

37. Országos Tudományos Diákköri Konferencia

Had- és Rendészettudományi Szekció

Budapest, 2025. április 22–24.

Nemzeti Köszolgálati Egyetem

Hadtudományi és Honvédtisztképző Kar

---

**A Magyar Honvédség hírközlési hálózatának fejlesztése:  
stratégiai, szabályozási és technológiai kihívások**

Jelige: *„Az információ hatalom”*

Pályamunka lezárásának időpontja: 2024. október

2025.

## Tartalomjegyzék

|     |                                                                                                                  |    |
|-----|------------------------------------------------------------------------------------------------------------------|----|
| 1   | Az állam és a közigazgatás szerepe a honvédelmi hálózatfejlesztés támogatásában.....                             | 3  |
| 1.1 | Magyar Kormány részvétele a hírközlőhálózat modernizálásában.....                                                | 4  |
| 1.2 | A Honvédelmi Minisztérium álláspontja a nemzetbiztonsági kihívások és a hazai védelmi fejlesztések kapcsán ..... | 7  |
| 1.3 | Korábbi fejlesztési programok .....                                                                              | 7  |
| 1.4 | A védelemgazdaság és a biztonságpolitika szerepe a hírközlési hálózatok fejlesztésében .....                     | 9  |
| 2   | A NATO elvárásai a gazdaság és az infrastruktúra védelmének támogatásában.....                                   | 9  |
| 2.1 | Védelmi kiadásokra vonatkozó adatok .....                                                                        | 10 |
| 2.2 | A NATO szabványok és a kommunikációs követelményeknek való megfelelés ....                                       | 13 |
| 2.3 | A szabványosítás folyamati Magyarországon.....                                                                   | 16 |
| 3   | A Magyar Honvédség Hírközlő hálózata .....                                                                       | 17 |
| 3.1 | Kommunikáció a honvédségben .....                                                                                | 18 |
| 3.2 | Zárt infokommunikációs hálózatok funkcionális csoportosítása .....                                               | 18 |
| 3.3 | Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózata.....                                              | 22 |
| 3.4 | MH szárazföldi tábori-harcászati rendszer.....                                                                   | 25 |
| 3.5 | MH KCEHH Stacioner hálózata .....                                                                                | 25 |
| 3.6 | Hírközlési hálózat továbbfejlesztési lehetőségei.....                                                            | 29 |
| 4   | LTE 450-es vezeték nélküli hálózat .....                                                                         | 31 |
| 4.1 | Az LTE hálózat eredeti célja és jövője.....                                                                      | 31 |
| 4.2 | A TETRA-hálózat elavultsága és az LTE450 lehetőségei .....                                                       | 35 |
| 5   | Az adatforgalom növekedése és a hálózatok kihívásai .....                                                        | 35 |
| 5.1 | Cloud computing.....                                                                                             | 36 |
| 5.2 | Edge computing.....                                                                                              | 36 |
| 5.3 | Hálózatok alkalmazkodása a cloud és edge computing-hoz .....                                                     | 37 |
| 5.4 | Az IoT és az IoBT .....                                                                                          | 37 |
| 5.5 | Az adatforgalom növekedésének kihívásai és megoldási lehetőségei .....                                           | 37 |

|     |                                                              |    |
|-----|--------------------------------------------------------------|----|
| 6   | Értékelés .....                                              | 38 |
| 6.1 | H1 hipotézis értékelése.....                                 | 38 |
| 6.2 | H2 hipotézis értékelése.....                                 | 39 |
| 7   | A vizsgálat összegzése és az kutatás végkövetkeztetései..... | 41 |
| 8   | Jegyzékek .....                                              | 42 |
| 8.1 | Ábrajegyzék .....                                            | 42 |
| 8.2 | Táblázatjegyzék.....                                         | 42 |
| 8.3 | Rövidítések jegyzéke.....                                    | 43 |
| 9   | Érintett jogszabályok.....                                   | 45 |
| 10  | Irodalomjegyzék.....                                         | 46 |

## **Bevezetés**

A kutatási téma a Magyar Honvédség hírközlés hálózatának vizsgálatára összpontosít, amelyben célom a honvédség távközlését biztosító hírközlési hálózatok korszerűsítése és modernizálási lehetőségeinek feltárása.

Gyakornoki munkavégzésem során volt lehetőségem elmélyülni a távközlési szektort érintő fejlesztési projekteken, amely során bebizonyosodott számomra ezen terület jelentősége. Nemcsak hazai szinten, de nemzetközi szinten is rendkívül nagy relevanciája van az érintett kérdéskörnek, hiszen számos Európai Unió (a továbbiakban: EU) és nemzetközi stratégia is kiemelt prioritással kezeli a távközlési szektorral kapcsolatos célkitűzéseket. Úgy gondolom, hogy a Magyar Honvédség (a továbbiakban: MH / honvédség) hírközlési hálózatának fejlesztése is rendkívül aktuális kérdés napjainkban és érdemes ennek a fejlesztésére is minél nagyobb figyelmet fordítani. Ehhez viszont elengedhetetlen a honvédségnél jelenleg is működő hírközlési hálózat vizsgálata, a fejlesztési lehetőségek feltérképezése, valamint a vezetékes és vezeték nélküli hálózat modernizációjával kapcsolatos koncepcióalkotás, figyelembe véve azt, hogy a műholdas kommunikáció nem tartozik a vizsgálat tárgykörébe.

A honvédség hírközlési hálózatának fejlesztését elengedhetetlennek tartom a 21. századi kihívásokra való felkészüléshez. Az elmúlt évek megpróbáltatásai (Covid 19 által okozott veszélyhelyzet, Orosz-Ukrán háború, migrációs nyomás, energia válság) hatására a biztonsági környezet teljes mértékben átalakult, a fejlett infrastruktúra és képességfejlesztés pedig hozzájárulhat az ütőképes és modern Magyar Honvédség kialakításához. A honvédség hírközlési hálózata kulcsszerepet játszik az ország védelmének megőrzésében és a biztonság fenntartásában. A katonai kommunikáció megerősítésében kiemelt szerepet tölt be a hírközlési technológiák modernizálása, hiszen a harci környezetben elengedhetetlen a gyors és hatékony kommunikáció és a megbízható információcsere. Célom, hogy a dolgozatom során tett megállapítások és javaslatok alkalmazhatóak legyenek a honvédség hírközlési hálózatának jövőbeni fejlesztése során, valamint, hogy a kutatás eredményei segítsék a védelmi stratégiák fejlesztését. Fontos azonban az, hogy ennek a fejlesztése összhangban legyen a gazdaságpolitikai és védelempolitikai célokkal, valamint az is kiemelt jelentőséggel bír, hogy a különböző vezetékes és vezeték nélküli technológiák korszerűsítése miként valósítható meg a biztonság és a hatékonyság jegyében.

Ebből adódóan kutatási tevékenységem során az alábbi kérdésre keresem a választ:

*Milyen módon korszerűsíthető a Magyar Honvédség elektronikus hírközlési hálózata úgy, hogy egyszerre feleljen meg a gazdasági hatékonyság, a technológiai fejlesztések mind a védelempolitikai célok követelményeinek?*

A NATO követelményeinek és a Honvédelmi Minisztérium elvárásainak érdekében, az MH hírközlési hálózatának fejlesztése megköveteli, hogy a 2014-es megállapodás alapján GDP 2%-át (Lunn and Williams, 2017) honvédelemre fordító beruházások egy részét telekommunikációs infrastruktúra fejlesztésre irányítsák. A sikeres katonai műveletek megvalósítása érdekében a hírközlési hálózat fejlesztését az alábbi két hipotézis köré építem:

*H1: A magyar honvédség kommunikációs céljainak megvalósítása többségében új hálózatok építése nélkül, a meglévő hálózatok felhasználásával is biztonságos és költséghatékony módon megvalósítható.*

*H2: Az LTE 450-es mobilhálózat a Magyar Honvédség műholdas kommunikációján túlmenően nem lesz önmagában képes biztosítani a vezetékek nélküli kommunikációs igényeket, annak fejlesztéséhez csak részben tud majd hozzájárulni.*

Kutatási céljaim elérése érdekében főként kvalitatív kutatási módszereket alkalmaztam, a későbbi kvantitatív kutatás megalapozásához:

- Tanulmányoztam a Magyar Honvédség hírközlési hálózatát és fejlődéstörténetét.
- Felkutattam és feldolgoztam a témához kapcsolódó szakirodalmat, szabályzatokat, tudományos szócikket, közleményeket és értekezéseket.
- A rendelkezésemre álló információkat strukturáltam, feldolgoztam, majd másodelemzést végeztem.
- Számadatokat, grafikus ábrázolásokat és vizuális eszközöket alkalmaztam az adatok szemléltetése érdekében.
- Megvizsgáltam a nemzetközi szabványoknak való megfelelési szempontokat.
- Feltérképeztem a hírközlési infrastruktúra fejlesztési irányainak és innovatív megoldásainak lehetséges irányvonalait.
- A kutatási területemhez tartozó szakemberekkel folyamatos konzultációt folytattam.

## **1 Az állam és a közigazgatás szerepe a honvédelmi hálózatfejlesztés támogatásában**

Jelen vizsgált hírközlőhálózat alanya a Magyar Honvédség. A Magyar Honvédség fegyveres állami szervezet, amely polgári irányítás alatt álló központi parancsoki rendszerben működik. Fő feladatát Magyarország Alaptörvényének 45. cikk első bekezdése taglalja: *„Magyarország fegyveres ereje a Magyar Honvédség. A Magyar Honvédség alapvető feladata Magyarország függetlenségének, területi épségének és határainak katonai védelme, nemzetközi szerződésből eredő közös védelmi és békefenntartó feladatok ellátása, valamint a nemzetközi jog szabályaival összhangban humanitárius tevékenység végzése.”* Ezen kívül az Észak-atlanti Szerződés értelmében (NATO, 2024b) a Magyar Honvédség kiemelt feladatai közé tartozik a NATO politikai és katonai szövetségének védelme, amelynek Magyarország 1999. március 12-e óta teljes jogú tagja (Magyar Nemzet, 2022).

A közigazgatás egyik kiemelt feladata annak megszervezése, hogy a honvédség számára rendelkezésre álljanak a szükséges erőforrások. Fontos, hogy a honvédelemben részt vevő állampolgárok megfelelően fel legyenek készítve a katonai szolgálat eredményessége érdekében, valamint az anyagi eszközök készenlétbe helyezéséről is gondoskodni kell, mivel ez nélkülözhetetlen az ország védelmének megőrzése szempontjából. Jelen tárgyalt kutatási kérdés tekintetében az utóbb említett közigazgatási feladat részletezése érdekelt. Fontos, hogy a honvédelem során alkalmazott védelmi eszközök céljuknak megfelelő állapotban legyenek, annak érdekében, hogy a háború kitörése vagy védelmi beavatkozás idején azonnal használhatóak legyenek. Ezeket az elvárásokat már a békeidő során biztosítani kell. A feladat biztosításához szükséges a kormányzati igazgatási szervek felkészítése, a honvédelmi tartalékok stratégiai kezelése, a hátországvédelmi szervezetek előkészítése, a nemzetgazdaság felkészítése, a lakosságot érhető anyagi javak minimalizálása, a szükséges anyagi javak igénybevétele felbecsülése, az állampolgárok személyi felkészítése, valamint a hadszíntér előkészítése. Kutatásom ezen része az utoljára említett részfeladat ismertetésére fókuszál. A hadszíntér-előkészítés rendkívül fontos, hiszen ez biztosítja az országterület védelmi jellegű előkészítését. Ide sorolható a műszaki létesítmények megjelölése, műszaki feltételek megteremtése és a hadműveleti alkalmazások alkalmassá tétele mellett a hírközlési hálózat optimálissá tétele is (Kaló et al., 2022).

### **1.1 Magyar Kormány részvétele a hírközlőhálózat modernizálásában**

Magyarországon három hatalmi ágot különíthetünk el, a törvényhozó hatalmi ágot, az igazságszolgáltatást és a végrehajtó hatalmat. A Kormány a végrehajtó hatalom csúcsszerve, melynek fő feladata az ország stratégiai irányvonalának meghatározása (Tóth, 2017). Magyarország Kormányának továbbá elsőrendű feladatát képezi a magyar állampolgárok biztonságának megőrzése és biztosítása, valamint minden eszközeivel támogatni kell az ország területének sérthetlenségét és területi integritását. A Kormány korábban meghatározott kiemelt prioritással kezelt fejlesztési területei között szerepel a Magyar Honvédség fejlesztése és modernizálása. Mindemellett a Kormány elkötelezettségét a haderő modernizálása mellett mi sem bizonyítja jobban, hogy az elmúlt két évtizedben az ország infokommunikációs szolgáltatásaihoz szükséges elektronikus hírközlőhálózat fejlesztése érdekében az Európai Unió társfinanszírozásával számos pályázat került támogatásra. Az infrastruktúra fejlesztése nem csak a MH részéről fontos, hanem szélesebb nemzetközi szempontból is ahogy azt a DESI (European Commission, 2024) szemléletmód is tükrözi.

#### *Szélessávú infrastruktúrafejlesztési pályázatok*

Az alábbi táblázat jól tükrözi azt, hogy az elmúlt 20 év során számos szélessávú infrastruktúra fejlesztés és támogatás valósult meg, amelynek eredményeként több tízezer kilométer hosszú nyomvonal került kialakításra. Ezeknek a fejlesztéseknek az összértéke, az adott évi árfolyami változásokat figyelmen kívül hagyva, hozzávetőleg 102 603 534 138 Ft volt. Ez a költségvetési keret jó kiindulópontja lehet a jövőbeni szélessávú infrastruktúra fejlesztések költségvetésének meghatározásában.

1. táblázat Szélessávú infrastruktúrafejlesztési pályázatok

| <b>Pályázati azonosító</b>                   | <b>Pályázat neve</b>                                                                                                                                      | <b>Megjelenés éve</b> | <b>Keretösszeg</b> |
|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------|
| <i>HHÁT 2</i><br>(Kis, 2017)                 | Szélessávú infrastruktúra-fejlesztés (szélessávú internethozzáférés megvalósítása)                                                                        | 2003                  | 737 043 000 HUF    |
| <i>HHÁT 3</i><br>(Kis, 2017)                 | Szélessávú infrastruktúra-fejlesztés (innovatív megoldások támogatásával)                                                                                 | 2003                  | 246 353 250 HUF    |
| <i>GVOP 4.4.1</i><br>(Kis, 2017)             | Szélessávú internet-infrastruktúra kiépítésének és a szolgáltatás beindításának támogatása Magyarország üzletileg kevésbé vonzó településein              | 2004                  | 2 020 384 678 HUF  |
| <i>GVOP 4.4.2</i><br>(Kis, 2017)             | Szélessávú internet-infrastruktúra fejlesztés (az önkormányzatok partner bevonásával tervezhették, építhették és tarthatják fenn a szélessávú hálózatot). | 2005                  | 10 724 604 270 HUF |
| <i>GOP 3.1.1.</i><br>(Kis, 2017)             | Hálózati infrastruktúra létrehozása                                                                                                                       | 2007                  | 3 017 881 784 HUF  |
| <i>GOP 3.1.2.</i><br>(PALYAZAT.gov.hu, 2012) | Szélessávú körzethálózati fejlesztések támogatása                                                                                                         | 2012                  | 20 000 000 000 HUF |
| <i>KMR_2016</i><br>(Pályázati Portál, 2017)  | Újgenerációs NGA és felhordó hálózatok fejlesztése a Közép-Magyarország Régióban                                                                          | 2016                  | 5 700 000 000 HUF  |

|                                                        |                                                                                                                                                      |      |                                |
|--------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|------|--------------------------------|
| <i>GINOP 3.4.1.</i><br><i>(PALYAZAT.gov.hu, 2024)</i>  | Újgenerációs NGA és felhordó hálózatok fejlesztése                                                                                                   | 2016 | 9 040 000 000 HUF <sup>1</sup> |
| <i>GINOP 3.4.2.</i><br><i>(PALYAZAT.gov.hu, 2022)</i>  | Intézmények hálózati hozzáféréseinek, kapcsolatainak fejlesztése                                                                                     | 2016 | 1 319 789 907 HUF              |
| <i>GINOP 3.4.3.</i><br><i>(KIFÜ, no date a)</i>        | Kormányzati hálózatok konszolidációja, kapacitásainak, teljesítményének növelése                                                                     | 2016 | 4 285 700 000 HUF              |
| <i>GINOP 3.4.5</i><br><i>(KIFÜ, no date b)</i>         | Kormányzati hálózatok konszolidációja, kapacitásainak, teljesítményének növelése és intézmények hálózati hozzáféréseinek, kapcsolatainak fejlesztése | 2017 | 4 730 000 000 HUF              |
| <i>GSM-R rendszer</i><br><i>(NISZ Zrt., no date a)</i> | GSM-R rendszer beszerzése és kapcsolódó szolgáltatások                                                                                               | 2016 | 9 566 316 866 HUF              |
| <i>NTG</i><br><i>(NISZ Zrt., no date b)</i>            | Nemzeti Távközlési Gerinchálózat                                                                                                                     | 2013 | 3 200 000 000 HUF              |

<sup>1</sup> Ez az összeg csak a pályázatok kezdetén volt ilyen mértékű: 2024-ig összességében már 65-68 milliárd Ft támogatást hívtak le. A pontos végösszeg egyelőre nem ismert, mivel az utolsó elszámolási kör igénylése jelenleg is folyamatban van az EU felé. Bár az érték ennél lényegesen magasabb, a dokumentum készítésekor a pontos adat még nem áll rendelkezésre.

## **1.2 A Honvédelmi Minisztérium álláspontja a nemzetbiztonsági kihívások és a hazai védelmi fejlesztések kapcsán**

2024 májusában írta alá a Honvédelmi Minisztérium (a továbbiakban: HM / minisztérium) és a Magyar Tudományos Akadémia (a továbbiakban: MTA) elnöke az együttműködésről szóló megállapodást, melynek fókuszában az áll, hogy a haderő fejlesztéséhez nélkülözhetetlen az MTA, illetve a tudományos körök támogatása. Szalay-Bobrovniczky Kristóf honvédelmi miniszter ennek okát is megjelölte, miszerint *„a veszélyek korában szükség van a haderő fejlesztésére, a társadalom ellenállóképességének megerősítésére, de ezt a fejlődő és átalakuló honvédség esetében csak a legmagasabb tudományos körök támogatásával tudják megtenni.”* A MTA által végzett kutatások széleskörűen hozzájárulnak az ország fejlődésén túlmenően az ország állampolgárainak érdekeinek szolgálásához, a honvédelem erősítéséhez és a biztonság megtartásához (MTI, 2024).

