléséhez.
A kiemelten védett objektumok vonatkozásában az RF-monitor rendszer szükségessége alapvetően az információvédelem területéhez kapcsolódik. A lehallgatás elleni védelem funkciójának az információszivárgási csatornák detektálását tekinthetjük.

A hipotéziseim közül a harmadik egy részére és a negyedik témakörre vonatkozó megállapításaim ebben a fejezetben kerülnek kidolgozásra.

3.1 Információszivárgási-csatornák

Az információszivárgási csatornák képviselik a megszerzendő adatok, információk átvitelét, kisugárzását, közvetítését vagy megjelenítését lehetővé tevő berendezések, illetve egyéb technikai megoldások összességét. Két formáját azonosíthatjuk attól függően, hogy milyen jellegű emberi magatartás szükséges az információ megszerzéséhez. Ez lehet célzatos tevékenység, ami közvetlen az információ megszerzésére irányul, ezt nevezzük aktív-, vagy valamilyen mulasztásból, gondatlanságból eredő cselekmény, amely lehetővé teszi az adatokhoz való hozzáférést, ezt nevezzük passzív szivárgási csatornának. A gyakorlatban a következő módokon találkozhatunk vele.

3.1.1 Aktív információszivárgási csatorna

A megszerezni kívánt információ érdekében célzatos cselekményt hajt végre az elkövető, az által, hogy egy arra alkalmas technikai eszközzel a célszemély vagy társaság közvetlen közeléből a szóban elhangzottakat, az ott történt eseményeket, írásos anyagokat, illetve ezeket magából az infokommunikációs rendszerből kinyerve, a résztvevők tudta és beleegyezése nélkül rögzíti vagy továbbítja. Az internetes kereskedelemnek köszönhetően, gyakorlatilag a professzionális lehallgató berendezések képességeihez hasonló eszközök vásárolhatók, engedély nélkül.

3.1.2 Passzív információszivárgási csatorna

Ebbe a kategóriába sorolhatjuk az összes olyan elektronikai eszközt, berendezést, hang-, kép-, adattovábbítására képes rendszert, amelyek az üzemszerű, illetve adott esetben attól eltérő működésük következtében, lehetőséget teremtenek az információ egy részének vagy akár a teljes egészének megismerésére.

Az információbiztonság megfelelő szinten tartása végett szükséges az információszivárgási csatornák felderítése és folyamatos ellenőrzése, valamint lehetőség szerinti megszüntetése. A folyamat összetettségére való tekintettel, ez a fajta „ellentevékenység” egy komplex védelmi rendszer kialakítását teszi szükségessé.
A védelmi intézkedések szerves részét képezi az úgynevezett technikai elhárítás (TSCM[50]) és a lehallgatás elleni védelem.

3.1.3 Technikai átvizsgálás

A technikai elhárítás az információvédelem tekintetében egy olyan vizsgálati, megelőzési és ellenőrzési eljárások összessége, amelyek célja az információs tér védelme az elektronikus lehallgató és megfigyelő eszközökkel szemben. A TSCM során megfelelően képzett szakemberek műszaki vizsgálatokat hajtanak végre – kiemelten a rádiófrekvenciás-, akusztikai- és vezetékalapú csatornákon – annak érdekében, hogy felderítsék a nem engedélyezett információgyűjtésre vagy egyéb szivárgásra alkalmas berendezéseket. A szükséges előképzettség mellett ki kell emelni azt a szempontot is, hogy a feladathoz illeszkedő – műszaki paraméterű és méréshatárú – mérőműszert alkalmazzunk a vizsgálatok végrehajtása során.
A következő pontban határozom meg azt a közös jellemzőt, amely lehetőséget nyújt a rejtett lehallgató berendezések és az elektronikus, valamint a távirányításos IED detektálhatósága között.

3.2 A lehallgató eszköz vs. távirányítású improvizált robbanó szerkezet

A rádióspektrum vizsgálata során a detektálás tekinthető a közös felületnek taktikai szempontból. A TSCM tevékenység alkalmával végrehajtott RF-mérések esetében gyakorlatilag a néhány kHz-es jelektől kezdve, a hétköznapi infokommunikációs berendezéseink által használt pár GHz-es frekvenciájú sugárzásokat vizsgáljuk. A két különböző célból alkalmazott rejtett eszközök az elektronikai vezérlő-működtető egységek területén képeznek közös halmazt, amely lehetővé teszi számunkra az elektromágneses sugárzás mérésén keresztül a detektálhatóságukat.
A kiemelten védett objektumok biztonságtechnikai rendszerei részére meghatározó szempont, hogy a robbantás-, lehallgatás elleni védelmi képessége a lehető legmegbízhatóbb legyen a felderítés szempontjából. A feladat maradéktalan végrehajtására érdekében, elengedhetetlen ezen szempontból a detektálást közös felületen

[50] Technical Surveillance Counter Measures – technikai elhárítás

történő kezelése. A rádiófrekvenciás monitorrendszerben rejlő képességek használatával, megfelelő módon történő paraméterezésével lehetőségünk van ez által, a komplex biztonsági rendszerünk védelmi fokozatának kiterjesztésére.

A következő pontokban ismertetem a távirányítású lehallgató eszközök általános felépítését, kihangsúlyozva azon egységeit, amelyek közvetlenül hatással vannak a rádióspektrumon keresztül történő detektálhatóságuknak.

3.2.1 távirányítású lehallgató eszköz általános felépítése

A következő ábrán a távirányítású lehallgató készülék elvi felépítése látható, azon fő részeinek feltüntetésével, amelyek közvetlenül szerepet játszhatnak a korábban vizsgált detektálási szempontok szerint.

18. ábra Távirányítású lehallgatóeszköz elvi felépítése

A 18-as ábra bal oldalán látható a távirányítású lehallgatóeszköz blokkvázlata, amely tartalmazza a fő funkciókat ellátó részegységeket. Az egyik leglényegesebb különbség a korábban részletesen bemutatott távirányítású IED-hez képest, hogy az eszköz működése során kétirányú kommunikáció is lehetséges. Amennyiben a rejtett lehallgató berendezés kizárólag vevőegységet tartalmaz, a detektálást tekintve hasonló eljárásmódot kíván, mint az RC-IED-k esetében. Adóegységet is tartalmazó eszköz működése során, a rádióspektrumban egyértelmű jelet láthatunk, amennyiben online módban van. A „tárol és továbbít” működésű rejtett lehallgatóeszközök esetében, kizárólag az adattovábbítás során láthatunk nagyszintű jeleket az éterben.

A távolról ki-be kapcsolható lehallgatóeszköz, amely nem alkalmas adattovábbításra, a detektálás lehetősége szintén a vezérléséhez tartozó vevőmodul által kibocsátott parazita elektromágneses hullámok érzékelésén keresztül megvalósítható.

3.3 A rádióspektrum monitor rendszer

A modern biztonságtechnika egyik kiemelkedően fontos, ugyanakkor gyakran kevésbé ismert eleme a rádióspektrum monitor rendszer, amely a vezetéknélküli kommunikációval összefüggő fenyegetettségek – köztük az információvédelemhez kapcsolódó és a RC-IED-k okozta kockázatok – észlelésére és elemzésére szolgál. Az RF-spektrum monitorozása napjainkban már elengedhetetlen részét kell, hogy képezze a komplex objektumvédelmi rendszereknek, különösen a kiemelten védett létesítmények esetében.

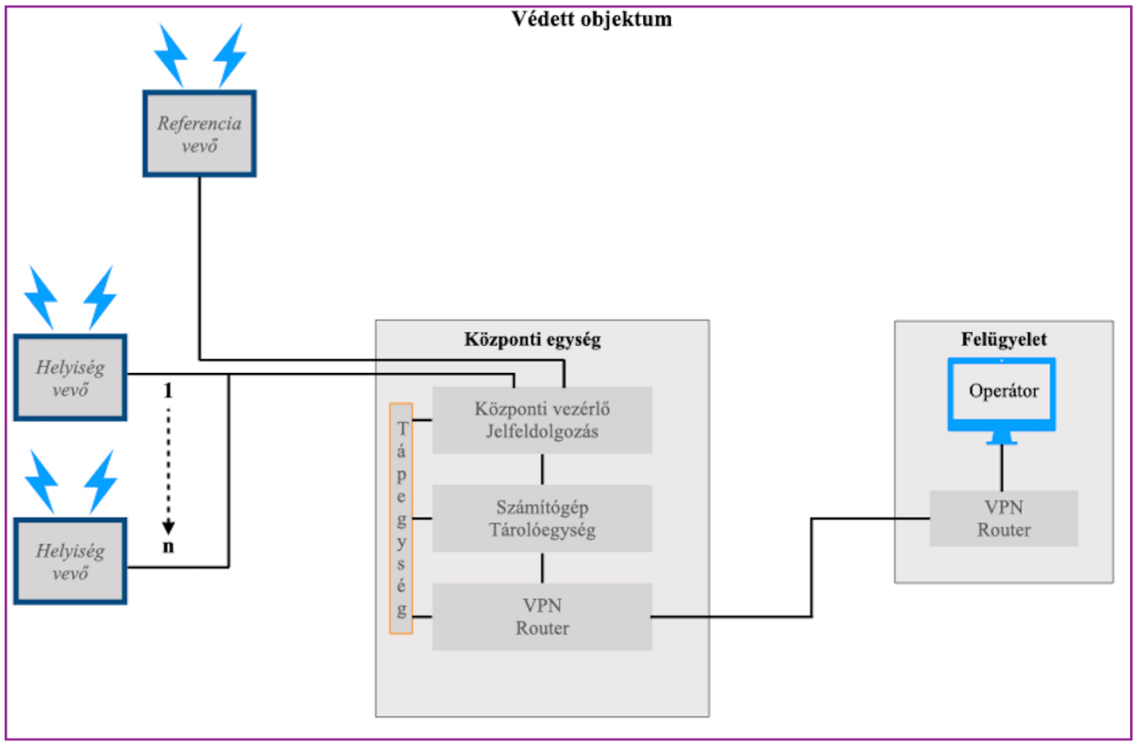
A rádióspektrum monitor rendszerek célja, hogy valós időben detektálják az ismeretlen vagy nem engedélyezett rádiójelek jelenlétét, azok spektrális jellemzőit (pl.: frekvencia, moduláció, sávszélesség, időtartam) és térbeli forrását. Ez a képesség lehetővé teszi olyan fenyegetések azonosítását, mint:

- rejtett lehallgatóeszközök (pl.: GSM, LTE – rögzítők, BLE modulok);
- mobil- vagy rádióindítású IED-ek;
- drónvezérlési jelek;
- illetéktelen hálózat aktivitás (pl.: wifi AP-k).

A rendszer működése jellemzően hardver és szoftver komponensekre bontható. A hardveres részt képezik az antennák, spektrumanalizátor, míg a szoftveres rész a jelfeldolgozásban, azon belül is a mintázatok azonosításában és a riasztások kezelésében játszik szerepet.

Az RF-monitor rendszer stratégiai előnye, hogy integrálható más biztonsági rendszerrel, mint például behatolásjelző-rendszerrel vagy videóanalitikával, így egy komplex védelmi architektúra építhető ki. Az ilyen megoldások 24/7 működésű, autonóm riasztási és naplózási képességekkel rendelkeznek, és elősegítik a rendkívüli események utólagos rekonstruálhatóságát is.

A következő ábrán egy RF-monitor rendszer elvi felépítése látható, amelynek kiépítésével a védendő objektumon belül, az adott térrészeken elhelyezett modulok és hozzájuk csatlakoztatott antennák segítségével, képesek lehetünk az ott történő elektromos „rezgések” detektálásra. A rendszer főbb összetevőit és a működésére vonatkozó jellemzőit a kutatásom céljához kapcsolódóan részletezem, kiemelve azon tulajdonságait, amelyek meghatározóak lehetnek a hatékony „érzékelés” szempontjából.



19. ábra Elosztott paraméterű mérőhálózat elvi rajza

A 19-es ábrán egy elosztott paraméterű mérőhálózat felépítése látható főbb elemeinek feltüntetésével. A kép bal oldalán helyezkednek el a mérőmodulok, amelyeket közvetlenül az adott irodákba vagy tárgyalókba kell felszerelni, ahol detektálni akarjuk az elektormágneses rezgéseket és felfedni az információszivárgási csatornákat.

A központi egység feladata a mért adatok valós időben történő összehasonlító elemzése. Nagyon fontos szempont a modulok által detektált jelek, egymáshoz viszonyítva szinkronban történő feldolgozása, mert ezen adatok mindegyike lényeges lehet a rejtett eszköz által keltett elektromágneses sugárzás, a lehető legpontosabb helymeghatározásában.

