NEMZETI KÖZSZOLGÁLATI EGYETEM
HADTUDOMÁNYI ÉS HONVÉDTISZTKÉPZŐ KAR
KATONAI MŰSZAKI DOKTORI ISKOLA

Megyeri Lajos

A katonai műveletek infokommunikációs támogatásának biztonsága katonai és polgári információs infrastruktúra alkalmazásával.

Doktori (PhD) értekezés

Témavezető:
Dr. Farkas Tibor (PhD)
egyetemi docens

……

BUDAPEST, 2023.

TARTALOMJEGYZÉK

Bevezetés, fogalmak tisztázása **4**

A tudományos probléma megfogalmazása……**8**

Hipotézisek: **10**

A kutatási téma körülhatárolása **11**

Területi behatárolás: **12**

Kutatási célok **13**

Kutatási módszerek **13**

Az értekezés felépítése **14**

Fogalmi és formai meghatározások: **15**

1. Fogalmak értelmezése **16**

1.1. Katonai műveletek fogalmi meghatározása **16**

1.1.1. Háborús műveletek 18

1.1.2.Nem háborús műveletek 19

1.1.3.A nem háborús katonai műveletek felosztása: 19

1.2. Az Infokommunikáció fogalomrendszere: **23**

1.2.1. Kiberműveletek 27

1.3. Információvédelem fogalomrendszere **28**

1.3.1. Információbiztonság 29

1.3.2.Kockázatkezelés 42

Összefoglalás,következtetések……**46**

2. A katonai műveletek infokommunikációs támogatásának lehetőségei katonai információs infrastruktúra alkalmazásával. **488**

2.1. Nemzeti stacioner rendszerek **499**

2.1.1. Nemzeti stacioner hírhálózat 51

2.1.2.NATO stacioner hírhálózat 52

2.1.3. Katonai műholdas rendszerek 55

A Műholdas kommunikációs rendszerek általános jellemzői: 57

A katonai kommunikációs műholdak 66

2.2. Telepíthető (Mobilizálható) rendszerek **68**

2.3. A katonai infokommunikációs rendszerek adatkezelésének információbiztonsága **73**

2.3.1. Nem minősített adatok védelmének lehetőségei 73

Elektronikus aláírás 77

2.3.2. Minősített adatok védelmének lehetőségei. 79

A nemzeti minősített adatok minősítési szintjei: 81
A biztonsági területek típusai: 85
Minősítés szükségessége..... 94
Papír alapú minősített adatok:..... 95
Hang alapú minősített adatok 96
2.4.Nemzeti és NATO adatok minősítési eljárásrendje 99
2.4.1.Új adatvédelmi osztály szükségessége röviden és részletesen. 102
Összefoglalás,következtetések…...……...……104
3. A katonai műveletek infokommunikációs támogatásának lehetőségei nem katonai információs infrastruktúra alkalmazásával 108
3.1. Kormányzati, közszolgálati célú rendszerek, információvédelmi eljárásrendek, alkalmazhatóságuk katonai igénybevételre. 109
3.1.1.Stacioner elemek, információvédelmi eljárásrendek, alkalmazhatóságuk katonai igénybevételre:..……109
3.2. Kereskedelmi célú rendszerek, információvédelmi eljárásrendek, alkalmazhatóságuk katonai igénybevételre: 116
3.2.1. Polgári műholdas szolgáltatások igénybevétele 116
3.3.Nem minősített adat továbbítása polgári infrastruktúra igénybevételével: 126
3.4. Rejtjelzés..... 129
3.4.1..Rejtjelzés szükségessége és lehetőségei: 129
3.4.2. Rejtjelző eszközök: 13231
3.4.3. A rejtjelzés helyszínei:..... 138
3.4.4.TEMPEST..... 142
3.5. Összegzés, következtetések: ..... Hiba! A könyvjelző nem létezik.
ÖSSZEFOGLALÓ..... 147
Javaslataim, gyakorlati felhasználhatóság:..……151
Irodalomjegyzék:……154
Publikációs jegyzék:...……159

„Si vis pacem, para bellum!”[1]

Bevezetés, fogalmak tisztázása

A technikai eszközök és a társadalmak átalakulásával, fejlődésével együtt a világ hadseregei is folyamatosan formálódnak. Esetenként a társadalmi fejlődés zászlóshajói, új találmányok mecénásai, ötletgazdái, máskor a civil társadalom vívmányainak másodlagos használói. Ez nagyban függ attól is, hogy az adott társadalom mennyire becsüli meg saját védelmi erőit. Tény, hogy a katona nem termel közvetlenül anyagi javakat azonban jelenléte minden korban elengedhetetlen egy önálló nemzetállam megalakulásához, fennmaradásához. Az ókor egyik neves római költője, Publius Flavius Vegetius Renatus szerint:„ Ha békét akarsz, készülj a háborúra”

A 20. század konfliktusaiban még a tömeghadseregeké volt a főszerep, a döntő csatákat többnyire a lakott területektől távoli hadszíntereken vívták. Véleményem szerint a technikai eszközök fejlődésével és a társadalmak átalakulásával a hadseregek struktúrája is nagymértékben megváltozott.

A Haza fegyveres védelméért felelős katonai szervezet is az államalapítás óta folyamatosan változik. A rendszerváltást megelőzően a Magyar Néphadsereg létszáma kb. 200 000 fő volt. A honvédelmet már akkor nemzetközi kötelékben (Varsói Szerződés)[2] tervezték megvalósítani. A mai Magyar Honvédség létszáma az akkori, tényleges szolgáltot teljesítő sorállományú katonákkal együtt szervezett, számos önálló katonai egységgel rendelkező haderőnek csak a 10-20 százaléka. Hazánk védelme most béke állapotban sorállományú katonák szolgálata nélkül, baráti államokkal közös katonai szövetségen alapul.

„Az ország katonai biztonsága egymást kiegészítő pillérekre épül. Az egyik pillér a korszerű nemzeti haderő, amelyet a regionális együttműködés magasabb szintű védelmi rendszerei és együttműködési formái egészítenek ki. Biztonságunk katonai dimenziójának másik pillérét a NATO által biztosított kollektív védelem alkotja”(Magyarország Nemzeti Katonai Stratégiája, 2021)

Tapasztalatom alapján a Magyar Honvédség létszámából adódón kiemelten fontos, hogy a rendelkezésre álló anyagi és humán erőforrásokat a legoptimálisabban kihasználva, akár

[1] Ha békét akarsz, készülj a háborúra - Publius Flavius Vegetius Renatus

[2] A Varsói Szerződés a közép- és kelet-európai szocialista országok védelmi katonai-politikai szervezete volt. Varsóban, Lengyelországban alapították meg 1955. május 14-én a Szovjetunió javaslatára. 1991-ben bomlott föl.

a megszokott, szabályzatokban rögzített harceljárásokat újragondolva teljesítse rendeltetésből adódó és nemzetközi szerződések által előírt feladatait.

Korunk egyik legjelentősebb, a mindennapi életet és a védelmi stratégiákat egyaránt átalakító változása a számítástechnika ugrásszerű és jelenleg is folyamatos fejlődése. A kommunikációs eszközök (telefon, rádió, telemédia) és az internet megjelenésével kialakult informatikai rendszerek kezdetben elkülönülten működtek. A félvezető alapú technika és ennek alapján a digitalizáció fejlődésével az analóg jelfeldolgozó eszközök egyre inkább kiszorultak az elektronikai ipar eszköztárából. A Magyar Honvédségben az áttérés a digitális technológia alkalmazására az erőforrások szűkössége és a NATO tagországok haderőivel való minimum interoperabilitás fenntartása érdekében csak lépcsőzetesen került sor. E sorok írásakor is működnek analóg jelfeldolgozáson alapuló infokommunikációs rendszerek, bár felhasználásuk köre folyamatosan szűkül. Még a legmodernebb harcászati rádióeszközök is alkalmazhatóak szükség esetén analóg AM/FM[3] üzemmódban. Ennek ellenére, jelenleg amikor adatfeldolgozó rendszerekre gondolunk, ezek alatt már döntő többségben a modern szóhasználatban meggyökeresedett „infokommunikáció” szót értünk. A híradó eszközök döntő többsége szoftver alapú, számítógép vezérlésű, digitális jelfeldolgozással működik. A katonai műveletek támogatásában alkalmazott infokommunikációs eszközök jelentős része ugyanolyan standard szabványok alapján működik, mint a civil szférában hasonló feladatra tervezett eszköz. Ennek egyik oka a költséghatékonyság. A katonai alkalmazásra szánt infokommunikációs eszközöket általában olyan, megbízható referenciákkal rendelkező, meghatározott minőségbiztosítási követelményeket is teljesítő beszállítók, gyártók állítják elő és adják át használatra, amelyek polgári használatra is készítenek hasonló eszközöket. A katonai megrendelések önmagukban általában nem elegendőek egy minőségi eszközöket gyártó vállalat gazdaságos működtetéséhez.

Az informatikai és távközléstechnikai szabványoknak való megfelelés azért is fontos, mert még a standard, hagyományos híradó biztosítási tervekben is évtizedek óta szerepet kap a katonai célokra lebiztosított civil szolgáltatások igénybevétele. A polgári célú rendszer katonai alkalmazásra való hatékony igénybevétele pedig megköveteli az alkalmazott eszközök és eljárások kompatibilitását. Az infokommunikációs rendszerekben kezelt adatok védelmében, az adatok szenzitivitása és a jogszabályokban

[3] AM – ampitúdó moduláció, FM-frekvencia moduláció – analóg információtovábbítási technológiák rádióhullámok segítségével

foglalt követelmények alapján a civil és a katonai szféra is használ különböző eszközöket, részegységeket, algoritmusokat és eljárásrendeket.

A katonai szervezetek központilag meghatározott állománytáblával és felszerelési jegyzékekkel rendelkeznek a fegyvernem vagy szakcsapat alaprendeltetése szerint. Ezeknek a szervezeteknek az érvényben lévő hazai és NATO szabályzatok alapján előre elkészítik az infokommunikációs támogatási tervet is. Ezen tervek megvalósításával egy a miénkhez hasonló hadikultúrájú, hasonló harcmodorban küzdő ellenséggel szemben sikeres harctevékenységet folytathatunk.

A katonai műveletekre és azok infokommunikációs biztosítására azonban az eszközök fejlődése mellett nagy hatással van a hibrid vagy aszimmetrikus hadviselés megjelenése is.

A nemzetközi szakirodalomban nincs konszenzus arról, hogy mit is takar a hibrid hadviselés fogalma. A szakmai álláspontokat négy fő csoportba lehet sorolni. Az első csoportba tartoznak azok az értelmezések, amelyek szerint a hibrid hadviselés más, mint a korábbi háborúk, újfajta stratégiai szemléletet jelent, és a vele szemben történő fellépésnek is speciális és modern követelményei vannak. A második csoport szerint a hibrid hadviselés elemei már korábban is megjelentek a háborús konfliktusokban, de mai megjelenési formájában mégis alapvetően újszerű stratégiai kihívás. A harmadik csoport szerint a hibrid hadviselés fogalma nem nyújt semmilyen újdonságot, és nem segít megérteni a 21. század biztonsági környezetét. A negyedik csoportba a hadtudomány orosz művelőit sorolhatjuk, akik szerint a hibrid hadviselés a nyugati hatalmak Oroszország elleni stratégiája.(Somodi & Kiss, 2019)

A hibrid hadviselés álláspontom szerint a hagyományos és nem hagyományos hadviselés együttes alkalmazását jelenti. Aszimmetrikus hadviselés esetén a tradicionális hadikultúra képviselői ütköznek meg az irreguláris hadikultúra képviselőivel, az ebben részt vevő felek fegyveres harcának filozófiája jelentős mértékben különbözik A közelmúlt katonai konfliktusait és hadi eseményeit – a hadikultúrák szemszögéből vizsgálva – két kategóriára bonthatjuk. A szimmetrikus katonai összecsapások jellemzője, hogy alapvetően hasonló hadikultúrák vívnak harcot egymással, míg az aszimmetrikus konfliktusokban eltérnek az alkalmazott hadikultúrák.(Porkoláb, 2020)

Resperger István szerint a „hibrid hadviselés a hagyományos reguláris (lineáris, konvencionális) és az irreguláris (nem lineáris, nem konvencionális) hadviselés puha, közepes és kemény módszereinek, eljárásainak rugalmas alkalmazása abból a célból, hogy az ellenség államát, fegyveres erőit működésképtelenné, védtelenné tegyük és

akaratunkat rákényszeríthessük, legfőképpen azzal a stratégiai céllal, hogy az erőszak szintje a konfliktus folyamán ne haladja meg a háborús szintet”(Resperger, é. n.)

A hagyományos műveletekkel szemben a hibrid műveletek a különböző eszközeiket (diplomáciai, nemzetbiztonsági, katonai, gazdasági, kiber, információs, pszichológiai), a hagyományos és aszimmetrikus módszereket felváltva alkalmazzák az adott ellenség védtelenné tétele érdekében.(Resperger, é. n.)

A katonai műveletek infokommunikációs támogatásának igazodnia kell a harctevékenység jellegéhez. A Hasonló hadikultúrájú, reguláris csapatok konfliktusa esetén a tankönyvekből is tanult, a híradó és informatikai szabályzatokban leírt, kidolgozott eljárásrendek a Honvédségnél rendszeresített infokommunikációs eszközök szakszerű használatával alkalmazhatóak.

Az érvényben lévő stratégia szerint „Bár továbbra is kiemelt fontosságú eszköz a katonai erő alkalmazása, az államok törekednek a katonai konfrontáció időben és térben történő minimalizálására, és egyre inkább előtérbe kerülnek a fegyveres konfliktus szintjét el nem érő, nehezen nyomon követhető incidensek. Az ilyen, úgynevezett hibrid hadviselés során állami és nem állami szereplők katonai és nem katonai eszközöknek egy meghatározott stratégiai cél érdekében történő összehangolt felhasználásával törekednek érdekeiket a szemben álló fél kárára érvényesíteni”.(Magyarország Nemzeti Katonai Stratégiája, 2021)

A nem hagyományos, aszimmetrikus katonai műveletek esetén véleményem szerint nem mindig támaszkodhatunk kizárólagosan a katonai, technikailag és szolgáltatásnyújtás tekintetében is elkülönült infokommunikációs hálózatokra. A műveleteket esetenként civilek által lakott, polgári szolgáltatásokat igénybe vevő lakosság környezetében (városok, lakott települések) szükséges végrehajtani. Amennyiben a műveletek jellege nem totális háború jellegű, hanem a polgári létesítmények és javak megóvásával valósul meg, mint például a legtöbb béketeremtő misszióban, akkor a polgári infokommunikációs hálózatok működőképesek maradnak. Mobilkommunikációs hálózatok, internetkapcsolatok nélkül a modern kor társadalma a napi életét is sokkal nehezebben szervezi és éli meg. Ebben a speciális műveleti környezetben lehet meghatározó szinten létjogosultsága a polgári információs infrastruktúra és infokommunikációs eszközrendszerek akár ad hoc jellegű katonai alkalmazásának.

Geopolitikai elemzések alapján, a nemzeti katonai stratégia szerint: „Egy állami szereplő által hazánk ellen indított váratlan fegyveres támadás valószínűsége alacsony. A 21. században állandósulnak a nem állami szereplők jelentette kihívások, amelyek

kezeléséhez a Magyar Honvédség elsősorban azok keletkezési helyén, a válságkezelési műveletekben való szerepvállalása révén járulhat hozzá.” (Magyarország Nemzeti Katonai Stratégiája, 2021)

Ezért dolgozatomban nem törekszem a katonai műveletek teljes spektrumának infokommunikációs elemzésére. Kiemelten a nem háborús műveletekben a fegyveres békeműveletek, katonai segítségnyújtás és humanitárius segítségnyújtás infokommunikációs támogatásának biztonsági kihívásait vizsgálom. Mindezek mellett, a jelenlegi feszült nemzetközi helyzet, az orosz-ukrán konfliktus miatt a háborús kapcsolódásokat is kutatásom területeként azonosítom.

Katonai pályafutásom alatt volt lehetőségem nemzetközi környezetben részt venni kontingens híradó informatikai biztosítási terv elkészítésében, megvalósításában, üzemeltetésében. A feladatok végrehajtása során szerzett tapasztalataim ösztönöztek jelen disszertáció megírására. Biztos vagyok benne, hogy a hipotézisekben megfogalmazott gondolatok figyelembe vétele hozzájárulhat egy rugalmas és hatékony, anyagi erőforrásokkal jól gazdálkodó, az információbiztonság alapelveinek megfelelő infokommunikációs rendszer tervezéséhez, kivitelezéséhez, üzemeltetéséhez.

A tudományos probléma megfogalmazása:

A kétpólusú világrend megszűnésével megváltozott hadviselési elveket alkalmaznak valamennyi hadszíntéren, mely előre vetíti a fegyveres küzdelem megvívásának alapvető megváltozását a katonai műveletek minden kategóriájában. Megszűnt az egymásnak feszülő tömeghadseregek ideológiája. Ennek következtében átgondolásra, majd átszervezésre került a haderő felépítése, megváltozott az infokommunikációs támogatási igénye is. Az infokommunikációs eszközrendszerek forradalmi fejlődése a civil és a katonai szférában is új információtovábbítási technológiák, eljárásrendek kialakulásához vezettek. A kis költségvetési forrással rendelkező hadseregek infokommunikációs fejlettségét a nyereségorientált polgári szféra megelőzte. A profitorientált gazdasági társaságok természetesen átadják a technológiájukat, eszközrendszereiket, megfelelő díjazás fejében. Ehhez azonban a hadseregek erőforrásra van szüksége. Jelen pillanatban Magyarországon az eddigieknél sokkal nagyobb ütemben zajlik a haderő eszközrendszerének modernizációja. Kutatási eredményeim és szakmai tapasztalatom alapján a katonai döntéshozókat a korszerűsítés keretében meg kell győzni az infokommunikációs rendszerek fejlesztésének égető szükségességéről és a folyamatos fejlesztés fontosságáról. Amíg egy jól bevált, kinetikus energiájú fegyver kisebb átalakításokkal akár évtizedekig is elláthatja feladatát, az infokommunikációs

rendszerekben alkalmazott hardver-szoftver elemek csak folyamatos fejlesztéssel biztosíthatják a kor színvonalának megfelelő, biztonságos infokommunikációs támogatást. A beszerzési eljárások jogszabályok szerinti lebonyolítása esetenként évekbe telik. Ez napjainkban Hazánkban fokozottan érvényes, A digitális technológia fejlődési sebességét tekintve mire egy infokommunikációs eszközparkot rendszerbe állítanak, technológiailag vagy szoftveresen már szinte elavul.

A katonai műveletek során az infokommunikációs támogató rendszerekben feldolgozott nyílt, nem nyilvános adatok továbbítása a jelenlegi jogszabályoknak megfelelően rejtjelzetlen formában történik. A nem háborús műveletek végrehajtása során a napi élet zavartalan biztosítása érdekében keletkező (logisztikai, ellátási, szervezési) adatok döntő többsége nem minősített. Ezen adatok a továbbításuk során ki vannak téve érdekeinkkel szembenálló fél vagy felek információszerzésre irányuló tevékenysége veszélyének. Különösen nagy ez a veszély a katonai erő külföldi alkalmazása során. Ezért véleményem szerint a katonai műveletek külföldi végrehajtása esetén, amennyiben az infokommunikációs rendszer külföldi polgári információs infrastruktúra elemet is érint, rejtjelzéssel kell védenünk a nyílt, nem nyilvános adatainkat is.

A katonai műveletek infokommunikációs támogatásának a kezelt adatok mennyiségét tekintve kicsi, de annál fontosabb részterülete a minősített adatok – köznyelvben titkos adatok – kezelése. Ezen a részterületen az alkalmazható eljárásrend jogszabályok által szigorúan körülhatárolt. Az infokommunikációs rendszereknek a katonai műveletek sajátosságai szerinti rugalmas tervezhetőségéhez nem biztosítanak sok lehetőséget. Ez véleményem szerint a jelenlegi felgyorsult, katonai műveletek gyors és rugalmas áttervezhetőséget igénylő hadműveleti körülmények között a béke, béketámogató vagy harctevékenység sikeres megvívását is veszélyeztetheti.

Tudományos kutatómunkám alapvetően gyakorlati tapasztalatokra is támaszkodva a vonatkozó jogszabályokat a megvalósulás szempontjából vizsgáló kritikai elemző kutatás, melynek célja, hogy a vonatkozó doktrinális hátteret, a katonai, polgári eljárásrendeket, infokommunikációs szabványokat, szabályokat vizsgálva olyan nemzeti infokommunikációs támogatási modellt állítsak össze, amely eredményesebben támogatja a NATO és az EU által kiadott, a nemzeti és nemzetközi jogszabályokban és doktrínákban meghatározott védelmi célok elérésének infokommunikációs biztosítását hazánkban és a nemzetközi katonai alkalmazások folyamán egyaránt. Kutatómunkám végcélja olyan szakmai ajánlások megfogalmazása, amelyek nem teoretikusan, hanem a valós műveleti tervezésben és a feladatok végrehajtásában is segítik a katonai műveletek

infokommunikációs támogatásának biztonságos és hatékony eljárásrendjének kialakítását és üzemeltetését.

Hipotézisek:

1. *A Magyar Honvédség egységei katonai műveleteket támogató infokommunikációs rendszerének kialakításában költséghatékonynak, a súlypontjában megváltozott feladatrendszer támogatására képes rendszernek kell lennie. Ezen célok megvalósulását elősegíthetik a jelenlegi híradó és informatikai technikai eszközpark bázisán, egy nem homogén, a katonai művelet jellegétől függően egyedileg kialakított infokommunikációs támogató rendszerek, amelyek lehetőség szerint markánsan támaszkodnak a műveleti területen elérhető polgári információs infrastruktúra elemekre. A műveleti biztonság fenntartása érdekében az infokommunikációs támogató rendszer azon szakaszain, amelyet nem ellenőrizhetünk folyamatosan, a nyílt,* ***nem nyilvános adatainkat is rejtjelzéssel védve szükséges továbbítani****.*
2. *A Katonai egységeknél végrehajtói szinten kiemelkedő fontosságú, hogy a műveletek során az adattovábbítást, elsősorban a vezetéknélküli (rádió kommunikáció) esetén az infokommunikációs rendszert megfelelő védelmi intézkedések betartásával megvalósítható, hatékonyan működő rendszert alkotva tervezzék, szervezzék és alakítsák ki. A tervező és végrehajtó feladatok biztonságát megnövelheti, ha ennek érdekében a Magyar Honvédségen belül jogszabályi változtatásokat hajtanak végre.* ***Létrehozható a Honvédségen belül egy új biztonsági osztály[4]****, amelybe a nem minősített, de elektronikus úton történő továbbítás esetén fokozottan védendő adatokat sorolhatunk. Ezek az adatok a meglévő, minősített adatokat kezelő rendszerek rejtjelző eszközrendszerével védhetőek, de az adat, mivel nem minősített, adminisztratív szempontból a minősített adatok védelméről szóló törvényben[5] nem érintett, ezért nem terhelik a minősített adatok védelmére előírt, a katonai műveletek végrehajtása során esetenként igen nehezen betartható adminisztratív szabályok.*
3. *A katonai műveletek végrehajtása során a tervező, szervező és végrehajtó tevékenységek hatékonyságát szignifkánsan megnövelheti a* ***nemzeti adatok minősítési eljárásának újragondolása,*** *különös tekintettel az ideiglenesen*

[4] 94/2009 HM utasítás írja elő az adatok biztosági osztályokba történő besorolásának rendjét.
[5] 2009 évi CLV törvény a minősített adatok védelméről.

felállított, fegyveres műveletek végrehajtására kialakított alegységek tekintetében. A minősített adatok elektronikus kezelésére vonatkozó nemzeti és NATO szabályozás nem egységes. Kutatásaim és szakmai tapasztalatom alapján feltételezem, hogy a működőképesség fokozható, ha, műveleti körülmények között, különleges jogrendben a katonai vonatkozású nemzeti adatok minősítésére a NATO eljárásendjét alapul véve bővítjük a minősítésre jogosult személyek körét.

A kutatási téma körülhatárolása

Az egyre hatékonyabb informatikai eszközök és alkalmazások megjelenésével és elterjedésével a hadviselés szerkezete, kultúrája, valamint módja is átalakuláson megy keresztül. Ezeket a változásokat az informatikai technológiáknak aktívan kell támogatniuk, miután az információs fölény kialakítása meghatározóvá válik a hadviselés eredményességét illetően a hálózatközpontú katonai művelet lényege, hogy a politikai-katonai döntéshozatali rendszer, valamint a hadszíntéri végrehajtó rendszer teljes egésze egy közös, valós idejű információs rendszerbe van szervezve oly módon, hogy egy rendszert alkot a felderítés, a döntés és a fegyverzet a katonai műveletek végrehajtása teljes időtartamában(Szendy, 2017)

Az infokommunikációs rendszerekhez tartoznak:

- az informatikai rendszerek és hálózatok, ide értve az internet szolgáltatást is;
- a vezetékes, a mobil, a rádiós és műholdas távközlés;
- a vezetékes, a rádiófrekvenciás és műholdas műsorszórás;
- a rádiós vagy műholdas navigáció;
- az automatizálási, vezérlési és ellenőrzési rendszerek (SCADA, távmérő, távérzékelő és telemetriai rendszerek, stb.);
- a fentiek felderítéséhez, lehallgatásához vagy zavarásához használható rendszerek eszközei, eljárásai, valamint az üzemeltető és a felhasználó személyek is. (Muha, 2009)

Muha Lajos felsorolásából nem kívánom vizsgálni az automatizálási, vezérlési és ellenőrzési rendszereket és kommunikációs rendszerek felderítéséhez, lehallgatásához vagy zavarásához használható rendszerek eszközei, eljárásait.

A szakterület igen szerteágazó, feltérképezése messze meghaladja ennek a dolgozatnak a kereteit, ezért dolgozatomban a katonai műveletek infokommunikációs támogatása alatt

az alegységek, egységek híradását, kommunikációs célú informatikai biztosításának részleteit vizsgálom. A szakmai doktrina szerint:

„híradás: a katonai vezetés alapvető eszköze a szóbeli, képi és írásbeli információk, adatok továbbítására, amely tartalmazza a végrehajtás technikai, eljárásbeli és humán összetevőit.

híradó, informatikai rendszerek: a katonai vezetési-irányítási rendszer egyik alapvető eleme, amely az információk, adatok elektronikus gyűjtésére, továbbítására, feldolgozására, tárolására, kezelésére, megjelenítésére és védelmére szolgál. A híradó és informatikai rendszer a katonai vezetés alapvető vezetési eszköze. Biztosítja az alárendeltek feladatai meghatározásának, tevékenységük vezetésének és irányításának, a katonai tevékenységek tervezésben és végrehajtásában résztvevő szervezetek és személyek együttműködésének technikai feltételeit.

A csapatok tevékenységének támogatása fajtája szerint lehet harci támogatás és harci kiszolgáló támogatás. A híradó és informatikai támogatás a harci **támogatás** része. A katonai törzsek híradó és informatikai főnökségei, híradó és informatikai szervezeti elemei a feladatok sikeres végrehajtása érdekében a harci támogatás elemeként híradó és informatikai támogatási tervet készítenek.

informatikai támogatás: a katonai szervezetek feladatainak tervezéséhez és végrehajtásához szükséges információk feldolgozásához, tárolásához, kezeléséhez, és rendelkezésre bocsátásához szükséges informatikai szolgáltatások kialakítására, nyújtására és fenntartására irányuló szaktevékenységek és eljárások összessége.

híradó, informatikai rendszerek: a katonai vezetési-irányítási rendszeregyikalapvető eleme, amely az információk, adatok elektronikus gyűjtésére, továbbítására, feldolgozására, tárolására, kezelésére, megjelenítésére és védelmére szolgál.”

(Hír/4, 2013a)

Dolgozatomban nem választom élesen külön a szabályzat által megfogalmazott híradó és informatikai támogatás fogalomkörét.

Területi behatárolás:

Magyarország biztonságpolitikai koncepciója alapján határon belüli területvédelmi és nemzetközi szervezetekkel együttműködve kis alegységekkel végrehajtott nemzeti katonai műveletek infokommunikációs támogatását valamint szövetségi kötelezettségvállalás alapján a határainkon túli nem háborús műveletek infokommunikációs támogatását vizsgálom. A minősített adatok kezelésének szabályait a NATO valamint a nemzeti hatályos jogszabályok által teremtett keretek között kutatom.

Tapasztalatfeldolgozás céljából a jelenleg zajló Orosz Ukrán konfliktus infokommunikációs vetületét is elemzem, a számomra elérhető nyílt forrású információk alapján.