A Honvédelmi Minisztérium kiemelten támogatja a katonai hírközlés fejlesztését és korszerűsítését, hiszen ezek a modern honvédség alapját képezik. A fejlesztési javaslat nem csupán az információáramlást segíti elő a hadviselésben, hanem az operatív készségek fenntartásához is hozzájárul. A honvédség modernizálására és fejlesztésére 2016 óta helyez nagyobb hangsúlyt Magyarország, ennek részben egyik oka az európai védelmi képességének megerősítése, valamint az ország védelmi iparban való érvényesülése (MTI, 2022).

## **1.3 Korábbi fejlesztési programok**

Már a korábbi fejlesztési programok reagáltak a kihívásokra, de az elektronikus információs rendszerek tovább fejlődtek, és új struktúrákat hoztak létre. A *Nemzeti Kutatás-fejlesztési és Innovációs Stratégia 2020* összhangban áll a honvédség hírközlési hálózatának modernizálásával. A MH digitalizációs felzárkózása kulcsfontosságú, a stratégia pedig fontos alapot nyújthat a honvédség jövője szempontjából. A stratégia a technológiai és innovációs fejlesztésekre fókuszál, ez fontos lehet a katonai képességek nemzetközi standardokhoz igazításának, valamint a kommunikációs rendszerek fejlesztése szempontjából, amelyek elengedhetetlenek a hadviselés korszerűsítése érdekében (NKFIH, 2017).

A korábbi *Nemzeti Katonai Stratégia* is alapot nyújthat a Magyar Honvédség fejlesztéseire, hiszen már 2012-ben kihangsúlyozta a modern technológia jelentőségét, és külön fókuszot helyezett a hírközlési és kommunikációs műveletek fontosságára is. A stratégia továbbá kiemelte azt is, hogy a gyors információáramlás és a biztonságos kommunikáció elengedhetetlen a sikeres honvédelmi feladatok ellátásához. Ezek tükrözik, hogy a stratégia már 2012-ben előrevetítette a hírközlési infrastruktúra fejlesztési szükségességét (Honvédelmi Minisztérium, 2012).

A 2021-es Nemzeti Katonai Stratégia folytatja a 2012-es stratégia irányvonalát, hangsúlyozva a fejlett technológiát és a biztonságos kommunikáció fontosságát. Az új stratégia tovább erősíti a védelmi erők modernizációs célkitűzéseit alátámasztó kommunikációs infrastruktúra fejlesztését is (Honvédelmi Minisztérium, 2021).

Az említett stratégiák mellett a *Kormány Zrínyi Honvédelmi és Haderőfejlesztési Program* (a továbbiakban: Zrínyi 2026 HHP) keretében kívánja támogatni a haderő modernizálását, ennek költségvetése 3500 milliárd forint. A Zrínyi 2026 HHP nemcsak a jelentős technikai fejlesztéseket célozza meg, hanem a katonák létszámának 30 ezer főre, a tartalékos állomány kétezer főre emelését tervezi (B. Müller, 2018). A Zrínyi 2026 HHP átfogó célja a Magyar Honvédség digitális alapú modernizálása, amely lehetővé tenné a katonai és nemzetbiztonsági rendszerek külön-külön működését, amelyek támogatnák a kormány infokommunikációs feladatait. A program a digitális és hálózati rendszerek fejlesztésére összpontosít, beleértve a mesterséges intelligenciát, a robotikát és a kiberbiztonságot. Továbbá kiemelt céljai között szerepel a modern haditechnikai eszközök beszerzése, a katonák digitális felkészítése, valamint a légi és szárazföldi erők képességeinek növelése. A Zrínyi 2026 HHP részét képezi a fejlettebb logisztikai rendszerek kialakítása is (Babos *et al.*, 2021).

A Magyar Kormány a Honvédelmi Minisztérium útján támogatja a honvédséget. A haza biztonságának érdekében elismerik a katonák munkáját, biztosítják a szükséges munkakörülményeket, új életpályamodellt alkalmaznak, a magyar hadipart újraélesztése mellett tevékenykednek, továbbá modern technikai eszközökkel igyekeznek támogatni a honvédelem munkáját és fejlesztését. Ebből adódóan elmondható, hogy a honvédség hírközlési hálózatának fejlesztése is összhangban áll a kormány által elindított Zrínyi Honvédelmi és Haderőfejlesztési Programmal. Benkő Tibor korábbi honvédelmi miniszter megfogalmazta, hogy azért van szükség a honvédelem fejlesztésére, hogy *„e megváltozott biztonsági környezetben is mindig, minden körülmények között garantálni lehessen hazánk biztonságát.”* A program kifejti, hogy a magyar katonák széleskörű feladatainak ellátásához szükséges technikai eszközök fejlesztése is elengedhetetlen a honvédség fejlesztésének érdekében (Kormány Információ, 2019).

Ebből adódóan a program céljai közé tartozik a honvédség teljeskörű digitalizációja, valamint a vezetési és irányítási rendszer fejlesztése, melynek alapvető infrastruktúrája az MH Kormányzati Célú Elkülönült Hírközlő Hálózata (a továbbiakban: MH KCEHH).

#### **1.4 A védelemgazdaság és a biztonságpolitika szerepe a hírközlési hálózatok fejlesztésében**

A védelemgazdaság szerepe meghatározó a hírközlési hálózatok fejlesztésében, hiszen szerepe kiterjed a védelmi infrastruktúra, köztük a hírközlési hálózatok fejlesztésére is. Ezeknek a hálózatoknak a fejlesztése stratégiai fontosságú, hiszen ezek biztosítják a honvédség számára szükséges kommunikációs és információs rendszereket, a békeidőben, és a válsághelyzetben egyaránt. A védelemgazdaság finanszírozása, az erőforrások hatékony felhasználása és ezeknek a megtervezése szorosan összefügg a honvédség technológiai infrastruktúrájának fejlesztésével. A védelemgazdaság mellett a biztonságpolitika is átfogó keretet képez a nemzeti védelmi stratégia kialakításához, amely magába foglalja a hírközlési hálózatfejlesztést is. A külső fenyegetések és az ország biztonságát érintő kihívások közvetlen hatást gyakorolnak a hírközlési hálózatok stratégiai fontosságára, hiszen ezek a hálózatok nélkülözhetetlenek a nemzetvédelmi intézkedések koordinálásában, a gyors reakció biztosításában, valamint a hatékony kommunikáció fenntartásában a különböző biztonsági és védelmi helyzetekben.

A hírközlési hálózatok fejlesztése során jelentkező technológiai kihívások, mint például a kiberbiztonság, az adatvédelmi szempontok vagy a hálózatok modernizálása, szoros összefüggésben állnak a biztonságpolitikával. A biztonságpolitika keretein belül meghatározott célok és stratégiák alakítják a hírközlési hálózatok fejlesztésére vonatkozó szabályozási környezetet. A kutatás ezekre a kihívásokra és a megfelelő technológiai megoldásokra is koncentrálni, hiszen a hálózatok fejlesztése elengedhetetlen a védelemgazdaság és a nemzeti biztonság céljainak eléréséhez.

## **2 A NATO elvárásai a gazdaság és az infrastruktúra védelmének támogatásában**

A NATO, mint a világ legnagyobb katonai szövetsége, kiemelt figyelmet fordít a tagállamok gazdasági és infrastrukturális védelmére, mivel ezek alapvetően befolyásolják a közös biztonságot. A gazdasági és infrastrukturális rendszerek védelme mellett a kommunikációs és hírközlési hálózatok fejlesztése is alapvető fontosságú. A gyors, biztonságos és megbízható információáramlás elengedhetetlen a szövetségesek közötti hatékony együttműködéshez és a védekezéshez. A NATO is jelentős fejlesztéseket hajtott végre, hogy megfeleljen a modern kommunikációs követelményeknek és biztosítsa a rendszerek kompatibilitását.

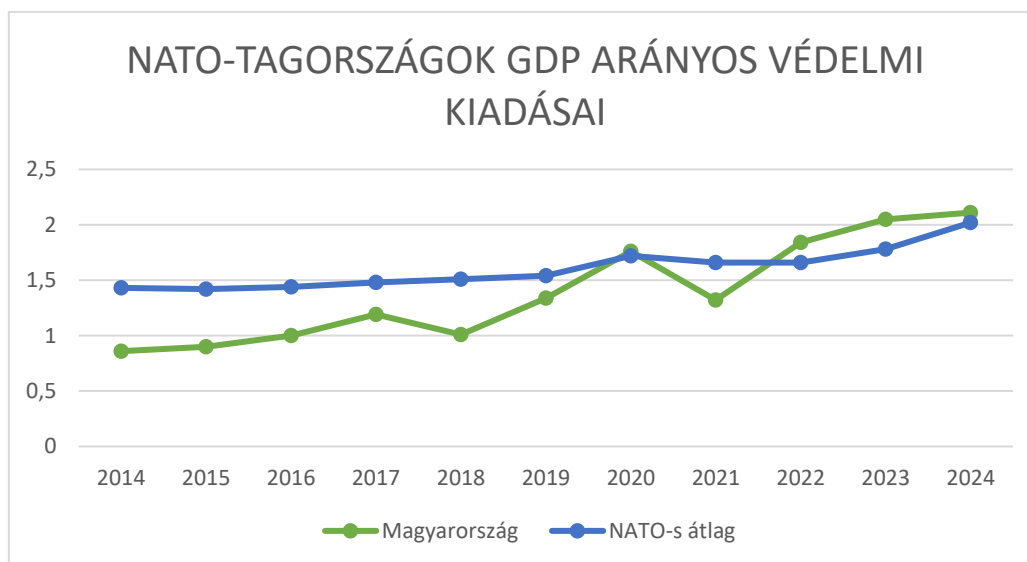
A NATO által támasztott elvárások, mint a védelmi kiadások biztosítása, a szabványosítás és a megfelelő kommunikációs infrastruktúra kiépítése, mind hozzájárulnak a gazdaság és az

infrastruktúra védelméhez. A hírközlési rendszerek fejlesztése nemcsak a hadsereg működését, hanem a civil és katonai integrációt is erősíti, elősegítve a gyors reagálást a válsághelyzetekben. A jelen fejezet célja, hogy bemutassa a NATO elvárásait a kommunikációs infrastruktúra terén, különös figyelmet fordítva a szabványoknak való megfelelésre és a jövőbeli fejlesztési lehetőségekre.

## 2.1 Védelmi kiadásokra vonatkozó adatok

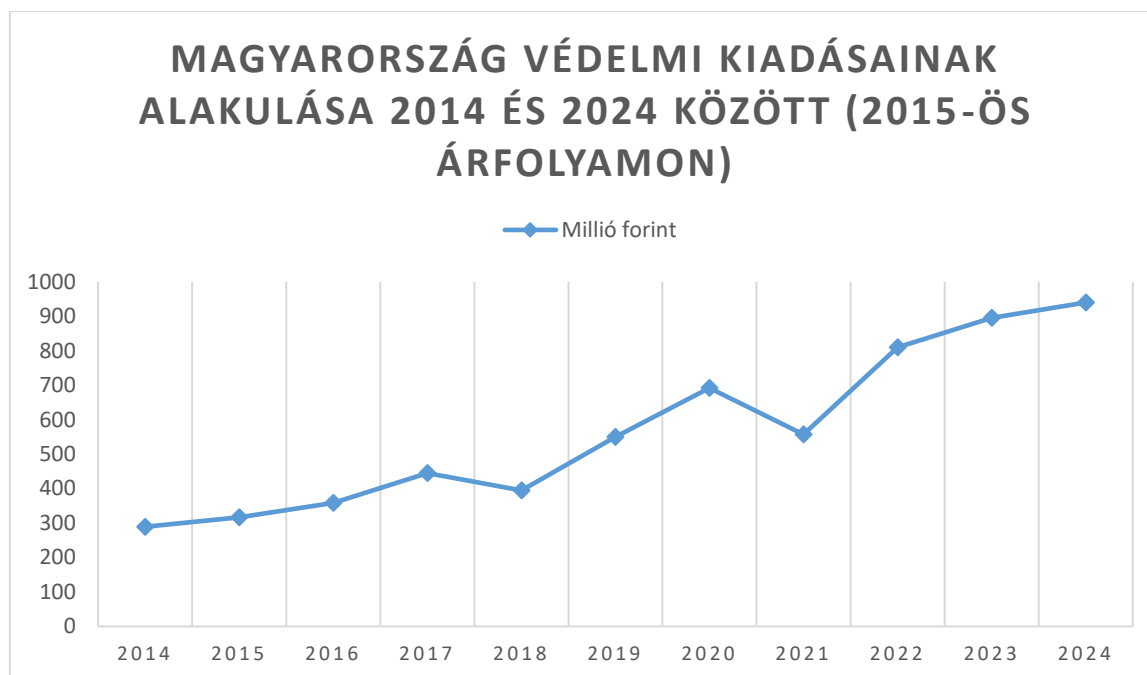
2014-ben a NATO tagállamai vállalták, hogy a védelmi kiadásaik 2024-re elérik az állami költségvetésük 2 százalékát, a katonai kiadások 20 százalékát pedig beszerzésekre és fejlesztésre fordítják. Zrínyi 2026 HHP célkitűzésként határozta meg az, hogy a védelmi kiadások 2024-re elérik a NATO 2 százalékos irányelvét, azonban ezt az elvárást Magyarország már 2023-ban sikeresen teljesítette:

*1. ábra NATO-tagországok GDP arányos védelmi kiadásai – saját szerkesztés (forrás: NATO Public Diplomacy Division, 2024)*



A NATO 2014-től kezdődően minden évben összegyűjti és rendszerezi a NATO tagjaira vonatkozó védelmi kiadásokkal kapcsolatos adatait. Ennek célja, hogy a szövetséges védelmi minisztériumok számot adjanak a tervezett jövőbeni védelmi kiadásokról. Ebben a fejezetben a NATO Európai Bizottság Gazdasági és Pénzügyi Főigazgatóságától (a továbbiakban: DG ECFIN) és a Gazdasági Együttműködési és Fejlesztési Szervezettől (a továbbiakban: OECD) származó gazdasági és demográfiai információkat használok fel elemzésem kiindulópontjaként (NATO Public Diplomacy Division, 2024).

2. ábra Magyarország védelmi kiadásainak alakulása 2014-2024 között 2015-ös árfolyamon-saját szerkesztés (forrás: NATO Public Diplomacy Division, 2024)



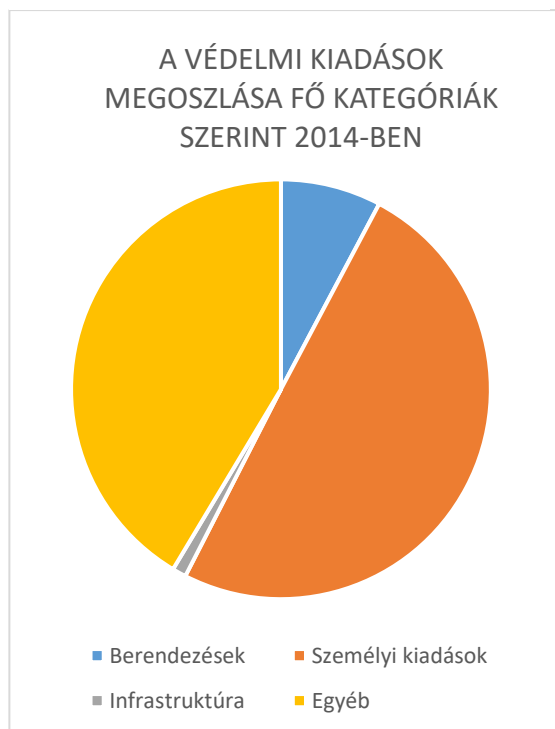
A diagramm jól tükrözi a védelmi kiadások növekedését az elmúlt 10 év vizsgálatában. 2014-ben a védelmi kiadások mértéke 289,213 millió forint volt, amely 2015-ös árfolyamon számolva, 2024-re 939,948 millió forintra növekedett, ez több, mint háromszoros növekedést jelent. 2018-ban és 2021-ben enyhe csökkenés látható, az elmúlt évek növekedéséhez képest. 2021-től kezdődően a védelmi kiadások mértéke ismét gyorsan növekedett, 2023-ban 895, 296 millió forint volt, 2024-re pedig 939,948 millió forintra becsülhető.

Az, hogy a védelmi kiadások mértéke a háromszorosára nőtt ez elmúlt egy évtizedben jól bizonyítja, hogy Magyarország reagál a NATO-kötelezettségeire, hiszen 2014 óta a céljuk a védelmi kiadások fokozatos növelése.

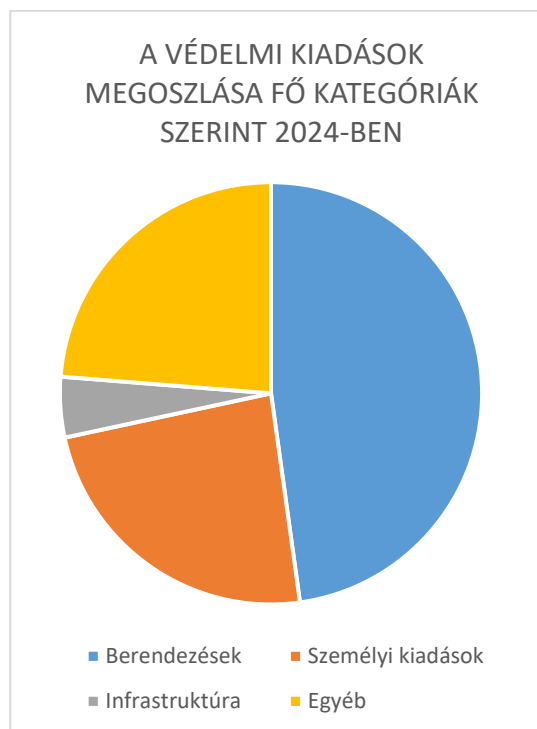
A következő ábra pedig a védelmi kiadások kategóriák szerinti megoszlását jeleníti meg. A védelmi kiadások összetétele jelentősen megváltozott 2014 és 2024 között. 2024-ben a berendezésekre szánt kiadások mértéke 47,81 százalék körül alakul. Ezen kiadások megnövekedése is jól tükrözi azt, hogy a katonai berendezések és az eszközök modernizációja a védelmi politika fő fókuszává vált. 2024-re a berendezések fejlesztésére szánt költségvetés csaknem a hatszorosára növekedett a 2014-es 7,76 százalékhoz képest (NATO Public Diplomacy Division, 2024). Az infrastruktúra aránya is növekedést mutat, azonban ennek mértéke még mindig alacsony a tervezett 4,63 százalékkal. Ezzel ellentétben a személyi kiadások aránya csaknem a fejlére csökkent ezen időszak alatt, valamint az egyéb kategória alá

eső kiadások is csökkennek, ami arra utalhat, hogy a kategória alá eső kiadásokat átcsoportosíthatták az infrastruktúra fejlesztéshez, vagy a beruházások alá.