A felügyeleti egység - a mai átviteltechnikának megfelelően - akár a védett objektumtól eltérő helyen is elhelyezésre kerülhet. Ez a feltétel természetesen a reagáló erőkre nem érvényes, mivel a jelentkező anomáliák azonosítása jelentős késedelemmel járhat. Szükséges lehet közvetlenül, kézi mérések segítségével pontosítani a rendszer által detektált jeleket.

3.3.1 Spektrumanalizátorok szerepe az RF-monitor hálózatok esetében

A spektrumanalizátorok a rádiófrekvenciás spektrum vizsgálatára szolgáló kiemelten fontos mérőeszközök, amelyek lehetővé teszik az elektromágneses jelek frekvencia szerinti eloszlásának mérését, megjelenítését és elemzését. Alkalmazásuk

elengedhetetlen az RF-monitorrendszerek működésében, mivel ezek biztosítják a védett objektumokban elhelyezett modulok segítségével az elektromágneses környezet valós idejű felügyeletét, ezzel lehetővé téve a nem kívánt rádiósugárzások, lehallgatási kísérletek vagy RC-IED-hez köthető rádiójelek detektálását.

A spektrumanalizátor működésének alapja a beérkező rádiófrekvenciás jel frekvenciaösszetevőkre bontása, amely történhet:

- söpréssel hangolt szuperheterodin elven működő (swept-tuned[51]);
- valós idejű digitális feldolgozással (real-time FFT);
- vagy hibrid módszerekkel, ahol a cél a gyors válaszidő és a nagyfokú spektrális érzékenység együttes biztosítása.

A swept-tuned eszközök a vizsgálni kívánt frekvenciasávon végighangolódnak, és minden ponton mérik a jel teljesítményét. Ezek pontos, de időben nem folyamatos monitorozást biztosítanak, így a rövid idejű úgynevezett tranziens jelek detektálása esetleges lehet. Ezzel szemben a valós idejű spektrumanalizátorok (RTSA[52]) a teljes megfigyelt sávot egyidejűleg vizsgálják digitális Fourier-transzformációval (FFT), így kiválóan alkalmasak gyorsan váltakozó vagy rövid idejű rádióimpulzusok rögzítésére. [32]

A spektrumanalizátorok fő jellemzői a következők:

- frekvenciatartomány (az az RF-intervallum, amelyben az eszköz képes mérni);
- felbontási sávszélesség (RBW[53] az a legkisebb frekvencia-intervallum, amelyben a jel még különállóként jeleníthető meg);
- valós idejű jel „elkapás” (POI[54] - az eszköz képessége egy rövid idejű jel detektálására adott körülmények között);
- dinamika tartomány (a legnagyobb és legkisebb mérhető jelszintek közötti különbség);
- érzékenység (a legkisebb észlelhető jel, amely még megkülönböztethető a zajtól).

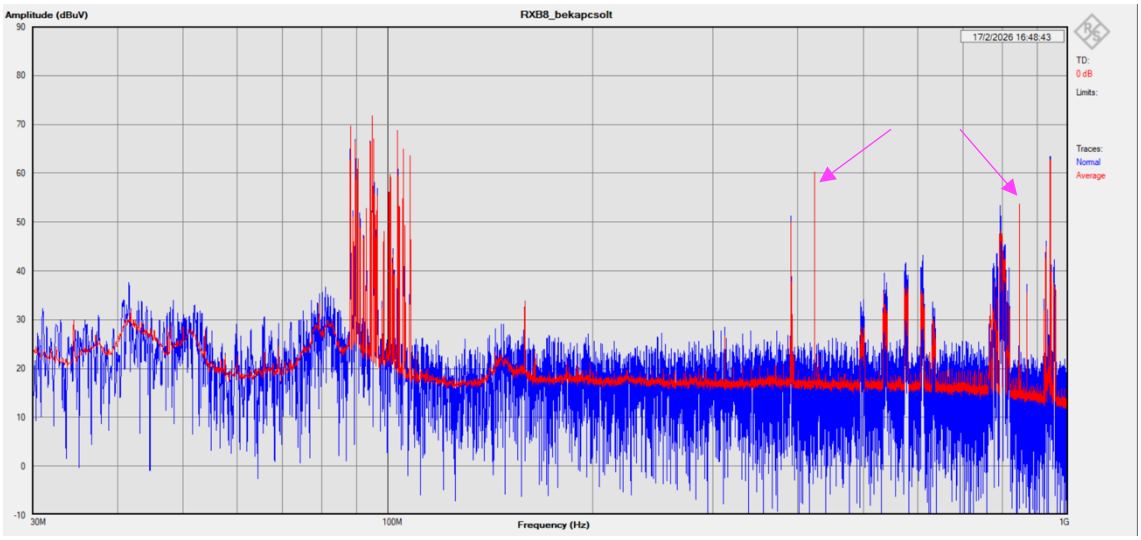
A rádióspektrum monitorrendszerek hatékonysága jelentős mértékben függ a használt spektrumanalizátor típusától és a rendszeres TSCM-ellenőrzéseket végrehajtók felkészültségétől, körültekintő munkájától. A komplex védelmi rendszerekbe integrált

[51] swept-tuned - söprőhangolt
[52] Real-Time Spectrum Analyzer – valós idejű spektrumanalizátor
[53] Resolution Bandwidth – felbontási sávszélesség
[54] Probability of Intercept – jel „elkapás” valószínűsége

valós idejű analizátoroknak képesnek kell lennie az automatikus anomália-felismerésre, jelazonosításra, sőt akár gyanús RF-tevékenység lokalizálására is.

A rádióspektrum szemléltetésére szolágáló ábrákon, korábban az RC-IED-k működtető áramkörénél (RXB8 vevőmodul) használt EMC precomplience szoftver megjelenítését használom, a könnyebb összehasonlíthatóság végett.

A következő ábrán a rádiós spektrum 30MHz-1000MHz-ig terjedő tartománya látható.



20. ábra RF spektrum 30MHz-1GHz-ig bekapcsolt RXB8 vevőmodul

A spektrumképen a nyíllal jelzett frekvenciakomponensek jelzik a vevőmodul oszcillátorának az elektromágneses sugárzását, amelyet a körülötte található jelek közül kell tudnunk azonosítani, lehetőleg a bekapcsolás pillanatában. Az operátor általi vizuális azonosítás lehetősége természetesen lehetséges módja az idegen jelek detektálásának, de a hatékonyságot tekintve már nem mondható jó megoldásnak. Napjaink nagysebességű kommunikációs hálózatainak elterjedése következtében, a detektáló rendszerünknek is képesnek kell lennie kezelni, a hozzá kapcsolódó éterben megjelenő rádiójeleket. Ennek ellenére a kezelőszemélyzet folyamatos képzését nem szabad elhanyagolni, szükséges az állandó ismeretbővítés mind a lehetséges rejtett eszközök vonatkozásában és természetesen a vezetéknélküli technológia legújabb vívmányait tekintve egyaránt.

A következő pontokban az RF-monitor rendszer főbb paramétereit ismertetem elsődlegesen olyan aspektusból, amelyek fontos szerepet játszhatnak a korábban bemutatott úgynevezett parazita spektrumösszetevők detektálásában.

3.3.2 Érzékelési határ

Az RF-monitor rendszer központi hardver elelmét képezi a spektrumanalizátor, amelynek mérési képességeit alapvetően az eszköz érzékenysége határozza meg, amely szoros összefüggésben áll az érzékelési határral és a zajszinttel.

Az érzékelési határ - minimum detektálható jelszint - azon legkisebb bemeneti jelszint, amelyet még megbízhatóan meg tud különböztetni a műszer a rendszer saját zajától. Ez a határ nem abszolút érték, hanem statisztikai jellegű, és tipikusan egy adott jel–zaj viszony (SNR[55]), például 3 dB vagy 10 dB mellett definiálják. Az érzékelési határt alapvetően a spektrumanalizátor belső zajszintje korlátozza, amelyet a bemeneti fokozatok, keverők és erősítők zajtényezője határoz meg.

A spektrumanalizátorok zajszintjének egyik kulcsparamétere a DANL[56], azaz a kijelzett átlagos zajszint. A DANL azt a zajszintet reprezentálja, amely a kijelzőn megjelenik, amikor a bemenet lezárt - tipikusan 50 Ω-os lezárással -, és a műszer saját zaját mérjük. A DANL értéke általában dBm-ben vagy dBm/Hz-ben kerül megadásra, és közvetlenül jelzi a műszer zajszintjét.

A DANL értéke következő tényezőtől függ:

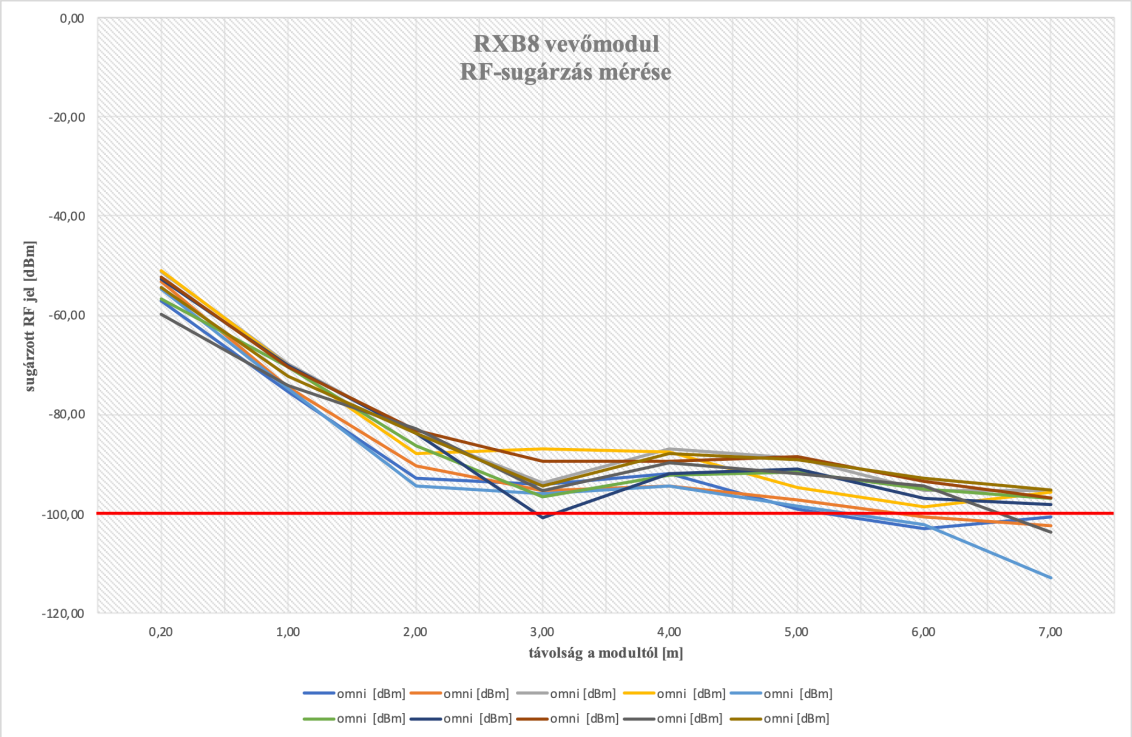
- felbontási sávszélesség (RBW);
- videósávszélesség (VBW);
- bemeneti csillapítás és előerősítés;
- detektálási mód (RMS detektorok);
- hőmérséklet és zajtényező (kTB). [33]

A DANL és az érzékelési határ szoros kapcsolatban állnak, egy jel csak akkor detektálható megbízhatóan, ha annak szintje meghaladja a DANL által meghatározott zajszintet egy adott SNR-rel. Következésképpen a spektrumanalizátor dinamikatartományának alsó határát a DANL határozza meg.

A kutatásom során egy valós irodai környezetet használtam a tesztmérések elvégzése helyszínéül. A méréseket megelőzően szimulációkat végeztem a rádiós környezet és a terjedési módok szemléltetése érdekében, majd konkrétan a korábban bemutatott vevőmodulok jelszintjeit vizsgálatam egy kézi spektrumanalizátorral és hozzákapcsolt omni-, majd egy LP[57] antennával.

[55] Signal to Noise Ratio – jel-zaj viszony
[56] Displayed Average Noise Level – megjelenített átlagos zajszint
[57] LP – Logaritmus-periodikus antenna

A különböző távolságból végrehajtott méréseket az adott irodához igazítva, 0,2 -7 m -es tartományban végeztem, annak igazolására, hogy az RF-mérőrendszer milyen jelszinten képes detektálni az adott jeleket.