Kutatási célok

Kutatási hipotéziseim szakmailag kellően alátámasztott igazolását az alábbiakban részletezett célokon keresztül kívánom elérni:

1. **Értékelni** a rendelkezésre álló nyílt forrásokból kutatható NATO és hazai doktrínák infokommunikációs támogatással kapcsolatos szabályozási rendszerét, különös tekintettel az információbiztonsági követelményekre, ajánlásokra. **Megvizsgálni** a katonai szervezeteknél jelenleg alkalmazott stacioner és telepíthető infokommunikációs rendszerek felépítését, **megvizsgálni** a telepítésükkel és üzemeltetésükkel kapcsolatos információbiztonsági előírásokat, belső szabályozókat. **Értékelni** a jelenleg alkalmazott eljárásrendek szervezési és technológiai határait az alaprendeltetésből adódó feladat végrehajtási lehetőségei és az információbiztonsági szempontok alapján.
2. **Meghatározni** azon katonai műveletek spektrumát, amelyek végrehajtása kapcsán van létjogosultsága a műveletet támogató infokommunikációs rendszerek polgári információs infrastruktúrával való biztonságos és hatékony támogatásának. **Javaslatot tenni** a polgári információs infrastruktúra alkalmazási lehetőségeire az általam vizsgált katonai műveletek végrehajtásának infokommunikációs biztosítása érdekében.
3. **Megvizsgálni** és összehasonlítani a nemzeti és NATO minősített adatok kezelésére vonatkozó jogszabályokat. **Elemezni** a minősítői jogkör alacsonyabb szintre delegálásból fakadó előnyöket és hátrányokat.
4. A katonai műveletek adatkezelési eljárásainak szakmai elemzésével **kidolgozni** a katonai műveletek végrehajtása során keletkezett információk minősítési szintje meghatározásának ajánlását.

Kutatási módszerek

Kutatási módszerem alapvetően kevert típusú, amely esetén mind az általam létrehozott új adatokat, mind a forrásokban fellelhető, mások által gyűjtött vagy feldolgozott adatokat (primer/szekunder) felhasználom,

1. **Kvalitatív** módszerrel részletesen **megvizsgálom** és **összehasonlítom** a rendelkezésre álló nyílt forrásokból kutatható NATO és hazai doktrínák infokommunikációs támogatással kapcsolatos szabályozási rendszerét, különös

tekintettel az információbiztonsági követelményekre, ajánlásokra. **Deduktív** módszerrel tekintem át a katonai szervezeteknél jelenleg alkalmazott stacioner és telepíthető infokommunikációs rendszerek felépítését, és vizsgálom a telepítésükkel és üzemeltetésükkel kapcsolatos információbiztonsági előírásokat, belső szabályozókat. **Deduktív** eljárással határozom meg a jelenleg alkalmazott eljárásrendek szervezési és technológiai határait a feladatok végrehajtási lehetőségei alapján.

2. **Induktív** módszerrel határozom meg azon katonai műveletek spektrumát, amelyek végrehajtása kapcsán van létjogosultsága a műveletet támogató infokommunikációs rendszerek polgári információs infrastruktúrával való biztonságos és hatékony támogatásának, és javaslatot teszek a polgári információs infrastruktúra alkalmazási lehetőségeire katonai műveletek végrehajtásának infokommunikációs támogatása érdekében.
3. **Kvalitatív** módszerrel vizsgálom meg és hasonlítom össze a nemzeti és NATO minősített adatok kezelésére vonatkozó jogszabályokat. elemzem a minősítői jogkör alacsonyabb szintre delegálásból fakadó előnyöket és hátrányokat.
4. A katonai műveletek adatkezelési eljárásainak szakmai elemzésével **kvalitatív** módon dolgozom ki a katonai műveletek végrehajtása során keletkezett információk minősítési szintje meghatározásának ajánlását.

Az értekezés felépítése

A bevezetésben kitérek a téma időszerűségére, helyére és szerepére a katonai műszaki tudományok, védelmi elektronika, informatika és kommunikáció tudományterületén az ország geopolitikai helyzetének és nemzeti stratégiáinak tükrében. Bemutatom a felállított hipotéziseimet, melyeket a dolgozat érdemi részében kutatási eredményekkel és elemzésekkel igazolok. Röviden vázolom az értekezés, és a témafeldolgozás célkitűzéseit. Ismertetem a célok elérése érdekében alkalmazott kutatási módszereket, a kutatási témavizsgálati szempontjait, valamint a felhasznált forrásokat. Meghatározom a kutatási terület általam vizsgált részeinek határait, valamint az általam részletesen vizsgálandó, kiemelten kezelt elemeit. Áttekintem és elemzem a hazai katonai, a témához kapcsolódó NATO szakirodalmat és a polgári infokommunikáció szabályozási rendszerét. Ajánlásokat teszek a kutatásaim során részletesen vizsgált szabályozási elemek módosításának lehetőségeire, hipotéziseim elemzése, igazolása kapcsán feltárt problémák megoldására, dolgozatom igazolt eredményeinek gyakorlati hasznosítására.

Fogalmi és formai meghatározások:

Az értekezésben követem a jelenleg érvényben levő Ált/43 ÖHD 3, a HIR/4 - Magyar Honvédség Összhaderőnemi Híradó és Informatikai Doktrína kifejezéseit és a NATO infokommunikációval és annak biztonságával foglalkozó STANAG kiadványok gondolatmenetét. Az infokommunikáció fogalomkörébe tartozó kifejezéseket Kovács László és Haig Zsolt publikációi alapján értelmezem. A katonai információbiztonsággal kapcsolatos fogalmak és eljárásrendeket Kassai Károly és Muha Lajos munkáiban és a jogszabályokban leírtak szerint határozom meg. A hivatkozásokat, lábjegyzeteket illetően az MSZ51 ISO52 690 szabvány előírásait követem. Az értekezés felépítéséhez Gőcze István tudományelméleti és kutatásmódszertani tanulmánya nyújt alapot.

1.FOGALMAK ÉRTELMEZÉSE

Dolgozatomban, - már a címében is - több olyan fogalom megtalálható, amelyek szakterületenként eltérően értelmezhetők. Ezért az alábbiakban pontosítom, hogy jelen értekezésemben melyk fogalmi meghatározásokat tartom relevánsnak.

1.1 Katonai műveletek fogalmi meghatározása

A modern hadtudományi értelmezések szerint a jelen kor hadviselésének meghatározó jellemzői a hatásalapúság, illetve a hálózatos jelleg.

A hálózatközpontú katonai művelet lényege, hogy a politikai-katonai döntéshozatali rendszer,valamint a hadszíntéri végrehajtó rendszer teljes egésze egy közös, valós idejű információs rendszerbe van szervezve oly módon, hogy egy rendszert alkot a felderítés, a döntés és a fegyverzet a katonai műveletek végrehajtása teljes időtartamában. (Szendy, 2017)

Ezen elv alapján szervezett infokommunikációs alrendszereknek az információfeldolgozás szempontjából folyamatosan átjárhatónak, együttműködőnek kell lennie. Ez elsősorban a vezeték nélküli eszközök, rádiók esetében okoz gondot. Több forrásból származó, egymással csak részben kompatibilis eszközökkel csak átgondolt szervezési intézkedésekkel lehet működő infokommunikációs hálózatokat építeni.

A NATO Katonai Bizottsága 2006-ban kiadott MCM-0052-2006 dokumentumban, a hatásalapú katonai művelet fogalmát a következőképpen határozta meg: „...a szövetség tagállamai és a katonai műveletben érintett nem NATO-országok részére rendelkezésre álló különböző eszközök koherens és átfogó alkalmazása olyan hatások kiváltása érdekében, amelyek nélkülözhetetlenek a tervezett feladatok és legfőképpen a NATO végső céljának eléréséhez.”[6]

Bár a fogalmi meghatározás újkeletű, a hatásalapúságot a hadseregek más néven már ezt megelőzően is alkalmazták. Több ország nemzetközi szerződésen alapuló védelmi rendszerében már korábban is használták azt a szervezési elvet, hogy a tagországok fegyveres erői nem azonos képességeket fejlesztettek. Egymással egyeztetve, nemzeti sajátosságok alapján egyik a szárazföldi, másik a légi, harmadik tengeri/folyami stb. harceljárások alkalmazásához fejlesztette saját haderejét, a hadiipari fejlesztések több területe is ennek megfelelően került végrehajtásra.

[6] MC position on an effect based approach to operation (North Atlantic Military Committee - 6. June 2006. forrás: https://www.nato.int/docu/stratdoc/eng/a680116a.pdf

Az ilyen nemzetközi haderő infokommunikációs támogatása még nagyobb kihívás, mint a nemzeti haderő támogatása. A nemzetközi szerződések nem térnek ki az együttműködés részleteire. A NATO esetén az együttműködés egységesítése úgynevezett STANAG[7] szabályozók révén valósul meg. A szabályozók nem térnek ki konkrét infokommunikációs eszköz megnevezésekre, a működtetés során alkalmazandó, kötelező érvényű paramétereket, - mint például üzemmód, modulációs mód, frekvencia gazdálkodás - sem minden esetben határoznak meg, ami a megnehezíti a NATO erők infokommunikációs támogatásának tervezését, végrehajtását.

Mivel a Magyar Honvédség elsősorban a haza fegyveres védelmére elkötelezett, ezért, bár a hatásalapú hadviselés elmélete szerint szövetségi érdekből fejleszti a haderejét, a haza védelme érdekében kénytelen egy önmagában is hatásosan alkalmazható haderőt rendszerben tartani. Infokommunkáció szempontjából ez azt jelenti, hogy nem támaszkodhatunk minden esetben a NATO szövetségi infokommunikációs eszközrendszereire, nemzeti érdekből, saját erőből tervezni és üzemeltetni kell a Magyar Honvédség katonai műveleteinek támogatásához szükséges infokommunikációs rendszereket.

A NATO 2006-tól megkísérli összehangolni a tagállamok képességfejlesztéseit, azonban az egyes államok eltérő gazdasági teherbíró képessége, nemzeti ipari érdekei, továbbá a rendelkezésre álló erőforrások különböző nagysága, és nem utolsósorban a meglévő haderő szervezeti méretei, összetétele, az eltérő fegyverzete (katonai-technológiai fejlettsége) mind a mai napig nehezíti, és bonyolulttá teszi a hatásalapú műveletek végrehajtására irányuló hatékony képességek kialakítását. (Szendy, 2017)

A NATO létrehozott egy olyan szervezetet is, amely összefogja a katonai szövetség tagállamaiban kialakított innovációs ökoszisztémákat, és ezzel segít összhangba hozni és felpörgetni a különböző innovációs fejlesztéseket. Ez a DIANA[8] program. „A DIANA képességfejlesztő központjait (akcelerátor, azaz gyorsító program) és tesztközpont-hálózatát kifejezetten arra tervezték, hogy az egyetemeket, ipari és kormányzati szereplőket, start-upokat és más fejlesztőket összekösse a végfelhasználókkal, tudósokkal és rendszerintegrátorokkal annak érdekében, hogy előmozdítsák a kettős felhasználású mélytechnológiák fejlesztését, ezáltal megoldást kínálva a világ legsürgetőbb biztonsági és

[7] Standardization Agreement for procedures and systems and equipment components) Egységesítési egyezmény eljárásokra, rendszerekre és felszerelésekre)

[8] Defence Innovation Accelerator for the North Atlantic - Észak-Atlanti Védelmi Innovációs Akcelerátor

védelmi kihívásaira."[9]Jelenleg Magyarországon az elmúlt évtizedekhez képest minden eddiginél nagyobb arányú képességfejlesztési program indult.

Fentiekből következik, hogy a hatásalapúság biztosítása érdekében olyan infokommunikációs rendszereket célszerű alkalmaznunk, melyek nemzetközi szabványok szerint a működésük teljes spektrumában kompatibilisek egymással. A haderő nemzeti érdekből történő alkalmazása esetén az infokommunikációs rendszernek önállóan is alkalmasnak kell lennie az önálló katonaiműveletek támogatására. Ebben az esetben nem elvárás a NATO eszközökkel való kompatibilitás de a párhuzamosan működő rendszerek alkalmazásának elkerülésére, az emberi és anyagi erőforrások gazdaságos kihasználása érdekében célszerű hazai rendszerek kialakításánál is szem előtt tartani a NATO rendszerekhez való kapcsolódási képességeket.

1.2. Háborús műveletek

A **támadás** alapvető, fő vagy döntő harctevékenységi fajta, melyet a kezdeményezés megszerzése vagy megtartása, a koncentrált erőkifejtések sorozata jellemez a célkitűzések elérése érdekében. Sajátosságai a harci erő összpontosítása, a manőverek gyorsasága, a lendület fenntartása, az ellenségre való komplex ráhatás folyamatossága a teljes mélységben, az ellenség gyenge pontjainak gyors kihasználása és a főcsapás irányának ezzel összhangban történő áthelyezése.

„A **védelem** ideiglenes, kikényszerített vagy vállalt harctevékenységi fajta, és mindig a kezdeményezés megszerzéséért folyik. A védelmi harcot a csapatok a támadó ellenséggel szemben előre elkészített, vagy a harc folyamán elfoglalt területen folytatnak. Az alegységek többféle védelmi jellegű tevékenységet folytathatnak, mely szerint a védelem formája lehet: – a támadó ellenség elleni védelmi tevékenység, vagyis a védelmi harc; – a bekerítést végrehajtó és folytató ellenség elleni tevékenység, vagyis a bekerítésben vívott harc ". (MH Harcszabályzat, 2013)

Dolgozatomban, a feldolgozandó információk mennyisége és összetett struktúrája miatta továbbiakban a támadás és védelem végrehajtása módozatainak infokommunikációs támogatását külön nem vizsgálom.

[9] https://honvedelem.hu/hirek/a-nato-diana-programja-uj-lehetosegeket-kinal-magyarorszag-szamara-vedelmi-es-biztonsagi-kerdesekben.html Letöltés ideje: 2023.10.24

1.3. Nem háborús műveletek

„Nem háborús műveletek azok a tevékenységek, amelyeket békében, konfliktus (instabil) helyzetben vagy háborúban harcterületen kívüli tevékenységekre ideiglenesen létrehozott katonai erőket is magukba foglaló szervezetek folytatnak – hazai vagy nemzetközi mandátumban kijelölt területen – az alapvető emberi jogok biztosítása, a civil lakosság biztonságának megteremtése, javítása, a nemzeti vagy kijelölt terület vagyonának megóvása, a nemzeti vagy nemzetek közötti kapcsolatok normalizálása, a béke megteremtésének, megtartásának elősegítése, a gazdasági és politikai stabilizáció előmozdítása érdekében.” (MH Harcszabályzat, 2013)

A béketámogató műveletek mandátum alapján lehetnek:

- ENSZ által vezetett műveletek;
- NATO által vezetett műveletek (mandátum delegálásával);
- EU által vezetett műveletek (mandátum delegálásával);
- EBESZ által vezetett műveletek (mandátum delegálásával);
- Camp David-i egyezmény alapján – vezetett műveletek.

A béketámogató műveletek nemzetközi jogi alapja az ENSZ alapokmánya. Az alapokmány VI. fejezete tartalmazza azokat az intézkedéseket és tevékenységeket, amelyek a világban kialakult viszályok békés rendezésére vonatkoznak. A VII. fejezet az ENSZ-nek a fegyveres erők alkalmazását, a kényszerítő intézkedések megtételét engedélyezi, illetve szabályozza. Itt vannak lefektetve azok az intézkedések, eljárások, amelyeket a BT alkalmazhat a békét veszélyeztetőkkel, megszegőkkel és támadó tevékenységet folytatókkal szemben.

1.2.1.A nem háborús katonai műveletek felosztása:

A nem háborús katonai műveletek fajtái:

Békeidőszaki műveletek:

– Nem harci kiürítés.

– Hazai polgári hatóságok támogatása.

– Humanitárius segítségnyújtás és katasztrófaelhárítás.

– Kutatás-mentés.

– Légtér-ellenőrzés.

Válságkezelő műveletek:

– Béketeremtés,

– Békefenntartás,

– Békekikényszerítés,
– Békemegerősítés,
– Humanitárius segítségnyújtás,
– Migráció kezelése,
– Katasztrófaelhárítás katonai feladatai,
– Belső rend helyreállítása,
– Felkelés elleni műveletek,
– Mentor és kiképző műveletek,
– Terrorizmus elleni küzdelem, (MH Harcszabályzat, 2013)

A fegyveres konfliktusok háborús, illetve nem háborús (válságreagáló) katonai műveletként is értelmezhetőek. A fegyveres konfliktusok általában szomszédos államok (államcsoportok) között, elsősorban a határkörzetekben, tengeri (óceáni) partmellékeken, szigeteken, valamint az államok belső határain, autonóm és nemzetiségi területeken, illetve geopolitikai, geostratégiai ütközőterületen, gazdaságilag illetve katonailag fontos körzetekben keletkeznek és folynak le. Fegyveres konfliktusként foghatók fel a szándékos, fegyveres légtérszuverenitást-sértő behatolások, illetve azok fegyveres elhárítása, valamint a különleges (speciális) erőkkel történő mélységi, mögöttes területi behatolás és feladatvégrehajtás is, illetve annak fegyveres felszámolása.

A terror elleni küzdelem, illetve a szabadság kiterjesztését támogató katonai műveletek alatt értjük: a politikai akarat támogatásának különböző formáit, így a katonai erővel való emonstrálást; a megelőző katonai fellépést, kiemelten annak leghatározottabb formáját – a megelőző csapást; az általános katonai fellépést, vagyis a katonai erő bevetését; a stabilizálás, illetve demokratizálás katonai erővel történő támogatását.(Deák, 2005)

A Magyar jogrend legfőbb szabályrendje, az Alaptörvény 45. cikk kimondja, hogy 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.

A Magyar Honvédség irányítására – ha nemzetközi szerződés másként nem rendelkezik – az Alaptörvényben és sarkalatos törvényben meghatározott keretek között az Országgyűlés, a köztársasági elnök, a Honvédelmi Tanács, a Kormány, valamint a feladat- és hatáskörrel rendelkező miniszter jogosult. A Magyar Honvédség működését a Kormány irányítja. (Alaptörvény, 2011)

(1) A Kormány engedélyezi a Magyar Honvédség, illetve külföldi fegyveres erők j) pontja szerinti,

a) az Észak-atlanti Tanács döntésén alapuló alkalmazását, illetőleg

b) az Észak-atlanti Szerződés Szervezete döntésén alapuló más csapatmozgásait.

(2) A Kormány az (1) bekezdés alapján hozott döntéséről haladéktalanul beszámol az Országgyűlésnek a köztársasági elnök egyidejű tájékoztatása mellett. (Isaszegi, 2005)

Tehát békeidőszakban a Magyar Honvédség a Kormány közvetlen irányítása alatt működik, nemzetközi kötelezettségvállalás esetén a feladat ellátásához parlamenti felhatalmazás is szükséges.

A fenti részletes jogi és katonai szabályrendszerek idézése alapján könnyen belátható, hogy a nem háborús műveletek infokommunikációs támogatása összetett feladatrendszer. A különböző feladatok más – más támogatási részfeladatot vonnak maguk után. Egy jól megtervezett infokommunikációs támogató rendszernek véleményem szerint biztosítania kell valamennyi részfeladat elengedhetetlenül szükséges infokommunikációs támogatását. Megfelelő végponti eszközök, perifériák biztosításával pedig a speciális igények is kielégíthetők kell, hogy legyenek.

Nemzeti válságkezelő műveletek esetén határainkon belül a Honvédségnek a társszervekkel (Katasztrófavédelem, Terrorelhárítási Központ, Rendőrség, stb.) közös infokommunikációs hálózatot is kell szervezni, üzemeltetni. Jelen geopolitikai helyzetben a nem háborús műveletek békeidőszakban, hazánkban eddig már végrehajtott feladatai voltak és jelenleg is zajló műveletei:

- migráció kezelés;
- katasztrófa elhárítás;
- humanitárius segítségnyújtás.

Az évek óta tartó és szűnni nem akaró menekült áradat kezelésére a kezdetektől fogva alkalmazták a Magyar Honvédség kijelölt erőit. A jelenleg a szomszéd országban zajló háború elől menekülők fogadására, humanitárius segítségnyújtásra szintén bevonták a Honvédséget.

A nemzetközi műveletek megtervezésekor figyelembe kell venni a feladatok infokommunikációs támogatási igényét is. A nemzetközi feladat végrehajtása érdekében létesítendő infokommunikációs rendszerek megtervezése, eszközeinek beszerzése, beüzemelése, a rendszer jogszabályi előírások szerinti működéséhez szükséges engedélyek beszerzése annak a szervezetnek a feladata, amely nemzetközi felhatalmazás alapján felelős a feladat végrehajtásáért. Ha a feladatot a NATO kapja, akkor a teljes

tervező, szervező, végrehajtó tevékenység a NATO feladata és felelőssége. A feladat során támaszkodnak a nemzetközi feladatba bevont nemzetek eszközeire, de igénybe vesznek kifejezetten NATO közös infokommunikációs rendszereket és NATO beszerzésű eszközöket is.

Személyes tapasztalatom szerint a Magyar Honvédség nemzetközi feladatokba bevont erőinek a nemzetközi kötelezettségvállalásból adódó feladatok érdekében telepítendő infokommunikációs rendszerek beszerzésével, üzemeltetésével kevés nehézsége volt eddig, mert ezeket a rendszereket nem hazai költségvetési forrásból kellett beszerezni hanem a Szövetség javítási és karbantartási lehetőséggel együtt biztosította azokat.

Nagyobb nehézséget a Nemzeti felelősségű rendszerek tervezése és üzemeltetése jelenti. Ez áll egyrészt a műveleti területen létesített táborok belső infokommunikációs rendszeréből, másrészt a külföldi állomáshely és a magyarországi elöljáró vezetési pont közötti infokommunikációs rendszer tervezéséből, telepítéséből és üzemeltetéséből áll.

A külföldi telepítésű infokommunikációs rendszerek üzemeltetése esetén külön kihívás a rendszer működését biztosító eszközök javításának, karbantartásának biztosítása. Nagy előrelátást és szervezőkészséget igényel a szükség esetén alkalmazott rejtjelző eszközök folyamatos rejtjelkulccsal való ellátása is.

Az MH Harcszabályzat a nem háborús műveletek végrehajtása esetén véleményem szerint helyesen kiemelt jelentőséget tulajdonít a terrorizmus elleni küzdelemnek, amely a Harcszabályzat szerint:

„A terrortámadásokkal szembeni sebezhetőség minimumra csökkentése elsődleges (passzív) védekezés során, ami a katonai információvédelmet, a katonai kommunikációs rendszer védelmét, a személyi és objektumvédelmi rendszabályok foganatosítását jelenti. A terrorizmus elleni aktív küzdelem (megelőzés, elrettentés, válaszadás) végigvonul a katonai műveletek minden területén. A művelet során aktív – katonai kötelékkel végrehajtott – tevékenység vállalása nem történik, ellenben azokhoz valamilyen támogatást (tervező, felkészítő munka végzése, technikai eszközök biztosítása, illetve átadása) nyújtanak.” (MH Harcszabályzat, 2013)

A szabályzat megfogalmazásából is kitűnik, hogy a nem háborús műveletek esetén, amelyek nem csak hadműveleti területen, harcmezőn zajlanak, hanem civil – polgári környezetben is, a műveletet végrehajtó állomány jobban ki van téve a nem katonai, terrorista, gerilla harcmodort alkalmazó, esetenként nem azonosítható erők támadásának. Ez az állítás az infokommunikációs rendszerek támadhatóságára fokozottan igaz lehet. Az infokommunikációs rendszerek folyamatos rendelkezésre állása nagyban függ a

kritikus információs infrastruktúra elemek védelmének szükség szerinti, Európai Unió államaiban jogszabályban meghatározott biztosításától.

1.3. Az Infokommunikáció fogalomrendszere:

A digitális technológia elterjedésével megkezdődött a számítógép, a vezetékes és vezeték nélküli távközlési eszközök, továbbá az elektronikus média műszaki közeledése, technikai konvergenciája, majd közös termékben való összeolvadása. A műszaki fejlesztések lehetővé tették az áttérést a multimédiás jeltovábbításra a kommunikációs csatornán. Ezáltal megvalósul a beszédhang, zene, szöveg, rajz, álló– és mozgókép egy csatornán történő továbbítása. Lehetővé vált korábban elkülönült információ kezelésmódok összekapcsolása és kombinálása, infokommunikációs alkalmazások és ezekre épülő vállalkozások létrejötte.(Haig & Kovács, 2012)

Az **infokommunikációs rendszerek** magukba foglalják az adatok gyűjtésére, felvételére, tárolására, feldolgozására (megváltoztatására, átalakítására, összegzésére, elemzésére, stb.), továbbítására, törlésére, hasznosítására (ideértve például a nyilvánosságra hozatalt is), és felhasználásuk megakadályozására használt elektronikus eszközöket, eljárásokat, valamint az üzemeltető és a felhasználó személyeket is.(Muha, 2009)

A digitális technológia fejlődésével a korábban híradó és informatikai szakterületek a Honvédség vezetési szintjein infokommunikációs szakterületté forrtak össze. A Magyar Honvédség Összhaderőnemi Híradó és Informatikai Doktrina (Hír/4, 2013b) bevezetésében és fogalommagyarázatában még híradó és informatikai támogatási területeket határoz meg. A Hálózatalapú Műveleti Képesség vizsgálatában már megjelenik az infokommunikáció szókapcsolat, de a szabályzat nem értelmezi az infokommunikáció fogalmát. Az Európai Unió állásfoglalása a fogalomról a Hírközlési és Informatikai Tudományos Egyesület[10] szerint: Az infokommunikáció az Európai Unió hivatalos szóhasználatában az információtechnológia (Information Technology) és a távközlés (Telecommunications) konvergenciáját, szakterületeinek integrálódását fejezi ki. Gyakran használt rokon fogalom az ICT (Information and Communication Technology)

[10] https://www.fogalomtar.hte.hu/wiki/-/wiki/HTE+Infokommunikacios+Fogalomtar/Infokommunik%C3%A1ci%C3%B3

A fogalmi meghatározást tovább szűkítve infokommunikáció szóhasználatkor a szakterület katonai felosztása szerinti híradó, informatikai és információvédelmi részterületeket vizsgálom.

A civil társadalom információs infrastrukúrája fogalmi meghatározása szükséges ahhoz, hogy szakmai összehasonlítást a katonai – polgári infokommunikációs hálózatok között. Egy szakszerű megfogalmazás szerint az információs társadalom működéséhez szükséges információk előállítására, szállítására és felhasználására különböző rendeltetésű, funkciójú és típusú infrastruktúrarendszerek, hálózatok állnak rendelkezésre. Ezek összessége képezi az információs társadalom komplex információs infrastruktúráját. (Thomas, 2006)

Muha Lajos megfogalmazása szerint **kritikus infrastruktúraként** kell kezelnünk azon létesítményeket, eszközöket vagy szolgáltatásokat, amelyek működésképtelenné válása, vagy megsemmisülése a nemzet biztonságát, a nemzetgazdaságot, a közbiztonságot, a közegészségügyet vagy a kormány hatékony működését gyengítené, továbbá azon létesítményeket, eszközöket és szolgáltatásokat, amelyek megsemmisülése a nemzeti morált vagy a nemzet biztonságába, a nemzetgazdaságba, vagy a közbiztonságba vetett bizalmat jelentősen csökkentené. **Kritikus információs infrastruktúrák** azon az infokommunikációs létesítmények, eszközök vagy szolgáltatások, amelyek önmagukban is kritikus infrastruktúra elemek, továbbá a kritikus infrastruktúra elemeinek azon infokommunikációs létesítményei, eszközei vagy szolgáltatásai, amelyek működésképtelenné válása, vagy megsemmisülése a kritikus infrastruktúrák működésképességét jelentősen csökkentené.(Muha, 2009)

Konkrétabb értelmezés szerint: „Egy ország információtechnológiára alapozott infrastruktúrája joggal nevezhető a társadalom idegrendszerének, és ennek következtében az információs infrastruktúrák, illetve azok részei is a kritikus infrastruktúrák közé sorolandók. E megállapítás szerint, pl. egy ország nyilvános mobil távközlő hálózatai, mint önmagukban is kritikus infrastruktúrák, egyben kritikus információs infrastruktúráknak is minősülnek, illetve pl. az energiaellátó rendszert irányító, vezérlő számítógép-hálózat is ez utóbbiak közé sorolandó”(Haig & Kovács, 2012)

A Magyar jogszabályokban a kritikus infrastruktúra fogalom helyett a létfontosságú rendszerelem fogalomkör jelenik meg. Jelen kutatásnak nem tárgya a két megfogalmazás közötti azonosságok és különbözőségek elemzése. Mivel az ország területén végrehajtott katonai műveletek során használatba kerülhetnek a nemzeti létfontosságú rendszerelemek

szolgáltatásai, mindenképpen vizsgálnom kell a különböző létfontosságú rendszerelemek védelmének jogi szabályozását.