4. ábra A védelmi kiadások megoszlása fő kategóriák szerint 2014-ben – saját szerkesztés (NATO Public Diplomacy Division, 2024).



3. ábra A védelmi kiadások megoszlása fő kategóriák szerint 2024-ben – saját szerkesztés (NATO Public Diplomacy Division, 2024).



2014 és 2022 között a NATO tagállamainak haderőinél jelentős növekedés volt megfigyelhető. Litvánia hadserege 2014-hez képest megduplázódott, 2022-ben a katonák létszáma elérte a 17,2 ezer főt. Ezt követte Lettország 63 százalékos növekedéssel, Csehország 33 százalékos növekedéssel, majd Lengyelország 23 százalékos növekedéssel. A honvédség növekedésének tekintetében Magyarország az 5. helyen áll a NATO tagállamain belül, hiszen haderejét 22 százalékkal növelte, ami 2022-ben 21,4 ezer főt jelentett. Ezekből az adatokból jól látható, hogy a Közép-Kelet európai országok jelentős mértékben megnövelték a haderejüket, feltehetően a régióban bekövetkezett geopolitikai változásokra reagálva. Ezek az országok a katonai létszámbővítés mellett jelentős modernizációt is végrehajtottak.

Az elmúlt években a NATO elvárásainak megfelelően a visegrádi országok is egyaránt fejlesztési projektekbe kezdtek a hadvédelmet illetően. Az országspecifikus tényezők miatt a fejlesztési ütemterveik sok mindenben eltérnek, azonban a Visegrádi Együttműködés (a továbbiakban: V4-es országok) országaira egyaránt jellemző, hogy a kiadások jelentős részét a katonai állomány növelésére, illetve a haderő fejlesztésére és modernizálására fordítják. Lengyelország hajtja végre a régió legnagyobb programját, hiszen 2035-re 123 milliárd eurót

kíván befektetni a honvédelem fejlesztésébe, míg Magyarország a második helyen 2026-ig 10 milliárd eurós programot kíván végrehajtani. Ezen országok mellett Szlovákia és Csehország is jelentős lépéseket tesz a NATO elvárásainak való megfelelésért, a modernizációért, hiszen az elkövetkezendő években ezen fejlesztési programok megvalósítása kulcsfontosságú lesz a Közép-Kelet európai biztonság megőrzése szempontjából (B. Müller, 2020).

## **2.2 A NATO szabványok és a kommunikációs követelményeknek való megfelelés**

A NATO-val való szoros együttműködés elengedhetetlen a honvédség hírközlésének fejlesztése szempontjából. Ennek fő oka az interoperabilitás kialakítása, amelyet a NATO szabványokhoz való alkalmazkodás tesz lehetővé. Ezeket a követelményeket szemlélteti jelen fejezet:

### *I. NATO Network Enabled Capability*

A NATO Network Enabled Capability (Farkas, 2020), azaz a NATO nyújtotta képesség (a továbbiakban: NNEC) a végrehajtók, az információgyűjtők és a döntéshozók összekapcsolásához járul hozzá, melynek célja, hogy létrejöjjön a szervezet hálózatalapú hadműveleti képessége. Az információs technológia biztosítja ezen műveleteknek az alapját. A sokrétű információáramlás biztonságos továbbításához nélkülözhetetlen egy megfelelő paraméterekkel ellátott híradó és informatikai rendszer. Tőreki Ákos már 2010-ben megfogalmazta „*A Magyar Honvédség stacioner kommunikációs rendszerének vizsgálata*” nevezetű tanulmánya során, hogy a Szövetségi műveletekben és a NATO rendszereihez való csatlakozás során történő hatékonyabb részvétel érdekében a fejlesztéseket a hálózatalapú megoldások irányába kell tovább vinni (Tőreki, 2010).

### *II. STANAG*

A Standardization Agreement (a továbbiakban: STANAG) a NATO tagországai közötti szabványosítási megállapodásokat jelenti (Khan *et al.*, 2021). Feladata, hogy egységesítse a katonai műveletek során használt folyamatokat, rendszereket és eszközöket, ezzel biztosítva az interoperabilitást. Az előírt szabványok alkalmazása hozzájárul a reakcióidő csökkentéséhez és a műveleti költségek optimalizálásához, ezáltal növelve a NATO műveleti hatékonyságát.

A STANAG-ok kiterjednek a technikai és működési szabványokra, például a fegyverek kaliberére, vagy a kommunikációs eljárásokra és azok titkosításra. A NATO Szabványosítási Dokumentumok Adatbázisa (a továbbiakban: NSDD) tartalmazza az összes kapcsolódó dokumentumot és nemzeti ratifikációs információt.

A NATO Szabványügyi Hivatala (a továbbiakban: NSO) is kulcsszerepet játszik a szabványosítási folyamatok koordinálásában, különösen a NATO Védelmi Tervezési Folyamat (a továbbiakban: NDPP) támogatásában, amely a szövetséges erők közötti interoperabilitás

növelését célozza. A NATO terminológiát a NATOTerm (*NATO Term - CIMIC-COE*, no date) adatbázis kezeli, amely több mint tízezer meghatározást tartalmaz.

Összességében a STANAG-ok és egyéb szabványosítási eszközök alapvetőek a NATO többnemzetiségű erőinek sikeres működéséhez (NATO OTAN, 2022).

### III. NATO CIS

A Communication and Information Systems (a továbbiakban: CIS) célja a kommunikációs és információs rendszerek tagállamok közötti összehangolása (Bihun *et al.*, 2019). A nemzetek által telepített kommunikációs modulok (a továbbiakban: DCM-ek) integrált hálózatot alkotnak, amely támogatja a NATO műveleteinek sikerét. Az ábra az NCISG struktúráját jeleníti meg, amely parancsnoki rendszerben működik:

5. ábra NCISG struktúra (forrás: <https://ncisg.nato.int/about-us>)



A NATO Signal Battalion (a továbbiakban: NSB) olyan szakosodott katonai egység, amely kulcsszerepet játszik a katonai kommunikációs és információs rendszerek (a továbbiakban: CIS) támogatásában. Feladata, hogy megbízható és biztonságos kommunikációt biztosítson a NATO műveleteiben, lehetővé téve a gyors és hatékony irányítást. Az NSB szakértelme nélkülözhetetlen a műveletek sikeres végrehajtásához. Mindhárom zászlóalj kulcsszerepet játszik abban, hogy a NATO gyorsan telepíthető és folyamatosan működő kommunikációs és információs rendszerekkel tudja támogatni a hadműveleteket és gyakorlatokat (NCISG | About us, no date).

2. táblázat Az NSB adatai és feladatai (forrás: <https://ncisg.nato.int/about-us>)

| <b>Egység száma</b> | <b>Központja</b>            | <b>Tagországok</b>                                                        | <b>Feladat</b>                                                                                                                                                               |
|---------------------|-----------------------------|---------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. NSB              | Wesel,<br>Németország       | Németország,<br>Hollandia, Nagy-Britannia, Dánia, Horvátország            | Feladatuk a telepíthető kommunikációs modulok (a továbbiakban: DCM) kezelése és a karbantartási egységek (a továbbiakban: M&S Coy) irányítása és kiképzése.                  |
| 2. NSB              | Grazzanise,<br>Olaszország  | USA, Németország, Olaszország, Románia, Bulgária                          | Biztosítani kell a NATO parancsnokságok számára a kommunikációs rendszereket és szolgáltatásokat, beleértve a telepített helyi hálózatok adminisztrálását és karbantartását. |
| 3. NSB              | Bydgoszcz,<br>Lengyelország | Lengyelország, Csehország, Szlovákia, Litvánia, Magyarország, Törökország | Feladatuk a rugalmas és megbízható stratégiai kommunikáció biztosítása a NATO valamennyi telepített parancsnoksága számára.                                                  |

#### IV. Kiberbiztonsági követelmények

A honvédség hírközlési hálózatának fejlesztésének szigorú információbiztonsági és kiberbiztonsági követelményeknek kell megfelelnie, annak érdekében, hogy biztosítani lehessen az információk védelmét, a rendszer stabilitását, valamint működési hatékonyságát.

A NATO Kibervédelmi Irányelveit (NATO, 2024a) is figyelembe kell venni a fejlesztés kapcsán. Ezek az irányelvek meghatározzák a titkosítási és adatvédelmi szabványokat, beleértve a titkosítási eljárásokat.

A titkosítási protokollok alkalmazása elengedhetetlenek annak érdekében, hogy a hálózaton áthaladó adatok védve legyenek az illetéktelen hozzáférésektől. Az egyik ilyen alapvető elvárás a katonai kommunikációban a 256 bites Advanced Encryption Standard (a továbbiakban: AES) titkosítás (Abikoye *et al.*, 2019). A hálózati integritást, azaz a rendszer zavartalan működését és az adatforgalom megbízhatóságát is biztosítani kell a fejlesztésnek. Ehhez elengedhetetlenek a behatolásészlelő rendszerek (IDS/IPS) alkalmazása, hiszen ezek képesek időben felismerni és

elhatárolni a külső támadásokat (Simo, Iantovics and Tokody, 2023). A NATO tagállamainak rendelkezniük kell az előírt szabványoknak megfelelő biztonsági mechanizmusokkal, ezeknek észlelniük kell a nem várt fenyegetéseket és anomáliákat. Magyarország részese a NATO Kooperatív Kibervédelmi Kiválósági Központnak, melynek feladata a gyors incidenskezelés és a sérülékenység csökkentése (Tóth, 2018). A NATO által használt Red Teaming módszerek is hozzájárulnak a hálózatok kibervédelméhez (Oakley, 2019). A kiberbiztonság részeként azonban kiemelt szerepe van a fizikai védelem kiépítésének, amelynek nagy jelentősége van a hálózati csomópontok és az adatközpontok biztonságában. Emellett nélkülözhetetlen a redundáns infrastruktúra kialakítása is, hiszen célja az, hogy az esetleges támadás vagy technikai probléma esetén is zavartalanul folytatódhasson a kommunikáció és az adatforgalom.

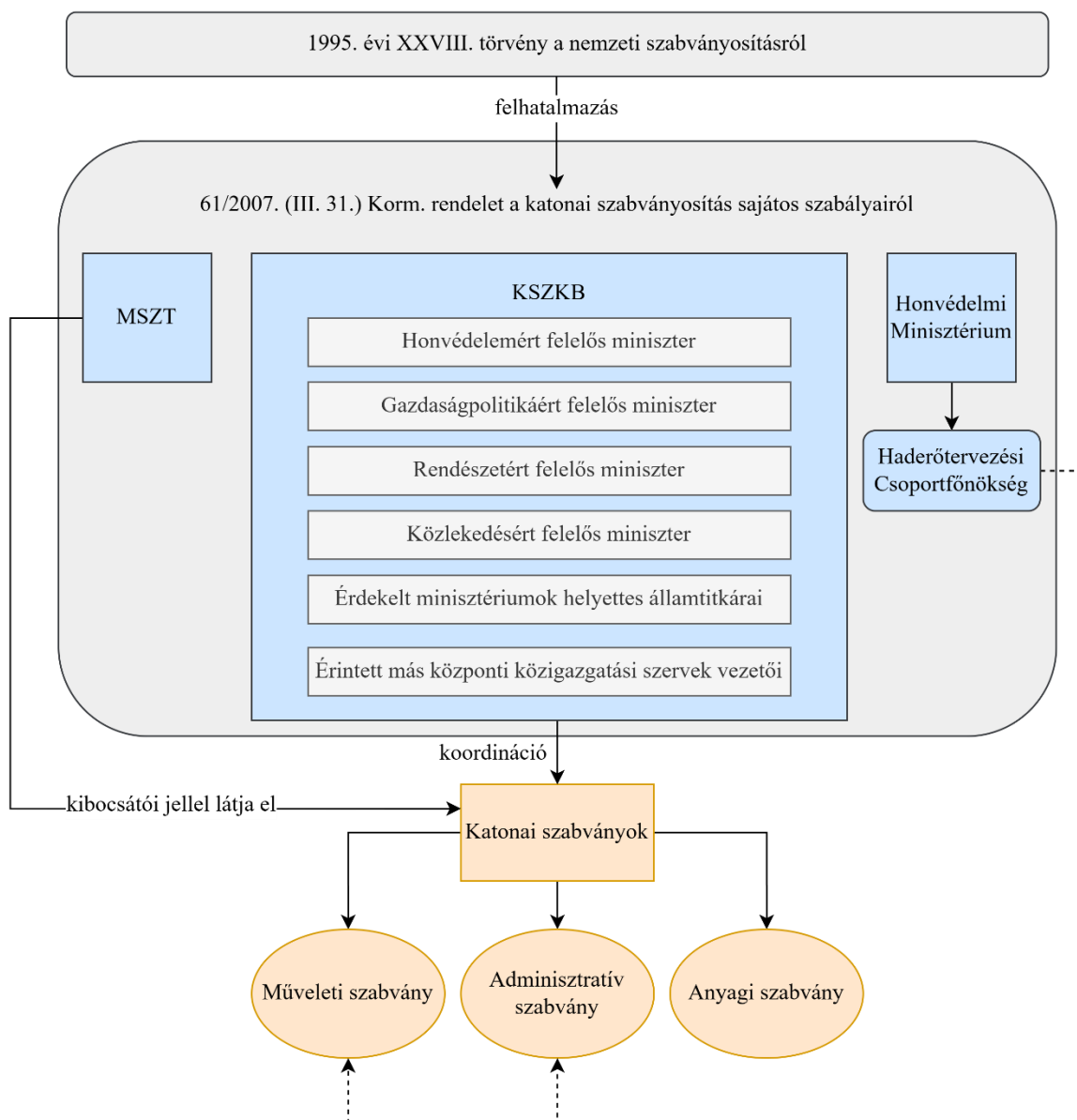
### **2.3 A szabványosítás folyamati Magyarországon**

A katonai szabványoknak három kategóriáját különböztetjük meg:

- a műveleti,
- az adminisztratív és az
- anyagi szabványt.

Az utóbbi irányításáért a magyar Honvédelmi Minisztérium, míg kiadásáért a Magyar Szabványügyi Testület (a továbbiakban: MSZT) a felelős. A másik két szabvány a Haderőtervezési Csoportfőnökség hatásköre alá tartozik, amely a Honvéd Vezérkar főnökének szolgálati alárendeltségébe tartozó katonai szervezet. A szabványokat közzé kell tenni a Honvédelmi Minisztérium hivatalos lapjában. A katonai szabványosítással kapcsolatos koordinációért a Katonai Szabványügyi Koordinációs Bizottság (a továbbiakban: KSZKB) a felelős, amelyben a minisztériumok és a központi államigazgatási szervek képviselői vesznek részt. A katonai szabványosítással felmerülő igényeket, valamint a KSZKB működési feltételeit a honvédelemért felelős miniszternek kell megfogalmazni. A szabványosítás részletes szabályait a *61/2007. (III.31.) Kormányrendelet* fogalmazza meg a nemzeti szabványosításról szóló *1995. évi XXVIII. törvény* felhatalmazása alapján. Ki kell emelni, hogy ezeknek a szabványoknak a költségeit a megrendelő szervezet viseli, de a Honvédelmi Minisztérium tervezi meg.

6. ábra Szabványosítási folyamat – saját szerkesztés (61/2007. (III. 31.) Korm. rendelet a katonai szabványosítás sajátos szabályairól című törvény alapján)



### 3 A Magyar Honvédség Hírközlő hálózata

A modern haderő működésének alapvető pillére a gyors, megbízható és biztonságos kommunikáció, amely lehetővé teszi a hatékony parancsnoki irányítást, az információáramlást és az operatív döntéshozatalt. Az MH hírközlő hálózata ennek az alapvető igénynek az ellátását célozza, biztosítva a katonai szervezetek közötti gyors és zavartalan adatforgalmat.

A hírközlés nem csupán a mindennapi működéshez elengedhetetlen, hanem a katonai műveletek során is kritikus szerepet játszik. A hatékony információcsere és a hálózatok biztonságos működése is elengedhetetlen a sikeres bevetésekhez és a nemzetbiztonsági célok

eléréséhez. Az MH hírközlő infrastruktúrája folyamatosan fejlődik, hogy lépést tartson a technológiai újításokkal és azért, hogy megfeleljen az egyre magasabb szintű biztonsági és kommunikációs elvárásoknak.

A következő fejezetekben részletesen bemutatásra kerül a honvédség kommunikációs rendszere, a zárt infokommunikációs hálózatok funkcionális csoportosítása, valamint az egyes hírközlési alrendszerek működése. Ezen kívül szó lesz a jövőbeli fejlesztési lehetőségekről is, amelyek hozzájárulhatnak a honvédség operatív képességeinek további növeléséhez.

### **3.1 Kommunikáció a honvédségben**

A digitalizáció hatására a nemzetközi és a magyar katonai kommunikáció is teljesen átalakult. Kezdetben a távirati technológiák és rádiótechnológiák jelentették a kommunikációs infrastruktúra alapjait, azonban az évek során egyre növekvő kockázatok (például az adatbiztonság és kibertámadás) egyre nagyobb fenyegetéseket jelentettek, így a kommunikációs rendszerek modernizálása mára elengedhetlenné váltak. Az információk biztonságos áramlása és az adatok megbízhatósága mellett az információáramlás gyorsasága is javulást eredményezett, melynek köszönhetően nőtt a védelmi reakcióképesség.

