KARDOS TAMÁS ZSOLT

Az Egységes Digitális Rádió-távközlő Rendszer (EDR) továbbfejlesztési lehetőségei

The opportunities for the development of the Unified Digital Radio Communications System (EDR)

DOI: HTTPS://DOI.ORG/10.53793/RV.2021.3.2

Absztrakt

Kutatásom célja bemutatni az EDR rendszer (Egységes Digitális Rádió-távközlő Rendszer) továbbfejlesztési lehetőségeit a technológia és az elvárások tükrében. Irodalomkutatásommal az elmúlt évek hazai történéseit foglaltam össze, ezzel párhuzamosan bemutatva az 5. generációs mobilszolgáltatást és a meglévő EDR technológiát. Kutatásom alapján megállapítom, hogy az 5. generációs technológia képes kiszolgálni a készenléti szolgálatok által elvárt jövőálló mobilkommunikációs igényeket. Mivel több fázisban valósul meg ez az új technológia, adott a lehetőség, hogy az 5. generációs mobilszolgáltatás tervezése során szabványosításra kerüljön a készenléti mobilszolgáltatások által elvárt szintű szolgáltatás biztonság és megbízhatóság.

KULCSSZAVAK: EDR, SZÉLESSÁVÚ KÉSZENLÉTI KOMMUNIKÁCIÓ, 5G MOBILKOMMUNIKÁCIÓ.

Abstract

The aim of my research is to present the possibilities of further development of the EDR system (Unified Digital Radio Communications System) in the light of technology and expectations. With a literature research, I summarized the Hungarian events of recent years, in parallel, presenting the 5th generation mobile communication service and the existing EDR technology. Based on my research, 5th generation mobile communication technology is able to serve the future-proof mobile communication needs of Public Protection and Disaster Relief (PPDR) communication. As this new technology is implemented in several phases, there is an opportunity to standardize the aimed level of service reliability and security required by Public Protection and Disaster Relief during the design of the 5th generation mobile service.

KEYWORDS: UNIFIED DIGITAL RADIO COMMUNICATIONS SYSTEM (EDR), BROADBAND PUBLIC PROTECTION AND DISASTER RELIED (BB-PPDR), 5G MOBILE COMMUNICATION.

Miért szükséges szélessávú közrend- és katasztrófavédelmi rendszer?

Bevezetés

Az információs társadalom és a kritikus infrastruktúrákat veszélyeztető fenyegetések egyre nagyobb kihívások elé állítják a közrendvédelmi és katasztrófavédelmi, azaz a készenléti szolgálatokat. Ahhoz, hogy ezek a szervezetek minél hatékonyabban láthassák el feladatukat, szükséges, hogy az infokommunikációs hálózatuk is megfeleljen a mai kor magas követelményeinek.

Magyarországon jelenleg a kormányzati célú hálózatokról szóló 346/2010. (XII.28) Korm. rendelet alapján és az abban meghatározott jogosult szervezetek részére feladatellátásuk során a hang-, és korlátozott mértékben az adatátviteli képességet az országosan kiépített Egységes Digitális Rádió-távközlő hálózat (EDR) rendszer biztosítja. A Rendeletben szereplő definíció szerint az EDR, a Schengeni Megállapodás, a Schengenben 1990. június 19-en aláírt Végrehajtási Egyezménynek 132., illetve 44. cikkében meghatározott követelményeket kielégítő, az Európai Távközlési Szabványosítási Intézet szabványa szerint működő e digitális, nyalábolt (trönkölt), kormányzati célú rádióhálózat.

A rendszer kiépítése 2006-ra történt meg, TETRA (Trans-European Trunked Radio) alapon. A folyamatos hálózatfejlesztés eredményeképp ma kb. 350 bázisállomásból álló, IP átviteltechnikán alapuló országos lefedésű EDR hálózat áll rendelkezésre.