Törvényi megfogalmazás szerint: „**létfontosságú rendszerelem**: az 1. mellékletben meghatározott ágazatok valamelyikébe tartozó szolgáltatás, eszköz, létesítmény vagy rendszer olyan rendszereleme, továbbá azok által nyújtott szolgáltatások, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához, az ország honvédelméhez, – és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna."

nemzeti létfontosságú rendszerelem: e törvény alapján kijelölt létfontosságú rendszerelem, amelynek kiesése a létfontosságú társadalmi feladatok folyamatos ellátásának hiánya miatt elsősorban Magyarországon lenne jelentős hatással.(2012. évi CLXVI. törvény, é. n.)

Az 1. mellékletben felsoroltak közül dolgozatomban releváns az Infokommunikációs technológiák ágazat, internet-hozzáférési szolgáltatás és internet-infrastruktúra, elektronikushírközlési szolgáltatások, elektronikus hírközlő hálózatok, postai szolgáltatások alágazat valamint a Honvédelem ágazat honvédelmi rendszerek és létesítmények alágazata.

A létfontosságú rendszerelemmé nyilvánítás eljárásrendjét és a létfontosságú rendszerelemnek nyilvánított elem működtetésével kapcsolatos részletes szabályozást a fenti törvény valamint a végrehajtására kiadott Kormányrendelet határozza meg. (65/2013. (III. 8.) Korm. rendelet, é. n.) Az ágazati hatóságok a jogszabályokban rögzített kritériumok alapján nyilváníthatnak valamely rendszerelemet létfontosságúnak. Az eljárásrend honvédelmi szempontból kiemelt eleme, hogy a honvédelmi rendszerek és létesítmények ágazati kijelölő hatósága (A Honvédelmi Minisztérium Hatósági Főosztálya) az 1. mellékletben meghatározott, nem honvédelmi ágazatba tartozó rendszerelemet honvédelmi érdekből, kormányrendeletben meghatározott honvédelmi kritériumok alapján, az alábbiakban részletezett horizontális kritériumok vizsgálata nélkül nemzeti létfontosságú rendszerelemmé (a továbbiakban: ágazaton kívüli honvédelmi rendszerelem) kijelölheti.

Horizontális kritérium: azok a szempontok, az azokhoz tartozó küszöbértékek, műszaki vagy funkcionális tulajdonságok, amelyek egy eszköz, létesítmény rendszerelemének kiesése által kiváltott hatásra vonatkoznak, és amelyek teljesülése esetén – figyelemmel a bekövetkező emberiélet-veszteségekre, az egészségre gyakorolt hatásra, a gazdasági és

társadalmi hatásokra, a természetre és az épített környezetre gyakorolt hatásra – az eszköz, létesítmény, rendszer vagy azok része létfontosságú rendszerelemmé jelölhető ki attól függetlenül, hogy mely ágazatba tartozik.

Tehát a HM Hatósági Főosztálya honvédelmi érdekből létfontosságú rendszerelemmé jelölhet ki nem honvédelem ágazatba tartozó, polgári szervezetek által működtetett civil rendszereket is. Előírhat olyan szakmai, biztonsági követelményeket, amelyek betartását egy profitorientált polgári cég, szervezet nem tartaná szükségesnek, de létfontosságú rendszerelemként az ország honvédelmi képességének fenntartása érdekében jogszabályban foglalt kötelezettsége okán kénytelen megtenni. Fentieket jól példázza az alábbi eset: A COVID 19 járvány terjedésének lokalizálása és a polgárok által igénybevett, a társadalom működésének a különleges helyzetben is zavartalan szolgáltatások biztosítása érdekében a Magyar Kormány számos intézkedést tett, melynek keretében a HM Hatósági Főosztálya több, nem a Honvédelmi ágazatba tartozó kereskedelmi, energetikai és pénzpiaci vállalkozás egyes működési elemeit nemzeti létfontosságú rendszerelemmé nyilvánította.[11]

A fentieken túlmenően a honvédelem ágazatba tartozó, honvédelmi létfontosságú rendszerelemek azonosítására kijelölésére, kijelölésének visszavonására és védelmére külön jogszabályt alkottak, melynek megfogalmazásában honvédelmi létfontosságú rendszerelem: a honvédelemről és a Magyar Honvédségről szóló 2021. évi CXL. törvény 3. § 14. pontja szerinti honvédelmi szervezet, valamint a honvédelemért felelős miniszter tulajdonosi joggyakorlása alatt álló gazdasági társaságok által működtetett vagy használt rendszerelem és létesítmény (359/2015. (XII. 2.) Korm. rendelet, é. n.)

A jogszabály tehát elsősorban a katonai szervezetek tulajdonában álló rendszerekre vonatkozik. Érdemes megemlíteni, hogy jelenleg a honvédelmi informatikai támogató rendszer hálózatában üzemelő számítógépek jelentős része nem a Magyar Honvédség tulajdona, az eszközöket civil gazdasági társaságtól bérelve kölcsönszerződés alapján használjuk.

A jogszabály a honvédelmi létfontosságú rendszerelem azonosításával, kijelölésével, ellenőrzésével kapcsolatosan részletes szabályozást nem tartalmaz, ezért ezeket a korábban kiadott, a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvényben(2012. évi CLXVI. törvény, é. n.) valamint a végrehajtására kiadott 65/2013. (III. 8.) Korm. rendeletben

[11] Személyes tapasztalat a Honvédelmi Irányító Törzs tagjaként az Operatív Törzs és a Magyar Villamos Művek Zrt közötti kapcsolattartói feladatok ellátása során.

(65/2013. (III. 8.) Korm. rendelet, é. n.)foglaltak szerint kell értelmezni. Egyik legfontosabb kézzelfogható védelmi intézkedés, hogy a kijelölt rendszerelem üzemeltetőjének üzemeltetői biztonsági tervet kell készítenie, majd az üzemeltetői biztonsági tervet szükség esetén soron kívül módosítja, és a módosítással érintett részt megküldi a kijelölő hatóság részére.

359/2015. (XII. 2.) Korm. rendelet a korábbi törvényi szabályozást kiegészítve véleményem szerint két fontos fogalomkört is definiál.

A jogszabály meghatározza. mit minősítünk **rendkívüli eseménynek**: „olyan esemény, amely során a rendszerelem rendeltetésszerű működésének, üzemfolytonosságának veszélyeztetése, akadályozása olyan mértékű, hogy a rendszerelem részben, vagy egészben elveszíti azt a képességét, amelyet a honvédelmi ágazat kijelölő hatósága a kijelölő határozatában honvédelmi érdekből létfontosságúnak minősített, és mindez a honvédelmi feladatok ellátását lehetetlenné teszi, vagy azok ellátásában súlyos zavart okoz.”

A másik fontos meghatározás a honvédelmi létfontosságú **elektronikus információs rendszerelem**: az Lrtv. alapján „európai vagy nemzeti létfontosságú rendszerelemmé kijelölt létfontosságú elektronikus információs rendszer vagy kizárólag elektronikus információs rendszer működésétől függő kijelölt képesség, amelyek működésképtelenné válása vagy megsemmisülése a honvédelmi ágazat működésképtelenségét vagy súlyos zavarát okozza, és nem vagy csak a honvédelmi érdek aránytalanul nagy sérülésével helyettesíthető.”

Az elektronikus információs rendszerelem fogalma a fenti jogszabályon túl más katonai szabályozóban, dokumentumban nem jelent meg, a fogalom további elemzésére jelen dolgozatom terjedelmének határai miatt nem térek ki.

1.3.1 Kiberműveletek

A „kiberműveletek” egy folyamatosan növekedő, átalakuló, az infokommunkációs rendszerekhez szorosan kapcsolható terület.

A NATO 2016 évi csúcsértekezletének hivatalos zárónyilatkozatában műveleti területnek ismerte el a kiberteret.(*Warsaw Summit Key Decisions*, é. n.)

A Nemzeti Kiberbiztonsági Stratégiában használt megfogalmazás szerint „a kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában

megjelenő társadalmi és gazdasági folyamatok együttesét jelenti.”(Magyarország Nemzeti Kiberbiztonsági Stratégiája, 2013)

Kovács megfogalmazása szerint:” Kibertér: felhasználók, eszközök, szoftverek, folyamatok, tárolt vagy átvitel alatt lévő információk, szolgáltatások és rendszerek gyűjtőfogalma, amelyek közvetlenül vagy közvetett módon számítógép-hálózathoz vannak kapcsolva”.Mindez hétköznapi nyelvre fordítva: „kibertér a hálózatok és benne az internet, valamint a hálózathoz vezetéken vagy vezeték nélkül csatlakozó eszközök működési tartománya”(László Kovács, 2018)

Haig értelmezése szerint a kibertér fogalomkörébe tartozó, „A hálózatos infokommunikációs technológia igen jó lehetőségeket teremt a kognitív hatásokat előidéző különféle eszközök és módszerek alkalmazására. Az internet és benne a közösségi média pedig jelentősen kiszélesítik a kognitív befolyásolás és manipuláció lehetőségeit.” (Haig Zsolt, 2022)

A fenti idézetekből látható, hogy a kibertér fogalomkörébe tartozó részterületek elemzése szerteágazó és dolgozatom szempontjából távoli tudományterületekre vezethet.

A megfogalmazások alapján az általam vizsgált rendszerek is a kiberbiztonság fogalomkörébe tartoznak. Vizsgálataimat, elemzéseimet a Magyar Honvédségnél jelenleg hatályos szervezeti felépítése és működési rendje alapján tervezem kidolgozni. Jelenleg a Magyar Honvédség infokommunikációs és információvédelmi tevékenysége önálló szakterület, nem része a Kiberműveleti Parancsnokság jelenlegi feladatrendszerének. A kiberműveleti erők feladataikat a 2021. évi CXL törvényben, a katonai kibertér műveletekre vonatkozó különös szabályokban meghatározott jogosultságaik alapján látják el. Feladatrendszerük természetesen kapcsolódik a saját csapataink információinak megóvásához, ellenséges passzív vagy aktív információszerző, megsemmisítő tevékenységek elhárítására, megakadályozására. Mindezek ellenére, a vizsgált területet behatárolva, jelen dolgozatban a kiberműveletek fogalomkörét nem vizsgálom önállóan, csak amennyiben az általam vizsgált területekhez szorosan és el nem választhatóan kapcsolódnak.

1.4. Információvédelem fogalomrendszere

Ezen a területen a fogalmak értelmezése szakterülettől függően különböző. Dolgozatomat a továbbiakban az alábbi értelemzések alapján készítettem el:

Az **információvédelem** az általános védelmi rendszabályok és eljárások alkalmazása az információ megsemmisülésének vagy kompromittálódásának megelőzése, felfedése ellen és helyreállítása céljából.(Muha, 2009)

1.4.1. Információbiztonság

Az **információbiztonság** a szóban, rajzban, írásban, a kommunikációs, informatikai és más elektronikus rendszerekben, vagy bármilyen más módon kezelt információk védelmére vonatkozik.(Muha & Krasznay, 2018)

Az információvédelem részterületet katonai vonatkozásban az alábbiak szerint csoportosítom:

- Személyi biztonság,
- Fizikai biztonság,
- Adminisztratív biztonság,
- Elektronikus információbiztonság.

Az elektronikus információbiztonság az alábbi részterületeket foglalja magában:

- számítógép biztonság
- hálózati biztonság
- átviteli biztonság
- kisugárzás elleni védelem
- rejtjelzés

Katonai vonatkozásban fontos az adatok osztályba sorolása is, mert ennek alapján kell az adatok védelmével kapcsolatos, jogszabályban foglalt intézkedéseket megfogalmazni, alkalmazni.

Alapfogalmak:

Nyílt adatok védelmével kapcsolatos fogalmak tisztázása:

Értelmezésem szerint a biztonsági osztály kategóriák szabályrendszere a **nyílt adatok** kezelésével kapcsolatban határoz meg szabályokat. Tapasztalatom alapján az adatkezelések több mint 99% nyílt adatok felhasználásával történik, ezért ez a terület kiemelkedő fontosságú a honvédelmi célú infokommunikációs rendszerek biztonságos üzemeltetésének vizsgálatakor.

- **Biztonsági osztály**: az elektronikus információs rendszer védelmének elvárt erőssége;
- **Biztonsági osztályba sorolás**: a kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása;

Az információs rendszer védelmére fordított kiadások a kockázatarányosságra épülnek, azaz csak a lehetségesen bekövetkező veszteségek és károk nagyságrendjével arányosan indokolt az anyagi ráfordítás. Azt, hogy milyen mértékben kell az információs rendszer védelmére költeni a kezelt adatok a bizalmasságának, a sértetlenségének vagy a rendelkezésre állásának, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása elvesztésével okozott károk nagyságrendjével lehet megállapítani.

A hatályos jogi szabályozás a nemzeti adatvagyont kezelő rendszerek esetében a sértetlenség, a létfontosságú információs rendszerelemek esetében a rendelkezésre állás követelményét emeli ki, a különleges személyes adatokkal kapcsolatban pedig alapvető igényként fogalmazza meg a bizalmasság fenntartását.

- **biztonsági szint**: a szervezet felkészültsége az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;
- **biztonsági szintbe sorolás**: a szervezet felkészültségének meghatározása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;

A biztonsági osztályba sorolás alkalmával – az érintett elektronikus információs rendszer vagy az általa kezelt adat bizalmasságának, sértetlenségének vagy rendelkezésre állásának kockázata alapján – 1-től 5-ig számozott fokozatot kell alkalmazni, a számozás emelkedésével párhuzamosan szigorodó védelmi előírásokkal együtt.(2013 évi L törvény, 2023)

A 41/2015. BM rendelet az „információs rendszer” fogalmat használja ott, ahol én dolgozatom egyéb részeiben infokommunikációs rendszert értek. Ezért a szöveghűség és az egységes értelmezés érdekében az adatok biztonsági osztályba sorolásának jogmagyarázata kapcsán a jogszabályban megjelenő „információs rendszer” fogalmat fogom használni.

A Magyar Honvédség adatkezelő rendszereit a jogszabályban foglaltak szerint minimum a 4., maximum az 5. biztonsági osztályba kell sorolni azért is, mert a Magyar Honvédség zárt célú elektronikus információs rendszert üzemeltet (2013 évi L törvény **9. §** (2)), az adatkezelő rendszereknek ezek alapján meg kell feleljenek a 41/2015BM rendeletben meghatározott biztonsági követelményeknek. A 41/2015 BM rendelet a biztonsági osztályokat a következők szerint definiálta:

A 4. biztonsági osztály esetében:

- nagy káresemény következhet be, mivel különleges személyes adat nagy mennyiségben sérülhet;
- személyi sérülések esélye megnőhet (ideértve például a káresemény miatti ellátás elmaradását, a rendszer irányítatlansága miatti veszélyeket);
- az érintett szervezet üzlet-, vagy ügymenete szempontjából nagy értékű, üzleti titkot, vagy különösen érzékeny folyamatokat kezelő elektronikus információs rendszer, vagy információt képező adat tömegesen, vagy jelentősen sérülhet;
- a káresemény lehetséges társadalmi-politikai hatásaként a jogszabályok betartása, vagy végrehajtása elmaradhat, bekövetkezhet a bizalomvesztés a szervezeten belül, az érintett szervezet felső vezetésében, vagy vezetésében személyifelelősségre vonást kell alkalmazni;
- a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 10%-át.

Az 5. biztonsági osztály esetében:

- kiemelkedően nagy káresemény következhet be, mivel különleges személyes adat kiemelten nagy mennyiségben sérülhet;
- emberi életek kerülnek közvetlen veszélybe, személyi sérülés nagy számban következhet be;
- a nemzeti adatvagyon helyreállíthatatlanul megsérülhet;
- az ország, a társadalom működőképességének fenntartását biztosító létfontosságú információs rendszer rendelkezésre állása nem biztosított;
- a lehetséges társadalmi-politikai hatás: súlyos bizalomvesztés az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek;
- az érintett szervezet üzlet- vagy ügymenete szempontjából nagy értékű üzleti titkot, vagy kiemelten érzékeny folyamatokat kezelő elektronikus információs rendszer, vagy információt képező adat tömegesen vagy jelentősen sérülhet;
- a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 15%-át.

A 4.-5. biztonsági szervezeti szint azonosításához szükséges követelményeit a 41/2015. (VII. 15.) BM rendelet 2. számú melléklete részletesen tartalmazza.

A biztonsági osztályba sorolást a szervezet vezetője hagyja jóvá, és felelős annak a jogszabályoknak és kockázatoknak való megfelelőségéért, a felhasznált adatok teljességéért és időszerűségéért. A biztonsági osztályba sorolást a szervezet informatikai biztonsági szabályzatában (EIBSZ)[12] rögzíteni kell. Mivel a kockázatok folyamatosan változnak, az elektronikus információs rendszerek osztályba sorolását biztonsági osztályba sorolást legalább háromévenként vagy szükség esetén soron kívül, dokumentált módon felül kell vizsgálni.

A felülvizsgálatot az osztályba sorolásért felelős szakállomány hajtja végre és azért, hogy a szabályok betartása mindenki számára kötelező legyen, minden esetben a szervezet vezetője hagyja jóvá.

Véleményem szerint a felülvizsgálati kötelezettség szükséges, nemzetközi ajánlásokban is megjelenő előírás, de az információs rendszerek biztonságáért felelős szakállomány felelőssége, hogy ez az aktus ne egy gépies, automatikus, bürokratikus kötelesség legyen, hanem a helyi viszonyokat, változásokat valóságosan lekövető, a folyamatos egyenszilárdságú védelmet biztosító eljárás. A nyílt katonai információs rendszereket üzemeltető szakállomány akár katona, akár szerződéses munkaviszonyba álló civil személyzet a katonai függőségi viszonyokhoz és szigorúan kötött napi és munkarendhez szocializálódott, így a jogszabályi előírások betartása és betartatása számukra nem jelent kilépést a saját komfortzónájukból.

Ha az elektronikus információs rendszerrel rendelkező szervezetre vagy a szervezeti egységre a 41/2015 BM rendelet előírásai szerint kidolgozott szabályzatokban meghatározott adminisztratív és fizikai védelmi intézkedésektől egy elektronikus információsrendszer esetében a magasabb védelmi igény miatt el kell térni, az eltéréseket az érintett elektronikus információs rendszer a rendelet előírásai szerint kidolgozott szabályzatában kell rögzíteni. (41/2015. (VII. 15.) BM rendelet, 2018)

Tehát a jogszabály által előírt védelmi intézkedéseken túl, a rendszer üzemeltetéséért felelős szervezet vezetője az előírtaknál szigorúbb intézkedések betartását is előírhatja, de az eljárásrendeket rögzítenie kell az elektronikus információbiztonsági szabályzatában. Tehát ha például kockázatelemzés eredményeképpen olyan sebezhetőségeket találnak, amelyek speciálisan bizonyos információs rendszereket érintenek, szigoríthatnak a jogszabályban előírt védelmi intézkedéseken. Ha viszont úgy ítélik meg, hogy bizonyos jogszabály által előírt védelmi intézkedés foganatosítása nem

[12] EIBSZ – Elektronikus Információbiztonsági Szabályzat

szükséges, akkor sem tekinthetnek el a kötelezően előírt intézkedések megtételétől. Ez a szabályozás segíti elő, hogy az azonos vagy hasonló célú információs rendszereket azonos elvek alapján, egységes védelmi intézkedésekkel védjék.

A minősített adatok védelmével kapcsolatos fogalmak tisztázása:

A közszférában egyedülálló módon a Magyar Honvédségnél jogszabályok alapján létrejött egy adatkezelési szint, amit úgy nevezünk, hogy „ nem nyilvános ”.

Ez a kategória a nyílt és a minősített adatkezelési szint között foglal helyet. Keletkezését a 2011. évi CXII. törvénynek köszönheti, amely szerint:

Az állami feladatot ellátó szerv kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat. (2011. évi CXII. törvény, 2023)

A jogszabály alapján a Magyar Honvédségnél, mint állami feladatot ellátó szervezetnél keletkező valamennyi adatot kérésre ki kellene adni. Ez ellenkezik a Honvédelem érdekeivel. A teljes adatállomány minősítése dolgozatomban később, a minősített adatok védelménél részletezett okokból kifolyólag nem megoldható. Ezért a jogszabályt 2013.-ban módosították:

„27. § (2) A közérdekű és közérdekből nyilvános adatok megismeréséhez való jogot – az adatfajták meghatározásával – törvény a) honvédelmi érdekből; b) nemzetbiztonsági érdekből; … korlátozhatja.” (2011. évi CXII. törvény, 2023)

„15. § (1) A honvédelmi szervezetek személyi állományára vonatkozó – a Honvédség védelmi képességének, hadrafoghatóságának biztosításával összefüggő – adatok honvédelmi és nemzetbiztonsági érdekből a keletkezésüktől számított harminc évig nem nyilvánosak. Ezen adatok megismerését a fenti érdekek mérlegelésével a honvédségi szervezet tekintetében a Honvéd Vezérkar főnöke engedélyezheti.”

(3) A honvédelmi szervezet felépítésére, működésére, haditechnikai eszközeire és anyagaira, valamint hadfelszerelésére vonatkozó adatok honvédelmi és nemzetbiztonsági érdekből a keletkezésüktől számított harminc évig nem nyilvánosak. Ezen adatok megismerését a fenti érdekek mérlegelésével a honvédségi szervezet tekintetében a Honvéd Vezérkar főnöke engedélyezheti. (2021. évi CXL, 2023)

A fenti adatokra mondja a szabályokat felszínesen ismerő személy, hogy „ 30 évre titkosítva van”. A nem nyilvános adatok védelme sajnos erősen korlátozott, adatkezelés személyi, fizikai, adminisztratív és elektronikus információvédelmi szempontból meg sem közelíti a minősített adatok kezelésénél alkalmazott védelmi rendszabályokat, eljárásrendeket. Véleményem szerint katonai műveletek végrehajtása során keletkező adatok védelméhez a fenti jogszabály alapján előírt szabályrendszer és védelmi eljárási rend nem elegendő

A védelmi szint következő lépcsőfokai a **minősített adatok**. Jogszabály szerint:

nemzeti minősített adat: a minősítéssel védhető közérdekek körébe tartozó, a minősítési jelölést az e törvényben, valamint az e törvény felhatalmazása alapján kiadott jogszabályokban meghatározott formai követelményeknek megfelelően tartalmazó olyan adat, amelyről – a megjelenési formájától függetlenül – a minősítő a minősítési eljárás során megállapította, hogy az érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele a minősítéssel védhető közérdekek közül bármelyiket közvetlenül sérti vagy veszélyezteti (a továbbiakban együtt: károsítja), és tartalmára tekintettel annak nyilvánosságát és megismerhetőségét a minősítés keretében korlátozza. (2009 évi CLV törvény, 2022)

A minősített adatok fajtáival, minősítési szintjeivel és a keletkezésükhöz, kezelésükhöz szükséges szabályrendszerrel, valamint annak véleményem szerinti hiányosságaival a további elemzésekben részletesen kitérek.

Az alábbi alapvető információbiztonsági követelmények a nyílt és minősített adatkezelő rendszerekre egyaránt értelmezhetőek, csak szakterületenként eltérő súlyozással és tartalommal.

Az állami és önkormányzati szervekre, tehát például a Magyar Honvédségre, a Kormányzati és Önkormányzati infokommunikációs rendszerekre egyaránt vonatkozó Törvényi szabályozás szerint a törvény hatálya alá tartozó elektronikus információs rendszerek teljes életciklusában meg kell valósítani, biztosítani kell az elektronikus információs rendszerben kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása, valamint zárt, teljes körű, folytonos és kockázatokkal arányos védelmét. (2013 évi L törvény, 2023)

A fenti, valamint a továbbiakban idézett jogszabályokban és általam megfogalmazott állásfoglalásokban szereplő fogalmakat az alábbiak szerint értelmezem:

Biztonság: a rendszer olyan, a védelem nem kielégítő megvalósítását elszenvedő, a védelmet előíró, továbbá a védelemért felelős személyek és szervezetek együttese számára kielégítő mértékű állapota, amelyben zárt, teljes körű, folytonos és a kockázatokkal arányos védelem valósul meg.

Védelem: Az informatikai biztonság az informatikai rendszer olyan az érintett számára kielégítő mértékű állapota, amelyben annak védelme az informatikai rendszerben kezelt adatok bizalmassága, értetlensége és rendelkezésre állása, valamint a rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos (Muha, 2008)

A védelem feladatai:

- megelőzés (a fenyegetés hatása bekövetkezésének elkerülése);
- korai figyelmeztetés (valamely fenyegetés várható bekövetkezésének jelzése a fenyegetés bekövetkezése előtt annyi idővel, hogy hatékony védelmi intézkedéseket lehessen hozni.);
- észlelés (a biztonsági esemény bekövetkezésének felismerése);
- reagálás (a bekövetkezett biztonsági esemény terjedésének megakadályozására vagy késleltetésére, a további károk mérséklésére tett intézkedés);
- eseménykezelés (az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység).

A védelem tehát olyan tevékenységek összessége, amellyel a biztonságot, mint elvárt állapotot kívánjuk elérni.

Bizalmasság: *az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.*(2013 évi L törvény, 2023)

Ennek a követelménynek az infokommunikációs rendszerek általában jelszó használatával tesznek eleget. A legegyszerűbb, végponti rádiók használata esetén lehet, hogy nem használnak jelszót sem. A rádió vagy végponti vezetékes eszköz, - telefon - használatára műveletek végrehajtása esetén gyorsan szükség lehet. Ebben az esetben a védelmi intézkedések elsősorban fizikai jellegűek. Az eszköz szállítása, tárolása,

használata során fizikai biztonsági és adminisztratív szabályokat kell betartani. A rádiók programozása és nem kifejezetten informatikai rendszer részét képező egyéb berendezések, pl. rejtjelző eszközök - a menürendszerbe való belépés előtt egy vagy több, mindenki számára közös – jelszót igényelnek.

A kifejezetten informatikai rendszerek – számítógépek jelszóházirendeket alkalmaznak a rendszerben tárolt adatok bizalmasságának megőrzéséhez.

A felhasználó azonosítása egyedi felhasználónév és jelszó alkalmazásával, vagy biometrikus azonosító alkalmazása esetén kétfaktoros hitelesítéssel történik.

Véleményem szerint a jövőben az egyre bonyolultabb jelszavak fejben tartásának követelménye teljesítése szinte lehetetlenné válik, ezért a biometrikus azonosítás előtérbe kerülhet a személy hitelesítési folyamatban. Ennek egyenlőre egyik akadálya a biometrikus azonosítók tárolásának GDPR szabályozása. A téma részleteiről a „Arcfelismerő rendszerek alkalmazhatósága a COVID járvány előtt és a járvány szigorított körülményei között" című előadásomban publikáltam a következőket: „Az Apple szerint a Touch ID (azaz ujjlenyomat-feloldás) esetében 1: 50 000-es esély van a telefon véletlenszerű kinyitására illetéktelen ujj használatakor. A Face ID (arcfelismerő funkción alapuló feloldás) esetén ugyanez az arány jelentősen kisebb, 1: 1 000 000 – (kivéve egypetéjű ikrek) Tehát a 3D-s arcfelismerő funkciójuk többszörösen biztonságosabb, mint az ujjlenyomatolvasók" (Megyeri Lajos, 2021) A minősített adatot kezelő rendszerhez való hozzáférést biztosító jelszónak a kis- és nagybetű, szám és speciális karakter négyes kombinációból legalább hármat kell tartalmaznia.

A jelszó hossza: legfeljebb „Korlátozott terjesztésű!" minősítési szintű adatot kezelő rendszer esetén legalább 12 karakter; „Bizalmas!" vagy annál magasabb minősítési szintű adatot kezelő rendszer esetén legalább 14 karakter. A jelszavak élettartama nem lehet 90 napnál hosszabb. A legutóbb használt 24 jelszó használata nem engedélyezett. A felhasználók figyelmét fel kell hívni a könnyen kitalálható jelszavak mellőzésére, illetve arra, hogy a jelszavak visszakereshető rögzítése elkerülendő.

A minősített adatot kezelő rendszeren a fiókzárolási küszöbérték beállítását úgy kell elvégezni, hogy a rendszer a harmadik sikertelen bejelentkezési kísérletet követően a felhasználót egy órára kizárja a rendszerből.(EBK, 2023)

Bár a Nemzeti Biztonsági Felügyelet által meghatározott Biztonsági követelmények lehetővé teszik, a biometrikus azonosítás a minősített adatkezelő rendszerek felhasználóinak azonosítására még nem elterjedt.