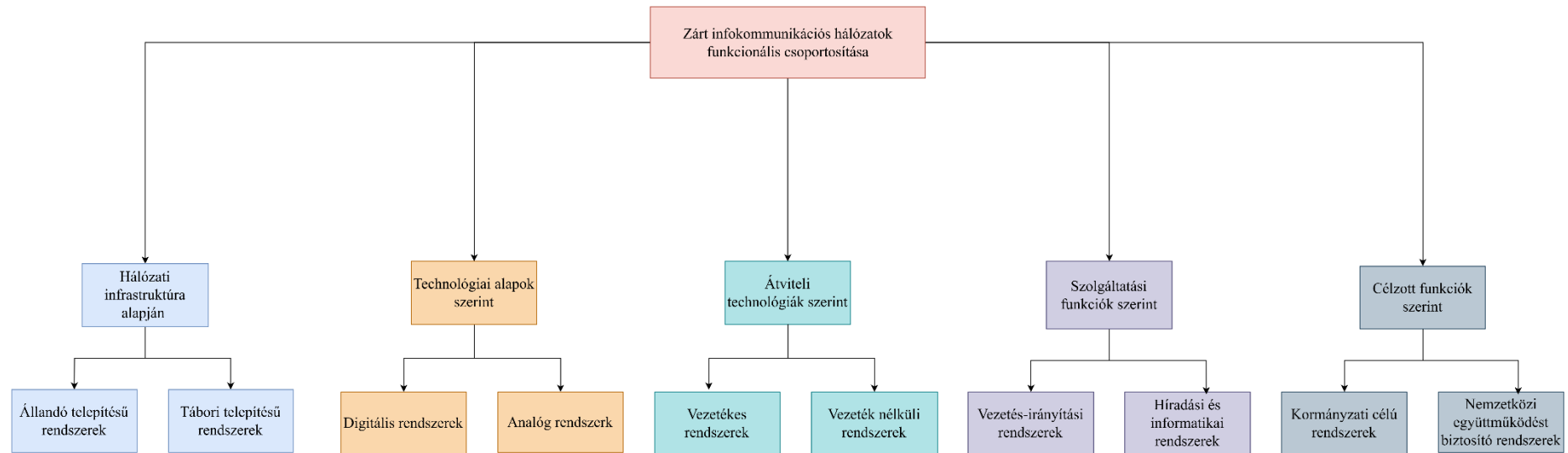
Habár a műholdas kommunikáció nem tartozik a vizsgálat tárgykörébe, de a vezetéknélküli átviteli rendszerek mellett, a műholdas technológia is hozzájárult a gyors információáramláshoz és a honvédség helyzetismertetéséhez. A szárazföldi rendszerek biztonságos adatátvitel tekintetében a titkosított kommunikációs csatornák alkalmazása nélkülözhetetlen. A vezetéknélküli kommunikációs technológiák feladata (például a mobilhálózatok és taktikai rádiók) a különböző operatív környezetek összeköttetése. A technológia által kínált gyors adatsere hozzájárul a döntéshozatal hatékonyságához és gyorsaságához, ezenkívül képes a gyors telepítésre és információterjesztésre is. Az integrált titkosítási algoritmusokkal és frekvenciaugratási technikákkal a katonai egységek többnyire védve vannak a kibertámadásokkal szemben. A legmodernebb vezetéknélküli technológiai megoldásokba fektetéssel Magyarország növelheti a felkészültségét és működési hatékonyságát, hiszen ezáltal az információáramlást zökkenőmentessé teszi, valamint a helyzetfelismerést is könnyebben elérhetővé teszi a katonai egységek számára. Véleményem szerint ennek az egyik lehetséges megoldása lehet a későbbiekben részletezésre kerülő LTE 450-es vezetéknélküli hálózat alkalmazása (Military Sphere Editorial Team, 2024).

### **3.2 Zárt infokommunikációs hálózatok funkcionális csoportosítása**

A zárt infokommunikációs hálózatok funkcionális csoportosításának is kiemelt szerepe van a hírközlési hálózatok fejlesztésében, hiszen ez a módszer átláthatóvá és megkülönböztethetővé

teszi azokat a rendszereket, amelyek eltérő feladatokat és különböző célokat látnak el. Az infokommunikációs hálózatok szerinti funkcionális csoportosítással a célom, hogy a kutatási területem specifikus igényei azonosításra kerüljenek, megkülönböztetve a más funkcionálissal rendelkező technológiáktól. Véleményem szerint a zárt infokommunikációs hálózatok funkcionális csoportosítása elengedhetetlen eszköz jelen fejlesztési koncepció tekintetében, hiszen ez a módszer lehetővé teszi a különböző rendszerek egyedi igényeinek azonosítását és feladatainak pontosabb megértését. A lenti ábra bemutatja a zárt infokommunikációs hálózatok funkcionális csoportosítását:

7. ábra Zárt infokommunikációs hálózatok funkcionális csoportosítása – saját szerkesztés



A 7. számú ábrán látható első kategória alapját a hálózati infrastruktúra képezi, amely alapján megkülönböztetünk állandó és tábori telepítésű rendszert. Az állandó telepítésű, stacioner rendszerek olyan infrastruktúrát jelentenek, amelyek hosszútávon kiszolgálják a kommunikációs igényeket. Ezzel ellentétben a tábori rendszerek gyorsan telepíthetők és nagyobb mobilitást nyújtanak, amik nélkülözhetetlenek a katonai műveletek során. A tábori rendszerek képesek biztosítani a információáramlást, valamint könnyebben alkalmazhatóak a változékony katonai környezetben is (Tőreki, 2010).

Technológiai alapok szerint két csoport különíthető el: az analóg és a digitális rendszerek. Az utóbbi rendszerek modern technológiai megoldásokra épülnek. Ezek a rendszerek biztosítják a nagy adatsebességet, valamint a fejlettebb titkosítást is. Az analóg rendszerek alapját viszont régebbi technológia nyújtja, amely kevésbé hatékony. Ezeket olyan környezetben célszerű használni, ahol a digitális infrastruktúra sérülékeny, vagy nem elérhető.

Az átviteli technológiák alapján megkülönböztetjük a vezetékes, valamint a vezeték nélküli rendszereket. A vezetékes rendszerek működése fizikai kapcsolatot igényel, például a kábelhálózatot. Ezáltal képesek a stabil és megbízható kapcsolat kialakítására, ami rendkívül fontos a kormányzati és a katonai infrastruktúrák esetében. Ezzel ellentétben a vezeték nélküli rendszerek rádióhullámokon vagy mikrohullámokon képesek az információkat továbbítani. Ennek előnye a rugalmasság, valamint a gyors telepíthetőség. Sokszor olyan esetekben alkalmazzák, amikor a vezetékes infrastruktúra kiépítése túl költséges és időigényes lenne.

A szolgáltatási funkció alapján elkülöníthetjük a vezetés-irányítási és a híradás-informatikai rendszereket. A vezetés-irányítási rendszerek hozzájárulnak a gyors és hatékony döntéshozatalhoz, a híradás-informatikai rendszerek pedig az információáramlás biztonságát támogatják.

A hálózatokat megkülönböztethetjük célzott funkciójuk alapján is. Az egyik ilyen kategória a kormányzati célú hálózat, amely a nemzeti szintű kommunikációt támogatja, a másik típus pedig a nemzetközi együttműködést támogató rendszerek. Az utóbbi lehetővé teszi a hatékony kommunikációt és kooperációt a különböző nemzetek katonai és civil szervezetei között, például a NATO esetében. Ezek a rendszerek rendkívül fontosak a közös ügyek tekintetében, így fejlesztésük során kiemelten figyelembe kell venni a nemzetközi szabványokat és a rendszerintegráció szükségességét is.

A különböző funkcionalitású rendszerek közötti különbségek meghatározzák a fejlesztés irányát. A stacioner hálózatok esetében például a fejlesztés célja a hosszú távú stabilitás és a biztonságos adatátvitel. Ezzel ellentétben a tábori rendszerek fejlesztésénél kiemelten fontos a megfelelő mobilitás és a változó környezetben történő gyors adaptáció.

A digitális rendszerek korszerűsítési igényei nélkülözhetetlenek ahhoz, hogy lépést tudjunk tartani a rohamosan fejlődő technológiai környezettel és az egyre növekvő adatforgalmi igényekkel, hiszen a jövő fejlesztései alapvetően a digitális technológiák köré épülnek.

Az átviteli technológiák fejlesztése során is figyelembe kell venni a vezetékes és vezeték nélküli rendszerek eltérő igényeit is. A vezeték nélküli hálózatok fejlesztései elősegítik a gyors mozgathatóságot és rugalmasságot, míg a vezetékes hálózatok fejlesztésével nagyobb stabilitást és biztonságot érhetünk el, ami kritikus lehet például a katonai rendszerek esetén, ahol az adatbiztonság kiemelt fontosságú.

### **3.3 Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózata**

A Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózata a katonai vezetési és irányítási rendszerek alapvető infrastruktúráját jelenti. Ebből adódóan bármilyen rendszer és hálózat képességfejlesztésének tekintetében figyelembe kell venni az MH KCEHH működését is (Pölöskei, 2021). A modern technológiai környezet folyamatos újításokat és fejlesztéseket követel meg annak érdekében, hogy a honvédelmi rendszerek hatékonyan tudjanak működni a békeidőben és a különleges jogrend idejében is egyaránt.

*Az 55/2013. (IX. 13.) HM utasítás a Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózatának békeidejű üzemeltetési és felügyeleti rendjéről, valamint a központilag biztosított szolgáltatások igénybevételének szabályairól* pontosan szabályozza a MH KCEHH békeidőben történő üzemeltetését és felügyeleti rendjét, valamint a központilag biztosított szolgáltatások igénybevételének szabályait. Az MH KCEHH híradási, informatikai és információvédelmi központokat foglal magában, ezekhez kapcsolódó olyan infrastruktúrákkal, mint például mikrohullámú állomások, antennatornyok és különféle átviteli rendszerek.

Az MH KCEHH feladata, hogy stabil és megbízható rendszereket üzemeltessen, amelyek képesek támogatni a katonai vezetést és az ehhez kapcsolódó műveleteket mind nemzeti, mind nemzetközi szinten. Nem csak a Magyar Honvédséggel, hanem más kormányzati és nemzetközi hálózatokkal is együttműködhet (pl. NATO, EU) elősegítve ezzel a híradási rendszerek hatékony működését. A hálózati interoperabilitás nagyon fontos a nemzetközi katonai és diplomáciai együttműködés során, hiszen a sikeres műveletekhez nélkülözhetetlen a gyors információáramlás.

Az MH KCEHH működésének meghatározó része a híradó- és informatikai központok fenntartása és üzemeltetése, amely a hálózatgazda szakmai irányítása alatt álló katonai személyzet feladata. Ezek a szakemberek felelősek azért, hogy a rendszerek zavartalanul és biztonságosan működjenek. Ki kell emelni, hogy az MH KCEHH önállóan is képes működni, függetlenül más hálózatoktól. Az MH KCEHH magába foglalja a Honvédelmi Minisztérium

vagyonkezelésében lévő stacioner, vagyis fixen telepített, valamint tábori, azaz mobilizálható elemeket is. A hírközlési rendszerek fejlesztésekor komplex megközelítésre van szükség, mivel a tábori és állandó hálózatok egymást kiegészítik, és átjárhatóságot kell biztosítani közöttük. Fontos, hogy a rendszerek ellenállóképesek legyenek, és megfelelő tartalékrendszerekkel rendelkezzenek, például az optikai hálózatoknak legyen mikrohullámú tartalékuk.

Elmondható, hogy az MH KCEHH nem csupán egy egyszerű katonai hírközlési hálózat, hanem egy rendkívül komplex módon működő rendszer, hiszen ez a hálózat biztosítja a honvédelem infokommunikációs és információvédelmi igényeinek teljes körű kiszolgálását.

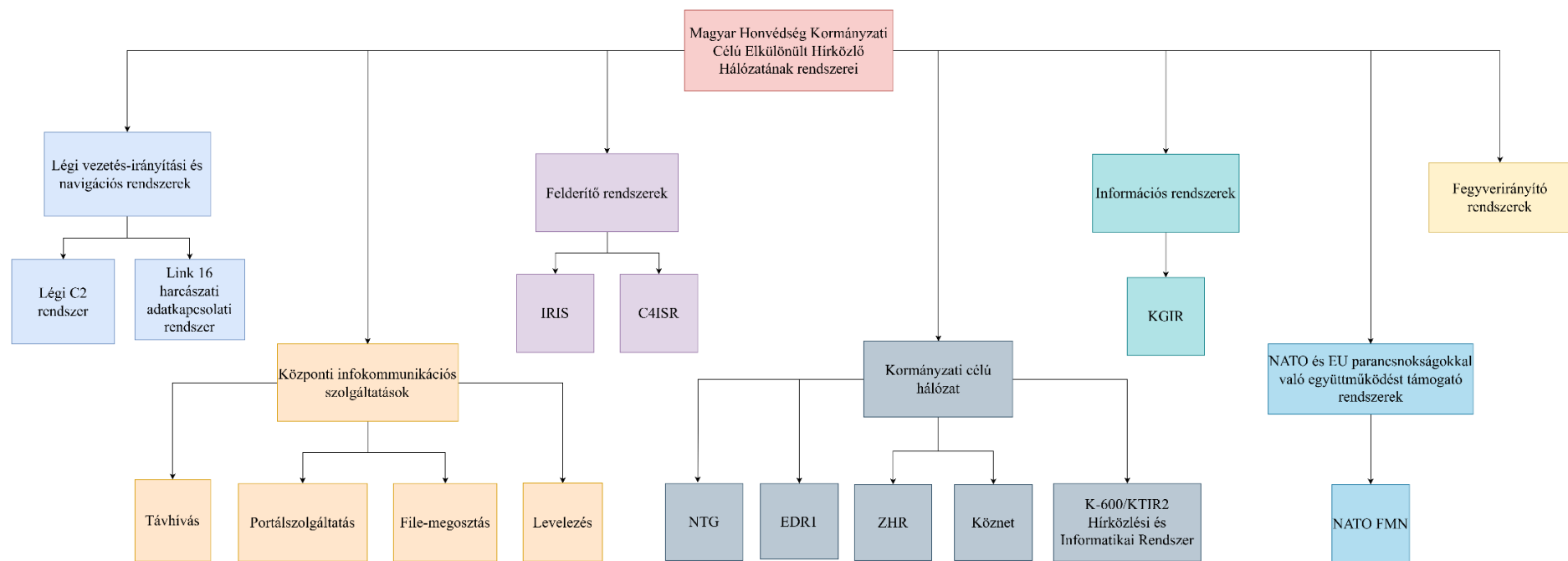
Az MH KCEHH által biztosított központi infokommunikációs szolgáltatások, mint például a távhívások, levelezési rendszerek, fájlmegosztás és portálszolgáltatások, alapvető szerepet játszanak a katonai személyzet mindennapi munkájának támogatásában, hiszen ezek a rendszerek lehetővé teszik a gyors és biztonságos információcserét. Mindemellett olyan információs célrendszerek is rendelkezésre állnak, mint például a Katonai Gazdálkodási és Informatikai Rendszer (a továbbiakban: KGIR), amely az adminisztratív és vezetési folyamatok támogatásában segít (Szabados, 2018). Ez a rendszer biztosítja, hogy a katonai szervezet hatékonyan tudjon működni, és megfeleljen a modern vezetési kihívásoknak.

Az MH KCEHH által üzemeltetett felderítő rendszerek, mint az IRIS és a C4ISR, szintén kritikus szerepet töltenek be a hadműveletek során, hiszen ezek a rendszerek felelnek a stratégiai döntéshozatalhoz szükséges adatok gyűjtéséért és elemzéséért, lehetővé téve, a gyors döntéshozatalt (Bihl and Talbert, 2020).

Ezen kívül, az MH KCEHH által működtetett fegyverirányító rendszerek is kiemelt szerepet játszanak a harci műveletek során. Ennek oka, hogy a fegyverirányító rendszerek révén a katonai egységek pontosabban és gyorsabban tudják végrehajtani feladataikat, ami döntő fontosságú lehet a modern hadviselésben.

Összességében elmondható, hogy az MH KCEHH által üzemeltetett rendszerek és infrastruktúrák együttesen biztosítják a Magyar Honvédség műveleti képességeit. Ezek a komplex, jól integrált rendszerek lehetővé teszik a modern katonai kihívások hatékony kezelését, biztosítva a honvédelem és a nemzetközi együttműködések sikerét.

8. ábra Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózatának rendszerei – saját szerkesztés



### **3.4 MH szárazföldi tábori-harcászati rendszer**

Az MH szárazföldi tábori rendszerét jelenleg digitális rádiók képezik, amelyek elsősorban hangalapú kommunikációra épülnek. A jelenleg használt berendezések a Kongsberg és Harris digitális rádiócsaládok termékei közé tartoznak, azonban ezek csak korlátozottan biztosítják az IP-alapú adatkommunikációs képességeket. Bár ez az IP-alapú kommunikáció némi rugalmasságot kínál, a jelenlegi rendszer nem alkalmas a modern adatalapú kommunikációs igények teljes körű kielégítésére (Kovács, 2022).

Nagy problémát jelent ugyanis, hogy a rendszer nem képes biztosítani a szükséges sávszélességet a nagy mennyiségű adatok hatékony továbbításához, ami különösen fontos lenne a mai hadviselési követelményeknek megfelelően. Az IP-alapú adatkommunikáció képes hálózatként működni, azonban csak szigorú korlátok között. Ennek korlátjai a következők: a felhasználók számának növekedésével az ugrások száma is növekszik az adattovábbítás során, ami lassítja és megnehezíti a kommunikációt. Emellett a rendszer rugalmatlan, mivel az ugrási pontok beállításai előzetes feladatvégrehajtást igényelnek, ami időigényes és helyspecifikus.

Ez a technológia ma már idejétmúltnak tekinthető, és nem képes biztosítani azt a szükséges kapacitást és rugalmasságot, amely a modern harcászati műveletek zökkenőmentes végrehajtásához elengedhetetlen. A sávszélesség korlátozott volta, valamint a bonyolult hálózati konfigurációk miatt a jelenlegi rendszer nem támogatja megfelelően a gyors, megbízható adatcserét, ami nélkülözhetetlen lenne az adatalapú kommunikáció esetében. Ebből adódóan indokolt a rendszer korszerűsítése, amely lehetővé teszi a nagyobb adatforgalom kezelését és a hatékonyabb, rugalmasabb kommunikációs megoldások alkalmazását.

Összességében tehát a jelenlegi MH szárazföldi tábori-harcászati kommunikációs rendszer főként a hangalapú kommunikációra támaszkodik és korlátozott IP-alapú adatkommunikációs képességei miatt nem képes a mai adatigényes feladatok hatékony támogatására. A fejlesztés egyik elsődleges célja a sávszélesség növelése és a rendszer rugalmasságának javítása, hogy a harcászati műveletek során megbízható, gyors és biztonságos kommunikációt lehessen biztosítani (Szeleczki and Farkas, 2022).

### **3.5 MH KCEHH Stacioner hálózata**

A Magyar Honvédség stacioner hálózata az országos optikai gerinchálózatra épül. A stacioner hálózat képes a rendkívül nagy sebességű és sávszélességű hálózatok összekapcsolására, különösen nagy távolságokon. Fő funkciója, hogy lehetővé tegye a nagy távolságokra történő adatátvitelt, miközben teljes területi lefedettséget biztosít az úgynevezett gerinchálózatokon

keresztül. A gerinchálózat több száz kilométer hosszú optikai kábelekből, valamint aktív és passzív adatátviteli és jelerősítő eszközökből áll össze.