Az alábbi készenléti szervezetek használják az EDR rendszert: Belügyminisztérium, Országos Rendőr-főkapitányság, Büntetés-végrehajtás Országos Parancsnoksága, Nemzeti Közlekedési Hatóság, Magyar Honvédség, Országos Mentőszolgálat, Alkotmányvédelmi Hivatal, Nemzeti Élelmiszerlánc-biztonsági Hivatal, Országos Vízügyi Főigazgatóság, Országos Idegenrendészeti Főigazgatóság, Nemzeti Védelmi Szolgálat, Katonai Nemzetbiztonsági Szolgálat, Terrorelhárítási Központ, Nemzetbiztonsági Szakszolgálat, Országos Katasztrófavédelmi Főigazgatóság, Terrorelhárítási Információs és Bűnügyi Ellenőrző Központ, Információs Hivatal, Nemzeti Adó- és Vámhivatal. Továbbá az ágazati kijelölt létfontosságú rendszerelemek, a felsőküszöbértékű veszélyes üzemek és a nagy országos szolgáltatók veszélyhelyzeti kommunikációs rendszere. Ez utóbbi szolgáltatók önkéntes csatlakozása a Belügyminiszter engedélyével történhetett meg.

Az EDR rendszer bemutatása

Az EDR a TETRA technológiára épül, mely egy, a professzionális felhasználói igények kielégítésére alkalmas mobil hírközlő rendszer, szelektív és csoportkommunikációs beszéd és adatátviteli szolgáltatásokkal. Alkalmazhatóságát a fejlett digitális jelfeldolgozási eljárásokra épülő átviteltechnika által biztosított zavarcsökkentett összeköttetések létesítésének lehetősége, a magas rendelkezésre állás, a gyors hívásfelépítés (~0,5s), az információvédelmi megoldások, és számos egyéb járulékos szolgáltatás biztosítja.

A TETRA rendszer által nyújtott szolgáltatások – más hírközlő rendszerhez hasonlóan – három csoportba sorolhatók. A teleszolgáltatások a végfelhasználói rádióterminál segítségével vehetők igénybe (pl. beszédhívás), míg a hordozószolgáltatások eléréséhez valamilyen külső berendezés csatlakoztatására van szükség (pl. számítógép, GPS vevő). A kiegészítő szolgáltatások a teleszolgáltatásokat (vagy azok igénybevételének módját) változtatják meg, illetve egészítik ki.

Az egyéni (ONE-TO-ONE) -, csoport-, körözvény- és expressz (PUSH-TO-TALK) hívás a fentiek alapján a teleszolgáltatások csoportjába tartozik. A csoporthívás, mint a készenléti szervek beszédkommunikációjának legfontosabb platformja – a katonai alkalmazásoknál megszokott rádióháló szervezésű híradáshoz hasonlóan – egy félduplex megoldás. Ez annyit jelent, hogy egy csoportban egyidejűleg csak egyetlen tagállomás forgalmazhat, míg a továbbított információt a többi felhasználó hallgatja. A teljes TETRA hálózaton egyszerre akár több száz, egymástól teljesen független beszédcsoport is üzemelhet egymás zavarása nélkül, ami biztosítja a rendszert használó készenléti szervezetek és más felhasználói csoportok biztonságos híradását. Egy terminálra feltöltött beszédcsoportok közül a kezelő a csoportválasztó gomb (vagy menü) segítségével tudja kiválasztani a számára aktuálisan éppen szükségeset. A hálózatba definiált, megfelelő jogosultságokkal rendelkező diszpécser képes nagyon rövid idő alatt az egyes csoportok összekapcsolására (közös beszédcsoportba történő rendezésére), ami nagyban segíti – például egy katasztrófa esetén – a mentésben résztvevő különböző egységek (rendőrök, mentők, katonák stb.) közti együttműködést. (Ez a megoldás – az egységes európai szabványnak köszönhetően – nemzetközi feladatok együttműködési híradásának szervezésére is alkalmazható!) A felhasználó egyéni hívásokat – a hálózatban számára beállított jogosultságoknak megfelelően – kezdeményezhet (és fogadhat) akár saját csoporton belül, akár másik csoportba (TETRA), de lehetséges összeköttetés létrehozása egy másik alközponti szám, illetve nyilvános vezetékes-, vagy mobiltelefon előfizetői szám irányába is. Ebben az esetben a kommunikáció két felhasználó között zajlik, azt más tagállomás nem hallja. A tárcsázás megkönnyítését a beépített telefonkönyv mellett programozott gyorshívó gombok is segíthetik.