A rendszer bizalmassága természetesen egyéb rendszabályok betartása mellett annál nagyobb, minél bonyolultabb, hosszabb a jelszó és minél sűrűbben cserélik másikra. A jelszó a felhasználó identitása, egyedi azonosítója, azt nem árulhatja el senkinek és nem írhatja le sehova sem, kivéve a rendszer biztonsági menedzsment állományát. A biztonsági személyzet jelszavait olyan fizikai biztonsági körülmények között kell tárolni (biztonsági tárolóban) amely helyszínen olyan minősítési szintű adatok is tárolhatók amilyen minősítési szintű adatok feldolgozhatók azon az infokommunikációs rendszeren, amelynek a biztonsági jelszavait őrzik. A jelszavak tárolásánál jogszabályban meghatározott adminisztratív intézkedéseket is be kell tartani, amely meghatározza a jelszó tároló borítékokkal kapcsolatos eljárásrendet is. Az eljárás részleteit a 161/2010 Kormányrendelet határozza meg.

Személyes véleményem, hogy a jelszavak bonyolultságának, hosszának, cseréje gyakoriságának növelése, bár hozzájárul a bizalmasság megőrzéséhez, nagyban megnehezíti egy másik feltétel, a rendelkezésre állás teljesülését. Volt alkalmam minősített elektronikus adatkezelő rendszer biztonsági felügyelő beosztást ellátni. Személyes tapasztalatom, hogy a felhasználók több alkalommal (havi szinten átlagosan 3-4 alkalommal) nem emlékeztek pontosan a saját jelszavaikra.A jelszó hiányában nem férhettek hozzá azonnal az adatkezelő rendszeren tárolt saját adataikhoz sem. Új jelszó generálása egy hálózatba szervezett, központilag menedzselt rendszerben akár napokba is telhet. Ez a késlekedés katonai műveletek esetén véleményem szerint nem engedhető meg. A mai, digitális világban egy átlagos felhasználónak meg kell jegyeznie az általa használt valamennyi, nyílt és minősített infokommunikációs rendszere jelszavát, a telefonja, saját számítógépe, banki bejelentkezési, ügyfélkapu, levelező rendszerei, közösségi oldalai, lakóház kapu kódja jelszavát. Magáncélú rendszerek jelszavai tárolhatóak jelszókezelő alkalmazásokban, amelyek biztonságosságáról szakemberek is egymástól eltérően nyilatkoznak. Az operációs rendszerekhez és a BIOS.-hoz való hozzáféréshez ilyen alkalmazás nem használható. A jelszavak bonyolultsága és kötelezően gyakori cseréje magában hordozza a jelszótévesztés lehetőségét.

A biometrikus azonosítás:

A magyar jog megfogalmazása szerint: „biometrikus adat: egy természetes személy fizikai, fiziológiai vagy viselkedési jellemzőire vonatkozó olyan, sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, mint például az arckép vagy a daktiloszkópiai adat”(2011. évi CXII. törvény, 2023)

A biometrikus adatok a jogszabály szerint különleges adatnak[13] számítanak ezért tárolásukra, kezelésükre, továbbításukra a törvény speciális követelményeket ír elő. A minősített adatok védelmének jogos érdeke jogalapot teremt a biometrikus adatok kezelésére. Az ilyen adatokat kezelő rendszer beállításainál fontos, hogy a felhasználók biometrikus adatait csak addig tárolhatja a rendszer, ameddig a belépéshez szükséges személyes hitelesítés a célja. A felhasználónak a rendszerből való törlése esetén a személy biometrikus adatainak is meghatározott határidőn belül törlődniük kell.

A biometrikus azonosító olyan biológiai jegy, amely nagy mértékben egyedi (minden emberre vonatkozóan más- és más) és alkalmas arra, hogy megfelelő berendezések könnyen gyorsan felismerjék, így egy adott informatikai rendszerben a személyek - felhasználók - személyi azonosítását lehetővé tegye. Ilyen lehet az ujjnyomat, az írisz (szivárványhártya) mintázata, de akár az arckép vagy a hang is.

A minősített adatok kezelésénél véleményem szerint csak az ujjnyomat azonosításnak lehet létjogosultsága. Bár az arc vagy az írisz azonosítás hasonlóan pontos lehet, de ezekhez mindenképpen optikai beviteli eszközt, kamerát kell használni, amelynek a használata minősített adatkezelő rendszereknél fenyegetést jelenthet a rendszerben tárolt adatok bizalmasságára.

Meggyőződésem, hogy a jövőben a magáncélú és az állami, közfeladatot ellátó infokommunikációs rendszerekben kezelt adatok bizalmasságának megőrzéséhez a legbiztonságosabb és leghatékonyabb módja a biometrikus azonosítás[14] lehet.

A jogszabály által megkövetelt kétfaktoros azonosítás másik eleme lehet egy rövid un. „PIN” kód, amelynek a megjegyzése lényegesen könnyebb, mint a jelenleg használt 14

---

[13] *különleges adat:* a személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok,(2011. évi CXII. törvény, 2023)

[14] Biometrikus azonosító

Olyan biológiai jegy, amely nagy mértékben egyedi (minden emberre vonatkozóan más-és más) és alkalmas arra, hogy megfelelő berendezések könnyen gyorsan felismerjék, így egy adott informatikai rendszerben a személyek - felhasználók személyi azonosítását lehetővé tegye. Ilyen lehet az ujjlenyomat, az írisz (szivárványhártya) mintázata, de akár az arckép vagy a hang is. Mivel a teljesen pontos egyedi azonosítás ilyen jegyek segítségével költséges és lassú lehet, sokszor kombinálva használják egyéb technikai azonosítóval (jelszó, PIN kód, azonosító kártya, stb.)Forrás:https://fogalomtar.aeek.hu/index.php/Biometrikus_azonos%C3%ADt%C3%B3 Letöltés ideje:1023.01.25.

karakteres jelszóé. Ezen kívül a PIN kódok rendszeres váltását általában még a legszigorúbb ellenőrző rendszerek sem követelik meg.

A folyamatos rendelkezésre állás érdekében javaslom, hogy a belépéshez minden felhasználóhoz két különböző ujjnyomat rajzolatot rendeljen a rendszer, a jobb és a bal kézről egyet-egyet, esetleges bőrsérülések esetén nagyobb esély legyen a felhasználó hitelesítésére. Ezen kívül javaslom, hogy a beléptető rendszer két egymástól független ujjnyomat leolvasóval rendelkezzen. Bármelyik meghibásodása esetén a másik leolvasó használatával biztosítható a rendszerhez történő hozzáférés. Véleményem szerint az infokommunikációs eszközök beszerzési árait ez a kiegészítő részegység nem növeli meg szignifikánsan. Egy TEMPEST védelmi képességű számítógép jelenlegi árát most is millió forint nagyságrendben állapítják meg, amelyhez képest az ujjnyomat olvasó periféria elenyésző mértékű pluszköltséget jelent.

Sértetlenség: *az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható.*

Tehát arra vonatkozik, hogy az adat fizikailag és logikailag teljes és bizonyítottan vagy bizonyíthatóan az elvárt forrásból származik.

A sértetlenség biztosítása tárolt adatok esetében a hozzáférések szigorú felügyeletét jelenti, amely megakadályozza jogosulatlan személy hozzáférését az adatokhoz. Ez fizikai és adminisztratív védelmet egyaránt jelent. Hálózatban működő infokommunikációs rendszerek esetében szoftveres megoldásokkal biztosítják s hitelességet és a megváltoztathatatlanságot.

A szoftveres megoldás legelterjedtebb változata az elektronikus aláírás rendszere, melynek működésére, polgári és katonai alkalmazásának lehetőségeire dolgozatom további fejezeteiben részletesen kitérek majd.

Rendelkezésre állás: *annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek;*

Véleményem szerint a civil és a katonai infokommunikációs rendszerek esetében is ez a legnehezebben teljesíthető, legtöbb kihívást magába foglaló feltétel. Önállóan üzemelő munkaállomások esetén az a helyben tárolt adatok esetében az adathordozó fizikai

sérülését, megsemmisülésének lehetőségét kell elfogadhatóan alacsony szinten tartani. Ezt az adatok fizikailag különválasztott biztonsági másolataival, RAID[15] technológia alkalmazásával és új eszközök esetén a fizikai behatásokkal szemben kevésbé érzékeny SSD[16] adattárolók alkalmazásával érik el.

A rendelkezésre állás biztosítása hálózatban együttműködő, általában szerver számítógép támogatásával szervezett rendszerek esetén már koránt sem ilyen egyszerű. Kulcsfontosságú jelentősége van a munkaállomás és a támogató, általában adattároló szerver számítógép közötti kapcsolat folyamatosságának, kezelt adatok bizalmas tárolásának és továbbításának, katonai infokommunikációs rendszerek esetén a rendszer működésése rejtettségének. Minden esetben fontos, de katonai műveletekben kiemelt jelentőségű a nem helyben tárolt adatok lehetőleg folyamatos elérése. Katonai vonatkozásban, különösen háborús katonai műveletek esetén a folyamatos elérés nem azt jelenti, hogy a kapcsolat állandó. Egy folyamatosan élő kapcsolat könnyebben felfedhető, lehallgatható, zavarható a szembenálló fél részéről. Alkalmazástól függően az infokommunikációs eszköz geolokációs helye is beazonosítható. Ezekben az esetekben a rendelkezésre állás azt jelenti, hogy a rendszer infokommunikációs eszközei bekapcsolásuk esetén a lehető leggyorsabban kapcsolódjanak össze adattovábbítás vagy adatcsere végrehajtása céljából.

Az információk folyamatos elérhetőségének biztosítása, a rendszert rendelkezésre állása százalékos formában is kifejezhető. Magasabb rendelkezésre állást több rendszerelem erőforrás alkalmazásával lehet elérni, ami nagyobb anyagi befektetést igényel. A rendszer bármely elemének meghibásodása esetén a részegység mielőbbi cseréjét vagy feladatának átterhelését más elemekre, komoly mérnöki, informatikusi tervező és végrehajtó munkával lehet biztosítani. A rendszerelemek folyamatos, szünetmentes tápellátása például ennek a területnek csak egy kicsi, de kulcsfontosságú részterülete. Speciális informatikai eszközök, például TEMPEST tanúsítványú számítógépek esetén, melyek beszerzése az általános rendeltetésű, hasonló kapacitású számítógépek sokszorosába kerül, előtérbe kerülhetnek az üzemeltető szervezet financiális lehetőségeinek a határai is. Véleményem szerint az egyik legfontosabb befolyásoló tényező az információ tárolásának helye. A helyben tárolt adatokhoz lehet a leggyorsabban és biztonságosabban hozzáférni. Az információ távoli elérése bármilyen megvalósítás esetén magasabb

[15] RAID-Redundant Array of Independent Disk ~Redundáns információ független lemezre

[16] SSD-Solid State Driver ~ Szilárd test meghajtó

technikai követelményeket igényel és biztonsági kockázatokat is rejt. A rendelkezésre állás tehát egy pénzben is kifejezhető kategória, akár átmeneti hiánya azonban kritikus infrastruktúrák működtetésének biztosítása vagy katonai alkalmazások esetén akár emberéleteket is követelhet.

Zárt védelem: *az összes számításba vehető fenyegetést figyelembe vevő védelem*.

Az infokommunikációs rendszerek felépítésüktől (hardver, szoftver), üzemeltetésük módjától, feladatrendszerüktől, fizikai elhelyezésüktől függően rendszerelemeiket tekintve különbözően sebezhetőek, és más-más fenyegetések irányulnak rájuk. Az adatkezelő rendszerek tervezésekor kockázatelemzést kell végezni, amelyben azonosítani kell a sebezhetőségeket és releváns fenyegetéseket. Ki kell dolgozni a fenyegetésekkel szembeni szükséges ellenintézkedéseket, különös tekintettel arra, ahol egy sebezhetőségre fenyegetés irányul. Az infokommunikációs rendszer védelmét ennek alapján kell szervezni, üzemeltetni. Ezt a témát részletesen elemeztem „Kockázatkezelés, tudomány vagy kuruzslás és a Secure mantenance of eletronic information system in Public service című cikkeimben melyekben a következő eredményre jutottam:

Napjaink bonyolult világában a tudományterületek specializálódása révén komoly tudásanyag gyűlt össze a kockázatelemzésről az élet minden területéről.

Minden kockázatot elkerülve, az abszolút biztonság állapotát sajnos soha nem lehet elérni. Minden lény, eszköz, rendszer és társadalom sebezhető. Végtelen idő, pénz és munka nem biztosítható a biztonság megteremtéséhez. Az erőforrások ésszerű felhasználására van szükség, és ebben nyújthat segítséget a kockázatok feltárása, elemzése.(Megyeri Lajos, 2018c)

„A kockázatelemzési módszerek közül információs rendszerek esetében Véleményem szerint a CRAMM típusú kockázatelemzés a legkönnyebben és leghatékonyabban alkalmazható. Jó támpontok lehetnek a vagyontárgyak, fenyegetések, sebezhetőségek előre elkészített listái. Számításai logikusak, nem igényelnek különleges képességeket, ami azért fontos, mert a jogszabályok alapján sok telepítési helyen kell egyszerre elkészíteni az elemzést és a szakemberek ismeretei sem egyformák.”(Megyeri Lajos, 2017)

Teljes körű védelem: *az elektronikus információs rendszer valamennyi elemére kiterjedő védelem*

Az elektronikus információs rendszer elemei az alábbiak: (Muha & Krasznay, 2018)

Tárgyiasult elemcsoportok:

- környezeti infrastruktúra,

- hardver,
- adathordozók,
- dokumentumok, iratok.

Logikai elemcsoportok:

- szoftver,
- adatok,
- kommunikáció.

Személyi elemcsoport:

- személyzet,
- felhasználók,
- ellenőrök.

Az infokomunikációs rendszer tervezésekor, kialakításakor és üzemeltetése során a fenti csoportok valamennyi elemét egyenként vizsgálni kell a védelem szempontjából.

Folytonos védelem: *az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem*

A védelmi intézkedéseket a rendszer biztonsági szabályzatában rögzített időközönként illetve a rendszer működésének biztonságát érintő bármilyen változás után felül kell vizsgálni. Ha szükséges, a védelmi rendszabályokon, eljárásokon változtatni kell.

1.4.2.Kockázatkezelés

Kockázatokkal arányos védelem**:** *az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével;*

A kockázatkezelés két alapvető formája lehet:

- Kockázatkerülés

Bizonyos károk, veszteségek esélyének a teljes kiküszöbölését jelenti. Jelentheti azt, hogy a szervezet az elemzés alapjául szolgáló tevékenységével a kockázatok növekedése miatt felhagy. Általános, minden területre kiterjedő kockázatkerülés nem lehetséges, mert ez a vizsgált rendszer működésképtelenségét jelentené. Egyes szolgáltatások megszüntetése a túlzottan magas kockázat miatt azonban lehetséges. Ezt az elvet katonai feladattervezés során, feladataink maradéktalan végrehajtása érdekében általában nem alkalmazzuk.

- Kockázatok csökkentése

Ez az elv jelenti az igazi kockázatkezelést, mert itt a kockázat csökkentésére a szervezet saját szervezési vagy hardver – szoftver eszközeit használjak fel. Ez az elv jelenleg a

katonai infokommunikációs feladattervezés egyik alapja. Hátránya a nagy erőforrásigény és a manőverező képességek korlátozott alkalmazhatósága. Az eljárások, melyek ebbe a csoportba tartoznak, három részre oszthatók.

A kármegelőző (pre-loss) elvek biztosítják azt, hogy a szervezet gazdaságosan, a jogszabályoknak megfelelően működjön. Itt nem az a cél, hogy teljes mértékű biztonságot érjenek el, hiszen ez gyakorlatilag lehetetlen. Ebbe a csoportba tartozik az épületek, gépek, járművek, berendezések szabályszerű, rendszeres karbantartása, informatikai rendszerek védelmi rendszere, tűzfal, kártékony programok elleni védelem, szabályzatok, utasítások kidolgozása, betartása.

A másik csoport a kárenyhítést célozza. Az úgynevezett pro-loss vagyis kárenyhítő kockázatkezelés a károk bekövetkezésének megakadályozásával nem foglalkozik, mert itt a bekövetkezett károk hatásának enyhítése a cél. Alapvető követelmény a rendszer visszaállítása a lehető legrövidebb időn belül a lehető legkisebb adatveszteséggel. Fontos, hogy a szervezet alaprendeltetésből adódó működőképessége folyamatosan fennmaradjon.

A harmadik kategóriába tartoznak azok a vállalt kockázatok, melyek nem igényelnek semmiféle intézkedést. Ennél a stratégiai részterületnél a passzivitás az irányadó. Ezek olyan kockázatok melyek elhanyagolhatóak, elenyészőek, de mégsem illenek bele az előbbi két csoportba. Egyes terminológiákban ezt maradvány kockázatnak nevezik, melyet a szervezet vezetőjének írásban el kell fogadnia.

<u>Kockázatmegosztás, kockázatáthárítás</u>

Ezt az eljárásrendet követjük, amikor a rendszert tervező, üzemeltető szervezet a kockázatok egy részét egyedül nem képes vagy nem kívánja vállalni, ezért áthárítja azokat. A partner lehet állami szervezet, hatóság, üzleti partner, befektetők, pénzintézetek, biztosítótársaságok. Az üzleti szerződések feltételeinek megfelelő alakítása lehet az egyik módja a kockázat áthárításának. A szerződés megkötésekor mérlegelni kell a kockázatokat és azok elosztását a szerződő felek között. Ez az eljárásrend véleményem szerint katonai műveletek támogatása esetén csak nagyon pontosan megfogalmazott és valamennyi információbiztonságra vonatkozó, jelen dolgozatban megemlített jogszabályi előírás figyelembe vételével kötött szerződésekkel lehetséges.

A rendszer tervezésekor, üzembe helyezés előtt kockázatelemzést kell készíteni. Az informatikai rendszerek esetében a kockázatvállalás önmagában nem eredményez kimutatható nyereséget. Ha védelmi rendszerünket a kockázat elemzésnek köszönhetően

jól alakítjuk ki, akkor nem következik be kár, veszteség. Ezért nehéz a tulajdonost, döntéshozót rábírni arra, hogy anyagi erőforrásokat fordítson a biztonságra, mert az ebből fakadó „elmaradt kár" nehezen mutatható ki mindaddig, amíg valós biztonsági esemény kapcsán veszteség nem éri a tulajdonost. Jogszabályi megfogalmazás szerint: „kockázatelemzés: fenyegetettségi és kockázati tényezők vizsgálata a rendszerelemek sebezhetőségének, valamint a megzavarásuk vagy megsemmisítésük által okozott következmények értékelése céljából;" (65/2013. (III. 8.) Korm. rendelet, é. n.)

Meglátásom szerint a fogalom így nem letisztult, a kockázati tényezők vizsgálata alatt sok mindent lehet érteni. A jogszabály nem ad egyértelmű iránymutatást a kockázatelemzés végrehajtásának módszerére bár a kockázatok azonosításának és értékelésének a módját részletesen leírja, mivel a rendszerelemet fenyegető kockázati lista készítését határozza meg majd a kockázatok valószínűsíthető okainak feltárását írja elő a prognosztizálható negatív hatás meghatározásával együtt.

A kockázatok értékelését írja elő, majd a kockázatok kezelését a kockázati szint függvényében. Ez a metódusra véleményem szerint a CRAMM típusú kockázatelemzés képes bár a jogszabály a kockázatelemzés módját nem határozza meg.

A kockázatelemzések módjainak részletes elemzése túlmutat jelen disszertáció keretein ezért a továbbiakban csak vázlatosan tekintem át a végrehajtandó lépéseket.

Először azonosítani kell a védendő vagyontárgyakat, rendszerelemeket:

- Elsődleges vagyontárgyak:
  - Információ
    - „élet fontosságú" információk amelyek szükségesek a szervezet küldetéséhez
    - A helyi törvények által védett információk
    - Stratégiai információk
    - Nagy értékű információk amelyeknek a beszerzése nagy bekerülési költségű
    - Egyéb információk
- Támogató vagyontárgyak:
  - Hardware
    - Aktív adatfeldolgozó berendezések
    - Hordozható berendezések
    - Stabil berendezések
    - Perifériák

    - Elektronikus adattárolók
    - Egyéb adattárolók
- Software
    - Operációs rendszerek
    - Kisegítő szoftverek (vírusirtók, naplózók…)
    - Alkalmazói szoftverek (irodai-, tervező-, …)
    - Speciális a szervezet számára kifejlesztett szoftverek
- Hálózat, tartalmazza az összes berendezést amely a különböző berendezéseket kapcsolja össze
    - Passzív és/vagy aktív kapcsolók (hub, switch, router…)
    - *Protokollok*
    - Kommunikációs interface-k
- Személyzet,
    - Döntéshozók
    - Felhasználók
    - Üzemeltető és biztonsági személyzet
    - Fejlesztők
- helyszín,
    - Külső környezet
    - A felügyelet alatt tartott terület (épület és telek)
    - Belső zóna
    - A működéshez szükséges szolgáltatások
    - A kommunikáció
    - Közművek

Ezt követően meg kell határozni, hogy az infokommunikációs rendszer elemeire milyen fenyegetések irányulnak. Vannak előre elkészített, általánosan jellemző fenyegetéseket felsoroló listák, melyek kiegészítéssel, pontosítással segítséget nyújtanak a konkrét infokommunikációs rendszerrel szembeni fenyegetések azonosításához (Elemi kár, zárlat, szándékos károkozás, elektronikus zavarás, impulzus, lehallgatás, …)

Következő lépésben meg kell vizsgálni, hogy a rendszer elemeinek milyen sebezhetőségei vannak. (tapasztalatlan üzemeltetők, védőföldelés hiánya, nyílt kommunikációs csatorna használata, érzékenység vízre, elektromágneses impulzusra, rázkódásra, vírusdefiníciók nem gyakori frissítése, …)

A sebezhetőségekre is vannak előre elkészített, infokommunikációs rendszerekre általánosan érvényes listák, melyek pontosításával könnyebbé tehető a vizsgált rendszer sebezhetőségi listája. Ezeket az információkat tapasztalt szakemberek üzemeltetési tapasztalatok alapján gyűjtötték tematikus listákba a kockázatelemzés elkészítésének megkönnyítése és egységesebb értelmezése céljából.
Miután a listák elkészültek, az előre kiválasztott típusú elemzési eljárással meg kell határozni a rendszer elemek védelmének rendszerét. Igen elterjedt pl. a Cramm típusú kockázatelemzés. Valamennyi elemzésnek az a lényege, hogy pontosan meghatározza az egyes rendszerelemek sebezhetőségének csökkentésére, az elemre irányuló fenyegetés elhárítására alkalmazandó valós technológiai vagy szervezési eljárást. A biztonsági intézkedések anyagi erőforrást igényelnek. A kockázatokkal arányos védelem azt jelenti, hogy nem költhetünk több pénzt a védelemre, mint amennyi pénzt az adatok érnek, amelyeket az eljárásokkal védünk. Ez a kereskedelemben viszonylag könnyen kiszámítható. Katonai műveletek esetén nehéz az információk értékét pénzben meghatározni. Minősített adatkezelés esetén pedig a kockázatelemzéstől függetlenül csak szigorú és költséges eljárásrend és technológiai fegyelem betartásával engedélyezett az infokommunikációs rendszer üzemeltetése. A kockázatelemzés eredményét létfontosságú rendszerelemek esetén úgynevezett azonosítási jelentésben meg kell jeleníteni. Az üzemeltető a kockázati szinteknek megfelelően foganatosít biztonsági intézkedéseket a rendszerelem biztonsága érdekében.

1.5.Összefoglalás, következtetések:

- A fejezetben behatároltam dolgozatom tárgyának definíciós hátterét, amely során meghatároztam és dolgozatom témájának szempontjából értelmeztem azokat a katonai műveleti és infokommunikációs fogalmakat, amelyek dolgozatom szempontjából fontos, megkerülhetetlen szakmai terminus technicusok.
- Megállapítottam, hogy nem támaszkodhatunk minden esetben a NATO szövetségi infokommunikációs eszközrendszereire, nemzeti érdekből, saját erőből tervezni és üzemeltetni kell a Magyar Honvédség katonai műveleteinek támogatásához szükséges infokommunikációs rendszereket, melyek nemzetközi szabványok szerint a működésük teljes spektrumában kompatibilisek egymással.
- Rámutattam, hogy a nem nyilvános adatok védelme sajnos erősen korlátozott, adatkezelés személyi, fizikai, adminisztratív és elektronikus információvédelmi szempontból meg sem közelíti a minősített adatok kezelésénél alkalmazott

védelmi rendszabályokat, eljárásrendeket. Véleményem szerint katonai műveletek végrehajtása során keletkező adatok védelméhez a fenti jogszabály alapján előírt szabályrendszer és védelmi eljárási rend nem elegendő.

- Előrevetítettem a hozzáférések hitelesítéséhez szükséges hitelesítési eljárásrend változásának a lehetőségét. Véleményem szerint a jövőben az egyre bonyolultabb jelszavak fejben tartásának követelménye teljesítése szinte lehetetlenné válik, ezért a biometrikus azonosítás előtérbe kerülhet a személy hitelesítési folyamatban. Ennek egyenlőre egyik akadálya a biometrikus azonosítók tárolásának GDPR szabályozása.
- Hangsúlyoztam az infokommunikációs rendszerekben tárolt adatok tárolási helyének fontosságát. Véleményem szerint a tárolás helye döntő fontosságú az infokommunikációs rendszerek rendelkezésre állási képességének biztosításához. A helyben tárolt adatokhoz lehet a leggyorsabban és biztonságosabban hozzáférni. Az információ távoli elérése bármilyen megvalósítás esetén magasabb technikai követelményeket, összetettebb eszközrendszer használatát igényli és az adatok továbbítása során nagyobb biztonsági kockázatokat is rejt.

2. A katonai műveletek infokommunikációs támogatásának lehetőségei katonai információs infrastruktúra alkalmazásával.

A katonai műveletek végrehajtása során a vezetés és irányítás folyamatos biztosítása valamint a legtöbb harcoló alegységnél a felderítési és cél információk szakadatlan biztosítása is elengedhetetlen feltétele a harc sikeres megvívásához vagy a békeművelet céljának eléréséhez.

Farkas és Szeleczki a fentieket így fogalmazta meg:

„A 21. században a harci tevékenységek során az információs berendezkedés fontossága, a digitalizáció, továbbá az információs fölény megszerzésére való törekvés megkérdőjelezhetetlen. A hadseregek haditechnikai korszerűsítési folyamatokon mennek keresztül, amely időszakosan a Magyar Honvédség számára is kihívásként jelenik meg. NATO-tagországként a fejlesztések egy része szövetségi követelményekben fogalmazódik meg. A dinamikusan változó információs helyzetekre felkészülve több fejlesztési folyamat is jellemzi hazánk katonai korszerűsítési folyamatait. A probléma a hiányos területekben felmérhető, s vele a jövőbeli harcászati képességek felbecsülhetők. Az infokommunikációs támogatás megvalósítása fontos eleme a haderő képességeinek fejlesztésében.”(Szeleczki & Farkas, 2022)

A fenti gondolatokat azért idéztem ide, mert a benne foglaltakkal egyetértve számomra láthatóvá vált, hogy a témával foglalkozó szakemberekben hasonló gondolatok fogalmazódnak meg. Emellett kijelenthető hogy Magyarországon jelenleg NATO tagságunk kezdete óta nem látott mértékben zajlik a haderő modernizációja, ennek keretében pedig az infokommunikációs rendszerek megújítása is. Lássuk, mit foglal magában a katonai információs infrastruktúra fogalomköre:„A **híradó és informatikai infrastruktúra** egyrészt biztosítja a különböző szaktevékenységekhez, szervezeti funkciókhoz rendelt speciális híradó és informatikai alkalmazói szolgáltatások (célrendszerek) működési környezetét, azok műszaki és szoftver alapjait, másrészt fenntartja, működteti és a felhasználók széles köre számára elérhetővé teszi azokat az általános híradó és informatikai szolgáltatásokat, amelyek a szervezetek és személyek számára napi tevékenységük során szervezeti hovatartozásuktól függetlenül szükségesek (irodai informatikai alkalmazások, elektronikus levelezés, telefon, fax stb.)

A **híradó infrastruktúra** a stacioner telepítésű, állandó jellegű híradórendszer elemeiből – átviteli csatornák, rendezők, jelformálók, multiplexerek, modemek, mikrohullámú állomások, stacioner műholdvevők, kapcsoló berendezések, adatátvitelt felügyelő

berendezések és szoftverek, távbeszélő és fax készülékek stb. tevődik össze. A híradó infrastruktúra alapját képezi a békeidőszakban honi területen megvalósított híradó szolgáltatások biztosításának, a nagytávolságú hang, kép és adatátvitelnek, valamint felcsatlakozási lehetőséget biztosít a telepíthető híradórendszerek számára.