Az optikai kábelekben a nagy sáv szélességet a fényjelek Wavelength Division Multiplexing (a továbbiakban: WDM) eszközökkel történő továbbításával érik el. Az optikai eszközök már széles körben elterjedtek, azonban léteznek olyan mikrohullámú gerinchálózati eszközök, amelyek alternatív megoldást kínálnak. A rendszerhez tartoznak az úgynevezett Point of Presence (a továbbiakban: PoP) helyek is, amelyek olyan infrastruktúrák, ahol a hálózati eszközök fizikailag elérhetők és kezelhetők. Emellett a gerinchálózatok fontos részét képezik az Internet Exchange Points (a továbbiakban: IXP-k), amelyek a különböző hálózatok közötti adatcserét bonyolítják.

A gerinchálózatokat eredetileg a hangalapú telefonhálózatok kiépítésével fejlesztették ki, kezdetben rézérpárookra épülő adatátviteli technológiával. A piac liberalizációjával és a monopóliumok eltörlésével koncessziós jogokat osztottak ki az elsődleges területeken, ami elősegítette a technológia gyors fejlődését és modernizációját. Magyarországon már szinte csak a hadsereg hálózataiban található réz gerinchálózatok. A kereskedelmi hálózatokban az aggregációs hálózatokban már szinte egyáltalán nem használnak rézvezetékot, kivéve néhány kisebb települést, például Zala megyében vagy a távol eső, eldugott helyeken. A rézalapú megoldásoknál a kábel hossza jelentősen befolyásolja a teljesítményt és bár ez a technológia már nem a legkorszerűbb, továbbra is költséghatékony és életképes megoldás. Azok számára azonban, akik számára a stabilitás és a rendelkezésre állás elsődleges fontosságú, az üvegszál technológia ajánlott, mivel megbízhatóbb és nagyobb teljesítményt nyújt.

Bármilyen megbízható is egy gerinchálózat, önmagában nem elegendő a hatékony működéshez. Olyan gerinchálózathoz kell csatlakozni, amely biztosítja a felhasználók számára a csatlakozást, és elérhetővé teszi az adatforgalmat. Ezek a gerinchálózatok lehetővé teszik az adatok átvitelét a gerinchálózatról a végfelhasználókhoz, létrehozva egy teljes kommunikációs infrastruktúrát.

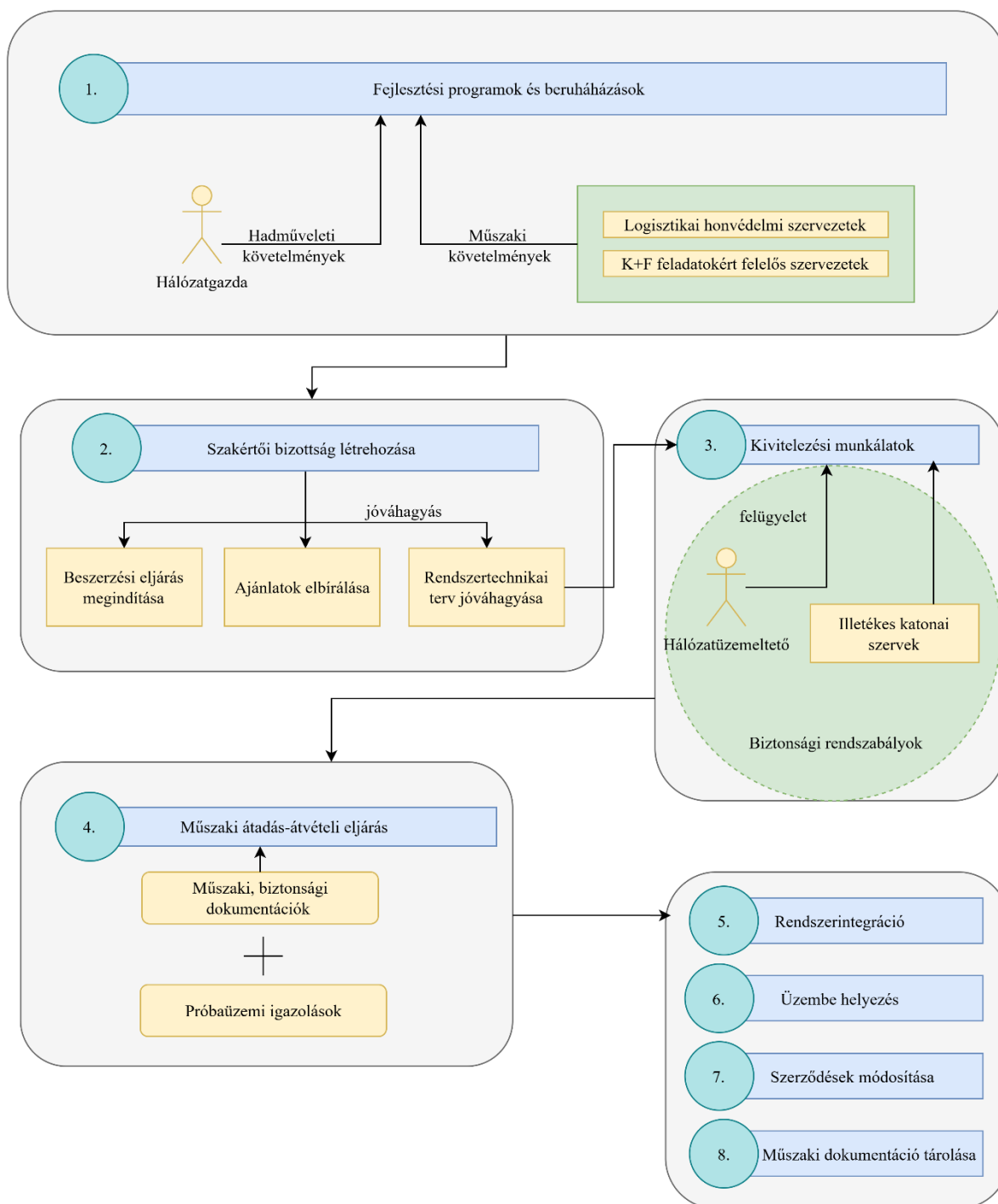
A lenti ábrán látható magyarországi üvegszál hálózati lefedettség több ezer kilométernyi teljesen redundáns üvegszál gerinchálózatot mutat, 11 határátkelőhellyel. Az optikai és vezeték nélküli kapcsolatok és hozzáférési hálózatok az egész ország területén teljes lefedettséget biztosítanak. Az országos átviteli műszaki hálózat SDH, DWDM és DF technológiákon alapul, IP, MPLS és Ethernet alapú csomagkapcsolási struktúrákkal. A hálózat különböző platformokon, például SS7, SIP és Centrex rendszereken keresztül támogatja a hangszoolgáltatásokat is.

<https://www.invitech.hu/szolgalatasi-teruletek>)



- 27 -

10. ábra A MH KCEHH fejlesztésének jogszabályi előírásai – saját szerkesztés (55/2013. évi HM utasítás alapján)



Amint az ábra is mutatja, az MH KCEHH fejlesztésének több lépés betartása mentén kell megvalósulnia: Első sorban a meg kell határozni a hadműveleti és műszaki követelményeket. A hálózatzagza feladata a hadműveleti követelmények meghatározása, a műszaki

követelmények előírásáért pedig a K+F feladatokért felelős szervek felelnek. Ezt követően létre kell hozni a szakértői bizottságot, akiknek el kell bírálniuk a kapott ajánlatokat, majd ezt követően indíthatják el a beszerzési eljárást. A szakértői bizottságban az érintett felek képviseltethetik magukat. A kivitelezési munkálatok csak a szakértői bizottság által jóváhagyott rendszertechnikai terv és a kivitelezési tervdokumentáció alapján kezdődhetnek meg. A munkálatok végrehajtása és a kivitelezés a hálózatüzemeltető és az illetékes katonai szervezetek felügyelete mellett történhet, mely során figyelembe kell venni a hatályos biztonsági előírásokat, amelyeket az illetékes katonai üzemeltető köteles betartatni. A helyszíni munkavégzés csak az informatikai központ szakemberei mellett végezhető. A fejlesztések átadásához műszaki átadás-átvételi eljárást kell lefolytatni, amelybe bevonásra kerülnek a minőségbiztosításért felelős szervek is. A sikeres átadás-átvételt követően műszaki és biztonsági dokumentációk, valamint a próbaüzem igazolásai szükségesek. Ezt követően a hálózatüzemeltető gondoskodik az új hálózati elemek üzemeltetési rendszerbe történő beillesztéséről. Az üzembe helyezést követően szükség esetén módosítani kell a fenntartási és üzemeltetési szerződéseket, a fejlesztésekkel kapcsolatos műszaki dokumentációt pedig több helyen szükséges tárolni, beleértve a híradó és informatikai központokat is.

A hadműveleti és műszaki követelmények, valamint a felelősségi körök meghatározása rendkívül fontosak az MH hírközlési hálózatának fejlesztésének szempontjából. Ez azért lényeges, mert a hadműveleti követelmények garantálják azt, hogy a hálózat megfeleljen a katonai céloknak és a működési igényeknek. A műszaki követelmények pedig biztosítják a technológiai megvalósíthatóságot és a biztonságos működési környezetet. Ezen követelményrendszerek összhangban állása kell ahhoz, hogy a hálózat stratégiai és technológiai szempontból is hatékonyan és megbízhatóan tudjon működni.

### **3.6 Hírközlési hálózat továbbfejlesztési lehetőségei**

A hírközlési hálózat modernizálása nagy kihívást jelent, mivel a növekvő forgalmi igények és az új technológiák támogatása szükségessé teszi a fejlesztést. Az MH hírközlési hálózatának korszerűsítése olyan komplex kihívás, amellyel kapcsolatban számos szempontot figyelembe kell venni, mint például a gazdasági hatékonyság kérdéskörét, a technológiai fejlesztéseket, vagy a védelempolitikai célok teljesítését. A stacioner hálózatokat az ellenséges haderő elsődleges célpontjai között tartják számon, ezért a mobil rendszerek fejlesztése is kulcsfontosságú a védelem szempontjából. A katonai kommunikációs igények rendkívül változékonyak, így ezt figyelembe kell venni a meglévő rendszerek fejlesztésével kapcsolatosan. Jelen fejezetben azt vizsgálom, hogy milyen megoldások járulhatnak hozzá az

MH kommunikációs hálózatának korszerűsítéséhez, figyelembe véve a költséghatékonyságot és a technológiai megfelelőséget.

Kutatásom során arra a következtetésre jutottam, hogy a honvédség kommunikációs igényei jelentős részben a meglévő hálózatok felhasználásával is kielégíthetők, anélkül, hogy teljesen új hálózatokat kellene kiépíteni. Ez a megoldás jóval költséghatékonyabb lehetőséget kínál, amely lehetővé teszi azt, hogy szükségtelen kiadások terheljék a költségvetést. Például az MH jelenlegi mikrohullámú hálózata már most is képes viszonylag gyors adatátvitelre, különösen a tábori területeken és mobil hírközpontoknál. Ezt a meglévő rendszert azonban fejleszteni kell ahhoz, hogy kielégítse a jövőbeni igényeket, különösen a nagyobb adatforgalmat és sáv szélességet igénylő alkalmazások esetében.

Az LTE 450-es mobilhálózat hozzájárulhat a fejlesztésekhez, azonban a teljes kommunikációs kapacitás biztosítása érdekében további technológiai megoldásokra lehet szükség. Az LTE rendszerek nem alkalmasak arra, hogy nagy mennyiségű adatot kezeljenek, különösen, ha olyan specifikus katonai kommunikációs alkalmazásokról van szó, mint a műholdas adatátvitel.

A Kongsberg és Harris digitális rádiók esetében az IP-alapú adatkommunikáció korlátozott képességei miatt nem alkalmasak a nagy sáv szélességet igénylő forgalomra. A jövőbeni katonai adatkommunikációs rendszerekhez olyan megoldásokra lesz szükség, amelyek biztosítják a nagy sáv szélességet és a gyors adatátvitelt. Erre számos lehetséges megoldás kínálkozik, amelyeket érdemes megvizsgálni az MH hálózati fejlesztéseinek tervezésekor.

Többcsatornás rádiórendszerek alkalmazása lehetővé teszi, hogy több adatcsatornát párhuzamosan kezeljenek, ezáltal növelve a rendelkezésre álló sáv szélességet. A Tactical Data Link (a továbbiakban: TDL) rendszerek, mint a Link 16 vagy Link 22, kifejezetten a katonai kommunikáció hatékonyságának növelésére szolgálnak, és képesek többféle adatforrást integrálni, így jelentősen javítják a hálózati kapacitást és megbízhatóságot.

Az optikai hálózatok bevezetése szintén elengedhetetlen a nagy sáv szélességű adatátvitelhez. A digitális rádiós rendszereket kiegészítve az optikai kábelek rendkívül magas adatátviteli sebességet biztosítanak, amely különösen a nagy mennyiségű adatok esetén létfontosságú. Habár az optikai hálózat kiépítése drága és időigényes, viszont hosszú távon stabil és nagy kapacitású adatkapcsolatokat nyújt, amelyek nélkülözhetetlenek a modern honvédség számára. A mikrohullámú rádiók továbbra is fontos szerepet játszanak az MH távoli helyszínein történő adatátvitelében, különösen ott, ahol az optikai hálózat nem érhető el. Ezek a rendszerek azonban korlátozott sáv szélességet biztosítanak, különösen nagy távolságok esetén, ezért integrálni kell őket más technológiákkal, például az 5G, 4G és az LTE hálózatokkal, amelyek növelhetik az adatátvitel sebességét és megbízhatóságát.

Az 5G és 6G hálózati rendszerek még fejlettebb megoldásokat kínálnak a jövőben, mivel képesek lesznek a növekvő adatigények kielégítésére alacsony késleltetéssel és nagy sávszélességgel. Ezek a hálózatok kulcsfontosságúak lesznek a járművektől a műveleti központokig terjedő adatkapcsolatok biztosításában, és lehetővé teszik a valós idejű kommunikációt a katonai műveletek során.

Egy másik lehetséges fejlesztési irány az adaptív sávszélesség-elosztás bevezetése, amely lehetővé teszi az adatforgalom dinamikus kezelését a különböző felhasználók között. A QoS protokollok például optimalizálják az adatátvitel prioritásait, biztosítva, hogy a legfontosabb kommunikációs csatornák mindig előnyt élvezzenek (Porteleki, 2020).

Összefoglalva, a Magyar Honvédség elektronikus hírközlési hálózatának korszerűsítése olyan megoldások integrálását igényli, amelyek a meglévő rendszerek fejlesztésére és új technológiák bevezetésére egyaránt építenek. A mikrohullámú hálózat fejlesztése képes kielégíteni a rövid távú igényeket, de a hosszú távú, nagy sávszélességet és megbízható adatkapcsolatot igénylő fejlesztésekhez az optikai gerinchálózat kiépítése elengedhetetlen. Az optikai hálózat képes biztosítani azokat a technológiai feltételeket, amelyek szükségesek a jövő katonai kommunikációs rendszereinek hatékony és fenntartható működéséhez.

A fent tárgyalt megoldások együttes alkalmazása biztosíthatja, hogy a Magyar Honvédség kommunikációs hálózata a modern kihívásoknak megfelelően működjön, miközben teljesíti a gazdasági hatékonyság és a védelempolitikai célok követelményeit. A jövőbeni fejlesztések során nem csupán a jelenlegi igények kielégítésére kell koncentrálni, hanem arra is, hogy a technológiai innovációk folyamatos bevezetésével biztosítsuk a honvédség stratégiai céljainak hosszú távú megvalósítását.

## **4 LTE 450-es vezeték nélküli hálózat**

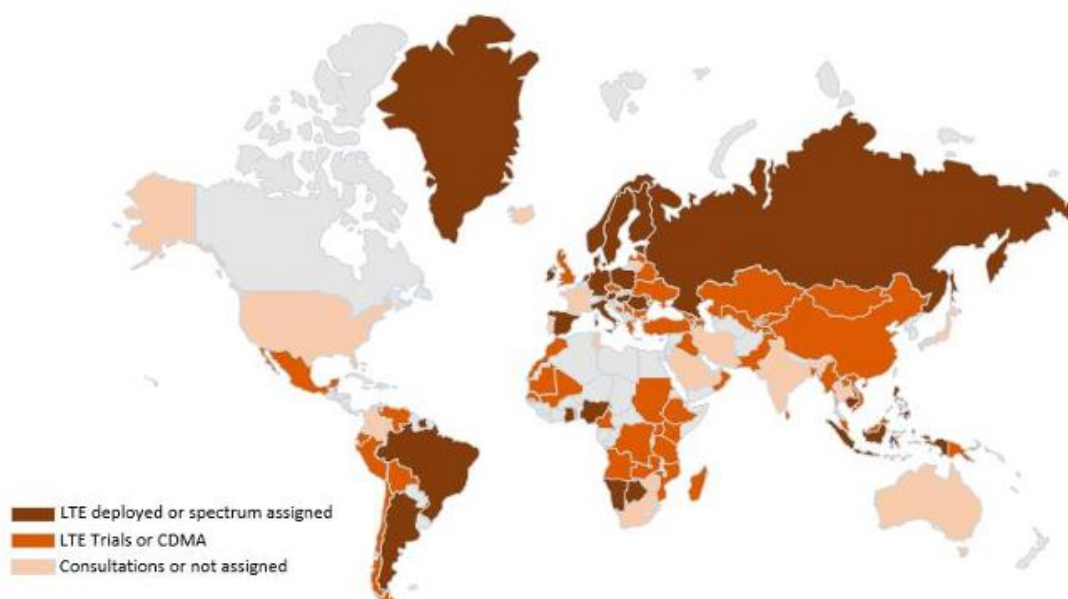
### **4.1 Az LTE hálózat eredeti célja és jövője**

Jelen fejezetben arra keresem a választ, hogy az LTE 450 MHz-es hálózat lehet-e a jövő vezeték nélküli kommunikáció megoldása az MH számára. A Long Term Evolution (a továbbiakban: LTE) egy olyan technológia, amely nagy sebességű internetet képes biztosítani a mobilhálózatokon. A 410-470 MHz-es szabvány jó területi lefedettséget biztosít relatív kevés (körülbelül 500 db) bázisállomással, de viszonylag kevés felhasználót képes egyidejűleg kiszolgálni, és őket sem nagy sávszélességgel. A kereskedelmi célú mobiltávközlésben viszont minden bizonnyal az LTE a legszélesebb körben elterjedt olyan rendszer, amely képes a megbízható, biztonságos és gyors adatátvitelre.