A kiegészítő szolgáltatások számos olyan lehetőséget is biztosítanak a nyilvános hírközlő rendszerek esetében megszokottak mellett (mint például hívásátirányítás, hívásvárakoztatás, hívástartás, hívástiltás, hívó fél azonosítás), melyek speciálisan a készenléti szervek igényeinek megfelelően kerültek kialakításra. A vészhívás funkció a bajba jutott felhasználó számára egyetlen gombnyomással elérhető, melynek következtében segélykérését a csoport összes tagállomása és a diszpécser is fogadja, akár a meglévő összeköttetések bontása árán is. A dinamikus csoport hozzárendelés segítségével lehetőség van arra, hogy a jogosultsággal rendelkező diszpécser a hálózaton keresztül, a technikailag arra alkalmas terminálokra újabb csoportokat programozzon, vagy adott feladat végrehajtása érdekében független csoportokban tevékenykedő felhasználókat közös csoportba szervezzen. (A feladat végrehajtását követően a feltöltött csoportokat a diszpécser törölheti.) A belehallgatás funkció segítségével a jogosultsággal rendelkező diszpécser betekintést nyerhet a saját felügyelete alá tartozó két felhasználó közti hívásba (azok tudomása nélkül), ezzel ellenőrizve például a forgalmazás szabályainak betartását. Hasonló szolgáltatás a környezet figyelés, melynek aktiválása esetén a jogosult diszpécser (parancsnok) a saját csoportjában bármely rádióterminált észrevétlenül adásra kapcsolhatja, így szerezve tudomást például egy

ipari baleset, vagy a valamilyen okból kifolyólag tevékenységében korlátozott felhasználó környezetében történtekről. Mind az áramkör-, mind pedig a csomagkapcsolt adatátvitellel, illetve a rövid adatokkal kapcsolatos szolgáltatások a hordozószolgáltatások csoportjába tartoznak. A TETRA hálózatokon hibajavító képesség szempontjából háromféle áramkörkapcsolt adatátvitel valósítható meg, úgymint a különösen védett 2,4 kbit/s, a védett 4,8 kbit/s és védelem nélküli 7,2 kbit/s sebességű. Ilyen jellegű összeköttetések esetén az átviteli csatorna a hívás idejére, a forgalomtól függetlenül lefoglalásra kerül, mely a hálózat áteresztőképességének szempontjából nem túl előnyös, ezért ezt a megoldást ritkán használják. A csomagkapcsolt adatátvitel rugalmasságának köszönhetően sokkal elterjedtebb megoldás, hiszen ebben az esetben a hívás ideje alatt ugyan folyamatos összeköttetés jön létre a logikai csatornán, a fizikai csatorna (7,2 kbit/s) azonban csak a tényleges forgalom függvényében kerül lefoglalásra. (A hibajavításról ebben az esetben az igénybevett alkalmazásnak kell gondoskodnia.) A rövid adatszolgáltatás négyféle hosszúságú üzenet (16, 32, 64, 2047 bit) továbbítására biztosít lehetőséget, melyek segítségével státuszüzenetek, GPS adatok és SMS üzenetek küldhetők. (Németh 2006)

Az EDR szélessávúsítás előkészítése

Az EDR hálózat nyújtotta hangalapú kommunikáción túl szükség lenne a készenléti szolgálatok feladatainak ellátásához az EDR hálózat korlátozott adatátviteli képességégének növelésére.

Magyarország Kormánya – összhangban az Európai Unió elvárásaival – az Egységes Digitális Rádiótávközlő rendszer szélessávú képességének továbbfejlesztéséről szóló 1854/2016. (XII. 27.) Korm. határozatban felkérte a belügyminisztert, hogy együttműködésben az érintettekkel készítsen megvalósíthatósági tanulmányt az EDR szélessávú képességének továbbfejlesztéséről, valamint felkérte a Nemzeti Média- és Hírközlési Hatóság (NMHH) Elnökét, hogy működjön közre a tanulmány elkészítésében. Az NMHH feladatául adta, hogy a szervezetnek biztosítani kell a szükséges frekvenciát és sávszélességet.