21. ábra RXB8-as vevőmodul RF-sugárzás mérésének diagramja

A 21-es ábrán a 10 db RXB8-as modul adott távolságokban elvégzett méréseinek az összefoglaló diagramja látható. A piros vízszintes vonallal jelöltem a -100dBm-es érzékelési határt szimbolizáló küszöbértéken, amelyet mindenképpen el kell érnie a jelforrás által kisugárzott elektromágneses jelnek az adott távolságban, hogy az RF-monitor rendszerünk detektálni tudja.

3.3.2.1 Antenna karakterisztika

A vevőantennák az elektromágneses hullámok vételére szolgáló alapvető szerkezetek, amelyek a térben terjedő elektromos- és mágneses térkomponenseket elektromos jellé alakítják. Az antenna működése reciprocitási elven alapul, így sugárzó és vevő üzemmódban azonos elektromágneses tulajdonságokkal rendelkezik. [34] A vevőantennák viselkedése ezért a sugárzási karakterisztikákon keresztül is leírható.

A vevőantenna egyik legfontosabb tulajdonsága a térbeli szűrő jelleg, amely azt fejezi ki, hogy az antenna nem vesz azonos súllyal minden irányból érkező jelet. Az antenna a tér egyes irányaiból érkező elektromágneses energiát hatékonyabban csatolja ki, míg más

irányokból érkező jeleket csillapít. Ennek a hatásnak jelentősége van az interferenciával terhelt környezetben, ahol az antenna irányítottsága révén javítható a jel–zaj viszony.
A térbeli szűrés matematikailag az antenna iránykarakterisztikájával írható le, amely megadja az antenna által vett - vagy sugárzott - teljesítmény szögfüggését. Az iránykarakterisztika általában gömbi koordinátákban kerül megadásra, és főbb jellemzői közé tartozik a főnyaláb, az oldalnyalábok, valamint a félértékszélesség. [34] Az antenna térbeli szelektivitását a főnyaláb szögnyílása és az oldalnyalábok elnyomása határozza meg.
Az antennanyereség az egyik legfontosabb teljesítményjellemző, amelyet az antenna adott irányban sugárzott - vagy vett - teljesítménysűrűségét viszonyítja egy referenciaantennához, tipikusan izotróp sugárzóhoz. A nyereség tartalmazza az antenna irányítottságát és hatásfokát is, és általában dBi egységben adják meg. [35] A vevőantennák esetében a nagyobb nyereség egy adott irányból érkező jel nagyobb hatásos vételét jelenti, ami közvetlenül javítja a rendszer érzékenységét.
Az antenna érzékenysége szoros kapcsolatban áll az ún. effektív apertúrával, amely azt a felületet foglalja magába, amelyen keresztül az antenna a beérkező elektromágneses energiát „begyűjti”. Az effektív apertúra és a nyereség között az alábbi összefüggés áll fenn:

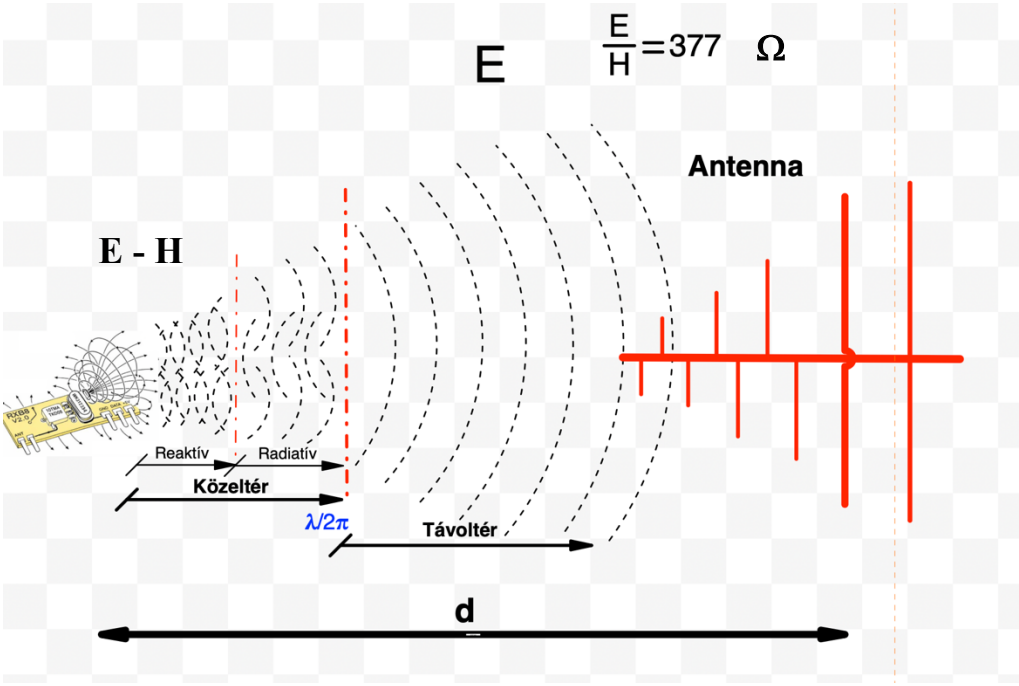
$$A_e = \frac{\lambda^2 G}{4\pi}$$

Ahol A_e az effektív apertúra, λ a hullámhossz, G az antenna nyeresége. [34] Ebből következik, hogy nagyobb nyereségű antenna nagyobb hatásos energiagyűjtő képességgel rendelkezik, ami alacsonyabb jelszintek detektálását teszi lehetővé. A mi esetünkben pont erre van szükség bizonyos frekvencia tartományokban.
A vevőantenna teljesítményét továbbá befolyásolja a környezeti zaj, az illesztetlenség, valamint a polarizációs veszteségek. A maximális teljesítménykicsatolás feltétele az impedanciaillesztés, míg a polarizációs egyezés biztosítja, hogy az antenna a beérkező hullám elektromos térerősségének megfelelő komponensét hasznosítsa.

Összefoglalva, a vevőantennák térbeli szűrőként viselkednek, ahol az iránykarakterisztika határozza meg az irányfüggő érzékenységet, míg a nyereség és az effektív apertúra a vételi hatékonyságot szabja meg. Ezek a paraméterek

kulcsfontosságúak az objektumvédelem területén a rádiófrekvenciás rendszerek tervezése és kiépítése során.

A következő ábrán a korábban bemutatott elektronikai modul közeltéri sugárzása mellett, a detektálása céljából elhelyezett antenna közötti főbb tulajdonságokat ismertetem.



22. ábra Vevőantenna távolsága a rejtett elektronikai eszköztől

A 22-es ábrán látható, hogy a közeltér sugárzó után a távoltér mező régiója következik. Ebben a régióban az elektromágneses mezőket a radiatív mezők uralják. Az E és H mezők merőlegesek egymásra és a terjedési irányra, akárcsak a síkhullámoknál. Az elektromágneses sugárzás hullámhossza határozza meg a közel- és távoltér arányát a vevőantennához viszonyítva. A távoltérben ($\lambda/2\pi$) a rádióhullámok terjedése során az elektromos tér (E) dominál, ez hatással van az alkalmazható antenna típusára a detektálás hatékonysága miatt. Ebben a távolságban síkhullámokat érzékelünk, és antennákat használunk a jelek vételére. Az $\frac{E}{H}$ hányados jelképezi a távoltér hullámimpedanciáját, ami $d>\lambda$ estén 377 Ω-nak adódik

Az antenna karakterisztika, valamint a közel- távoltér hatásának az egyéb célból történő alkalmazását jelentheti, adott esetben a személy érzékelése annak közvetlen közelében. A sugárzó közeltérben a két hullámforma fázisba kerül, de az egyéb alkatrészekről még passzív reflexió következtében elektromágneses sugárzás verődhet vissza az „antennába”, amelynek során az elektromágneses tér torzul (ezt a tulajdonságot

alkalmazzák adott esetben az antenna karakterisztika módosítására pl.: Yagi-Uda – reflektorok, direktorok).

Ennek a fizikai folyamatnak a gyakorlatban történő megjelenési formája, amikor közel kerülünk egy hangolt FM rádióhoz – módosítjuk annak antenna karakterisztikáját a testünk közelsége által – az adás elhalkul vagy adott esetben felerősödik.

A következő ábrán egy spektrumanalizátor kijelzője látható egy olyan szituációt szemléltetve, amikor az emberi test az antenna közelébe kerül és jól látható módon hatást gyakorol a vett jel spektrumképére.

23. ábra A spektrum leszívás szemléltetése két különböző sávszélességű digitális jelen

A baloldali ábrán a szélessávú digitális TV adás jele látható a jellegzetes „beszakadás” mintázattal, amely az antenna előtt bizonyos távolságban mozgó személy hatására alakult ki. A jelben található beesés a mozgással egyidőben haladt végig a spektrumképen. A jobboldali ábrán egy keskenysávú digitális jel spektruma látható, amely az emberi test közelségének hatására nem az előbb bemutatott jelenséget produkálta, hanem - a jelszintet tekintve - teljes szélességében változtatta azt.

Kellő intelligenciával rendelkező RF-monitor rendszer képes lehet a spektrumban megjelenő makrókörnyezet jeleit vizsgálva, adott esetben emberi jelenlétet is detektálni a védett területen az antennák megfelelően koordinált elhelyezésével.

A következő pontokban ismertetem az antennák elhelyezésének fontosabb szempontjait, hogy mely paraméterek határozzák meg a felszerelés helyét egy RF-monitor rendszer esetében.

3.3.2.2 Antennák elhelyezése

A karakterisztikának megfelelően kialakított antenna „rejthetősége” és a védendő helyiség jellege és berendezése, együttesen határozzák meg a legideálisabb elhelyezési

pont megtalálását. A tervezési és természetesen a kivitelezési munkálatok során, az egyik legnagyobb dilemmát okozó kérdés a belsőépítészek és a biztonságtechnikai mérnökök között, hogy hova kellene elhelyezni, és a végén ténylegesen hol kerül felszerelésre az antenna az adott térrészen.

A következő ábrán a tesztkörnyezet főbb tulajdonságait és a vevőmodul sugárzási adatait betáplálva, az Indoor RadioPlanner2.1 vezetéknélküli szimulációs szoftveren lefuttatva, a következő lefedettségi képet kaptam.

24. ábra RC-IED RF-sugárzása 422MHz-es frekvencián tesztkörnyezetben szimulálva

Az ábra bal felső részén látható a rejtett vevőegység az irodai teszt környezetben, az épület szerkezetére meghatározott paraméterekkel megadva (szoba alapterülete, belmagasság, 150mm-es vasbeton falak, elektronikai szempontból városi környezet). A szimuláció során látható a jelerősség csökkenése a távolság függvényében, továbbá a nyílászáró okozta úgynevezett „kifújási sáv", valamint a belső bútorzat okozta csillapítási sáv a szomszédos területekre vonatkozólag.

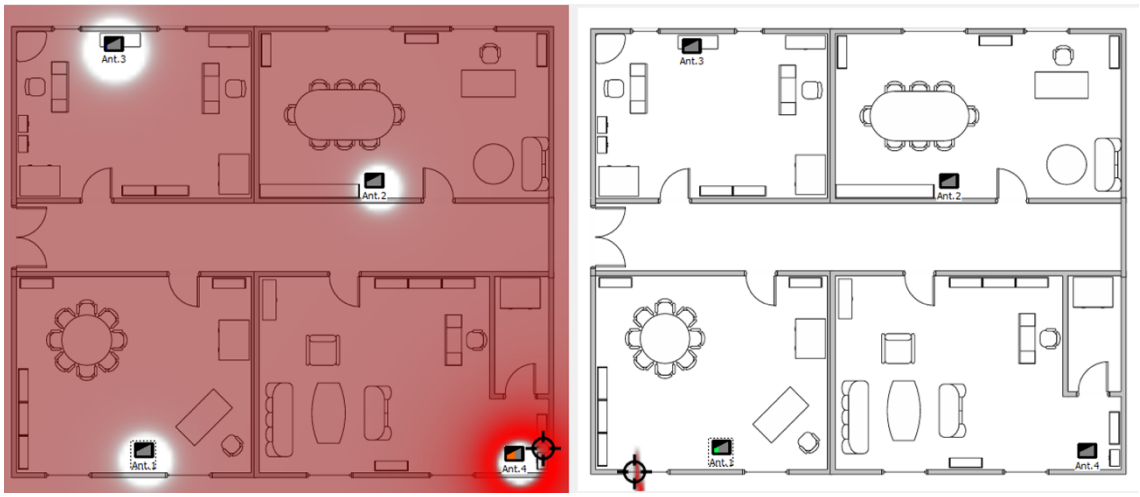
Az RF-monitor rendszer érzékelési határát nagyban befolyásolja az egyes modulok adott védendő térrészben való elhelyezésének lehetősége, ugyanis az összekötő vezetékek, valamint az antenna kábelek mind-mind csökkentik a mérni kívánt jel szintjét. Ezeket a

szempontokat figyelembe véve a lehető legközelebb kell felszerelni a vevőmodulokat az objektum védett helyiségeihez.