Ezeknek a hálózatoknak a legnagyobb előnye, hogy kevesebb bázisállomással is képesek nagy területet lefedni. Ennek köszönhetően gyorsabban kiépíthetőek a szükséges hálózatok, így a kevesebb telepítési pontot igényelnek, amiből adódóan az üzemeltetési és építési költségei jóval költséghatékonyabbak. Ezt a hálózatot világszerte és nemzetközi szinten is egyre több helyen használják, hiszen képes az okoseszközök közötti gyors és hatékony kommunikációra, viszont jelenleg ennek előnyeit főképp a közműszektorban, közlekedési szektorban, a közbiztonságban, valamint a készenléti szolgálatokban hasznosítják. Az LTE mint szabványcsalád valóban korszerű, de a különböző frekvenciatartományokban eltérő módon kerül alkalmazásra, így a 450 MHz-es és a 1800 MHz-es sávok közötti különbségek is jelentősek. A 450 MHz-es sáv speciális felhasználási esetekre van optimalizálva, például nagyobb hatótávot biztosít, ami alacsony népsűrűségű területeken vagy ipari megoldásoknál előnyös. Ez a frekvencia azonban korlátozott sáv szélességet nyújt, így a sebesség alacsonyabb lehet, mint a magasabb, például 1800 MHz-es sávokban, ahol az LTE-t jellemzően nagyobb adatsűrűségű területeken használják, gyorsabb sebességet biztosítva. Ezzel szemben a 1800 MHz-es és egyéb magasabb frekvenciasávokban az LTE hálózatok sokkal nagyobb kapacitást és sebességet kínálnak, mivel ezeket elsősorban városi, sűrűn lakott területekre tervezték, ahol a sebesség és a teljesítmény a legfontosabb szempont. A 450 MHz-es hálózat esetében tehát inkább a lefedettség, míg a magasabb frekvenciák esetén a sáv szélesség és a sebesség áll a középpontban. Az LTE 450-es vezeték nélküli hálózat ismertetéséhez a *450 MHz Szövetség (a továbbiakban: Szövetség) 2023-ban megjelent nyilvános jelentését* vettem kiindulópontként (450 MHz Alliance, 2023). A Jelentéshez a Szövetség világszerte adatgyűjtést végzett, melynek alanyai az érintett üzemeltetők és szabályozó hatóságok voltak. A Szövetség egy olyan érdekvédelmi csoport, amely a 380-512 MHz tartomány közé eső sávban végrehajtott telepítéseket támogatja. Fő feladataik közé tartozik többek között a globális együttműködés, a technikai oktatás, valamint a szabványok, funkciók és szolgáltatások folyamatos fejlesztése. Kereskedelmi forgalommal jelenleg huszonhat LTE-hálózat működik, négy hálózat pedig tesztelés alatt áll. A 410 MHz és 450 MHz sávokban a CDMA hálózatok még jelen vannak, de a CDMA 2000 technológia fokozatosan kifutóban van, és a legtöbb országban megszüntetik. Az LTE-re való átállás ezen frekvenciasávokban korszerű megoldásnak számít, különösen a 450 MHz-es sávban, de fontos tisztázni, hogy a kereskedelmi mobilhálózatok világszerte már szinte sehol nem használják a 450 MHz-et. Ennek oka, hogy ez a sáv nem képes nagy sáv szélességgel sok felhasználót kiszolgálni. Így az LTE-re való átállás leginkább speciális felhasználási területeken jellemző, ezért az eredeti állítás inkább a 450 MHz-re korlátozódik.

A 450 MHz-es frekvenciasávban használható LTE technológia a 4G szabvány része, amelyet a 3GPP nemzetközi szervezet dolgozott ki. Az említett szabvány magas szinten biztosítja a fejlett megbízható adatátviteli megoldásokat, illetve a magas szintű hang- és adatkapacitásokat. Ez a technológia ideális lehet az alacsony népességű távoli területeken, hiszen a 450 MHz-es frekvencia alacsonyabb, így a jel könnyebben terjed a nagyobb távolságokon is, mindemellett kiváló lefedettséget biztosít, és jóval energiatakarékosabb és költséghatékonyabb megoldás is. Az elmúlt évek során számos országban kiépítésre került a hálózat, amely jelentős előrelépéseket eredményezett. Írországban, Németországban és Lengyelországban folyamatban vannak a hálózatépítési projektek, Malajziában pedig próba hálózatokat telepítenek. Európa különösen aktív ezen a téren, hiszen számos európai országban zajlanak a szabályozási folyamatok, illetve a spektrumkiosztási konzultációk (450 MHz Alliance, 2023). A következő ábra a 380 MHz, 410 MHz és a 450 MHz frekvenciasávok globális használatát jeleníti meg, különböző alkalmazásokra fókuszálva:

*11. ábra A 380 MHz, 410 MHz és a 450 MHz frekvenciasávok globális használata, különböző alkalmazásokra fókuszálva (450 MHz Alliance, 2023)*



**Figure 2.** The world map of 380 MHz, 410 MHz and 450 MHz deployment.

A sötétbarna országok jelenítik meg a már letelepített LTE hálózatokat, a világos narancs színű országokban már LTE próbák vagy CDMA hálózatok vannak folyamatban, míg a narancssárga színnel jelölt országokban még egyáltalán nincs kiépítve spektrum, vagy csak kezdetleges konzultációk zajlanak. A képen Magyarország sötétbarna színnel van jelölve, amiből az a következtetés vonható le, hogy az ország aktív szereplője lehet az alacsony frekvenciasávú LTE

hálózatok kiépítésében. Ez különösen fontos lehet a különböző kritikus kommunikációs rendszerek működtetése szempontjából. Ez a spektrum ideális lehet a privát hálózatok kiépítésére, amelyek a kritikus infrastruktúrát támogatnák (450 MHz Alliance, 2023).

Magyarországon korábban az MVM NET biztosította a 450 MHz-es licencet, amelyet leginkább az okos város és okos mérők alkalmazására hasznosítottak. Az MVM NET 2023 végéig volt a 450 MHz-es frekvenciára épített LTE hálózat üzemeltetője, miután 10 évre szóló használati jogot kapott a Nemzeti Média- és Hírközlési Hatóságtól (a továbbiakban: NMHH). Az üzemeltetés azonban végig veszteséges maradt a vállalat számára, hiszen az éves működési költségek (OPEX) többszázmilliós nagyságrendet értek el, miközben a bevételek, például a parkolási rendszerek és egyéb szolgáltatások kiszolgáltatásából származó jövedelem nem érte el ezt a szintet. A kevés ügyfélből adódóan viszonylag egyszerű volt az átállás megszervezése, vagyis az érintett szereplőket rávenni arra, hogy más hálózatokra váltsanak. Ennek köszönhetően a hadsereg számára 2024-ben már egy „üres” hálózatot lehet átadni, mivel a korábbi felhasználók fokozatosan elhagyták a rendszert.

Az LTE 450 frekvenciasáv alkalmazásának számos lehetősége van. Ezek a hálózatok lehetővé teszik az okoshálózatok és más intelligens megoldások kiépítését. Ezek a dedikált hálózatok megbízható kapcsolatot képesek nyújtani a közműszolgáltatók számára is, mint például a helyi energiaelosztó rendszerek vagy az elektromos jármű töltőállomások. A közlekedési infrastruktúrák, mint például a vasutak is igénylik a nagy területű lefedettséget, így ezen a területen is eredményesen használható. A vidéki területek szélessávú hozzáférési pontjaira is megoldást nyújthat, így ezen elzárt területek összekapcsolására is alkalmas lehet. Ezenkívül a közbiztonság fenntartásában is kulcsszereplő lehet az LTE 450-es hálózat, hiszen a nagy lefedettségnek köszönhetően képes a biztonságos szélessávú adatátvitelre és a gép-gép közötti kommunikációra. A 450 MHz-es frekvenciasáv a honvédelmi alkalmazás során is számos előnyt kínál, hiszen kiválóan alkalmas a hosszú távú kommunikációra. A magasabb frekvenciasávú jelekkel ellentétben ez a frekvenciaállomány alkalmas arra, hogy a rádióhullámok jól terjedjenek a nehéz terepviszonyok esetében is. Ez kulcsfontosságú lehet a katonai műveletek során és a katonai egységek koordinálásában, hiszen elengedhetetlen a megbízható kapcsolat kialakítása.

Összegzésként elmondható, hogy az LTE 450 MHz-es technológiának rendkívül nagy szerepe lehet a jövő vezetékek nélküli kommunikáció modernizálásában, különösen Európában. A harctéren jelenlévő digitalizációs feladatok biztonságos ellátásához szükség van az új, rugalmas, szárazföldi kommunikációs rendszerekre. Véleményem szerint az egyik ilyen

potenciális megoldás lehet vezeték nélküli lefedettséget biztosító LTE 450-es hálózat, hiszen mindamellett, hogy rugalmas, képes a nagy sáv szélesség biztosítására is, figyelembe véve a speciális információelosztási igényeket.

#### **4.2 A TETRA-hálózat elavultsága és az LTE450 lehetőségei**

A magyarországi Egységes Digitális Rádiórendszer (a továbbiakban: EDR) a Terrestrial Trunked Radio (a továbbiakban: TETRA) technológián alapul, amelyet a Pro-M Zrt. üzemeltet. Ezt a hálózatot elsősorban katasztrófavédelmi és vészhelyzeti kommunikációra használják, de közel két évtizede nem került jelentős korszerűsítésre, ezért elavultnak tekinthető. A Pro-M Zrt. eredetileg a Magyar Telekom csoport része volt, de ma már az állami tulajdonú NISZ Zrt. alatt működik, mivel a Magyar Kormány igyekszik a kritikus kommunikációs infrastruktúrát állami ellenőrzés alatt tartani (Mediaworks Hungary Zrt, 2020).

Az elavult TETRA-hálózatra lehetséges megoldás lehet az LTE 450 hálózat, amely kevesebb bázisállomással nagyobb területeket képes lefedni, és titkosított adatkommunikációval magas rendelkezésre állást biztosít. Ez különösen fontos katasztrófavédelmi helyzetekben, ahol a hagyományos kereskedelmi hálózatok túlterheltek lehetnek (Gert Jan Wolf, 2018). Az LTE450 adatátviteli sebessége hozzávetőlegesen 30-40 Mbps körül van, ami elegendő a telefonálásra és az alapvető adatátvitelre, de nem elegendő a nagyméretű videóátvitelre vagy több felhasználó egyidejű kiszolgálására. A jövőben a hálózat fontos szerepet játszhat a gépek közötti kommunikációban (a továbbiakban: M2M) is, például az intelligens mérőrendszerekben vagy az intelligens közlekedési megoldásokban (Mediaworks Hungary Zrt, 2020).

Az LTE450 előnyei közé tartozik a biztonságos kommunikáció biztosítása, különösen zárt és védett környezetben, például katasztrófák esetén, ahol a hadsereg hatékonyan tudja használni. Összességében az LTE450 biztonságos, de kapacitáskorlátozott megoldás, amely bizonyos helyzetekben, különösen katasztrófavédelmi helyzetekben hatékonyan használható, de nem helyettesíti teljes mértékben a TETRA-hálózatot, főleg, ha nagy mennyiségű adatátvitelre van szükség (Gert Jan Wolf, 2018).

### **5 Az adatforgalom növekedése és a hálózatok kihívásai**

A honvédelmi kommunikáció fejlesztése szempontjából kulcsfontosságú, hogy megértsük az adatforgalom folyamatos növekedésének hatását és a hálózati infrastruktúráknak a modern hadviselés dinamikus igényeihez való alkalmazkodásával kapcsolatos kihívásokat.

## 5.1 Cloud computing

A cloud comping felhőalapú számítástechnikát jelent, amelynek célja a számítástechnikai erőforrások (például tárolás) interneten történő tárolása. Alapelveit az önkiszolgálás, a rugalmasság, valamint a széles hálózati hozzáférhetőség jelenti (Mell, Grance and Mell, 2011). Előnyei közé sorolható a költséghatékonyság, a rugalmasság és a magas rendelkezésre állás, hátrányai közé pedig az adatbiztonsági kockázatok, az internetkapcsolati függősége és a lehetséges hálózati késleltetés sorolható (Bello *et al.*, 2021).

A felhőszolgáltatásoknak három típusát különböztethetjük meg:

- IaaS (Infrastructure as a Service): virtuális gépek és tárolási megoldások,
- PaaS (Platform as a Service): fejlesztési platformok és a
- SaaS (Software as a Service): kész szoftveralkalmazások (Wulf *et al.*, 2021).

A felhőalapú szolgáltatások egyre növekvő jelentősége új kihívásokat vet fel, mint például a biztonsági intézkedéseket és a sávszélesség menedzsmentet (Basu *et al.*, 2018).

Bihaly Barbara „*A felhőalapú szolgáltatások alkalmazása az amerikai hadseregben, különös tekintettel a U.S. Army stratégiájára*” című kutatásában megfogalmazza a felhőalapú számítástechnika fontosságát a kormányzati és katonai alkalmazások számára, különös tekintettel az amerikai hadsereg stratégiájára. A technológiai fejlődés és az információs és kommunikációs rendszerektől való növekvő függőség arra készítette a védelmi ügynökségeket, hogy korszerűsítsék rendszereiket, ami a hatékonyság és a költséghatékonyság szempontjából számos előnyt kínál. A felhőmegoldások gyors információmegosztást és rugalmasságot biztosítanak, de biztonsági kérdéseket is felvetnek, amelyeket a CIA-elvek (bizalmasság, integritás, rendelkezésre állás) fényében kell figyelembe venni. A felhőalapú megoldások kulcsfontosságúak a hadsereg informatikai infrastruktúrájának fejlesztésében, mivel lehetővé teszik a központosított adatkezelést és a szoftverek gyors telepítését (Bihaly, 2022).

## 5.2 Edge computing

Az edge computing peremhálózati számítástechnikát jelent, amely a számítástechnikai feladatoknak a helyi és a felhasználókhöz közel történő végrehajtását jelenti, amely által csökkenhet az adatátvitel késleltetése. Előnyei közé tartozik az előbb említett csökkentett késleltetés, a sávszélesség-hatékonyság, valamint a növekvő adatbiztonság, hátrányai között pedig a korlátozott erőforrások és a megoldások komplexitása áll (Cao *et al.*, 2020). Az edge computing alkalmazási területei közé sorolhatóak az IoT eszközök és a mesterséges intelligencia ( a továbbiakban: MI) alkalmazások is (PremSankar, Di Francesco and Taleb,

2018). Az MI alkalmazása is kulcsszerepet játszik a hatékony adatelemzés és döntéshozatal szempontjából.

A honvédelmi kommunikációban egyre fontosabbá válik az edge computing szerepe, mivel lehetővé teszi, hogy az adatokat a helyszínen, a forráshoz közel dolgozzák fel. Ez különösen hasznos a katonai műveletekben, ahol a valós idejű információk gyors elemzése és az azokra való gyors reagálás kritikus fontosságú. Az edge computing technológia lehetővé teszi, hogy az adatok feldolgozása minél közelebb történjen az adat keletkezésének helyéhez, így már csak az értékelt és feldolgozott információ kerül tovább a központba.

### **5.3 Hálózatok alkalmazkodása a cloud és edge computing-hoz**

Ki kell emelni, hogy a hagyományos architektúrák nem képesek hatékonyan kezelni a felhő és peremhálózatok (Vissicchio, Vanbever and Bonaventure, 2014). A modernizálás magába foglalja az Software-Defined Networking (a továbbiakban: SDN) és az Network Functions Virtualization (a továbbiakban: NFV) technológiák bevezetését is. Az SDN technológia lehetővé teszi a központi vezérlést (Haji *et al.*, 2021), az NFV technológia pedig a hálózati funkciók virtualizációjáért felel (Kaur, Mangat and Kumar, 2020). Az 5G technológia előnyeit is ki kell emelni, amely gyorsabb adatátvitelt és alacsonyabb késleltetést biztosít, amely kedvez az edge computingnek (Hassan, Yau and Wu, 2019).

### **5.4 Az IoT és az IoBT**

Az Internet of Things (a továbbiakban: IoT) egy olyan hálózat, amelynek feladata az adatgyűjtés és adatmegosztás. Az Internet of Battlefield Things (a továbbiakban: IoBT) pedig bevonja a biometrikus eszközöket, amelyek a testhez kapcsolódó adatokat gyűjtik és kezelik. A szenzorok és eszközök növekvő száma új adatforgalmat generál, amely kihívásokat okoz a hálózatokon. A nagy adatmennyiség kezelése is nehézséget okoz a sávszélesség és a késleltetés szempontjából. Az IoT és az IoBT új követelményeket támasztanak a hálózatokkal szemben, beleértve a biztonsági intézkedések fokozását és adatkezelését (Hu, Sanjab and Saad, 2019).

Az IoT és az IoBT technológiáinak integrálása a védelmi kommunikációs rendszerekbe innovatív lehetőségeket kínál. Az IoT lehetővé teszi a különböző érzékelők és eszközök hálózatba kapcsolását, amelyek folyamatosan adatokat gyűjtenek és továbbítanak, és így valós idejű információkkal látják el a katonai egységeket.

### **5.5 Az adatforgalom növekedésének kihívásai és megoldási lehetőségei**

Az IoT eszközök növekvő adatforgalma új adatfeldolgozási kihívásokat teremt. A nagy adatfeldolgozási technológiák és az MI kulcsszerepet játszanak az adatok gyors és hatékony

kezelésében. A gépi tanulás segíthet az anomáliák észlelésében, miközben az adatvédelmi kérdések, például a személyes adatok védelme egyre fontosabbá válik. A hálózati infrastruktúra korszerűsítése és a SDN bevezetése javíthatja a biztonságot és csökkentheti a késleltetést. Összességében a Big Data és az MI integrációja is segíteni fogja a jövőbeli adatáramlások hatékony kezelését.

## **6 Értékelés**

### **6.1 H1 hipotézis értékelése**

*H1: A Magyar Honvédség kommunikációs céljainak megvalósítása többségében új hálózatok építése nélkül, a meglévő hálózatok felhasználásával is biztonságos és költséghatékony módon megvalósíthatók.*

Az első hipotézis azt állítja, hogy a Magyar Honvédség kommunikációs céljai többségében új hálózatok építése nélkül, a meglévő hálózatok felhasználásával is biztonságosan és költséghatékony módon megvalósíthatók. Az alábbi információk alapján ezt a hipotézist csak részben lehet alátámasztani, mivel számos tényező utal arra, hogy a meglévő infrastruktúra önmagában nem lesz elegendő.