A megvalósíthatósági tanulmánynak az alábbi három fő kérdésben kellett irányt mutatnia:

1. A használandó frekvenciasáv kijelölésében;
2. A sávszélesség igényének meghatározásában;
3. A használandó üzleti/hálózati modell kérdésében (saját hálózat kiépítése vagy használata, vagy a kettő kombinációja).

Az NMHH a 2015. évi munkaterve alapján elvégezte a nemzeti igények feltárását, a hálózati és szolgáltatási modellekre vonatkozó elképzelések azonosítását.

1. A frekvenciasáv kérdése

A Schengeni Megállapodás Végrehajtási Egyezménye és a nemzetközi előírások alapján a 700 MHz-es sáv kerül definiálásra, mint a szélessávú PPDR rendszerek alapvető harmonizált spektruma azzal, hogy kiegészítőspektrum a 400 MHz-es sávban biztosítható.

Miért jó a 700 MHz-es sáv?

A sávra jellemző fizikai tulajdonságok lehetővé teszik nagy kiterjedésű területek költséghatékony lefedését, a 700 MHz-es frekvenciasávba eső spektrum egyszerre biztosítja az országos lefedettséget és a beltéri használatot. A 700 MHz-es sáv különös jelentőséggel bír az 5G megvalósítása szempontjából is. A 700 MHz-es sáv az úgynevezett 5G pionírsávok egyike. Ez az ITU (International Telecommunication Union) terminológiában bevezetett 5. generációs mobil technológia, elterjedtebb nevén az 5G egyik frekvenciasávja.

2. A sávszélesség kérdése

Megfogalmazásra került továbbá, hogy a BB PPDR rendszerekhez legalább 2x10 MHz

biztosítása szükséges.

A sávszélesség követelmény – a felhasználás módjából adódóan vizsgálva – a mindennapi műveletek, a nagy veszélyhelyzetek, a nyilvános események, illetve a katasztrófaelhárítás során fellépő adatátviteli igényt biztosítja. A spektrum és infrastruktúra követelmények többségét a napi műveletek – amelyeket rutinszerűen végeznek – határozzák meg. A nagyméretű szükséghelyzet és/vagy nyilvános esemény (olimpia, G8 csúcs stb.) esetén többlet erőforrás igény merülhet fel, tervezhetően. A katasztrófaelhárítási tevékenységek esetén – földrengés, szélvihar, áradás vagy fegyveres konfliktus esetén – ad-hoc hálózatokra, illetve megnövekedett sávszélesség igény azonnali kielégítésére van szükség, igen rövid idő alatt. (ECC Report 199 „A" 2013)

3. A használandó üzleti/hálózati modell kérdése

- Dedikált nemzeti szélessávú PPDR hálózat

Lehetőség a hálózatfelügyelet, lefedés-, kapacitás- és rendelkezésre állás, tervezés kézbentartására, valamint a nemzeti igények szerinti speciális funkciókkal és biztonsági intézkedésekkel való ellátásra;

- PPDR szolgáltatásnyújtás kereskedelmi hálózaton

Előnye: méretgazdaságosságból adódó üzemeltetési és fejlesztési költséghatékonyság;

Megoldandó: lefedés-, kapacitás- és rendelkezésre állás, priorizálási és biztonsági funkciók a mobilszolgáltatóval való szerződéses alapon;

- Hibrid megoldás

A dedikált szélessávú PPDR hálózat lefedettség és kapacitás korlátainak kiegészítése kereskedelmi hálózattal. Feltétele a nemzeti és nemzetközi roaming lehetősége a két hálózat között.