3.3.3 Térbeli elválasztás

Az elosztott paraméterű mérőhálózatok nyújtotta lehetőségek közül azon képességét emelném ki, amelynek segítségével meg tudjuk határozni az elektromágneses sugárzás helyét az objektumon belül. A védendő térrészen elhelyezett mérőmodulok - a megfelelően kiválasztott és illesztett antennák segítségével – jellemzően a térerősség mérésével, relatív pontosan képesek meghatározni a sugárforrás helyét az adott épületrészben. A kiemelten védett épületeink komplex biztonságtechnikai rendszere ezen képesség nélkül, meglehetősen védtelenné válik a rejtett lehallgató berendezések és az EIED-k megfelelő időben történő detektálása terén. Napjaink fejlett szoftverrádió technológiáját is fegyelembe véve egy ilyen rendszer kiépítése már nem jelent extra költségeket, szemben az általa nyújtott plusz biztonsági szolgáltatások értékével összehasonlítva.

A következő kettős ábrán szeretném bemutatni a tesztkörnyezet segítségével a kis-, és nagyszintű jelek megkülönböztetésének a megjelenítését.

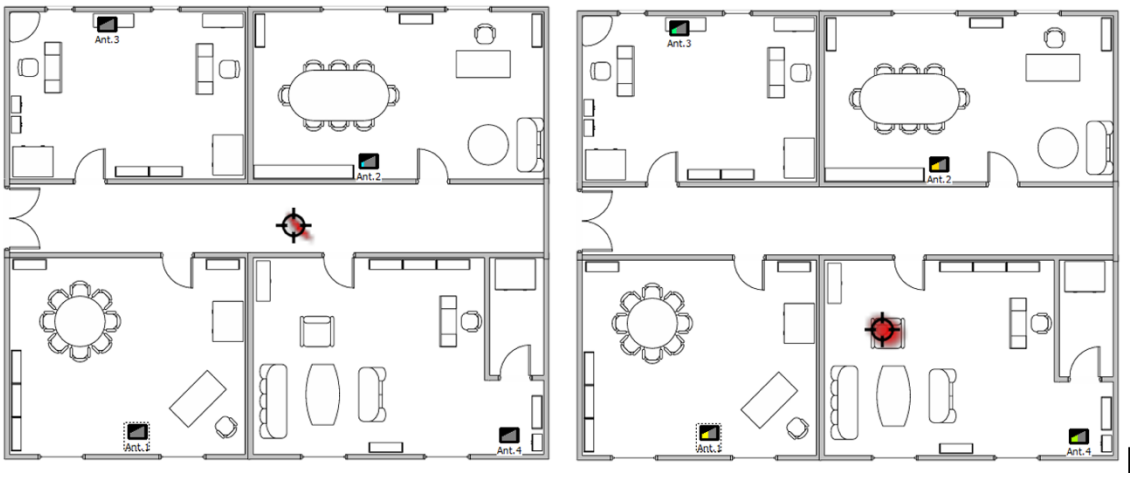


25. ábra Nagy-, és kisszintű külső jelek alaprajz szerinti meghatározása

A kép bal oldalán látható egy külső relatív nagyszintű jel érzékelésének az ábrázolása a térerősség függvényében (termikus színskála). Ennek segítségével a jel lehetséges sugárzási irányáról is kapunk információt, ami hatékonyabbá teszi a jelforrás esetleges beazonosításának és helymeghatározásának a képességét. A jobb oldali részen egy szintén külső elektromágneses sugárzás hatását láthatjuk - közvetlenül az ablakban

jelölve – relatív kis jelszinttel ábrázolva, amely nagy segítséget jelent a térbeli elválasztás során.

A következő képpáron ugyanezen elv alapján a belső térben keletkezett jelek ábrázolása látható, amelynek segítségével az adott térrészben tudjuk a jelforrás helyét meghatározni.



26. ábra Jelforrás detektálása belső térrészen

A kép bal oldalán szemléltetem az RXB8 típusú vevőegység - folyosón történő bekapcsolását követően - a mérőrendszer által érzékelt és megjelenített helyét. A jobb oldalon konkrétan egy az adott irodahelyiségben lévő fotelben elrejtett jelforrás képe látható. Mindkét esetben jól kivehető módon és pontosan jelezte a monitor-rendszer a védett épületrészben a rádióforrás elhelyezkedését.

3.3.4 A detektálás valószínűsége (POD[58])

A lehallgatás elleni védelem során a TSCM[59] tevékenység egyik legfontosabb részeként említik a szakértők a rádióspektrum folyamatos felügyeletét, a védendő objektumon belül. Az információvédelem alapját képező taktikai elem - spektrumanalízis - megszakítás nélküli végzése elengedhetetlen a rejtett megfigyeléssel szembeni hatékony védekezés szempontjából. A mai rádiótechnológia kínálta lehetőségek (SDR) képesek biztosítani számunkra a megfelelő paraméterű rendszer kiépítésének a lehetőségét. A technikai elhárítást végzők körében sokszor alakul ki hamis biztonságérzet az átvizsgálás során, mégpedig a rádióspektrum ellenőrzésével összefüggésben. A kellő felkészültség hiányában a feladatot végrehajtók hajlamosak abban a tévhitben befejezni a munkájukat, hogy az átvizsgálás ideje alatt folytatott frekvencia ellenőrzés - aktív vezeték nélküli

[58] Probability of Detection - detektálás valószínűsége
[59] Technical Surveillance Countermeasures - rejtett lehallgató-, megfigyelő eszközök felkutatásának végrehajtása

eszköz kutatására vonatkozólag - valós negatív eredményt jelentett. A spektrum monitor rendszerekre vonatkozólag létezik egy jelölő szám, amely százalékos arányként mutatja, hogy a frekvencia vizsgálat ideje alatt, milyen hatásfokkal képes felderíteni az ismert jelek közül a rejtett eszköz elektromágneses hullámait. A mérési tevékenységet statisztikai szempontból megközelítve egyértelművé válik mindenki számára, hogy az úgynevezett POD értéke a vizsgálat időtartamára levetítve, elenyésző százalékot jelent az éves óraszámhoz viszonyítva. [36]

Konkrétan vizsgálva a POD által meghatározott százalékot egy rendszeresen átvizsgált objektum esetén:

- a frekvencia ellenőrzési tevékenység heti 2 óra időtartamban, éves viszonylatban körülbelül 100 órát jelent;
- az éves óraszámhoz viszonyítva1%-os találati arányt képvisel.

A detektálás valószínűségét tovább növelheti a mesterséges intelligenciával támogatott jelfeldolgozó rendszer, amely a folyamatos (7/24) mérésekből képez mintázatot, és keres összefüggéseket az eltérések között. A rejtett megfigyelőeszközök közül, a „tárol és továbbít" típusú fajtáira, kizárólag a folyamatos spektrumellenőrzés jelenthet 100%-os felderítési képességet.

3.3.5 Jelanalízis

A rádiófrekvenciás spektrum mérésének egyik alapvető célja, hogy az elektromágneses környezetben megjelenő jeleket azonosítani, osztályozni és értelmezni lehessen a frekvencia-, idő-, amplitúdó és fázis jellemzőik alapján. A jelanalízis folyamata az RF-monitor rendszerek esetében nem csupán teljesítménymérést, hanem a moduláció-azonosítását, spektrális elfoglaltság nyomon követését, valamint az anomáliadetektálást is magában foglalja.

A jelanalízis több síkon értelmezhető:

- Időtartományban (amplitúdó-idő viszonyának vizsgálata pl.: burkolóelemzés, triggerelés);
- Frekvenciatartományban (spektrumvizsgálat-FFT, szűrés, spektrumsűrűség-PSD[60] és csúcsteljesítmény alapján);

[60] Power Spectral Density - teljesítmény spektrális sűrűsége

- Modulációanalízis: digitális modulációk (pl. QPSK[61] 16-QAM[62],) azonosítása konstellációs diagramok segítségével.

Spektrum-idő elemzés (Time–Frequency Analysis): rövid idejű jelek vagy időben változó spektrumú jelek vizsgálata spektrogram, wavelet[63] vagy STFT [64]eszközökkel.

A modern spektrumanalizátorok – különösen a valós idejű eszközök – integrálnak olyan jelanalízis-funkciókat, amelyek lehetővé teszik:

- jelburkoló és csúcsdetektálás;
- spektrális maszk szerinti összehasonlítás;
- automatikus spektrummintázat-felismerés;
- „ujjlenyomat" azonosítás, azaz azonos RF-források főbb jellemzők alapján való felismerése.

Ezek teszik lehetővé, hogy az RF-monitor rendszer ne csupán észlelje a spektrumösszetevőket, hanem aktív módon osztályozza a jelenlévő jeleket.
A jelanalízis során különböző típusú rádiójelek viselkedését kell értékelni:

- CW[65] (folyamatos vivőjelek, gyakran használt bugok, rejtett adók);
- burst (rövid, impulzusszerű jelek, gyakoriak IED-vezérlésnél);
- különböző frekvenciamodulált jelek (radarok vagy RF-zavaró rendszerek).

Az azonosítás alapja a spektrális viselkedés, időbeli mintázat és modulációtípus, amelyeket a spektrumanalizátor belső DSP[66] egysége vagy külső jelfeldolgozó algoritmusok azonosítanak.
A jelanalízis pontos végrehajtása kritikus jelentőségű a lehallgatás elleni védelemben valamint az RC-IED-ek kapcsolódó felderítésben, megelőzésében.
AI támogatott elemző szoftver, amely képes a monitor-rendszer korábbi mérési adatait is egységesen és összefüggéseiben kezelni. A normál mintázatokat folyamatosan, valós időben vizsgálva tudja detektálni a rádiós spektrumban jelentkező anomáliákat, és azokat jelzés formájában továbbítani az operátoroknak.

[61] Quadrature Phase-Shift Keying - kvadratúra fázisbillentyűzés
[62] Quadrature Amplitude Modulation - kvadratúra amplitúdómoduláció
[63] wavelet analízis
[64] Short-Time Fourier Transform - rövid idejű Fourier-transzformáció
[65] Continous Wave – folyamatos jel
[66] Digital Signal Processor - digitális jelfeldolgozó processzor

3.3.5.1 POI[67] a jel „elkapás” valószínűsége

A POI — egy meghatározó paraméter a spektrumanalizátorok működéséhez kapcsolódóan. Ez a paraméter fejezi ki, hogy a vizsgált rádiójel, milyen valószínűséggel kerül detektálásra az adott spektrumanalizátor által, figyelembe véve a jel időtartamát, frekvenciáját, ismétlődési szekvenciáját, valamint a dinamikai tartományhoz való arányát, azaz a jelszintet.

A POI-t a következő tényezők befolyásolhatják:

- a spektrumanalizátor pásztázási (sweep-time) sebessége;
- felbontási sávszélesség (RBW);
- a detektálási módszer (real-time vs. swept-tuned);
- valamint az alkalmazott digitális jelfeldolgozás (FFT-alapú, pretriggering).