A jelenlegi MH transzporthálózat számos eleme már elavult. A hálózat nagy részét olyan mikrohullámú összeköttetések alkotják, amelyek nem képesek nagy adatátviteli sebességre, míg más részei régi rézkábeles technológiára épülnek, ami szintén elavult és már nem felel meg a modern katonai igényeknek. Az optikai nyomvonalak jelenléte minimális, és a bérelt vonali kapcsolatok is csak részleges megoldást nyújtanak. Ez egyértelműen jelzi, hogy a meglévő hálózatok állapota nem kielégítő a honvédség kommunikációs igényeinek szempontjából, különösen akkor, ha a modern adatátviteli sebesség és a biztonságos kommunikáció is prioritás. Magyarországon az elmúlt 20 évben jelentős mennyiségű hírközlőhálózati fejlesztés valósult meg, amelyek egy része a Magyar Honvédség számára is potenciálisan felhasználható. Ezek a fejlesztések főként az aggregációs és elérési hálózatokat érintették. Jelentős mértékben hozzájárultak az országos infrastruktúra bővítéséhez, amelybe a honvédség is bekapcsolódhat. Meg kell említeni például a vasúti hálózatokat és a közutak melletti infrastruktúrákat is, amelyek részben felhasználhatók lennének a honvédségi célok megvalósítására. Ezek a meglévő hálózati elemek hozzájárulhatnak a költségek csökkentéséhez, mivel elkerülhetővé válna bizonyos új infrastruktúrák kiépítése. Viszont azt szem előtt kell tartani, hogy a vasút mentén történő építkezés rendkívül összetett az engedélyeztetési folyamat bonyolultsága miatt.

Továbbá a tervezett fejlesztések során fontos meghatározni, hogy milyen mélységben kívánjuk a hálózatot elhelyezni. Minél mélyebb a hálózati elemek elhelyezése, annál drágább lesz a kivitelezése is, azonban figyelembe kell venni a hálózat biztonságát és védelmét is egyaránt.

Ugyanakkor a teljes kommunikációs igények kielégítése érdekében nem lehet megkerülni az új hálózatok kiépítését és modernizációját sem. A jelenlegi infrastruktúra fejlesztéséhez és bővítéséhez komoly beruházásokra van szükség, amelyek során figyelembe kell venni a kiépítendő nyomvonalak hosszát, a megvalósulási helyszínek sajátosságait, és a költségvetési szempontokat is. Ezek a beruházások várhatóan jelentős hatást gyakorolnak majd a rendelkezésre álló humánerőforrás kapacitásaira is. Tekintettel arra, hogy már a korábban megvalósuló Szupergyors Internet Program kivitelezése során is komoly kihívásokat okozott a tervezői és kivitelezői munkaerő ideiglenes hiánya, abból adódóan az ennél lényegesen nagyobb volumenű projekt esetében is különösen gondos és alapos előkészületekre lesz szükség a humánerőforrás területén, hogy a szükséges kapacitás biztosítható legyen.

Összességében az első hipotézis csak részben igazolható a fenti információk alapján. Bár a meglévő hálózatok egy része felhasználható a Magyar Honvédség kommunikációs céljainak megvalósításához, és ez hozzájárulhat a költséghatékonysághoz, a teljes kommunikációs igények kielégítése érdekében az új hálózatok kiépítése és a meglévő hálózatok fejlesztései is elengedhetetlenek.

## **6.2 H2 hipotézis értékelése**

*H2: Az LTE 450-es mobilhálózat a Magyar Honvédség műholdas kommunikációján túlmenően nem lesz önmagában képes biztosítani a vezeték nélküli kommunikációs igényeket, annak fejlesztéséhez csak részben tud majd hozzájárulni.*

Az általam felállított második hipotézis szerint az, hogy az LTE 450-es mobilhálózat nem lesz önmagában elegendő ahhoz, hogy a Magyar Honvédség vezeték nélküli kommunikációs igényeit teljes mértékben kielégítse, és csak részben tud majd hozzájárulni a kommunikáció fejlesztéséhez.

Az LTE 450-es technológia előnye abban rejlik, hogy széles lefedettséget is viszonylag stabil kapcsolatot biztosít, ami előnyös lehet a Magyar Honvédség számára a különböző helyszíneken történő kommunikáció fenntartásában. Azonban ennek a technológiának az adatátviteli sebessége korlátozott, ami nem teszi lehetővé a modern katonai alkalmazások számára szükséges nagy adatmennyiség és sáv szélesség biztosítását. Az LTE 450-es technológia nem

képes kielégíteni az olyan összetett feladatok igényeit, mint például a valós idejű adatátvitel, a műholdas kommunikáció vagy a taktikai adathálózatok működtetése. Ez különösen kritikus a modern hadviselésben, ahol a nagy mennyiségű adat gyors és megbízható továbbítása elengedhetetlen a sikeres műveletekhez.

Az LTE 450-es hálózat tehát nem alkalmas arra, hogy egyedüli megoldásként szolgáljon a Magyar Honvédség vezeték nélküli kommunikációs igényeinek kielégítésére. A technológia inkább kiegészítő szerepet tölthet be a kommunikációs infrastruktúra fejlesztésében, de önmagában nem képes a teljes igények kiszolgálására. Ez összhangban áll a második hipotézis állításával, miszerint az LTE 450-es hálózat csak részben tud hozzájárulni a kommunikációs fejlesztésekhez, és nem jelent önálló megoldást.

Továbbá a Magyar Honvédség számára elengedhetetlen, hogy más technológiai megoldásokat is integráljon a vezeték nélküli kommunikáció fejlesztése érdekében. Az 5G technológia, az optikai hálózatok, valamint a mikrohullámú rendszerek és taktikai adatkapcsolatok biztosíthatják azt a nagyobb sebességet, kapacitást és megbízhatóságot, amelyre a modern katonai műveletekhez szükség van. Ezek a technológiák jelenthetik a teljeskörű kommunikációs infrastruktúra alapját, amely képes lenne kezelni a nagyobb adatmennyiségeket és az összetett katonai alkalmazásokat. Emellett a vezetékes és vezeték nélküli hálózatok integrációja is kiemelten fontos a honvédségi kommunikációs hálózat fejlesztése során.

Ebből adódóan elmondható, hogy az LTE 450-es mobilhálózat önmagában nem lesz elegendő a Magyar Honvédség vezeték nélküli kommunikációs igényeinek kielégítésére, és csak részben tud majd hozzájárulni a kommunikáció fejlesztéséhez. Ahhoz, hogy a honvédség modern és megbízható kommunikációs infrastruktúrát tudjon kialakítani, további technológiai megoldásokra és ezek integrációjára van szükség. A második hipotézis tehát helytállónak bizonyul, mivel az LTE 450-es hálózat nem képes egyedül megfelelni a komplex katonai igényeknek.

## **7 A vizsgálat összegzése és az kutatás végkövetkeztetései**

A kutatás célja a Magyar Honvédség kommunikációs infrastruktúrájának fejlesztésére vonatkozó megoldások feltérképezése volt, különös figyelmet fordítva az LTE 450-es mobilhálózat alkalmazására és a meglévő infrastruktúra kihasználhatóságára. Az elemzések alapján a kutatás arra a végkövetkeztetésre jutott, hogy a honvédség kommunikációs rendszerének átfogó modernizációja elengedhetetlen a jövőbeli katonai műveletek és hadviselés követelményeinek kielégítése szempontjából.

Bár a meglévő hálózatok bizonyos mértékig kihasználhatók, nem nyújtanak megfelelő alapot a teljeskörű és korszerű katonai kommunikációs igények biztosításához. A modern hadviselés során elengedhetetlen a gyors adatátvitel, a megbízhatóság, a széles körű lefedettség, valamint a valós idejű kommunikáció biztosítása, amelyet az elavult infrastruktúrák és a jelenlegi meglévő technológiák nem tudnak maradéktalanul kiszolgálni.

A legújabb technológiai vívmányok (például az 5G, optikai hálózatok, mikrohullámú rendszerek) alkalmazása és integrálása lesz az, amely lehetővé teszi a Magyar Honvédség számára, hogy megfeleljen a modern hadviselés által támasztott igényeknek. Az LTE 450-es mobilhálózat szerepe hasznos kiegészítő megoldásként jelenhet meg, különösen a széleskörű lefedettséget igénylő helyzetekben, azonban önmagában nem lesz képes biztosítani a teljeskörű kommunikációs igényeket.

A kommunikációs rendszerek fejlesztésének sikeres megvalósításához nem csupán technológiai újításokra, hanem alapos előkészítésre, és a megfelelő humán erőforrások rendelkezésre állására is szükség van. Az infrastruktúra-fejlesztésekhez kapcsolódóan kulcsfontosságú, hogy a megfelelő szakértők és kapacitások időben biztosítva legyenek, hiszen a meglévő erőforrások és szakértői háttér korlátozott, ami tovább növeli a fejlesztések komplexitását és költségigényét.

Végül soron a kutatás azt mutatja, hogy a Magyar Honvédség kommunikációs rendszereinek modernizálása nem csupán technológiai szempontból, hanem stratégiai szinten is elengedhetetlen. Az integrált és korszerűsített kommunikációs infrastruktúra növeli a honvédség operatív képességeit, javítja a döntéshozatali folyamatok gyorsaságát és pontosságát, valamint lehetővé teszi a nemzetközi együttműködések és műveletek sikeres végrehajtását. A jövőbeli katonai kihívások kezeléséhez szükséges rugalmasság, biztonság és hatékonyság biztosítása érdekében a Magyar Honvédség számára elengedhetetlen a megfelelő kommunikációs rendszer kiépítése és fenntartása.

## **8 Jegyzékek**

### **8.1 Ábrajegyzék**

|                                                                                                                                                                                   |    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 1. ábra NATO-tagországok GDP arányos védelmi kiadásai – saját szerkesztés (forrás: NATO Public Diplomacy Division, 2024).....                                                     | 10 |
| 2. ábra Magyarország védelmi kiadásainak alakulása 2014-2024 között 2015-ös árfolyamon-saját szerkesztés (forrás: NATO Public Diplomacy Division, 2024).....                      | 11 |
| 3. ábra A védelmi kiadások megoszlása fő kategóriák szerint 2024-ben – saját szerkesztés (NATO Public Diplomacy Division, 2024). ....                                             | 12 |
| 4. ábra A védelmi kiadások megoszlása fő kategóriák szerint 2014-ben – saját szerkesztés (NATO Public Diplomacy Division, 2024). ....                                             | 12 |
| 5. ábra NCISG struktúra (forrás: <a href="https://ncisg.nato.int/about-us">https://ncisg.nato.int/about-us</a> ) .....                                                            | 14 |
| 6. ábra Szabványosítási folyamat – saját szerkesztés (61/2007. (III. 31.) Korm. rendelet a katonai szabványosítás sajátos szabályairól című törvény alapján).....                 | 17 |
| 7. ábra Zárt infokommunikációs hálózatok funkcionális csoportosítása – saját szerkesztés ...                                                                                      | 20 |
| 8. ábra Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózatának rendszerek – saját szerkesztés.....                                                                     | 24 |
| 9. ábra Optikai Hálózati lefedettség Magyarországon (forrás: <a href="https://www.invitech.hu/szolgáltatasi-teruletek">https://www.invitech.hu/szolgáltatasi-teruletek</a> )..... | 27 |
| 10. ábra A MH KCEHH fejlesztésének jogszabályi előírásai – saját szerkesztés (55/2013. évi HM utasítás alapján).....                                                              | 28 |
| 11. ábra A 380 MHz, 410 MHz és a 450 MHz frekvenciasávok globális használta, különböző alkalmazásokra fókuszálva (450 MHz Alliance, 2023) .....                                   | 33 |

### **8.2 Táblázatjegyzék**

|                                                                                                                                      |    |
|--------------------------------------------------------------------------------------------------------------------------------------|----|
| 1. táblázat Szélessávú infrastruktúrafejlesztési pályázatok .....                                                                    | 5  |
| 2. táblázat Az NSB adatai és feladatai (forrás: <a href="https://ncisg.nato.int/about-us">https://ncisg.nato.int/about-us</a> )..... | 15 |

### 8.3 Rövidítések jegyzéke

| <b>Rövidítés</b>       | <b>Magyarázat</b>                                                                                                 |
|------------------------|-------------------------------------------------------------------------------------------------------------------|
| <i>AES</i>             | Advanced Encryption Standard – Haladó titkosítási szabvány                                                        |
| <i>C4ISR</i>           | Command, Control, Communications, Computers, ISR – Parancsnokság, irányítás, kommunikáció, hírszerzés, felderítés |
| <i>CDMA hálózatok</i>  | Code Division Multiple Access – Kódosztásos többszörös hozzáférés                                                 |
| <i>CIA-elvek</i>       | Confidentiality, Integrity, Availability – bizalmasság, integritás, rendelkezésre állás                           |
| <i>CIS</i>             | Communication and Information Systems – Kommunikációs és információs rendszerek                                   |
| <i>Cloud computing</i> | Felhőalapú számítástechnika                                                                                       |
| <i>DCM</i>             | Deployed Communication Modules – Telepített kommunikációs modulok                                                 |
| <i>DESI</i>            | Digital Economy and Society Index – A digitális gazdaság és társadalom fejlettségét mérő mutató                   |
| <i>DF</i>              | Disk Free Unix Command – Szabad lemezterületet mutató Unix parancs                                                |
| <i>DG ECFIN</i>        | Directorate-General for Economic and Financial Affairs – NATO Gazdasági és Pénzügyi Főigazgatósága                |
| <i>DWDM</i>            | Dense Wavelength Division Multiplexing – Sűrű hullámhossz-multiplexelési technológia                              |
| <i>Edge computing</i>  | Peremhálózati számítástechnika                                                                                    |
| <i>EDR1</i>            | Event Data Recorder 1 – Eseményadat-rögzítő 1. verzió                                                             |
| <i>EU</i>              | Európai Unió                                                                                                      |
| <i>GSM-R</i>           | Global System for Mobile Communications - Railway – Vasúti GSM-alapú kommunikációs rendszer                       |
| <i>HM</i>              | Honvédelmi Minisztérium                                                                                           |
| <i>IaaS</i>            | Infrastructure as a Service – virtuális gépek és tárolási megoldások                                              |
| <i>IDS/IPS</i>         | Intrusion Detection/Prevention Systems – Behatolásészlelő/megelőző rendszerek                                     |
| <i>IoBT</i>            | Internet of Battlefield Things – Harcmezői dolgok internete                                                       |

|                      |                                                                                       |
|----------------------|---------------------------------------------------------------------------------------|
| <i>IoT</i>           | Internet of Things – Dolgok internete                                                 |
| <i>IRIS</i>          | Magyar Honvédség felderítő rendszerei                                                 |
| <i>K+F feladatok</i> | Kutatás-fejlesztési feladatok                                                         |
| <i>KGIR</i>          | Katonai Gazdálkodási és Informatikai Rendszer                                         |
| <i>KMR</i>           | Közép-Magyarország Régió                                                              |
| <i>KSZKB</i>         | Katonai Szabványügyi Koordinációs Bizottság                                           |
| <i>Link 16/22</i>    | Katonai adatátviteli rendszerek                                                       |
| <i>LTE</i>           | Long Term Evolution (4G mobiltechnológia)                                             |
| <i>Mbps</i>          | Megabit per másodperc (adatátviteli sebesség)                                         |
| <i>MH</i>            | Magyar Honvédség                                                                      |
| <i>MH KCEHH</i>      | Magyar Honvédség kormányzati célú hírközlő hálózata                                   |
| <i>MHz</i>           | Megahertz, frekvencia mértékegysége                                                   |
| <i>MI</i>            | Mesterséges intelligencia                                                             |
| <i>MSZT</i>          | Magyar Szabványügyi Testület                                                          |
| <i>MTA</i>           | Magyar Tudományos Akadémia                                                            |
| <i>NATO</i>          | North Atlantic Treaty Organization – Észak-atlanti Szerződés Szervezete               |
| <i>NATO FMN</i>      | NATO Future Mission Network – NATO Jövőbeli Küldetési Hálózata                        |
| <i>NDPP</i>          | NATO Defence Planning Process – NATO Védelmi Tervezési Folyamat                       |
| <i>NFV</i>           | Network Functions Virtualization – Hálózati funkciók virtualizálása                   |
| <i>NISZ Zrt.</i>     | Nemzeti Infokommunikációs Szolgáltató                                                 |
| <i>NMHH</i>          | Nemzeti Média- és Hírközlési Hatóság                                                  |
| <i>NNEC</i>          | NATO Network Enabled Capability – NATO hálózati alapú képesség                        |
| <i>NSB</i>           | NATO Signal Battalion – NATO Jelzőzászlóalj                                           |
| <i>NSDD</i>          | NATO Standardization Document Database – NATO Szabványosítási Dokumentumok Adatbázisa |
| <i>NSO</i>           | NATO Standardization Office – NATO Szabványügyi Hivatal                               |
| <i>NTG</i>           | National Telecommunications Backbone – Nemzeti Távközlési Gerinchálózat               |

|                        |                                                                                                            |
|------------------------|------------------------------------------------------------------------------------------------------------|
| <i>OECD</i>            | Organisation for Economic Co-operation and Development – Gazdasági Együttműködési és Fejlesztési Szervezet |
| <i>OPEX</i>            | Operational expenditure – üzemeltetési / működési költségek                                                |
| <i>PaaS</i>            | Platform as a Service – fejlesztési platformok                                                             |
| <i>Pop</i>             | Point of Presence – Hozzáférési pont                                                                       |
| <i>Pro-M Zrt.</i>      | Professzionális Mobilszolgáltató Zártkörűen Működő Részvénytársaság                                        |
| <i>QoS protokollok</i> | Quality of Service protocols – Minőségi szolgáltatás protokollok                                           |
| <i>SaaS</i>            | Software as a Service – kész szoftveralkalmazások                                                          |
| <i>SDH hálózat</i>     | Synchronous Digital Hierarchy – Szinkron Digitális Hierarchia                                              |
| <i>SDN</i>             | Software-Defined Networking – Szoftver által definiált hálózat                                             |
| <i>STANAG</i>          | Standardization Agreement – Szabványosítási Megállapodás                                                   |
| <i>TDL</i>             | Tactical Data Link – Taktikai adatkapcsolat                                                                |
| <i>TETRA</i>           | Terrestrial Trunked Radio – digitális rádiókommunikációs technológia                                       |
| <i>V4-es országok</i>  | Visegrádi négyek országai                                                                                  |
| <i>WDM</i>             | Wavelength Division Multiplexing – Hullámhossz-multiplexelés                                               |
| <i>Zrínyi 2026 HHP</i> | Zrínyi Honvédelmi és Haderőfejlesztési Program                                                             |

## 9 Érintett jogszabályok

- Magyarország Alaptörvénye (2011. április 25.)
- 55/2013. (IX. 13.) HM utasítás a Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózatának békeidejű üzemeltetési és felügyeleti rendjéről, valamint a központilag biztosított szolgáltatások igénybevételének szabályairól
- 61/2007. (III. 31.) Korm. rendelet a katonai szabványosítás sajátos szabályairól
- 1999. évi I. törvény a Magyar Köztársaságnak az Észak-atlanti Szerződéshez történő csatlakozásáról és a Szerződés szövegének kihirdetéséről
- 1995. évi XXVIII. törvény a nemzeti szabványosításról

## 10 Irodalomjegyzék<sup>2</sup>

450 MHz Alliance (2023) ‘Annual Global Update’. Available at: <https://450alliance.org/wp-content/uploads/2024/01/450Alliance-Annual-Global-Update-2023-ver-P.pdf>.