Úgy látszik, hogy mind a kijelölt frekvencia, mind a biztosítandó sávszélesség, mind a kereskedelmi modell az 4G/5G technológia használatát vetíti előre a szélessávú készenléti rendszerek megvalósítása esetében. A TETRA technológia helyett – mely kizárólag a készenléti szolgálatok igényeit figyelembe véve lett megtervezve – most egy nyílt és széleskörben használt mobiltávközlési technológiát kívánunk felhasználni. Ehhez szükséges megvizsgálni, hogy mely szempontokból tér el a kereskedelmi mobilhálózat használata a készenléti szervezetek által elvárt használattól. (1. táblázat)

Összehasonlítás	Általános használat	Készenléti használat
Szolgáltatási igények	Egyéni igények.	Ismerni a folyamatban lévő eseményeket, helyszíneket, átlátni az egységek, az állomány tevékenységét.
Optimalizálva	Az előfizető kiszolgálására.	A szervezet működésének támogatása, gyors válaszadás, hatékonyság, szükség esetén operatív információ nyújtása.
Adattárolás helye	Akár adatfelhőben, valahol a világban.	Csak kormányzati felhőben, minden adatot az országon belül, megbízhatóan védett környezetben kell tárolni.
Leggyakoribb kommunikációs típus	Személy-felhő között/személy-személy között.	PTT, csoportkommunikáció az operatív csoportokon belül beszédcsoport, videó csoport, adatcsoport.
Kommunikáció védelme	Alapszintű informatikai biztonság.	Magánhálózat (VPN), végpontok közötti titkosítás, készülék felügyelet, a teljes hálózat védelme, internetkapcsolat nincs engedélyezve.
Adatvédelem	Érzékeny személyi adatok és tartózkodási hely védelme.	Szolgálatban a követés, a tevékenység rögzítése mindig engedélyezett a személy elérhetősége, biztonsága és a hiteles tevékenysége miatt. A védett hálózatok és terminálok lehetővé teszik az érzékeny adatok zárt kezelését.
Elérhetőség	„Majd hívom újra…”	Azonnali elérhetőség, prioritásos hozzáférés.
Vizuális kommunikáció	A személy és a környezete látszik.	Feladatfüggő megjelenítés, információ továbbítása: hol van az állomány, a járművek, mi történik a műveleti területen?
Üzemeltetési biztonság	Üzleti alapon.	Elkülönített magánhálózat, autonóm üzem, minimum egynapos szünetmentes megtáplálás biztosítása rendszer szinten stb.
Lefedettség	Népsűrűség alapján.	Földrajzi területi lefedettség.
Beltéri lefedettség	Sűrűn látogatott helyszíneken.	Kockázatalapú, a műveleti helyszínek teljes lefedettsége.

1. táblázat: A kereskedelmi mobilhálózat és a készenléti hálózat elvárásainak összehasonlítása

Forrás: Merza, R. (2020) Kié a sávszélesség havária esetén?

Megfelelő az 5G?

Az EDR rendszer a világon sok helyen használt és bevált TETRA technológiát használja, mely zárt, publikusan nem elérhető eszközöket és technológiát biztosít. Ehhez képest, amennyiben az 5G technológia felhasználása mellett valósul meg a szélessávú készenléti rendszer, a következőkkel szembesülünk:

- Eddig zárt technológia, mely kiforrott, nem piaci kommersz HW-t használ, most a mindenki által használt hálózati eszközök és szoftverek felhasználása (végkészülék lehet speciális);
- Szabványosítás még folyamatban (5G), ellenben a régóta kiforrott, de emiatt elavult TETRA technológiával;
- Érzékeny és speciális információk továbbítása, pld. különleges adatok, melyek nem évülnek el, egy „publikus eszközön, hálózaton".

Ezek alapján megfelelő az 5G?

- Igen, épp a megfelelő időben jött és még időben vagyunk! – szabványosítás folyamatban még (következő fázisok);
- Megfelelő (pioneer) frekvencia, elegendő sávszélesség;
- Megbízhatóság és biztonság – 5G tervezési alapja!;
- Költségek csökkentése (készülék és hálózati oldalon) – több lehetséges szállító;
- Nagyobb függetlenség - több lehetséges szállító.