A valós idejű spektrumanalizátoroknál a POI értéke akár 100%-ot is elérheti, bizonyos időtartamú jelek esetén, amennyiben a jel nem esik a rendszer időfelbontási határán kívül. Ez különösen fontos az időben rövid, alacsony kitöltésű tényezőjű és nem periodikus rádiójelek detektálásánál. [33]

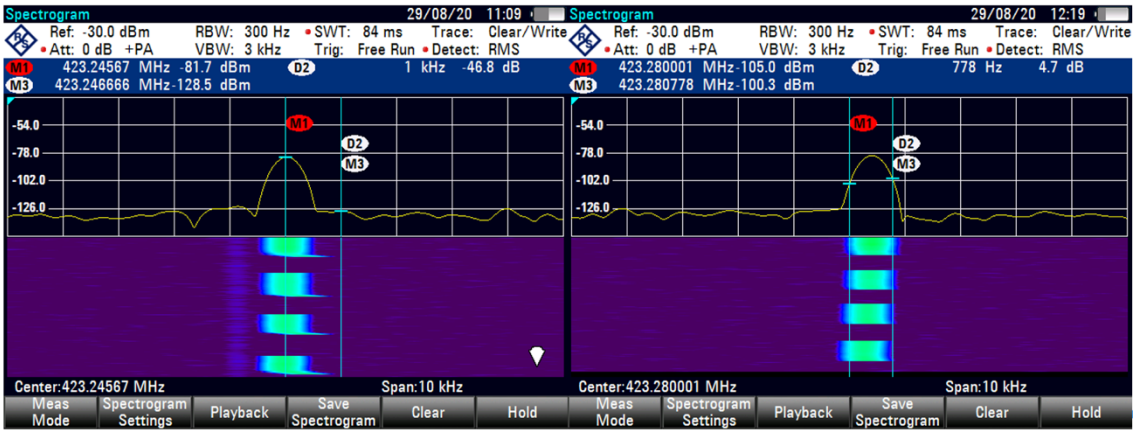
A POI a rádióspektrum-monitor rendszerek egyik meghatározó minőségi jellemzője, amely közvetlen hatással az RF-alapú biztonságtechnikai felderítési képességére. A védett objektumok esetében különösen indokolt olyan rendszerek alkalmazása, amelyek a rövid és nem előre jelezhető jelenségek rögzítésére is alkalmasak, minimalizálva a detektálás nélküli időszakok előfordulását.

3.3.5.2 Vevők detektálása, mintázatok azonosítása

Méréseket végeztem a vevőmodulok indulási folyamataiban jelentkező eltérések feltárása érdekében, valamint a folyamatos működés során tapasztalt különbségekkel kapcsolatban.

A következő ábrán két RXB8-as modul többször, egymás utáni bekapcsolás spektogramja látható, amely mérésnek a célja a PLL[68]-beállás mintázatainak rögzítése volt.

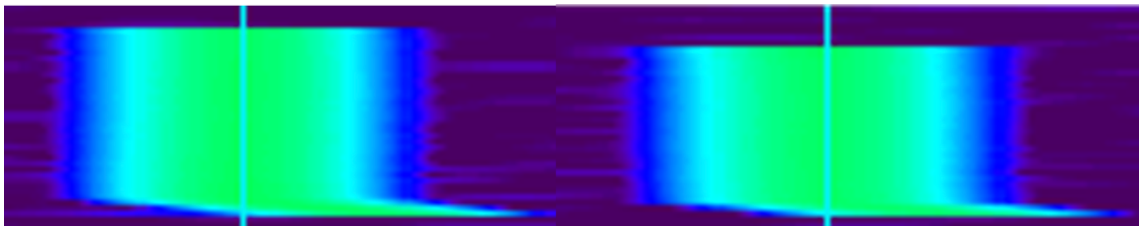
[67] Probability of Intercept – jel „elkapás” valószínűsége
[68] Phase-Locked Loop – Fáziszárt hurok



27. ábra A bekapcsolás pillanatának rögzítése

Az ábra baloldali részén lévő spektogramon látható indulási folyamat, szélesebb frekvenciasávban játszódik le, mint a jobb oldalon látszó másik vevőmodul bekapcsolása esetében. Ez a jelenség a zöld színű jel, jobb oldalán látható kicsúcsosodás alapján azonosítható, ahol egy kicsit nagyobb frekvencia mérhető a bekapcsolás pillanatában, majd a fáziszárt hurok szabályozásának hatására minimális csökkenést követően, beáll a tényleges értékre.

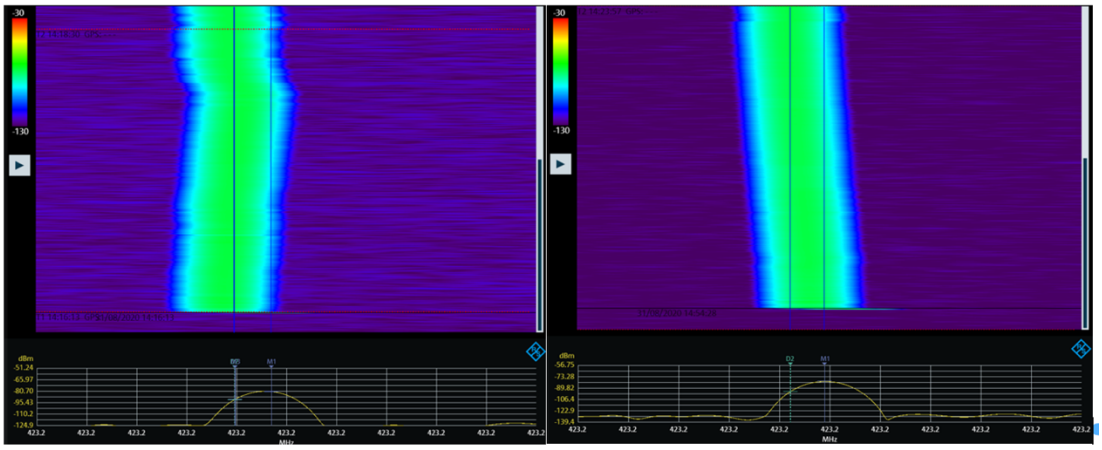
A modulok bekapcsolásuk során tapasztalt jellegzetességeinek és egyedi azonosíthatóságának a vizsgálata MATLAB segítségével (Függelék – 2. melléklet HTML).



28. ábra 2 vevőegység bekapcsolási pillanatáról készült spektogramjának összehasonlítása

A mérést követően a spektogramból kivágott jeleknek a PLL-beállását (egyedi azonosító jegyek megállapítása céljából) elemeztem pixel szinten. A látszólag egyforma indulási képek a valóságban mindig mutattak eltérést két modul összehasonlításakor.

A következő spektogram összehasonlítás a szabályozókörök beállása közötti eltérést hivatott szemléltetni. Szándékosan választottam két abszolút eltérő folyamatot ábrázoló képet, hogy érzékeltessem egy megfelelő felbontási képességgel rendelkező jelfeldolgozó rendszernek ez nem jelenthet kihívást.



29. ábra A PLL szabályozó kör bekapcsolást követő spektogramja

A vevőmodul bekapcsolása során a fáziszárt hurok beállásának a folyamatát rögzítettem egy spektrumanalizátorral abból a célból, hogy láthatóvá tegyem a két azonos típusú - de az alkatrészek paramétereinek szórása következtében jelentkező eltéréseket produkáló – szabályozó kör működését, fél perces időtartamban. A mintázatból egyértelműen kitűnik a frekvencia-menet időbeni változásai közötti különbség a két vizsgált vevőmodul esetében.

3.3.6 RF-árnyékolás hatásfoka a védelem szempontjából

A külső jelek elleni védelem elengedhetetlen a hatékony RF-monitor rendszer működéséhez. A detektálás hatásfokának javítása érdekében a jel-zaj viszony arány mértékét kell növelnünk, ehhez szükségesek bizonyos rádiófrekvenciás szempontból árnyékoló hatású anyagok beépítése a védett térrészek esetében.

A térelválasztó és térelhatároló elemek építőanyagainál is számolni kell már a tervezési fázisban. A falburkolatok rádiófrekvenciás tulajdonságai is meghatározzák a csillapítás-, és a reflexió mértékét. A reflexiók csökkentése a sugárforrás helyének a pontos meghatározásában lehet segítségünkre.

A helyiségekbe bevezető gépészeti rendszerek csatlakozási pontjain (átvezetések), szükséges RF-szűrők beépítése, a csatolások következtében jelen lévő parazitajelek csökkentése érdekében. A gyakorlatban tapasztalható, hogy az épületekbe szerelt gyenge-, és erősáramú vezetékek, fém csőhálózatok mindegyike antennaként viselkednek, ezek erősítik a makró környezetből származó rádiófrekvenciás jeleket.

A rádiófrekvenciás árnyékoláshoz kapcsolódó külföldön megjelent újságcikk írt róla, hogy az EU kémbiztos-bunker építését tervezi, amely minden vonatkozásban függetlenné tehető a külső környezetben jelen levő rádióhálózatoktól. A belső tárgyaló helyiségek abszolút árnyékoltak lesznek, mint egy Faraday-kalitka kerül kialakításra, a kiegészítő

terekkel együtt. A cél egy olyan környezet kialakítása, ahol biztonságosan tudnak tárgyalni, titkos információkat megosztani anélkül, hogy információszivárgás történne. [37]

Az információbiztonsághoz kapcsolódóan az egyik leglényegesebb szempont, hogy kívülről ne lehessen detektálni az épületben zajló kommunikációból, az ott működő adatátviteli rendszerekből. Továbbá nem elhanyagolandó szempont az sem, hogy adott esetben a védett objektumba bejuttatott lehallgató eszköz ne tudjon kifelé kommunikálni. Az információszivárgási csatornák okozta kockázatok csökkentése érdekében szükséges a megfelelő rédiófrekvenciás árnyékolás kiépítése a kiemelten védett objektumok esetében.

3.4 rezsim szabályok

A legszigorúbb szabályok is annyit érnek, mint amennyit betartanak belőlük, ez vonatkozik az adott rezsim intézkedésekre is egyaránt. Hiába a folyamatos felügyelet a szigorú beléptetési szabályok, az árnyékolt terület, ha mégis bejuthatnak a védett térrészre olyan elektronikai berendezések, amelyek potenciális kockázatot jelenthetnek információvédelmi szempontból.

Ezek általában a védett vagy bizalmas jellegű tárgyalások alkalmával jelentkező problémakör, hogy a hétköznapi infokommunikációs berendezéseinket, valamint az egyéb elektronikai viselt eszközeinket nem hagyjuk a tárgyaló kívül. A zavaró jelek megnehezítik vagy fals pozitív jelzéseket generálhatnak az RF-monitor rendszer számára, amivel növelik a kockázatot egy esetleges információvédelmi-, robbantásos támadás időbeni felismerésében.

Az említett szabályok kiemelt fontossággal bírnak a technikai átvizsgálások során, amikor is a méréseket végző személyek nem viselhetnek elektronikai eszközöket (mobiltelefon, okosóra, digitális fülhallgató). A mérések során közvetlenül az ilyen jellegű berendezések által kisugárzott jeleket keresik, ezért az össze közelben elhelyezkedő elektronikus szerkezet zavarólag hat az hatékony munkavégzésre.

3.5 esettanulmányok – robbantások (Brighton, Ahman)

A két eset tökéletesen szemlélteti a védett személyekhez tartozó helyiségek, épületek átvizsgálásában rejlő kockázatokat, és egyben kihívásokat is, amelyek végeredménye

rámutatott a biztonsági rendszerekben rejlő hiányosságokra, a bekövetkezett merényletek által.

Az első esemény a brit miniszterelnök, Margaret Thatcher elleni robbantásos merénylet, amelyet az IRA hajtott végre Brightonban 1984. október 12-én hajnalban. A robbantószerkezetet a Grand Hotel lakosztályának a fürdőszoba falába rejtették, egy hónappal a tervezett elkövetés előtt. A robbanóanyag becsült súlya 50 kg volt, az indítószerkezet egy hosszú késleltetésű időzített működtető egység. A miniszterelnök asszony a fürdőszobájából a detonáció előtt néhány perccel lépett ki és ezzel kisebb sérülésekkel megúszta a merényletet. A robbanás következtében a hotel érintett részén, több emelet is leomlott, maga alá temetve a bent tartózkodókat. A támadásban öten vesztették életüket és több mint 30-an sebesültek meg a leomló törmelékek miatt. Az utólagos nyomozás kiderítette, hogy az elkövetők már az esemény bekövetkezése előtt szeptemberben beköltöztek álnéven a szállodai szobába, hogy megtelepítsék a kiszemelt fürdőszoba helyiséget. [38] A robbantás bekövetkezéséből adódik, hogy a miniszterelnök látogatását megelőzően a biztonsági tűzszerészátvizsgálás során nem sikerült felfedezni a falba rejtett improvizált robbanószerkezetet és ezzel kis híján - mulasztásból - a védett személy halálát okozták.