Az **informatikai infrastruktúra** tartalmazza az informatikai rendszerszolgáltatásokat, az általános célú alkalmazói szolgáltatásokat, az operációs rendszereket, az informatikai hálózatfelügyeleti eszközöket, a webkiszolgálókat, adatbázis-kezelő rendszereket, a közös felhasználású számítógép szervereket, a számítógép munkaállomásokat, a perifériákat és háttértárolókat, az általános elektronikus biztonsági szolgáltatásokat, valamint az általános alkalmazói szolgáltatásokhoz kapcsolódó, és a felhasználók döntő része által igénybe vett szoftvereket, úgy mint az Office-t, vagy a fájlkezelő programokat.(Hír/4, 2013b)"

(A katonai infokommunikációs rendszerek tervezésének egyik meghatározó tényezője a továbbítandó adatok nyílt vagy minősített volta, minősítési szintjének meghatározása,)

2.1 Nemzeti stacioner rendszerek

Magyar Honvédség híradó és informatikai képességeivel szemben támasztott alapvető követelmények dolgozatom szempontjából legfontosabb elemei a következők:

- Biztosítsák a honvédségi szervezetek vezetési-irányítási, végrehajtási és együttműködési információs folyamatainak hatékony támogatását, tegyék lehetővé a szervezetek és feladatok széles körében felhasználható híradó és informatikai szolgáltatások biztosítását, képezzék alapját a honvédségi szervezetek integrált, egységes elvek és követelmények alapján kialakított információs rendszerének.
- Biztosítsák a honvédségi szervezetek vezető és végrehajtó állománya döntéseihez, tervezési-szervezési tevékenységeihez szükséges információk időbeni, hiteles, torzításmentes, megbízható és védett gyűjtését, továbbítását, tárolását, feldolgozását és rendelkezésre bocsátását a megfelelő formában, feldolgozottságban és tartalomban, biztosítsák a szervezeti feladatok végrehajtáshoz szükséges adatok megfelelő helyen, időben, tartalomban és formában történő rendelkezésre állását.
- Biztosítsák a fegyvernemek és szakmai honvédségi szervezetek speciális tevékenységének támogatását, képezzék alapját információs folyamataik végrehajtásának.

- Biztosítsák a hatékony információcserét a kormányzati, közigazgatási, rendvédelmi, katasztrófavédelmi, nemzetbiztonsági, mentési és tűzvédelmi szervezetekkel.
- Biztosítsák a hatékony, szabványos információcserét a NATO-parancsnokságokkal, a NATO és EU tagállamok védelmi minisztériumaival és fegyveres erőivel, a műveletekben együttműködő szövetséges erőkkel és nem kormányzati civil szervezetekkel.
- Biztosítsák a hatékony, műveleti követelményeknek megfelelő információcserét egyrészről az MH felső vezetése, műveleti vezetése és az MH erre kijelölt ügyeleti szolgálatai, másrészről a külföldi missziókban részt vevő katonai szervezetek között, biztosítsák a magyar missziós alegységek tevékenységének támogatását, kapcsolattartását az együttműködő erőkkel és szervezetekkel.(Hír/4, 2013b)

A fenti elvárásoknak megfelelő stacioner hírrendszer elemek:

A Magyar Honvédség Műveleti Vezetési Rendszere (MH MVR) működésének infokommunikációs támogatását a Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózatának (MH KCEHH) rendszerei, továbbá bérelt szolgáltatások biztosítják.

A MH Kormányzati Célú Elkülönült Hírközlő Hálózata (a továbbiakban: MH KCEHH): a nyilvános hírközlő hálózatoktól elkülönült, az MH honvédelmi feladatainak híradó és informatikai támogatása érdekében üzemeltetett állandó és telepíthető telepítésű híradó és informatikai rendszer;(55/2013 HM rendelet, é. n.)

Farkas megfogalmazása szerint: „ A kormányzati célú rendszerek elkülönített eleme a Magyar Honvédség hálózata,amely teljesen más szervezési elven alapul, illetve nem a Nemzeti Távközlési Gerinchálózatot használja felületként. Függetlenül működik tőle, de a hálózat beintegrálását biztosítja a kormányzati rend-szerbe egy kapcsolódási felületen. Ezáltal tehát a teljesen eltérő felépítésű és szolgál-tatást nyújtó rendszerről van szó, amely biztosítja a honvédség és szervezetei részére az infokommunikációs szolgáltatásokat”(Farkas, 2020)

A Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózata alapját impulzus kód modulációt alkalmazó berendezések alkotják, amelyek mikrohullámú összeköttetést biztosítanak mind adat, mind beszéd továbbításra. Ez a rendszer az állandó hírrendszer alapja, a napjainkban megvalósuló infokommunikációs kapcsolódások közel 90%-a ezen valósul meg. A hálózat Magyarország szinte teljes

területét lefedi, így minden egyes állandó állomáshelyként működő katonai objektumot összeköt. A Magyar Honvédség stacioner rendszereiben a mikrohullámú összeköttetések mellett folyamatosan fejlesztik a mai kor követelményeinek megfelelő optikai hálózatokat is.

A katonai objetumokon belüli összeköttetések, valamint nagy többségben a kapcsolatok a mikrohullámú hálózat és a végberendezések között fémalapú (réz, alumínium) kábelek alkalmazásával valósulnak meg. A végberendezésekkel együtt ilyen módon kapcsolódnak a forgalomirányítók és kapcsolók egymáshoz, ezáltal kialakítva az adott helyőrség kommunikációs és információs hálózatát.

Az állandó hírrendszer folyamatos működését biztosító katonai szervezeteket ugyan időszakonként átszervezik, az egyes működési területek határait, a különböző katonai szerezeteknek a teljes rendszer működtetésében részt vállaló felelősségét a rendszer zavartalan és megbízható működtetésének érdekében mindenkor pontosan meg kell állapítani.

2.1.1. Nemzeti stacioner hírhálózat

Az ország területén állandó elhelyezési körletekben és kiképzési objektumokban üzemelő infokommunikációs hálózat a Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózata (MH KCEHH). Jobbágy Szabolcs megfogalmazása szerint ez egy olyan speciális céllal megvalósított, zártcélú infokommunikációs hálózat, amely akár békeidőben, akár minősített időszakban a katonai felsővezetés döntéseinek, az MH vezetés és irányítási rendszereinek a támogatására hivatott azáltal, hogy biztosítja az ehhez szükséges technológiai-, technikai és szolgáltatási hátteret, illetve működési környezetet. Egy olyan, a már meglévő hálózati infrastruktúra, híradó és informatikai rendszerek és eszközök alapjain nyugvó korszerű hálózat, az MH egykori zártcélú hálózatának a továbbfejlesztése, amely egyelőre még inhomogén és részben konvergált, de már fejlett szolgáltatásokat nyújtani képes kritikus infrastruktúrának minősül.(Jobbágy, 2017)

A rendszer működtetésének részleteit 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 – írja elő.

Honvédelmi Katasztrófavédelmi Rendszer (HKR)

„Az Országos Katasztrófavédelmi Rendszer részét képező, a honvédelmi ágazat katasztrófavédelmi feladatainak irányítására, végrehajtására, valamint az országos katasztrófavédelmi feladatokban való közreműködés érdekében létrehozott, a Magyar Honvédség meglévő képességein alapuló, kijelölt szervezeti elemekből felépülő, ideiglenes szervezet.

A HKR híradása az MH állandó hírrendszere által biztosított elemekből áll. A HKR keretében a jogszabály szerint az MH vitéz Szurmay Sándor Budapest Helyőrség Dandár (MH BHD) működteti az MH BHD Katasztrófavédelmi Operatív Csoportot, tervezi, szervezi és végrehajtja a Stratégiai Műveleti Vezetési Csoport (SMVCS) – Katasztrófavédelmi Operatív Törzs (KOT) működésének valós biztosítási feladatait, különösen a híradó-informatikai, élelmezési és pihentetési feladatokat.

A rendszer része egy az MH intranethálózatára telepített dedikált számítógépcsoport. A munkaállomások adattárait a felkészülés időszakában feltöltik a tervezett feladatok végrehajtásához szükséges adatokkal, azokat rendszeresen pontosítják. A hálózat elemei megtalálhatóak minden szinten, biztosítva ezzel a valós idejű adatáramlás lehetőségét a tervező és a végrehajtó szintek között. A végrehajtás szintjén az operatív csoportok (OCS) irányítják a katasztrófavédelemre kijelölt alegységek munkáját a feladat végrehajtására kiutalt EDR-készülékekkel, illetve azadott katonai szervezet által szervezett híradócsatornákon, ami elsősorban rövidhullámú és kézi URH katonai rádiók alkalmazását jelentik”(Megyeri Lajos, 2018a).

A rendszerek folyamatos üzemeltetéséhez természetesen szakemberekre van szükség. Farkas és Hronyecz megállapítása szerint „A védelmi szféra egyes szervezeteinél dolgozó infokommunikációs szakemberek (különböző szintű vezetők és felelős beosztású személyek) alapvető ismereteit a különböző felsőoktatási intézmények, különböző szintű képzésein sajátítják el. Ezt követően a többéves szakmai tapasztalattal és a különféle továbbképzésekkel bővítik ki ismereteiket, de csak a saját szervezetükön belül”(Farkas & Hronyecz, 2018)

Tehát a rendszerek biztonságos üzemeltetéséhez szükséges állomány biztosítása előrelátó tervezést és a képzési tervek következetes végrehajtását is igényli.

2.1.2.NATO stacioner hírhálózat

A Többnemzetiségű katonai műveleteit támogató infokommunikációs rendszerek alapvető feladatai kutatásaim alapján:

- A Többnemzetiségű katonai egységek, támaszpontok közötti állandó infokommunikációs hálózat az egyik legfontosabb eszköz a szövetség katonai műveleteinek támogatásában.
- Az infokommunikációs hálózatok biztosítják a Nemzetek közötti gyors és biztonságos kommunikációt a katonai parancsnokságok és egységek között.
- A hálózatok magas szintű titkosítással és védelmi mechanizmusokkal rendelkeznek, hogy megakadályozzák az illetéktelen hozzáférést és a védekezzenek az állami és civil kiberfenyegetésekkel szemben.
- Az infokommunikációs hálózatok lehetővé teszik az információk gyors és hatékony megosztását a Nemzetek között, ami növeli a katonai műveletek összehangolását és hatékonyságát.
- Az infokommunikációs rendszerek segítségével a többnemzeti parancsnokságok valós időben nyomon követhetik a hadműveletek alakulását és az egységek helyzetét a világ különböző részein.
- A hálózatok lehetővé teszik a katonai felderítő és megfigyelő rendszerek adatainak gyors és pontos feldolgozását, hogy az információk időben eljussanak a döntéshozókhoz.
- Az infokommunikációs hálózatok további Nemzetekkel is összekapcsolódnak, hogy erősítsék a szélesenn körű nemzetközi együttműködést a katonai műveletek terén.
- A Többnemzetiségű erők infokommunikációs rendszerei rugalmasa bővíthetők, változtathatók, hogy alkalmazkodjanak a változó katonai igényekhez és technológiai fejlesztésekhez.
- Az infokommunikációs hálózatok működtetéséhez folyamatos, speciális képzést kapnak a többnemzeti erők infokommunikációs szakemberei, hogy hatékonyan használják és védelmezzék a hálózatokat.

A NATO mint muntinacionális katonai erő, a fenti kritériumokat is magában foglaló szabályrendszert alakított ki a tagállamok közös katonai műveleteinek hatékony végrehajtásához. A szabályrendszer természetesen az infokommunikáció részterületeire is kiterjedt. Dolgozatomban elsősorban a szárazföldi erők műveleteit támogató infokommunikációs rendszereket vizsgálom. Terjedelmi okokból nem kívánok kitérni a légierő és légvédelmi csapatok működését támogató infokommunikációs rendszerek vizsgálatára.

A NATO szárazföldi csapatok híradó és informatikai rendszerei kapcsolatának minimális mértékét az 5048. számú „Szabványosítási egyezmény” (STANAG - Standardization Agreement for procedures and systems and equipment components) határozza meg.
A STANAG 5048 (STANAG 5048, 2006) szerint:

- „A szárazföldi parancsnokságok között szükség van a híradó és informatikai rendszerek összekapcsolására a tűztámogatás, a logisztika, csapatlégvédelem, a csapatrepülő és a műszaki támogatás, vezetés, irányítás (C2) támogatás és a felderítés koordinálására.
- Egy a NATO által meghatározott szétbontakozásban a legmagasabb szintű nemzeti vagy többnemzetiségű harcászati parancsnokság, rendszerint a hadtest szint, ellátásra kerül információvédelemmel ellátott kapcsolattal a NATO közös felhasználású Integrált Híradó Rendszeréhez (NICS) beszéd, üzenet és adatinformáció csere céljából. A befogadó ország polgári és katonai hatóságaihoz a feladat végrehajtásához fontos kapcsolatok szintén létesítésre kerülnek.
- A szárazföldi csapatoknak esetenként híradó és informatikai kapcsolatot kell létesíteni, üzemeltetni és fenntartani a NATO haditengerészetével vagy légierejével, a nemzeti területvédelmi erőkkel, melyek nincsenek a NATO alárendeltségében, a nem- NATO erőkkel vagy más kormányzati szervekkel, melyeket jelen STANAG nem részletez. Ezen kapcsolatokat az alkalmanként megkötendő kölcsönös szerződések fogják részletezni
- A parancsnokság összes szintjének képesnek kell lennie az együttműködéshez szükséges információk cseréjére a befogadó ország területvédelmi parancsnokságaival, helyi védelmi erőkkel, más kormányzati szervekkel és nem kormányzati hivatalokkal (képviseletekkel)”

A NATO stacioner infokommunikációs hálózat gyakorlatilag a NATO szövetségi tulajdonában levő hálózati és végponti eszközökből, bérelt szolgáltatásokból és a végpontokhoz kapcsolódó telepíthető eszközökből áll Ezek az infokommunikációs eszközök a NATO különböző szintű parancsnokságait kötik össze.
Mivel a stacioner hálózat elemei földrajzilag kötött helyszíneken vannak telepítve, a Magyar Honvédség katonai műveleteit ezek az eszközök akkor tudják támogatni, ha a művelet NATO parancsnokság alatt kerül végrehajtásra. Természeresen ebben az esetben is szükséges az erők, eszközök, kapacitások számvetése térben és időben a szolgáltatások biztosíthatósága tekintetében

2.1.3 Katonai műholdas rendszerek

A katonai műholdas rendszerek alkalmazhatósága mind a stacioner mind a telepíthető híradás szegmensében az űrtechnológia fejlődésével összhangban folyamatosan növekvő jelentőséggel bírnak. A világűr dinamikus és gyorsan fejlődő terület, amely elengedhetetlen a Szövetség elrettentő és védelmi képességének fenntartásához. 2019-ben a szövetségesek elfogadták a NATO űrpolitikáját, és az űrt a légi, szárazföldi, tengeri és kibertér mellett új hadműveleti területként ismerték el. Ez a politika irányítja a NATO űrrel kapcsolatos megközelítését, és biztosítja a megfelelő űralapú támogatást a Szövetség műveleteihez és küldetéseihez olyan területeken, mint a kommunikáció, a navigáció és a hírszerzés.

Egyre több tevékenység függ a pontos helymeghatározástól. A katonai alkalmazású rakétákat ma már műhold irányítja. Az amerikai drónokat is, mint például a General Atomics MQ-9 Reapert nem csak földi sugárzású rádiójelek, hanem SATCOM műholdkapcsolat is irányít. A hadihajók és szinte minden szárazföldi vagy légi jármű elsődleges helymeghatározási módja a műholdas helymeghatározás egyik, a teljes Bolygót körbeölelő rendszerén (GPS[17]) alapul. A harci manőverek során a kommunikáció és a helymeghatározás valós időben történhet műholdon keresztül.

A műholdakon gyűjtött és továbbított információk kritikus fontosságúak a NATO tevékenységei, műveletei és küldetései számára, beleértve a kollektív védelmet, a válságreagálást és a terrorizmus elleni küzdelmet. A szövetségesek és a NATO a műholdak használatával gyorsabban, hatékonyabban és pontosabban reagálhatnak a válságokra.[18]

A NATO, reagálva elsősorban az Oroszország és Ukrajna közötti fegyveres konfliktus okozta feszültségre, másrészt a Kínai Népköztársaságnak a NATO által veszélyesnek ítélt katonapolitikai tevékenysége ellensúlyozására stratégiai döntéseket hozott:

„A világűr és a kibertér biztonságos használatának és a világűrhöz való korlátlan hozzáférésnek a hatékony elrettentés és védelem a kulcsa.

Fokozni fogjuk a hatékony működésre való képességünket a világűrben és a kibertérben, hogy megelőzzük, felderítsük, ellensúlyozzuk és megválaszoljuk a fenyegetéseket a fenyegetések teljes spektrumában, minden rendelkezésre álló eszközt felhasználva. A rosszindulatú kiberfenyegetések egyszeri vagy fokozódó, halmozott tevékenységi; vagy

[17] GPS - Global Positioning System – Globális helymeghatározó rendszer
[18] forrás: https://www.nato.int/cps/en/natohq/topics_175419.htm letöltés ideje: 2023.05.16

az űrbe, az űrből vagy az űrön belüli ellenséges műveletek; elérhetik a fegyveres támadásnak megfelelő szintjét, és ez arra késztetheti az Észak-atlanti Tanácsot, hogy az Észak-atlanti Szerződés 5. cikkére hivatkozzon.

Elismerjük a nemzetközi jog alkalmazhatóságát, és támogatni fogjuk a felelős magatartást a kibertérben és a világűrben. Fokozni fogjuk továbbá az alábbiak ellenálló képességét az űr- és kiberképességeket, amelyekre kollektív védelmünk és biztonságunk támaszkodik."[19]

Az Űr elengedhetetlen a Szövetség elrettentéséhez és védelméhez. A világűr alátámasztja a NATO azon képességét, hogy navigáljon és nyomon kövesse az erőket, hogy szándékos zavarokkal szemben is állóképes kommunikációval rendelkezzen, észlelje a rakétakilövéseket, és biztosítsa a hatékony vezetést és irányítást. A Föld körül keringő aktív műholdak több mint fele NATO-tagországokhoz vagy területükön alapuló társaságokhoz tartozik.

A NATO-szövetségesek egyre inkább az űrre támaszkodnak különféle nemzetbiztonsági feladatok ellátásában, valamint katonai műveletekben szerte a világon. Az űradatok, termékek és szolgáltatások kritikus fontosságúak, és közvetlenül támogatnak más működési tartományokat. [20]

A NATO STANAG 5048(STANAG 5048, 2006) szerint a harcászati műholdas híradás a következő képpen szervezhető:

„NATO tagállamok területén kívüli telepítéskor, a megfelelő összeköttetés érdekében rendszerint a nemzeti, a többnemzetiségű hadtest vagy az alkalmi harci kötelék részére UHF vagy SHF sávú egycsatornás harcászati műholdas híradás földi (TACSATCOM) végberendezései és szállítható SHF sávú többcsatornás harcászati műholdas híradás földi (TACSATCOM) végberendezései kerülnek biztosításra. Nemzeti UHF/SHF sávú egycsatornás vagy SHF sávú többcsatornás harcászati műholdas híradás földi (TACSATCOM) berendezései alkalmazhatók a nagytávolságú híradó és informatikai összeköttetések létesítésére. A megfelelő hatóságok engedélyével a NATO tulajdonú műhold hozzáférési lehetőség (műhold szegmens) kiutalható nemzeti harcászati műholdas híradás (TACSATCOM) létesítésére az alkalmazott szárazföldi erők részére, az AC/317-D/62-ban leírtak szerint."

A fentiekből számomra az következik. hogy a NATO a tagországok biztonsága érdekében az eddigiek feletti mértékben fokozni kívánja jelenlétét a világűr szegmensben, amely

[19] forrás: https://www.nato.int/cps/en/natohq/opinions_214382.htm?selectedLocale=en
[20] forrás: https://www.nato.int/cps/en/natohq/topics_175419.htm letöltés ideje: 2023.05.22

politika elősegítheti a katonai infokommunikációs rendszerek nemzeti fejlesztésének eddig anyagi erőforrások hiányában mostohán kezelt műholdas kommunkációs elemeinek erősödését.

Bár a NATO nyilvánvalóan elsősorban a szövetség kereteiben végrehajtandó műveletek infokommunikációs hálózatainak a fejlesztéséhez járul hozzá anyagilag, a rendszerek üzemeltetésére kiképzett állomány és a működtetett rendszerek egyes elemei részét képezhetik egy nemzeti műholdas infokommunikációs rendszernek is.

Jelenleg Magyarország tulajdonában nincs katonai alkalmazás céljából felbocsátott műhold. A NATO és a más országok által használt kifejezetten katonai célú műholdak műszaki paraméterei az adott ország vagy szövetség minősített adatai, ezért jelen dolgozatban csak az alkalmazásuk általános elveit mutatom be, technikai részleteket nem áll módomban vizsgálni. Jelen dolgozatban csak a polgári és katonai célra egyaránt igénybe vezető eszközöknek a honvédelem szempontjából fontos megvalósítási lehetőségeit vizsgálom.

A Műholdas kommunikációs rendszerek általános jellemzői:

A műholdak olyan mesterséges holdak, amelyek a Föld vagy más égitestek körül keringenek, és amelyeket meghatározott célokra használnak, többek között kommunikációra, navigációra, távérzékelésre, megfigyelésre és tudományos kutatásokra. A műholdak antennákkal, adókkal és vevőkészülékekkel vannak felszerelve a földi állomásokkal és más műholdakkal való kommunikációhoz. Energiaellátásukat beépített akkumulátorok és napelemek segítségével biztosítják. Mozgásukat a sikeres pályán tartás érdekében rendszeresen korrigálni kell egy földi állomás irányításával és saját hajtómű segítségével.

A kommunikációs műhold egy mesterséges műhold, amely transzponder és rádiótávközlési jelek használatával közvetít és erősít a forrás és a vevő között. A műhold úgy működik, hogy fogadja a Földről küldött rádiójeleket, és visszaküldi a rádiójeleket a Földre. A műhold a napelemek nagy tömbjeiből gyűjtött napenergiát használja, amelyek ellátják a műholdat a működéséhez és a Föld felé továbbításához szükséges összes elektromos energiával, és kis mennyiségű üzemanyagot használnak fel a megfelelő pályán tartásához. A kommunikációs műholdakat ma médiatartalmak sugárzására, internet hálózat bővítésére, kommunikációra, IoT-re, helymaghatározásra, katonai alkalmazásokra használják, a felhasználási lehetőségek folyamatosan bővülnek.[21] Egyik

[21] forrás: https://gsoasatellite.com/topics/the-fundamentals-of-satellite/ letöltés ideje: 2023.05.21.

legismertebb szolgáltató a jól ismert amerikai NAVSTAR GPS -rendszer, melynek vevőberendezései napjainkban szinte minden telefonban, fényképezőgépben, mozgó járműben, egyéb „digitálisan okos” eszközben megtalálható. A globális műholdas navigációs rendszereknek köszönhetően mára már napszaktól és látási viszonyoktól függetlenül, automatizáltan képesek vagyunk saját geolokális pozíciónk nagy pontosságú meghatározására. Ennek a mindennapi életben éppúgy, mint katonai alkalmazások terén nagy hasznát vesszük. Természetesen más országok is követték az USA példáját. Legismertebbek az Orosz Glonass és az európai Galileo.

A műholdas kommunikációs hálózat infrastruktúrális felépítése összetett, a következő elemekből áll:

Műholdak röppálya magassága az alábbiak szerint osztható fel:

- Geostacionárius pálya (GEO - GEostaconary Orbit): 35 786 Km.
  Egy geostacionárius pályán álló műhold rögzített helyzetben van a földi megfigyelő számára. Egy GEO műhold állandó sebességgel kering a Föld körül az Egyenlítő felett naponta egyszer. Mivel a GEO műholdak az Egyenlítő felett helyezkednek el, nincs kontaktus lehetőségük pólusok felett. Ezt a pályát a műholdas képalkotáshoz és telekommunikációs célokra használják. Leggyakoribb típusok, a jelenleg aktív műholdak több, mint a felét kommunikációs műholdak alkotják. A geostacionárius pályán keringő műholdak egyik nagy hátránya, hogy a Földtől való nagy távolságuk a nem teszi lehetővé a mobiltelefonos távközlésben való alkalmazásukat. Ehhez közelebb kell hozni a műholdakat a felhasználóhoz, vagyis alacsony pályára kell őket állítani. Ekkor azonban elveszítjük a geostacionárius holdak nagy előnyét, a geo-szinkron pályát. Az alacsony magasság miatt egy darab műhold kisebb ellátottsági területtel rendelkezik, ezért több, különböző pályasíkon keringő mesterséges holdat kell alkalmazni a Föld teljes területének a lefedéséhez.
- Közepes Föld körüli pálya (MEO – Medium Earth Orbit): 7 000 – 20 000 Km.
  A MEO a Föld körüli térnek az alacsony földi pálya feletti és a geostacionárius pálya alatti területe. Az Északi- és Déli-sarkot lefedő kommunikációs műholdakat is behesorolják a MEO-ba. A MEO műholdak keringési ideje körülbelül 2 és 24 óra között van. Manapság ezeket a műholdakat inkább navigációs rendszerekben használják, mint távközlési célokra. A GPS (Global Positioning System – globális helymeghatározó rendszer) műholdjai például MEO-műholdak. A rendszer műholdas szegmensének célja, hogy a Föld bármely

pontjából, bármely időpillanatban legalább négy mérésre alkalmas műhold legyen látható, amelyet a következő műhold-konfiguráció biztosít: az Egyenlítő síkjával 55 fokos szöget bezáró hat ellipszispályán, pályánként négy műhold kering, 12 sziderikus óra keringési idővel, a Föld felszínétől kb. 20 200 km magasságban. Teljes kiépítésében ez 24 műholdat jelent. A GPS műholdas szegmense folyamatos fejlesztés alatt áll. Az eszközök tervezett és várható élettartama miatt azokat folyamatosan cserélni kell, mely lehetőséget biztosít a fejlesztések implementálására. A rendszer 24 műholddal képes üzemelni, de ennél többet tartanak pályán a redundancia biztosítása okán.

- Alacsony Föld körüli pálya (LEO – Low Earth Orbit): 300–1500 km.
  A LEO műholdak a Földhöz legközelebbi pályán állnak. A közelség gyorsabb forgási periódust eredményez. Az alacsony földpályán lévő műholdak megváltoztatják helyzetüket a földi helyzethez képest. Emiatt a LEO műholdak gyakran egy olyan műholdak csoportjába tartoznak, amelyek összhangban működnek, más néven műhold-konstellációként. Ezt a pályát használja az IRIDIUM műholdas rendszer is. Mivel a műholdak alacsony Föld körüli pályán keringenek. ezért a Földfelszín teljes lefedéséhez 66 darab műholdra van szükség.[22]

A műholdas rendszerek egyszerűsített formában tárgyalva az alább részelemekből állnak:

Űr szergmens:

Maga a műhold illetve műholdak. Költséges és nagy mérnöki feladat az eszközök megfelelő pályára állítása, majd az eszközök saját hajtóműveik segítségével a pályán tartás. Funkciótól függően az elektromágneses spektrum különböző hullámhossztartományában működő adókat, vevőket, érzékelőket, képalkotó rendszereket is elhelyezhetnek rajta. Minden Űreszköznek van úgynevezett kihordási ideje, aminek hosszát a benne működő elektronika és nem utolsó sorban a hajtóműben levő üzemanyag mennyisége határozza meg.

Földi szegmens:

A földi szegmensben találhatóak az űrszegmens irányításáért, az eszközök pályára irányításáért, pályán tartásáért és funkcionális működéséért felelős eszközök. A földi állomások, irányítóközpontok részt vehetnek a jelfogadás és továbbítás folyamatában, de elsődlegesen felügyelik az űrszegmens eszközeinek állapotát és státuszát. Ezen kívül a

[22] forrás: https://gsoasatellite.com/topics/the-fundamentals-of-satellite/ letöltés ideje:2023.05.22.

földi szegmens tartalmazhat egyéb, az elemzéshez szükséges feldolgozó eszközöket is. Az állomások többfélék lehetnek: állandó telephelyű, mozgásban lévő, szállítható állomások, attól függően milyen telepítési mód szükséges az adott feladat végrehajtásához, szolgáltatás nyújtásához.