Az 5G biztonsági kihívásai és megfontolásai

Nagy változások történtek az információbiztonság, komputerbiztonság kapcsán az elmúlt években. Míg korábban a biztonság és a megbízhatóság nem volt alapvető cél, ma már elengedhetetlen egy rendszer teljes életciklusán keresztül, a tervezéstől a beszerzésen át, és az üzemeltetés során is alapvetően alárendelni folyamatainkat a biztonságnak. Az 5G – úgy gondolom – az első komplex telekommunikációs rendszer, mely ennek szellemében lett megtervezve és szabványosítva, ezáltal lehetőséget ad az alábbi, a teljes hálózati biztonságot lefedő megfontolásoknak:

- Átfogó és kockázatalapú biztonsági intézkedések;
- Szakadatlan folyamatnak tekinthető, mely magában foglalja:
- Beszállítók kiválasztását – hálózati elemek előállítását – hálózatok üzemeltetését (a teljes élettartam alatt);
- Nem technikai tényezők figyelembevételét – a beszállító kockázati profiljának kialakításakor;
- Nemzetbiztonsági szempontok figyelembevételét;
- Beszállítói lánc és beszállítótól való függés minimalizálását;
- Életcikluson átívelő biztonsági megfontolások figyelembe vételét a szabványosítás, fejlesztés, bevezetés és üzemeltetés során.

Az EDR szélessávúsításának jelenlegi helyzete és a fejlesztés iránya

Még 2019 során az 5G frekvenciák értékesítése megtörtént, de a hazai PPDR rendszer számára fenntartott 700 MHz-es sáv nem került értékesítésre. 2020 során több hazai szolgáltató is elindította kereskedelmi 5G szolgáltatását.

Az elkészült megvalósítási tanulmányt, a frekvenciagazdálkodási kérdésekben az NMHH-t, illetve az EDR-t üzemeltető Pro-M Zrt. véleményét is figyelembe véve az alábbi döntések születtek az EDR rendszer jövőbeli fejlesztéséről.

A Pro-M Zrt. középtávú fejlesztési stratégiája – az EDR evolúciós fejlődése

„A jelenleg meglévő szolgáltatás magas szintű biztosítása mellett elsődleges cél a hozzáadott értékkel bíró, magas rendelkezésre állású, prioritást biztosító készenléti szélessávú adatszolgáltatás bevezetése. A szélessávú szolgáltatások kiépítésével kapcsolatos külső tényezők rendelkezésre állása szempontjából a szolgáltatások evolúcióját két szakaszra osztják. Az elképzelt modell alapján a fejlesztés mindkét szakaszban a Pro-M Zrt. saját maghálózati infrastruktúrával nyújtja a szolgáltatást, amelyhez a készenléti igények teljesítése érdekében a meglévő rádiós hálózatok lefedettségét és kapacitásait magas hozzáadott értékkel optimálisan, maximálisan kihasználja. Első lépésként az EDR hangszolgáltatások szélessávú adatszolgáltatással történő kiegészítése (EDR 2.0), a jelenleg piacról igénybe vett szolgáltatások kormányzati körbe történő bevonásával. 2021-ig tervezett a saját maghálózati infrastruktúra építését, egyidejűleg szabályozott keretek között prioritást biztosítva a készenléti felhasználóknak a jelenleg rendelkezésre álló mobilrádiós infrastruktúrák használatával. Ennek során a Pro-M Zrt. a készenléti felhasználók számára titkosítási, központosított adatkezelési és végponti eszközmenedzsment szolgáltatásokat is nyújt. A következő fejlesztési fázis az előzőekre építve a jelenlegi TETRA hálózat integrációjával, szerves fejlődéssel egy önálló rádiós hálózat építését (EDR 3.0) célozza 2022-2025 időtávon, a nemzetközi szabványosítási folyamatok, valamint a hazai frekvencia allokációs

döntések várható meghozatala alapján, megfelelő forrás rendelkezésre állása esetén. A megépülő saját rádiós hálózat evolúciós átmenetet és folyamatosságot biztosít a szolgáltatások terén. A modell végső soron az állami rádiós hálózatra épül, kiegészítésként (helyi lefedettség és kapacitás célból) támaszkodik a publikus hálózatra." (Pro-M Zrt. 2019: https://www.pro-m.hu/Hirek/2019/ProMNews/)