A második eset Groznijban 2004. május 10-én történt, a Dinamó stadionban tartott ünnepi koncerten. Felrobbantották Ahman Kadirov csecsen elnököt a korábbi felújítási munkálatok közben előre beépített robbanóeszközzel. A távirányítású IED-t közvetlenül a díszvendégek tribünje alá, a betonalapba rejtették. A robbanás következtében az elnökön kívül még négyen életüket vesztették - köztük egy gyermek - és megsebesült 56 ember a csecsenföldi orosz hadsereg parancsnokával együtt. A merényletet követően a biztosági erők hatástalanítottak még egy IED-t a helyszínen. [39] A bekövetkezett merénylet tényéből adódik, hogy ebben az esetben sem sikerült maradéktalanul végrehajtani a tűzszerészátvizsgálást, mivel egy állítólag három hónappal korábban, a védett személyek emelvénye alá beépített pokolgép okozta a robbanást. A feltételezhető mulasztást támasztja alá az a tény is, hogy a merényletet követően előkerült egy második „éles” IED is a felrobbantott emelvény közelében.

3.6 Az RF-monitor rendszer hatékonyságának mérése

A rádiófrekvenciás spektrumfelügyeleti rendszerek biztonságtechnikai alkalmazásában különös jelentőséggel bír a működésük objektív mérhetősége. A hatékonyság

értékeléséhez olyan teljesítmény-mutatók használata indokolt, amelyek az rádiófrekvenciás környezet változékonysága és a detekciós feladat komplexitása ellenére is alkalmasak összehasonlítható és dokumentálható eredmények szolgáltatására.
A legfontosabb RF-monitoring hatékonysági mutatók az alábbiak szerint definiálhatók:

- *Észlelési valószínűség*: amely megmutatja, hogy az adott spektrumanalizátor milyen eséllyel detektálja a rövid időtartamú vagy tranziens jeleket adott időtartományon és sávszélességen belül;
- *Spektrumanalizátor zajszintje*: amely meghatározza a legkisebb érzékelhető jel nagyságát (érzékenységi küszöb). A detektálási megbízhatóság szoros összefüggésben áll az érzékenységi küszöb értékével és a környezeti zajviszonyokkal;
- *Anomáliák detektálási aránya*: azoknak az észlelt RF-jelzéseknek az aránya, amelyek nem felelnek meg a lokálisan definiált frekvenciahasználati szabályoknak vagy rezsimelőírásoknak. Ez a mutató kulcsfontosságú a jogosulatlan RF-jelenségek kiszűrésében;
- *Reagálási idő*: a rendszer által detektált incidens és az operátori riasztás vagy naplózás közötti időtartam. Fontos jellemző dinamikus, valós idejű fenyegetettségkezelés esetén;
- *Lefedettség*: érzékelőhálózat frekvencia-idő lefedettségének hiányosságaiból fakadó detekciós hézagok aránya.

A hatékonysági-értékek rendszeres mérése és auditálása segíti a rendszer validálását, valamint lehetővé teszi a védelem fejlesztési irányainak meghatározását. A védelmi infrastruktúráiban működő RF-monitor alkalmazások esetében is alapvetés, hogy a rendszer teljesítményét kvantitatív módon kell értékelni.

3.7 Következtetések

A rádióspektrum ellenőrzésének integrálása a technikai átvizsgálások folyamatába ma már nem csupán javasolt, hanem elengedhetetlen követelménye a kiemelten védett objektumok információvédelmi és robbantás elleni biztonságának. A technológiai fejlődés következtében megjelent, egyre kisebb méretű és fejlettebb rádiófrekvenciás eszközök – különös tekintettel a távolról vezérelhető lehallgató és robbantószerkezetekre

– olyan új kihívásokat teremtenek, amelyek kizárólag fejlett, folyamatos és célirányos spektrumfigyelő rendszerekkel kezelhetők hatékonyan.

A vizsgálatok során megállapítást nyert, hogy a rádióspektrum-ellenőrző rendszerek – különösen az RF-monitor hálózatok – képessé tehetők a különféle anomáliák, parazita sugárzások, valamint nem engedélyezett vagy rejtett rádiófrekvenciás eszközök detektálására. Ezzel párhuzamosan a technikai átvizsgálások hatásfoka is jelentősen javítható, különösen, ha azok nem kizárólag eseti, hanem folyamatos spektrumfigyeléssel kiegészítve történnek. A TSCM tevékenységek során a rádióspektrum monitorozás kulcsszerepet tölt be az aktív és passzív védelmi elemek kiegészítéseként.
Továbbá megállapítható, hogy a spektrumelemzés hatékonyságát növelheti, ha már az objektum tervezési fázisában definiálják a rádiófrekvenciás védelmi kritériumokat. A zavarérzékeny környezetek, a védett tárgyalók vagy biztonsági központok esetében a megfelelő árnyékolás, RF-monitor rendszer integrációjával, hozzájárul az objektumvédelmi rendszer integrált biztonsági szintjének emeléséhez.

Összességében megállapítható, hogy a rádióspektrum ellenőrzése a technikai átvizsgálások során történő rendszerszintű alkalmazása, elengedhetetlen a komplex védelmi rendszer kiépítése során. A proaktív jellegéből adódóan, képes adaptívan reagálni az RF-fenyegetettség dinamikusan változó környezetére.

A fejezethez tartozó forráselemzés 2026. január 30-án zárult le.
A kutatási célkitűzéseim közül az III és IV-es számú hipotézist fejtettem ki ebben a fejezetben.

A III. fejezethez kapcsolódó kutatási eredményeimet a következő publikációkban osztottam meg:

- A spektrum-monitor rendszerek jelentősége az objektumvédelem területén [Biztonságtudományi Szemle, 2021, III. évf. 1. szám]
- Az IoT-s eszközökkel megjelenő lehetséges kockázatok az objektumvédelem területén [BEREK HETVEN, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar Biztonságtudományi Doktori Iskola, Budapest 2019. (43-55. old.), Budapest, 2019.]
- PROTECTION AGAINST LISTENING vs. INFORMATION LEAKAGE CHANNELS [Biztonságtudományi Szemle, 2022. IV. évf. 1. szám]

ÖSSZEGZETT KÖVETKEZTETÉSEK

Lehetséges új irányvonal kidolgozása az objektumvédelem ezen speciális területén, ami elsősorban a rendvédelem egy meghatározó részét képezi a biztonságtechnikai rendszerek tervezése és kiépítése során. Paradigmaváltásra van szükség a speciális technikai egységek feladatvégrehajtása során.

Új tudományos eredmények /

Az értekezés a különösen védett objektumok biztonságának új aspektusára – a rádióspektrum alapú biztonságtechnikai rendszer kiegészítésre – fókuszál, információvédelmi és robbantás elleni védelem szintjének növelése érdekében, és az alábbi tudományos eredményekkel járul hozzá a objektumvédelem technikai fejlődéséhez:

- Új szempontrendszer kidolgozása a rádióspektrum-ellenőrzés technikai integrációjára a komplex objektumvédelmi rendszerekben, különös tekintettel az RF-alapú improvizált robbanóeszközök (RC-, mobil- és időzített IED-k) detektálására.
- Működő RF-monitor architektúra és detekciós folyamatmodellek kidolgozása, amelyek képessé teszik a rendszeresített TSCM eljárások kiegészítését automatizált spektrum-felügyeleti elemekkel.
- Történeti és statisztikai alapú osztályozás és aránybecslés a nyílt forrású (pl. YouTube) videómegosztó platformokon megjelenő IED-indítási módokra (RC, mobil, időzített), ami új módszertani megközelítést kínál az információalapú kockázatelemzéshez.
- A TEMPEST szabályozási keret és a valós idejű RF-monitor integrált alkalmazásának elemzése az információvédelem szempontjából, különös tekintettel a parazita kisugárzások és elektromágneses szivárgások elleni védekezésre.
- Mérhető hatékonysági mutatók (KPI) meghatározása az RF-monitor rendszerek teljesítményének értékelésére, beleértve a spektrumhasználat anomália-detektálási arányát, és az operatív válaszidőt.

Ajánlások

A „Kiemelten védett objektumok komplex védelme különös tekintettel a rádiófrekvenciás spektrum ellenőrzésére” című értekezésemben megfogalmazott eredményeket további felhasználásra javaslom a következőkben felsorolt területeken:

- Az objektumvédelem területén dolgozó szakemberek képzéséhez, a meglévő biztonsági rendszerek felülvizsgálatához, a komplex védelem megvalósításához új beruházások esetén.
- Az értekezésemben elsődlegesen a polgári életben alkalmazott házi készítésű robbanószerkezetek felépítését és detektálhatóságát vizsgáltam, amely rávilágított egy egységes IED kategorizáló rendszer szükségességére, a civil területekhez kapcsolódóan is. Ebben kiemelt figyelmet kell fordítani az indítási módok technikai megvalósítására, felépítésére, amely adott esetben alkalmassá teheti az elkövető profilozásában való alkalmazhatóságára.
- A bombakutató és tűzszerész képzések tananyagában célszerű lenne szerepeltetni, az elektronikus indítású IED detektálási lehetőségei között, hogy a különböző vegyi ellenőrzések mellett nagy segítséget jelentene a fizikai átvizsgálások kiegészítéseként.

IRODALOMJEGYZÉK

[1] Magyarország, Arcanum Adatbázis Kiadó, „Arcanum,” Arcanum, Letöltés helye: https://www.arcanum.com/hu/online-kiadvanyok/Lexikonok-a-magyar-nyelv-ertelmezo-szotara-1BE8B/o-o-4243C/objektum-4249B/?list=eyJmaWx0ZXJzIjogeyJNVSI6IFsiTkZPX0xFWF9MZXhpa29ub2tfMUJFOEIiXX0sICJxdWVyeSI6ICJvYmpla3R1bSJ9. [Hozzáférés dátuma: 15. 07. 2022.]

[2] Dr. Berek Lajos, Dr. Berek Tamás, Berek László, „SZEMÉLY- ÉS VAGYONBIZTONSÁG,” Budapest, ÓE-BGK 3071, 2016., pp. 93-95.

[3] Dr. Berek Lajos, in *Biztonságtechnika*, Budapest, Nemzeti Közszolgálati Egyetem, 2014., pp. 4-6.

[4] ZnZ, „SZECURINFO.hu/Biztonságtechnikai szakportál,” 13. 08. 2014. Letöltés helye: https://www.securinfo.hu/termekek/beleptetorendszerek/1216-csucstechnologia-a-szemelyatvizsgalasban-ellenorzes-millimeteres-alapossaggal.html. [Hozzáférés dátuma: 14. 10. 2018.]

[5] Domján András, „Hadmérnök,” 09. 2017. Letöltés helye: http://hadmernok.hu/173_03_domjan.pdf. [Hozzáférés dátuma: 20. 12. 2017.].

[6] *1994. évi XXXIV. törvény a Rendőrségről.*

[7] *160/1996. (XI. 05.) Korm. rendelet a védett személyek és a kijelölt létesítmények védelméről.*

[8] *19/2013. (V. 17.) ORFK utasítás a Magyarország érdekei szempontjából különösen fontos személyek védelmének, a kijelölt létesítmények őrzésének rendőrségi feladatairól.*

[9] Dr. Nagy Tamás, „A rendőrség személyvédelmi feladatai – visszatekintés az elmúlt 10 évre,” Magyar Rendészet 2021/2. 177—187. DOI: 10.32577/mr.2021.2.11, 2021.

[10] *A Kormány 322/2022. (VIII. 18.) Korm. rendelete a védett személyek és a kijelölt létesítmények védelméről szóló 160/1996. (XI. 5.) Korm. rendelet módosításáról.*

[11] MTI, „Index.hu,” 15. 11. 2013. Letöltés helye: https://index.hu/kulfold/2013/11/15/ketszazezer_dokumentumot_szivarogtathatott_ki_snowden/. [Hozzáférés dátuma: 12. 04. 2017.]

[12] I. Black, „The Guardian,” 03. 03. 2003. Letöltés helye: https://www.theguardian.com/world/2003/mar/20/eu.politics. [Hozzáférés dátuma: 11. 10. 2018.]

[13] K. A. N. Bertrand, 09. 04. 2023. Letöltés helye: https://edition.cnn.com/2023/04/09/politics/pentagon-leaked-documents-us-spying-allies-foes/index.html. [Hozzáférés dátuma: 20. 10. 2024.]

[14] Dr Berek Tamás, Berek László, Dr. Berek Lajos, „Személy- Vagyonvbiztonság,” Budapest, Óbudai Egyetem Bánki donát Gépész és Biztonságtechnikai Mérnöki Kar, 2016., pp. 4-6. old.

[15] Domján András, „Építőipari beruházások biztosítása, kiemelten védett objektumok esetén, különös tekintettel a fenyegetettségre,” MŰSZAKI KATONAI KÖZLÖNY XXVIII. évfolyam, 3. szám, Budapest, 2018.