Elsősorban a műholdak pozícióban tartása a feladatuk. Globális hálózat esetén a bolygó több pontján is telepíteni kell a földi állomásokat, hogy a rendszer valamennyi űreszközéhez hozzáférhessenek. Például a Galileo navigációs rendszer földi szegmense esetén ezek a navigációs rendszer támogatásáért felelős állomások olyan távoli helyeken is felépültek, mint az északi sarkvidéken található Svalbard, vagy a Csendes-óceán déli részén lévő Új-Kaledónia, de még az Antarktisz belsején is üzemel állomás[23]. A vezérlőközpontok által kiszámított pályamódosításokra több ok miatt is szükség van. Egyrészről a Föld (különösen az Egyenlítőnél), a Nap és a Hold gravitációs vonzása miatt, másrészről – ugyan kisebb mértékben, de – a Nap által kibocsátott sugárzás is hatást gyakorol a műholdak pályájára.

Véleményem szerint a műholdas rendszerek működésének egyik legkönnyebben sebezhető pontja a földi kiszolgáló elem. A műholdas eszközök folyamatos vezérlése érdekében viszonylag nagy, legalább több méter átmérőjű parabola antennát kell az állomás közelében felszerelni. A műhold eszközökkel az adatcsere szinte folyamatos kell, hogy legyen. Ezek a tulajdonságok nagyban megkönnyítik a földi kontrollközpont földrajzi helyzetének pontos megállapítását. A polgári kommunikációs műholdrendszerek esetén ezen állomások publikus, mindenki által megismerhető információk. Fegyveres összetűzés esetén ezen állomások állandó védelme folyamatosan nagy erőforrást igényel a légvédelmi és a szárazföldi csapatok részéről egyaránt. Gondoskodni kell az esetleges terrorakció vagy szabotázs lehetőségének minimalizálására is.

Felhasználói szegmens:

A felhasználói szegmens részei azok az eszközök, illetve szolgáltatások a kiszolgáló személyzettel együtt, amelyeket a rendszer végfelhasználói igénybe vesznek a lecsatlakozási ponttól (downlink) egészen a felhasználási pontig. Minden olyan berendezést, hardvert, szoftvert, algoritmust ide sorolunk, amivel képesek vagyunk kapcsolatba lépni az űralapú infrastruktúra olyan elemével, amelyen keresztül elérjük a kívánt szolgáltatást. A felhasználói szegmensbe sorolhatjuk a navigációs eszközöket,

[23] forrás:https://www.sgo-penc.hu/blog/index.php/2018/04/14/a-galileo-navigacios-rendszer-foldi-szegmense/

különböző célú (felderítő elemző, tűzvezető, felderítő, rakétaindítást korai előre jelző, levelezést biztosító stb.) számítógépes rendszereket, telefonokat, mobilokat, és a modern tudományos műszereket. Ehhez a szegmenshez tartoznak azok az alkalmazások is, amelyekkel a többi szegmensből (legfőképp az űrszegmens irányából) kapott információkat elemezzük, feldolgozzuk és értelmezzük. Kommunikációs felhasználás esetén minden műholdas rendszernek több, de legalább kettő felhasználói szegmense van.

Veszélyforrások:

Dolgozatom alaptémája az információbiztonság. Az első fejezetben az információbiztonság alapelvei között nagyon fontos részelemként mutattam be, hogy a minősített adatok kezelésének egyik fontos kritériuma a rendelkezésre állás[24]. Ez a feltétel elsősorban nem kriptográfiai, sokkal inkább technológiai kérdés, mégis, mint a bemutatott alapelvek egyike, nagyon fontos szerepet játszik az infokommunikációs rendszerek biztonságának biztosításában. Amennyiben egy összeköttetés végpontjai között megszűnik az elsődleges kommunikáció, egy jól tervezett és kiépített hálózatban a redundáns, másodlagos kommunikációs csatorna is ugyanolyan védettséget tud biztosítani a rendszerben kezelt adatok védelme érdekében.

Dolgozatomban a veszélyforrások elemzésénél a műholdas kommunikációs rendszerek működése elleni eljárásokat részletesebben vizsgálom, mint a hagyományos kommunikációs (rádió, rádiórelé, mikrohullám, troposzféra) alapú kommunikációs rendszerekkel szembeni fenyegetéseket. Ennek oka az, hogy egyrészt a hagyományos infokommunikációs rendszerek működését megzavaró vagy lehetetlenné tevő eljárásrendekről már számtalan értékes, minden potenciális fenyegetésre kiterjedő publikáció született a műveletek részletes elemzésével, másrészt szándékom szerint kutatásom infokommunikációs szolgáltatási lehetőségeket elemző részei elsődlegesen a műholdas szolgáltatások katonai alkalmazásának lehetőségeit, előnyeit, hátrányait hivatottak vizsgálni.

A világűr egyre zsúfoltabb, a birtoklásáért folyamatos verseny van kialakulóban a különböző nemzetek és multinacionális cégek között. Egyes országok, köztük Oroszország és Kína, az űrellenes technológiák széles skáláját fejlesztették ki és tesztelték. 2007-ben a kínaiak elismerték, hogy ASAT (Anti-SATellite) tesztet hajtottak végre egy saját meteorológiai műholdjuk megsemmisítésével, és több ezer törmelékdarabot hoztak létre, amelyek más űrjárműveket veszélyeztettek.[25] A NATO-

[24] CIA (Confidetality. Integrity, Avialability) alapelv – Bizalmasság, sértetlenség, rendelkezésre állás
[25] forrás: https://www.spacesecurity.info/en/what-are-the-threats-to-space-systems/

szövetségesek elítélték Oroszország 2021. november 15-i, szerintük meggondolatlan és felelőtlen műholdellenes rakétatesztjét is.[26]

Tehát az egyik feltételezhető veszélyforrás az estlegesen potenciálisan szembenálló felek műhold megsemmisítő kapacitása. Egy műhold „lelövése" azonban azonnal detektálható, a támadó fél könnyen beazonosítható és egyértelműen háborús cselekedetnek minősül. A támadó félnek az űrtechnológia alkalmazásának magas szintjén kell állnia, ezt csak megfelelő pénzügyi háttérrel is rendelkező úgynevezett nagyhatalmak képesek megtenni. Ezért ezt az eljárást a valóságban még senki nem alkalmazta.

Véleményem szerint a legnagyobb valós veszélyt a földi és űrszegmens közötti kapcsolatot elektromágnesesen zavaró eszközök jelenthetik.

Az ilyen tevékenység nehezebben detektálható, mivel a műholdas kommunikációban az eszközök számának növekedésével egyre növekvő mértékű szándékolatlan interferencia[27] zavar is felléphet. A műholdak által használt jelek frekvenciája és a Földtől való távolsága függvényében az időjárás is akadályozhatja a kommunikációt. Ezért nem mindig állapítható meg egyértelműen, ha egy rendszer szándékos zavarás alatt áll. A zavarforrás helye sem mindig mérhető be egyértelműen. A kommunikációt zavaró eszközök kifejlesztése, gyártása messze nem igényel akkora anyagi erőforrást, mint egy műholdas rendszer megalkotása vagy kinetikus energiájú fegyverrel való támadása.

A zavaró eszközöket lehet szelektíven alkalmazni, kikapcsolásuk után pedig a műholdas rendszer működése helyreállhat, a rendszer általában fizikailag nem sérül meg. Ezekkel a lehetőségekkel elektronikai hadviselési manővereket lehet tervezni és végrehajtani.

A Secure World Foundation szerint a műholdak zavarása két helyen történhet: az űrben, közvetlenül a műholdak megcélzásával, és a földön, ahol a zavaró jelekkel a vevőket célozhatják meg. Az űrben fellépő interferencia, az úgynevezett uplink zavarás, egy jelet kever az eredeti adásba, ami torzítja a műhold összes felhasználója által kapott információkat. Bart Hendrickx, a programot szorosan nyomon követő kutató szerint a Tobol szinte biztosan így működik.

A földi alapú módszer, az úgynevezett downlink zavarás, ugyanazon a frekvencián továbbítja a jelet, mint a műhold, ami megakadályozza, hogy a csatlakoztatott eszközök megkapják az eredeti jelet. Ennek a módszernek kisebb a hatásósugara, mert a hatékony

[26] forrás: https://www.nato.int/cps/en/natohq/topics_175419.htm letöltés ideje: 2023.05.22

[27] Az interferencia egy fizikai jelenség,akkor következik be, ha két különböző forrású, koherens hullám találkozik, azaz olyan hullámok, amelyek fáziskülönbsége állandó. Ekkor létrejönnek olyan pontok a térben, ahol a hullámok maximálisan erősítik, illetve olyanok, ahol maximálisan gyengítik egymást.

zavarás feltétele, hogy az antenna bemenetén a zavaró jel nagyobb amplitúdójú legyen mint a hasznos jel. Ennek a feltételnek a teljesítéséhez kellően közel kell kerülni a rendszerek antennáihoz, amelyeket meg akar zavarni.[28]

A nem kinetikus fizikai fenyegetések olyan fegyvereket jelentenek, mint a lézerek, a HPM (nagy teljesítményű mikrohullámú) fegyverek és az EMP (elektromágneses impulzus) fegyverek. Ezek olyan fegyverek, amelyek fizikai hatással vannak a célpontjukra, de nem hoznak létre fizikai vele kapcsolatot. Ezek a támadások gyakran fénysebességgel mennek végbe. A legtöbb esetben emberi szemmel láthatatlanok, ezért nagyon nehéz a támadó helyének pontos megállapítása.

A nagy teljesítményű lézerek használhatók az érzékeny műholdelemek, például napelemek megrongálására vagy tönkretételére. A lézerek az érzékeny műholdérzékelők ideiglenes vagy tartós elkápráztatására is használhatók. Egy műholdat a Földről lézerrel megcélozni nem kis feladat, hiszen a lézer áthalad a légköri rétegen. Ehhez nagyon jó minőségű sugárra és fejlett mutatóvezérlésre van szükség, nem beszélve a technológia kifinomultságáról és költségéről.

A támadó számára a műveletei tervezése szempontjából hátrányos, hogy nem lehet biztos benne, hogy a támadása sikeres volt-e vagy sem.

A HPM típusú fegyverrel megzavarható a műhold elektronikája, megrongálható a memóriában tárolt adatok, az operációs rendszerek újraindulhatnak, vagy magasabb teljesítményszinten visszafordíthatatlan károkat okozhatnak az elektronikus áramkörökben és processzorokban.

Az elektromágneses hullámok viszont szétoszlanak és gyengülnek a távolsággal és a légkörön való áthaladással. Ezért célszerű a HPM típusú támadást végrehajtani egy másik, pályán lévő műholdról. Ehhez a támadó félnek is komoly űrtechnológiával kell rendelkeznie.

Egy másik, elsősorban az optikai felderítő műholdakat érintő támadási technika a lézeres precíziós fegyverek alkalmazása. A műhold optikai érzékelőjét a ráirányított lézernyalábbal zavarják vagy „vakítják” meg. Ez a támadás nyilván csak rövid ideig tarthat és a műhold optikai érzékelőjében vagy képfeldolgozó rendszerében visszafordíthatatlan károsodásokat is okozhat. Mivel ez a támadási forma elsősorban nem a kommunikációs műholdak ellen irányul, a továbbiakban nem kívánom vizsgálni.

[28] forrás: https://www.washingtonpost.com/national-security/2023/04/18/discord-leaks-starlink-ukraine/?fbclid=IwAR1YpPUtAHbTu9CWetH41OWmMDlySGS9fjkUVMCewCTuqIK67M4ynh-sxsA letöltés ideje: 2023.05.23.

Kinetikus (hagyományos, fizikai) támadások:

Bár gondolatmenetem elején arra a következtetésre jutottam, hogy a mai fegyveres konfliktusok alkalmával a szembenálló felek, ha anyagi-technikai lehetőségeik megengedik, elsősorban az elektronikai harc (EW – Elektronic Warfare) eszközeivel igyekeznek a másik felet támogató műholdas kommunikációs rendszereket támadni, az események eszkalálódása esetén, a „totális háborúban" előkerülhetnek a teljes fizikai megsemmisítés eszközei is:

A fizikai kinetikus fenyegetések olyan fegyverek, eszközök a működtetésükhöz szükséges személyi és technikai háttérrel együtt, amelyek közvetlenül megkísérelnek csapást mérni vagy robbanófejet felrobbantani egy műhold vagy földi állomás közelében. Ez történhet a földről felbocsátott, folyamatosan emelkedő pályán mozgó ASAT[29]-el, vagy olyan ASAT segítségével, amely keresztezi a célműhold pályáját.

Az orbitális[30] ASAT abban különbözik a közvetlenül a földről emelkedő ASAT-tól, hogy egy orbitális pályán keringő ASAT-ot először pályára kell állítani, majd manőverezni kell, hogy elérje célját. Az ASAT eszközök napokig vagy akár évekig is alvó pályán maradhatnak, mielőtt aktiválnák őket. Az ilyen ASAT-ok fedélzetén található irányítási rendszer viszonylag magas szintű kifinomultságot és technológiát, valamint jelentős tesztelési és telepítési erőforrásokat igényel.

A földi állomások sebezhetőbbek, mint a keringő műholdak. A hagyományos fegyverek, földi támadás különleges erők alkalmazásával, irányított rakéták és nagy hatótávolságú rakéták fenyegetik őket. A földi állomásokat közvetetten is megzavarhatják az elektromos hálózat vagy a kommunikáció elleni támadások.

A földi szegmens elleni támadás véleményem szerinti egyik nem hagyományos módja lehet a nem egyenruhában, vagy „idegen zászlós"[31] műveletek segítségével végrehajtott szabotázs, ahol a támadó fél a félrevezető jelek miatt nem azonosítható egyértelműen. A módszer mondhatni ősrégi, de a jelen kor konfliktusaiban is előfordul, lásd Észak Atlanti áramlat tenger alatti gázvezetékének felrobbantása 2022 szeptember 27 –én.[32]

A kinetikus energiájú, fizikai támadások általában visszafordíthatatlan hatással vannak a célpontjukra. Ezért a támadás szinte azonnal észlelhető és a támadás forrása a földrajzi

[29] ASAT – Anti Satellite – Műhold (ellenes) - romboló

[30] Orbitális – Föld körüli pályán keringő

[31] „Idegen zászlós művelet" – más nemzetiségű iratokkal, felszereléssel akár egyenruhával végrehajtott művelet, a végrehajtó állomány nemzeti hovatartozása meghamisítása céljából.

[32] A vezeték szándékos felrobbantását az illetékes vizsgálóbizottság tényként ismerte el, a cselekményt elrendelő ország eddig publikusan, bizonyítékokkal alátámasztva nem került megnevezésre.

helyzete alapján könnyen beazonosítható lehet. Ha a támadás sikeres, hatása valószínűleg nyilvánosan látható lesz az orbitális törmeléken vagy a sérült földi állomáson keresztül. Mindez a nyílt háború elkerülése érdekében visszatartó erőt jelenthet az ilyen típusú támadások végrehajtásától.

A fizikai támadásokon és Elektronikai hadviselési manővereken kívül, jelenleg folyamatosan növekedő tendenciát mutató támadási forma a műholdas infokommunikációs rendszerek földi elemeit célzó úgynevezett „cybertámadás”

A kibertér NATO által elfogadott fogalmát jelen fejezetben már bemutattam.

A rádiófrekvenciás jelek továbbítását zavaró elektronikus támadásokkal ellentétben a kibertámadások célpontjai maguk az adatok, valamint az adatokat kezelő rendszerek. A műholdantennák, a földi állomások antennái, az állomásokat a földi hálózatokkal összekötő kommunikációs vonalak, a műholdhoz csatlakozó felhasználói terminálok mind potenciális támadási célpontok, és behatolási kísérletek lehetséges alanyai.

A számítógépes támadások segítségével megállapítható, hogy ki kivel kommunikál, lehallgatható a forgalom, vagy sérült adatok és hibásan formázott csomagok juttathatók be a rendszerekbe.

A számítógépes támadásokhoz magas szintű tudásra és a rendszer működésénekszéleskörű megértésére van szükség. Ezek azonban nem feltétlenül igényelnek túl jelentős anyagi erőforrásokat.

Az ilyen típusú kibertámadásokat éppen ezért akár magáncsoportok vagy magánszemélyek is lebonyolíthatják, ami azt jelenti, hogy a saját kiberműveleti (védelmi) képességekkel nem rendelkező állami vagy nem állami szereplő a lehetséges támadók széles skálájának lehet kitéve.

Egy műholdas infokommunikációs rendszer elleni kibertámadás adatvesztést, üzemzavart vagy akár egy műhold végleges elvesztését is okozhatja. Például, ha egy ellenfélnek sikerül átvennie az irányítást egy műhold parancsnoki és vezérlési rendszere felett, a támadó megszakíthat minden kommunikációt, megnövelheti az űreszköz belső energiafogyasztását, ezáltal kimerítheti az elektronika teljes tápellátását, károsíthatja elektronikus berendezéseit és érzékelőit, és végül visszafordíthatatlanul károsíthatja a műholdat.

A kibertámadások elkövetőinek pontos megállapítása nem egyszerű feladat. A támadók általában különféle módszereket alkalmaznak személyazonosságuk elrejtésére, mint például a névtelenséget biztosító szerverek használata. Az ilyen esetek kivizsgálása még állami szervezeteknek sem mindig egyszerű, jogszabály alapján történő felelősség

megállapítása pedig felkészült támadók vagy a támadásban állami szereplők közreműködése esetén pedig szinte lehetetlen.

A katonai kommunikációs műholdak

Olyan mesterséges holdak, amelyeket a katonai szervezetek használnak a műveleteik infokommunikációs támogatására. Ezek a műholdak lehetővé teszik a katonai erők számára, hogy megbízható és biztonságos kommunikációt folytassanak a földi bázisok, repülőgépek, hajók és egyéb katonai egységek között. Használata hadműveleti területen elterjedtté vált járművek és vezetési pontok közötti összeköttetés biztosítására is. (pl. IFTS[33] használata a Szövetséges ISAF[34] erők afganisztáni műveletei során) A legújabb fejlesztéseknek köszönhetően akár egyetlen katona a használatában levő kézi terminállal, „rádióval" közvetlen kapcsolatot teremthet az éppen felette levő műholddal.

A katonai kommunikációs műholdak alkalmazásának főbb területei:

1. Kommunikáció: A műholdak lehetővé teszik a katonai egységek közötti hang- és adatátvitelt, beleértve a szöveges üzeneteket, a képek és videók továbbítását, valamint a parancsok továbbítását és információk megosztását.

2. Helymeghatározás: A műholdak a globális helymeghatározó rendszerek (pl. GPS) segítségével pontos pozícióadatokat szolgáltathatnak a katonai egységeknek, ami elengedhetetlen a navigációhoz, a célpontok meghatározásához és az egységek mozgásának nyomon követéséhez. A célpontok meghatározásánál fontos a célpont mozgásának a sebessége is, mert a rendszer a műholdak földfelszíntől való távolságától függően késleltetéssel továbbítják az információkat. A késleltetés nagy sebességgel mozgó célpont esetén a célmeghatározás sikertelenségéhez is vezethet.

3. Megfigyelés és felderítés: A katonai kommunikációs műholdak képesek a földfelszín folyamatos megfigyelésére és felderítésére. Ez segíti a katonai hírszerzést, a célpontok kiválasztását, az ellenséges tevékenységek figyelemmel kísérését és a stratégiai információk gyűjtését. A műholdak kamerái az emberi szem számára láthatatlan hullámhossz tartományban is képesek felderíteni, ami olyan információk megszerzésére is lehetőséget ad, amelyet más forrásból nem lehetne elérni, pl infravörös tartományban a tárgyak és élőlények hőtérképezése.

4. Vezetés és irányítás: A műholdak lehetővé teszik a döntéshozó parancsnokok és beosztottjaik számára, hogy valós időben nyomon kövessék a hadműveleteket, akár a harcászati mozzanatokat, tájékozódjanak a helyzetükről, és adatokat gyűjtsenek a

[33] IFTS – ISAF Forces Tracking System - ISAF erők nyomonkövető rendszere
[34] ISAF – International Security Assistance Forces – Nemzetközi Béketámogató Erők

döntések meghozatalához. A műholdak segítségével a hadszíntér hadműveleti méretű állapotának, saját és ellenséges erők mozgásának folyamatos megfigyelése és elemzése is lehetővé vált.

Jelen dolgozatomban, témaválasztásom okán a műholdak nyújtotta lehetőségek közül a kommunikációs lehetőségeket, eljárásokat vizsgálom részletesen.

A katonai kommunikációs műholdakat általában a megfelelő anyagi erőforrás rendelkezésre állása esetén a nemzetek saját katonai szervezeteik kezelésükben tartják, és különleges biztonsági intézkedéseket alkalmaznak a védelmük érdekében. Ezek a műholdak általában a polgári technológiához képest magasabb fokú titkosítással, esetenként rejtjelző és anti-interferencia technológiával rendelkeznek, hogy minimalizálják a külső fenyegetéseket és a zavarás lehetőségét. Szövetségi együttműködés keretében számos példa volt rá, hogy például az USA hadereje közös katonai, humanitárius műveletek sikeres végrehajtása érdekében engedélyezte a Magyar Honvédség egyes katonai szervezetei részére műholdkapacitásának az ideiglenes igénybevételét.

A polgári célú, katonai alkalmazásra is igénybe vezető műholdak skálája folyamatosan bővülő tendenciát mutat. Közös jellemzőjük, hogy legalább részben magánvállalkozások, nyereségorientált üzletpolitikával szervezett egységekből állnak. Természetesen az Alkotmányban és törvényekben megfogalmazott honvédelmi érdekből kötelezhetők szolgáltatások nyújtására ennek érvényre juttatása azonban véleményem szerint több akadálya is ütközik:

- Jogszabályból fakadó kötelezettséget általában csak veszélyhelyzet illetve háborús készenlét esetén rónak a jogszabályok a polgári vállalkozásokra. Ez nem vonatkozhat NATO vagy más szerződéses kötelezettségből adódó feladatok vagy békeműveletek infokommunikációs támogatásának biztosítására.
- Külföldi vagy nemzetközi tulajdonú vállalkozás esetén a kötelező szolgáltatások nyújtásának előírására vonatkozó jogszabály nem vagy csak részben érvényesíthető a nem magyar tulajdonosok irányába.
- Honvédelmi alkalmazás esetén, a konfliktus bármely országgal szemben is áll fenn, nem prognosztizálható előre, hogy a külföldi tulajdonosok a konfliktusban érintett melyik féllel szimpatizálnak, ezáltal próbálják azt a felet saját eszközeikkel előnyhöz juttatni szolgáltatásaik nyújtása vagy megtagadása által.

2.2 Telepíthető (Mobilizálható) rendszerek

Jelenleg a szomszédos országban zajló fegyveres konfliktusok hatására a honvédelmi minisztérium és az MH kiemelt figyelmet és támogatást élvez a társadalom irányából. A katonai fejlesztések meggyorsultak, amelyek mindenképpen magukkal kell, hogy hozzák a támogató infokommunikációs rendszerek fejlesztését is.

A Varsói Szerződés megszűnése után a Magyar Honvédséget érintő átalakítások kapcsán nem épült ki a szervezeti és technológiai változásokat lekövető egységes infokommunikációs rendszer. Egyes részterületeket fejlesztettek a többi részterület rovására, részben a forráshiány részben a hosszú távú egységes koncepció hiánya miatt. Véleményem szerint eddig az infokommunikációs hálózat ötletszerű fejlesztésének a nagy vesztese a telepíthető híradás, ezen belül is a rádióhíradás volt.

Személyes véleményem, hogy a Honvédségnél, melynek alaprendeltetésből adódó feladata, hogy a Haza fegyveres védelmét területvédelmi műveletek alkalmazásával a terepen is megvédje, elengedhetetlenül szüksége van egy olyan korszerű rádiókommunikációs hálózatra, mely a NATO és nemzeti kötelezettségek infokommunikációs igényeinek egyaránt képes megfelelni. Jelenleg a honvédelmi tárca infokommunikációs irányitási rendszereinek működését, a kormányzati, illetve a szövetségi (NATO-) rendszerekkel való együttműködést biztosító katonai, infokommunikációs rendszerek létrehozása érdekében egységes infokommunikációs infrastruktúra megvalósítása kezdődött meg. A cél az, hogy az MH jelenlegi állandó telepítésű (stacioner), valamint telepíthető híradó és informatikai rendszerei és eszközei egységes rendszert alkossanak, szolgáltatásaikban, műszaki színvonalukban megfeleljenek a kor követelményeinek, elérjek vagy meghaladják az országos távközlési es a NATO-rendszerek, -szolgáltatások színvonalat.

Ezt a célt megvalósító folyamat az MH infokommunikációs rendszereinek digitális jelfeldolgozási módra való átállása, amelynek fejlesztési irányai a célok mielőbbi elérését szolgáljak. A digitalizáció keretében megvalósuló hálózat alapú infokommunikációs rendszer célja összekapcsolni a különböző vezetési szinteket, a szenzoroktól a legfelső katonai, illetve politikai döntéshozó szintig, a hatást kiváltani képes hadfelszerelésig, továbbá megteremteni az összeköttetést a stacioner, a telepíthető es a mobil katonai hírközlési rendszerek között.(Kovács, é. n.)

A fenti célokkal teljes mértékben egyetértek azzal a kiegészítéssel, hogy néhány egészen speciális szakterületen véleményem szerint marad némi létjogosultsága az analóg

eszközök, elsősorban rádiók használatának. Ez a speciális szakterület a víz alatti és föld alatti műveletek kategóriájának néhány eleme lehet.

A digitális jelfeldolgozás alapján ugyanis a kommunikáció alapvetően két állapotú lehet:

- a vételi helyen megfelelő térerősség esetén a vétel jó minőségben fogható, van összeköttetés;
- a vételi helyen a térerősség nem éri el a digitális előerősítő hatásos működéséhez szükséges szintet, nincs összeköttetés.

Ezzel szemben az analóg rádiók a vételi helyen gyengülő jelből gyengébb minőségű összeköttetést (hangerőt, érthetőséget) produkálnak, és a kommunikáció a térerősség csökkenésével arányosan, fokozatosan gyengül.

Olyan felhasználási helyen, mint például ismeretlen vagy elektromágneses szempontból erősen árnyékoló hatású falú épületbe való behatolás, pincébe menet, víz alá merülés. a fokozatosan gyengülő jel figyelmeztető lehet a végrehajtó állomány részére a kommunikáció megszűnésének a lehetőségére.

Digitális eszközök használata esetén a folyamatosan jó minőségű jel helyett egyik pillanatról a másikra teljesen megszűnik a kommunikáció, ami váratlan eseményként a zajló művelet végrehajtására hirtelen negatív hatással lehet.

A Magyar Honvédség által támasztott követelménynek megfelelően 2016-bankezdődött meg a HUNTACCIS telepíthető C2 vezetési és irányítási szoftverrendszer fejlesztése. A 2019 végén átadott rendszer alkalmazói felkészítették, és a rendszer a Brave Warrior 2020 gyakorlaton sikeres próbahasználaton esett át. Az alkalmazói tapasztalatok, és a felmerült új igények alapján várható a HUNTACCIS-rendszer továbbfejlesztése, magasabb vezetési szintekre történő kiterjesztése.

A Magyar Honvédség feladatait hatékonyan támogató informatikai rendszereknek, eszközöknek, képességeknek egységes rendszerbe kell illeszkedniük, az informatikai rendszerektől az informatikai részegységekig, hardver- és szoftverszinten interoperábilis módon együtt kell tudniuk működni. Ebből következően a HUNTACCIS-rendszer továbbfejlesztésének a vezetést támogató funkciók bővítése mellett előreláthatóan kiemelt feladata lesz a rendszer összekapcsolása a Magyar Honvédség más informatikai rendszereivel, szoftvereivel, beépítése a Zrínyi 2026 honvédelmi és haderőfejlesztési program keretében beszerzett egyes haditechnikai eszközökbe, valamint integrálása a tervezett digitáliskatona-képességgel.(Papp & Munk, 2021)

Az infokommunikációs támogatást biztosító informatikai rendszerek, eszközök együttműködésének alapvető feltétele az *informatikai interoperabilitás,* kölcsönös

képességük az általuk kezelt adatok szándékolt jelentését, értelmezését megőrző, az információcsere-igényeket kielégítő – esetleges átalakítások közbeiktatásával történő – cseréjére. Az interoperabilitás biztosítása abban az esetben jelent problémát, feladatot, ha az integrálandó eszközök, rendszerek között fennáll valamilyen szintű, jellegű eltérés, heterogenitás. A Magyar Honvédség jelenleg telepíthető hírrendszere a fejlesztések térben és időben történő elszigetelődése miatt ugyancsak heterogén. Véleményem szerint jelen pillanatban csak arra van lehetőség, hogy műveletet végrehajtó egységeken belül homogén infokommunikációs rendszert alkalmazzunk, a teljes Magyar Honvédség infokommunikációs rendszere belátható időn belül nem válik homogénné, tekintve, hogy ennek kimunkálására, véghezvitelére szakmai érvekkel alátámasztott koncepció, akarat, egységes terv nincs.