Az üzemeltető Pro-M Zrt. tervei szerint a szélessávú készenléti rendszer az alábbi két fázisban valósul meg:

1. EDR 2.0 – Szélessávú adatszolgáltatás a TETRA hang mellett

A 2020-2022-es időszávban cél az egységesen magas biztonság, a rendelkezésre állás és a területi lefedés mellett a hibrid készenléti mobilhálózati modell megvalósítása, mely az adatszolgáltatásra szabványosított technológia (4G LTE) használatával, aggregált szabványosított frekvenciakészlet felhasználásával valósul meg. A kiemelt fontosságú biztonság mellett szabványos elterjedt műszaki megoldást használ, ezzel biztosítva a végkészülékek és a berendezések, valamint a hálózat kiépítésének költséghatékonyságát. Kiépítésre kerül a saját maghálózati (core) infrastruktúra, míg a rádióhálózat (RAN) esetében részben felhasználva a meglévő 4G/5G kereskedelmi mobilhálózatok hozzáférési hálózatát. Tervek szerint 2025-ig a TETRA technológián alapuló EDR 1.0 hálózat biztosítja a hang alapú készenléti szolgáltatást.

2. EDR 3.0 – Hang és adatszolgáltatás 3GPP szabványos szélessávú hálózaton (4G/5G)

2025-ig cél a megfelelő önálló, dedikált 4G/5G rádiós hálózat (RAN) kiépítése, a TETRA rádiós hálózat integrációja és a forgalom átterhelése elsődlegesen a dedikált rádiós hálózatra, a publikus rádiós hálózat igénybevétel fenntartása ad-hoc igények kielégítésére.

A megvalósítandó EDR3.0 rendszer biztonsági kérdései

A készenléti hangkommunikáció eddig egy zárt és kiforrott technológián alapult, mind a végkészülékek, mind a hálózat elemei, de még a használt titkosító algoritmus beszerzése is csak állami szervezetek monopóliuma volt. Ez mind alapvetően változik meg azáltal, hogy a technológia és a berendezések hozzáférhetősége piaci lesz, valamint a használt protokollok és titkosítás is széles körben ismertek lesznek. További kihívás a szolgáltatások körének bővülése, megjelenik az érzékeny adatok továbbításának szükségessége, valamint az információk élettartama is változik. Maga a technológia sem kiforrott teljes mértékben, valamint folyamatos fejlesztés fogja még évekig jellemezni.

A támadásoknak való kitettség is nő, és további potenciális belépési pontok jönnek létre a támadók számára: mivel az 5G hálózatok egyre inkább szoftvereken alapulnak, nőni fognak a nagyobb biztonsági résekkel kapcsolatos, például a beszállítók gyenge szoftverfejlesztési folyamataiból eredő kockázatok. Ezek megkönnyítenék a támadók számára a hátsó ajtók (backdoor) elhelyezését és a rosszindulatú hozzáférést a termékekhez, ugyanakkor megnehezítenék észlelésüket.