[16] Bodrácska Gyula, Berek Tamás, „Megelőző intézkedések szerepe a komplex vagyonvédelem területén, építőipari beruházások biztosítása során,” *Hadmérnök V. Évfolyam 1. Szám,* pp. pp. 18-20., 2010. Március.

[17] P. Grier, „Air & Space Forces Magazine,” 12. 09. 2012. Letöltés helye: https://www.airandspaceforces.com/PDF/MagazineArchive/Documents/2012/September%202012/0912embassy.pdf. [Hozzáférés dátuma: 22. 10. 2018.]

[18] *2012. évi C törvény a Büntető Törvénykönyvről*

[19] B. A. Jackson, „rand.org,” 02. 03. 2008.. . Letöltés helye: https://www.rand.org/pubs/monographs/MG626.html. [Hozzáférés dátuma: 11. 08. 2017.]

[20] A. H. Cordesman, „csis.org,” 16. 03. 2006. Letöltés helye: https://csis-website-prod.s3.amazonaws.com/s3fs-

public/legacy_files/files/media/csis/pubs/060316_iraqctlessons.pdf. [Hozzáférés dátuma: 20. 10. 2018.]

[21] H. W. Ott, „daskalakispiros.com," 2009. Letöltés helye: https://daskalakispiros.com/files/Ebooks/Electromagnetic%20Compatibility%20Engineering.pdf. [Hozzáférés dátuma: 21. 10. 2019.].

[22] M. G. H. Johnson, High-Speed Digital Design: A Handbook of Black Magic, New Jersey: Prentice Hall PTR, 1993.

[23] Hatala András, és Kelemen Ferenc Jegyzet a katonai robbanótestek szerkezetének és működésének megismeréséhez és megértéséhez, Budapest: Vitaliq, 2003.

[24] Eric Bogatin, SIGNAL AND POWER INTEGRITY– SIMPLIFIED, Third Edition: Pearson, 2018..

[25] J. J. A. K. J. M. N. P. M. P. T. P. T. S. J. W. Zbigniew Bielecki, „researchgate.net," 2012. Letöltés helye: https://www.researchgate.net/publication/259864564_Sensors_and_Systems_for_the_Detection_of_Explosive_Devices_-_An_Overview. [Hozzáférés dátuma: 20. 10. 2018.]

[26] L. B. M. B. A. W. F. Gregory Mogilevsky, „researchgate.net," 06. 2012. Letöltés helye: https://www.researchgate.net/publication/258387262_Raman_Spectroscopy_for_Homeland_Security_Applications. [Hozzáférés dátuma: 03. 11. 2020.]

[27] F. Törvényszék, „jogkodex.hu," július 2021. Letöltés helye: https://jogkodex.hu/doc/3789846. [Hozzáférés dátuma: 10. 11. 2025.]

[28] Karsai Krisztina, Nagykommentár a Büntető Törvénykönyvhöz, Budapest: Wolters Kluwer Hungary Kft., 2019.

[29] MTI, „Origo.hu," 06. 08. 2018. Letöltés helye: https://www.origo.hu/nagyvilag/20180806-tobbeket-orizetbe-vettek-a-venezuelai-elnok-elleni-sikertelen-merenyletet-kovetoen.html. [Hozzáférés dátuma: 12. 12. 2019.]

[30] MTI, „Origo.hu,” 10. 01. 2019. Letöltés helye: https://www.origo.hu/nagyvilag/20190110-jemenben-dronnal-tamadtak-egy-diszszemlere.html. [Hozzáférés dátuma: 20. 12. 2019.]

[31] R. I.-R. V.431-8, „Nomenclature of the frequency and wavelength bands used in telecommunications,” ITU, Geneva, 2015.

[32] TEKTRONIX, „TEK.com,” 2017. Letöltés helye: https://download.tek.com/document/37W_17249_6_Fundamentals_of_Real-Time_Spectrum_Analysis1.pdf. [Hozzáférés dátuma: 05. 10. 2022.]

[33] KEYSIGHT, „keysight.com,” 2023. Letöltés helye: https://www.keysight.com/us/en/assets/3123-1934/application-notes/Understanding-Probability-of-Intercept-in-Real-Time-Spectrum-Analysis.pdf. [Hozzáférés dátuma: 20. 12. 2024.]

[34] C. A. Balanis, Antenna Theory 4th Edition Analysis and Design, New Jersey: Wiley-Blackwell, 2016..

[35] dr. Tolnai János, „puskas.hu,”. Letöltés helye: https://www.puskas.hu/r_tanfolyam/antennak_tapvonalak.pdf. [Hozzáférés dátuma: 11. 10. 2020.]

[36] P. D. Turner, „intersecmag.co.uk,” 20. 02. 2020. Letöltés helye: http://www.intersecmag.co.uk/remote-control/. [Hozzáférés dátuma: 10. 06. 2020.]

[37] Andrew Rettman, Nikolaj Nielsen, „EUObserver,” 08. 07. 2022. Letöltés helye: https://euobserver.com/world/155479. [Hozzáférés dátuma: 14. 07. 2022.]

[38] G. McIntyre, „cstpv.wp.st-andrews.ac.uk,” 11. 01. 2024. Letöltés helye: https://cstpv.wp.st-andrews.ac.uk/files/2024/01/The-Iron-Lady-and-the-IRA.pdf. [Hozzáférés dátuma: 10. 10. 2025.]

[39] Vargyai Gyula „HADTÖRTÉNELMI LEVÉLTÁRI KIADVÁNYOK,” 2002. Letöltés helye: https://mek.oszk.hu/04900/04964/html/. [Hozzáférés dátuma: 10 10 2018]

RÖVIDÍTÉSJEGYZÉK

AC Alternating Current – váltakozó áram

C-IED Counter-Improvised Explosive Device – Improvizált robbanószerkezet elhárítás

CW Continous Wave – folyamatos jel

DC Direct Current – egyenáram

DSP Digital Signal Processing **-** digitális jelfeldolgozó processzor

EMSEC Emission Security – kisugárzás biztonság

ETA Euskadi ta Askatasuna - Baszkföld és Szabadság

IED Improvised Explosive Device – improvizált robbanó eszköz

IRA Irish Republican Army - Ír Köztársasági Hadsereg

ITU International Telecommunication Union - Nemzetközi Távközlési Egyesület

FFT Fast Fourier Transform – gyors Fourier-transzformáció

KR Készenléti Rendőrség

LP Logaritmus-periodikus antenna

NLJD Non-Linear Junction Detector – félvezető detektor

ORFK Országos Rendőr-főkapitányság

PLL Phase-Locked Loop – fáziszárt hurok

POD Probability Of Detection - az észlelés valószínűsége

POI Probability of Intercept – jel „elkapás” valószínűsége

QAM Quadrature Amplitude Modulation – kvadratúra amplitúdó moduláció

QPSK Quadrature Phase shift Keying – kvadratúra fázis billentyűzés

RBW Resolution Bandwith – felbontási sávszélesség

RCIED - Radio Controlled Improvised Explosive Device – rádióvezérlésű improvizált robbanószerkezet

RF - rádiófrekvenciás

SFTF Short-Time Fourier Transform - rövid idejű Fourier-transzformáció

SIGINT Signals Intelligence – jelhírszerzés

TEK Terrorelhárítási Központ

TEMPEST Kompromittáló kisugárzás elleni védelem

TSCM Technical Surveillance Counter Measures – technikai elhárítás

UNMAS United Nations Mine Action Service

TÁBLÁZATJEGYZÉK

1. számú táblázat

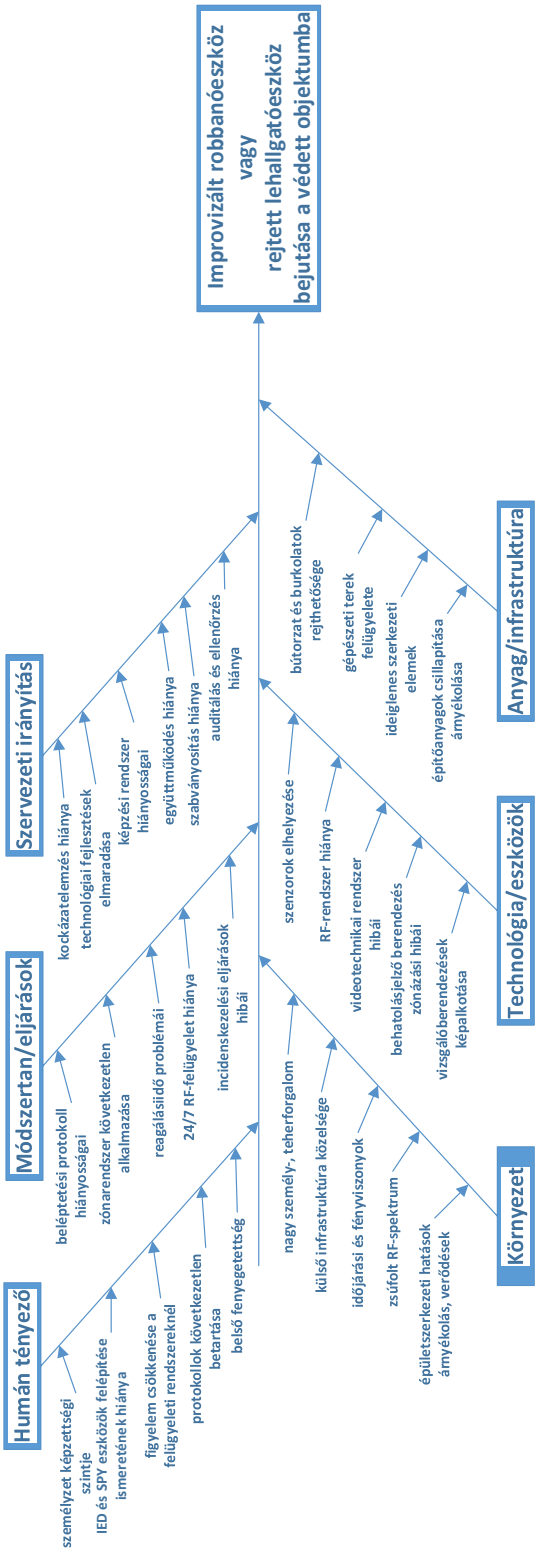
TÁVOLTÉRI MÉRÉSEK FSH8

távolság az RX modulról	1-es				2-es				3-as				4-es				5-ös				6-os				7-es				8-as				9-es				10-es			
[m]	omni [dBm]	omni S/N [dB]	HE_300 [dBm]	HE300 S/N [dB]	omni [dBm]	omni S/N [dB]	HE_300 [dBm]	HE300 S/N [dB]	omni [dBm]	omni S/N [dB]	HE_300 [dBm]	HE300 S/N [dB]	omni [dBm]	omni S/N [dB]	HE_300 [dBm]	HE300 S/N [dB]	omni [dBm]	omni S/N [dB]	HE_300 [dBm]	HE300 S/N [dB]	omni [dBm]	omni S/N [dB]	HE_300 [dBm]	HE300 S/N [dB]	omni [dBm]	omni S/N [dB]	HE_300 [dBm]	HE300 S/N [dB]	omni [dBm]	omni i S/N [dB]	HE_300 [dBm]	HE300 S/N [dB]	omni [dBm]	omni S/N [dB]	HE_300 [dBm]	HE300 S/N [dB]	omni [dBm]	omni S/N [dB]	HE_300 [dBm]	HE300 S/N [dB]
0,20	-57,10	63,10	-47,80	59,60	-53,20	62,50	-44,80	56,40	-51,20	60,60	-43,70	65,50	-51,00	64,40	-48,40	67,70	-54,70	64,90	-47,40	64,70	-56,70	57,90	-46,60	60,60	-52,70	57,70	-49,20	60,10	-52,30	61,00	-45,60	53,60	-59,80	59,30	-43,60	53,70	-54,40	58,20	-43,70	53,60
1,00	-75,50	52,20	-70,80	53,10	-74,40	59,40	-70,30	53,90	-69,80	56,80	-68,50	55,10	-70,20	66,10	-72,60	48,30	-74,70	55,10	-72,60	55,70	-70,30	60,40	-65,70	53,70	-70,20	59,10	-68,70	55,60	-70,50	58,70	-69,90	50,80	-74,20	60,70	-69,70	50,60	-72,30	59,60	-69,60	50,50
2,00	-92,90	38,50	-72,70	52,40	-90,50	44,30	-77,60	52,10	-83,80	59,50	-74,20	46,90	-87,90	46,30	-77,60	46,40	-94,30	42,70	-84,00	39,80	-86,30	48,00	-71,00	53,70	-83,90	48,30	-72,30	52,90	-83,10	57,40	-72,90	55,00	-83,00	52,50	-71,60	55,20	-83,80	48,90	-71,70	55,00
3,00	-94,00	37,90	-83,40	38,30	-95,30	33,70	-81,80	43,20	-93,70	40,00	-82,80	40,20	-86,90	43,90	-85,00	40,80	-96,10	31,60	-83,90	45,00	-96,70	31,00	-87,80	39,60	######	31,40	-86,40	40,80	-89,40	41,50	-82,90	45,50	-95,30	35,80	-82,80	45,20	-94,50	37,70	-82,70	45,10
4,00	-91,80	37,80	-83,90	43,50	-94,40	41,60	-77,30	52,70	-86,90	48,90	-78,90	48,20	-87,40	50,40	-84,20	42,30	-94,40	39,70	-87,40	36,80	-92,10	37,20	-75,60	49,80	-92,00	37,60	-77,80	44,60	-89,50	43,30	-78,80	48,30	-89,70	44,50	-79,10	48,30	-87,80	39,30	-79,20	48,40
5,00	-99,10	32,70	-86,70	46,90	-97,10	34,80	-79,90	45,90	-88,90	42,10	-81,80	43,70	-94,60	36,40	-85,30	40,10	-98,50	38,50	-83,90	48,20	-91,70	42,40	-86,70	44,50	-91,10	42,30	-86,10	41,70	-88,50	42,80	-88,30	39,90	-91,80	42,60	-88,20	39,80	-89,00	43,80	-88,10	39,70
6,00	-103,00	32,60	-95,40	34,80	-100,50	34,80	-94,20	35,90	-95,30	45,60	-92,00	38,40	-98,60	34,90	-94,60	32,70	-102,10	37,50	-104,30	27,80	-95,10	37,50	-92,20	39,70	-96,80	37,40	-97,60	31,30	-93,40	40,80	-91,70	34,90	-94,40	44,50	-90,90	34,60	-92,80	39,90	-90,80	34,50
7,00	-100,70	36,00	-90,10	36,90	-102,40	41,20	-89,90	34,80	-95,30	39,90	-92,90	41,00	-95,70	41,80	-101,20	29,10	-112,90	24,50	-94,40	39,60	-96,90	38,00	-89,80	38,00	-98,10	41,90	-92,50	41,80	-96,80	42,20	-90,10	42,70	-103,70	29,90	-89,90	42,50	-95,20	40,60	-89,80	42,50