A Magyar Honvédségben jelenleg a telepíthető hírrendszer és a kiépített, stacioner hírrendszer együtt biztosítja a működéshez szükséges és elégséges infokommunikációs támogatást

A Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózata biztosítja a felcsatlakozási pontokat a telepíthető területi és harcászati kommunikációs és információs rendszerek részére, valamint biztosítja a felcsatlakozó telepíthető vezetési pontok közötti összeköttetéseket. A rendszer működtetésének több elvi és gyakorlati megoldása is lehetséges, az egyes alakulatok csatlakozhatnak közvetlenül a stacioner rendszerhez, vagy a telepíthető alaphírhálózaton keresztül. Az alaphírhálózat a hírrendszer alkotórésze, amely egy adott katonai alkalmazási területen egységes terv szerint telepített alaphírközpontokból és az azokat összekötő híradó vonalakból áll, és ezáltal egy vagy több vezetési rendszerben a híradás alapját képezi.

„A telepíthető alaphírhálózat egy általános rendeltetésű kommunikációs hálózat valamennyi katonai szervezet harcvezetésének biztosítására, amely telepíthető alaphírközpontokból és a közöttük kiépített híradó összeköttetésekből áll. Jelenleg a Magyar Honvédségben ennek kiépítéséért az MH 43. Nagysándor József Híradó és Vezetéstámogató Ezred, Híradózászlóalj, Híradószázad, Alaphírközpont szakaszai felelősek. Minden egyes alaphírközpont szakasz telepít egy csomópontot az alaphírhálózaton belül a rendszeresített technikai eszközeivel. Jelenleg négy ilyen szakasz található az ezred szervezetében, melyből következik a telepíthető alaphírhálózat 4 csomópontos felépítése. A csomópontok mindegyikén 3 darab R-1406-os rádiórelé és 1 készlet KHK-12 kisegítő hírközpont kerül alkalmazásra:

Az eszközök jellegéből adódóan kiválóan látszik, hogy a mai Magyar Honvédség telepíthető alaphírhálózata analóg összeköttetések kiszolgálására alkalmas."(Tóth, 2015)

A fenti idézetet Tóth 2015 –ben írt doktori értekezéséből emeltem a dolgozatomba. Sajnos az azóta eltelt évek során csak a katonai szervezetek nevei változtak meg, a telepíthető hírrendszert alkotó eszközpark és az általuk nyújtott szolgáltatások nem fejlődtek. Az évtizedekkel ezelőtt korszerűnek számító vezetéknélküli eszközök a digitális jelek továbbítására egyáltalán nem, vagy csak korlátozásokkal alkalmasak. A jelenkorban a katonai műveletek támogatását hatékonyan biztosító, egyre növekvő adathalmaz feldolgozását megkövetelő rendszerek elemeiként egyáltalán nem alkalmazhatóak. Álláspontom szerint tehát jelenleg a Magyar Honvédség telepíthető, vezeték nélküli infokommunikációs eszközrendszere a katonai műveletek digitális adatfeldolgozó igényeit alapszinten sem képes támogatni. A telepíthető rendszerek működtetése kizárólag a kiépített stacioner, vezetékes infokommunikációs rendszerek nagymértékű igénybevételével biztosíthatók.

Ennek a problémának vizsgálatom szerint két racionálisan megvalósítható megoldása lehet:

1. Korszerű, szélessávú digitális vezetéknélküli jeltovábbító eszközrendszer (digitális relé, mobil mikrohullámú állomás) vásárlása és üzembe helyezése. Ebben az esetben teljesen önálló, zárt kommunikációs csatorna hozható létre. Előnye lehet, hogy saját üzemeltetés esetén a szolgáltatások a katonai alkalmazásokhoz gyorsan és hatékonyan változtathatók, az egyszeri bekerülési költség kifizetése után a rendszer fenntartása viszonylag kevés anyagi erőforrást igényel. Hátránya, hogy folyamatosan megfelelő tudású szakembergárda szükséges az üzemeltetéshez valamint a rendszer technikai amortizációja esetén cseréje újabb nagy anyagi erőforrást igényelhet.

2. Műholdas alapú vezetéknélküli jeltovábbító eszközrendszer vásárlása / bérlése. Vásárlás vagy saját műhold pályára állítása véleményem szerint az ország gazdasági teljesítőképessége alapján a Magyar Honvédség fejlesztésére fordítható anyagi erőforrás szűkössége miatt a közeljövőben nem várható.

Általam összegyűjtött tényezők, melyekkel egy saját műholdas rendszer üzemeltetése esetén szembe kell nézni:

- A műholdak pályára bocsátása bonyolult, drága és nem mindig sikeres feladat. A műholdak mérete és súlya korlátozza a hordozórakéták terhelhetőségét, ami hatással van az új műholdak beindításának sebességére és gyakoriságára.

- A műholdas hálózatok nem mindig képesek elegendően nagy adatátviteli sebességeket biztosítani a földi alapú rendszerekhez képest, az űrszegmens kapacitása utólag nem bővíthető.
- A műholdas kommunikációs rendszerek kiépítése és karbantartása nagy költségekkel jár, ami korlátozhatja az elérhetőségüket és elterjedésüket.
- Rossz időjárási viszonyok esetén a műholdas jelek gyengülhetnek vagy megszakadhatnak, ami átmeneti kapcsolati problémákat eredményezhet.
- A műholdak földi szegmense a felhasználás helyétől távol helyeken is lehet, így a hibák vagy meghibásodások javítása időigényes lehet.
- A műholdas hálózatok nagy területeket fednek le, ezért a hálózati infrastruktúra karbantartása és frissítése is nehezebb feladat lehet.
- Időnként előfordulhatnak jelzésintegritási problémák, interferencia zavarok, amelyek zavarokat okozhatnak a kommunikációban.
- A műholdak távolsága és mozgása miatt a földi terminálok kialakítása és beállítása is bonyolult lehet.
- A műholdaknak korlátozott élettartama van, ezért időnként új műholdakat kell indítani és a régieket ki kell cserélni.

A fenti lehetséges problémák tükrében véleményem szerint jelenleg a legésszerűbb megoldás egy már működő műholdas infokommunikációs rendszer szolgáltatásának a bérlése.

A szolgáltatás bérlése egy költségvetési szerv, mint a Magyar Honvédség részére számos jogszabály által megkötött, komoly bürokratikus eljárás. A szolgáltatások változtatása egy saját rendszer alkalmazásához képest mindenképpen nehézkesebb, esetenként, béke időszakban csak pályázati eljárás útján valósítható meg.

Ezen kívül eszköz vagy csatorna bérlése esetén a rendszer használónak minden esetben bíznia kell a szolgáltató szakmai képességeiben és a jogszabálykövető magatartásának folyamatosságában is.

Óriási előny azonban ebben az esetben, hogy az üzemeltetés nem a katonai szervezetek feladata. A szolgáltatói hálózat méretétől függően, a hagyományos földi kommunikációs rendszerekhez képest gyorsabban kialakítható egy eddig nem használt geolokációs területen (külföldön) végrehajtandó katonai művelet infokommunikációs támogatásának biztosítása.

2.3. A katonai infokommunikációs rendszerek adatkezelésének információbiztonsága

A Katonai célú infokommunikációs hálózatokban kezelt adatokat minden esetben védenünk kell. A védelem kialakításakor mérlegelni szükséges, hogy a rendszer által kezelt adat megsemmisülése, megváltozása, illetéktelen személy tudomására jutása milyen mértékben érinti hátrányosan a rendszert üzemeltető szervezet tevékenységét. Az információk biztonsága érdekében a Magyar Honvédség és a Katonai Nemzetbiztonsági Szolgálat (továbbiakban KNBSZ) közötti együttműködés törvény által előírt kötelezettség. Magyarország honvédelmi érdekeinek védelme és biztosítása, a kapcsolódó szövetségesi kötelezettségek teljesítése, valamint az országvédelem kibertér műveleti erőkkel történő fenntartása és fokozása érdekében a Honvédség és a KNBSZ kibertér műveleti erői közvetlenül együttműködnek egymással. A kibertér műveleti képességek fejlesztését, valamint a kapcsolódó tervezési, biztonsági és szabályozási feladatokat a Honvédség a KNBSZ-től kapott információk felhasználásával és a KNBSZ szakmai támogatásával látja el. Ha a kibertér műveleti képességek fejlesztése, a kapcsolódó tervezési, biztonsági és szabályozási feladatok nemzetbiztonsági vonatkozással bírnak, a végrehajtásukhoz a KNBSZ főigazgatójának egyetértése szükséges.(2021. évi CXL, 2023)

2.3.1 Nem minősített adatok védelmének lehetőségei

A nem minősített adatok védelmét legmagasabb jogszabályi szinten az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény határozza meg. A honvédelmi célú elektronikus információs rendszerek esetében, a fenti törvény szerinti hatósági feladatokat, a biztonsági felügyeletet a honvédelmi ágazaton belül működő, a Kormány által kijelölt szerv kormányrendeletben meghatározottak szerint látja el. Nem minősített adatokat kezelő zárt célú elektronikus információs rendszerekkel kapcsolatos hatósági, biztonsági felügyeleti feladatok ellátására a Kormány a Katonai Nemzetbiztonsági Szolgálat főigazgatóját jelöli ki. A felügyeleti hatósági jogkört a Katonai Nemzetbiztonsági Szolgálat látja el. Ilyen rendszerek többek között a honvédelmi célú közigazgatási döntés-előkészítő és vezetés-irányítási rendszerek és a honvédelmi stacioner és telepíthető, nemzetközi műveleteket, valamint gyakorlatokat támogató műveleti vezetési rendszerek is.(187/2015 Korm. rendelet, 2021)

A jogszabály által előírt biztonsági felügyeleti hatósági jogkör értelmezésem szerint azt jelenti, hogy a hatósági hazai vagy nemzetközi műveleti környezetben, telepíthető

elhelyezési körülmények között telepített nem minősített rádió, rádiórelé, műhold, vezetékes eszközök alkalmazásával létesített infokommunikációs rendszerekre is kiterjed. A hatósági jogkör érvényesítése véleményem szerint műveleti környezetben, elsősorban háborús műveletek tervezése, végrehajtása esetén az infokommunikációs támogatást végrehajtó állomány és a hatóság között részletes előzetes egyeztetést igényel. Műveleti feladatra kijelölt egységnek a művelet infokommunikációs rendszerének tervezése és üzemeltetése során a szolgálati és szakmai elöljárók valamint a felügyeleti Hatóság által támasztott követelményeknek egyaránt meg kell felelnie. Béke körülmények között, napiélet támogatása és kiképzési feladatok végrehajtása során a hatósági ellenőrzési feladatok végrehajthatók. Tapasztalatom szerint az ellenőrzés és feladatszabás szinte kizárólagosan a Magyar Honvédség állandó telepítésű infokommunikációs rendszereit érintik. Kérdés számomra, hogy rádióeszközök alkalmazása esetén a frekvencia, teljesítmény, alkalmazott üzemmód, alkalmazás időtartama, települési hely megválasztása bejelentés szerinti használata, végrehajtása és a rádióforgalmazás szabályainak betartásának ellenőrzése is a KNBSZ feladata és felelőssége vagy sem. Magyarország területén a rádiófrekvenciás kisugárzások szabály szerinti alkalmazásának polgári felügyelője a Nemzeti Média és Hírközlő Hatóság. Nemzetközi környezetben a feladat tovább bonyolódik a nemzetközi szerződések által támasztott követelményekkel valamint a befogadó ország rádiókisugárzással kapcsolatos esetlegesen a mienktől eltérő szabályozásának alkalmazásával is. Véleményem és tapasztalatom szerint csak a nemzeti jogszabályi meghatározások pontosításával, a rádióforgalmazási eljárásrendek alapján kidolgozott cselekvési változatok és felhasználóbarát segédletekkel válhat képessé a KNBSZ hatósága a jogszabályban foglalt kötelmei teljesítésére és ami ennél is fontosabb, válhat rugalmasabbá a katonai műveletek tervezésének infokommunikációs vetülete.

Országon belüli alkalmazás esetén az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény hatálya alá tartozó szervezetek vezetői számára „a szervezet elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályok” rögzítése és az informatikai biztonsági szabályzat kiadása jogszabály alapján előírt kötelezettséggé vált. A szabályzat kiadásának előkészítése az elektronikus információs rendszer védelméért felelős személy, honvédelmi szervezetek esetén az állományilletékes parancsnok feladata.

Ha az elektronikus információs rendszerrel rendelkező szervezetre vagy a szervezeti egységre a 41/2015 BM rendelet előírásai szerint kidolgozott szabályzatokban meghatározott adminisztratív és fizikai védelmi intézkedésektől egy elektronikus információs rendszer esetében a magasabb védelmi igény miatt el kell térni, az eltéréseket az érintett elektronikus információs rendszer e rendelet előírásai szerint kidolgozott szabályzatában kell rögzíteni.

A Magyar Honvédség nyílt infokommunikációs rendszereinek üzemeltetése során irányadó az 53/2022 HM utasítás. Ennek melléklete tartalmazza a rendszerek üzemeltetésével kapcsolatos részletes szabályozást. A dokumentum nyílt forrásból sajnos nem érhető el, de a jogszabály alapján igazodni kell az alábbi felépítéshez:

A 41/2015 BM rendelet *Védelmi intézkedési katalógus*ban az adminisztratív intézkedések között első helyen az IBSZ tartalmára vonatkozó előírások szerepelnek. Eszerint az IBSZ-ben rögzíteni kell:

1. a célokat, a szabályzat tárgyi es személyi (a szervezet jellegétől függően területi) hatályát,
2. az elektronikus információbiztonsággal kapcsolatos szerepköröket, a szerepkörhöz rendelt tevékenységet es a tevékenységhez kapcsolódó felelősséget,

valamint az információbiztonság szervezetrendszerének belső együttműködését,

3. az elektronikus információs rendszer biztonsággal kapcsolatos alábbi területekre, tevékenységekre vonatkozó előírásokat:

- kockázat elemzés (amely szorosan kapcsolódik a biztonsági osztályba es biztonsági szintbe soroláshoz),
- biztonsági helyzet- es esemény értékelés eljárási rendje,
- az elektronikus információs rendszer (ideértve ezek elemeit is) es információ technológiai szolgáltatás beszerzés (ha az érintett szervezet ilyet végez vagy végezhet),
- biztonsággal kapcsolatos tervezes (például beszerzés, fejlesztés, eljárás rendek kialakítása),
- fizikai es környezeti vedelem szabályai, jellemzői,
- az emberi erőforrásokban rejlő veszélyek megakadályozása (például személyzeti felvételi es kilépési eljárás során követendő szabályok, munka végzésre irányuló szerződésben a személyes kötelmek rögzítése, a felelősség érvényesítése stb.),

- az informatikai biztonság tudatosítására irányuló tevékenység es képzés az érintettszervezet összes közszolgálati vagy munka végzésre irányuló egyéb jogviszonyban álló alkalmazottainak, munkavállalóinak, megbízottjainak tekinteteben,
- az érintett szervezetnél alkalmazott elektronikus információs rendszerek biztonsági beállításával kapcsolatos feladatok, elvarasok, jogok (ha az érintett szervezetnél ez értelmezhető),
- üzlet-, ügy- vagy üzemmenet-folytonosság tervezése (igy különösen a rendszer leállás során a kézi eljárásokra történő átállás, visszaállás az elektronikus rendszerre, adatok pótlása stb.),
- az elektronikus információs rendszerek karbantartásának rendje,
- az adat hordozok fizikai es logikai védelmének szabályozása,
- az elektronikus információs rendszerhez való hozzáférés során követendő azonosítási es hitelesítési eljárás, es a hozzáférési szabályok betartásának ellenőrzése,
- ha az érintett szervezetnek erre lehetősége van, a rendszerek használatáról szóló rendszer bejegyzések értékelése, az értékelés eredményétől függő eljárások meghatározása,
- az adatok mentesének, archiválásának rendje,
- a biztonsági események – ideértve az adatok sérülését is – bekövetkeztekor követendő eljárás, ideértve a helyreállítást,
- az elektronikus információs rendszerhez jogosultsággal (vagy jogosultság nélkül fizikailag) hozzáférő, nem az érintett szervezet tagjainak tevékenységet szabályozó (karbantartok, magán- vagy polgári jogi szerződés alapján az érintett szervezet szamara feladatokat végrehajtok), az elektronikus információ biztonságot érintő, szerződéskötés során érvényesítendő követelmények
- szabály rendszer felállítása es alkalmazása a külső elektronikus információs rendszerekhez való kapcsolódáshoz (Nagyné, 2019)

A fenti rendszerek biztonságos üzemeltetéséhez a hatóság Információbiztonsági Szabályzat (továbbiakban EIBSZ) kidolgozását, az abban foglaltak betartását és rendszeres felülvizsgálatát írja elő.

Elektronikus aláírás

A kriptográfia egyik legfontosabb és a mindennapi életben is leggyakrabban alkalmazott terméke a digitális aláírás.

Fokozott biztonságú elektronikus aláírás olyan elektronikus aláírás, amelyik alkalmas az aláíró azonosítására, egyedülállóan az aláíróhoz köthető, olyan eszközökkel hoztak létre, amelyek kizárólag az aláíró befolyása alatt állnak es a dokumentum tartalmához olyan módon kapcsolódik, hogy minden – az aláírás elhelyezését követően a dokumentumban tett – módosítás érzékelhető.(Bérczes & Pethő, 2014)

Tehát a digitális aláírás olyan speciális aláírás, amelyet a személyazonosságot igazoló digitális tanúsítvány hitelesít. A digitális aláírást az elektronikus aláírás biztonságos változatának tekintik, mivel kriptografikus kulcs segítségével van összekapcsolva az aláírt dokumentummal, és az érvényessége ellenőrizhető. Ha megbízható harmadik féltől beszerzett digitális tanúsítványt használ az elektronikus aláíráshoz, az így kapott digitális aláírást gyakorlatilag lehetetlen hamisítani. Emellett megbízhatóan igazolja az aláíró személyazonosságát, valamint azt, hogy az aláírt dokumentumot nem változtatták meg, és hogy az aláírások érvényesek.

Hazánkban 2002 évben fogadta el az Országgyűlés a 2001. évi XXXV. törvényt az elektronikus aláírásról.

Az elektronikus aláírás szolgáltatás működésének lényege az alábbiak szerint foglalható össze.

Ha valaki, általában egy kormányzati vagy kereskedelmi szervezet szeretné, hogy nem védett úton (posta, email) küldött iratait más hivatalok, akár a Bíróság is hivatalosnak és a küldőtől származónak tekintsék, már nem csak a hivatalos pecsétekkel és közjegyzői ellenjegyzéssel tudják ezt megvalósítani.

Minden digitális tanúsítványhoz tartozik egy elektronikus kódpár, vagy más néven kulcspár, amely egy titkos kulcsból és egy nyilvános (publikus) kulcsból áll. A titkos kulcs a digitális tanúsítvány alanyának kizárólagos birtokában van, azzal senki más nem rendelkezik, míg a nyilvános kulcs bárki számára hozzáférhető.

Szükség van egy hitelesítő szervezetre, amely tárolja a nyílt kulcsokat és tanúsítja, hogy a nála tárolt nyílt kulcs melyik szervezethez tartozik. Ez ma már kereskedelmileg beárazott szolgáltatás. Ezek a kulcsok érvényességi idővel rendelkeznek. Lejárat esetén a szolgáltatást meg kell újítani. Ennek elmaradása esetén a hitelesítés a továbbiakban nem történik meg.

A digitális tanúsítványhoz tartozó titkos és nyilvános kulcspár segítségével hozhatunk létre elektronikus aláírást, illetve titkosíthatjuk dokumentumainkat, üzeneteinket. Az ilyen típusú kódolási eljárást nevezzük nyilvános kulcsú kódolási technológiának, míg a technológiához tartozó különböző eljárásrendeket, szervezetek, illetve eszközöket együttesen Nyilvános Kulcsú Infrastruktúrának (PKI – Public Key Infrastructure) nevezzük.

A nyilvános kulcsú kódolási technológia a gyakorlatban a legegyszerűbben úgy magyarázható, hogy ha az aláíró (titkos) kulccsal kódolunk egy dokumentumot, akkor az csak és kizárólag a titkos kulcshoz tartozó nyilvános kulccsal dekódolható. Így ha egy titkos kulccsal kódolt dokumentumot a tanúsítványban szereplő nyilvános kulccsal ellenőrzünk (dekódolunk) akkor biztosak lehetünk abban, hogy az adott dokumentumot a tanúsítványban szereplő személy írta alá.[35]

A Magyar Honvédségnél évtizedes elmaradás pótlására kerül sor, ha végre teljes körűen bevezetésre kerül az elektronikus aláírás szolgáltatás. A projekt több mint tíz évvel ezelőtt kezdődött, de a mai napig nem sikerült Magyar Honvédség szinten alkalmazható szolgáltatássá fejleszteni. Egyik legfontosabb, emberi erőforrást igénylő szervezetét, az aláíráshitelesítő alközpontot sok évvel ezelőtt létrehozták, de sokáig alig volt valós funkciója.

Elemzésem során a PKI technológiának két fontos és hasznos felhasználási lehetőségét találtam a Magyar Honvédség tekintetében:

1. A törvényi előírások szerint a minősített adat készítése esetén a minősítőnek a minősített adat létrejöttéhez a dokumentum első oldalának a tetején a minősítési szintet meghatározva saját kezű aláírásával kell ellátnia.(2009 évi CLV törvény, 2022) Jelenleg ha egy minősítendő dokumentumot a feladat ellátása céljából nem kellene papírra nyomtatni, a minősítési eljárás szabályos lefolytatásához mégis meg kell tenni. A kinyomtatott példányt az arra jogosult személy aláírja, majd a kész minősített dokumentumot szükség esetén szkenner segítségével ismét digitális, „file" formába alakítják át. Ez nyomtatási kapacitást igényel, a nyomtatott dokumentumot kezelni (tárolni, továbbítani) csak az érvényben lévő valamennyi biztonsági rendszabály betartásával szabad, ami további például tárolási kapacitásokat köz le. Ha a minősítő személyek digitális aláírási jogot kapnak és a jogszabály lehetővé

[35] https://www.digitdoc.hu/hatteranyagok/digitalis-hitelesites/hogyan-mukodik letöltés ideje: 2023.06.06.

teszi az irat alaki kellékeinek ilyen formába történő átalakításának a lehetőségét, a minősítési eljárás sokat egyszerűsödne, legalábbis azokban az esetekben, ahol az adatokat csak a minősítési eljárás lefolytatása céljából nyomtatták ki.

A PKI technológia lehetővé teszi, hogy a digitális aláírás szolgáltatás mellett az adatok digitális tárolása vagy továbbítása esetén a készítő személy vagy szervezet privát kulcsával magát az egész dokumentumot titkosítsa. Ez a védelem ugyan nem felel meg a minősített adatok továbbítására előírt elektronikus védelmi intézkedések szintjének, tehát minősített adatokat ilyen módon nem továbbíthatunk, de a Magyar Honvédség működéséhez szükséges nem minősített adatokat, amelyek az adatok több mint 99% át teszik ki, elláthatjuk ezzel a védelemmel.

2.3.2 Minősített adatok védelmének lehetőségei.

A minősített adatok védelmének alapvető szabályait a 2009 évi CLV törvény és az annak alapján, a jogszabályok értelmezését és alkalmazását segítő 90/2010 és 161/2010 kormányrendeletek határozzák meg.

A minősített adat fogalmát jelen dolgozatban a fogalmi meghatározások között jogszabály szerint fentebb már beidéztem. Lényegét tekintve, sok egyéb definíció teljesítése esetén olyan adatot tekintünk minősített adatnak, amelyhez a hozzáférést törvény által meghatározott módon és meghatározott időtartamra korlátozni kell. Az adat feldolgozójának nincs mérlegelési lehetősége az adathoz való hozzáférés engedélyezése vagy az adat tárolása, továbbítása tekintetében. Szigorúan előírt eljárásrendet kell követnie, melynek megsértése törvény alapján üldözendő, vétkes személy beazonosítása esetén minden esetben felelősségre vonást von maga után.

Az elektronikus információs rendszerek biztonsági menedzsmentje című cikkemben megfogalmazottak szerint:

„A Magyar Honvédségnél, mint a védelmi szféra valamennyi területén kiemelt jelentősége van a bizalmasságnak. Egyszerűen fogalmazva egy adat inkább semmisüljön meg, mint hogy illetéktelen személyek birtokába kerüljön.”(Megyeri Lajos, 2018b) Ez így betű szerint nincs a vonatkozó jogszabályokba foglalva, de a katonai alkalmazások gyakorlatában a tervezés és üzemeltetés során is ezt tartjuk szem előtt.

Minősített adatot kezelni csak a Nemzeti Biztonsági Felügyelet[36] (továbbiakban NBF) által kiadott írásos engedély alapján lehet, akkor, ha az állami vagy közfeladat ellátásához nélkülözhetetlen.

A minősített adathoz – törvényben meghatározott kivételekkel – személyi biztonsági tanúsítvánnyal és titoktartási nyilatkozattal rendelkező felhasználó kizárólag a számára kiadott felhasználói engedélyben meghatározott rendelkezési jogosultságokkal férhet hozzá.

Minősített adat az állami és a közfeladatok ellátásának biztosítása érdekében, a közérdekű adatok megismerésének alkotmányos jogából, illetve e jog kizárólag szükséges és arányos mértékű korlátozásával jön létre. A Magyar Honvédségnél keletkező adatokat honvédelmi érdekből lehet minősíteni.

A minősített adatok védelméről szóló törvényt 2009.-ben fogadták el. A védelmi rendszabályok részleteit a 90/2010 és 161/2010 kormányrendeletek tartalmazzák. Kutatásom során tapasztaltam, hogy az Egyesült Államok minősített információi védelméről szóló törvény szintén 2009 évben jelent meg, és a végrehajtási utasítás (Executive Order 13526 of December 29, 2009)[37] is 2009 évben. Az USA és Magyarország a jogszabályok felépítésében és tartalmában egymáshoz nagyon hasonlót alkotott. Egyetlen lényeges, eltérő elemet találtam a minősítési eljárásban: A Magyar jogszabályok csak teljes dokumentumok minősítését teszik lehetővé. Tehát például egy kinyomtatott „titkos" terv valamennyi oldalának valamennyi sora egyformán „titkos" minősítésű a tartalomjegyzéktől a záradékig. Az USA szabályozása lehetővé teszi, hogy egy dokumentumon belül bekezdésenként eltérő legyen a minősítési szint. Az aktuális minősítési szintet a bekezdés elején zárójelbe tett (C, S, CTS) (Confidental-Bizalmas, Secret-titkos, Cosmic Top Secret-szigorúan titkos) betűkkel jelölik. Az egész dokumentumot természetesen olyan védelmi intézkedések alkalmazásával kezelik (tárolják, felhasználják, továbbítják…) amelyek a dokumentumban lévő legmagasabb minősítési szintű adatra vannak előírva. Az adatok feldolgozása során viszont lehetőség van a teljes dokumentumból alacsonyabb minősítési szintű dokumentumba áthelyezni az arra a minősítési szintre minősített bekezdést. Ez a különbség azért is érdekes, mert a

[36] A *Nemzeti Biztonsági Felügyelet* feladata a minősített adat védelmének hatósági felügyelete, a minősített adatok kezelésének hatósági engedélyezése és felügyelete.

[37] https://www.govinfo.gov/content/pkg/FR-2010-01-05/pdf/E9-31418.pdf letöltés ideje: 2023.04.17

NATO minősített adatok kezelése ebben a tekintetben az USA szabályrendszerét követi, azaz bekezdésenként változhat a dokumentum minősítése.Eddigi tapasztalataim alapján véleményem szerint a minősített adatok kezelése során, az oktatás szempontjából mindenképpen hasznos lenne, ha a magyar szabályozási rendszer ebben a tekintetben is megegyezne az USA illetve a NATO szabályozással. Jelenleg ugyanis, ha egy tankönyv vagy szabályzat néhány oldalon tartalmaz szenzitív információkat, amiért az egész dokumentum minősítve van, ez lényegesen megnehezíti a tankönyv további nem minősített információkat tartalmazó oldalainak a megismertetését a hallgatókkal.

Javaslom a 2009 évi CLV törvény fentiekre vonatkozó részének felülvizsgálatát, átdolgozását a minősített adatok egy dokumentumon belüli szétválasztásával az adatok hatékonyabb felhasználhatóságának az érdekében.