- Az 5G hálózatok architektúrájának új jellemzői és az új funkciók miatt bizonyos hálózati berendezések és hálózati funkciók – mint például a bázisállomások vagy a hálózatok kulcsfontosságú műszaki felügyeleti funkciói – egyre sebezhetőbbé válnak;
- A mobilhálózat-üzemeltetők beszállítóktól való függéséhez kapcsolódó kockázatok növekednek. Ennek következtében a támadók több támadási útvonalat használhatnak fel, és növekszik az ilyen támadások potenciális hatása;
- A beszállítók által elősegített támadásokkal szembeni fokozott kitettséggel összefüggésben különösen fontossá válik az egyes beszállítók kockázati profilja, amely alapján leszűrhető, hogy mekkora annak a valószínűsége, hogy a beszállító rosszindulatú befolyás alá kerüljön;
- A beszállítóktól való nagyobb függőségből eredő fokozott kockázat: az egyetlen szolgáltatótól való jelentős függés növeli a potenciális ellátási zavar veszélyét, amely például kereskedelmi fennakadásból és annak következményeiből adódhat. A nagy függőség súlyosbítja továbbá a gyengeség vagy sebezhetőség potenciális hatását, valamint annak támadók általi kihasználhatóságát, különösen abban az esetben, ha olyan beszállítót érint, amely magas szintű kockázatot jelent;
- A hálózatok rendelkezésre állását és integritását érintő fenyegetések fogják a legjelentősebb biztonsági problémát jelenteni, a bizalmas adatkezelés és a különleges érzékeny adatok védelme mellett e hálózatok integritása és rendelkezésre állása fogja felvetni a legnagyobb nemzetbiztonsági aggályokat. (ECC 2019)

Összefoglalás

A kormányhatározat alapján készült megvalósíthatósági tanulmány alapján megtett intézkedések segítségével biztosított frekvencia készlet és sávszélesség lehetőséget ad arra, hogy a legmodernebb mobiltávközlési platformon, az 5. generációs

mobilrendszer képességeit felhasználva, a folyamatban lévő szabványosítást kihasználva egy jövőálló, megbízható és biztonságos, valamit költséghatékony szélessávú közrendvédelmi rendszert hozhassunk létre. Vizsgálataim alapján az 5G rendszer architektúrája és átfogó biztonsági szemlélete miatt -akár kiegészítő intézkedésekkel- jó alapot biztosít a készenléti szolgálatok által elvárt megbízhatóságú és biztonságú mobiltávközlő rendszer megvalósításához.

Melléklet

Rövidítések

3GPP	The 3rd Generation Partnership Project
5GPP	The 5G Infrastructure Public Private Partnership
BB-PPDR	Broadband Public Protection and Disaster Recovery
CEPT	European Conference of Postal and Telecommunications Administrations
ECC	Electronic Communications Committee
EDR	Egységes Digitális Rádió-Távközlő Hálózat
ETSI	European Telecommunication Standardization Institute
GPS	Global Positioning System
GSM	Global System for Mobile Communication
GSMA	GSM Association
HTE	Hírközlési és Informatikai Tudományos Egyesület
ITU	International Telecommunication Union
NMHH	Nemzeti Média és Hírközlési Hatóság
PTT	Push-to-Talk
TCCA	The Critical Communication Association
TETRA	Terrestrial Trunked Radio/Trans-European Trunked Radio
VPN	Virtual Private Network

Irodalomjegyzék

CEPT ECC Report 199 A. (2013) https://docdb.cept.org/download/35f6a2e2-1724/ECCREP199.PDF [Letöltve: 2021.07.30.].

Európai Bizottság (2019) Kérdések és Válaszok – A Bizottság közös uniós megközelítést szorgalmaz az 5G-hálózatok biztonsága tekintetében [2019. október 9-én aktualizált változat]. https://ec.europa.eu/commission/presscorner/detail/hu/MEMO_19_1833 [Letöltve: 2021.07.30.].

Merza, R. (2020) Kié a sávszélesség havária esetén? Előadás a THE INFOKOM 2020 konferencián. Kecskemét, 2020. november 18-20. https://www.hte.hu/documents/4652308/4684563/6_1_Merza_Roman.pdf [Letöltve: 2021.07.30.].

Németh, A. (2006) A katasztrófavédelmi kommunikáció alternatív megoldásai. In: Rajnai, Z. (szerk.) Kommunikáció 2006. Zrínyi Miklós Nemzetvédelmi Egyetem (Közszolgálati Egyetem) – HTE. pp. 237-239. https://www.puskashirbaje.hu/index_html_files/Kommunikacio_2006-NSZTK.pdf [Letöltve: 2021.07.30.].

Pro-M Zrt. középtávú fejlesztési stratégia (2019) https://www.pro-m.hu/Hirek/2019/ProMNews/ [Letöltve: 2021.07.30.].