ÁBRAJEGYZÉK

FÜGGELÉK

1. sz. melléklet – Ishikawa modell IED vagy rejtett SPY eszköz bejutása védett objektumba



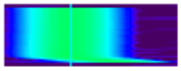
2. sz. melléklet – MATLAB szimuláció, spektogramok közötti különbség vizsgálata

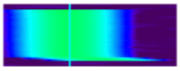
Képek beolvasása

```
img1 = imread('1_be_1_1.png');
img2 = imread('1_be_1_2.png');
```

Képek mutatása

```
figure
imshow(img1)
figure
imshow(img2)
```





Képek átkonvertálása fekete-fehér formátumra

```
img1BW = rgb2gray(img1);
img2BW = rgb2gray(img2);
```

Fekete-fehér képek bemutatása

```
figure
imshow(img1BW)
figure
imshow(img2BW)
```

A két kép kivonása egymásból

```
imgDiff = abs(img1BW - img2BW);
figure
imshow(imgDiff)
```

Információvédelmi Hatékonysági Mutatók (IHM) – RF-monitor rendszer méréséhez

Az alábbi táblázat egy strukturált mérési terv sablont mutat be, amely az RF-monitor rendszerre épülő információvédelmi hatékonysági mutatókat foglalja össze. A táblázat felsorolja az egyes IHM-ket, meghatározva nevüket céljukat, alkalmazási területüket, adatforrásukat, mérési gyakoriságukat, javasolt küszöbértéküket vagy döntési logikájukat, valamint a fontosabb megjegyzéseket és értelmezési tudnivalókat.

IHM neve	Mutató célja	Alkalmazási terület	Adatforrás	Mérési gyakoriság	Javasolt küszöbérték / döntési logika	Megjegyzés
Észlelési ráta (ÉR)	Annak mérése, hogy az RF-monitorozó rendszer az illetéktelen vagy gyanús rádiófrekvenciás jelek hány százalékát képes észlelni.	RF-monitor rendszer	RF-monitor rendszer naplófájljai és riportjai (észlelt események száma; tesztjeladók eredményei)	Folyamatos (real-time); havi/negyedéves értékelés	≥ 90%-os észlelési arány (ideális esetben közel 100%)	Ideális esetben 100%, de gyakorlatban 90% felett már megfelelő. Az értéket időszakos tesztsugárzásokkal célszerű ellenőrizni és kalibrálni.
Téves riasztási arány (TR)	Az összes riasztáson belül a téves (nem valós fenyegetést jelző) riasztások arányának meghatározása a rendszer megbízhatóságának jellemzésére.	RF-monitor rendszer	Riasztási logfájlok, operátori naplók (a riasztások utólagos minősítése; tévesnek bizonyult jelzések dokumentálása)	Folyamatos megfigyelés; havi értékelés	≤ 5% téves riasztási arány fenntartása	A túl sok téves riasztás erőforrást von el és gyengíti a rendszerbe vetett bizalmat. Magas érték esetén a monitorrendszer érzékenységét vagy szűrési beállításait módosítani kell a valódi fenyegetések jobb kiemelése érdekében.
Spektrum-lefedettség (%) (SL)	A monitorozott rádiófrekvencia-sávok és üzemidő lefedettségének mértéke – vagyis hogy a rendszer mennyire teljeskörűen figyeli a kijelölt spektrumot folyamatosan.	RF-monitor rendszer	Rendszer-riportok és konfigurációs adatok (lefedett frekvenciasávok listája; monitorozás üzemideje)	Folyamatos (24/7 rendszerüzem); havi összegzés	100% lefedettség a kritikus frekvenciasávokban; minimális holtidő	A monitorozásban fellépő bármely rés vagy kimaradás jelentősen csökkenti az észlelés valószínűségét. A lefedetlen frekvenciák vagy időablakok potenciális kihasználható rést jelentenek a fenyegetések számára, ezért minimalizálni kell őket.
Reagálási idő (RI)	A riasztás észlelése és az arra adott biztonsági reakció (beavatkozás) megkezdése közti idő mérése – a reagálási folyamat gyorsaságának jellemzésére.	Integrált (rendszer + személyzet)	Operátori napló és eseményjelentések (a riasztás időpontja és az intézkedés megkezdésének ideje)	Minden incidensnél rögzítve; havi átlagolás	Riasztást követően perceken belüli (pl. ≤ 5 perc) reagálás	A reagálási idő magában foglalja az észlelés és az első intézkedés közti intervallumot. 24/7 készenléti ügyelet és kidolgozott riasztási protokoll alkalmazása segít alacsonyan tartani. A gyors reagálás

3. sz. melléklet – RF-monitor rendszer hatékonyságának méréséhez segédlet 2.

IHM neve	Mutató célja	Alkalmazási terület	Adatforrás	Mérési gyakoriság	Javasolt küszöbérték / döntési logika	Megjegyzés
						csökkenti az incidensek hatását.
Kisugárzás-biztonság megfelelőségi arány (%) (KBM)	A védett berendezések és helyiségek azon hányada, amely megfelel a kompromittáló kisugárzás szabványoknak (kibocsátási határértékeknek), az információszivárgás elleni védelem szintjének mérésére.	kompromittáló kisugárzás elleni védelem	Kompromittáló kisugárzás minősítési jegyzőkönyvek; TSCM felmérési eredmények, árnyékolási tesztek, mérések	Éves vagy féléves auditok; eseti felülvizsgálatok	100% megfelelés a kritikus fontosságú berendezéseknél és helyiségeknél; összességében ≥ 95%	Bármely nem-megfelelőség kockázatot jelent, ezért azonosítása után mielőbbi intézkedés szükséges (pl. utólagos árnyékolás, eszközcseréje). A teljes körű megfelelés biztosítja, hogy az elektromágneses kisugárzás ne okozzon információszivárgást.
Kompromittáló kisugárzások észleléseinek száma (KKÉ)	A kompromittáló elektromágneses kisugárzások (pl. lehallgatást lehetővé tevő jelek, rejtett adóberendezések) észlelt eseményeinek száma egy adott időszakban.	RF-monitor rendszer	RF-monitor riasztási napló; TSCM jegyzőkönyvek (felderített rejtett adók vagy határérték feletti jelek listája)	Folyamatos megfigyelés; havi/negyedéves jelentés	0 (minden ilyen észlelés incidensnek minősül, azonnali kivizsgálást igényel)	Ideális esetben nem fordul elő ilyen esemény. Minden detektált kompromittáló jelenséget azonnal ki kell vizsgálni – lehet valódi lehallgatási kísérlet vagy ártalmatlan jelenség, de mindenképp intézkedést kíván. Ez biztosítja, hogy a fals riasztásokat kiszűrjék, a valódi fenyegetéseket pedig kezeljék.
Felülvizsgálati ütemterv betartása (%) (FVB)	Annak mérése, hogy a tervezett időszakos vizsgálatokat (pl. rendszeres TSCM vizsgálatok, auditok) az előírt gyakorisággal végrehajtják-e – ezzel biztosítva a védelem folyamatos fenntartását.	kisugárzás biztonság, kompromittáló kisugárzás elleni védelem	Karbantartási/ellenőrzési ütemterv és teljesítési jelentések; audit-nyilvántartások	Havi nyomon követes (az esedékes ellenőrzések megtörténtének vizsgálata)	100% (minden tervezett ellenőrzést időben el kell végezni)	Az ellenőrzések elmaradása vagy késedelme növeli a fel nem derített biztonsági rések és rejtett fenyegetések kockázatát. A rendszeres TSCM felülvizsgálatok betartása ütemezésének betartása kritikus a védelem szinten tartásához.

PUBLIKÁCIÓS JEGYZÉK

- **A kiemelten védett objektumok biztonsága a fenyegetettség tükrében**; HADMÉRNÖK XII. Évfolyam 3. szám – 2017. szeptember;
- **Építőipari beruházások biztosítása, kiemelten védett objektumok esetén, különös tekintettel a fenyegetettségre**; Műszaki Katonai Közlöny XXVIII. Évfolyam, 3. szám – 2018.;
- **Kiemelten védett objektumok robbantás elleni védelmének kiegészítése a biztonsági szint növelése érdekében**; Műszaki Katonai Közlöny XXIX. Évfolyam, 1. szám – 2019. március;
- **Az IoT-s eszközökkel megjelenő lehetséges kockázatok az objektumvédelem területén**; BEREK HETVEN, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar Biztonságtudományi Doktori Iskola, Budapest 2019. (43-55. old.) Budapest, 2019.;
- **A spektrum-monitor rendszerek jelentősége az objektumvédelem területén**; Biztonságtudományi Szemle, III. évf. 1. szám – 2021.;
- **"EVOLUTION" OF IMPROVISED EXPLOSIVE DEVICES (IED) IN THE LIGHT OF TECHNICAL DEVELOPMENT** - AZ IMPROVIZÁLT ROBBANÓESZKÖZÖK (IED) „EVOLÚCIÓJA” A TECHNIKAI FEJLŐDÉS SZEMSZÖGÉBŐL TEKINTVE Műszaki Katonai Közlöny 32. Évfolyam 1. szám 49–61. 2022.;
- **PROTECTION AGAINST LISTENING vs. INFORMATION LEAKAGE CHANNELS** - LEHALLGATÁS ELLENI VÉDELEM vs. INFORMÁCIÓSZIVÁRGÁSI-CSATORNÁK Biztonságtudományi Szemle IV. Évfolyam. 1. szám – 2022.

KÖSZÖNETNYILVÁNÍTÁS

Ezúton szeretném megköszönni Prof. Univ. Dr. Berek Lajos Tanár Úrnak azt a támogatást, segítséget és szeretetet, amit Tőle kaptam a képzés ideje alatt és a dolgozatom elkészítésével kapcsolatban. Köszönöm Tanár Úr, hittél bennem ez sokat jelentett számomra a munka során.

Köszönöm a többi Professzoromnak is a tanulmányaim ideje alatt átadott ismeretet és tudást, amelyek mind hozzájárultak a fejlődésemhez.

Szeretném továbbá megköszönni a családom által nyújtott segítséget és türelmet, hogy maradt elég időm az értekezés befejezéséhez.

Nagyon köszönöm mindenkinek!

Domján András

2025. április 06.