Abikoye, O.C. *et al.* (2019) ‘Modified Advanced Encryption Standard Algorithm for Information Security’, *Symmetry*, 11(12), p. 1484. Available at: <https://doi.org/10.3390/sym11121484>.

B. Müller T. (2018) ‘ADATOK A MAGYAR HONVÉDSÉGRŐL’, *Képviselői Információs Szolgálat*, 2018/7. *Infotabló*. [Preprint]. Available at: [https://www.parlament.hu/documents/10181/1489583/Infotablo\\_2018\\_7\\_honvedelmi\\_adatok.pdf/b576c3a8-d457-8db0-62e9-749482615fe1](https://www.parlament.hu/documents/10181/1489583/Infotablo_2018_7_honvedelmi_adatok.pdf/b576c3a8-d457-8db0-62e9-749482615fe1).

B. Müller, T. (2020) ‘Honvédelmi fejlesztések’, *Honvédelmi fejlesztések – Képviselői Információs Szolgálat*, 2020/64. *Infotabló* [Preprint]. Available at: [https://www.parlament.hu/documents/10181/4483210/Infotablo\\_2020\\_64\\_honvedelmi\\_fejlesztések.pdf/e2a8d83d-4173-531e-4254-250d61a0d1ee?t=1606429485826](https://www.parlament.hu/documents/10181/4483210/Infotablo_2020_64_honvedelmi_fejlesztések.pdf/e2a8d83d-4173-531e-4254-250d61a0d1ee?t=1606429485826).

Babos, T. *et al.* (2021) ‘Digital security policy in the cyber space’. MATE. Available at: [https://press.mater.uni-mate.hu/151/8/kibereng-final-digit\\_j%C3%B3%20ISBN-nel.pdf#page=41](https://press.mater.uni-mate.hu/151/8/kibereng-final-digit_j%C3%B3%20ISBN-nel.pdf#page=41).

Basu, S. *et al.* (2018) ‘Cloud computing security challenges & solutions-A survey’, in *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*. 2018 *IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 347–356. Available at: <https://doi.org/10.1109/CCWC.2018.8301700>.

Bello, S.A. *et al.* (2021) ‘Cloud computing in construction industry: Use cases, benefits and challenges’, *Automation in Construction*, 122, p. 103441. Available at: <https://doi.org/10.1016/j.autcon.2020.103441>.

Bihaly B. (2022) ‘A felhőalapú szolgáltatások alkalmazása az amerikai haderőben, különös tekintettel a U.S. Army stratégiájára’, *Hadmérnök*, 17(4), pp. 113–129. Available at: <https://doi.org/10.32567/hm.2022.4.8>.

---

<sup>2</sup> A tanulmány megírása során alkalmazásra került mesterséges intelligencia is (DeepL, OpenAI, Zotero), amely segítette az idegen nyelvű szövegek fordítását, az adatok feldolgozását és a hivatkozások kezelését.

Bihl, T.J. and Talbert, M. (2020) 'Analytics for Autonomous C4ISR within e-Government: a Research Agenda'.

Bihun, N. *et al.* (2019) 'ANALYSIS OF THE PECULIARITIES OF THE COMMUNICATION ORGANIZATION IN NATO COUNTRIES', *Advanced Information Systems*, 3(4), pp. 39–44. Available at: <https://doi.org/10.20998/2522-9052.2019.4.05>.

Cao, K. *et al.* (2020) 'An Overview on Edge Computing Research', *IEEE Access*, 8, pp. 85714–85728. Available at: <https://doi.org/10.1109/ACCESS.2020.2991734>.

European Commission (2024) *The Digital Economy and Society Index (DESI) | Shaping Europe's digital future*. Available at: <https://digital-strategy.ec.europa.eu/en/policies/desi> (Accessed: 22 October 2024).

Farkas, T. (2020) 'Communication and Information Services – NATO Requirements, Part I', *Land Forces Academy Review*, 25(4), pp. 281–289. Available at: <https://doi.org/10.2478/raft-2020-0034>.

Gert Jan Wolf (2018) *Pro-M Prepares for the Future of Critical Communications in Hungary, The Critical Communications Review*. Available at: <https://www.criticalcommunicationsreview.com/ccr/news/100645/pro-m-prepares-for-the-future-of-critical-communications-in-hungary> (Accessed: 21 October 2024).

Haji, S.H. *et al.* (2021) 'Comparison of Software Defined Networking with Traditional Networking', *Asian Journal of Research in Computer Science*, 9(2), pp. 1–18. Available at: <https://doi.org/10.9734/ajrcos/2021/v9i230216>.

Hassan, N., Yau, K.-L.A. and Wu, C. (2019) 'Edge Computing in 5G: A Review', *IEEE Access*, 7, pp. 127276–127289. Available at: <https://doi.org/10.1109/ACCESS.2019.2938534>.

Honvédelmi Minisztérium (2012) 'Magyarország Nemzeti Katonai Stratégiája'. Available at: [https://2015-2019.kormany.hu/download/a/40/00000/nemzeti\\_katonai\\_strategia.pdf](https://2015-2019.kormany.hu/download/a/40/00000/nemzeti_katonai_strategia.pdf).

Honvédelmi Minisztérium (2021) *Nemzeti Katonai Stratégia - Honvédelem*. Available at: <https://honvedelem.hu/hirek/nemzeti-katonai-strategia.html> (Accessed: 21 October 2024).

Hu, Y., Sanjab, A. and Saad, W. (2019) ‘Dynamic Psychological Game Theory for Secure Internet of Battlefield Things (IoBT) Systems’, *IEEE Internet of Things Journal*, 6(2), pp. 3712–3726. Available at: <https://doi.org/10.1109/JIOT.2018.2890431>.

Invitech. (no date) *Több mint 10.000 km hosszú optikai gerinchálózat*. Available at: <https://www.invitech.hu/szolgaltatasi-teruletek> (Accessed: 19 October 2024).

Kaló J. et al. (2022) *Honvédelmi alapismeretek*. Ludovika Egyetemi Kiadó. Available at: <https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/17745> (Accessed: 19 October 2024).

Kaur, K., Mangat, V. and Kumar, K. (2020) ‘A comprehensive survey of service function chain provisioning approaches in SDN and NFV architecture’, *Computer Science Review*, 38, p. 100298. Available at: <https://doi.org/10.1016/j.cosrev.2020.100298>.

Khan, N.A. et al. (2021) ‘Proposing an Algorithm for UAVs Interoperability: MAVLink to STANAG 4586 for Securing Communication’, in S.-L. Peng et al. (eds) *Intelligent Computing and Innovation on Data Science*. Singapore: Springer Nature, pp. 413–423. Available at: [https://doi.org/10.1007/978-981-16-3153-5\\_44](https://doi.org/10.1007/978-981-16-3153-5_44).

KIFÜ (no date a) *Kormányzati hálózatok konszolidációja, kapacitásainak, teljesítményének növelése – KIFÜ*. Available at: <https://kifu.gov.hu/projekt/kormanyzati-halozatok-konszolidacioja-kapacitasainak-teljesitmenyenek-novelese/> (Accessed: 22 October 2024).

KIFÜ (no date b) ‘Kormányzati hálózatok konszolidációja, kapacitásainak, teljesítményének növelése és intézmények hálózati hozzáféréseinek, kapcsolatainak fejlesztése – KIFÜ’. Available at: <https://kifu.gov.hu/projekt/kormanyzati-halozatok-konszolidacioja-kapacitasainak-teljesitmenyenek-novelese-es-intezmenyek-halozati-hozzafereseinek-kapcsolatainak-fejlesztese/> (Accessed: 22 October 2024).

Kis G. (2017) ‘Az állami beavatkozás szerepe az infokommunikációs infrastruktúra kialakításában - 2011/6. (47.), 231-238. o.’, *INFOKOMMUNIKÁCIÓ ÉS JOG*, 28 June. Available at: <https://infojog.hu/kis-gergely-az-allami-beavatkozas-szerepe-az-infokommunikacios-infrastruktura-kialakitasaban-20116-47-231-238-o/> (Accessed: 22 October 2024).

Kormány Információ (2019) 'A HAZA VÉDELME, A NEMZET SZOLGÁLATA'. Available at: [https://honvedelem.hu/files/files/116159/honvedseg\\_kiadvany\\_165x235mm\\_v2\\_6\\_.pdf](https://honvedelem.hu/files/files/116159/honvedseg_kiadvany_165x235mm_v2_6_.pdf).

Kovács, Z. (2022) 'A Magyar Honvédség harcászati rádiócsalád fejlesztésének helyzete a Zrínyi Honvédelmi és Haderőfejlesztési Program tükrében'. Hadmérnök.

Lunn, S. and Williams, N. (2017) *NATO Defence Spending: The Irrationality of 2%*. European Leadership Network. Available at: <https://www.jstor.org/stable/resrep17424> (Accessed: 19 October 2024).

Magyar Nemzet (2022) *NATO: Minden fontos tudnivaló egy helyen az Észak-atlanti Szerződés Szervezetéről, NATO: Minden fontos tudnivaló egy helyen az Észak-atlanti Szerződés Szervezetéről*. Available at: <https://magyarnemzet.hu/kulfold/2022/05/nato-minden-fontos-tudnivalo-egy-helyen-az-eszak-atlanti-szerzodes-szervezeterol> (Accessed: 21 October 2024).

Mediaworks Hungary Zrt (2020) 'Magyarországon az elsők között épült ki az LTE450', *Figyelő*. Available at: <https://figyelo.hu/pr/magyarorszagon-az-elsok-kozott-epult-ki-az-lte450-86314/> (Accessed: 21 October 2024).

Mell, P., Grance, T. and Mell, P. (2011) *The NIST Definition of Cloud Computing*. NIST Special Publication (SP) 800-145. National Institute of Standards and Technology. Available at: <https://doi.org/10.6028/NIST.SP.800-145>.

Military Sphere Editorial Team (2024) 'Decoding Hungarian Military Communication Systems - Military Sphere'. Available at: <https://militarysphere.com/hungarian-military-communication-systems/> (Accessed: 19 October 2024).

MTI (2022) *A magyar haderőfejlesztés hozzájárul az európai védelmi képességek megerősítéséhez - Honvédelem*. Available at: <https://honvedelem.hu/hirek/a-magyar-haderofejlesztes-hozzajarul-az-europai-vedelmi-kepessegek-megerositeséhez.html> (Accessed: 21 October 2024).

MTI (2024) *Együttműködési megállapodást kötött a Honvédelmi Minisztérium és az MTA*, <https://kormany.hu>. Available at: <https://kormany.hu/hirek/egyuttmukodesi-megallapodast-kotott-a-honvedelmi-miniszterium-es-az-mta> (Accessed: 19 October 2024).

NATO (2024a) *Cyber defence, NATO*. Available at: [https://www.nato.int/cps/en/natohq/topics\\_78170.htm](https://www.nato.int/cps/en/natohq/topics_78170.htm) (Accessed: 21 October 2024).

NATO (2024b) *The North Atlantic Treaty, NATO*. Available at: [https://www.nato.int/cps/en/natohq/official\\_texts\\_17120.htm](https://www.nato.int/cps/en/natohq/official_texts_17120.htm) (Accessed: 21 October 2024).

NATO OTAN (2022) *NATO - Topic: Standardization*. Available at: [https://www.nato.int/cps/en/natohq/topics\\_69269.htm](https://www.nato.int/cps/en/natohq/topics_69269.htm) (Accessed: 19 October 2024).

NATO Public Diplomacy Division (2024) 'Defence Expenditure of NATO Countries (2014-2024)'. Available at: [https://www.nato.int/nato\\_static\\_fl2014/assets/pdf/2024/6/pdf/240617-def-exp-2024-en.pdf](https://www.nato.int/nato_static_fl2014/assets/pdf/2024/6/pdf/240617-def-exp-2024-en.pdf).

*NATO Term - CIMIC-COE* (no date) *Civil-Military Cooperation Centre of Excellence*. Available at: <https://www.cimic-coe.org/cimic/Definitions/NATO-Term/> (Accessed: 21 October 2024).

*NCISG | About us* (no date). Available at: <https://ncisg.nato.int/about-us> (Accessed: 19 October 2024).

NISZ Zrt. (no date a) *GSM-R rendszer beszerzése és kapcsolódó szolgáltatások (szakaszolt projekt)*. Available at: <https://nisz.hu/projektjeink/gsm-r-rendszer-beszerzese-es-kapcsolodo-szolgaltat-d37> (Accessed: 22 October 2024).

NISZ Zrt. (no date b) *Nemzeti Távközlési Gerinchálózat (NTG) fejlesztése*. Available at: <https://nisz.hu/projektjeink/nemzeti-tavkozlesi-gerinchalozat-ntg-fejlesztese-d21> (Accessed: 22 October 2024).

NKFIH (2017) *Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal | Kutatási, fejlesztési és innovációs stratégia*. Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal, 2008. Minden jog fenntartva. Available at: <https://nkfi.gov.hu/hivatalrol/strategia-alkotas/kutatasi-fejlesztési-innovációs-strategia> (Accessed: 21 October 2024).

Oakley, J.G. (2019) *Professional Red Teaming: Conducting Successful Cybersecurity Engagements*. Apress.

PALYAZAT.gov.hu (2012) *GOP-2012-3.1.2 - Szélessávú körzethálózati fejlesztések támogatása (A PÁLYÁZAT LEZÁRULT!)* | *Széchenyi Terv Plusz*. Available at: <https://archive.palyazat.gov.hu/doc/3487> (Accessed: 22 October 2024).

PALYAZAT.gov.hu (2022) *GINOP-3.4.2-VEKOP-15 Intézmények hálózati hozzáféréseinek, kapcsolatainak fejlesztése (A PÁLYÁZAT LEZÁRULT!)* | *Széchenyi Terv Plusz*. Available at: <https://archive.palyazat.gov.hu/ginop-342-vekop-15-intzmnyek-hlzlzati-hozzfrseinek-kapcsolatainak-fejlesztse> (Accessed: 22 October 2024).

PALYAZAT.gov.hu (2024) *GINOP-3.4.1-20 Újgenerációs NGA és felhordó hálózatok fejlesztése (2. ütem)(LEJÁRT BENYÚJTÁSI HATÁRIDŐ!)* | *Széchenyi Terv Plusz*. Available at: <https://archive.palyazat.gov.hu/fhd-5712-ginop-341-20-jgenercis-nga-s-felhord-hlzlzatos-fejlesztse-2-tem#> (Accessed: 22 October 2024).

Pályázati Portál (2017) *Közlemény - Megjelent az NFM-KMR-2016 felhívás kitöltő programja - Pályázati Portál*. Available at: <https://www.palyazat.gov.hu/kozlemenyek/megjelent-az-nfm-kmr-2016-felhvs-kitlt-programja> (Accessed: 22 October 2024).

Pölöskei, J. (2021) 'Képességalapú haderőtervezés'. Honvédség Szemle.

Porteleki P. (2020) 'IoT integráció a Microsoft Dynamics ERP rendszerben', *Computers & Learning*, 3(1), pp. 1–11.

PremSankar, G., Di Francesco, M. and Taleb, T. (2018) 'Edge Computing for the Internet of Things: A Case Study', *IEEE Internet of Things Journal*, 5(2), pp. 1275–1284. Available at: <https://doi.org/10.1109/JIOT.2018.2805263>.

Simo, Z., Iantovics, L.B. and Tokody, D. (2023) 'Fejlett ágens alapú behatolásérzékelő rendszerek', *Production Systems and Information Engineering*, 11(2), pp. 43–48. Available at: <https://doi.org/10.32968/psaie.2023.2.4>.

Szabados, J.J. (2018) 'A logisztikai információs rendszer szükségessége és fejlesztési lehetőségei a Magyar Honvédségben'. Honvédségi Szemle.

Szeleczki S. and Farkas T. (2022) 'A Magyar Honvédség harcászati infokommunikációs hálózatainak korszerűsítési irányelvei', *Hadtudomány*, 32(1), pp. 74–92. Available at: <https://doi.org/10.17047/HADTUD.2022.32.1.74>.

Tőreki, Á. (2010) 'A Magyar Hadsereg stacioner kommunikációs rendszerének vizsgálata', *Hadmérnök V. Évfolyam 1. szám - 2010. március* [Preprint]. Available at: [http://hadmernok.hu/2010\\_1\\_toreki.pdf](http://hadmernok.hu/2010_1_toreki.pdf).

Tóth L. (2017) 'A végrehajtó hatalom prezidencializálódásának egyes aspektusai a II. és III. Orbán-kormányok esetében', *Parlamenti Szemle* [Preprint]. Available at: <https://parlamentiszemle.hu/wp-content/uploads/2018/02/parlamentiszemle-toth-laszlo.pdf>.

Tóth T. (2018) 'A NATO Kibervédelmi Kiválósági Központ bemutatása', *Nemzetbiztonsági Szemle*, 6(4), pp. 48–62.

Vissicchio, S., Vanbever, L. and Bonaventure, O. (2014) 'Opportunities and research challenges of hybrid software defined networks', *SIGCOMM Comput. Commun. Rev.*, 44(2), pp. 70–75. Available at: <https://doi.org/10.1145/2602204.2602216>.

Wulf, F. *et al.* (2021) 'IaaS, PaaS, or SaaS? The Why of Cloud Computing Delivery Model Selection : Vignettes on the Post-Adoption of Cloud Computing', in: *Proceedings of the 54th Hawaii International Conference on System Sciences, 2021*, pp. 6285–6294. Available at: <https://opus4.kobv.de/opus4-oth-regensburg/frontdoor/index/index/docId/791> (Accessed: 22 October 2024).