A nemzeti minősített adatok minősítési szintjei:

Amennyiben az adat nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele:

a) rendkívül súlyosan károsítja a minősítéssel védhető közérdeket, akkor „Szigorúan titkos!”,

b) súlyosan károsítja a minősítéssel védhető közérdeket, akkor „Titkos!”,

c) károsítja a minősítéssel védhető közérdeket, akkor „Bizalmas!”,

d) hátrányosan érinti a minősítéssel védhető közérdeket, akkor „Korlátozott terjesztésű!” minősítési szintű.

A külföldi illetve szövetségesi rendszerek által alkalmazott minősítési eljárások részben eltérnek a hazai szabályozástól. A külföldi minősített adatot az alábbiak szerint határozza meg a törvény:

Megjelenési formájától függetlenül az Európai Unió valamennyi intézménye és szerve, továbbá az Európai Unió képviseletében eljáró tagállam, a külföldi részes fél vagy nemzetközi szervezet által készített és törvényben kihirdetett nemzetközi szerződés vagy megállapodás alapján átadott olyan adat, amelyhez történő hozzáférést az Európai Unió intézményei és szervei, az Európai Unió képviseletében eljáró tagállam, más állam vagy külföldi részes fél, illetve nemzetközi szervezet minősítés keretében korlátozza.(2009 évi CLV törvény, 2022)

A NATO által használt minősítési szintek és azok nemzeti minősítési szintű megfelelője:

a) COSMIC TOP SECRET – „Szigorúan titkos!”

b) NATO SECRET – „Titkos!”

c) NATO CONFIDENTIAL – „Bizalmas!”

d) NATO RESTRICTED – „Korlátozott terjesztésű!”.

A nemzeti adatok minősítési eljárása során a következő, jogszabályban megfogalmazott alapelveket kell folyamatosan szem előtt tartani:

- ***Szükségesség és arányosság elve**: a közérdekű adat nyilvánosságához fűződő jogot minősítéssel korlátozni csak az e törvényben meghatározott feltételek fennállása esetén, a védelemhez szükséges minősítési szinttel és a feltétlenül szükséges ideig lehet.*

Ezt az elvet alkalmazva csak olyan adatot szabad minősíteni, amelynek nyilvánosságra kerülése sérti a honvédelmi érdeket. A minősített adatnak különböző minősítési, védelmi szintjei lehetnek. Minden adatok csak olyan szintre szabad minősíteni, amely szinthez rendelt biztonsági eljárásrend kellő mértékben védi az adat integritását. Egy gyors elévülésű harcászati adat, például egy harci jármű pillanatnyi helyzete és mozgásának iránya nem védendő olyan mértékben és időtartamig, mint például egy hadműveleti harcálláspont települési helyének koordinátái.

A minősített adatok védelmére érvényességi időt is meg kell állapítanunk a következők szerint:

„Szigorúan titkos!” és „Titkos!” minősítési szintű adat esetén legfeljebb 30 év,

„Bizalmas!” minősítési szintű adat esetén legfeljebb 20 év,

„Korlátozott terjesztésű!” minősítési szintű adat esetén legfeljebb 10 év lehet.

Az adatokat természetesen a maximális érvényességi időnél rövidebb időre is minősíthetünk, amelynek a megállapítása annak az ügyintézőnek a feladata, akinél az adat keletkezik. Az érvényességi idő szükség esetén, annak lejárata előtt tovább hosszabbítható. Az érvényességi időre azért van szükség, hogy elévült, szükségtelen adatokat ne védjünk feleslegesen, nagy anyagi és emberi erőforrás pazarlásával. Minél kisebb a minősített adat mennyisége, annál könnyebb a jogszabály által megszabott feltételek teljesítése.

A jelenlegi szigorú szabályozást megelőzően, 2009 előtt a Magyar Honvédségben a papír alapú minősített adatokat úgynevezett vasirat szekrényben is szabad volt tárolni. Szinte minden irodában volt ilyen szekrény. A 2009. évi CLV törvény alapján kiadott részletszabályozás már csak nagy biztonságú, jogszabályban rögzített biztonsági kategória előírásainak megfelelő tárolókban engedélyezi a papír alapú „Bizalmas” vagy annál magasabb szintű minősített adatok tárolását. A nagy biztonságú speciális tárolók NATO minősített adatok tárolására is alkalmasak de sokkal drágábbak elődieknél.

Tapasztalataim és kutatási eredményeim alapján az a meglátásom, hogy az anyagi erőforrások szűkössége és más irányba történő lekötése miatt a Magyar Honvédség jelenleg sem rendelkezik a minősített adatok biztonságos és jogszabályoknak megfelelő tárolásához szükséges, optimális mennyiségű biztonsági tárolóval. Ezért is fontos a minősítési szinteket és a keletkező minősített anyagok mennyiségét a lehető legalacsonyabb szinten tartani.

- ***Szükséges ismeret elve:*** *minősített adatot csak az ismerhet meg, akinek az állami vagy közfeladata ellátásához feltétlenül szükséges.*

Ezt a NATO terminológiában „Need to know" elvként ismerjük. A minősített adatokhoz való hozzáféréshez jogszabály által előírt különböző, a későbbiekben részletezett személyi biztonsági feltételeknek kell megfelelni. A Need to know elv azt jelenti, hogy ha egy ember (ügyintéző) rendelkezik a legmagasabb minősítési szintű adatok megismeréséhez szükséges valamennyi személyi biztonsági feltétellel, akkor sem jogosult valamennyi minősített adat megismerésére, csak azokra, amelyek ismerete, feldolgozása a saját (közfeladatot ellátó) munkájához szükséges. Egy híradó főnök például nem ismerheti meg a saját szervezete logisztikai főnökének azonos szintre minősített adatait, csak ha az a saját munkája ellátásához szükséges. Annak eldöntése, hogy melyik ügyintéző melyik adathoz, rendszerhez, számítógéphez férhet hozzá, a minősített adatot kezelő szervezetnél kötelezően kinevezett, úgynevezett Biztonsági vezető feladata.

A minősített adatok kezelése során követendő, NATO direktívában rögzített információbiztonsági alapelvek(CM 49):

a. ***Bizalmasság elve****: minősített adat illetéktelen személy számára nem válhat hozzáférhetővé vagy megismerhetővé*
b. ***Sérthetetlenség elve****: a minősített adatot kizárólag az arra jogosult személy módosíthatja vagy semmisítheti meg.*
c. ***Rendelkezésre állás elve****: annak biztosítása, hogy a minősített adat az arra jogosult személy számára szükség szerint elérhető és felhasználható legyen*.

A fenti elvek gyakorlati alkalmazása kutatásom alapján al alábbiakban valósulnak meg:

a. Bizalmasság elve:

Tulajdonképpen ezért kell a minősítési eljárást alkalmazni. A minősített adatokhoz való hozzáférésnek szigorú személyi feltételei vannak.

Minősített adatot csak az a személy használhat fel, akinek ez állami vagy közfeladat ellátása érdekében indokolt, és aki – törvényben meghatározott kivétellel – rendelkezik:

a) érvényes és a felhasználni kívánt adat minősítési szintjének megfelelő személyi biztonsági tanúsítvánnyal. S*zemélyi biztonsági tanúsítvány* az a tanúsítvány, amely érvényességi idejének lejártáig meghatározza, hogy valamely természetes személy milyen legmagasabb minősítési szintű adat felhasználására kaphat felhasználói engedélyt.
b) titoktartási nyilatkozattal: a minősített adatot felhasználó vagy megismerő személy nyilatkozata arról, hogy a minősített adat védelmére vonatkozó szabályokat megismerte, és az őt terhelő titoktartási kötelezettséget tudomásul vette.
c) felhasználói engedéllyel: állami vagy közfeladat végrehajtása érdekében a minősítő, illetve a felhasználói engedély kiadására jogosult vezető által, a minősített adat felhasználására jogosult személy részére írásban adott felhatalmazás, a minősített adattal kapcsolatos egyes rendelkezési jogosultságok meghatározásával.
A „Korlátozott terjesztésű!" minősítési szintű minősített adat állami vagy közfeladat ellátásához szükséges felhasználása esetén a felhasználó titoktartási nyilatkozatot tesz, és felhasználói engedéllyel kell rendelkeznie.
A személyi biztonsági tanúsítvány kiadásához az érintett – a nemzetbiztonsági szolgálatokról szóló törvényben meghatározott – *nemzetbiztonsági* ellenőrzésének (a továbbiakban: *nemzetbiztonsági* ellenőrzés) lefolytatása szükséges. A minősített adat felhasználásához szükséges személyi biztonsági tanúsítvány nem adható ki, illetve a már kiadott tanúsítványt vissza kell vonni, ha a *nemzetbiztonsági* ellenőrzés kockázati tényezőt tár fel. A személyi biztonsági tanúsítvány a *nemzetbiztonsági* ellenőrzésről készült kockázatmentes biztonsági szakvélemény kiállításától számított 5 évig érvényes. (2009 évi CLV törvény, 2022)
Az adat bizalmasságának megőrzése azt jelenti, hogy a minősített adatokat a fenti valamennyi feltételnek megfelelő személyek, úgynevezett titkos ügykezelők tárolják, és csak olyan személyeknek adhatják ki, akik szintén rendelkeznek a szükséges személyi biztonsági feltételekkel. Ha a minősített adat elektronikus rendszerben van tárolva (pl. számítógép háttértárolójában), akkor az elektronikus rendszerhez való hozzáférés jelszavas védelemmel van ellátva és a hozzáférés feltétele a minősített adat fajtájának és szintjének megfelelő személyi biztonsági feltételek teljesítése. További feltétel, hogy a minősített adat kezelője (ügyintéző) a jogszerűen birtokában tartott adatot köteles úgy kezelni, hogy illetéktelen személy az adathoz ne érhessen hozzá.
Mint azt a „Fizikai biztonság" című cikkemben részletesen kifejtettem, „jogszabály szerint az adatfeldolgozás során a minősített adat védelméről az adat megismerésére jogosult személy köteles gondoskodni. Ha például egy arra feljogosított személy a

biztonsági tárolóból napi munkavégzés céljából kivesz egy minősített adatot (papír, merevlemez, pendrive), akkor amíg az adat nem a biztonsági tárolóban van elzárva, az adat fizikai védelméről személyesen kell gondoskodnia."(Megyeri Lajos, 2023)

A minősített adatokat tárolás esetén jogszabály által előírt fizikai biztonsági körülmények között kell tartani. Ez konkrétan erős biztonsági tárolót, meghatározott vastagságú falakat, padlót, födémet, vasrácsot vagy biztonsági üveget, biztonsági ajtót, riasztó és üvegtörés érzékelő rendszert jelent. A fizikai kialakítás részletes szabályait a 90/2010 Kormányrendelet tartalmazza.

A minősített adat felhasználására és tárolására szolgáló helyszín fizikai biztonsági rendszere több egymásra épülő elemből áll. A fizikai biztonság külső elemei a védendő terület határait biztosítják. A fizikai biztonság közbenső elemei észlelik az illetéktelen behatolást és riasztják a reagáló erőt. A fizikai biztonság belső elemei a reagáló erő megérkezéséig késleltetik az illetéktelen behatolót a minősített adatokhoz történő hozzáférésben. Az eljárásrend kidolgozásakor külön gondot kell fordítani a következőkre is.

A „Bizalmas!" vagy ennél magasabb minősítési szintű minősített adat – néhány speciális kivételtől eltekintve, melyeket részben ismertetek – kizárólag I. vagy II. osztályú *biztonsági területen* használható fel és tárolható. Összességében elmondható, hogy béke körülmények között laktanyai elhelyezés esetén a fenti szabály betartása mindig kötelező. A minősített adatot tároló, továbbító, feldolgozó elektronikus eszközöket tehát alapvetően biztonsági területen kell tartani.

A biztonsági területek típusai:

I. osztályú biztonsági területnek minősül minden olyan helyszín, ahol „Bizalmas!" vagy annál magasabb minősítési szintű minősített adatot használnak fel, vagy használnak fel és tárolnak, vagy tárolnak olyan módon, hogy a területre való belépés egyben a minősített adathoz való hozzáférést is jelenti. A terület fizikailag körülhatárolt és védett, valamint a ki- és belépés ellenőrzött. A ki- és belépés csak beléptető rendszeren keresztül és csak azon személyek számára engedélyezhető, akik erre külön felhatalmazással és személyi biztonsági tanúsítvánnyal rendelkeznek. Ez a legmagasabb biztonságú terület. A fizikai körülhatárolás fontos része a beléptetés. Általában chip kártyás beléptető rendszert alkalmaznak. Aki nem rendelkezik megfelelő, belépésre feljogosított kártyával, az csak olyan személy kíséretében léphet a területre, aki rendelkezik a szükséges személyi biztonsági feltételekkel, és aki meggyőződött arról, hogy a belépni szándékozó személy rendelkezik a helységben feldolgozott legmagasabb

minősítési szintű adatok megismeréséhez előírt személyi biztonsági feltételekkel. A személyek belépésének időpontját, belépés célját, kisérő személy nevét nyilvántartásban rögzíteni kell. Rendeltetésszerűen használt biztonsági területre javítás, karbantartás, takarítás céljából is csak olyan személyek léphetnek be, akik a fent leírt személyi biztonsági tanúsítvánnyal rendelkeznek. Ez igen szigorú feltétel, a napi élet zavartalan biztosítása érdekében ilyen biztonsági területet csak akkor alakítsunk ki, ha mindenképpen szükséges, mert a minősített adatokat semmilyen módon nem tudjuk ideiglenesen sem eltakarni. Egy tipikus példa erre a veszprémi sziklában működő, Magyar Honvédség Légi Vezetési Pontja, amelynek egyik helységében a légi helyzetkép folyamatosan a falon látható. A helyzetkép minősített információnak számít, ezért a helység csak rendeltetésszerűen működő I. osztályú biztonsági területként alakítható ki. A szervezetek rejtjelzett kommunikációt biztosító rejtjelző eszközeit általában első osztályú biztonsági területen üzemeltetik, az eszközök folyamatos fizikai védelme biztosításának érdekében.

Ha I. osztályú biztonsági területen alakítjuk ki az infokommunikációs rendszer csomópontját, szervert, rádióadót, digitális elosztó hálózatot, stb. akkor figyelembe kell venni, hogy a karbantartó, javító szakállomány valamennyi tagjának, még a villany és fűtésszerelőnek is a helységben kezelt legmagasabb minősítési szintű adatok megismeréséhez szükséges személyi biztonsági tanúsítvánnyal kell rendelkeznie a biztonsági területre való szabályos belépéshez.

A Magyar Honvédség rendelkezik olyan rádióeszközökkel, amelyek rejtjelző részegységet is tartalmaznak. Ezekkel az eszközökkel szükség esetén minősített adatokat lehet továbbítani rádióhullámok segítségével. Az ilyen eszközöket külön jelöléssel (CCI)[38] látják el, és a NATO tagországok rádióforgalmi rendszerek tervezéséért, üzemeltetéséért felelős szervei a jelzés alapján ezeket az eszközöket különleges fizikai védelemmel, egyénileg kidolgozott adminisztratív eljárásrend betartásával tárolják, szállítják, üzemeltetik. A rejtjeltevékenység hatósági felügyeletét Magyarországon a Nemzeti Biztonsági Felügyelet látja el. Állásfoglalásuk szerint ezek a rádiók jogalkalmazás szempontjából rejtjelző eszköznek tekintendők. Az állásfoglalás alapján ezeket a rádiókat laktanyában csak I. osztályú biztonsági területen tárolhatják. A szállításra, kiadás- visszavételre, üzemeltetésre is szigorú előírások vonatkoznak.

[38] CCI - crypto controlled item – rejtjelző elszámolású eszköz

A rádiók műveletekben való felhasználásakor a szabályozók betartása nagy figyelmet és komoly szervezői tevékenységet igényel. Ha a rádióeszközök rejtjelző részegységét rejtjelkulccsal is feltöltik, a rádió a továbbiakban csak olyan személy részére adható át, aki legalább a rejtjelkulcs minősítési szintjével megegyező személyi biztonsági tanúsítvánnyal rendelkezik. Ez a feltétel nagy odafigyelést kíván a harcászati rádióforgalmi rendszerek tervezése során mert a harcoló szervezeteknél a szervezet méretéhez képest kevés katona rendelkezik bármilyen személyi biztonsági tanúsítvánnyal. Műveleti környezetben, esetleges ellenséges ellentevékenység közben, háborúban a tanúsítvány meglétének és szintjének ellenőrzése nem mindig egyszerű feladat.

A „viszonylag békés", missziós (külszolgálati) környezetben általánosan elterjedt módszer, hogy a katonai ID card[39] színe jelzi a tulajdonosa személyi biztonsági tanúsítványának szintjét. (piros - Nato secret, Sárga – Nato confidental, …) A tanúsítványok meglétének ID card színével történő jelölése véleményem szerint ötletes és békétől eltérő állapotban is gyors, szakszerű ellenőrzést jelenthet, alkalmazását egy egységes értelmezés érdekében szabályrendszerben történő rögzítést követően javaslom. Béke viszonyok között a rádiók szabályos laktanyai tárolásához az eszközök mennyiségének függvényében I. osztályú biztonsági területet vagy területeket kell kialakítani. A kialakítás elsősorban fizikai védelmi rendszabályokban foglalt követelmények teljesítését jelenti.

Fontos követelmény például a terület külső határán 30 cm téglafal vagy azzal egyenértékű falazat, az ablakon 15x15 cm rácsosztású, 1 cm vastagságú, minden ponton hegesztett rács vagy ezzel egyenértékű védelmi képességű biztonsági üveg, a feldolgozandó minősített adat szintjétől függően 5-10-15 perc betörési kísérletnek ellenálló biztonsági ajtó, minden nyílászárónál nyitásérzékelő, üvegtörés érzékelő, füst érzékelő, elektronikus riasztó berendezés mozgásérzékelőkkel. Ezek a minimum követelmények, amelyek teljesítése komoly anyagi erőforrást és kiépítési időt igényel. Véleményem szerint ezek a követelmények túlbiztosítják az eszközök fizikai védelmét, különösen, ha arra gondolunk, hogy ezeket a CCI rádiókat a gyakorlatokon a harctevékenységet gyakorló katonák a hátukon, oldalukon viselik az erdőben, akár hóban, sárban.

II. osztályú biztonsági területnek minősül minden olyan helyszín, ahol „Bizalmas!" vagy annál magasabb minősítési szintű minősített adatot használnak fel,

[39] ID card – Identity card, személyazonossági igazolvány

vagy használnak fel és tárolnak, vagy tárolnak olyan módon, hogy az illetéktelen hozzáférést belső intézkedésekkel meg lehet akadályozni. A terület fizikailag körülhatárolt és védett, valamint a ki- és belépés ellenőrzött és a minősített adatokhoz történő illetéktelen hozzáférés megakadályozása érdekében a *biztonsági területre* csak külön felhatalmazással lehet belépni. Személyi biztonsági tanúsítvánnyal nem rendelkező személy csak kísérettel léphet be.

Véleményem szerint ez a védelmi osztály a működtetés szempontjából a legoptimálisabb. Amennyiben egyéb törvényi előírás miatt nem kötelező az I. osztályú biztonsági terület kiépítése, minősített adat kezeléséhez minden esetben a II. osztályú biztonsági terület használatát javaslom. Kiépítése olcsóbb és gyorsabb, mint az I. osztályú biztonsági terület, üzemeltetés szempontjából pedig döntő különbség, hogy javító, karbantartó, ellenőrző személyek kísérettel a területre beléphetnek, a területen felügyelettel munkát végezhetnek.

Fizikai védelmi szempontból a legkisebb védelmet nyújtó minősített adatkezelés szempontjából releváns fogalom az adminisztratív zóna.

A „Korlátozott terjesztésű!" minősítési szintű minősített adat *biztonsági területen* kívül adminisztratív zónában is felhasználható és az adminisztratív zónán belül zárható irodabútorban, lemezszekrényben is tárolható.

Adminisztratív zónának minősül minden olyan helyszín, ahová a belépés ellenőrzött. A *biztonsági terület* körül adminisztratív zóna is kiépíthető.

Béke időszakban, állandó elhelyezési körletekben ez a zóna általában megegyezik a laktanya területével, határai a külső, védett kerítések. Az ellenőrzött belépés a kapun keresztül valósul meg, ahol élőerős őrzés vagy elektronikus áteresztő pont gondoskodik arról, hogy csak belépésre jogosult személyek léphessenek az objektum területére.

Műveleti körülmények között, amennyiben minősített adat feldolgozása is része a feladatnak, fontos az őrzött terület határának meghatározása. Ezt általában ideiglenes kerítéssel (például Gyoda[40].-val) oldják meg. A kerítés mentén rendszeresen járőrözést is biztosítani kell valamint meg kell szervezni a területre történő beléptetés eljárásrendjét. Mindezeket a tábor, harcálláspont kialakításakor, a biztonsági vezető által előre megszabott intézkedések keretében kell megvalósítani. Ezen intézkedések hiányában a telepíthető körülmények között a minősített információ feldolgozásának fizikai védelme nem biztosított.

[40] GYODA – Gyors telepítésű drótakadály

A minősített adatok felhasználásának a feltételei különbözőek lehetnek telepíthető elhelyezési körülmények között és hadműveleti, akár országhatáron kívüli területeken. A katonai szervezeteknek nagyon fontos, hogy laktanyai elhelyezési körülmények nélkül is képesek legyenek minősített adatok feldolgozására hiszen alaprendeltetésükből adódik, hogy békétől eltérő vagy missziós körülmények között is végre tudják hajtani feladataikat, méghozzá a vonatkozó jogszabályok betartásával. Különleges körülmények között véleményem szerint felértékelődik a minősített adatkezelés folyamata, egyrészt mert várhatóan nagyobb az adatforgalom, másrészt pedig a minősített jelentések, parancsok időbeli, folyamatos, biztonságos továbbítása eldöntheti egy harcfeladat teljesítésének sikerességét vagy kudarcát is. Az elvégzett kutatások és szakmai tapasztalataim alapján meglátásom szerint a kiképzési tervekben nem fordítanak kellő figyelmet a minősített adatok telepíthető körülmények közötti kezelésének gyakorlására. Ez a tevékenység plusz emberi erőforrást köt le a gyakorlatokon, de a gyakorlás során felszínre kerülnek az esetleges problémák, megoldandó részfeladatok valamint a minősített adat előállításában, tárolásában, továbbításában a kidolgozó állomány tapasztalatokra tehet szert.

A vonatkozó kormányrendelet szerint a katonai, nemzetbiztonsági, bűnügyi, létesítménybiztosítási és személyvédelmi műveletekben a személyi biztonsági tanúsítvánnyal rendelkező személy személyes felügyelete alatt álló, minősített adatot tartalmazó technikai eszköz, valamint a művelet végrehajtásához szükséges minősített adat, a minősített adatot kezelő szerv vezetője vagy a biztonsági vezető által meghatározott biztonsági intézkedések betartása mellett biztonsági területen kívül is felhasználható. (90/2010 Kormányrendelet, 2010) Nagyon fontos, hogy a minősített adatot kezelő szerv vezetője még békeállapotban készüljön fel a műveleti minősített infokommunikációs rendszer üzemeltetésére, a működtetés személyi, tárgyi és adminisztratív feltételeinek laktanyán kívüli biztosítására.

b. Sérthetetlenség elve*: a minősített adatot kizárólag az arra jogosult személy módosíthatja vagy semmisítheti meg.*

Az alapelv alapján papíralapú minősített adatok esetén szigorú adminisztratív eljárásrend alapján lehet a minősített adatokat – papírokat – megsemmisíteni. Általános alapelv, hogy az előző évben az ügyintézők által feleslegesnek ítélt minősített adatokat összegyűjtve bizottság közreműködésével, jegyzőkönyvezve semmisítik meg. A több példányban, más szervezeteknél meglévő példányok összegyűjtésére vagy a más szervezeteknél történő megsemmisítésére külön intézkednek.

A megsemmisítésről minden esetben megsemmisítési jegyzőkönyv készül. A jegyzőkönyv tartalmazza a megsemmisítésre kerülő többes példánysorszámú adathordozón szereplő minősített adatok azonosításához szükséges adatokat (iktatószám, minősítési szint, terjedelem, példánysorszám), valamint a megsemmisítés tényét, módját és dátumát, a megsemmisítésnél jelen lévők és a megsemmisítést engedélyező vezető aláírását.

Elektronikusan tárolt minősített adat esetén a megsemmisítést törlésnek nevezzük. Az adatok adathordozóról való törlésének szigorú szabályai vannak:

A törlésről minden esetben törlési jegyzőkönyv készül. A jegyzőkönyv tartalmazza a törlésre kerülő minősített adatok azonosításához a nyilvántartási számot, a minősítési szintet, – ha az adathordozóból megállapítható – a terjedelmet, a példánysorszámot, valamint a törlés módját és dátumát, a törlést engedélyező vezető és a törlést végző aláírását. A törlést a biztonsági vezető által a minősített adatot kezelő szerv állományából kijelölt, a törlendő minősített adatra érvényes felhasználói engedéllyel és személyi biztonsági tanúsítvánnyal rendelkező személy végezheti.(90/2010 Kormányrendelet, 2010)

A fenti szigorú szabályozásnak a Magyar honvédség műveleti, külszolgálati körülmények között úgy tud megfelelni, hogy a megsemmisítéseket lehetőleg elkerülik. Természetesen létezik egy, a háborús körülmények esetén alkalmazható, úgynevezett vészhelyzeti megsemmisítés. Ebben az esetben az a cél, hogy minősített adat semmiképpen ne kerülhessen illetéktelen, ellenség kezébe. A vészhelyzeti terv elkészítése és annak rendszeres begyakorlása minden minősített adatot kezelő szerv feladata, különös tekintettel veszélyes műveletek végrehajtása esetén. A vészhelyzeti tevékenységet szabályozó intézkedések és az ezek alapján elkészült tervek is minősítettek. A témában ezért jelen dolgozatom nyílt státuszából adódóan további elemzéseket nem folytatok.

A minősített adat adathordozón akkor kezelhető, ha a tényleges használatba vétel előtt az adathordozó nyilvántartásba került. A minősített adatot elektronikus rendszeren kezelő szerv az adathordozón feltünteti az azon tárolható legmagasabb minősítési szintű adat minősítési szintjét, valamint a nyilvántartási számot.

A minősített adatot tartalmazó adathordozón, (merevlemez, pendrive, ssd együtt digitális adathordozón), törlést erre a célra fejlesztett és a minősített adat kezelésért felelős hatóság által engedélyezett programmal szabad végrehajtani.

A teljesség igénye nélkül kiragadott példaként bemutatom egy NATO által használt, minősített adatok digitális megsemmisítésére engedélyezett törlő szoftverrel szemben támasztott követelményrendszer megoldását:

Blancoo3 Data cleaner 4.8(HMG)[41]

A HMG megtisztítja az összes adatot a merevlemeztől a NATO SECRET szintig. A szoftver asztali laptopokhoz, valamint RAID rendszerekkel rendelkező szerver környezetekhez készült. Bármilyen méretű ATA/IDE/SCSI/USB/SATA/Fibre Channel és FireWire lemezről felülírja az adatokat. Ezenkívül a szoftver törli a merevlemez összes rejtett/zárolt területét, és az újraleképezett szektorokat.

A továbbfejlesztett merevlemez-támogatás garantálja számítógépenként 4 HDD egyidejű nagy sebességű törlését. A szoftver különböző adathordozókon keresztül szállítható a célszámítógépre: hálózati floppy CD USB és előtelepítés.

A Blancco 4.8 HMG által törölt adatok semmilyen meglévő technológiával nem állíthatók vissza. A merevlemez(ek) megtisztítása után a szoftver automatikusan létrehoz egy részletes törlési jelentést a Hardver Asset Management információival, amely megfelel és meghaladja a kormányzati szabályozási követelményeket.

A teljes törlési folyamat digitálisan védett MD5 védelemmel és egy teljes ellenőrző modullal, amely megerősíti, hogy az adatok biztonságosan és teljes mértékben törlésre kerültek a merevlemezről. Az adattörlési és hardvereszköz-kezelési jelentést digitális aláírás is védi a jelentések manipulálásának megakadályozása érdekében. A Blancco 4.8 HMG mind az alacsonyabb, mind a magasabb felülírási szabványok szerint engedélyezett.

Bár a program engedélyezett NATO secret szintig adatok törlésére, a jelenlegi hazai szabályozás ennél szigorúbb feltételeket szab. A Nemzeti Biztonsági Felügyelet Elektronikus Biztonsági Követelménye (EBK., 2021) a következőket határozza meg.

A törlést végrehajtó szoftverek minősített adat törlése esetén csak meghatározott ideig lehet érvényes. Az adatvisszaállító eljárások fejlődése miatt időszakonként meg kell vizsgálni, hogy az eljárás még mindig biztonságos törlést eredményez vagy sem. Az adathordozókat életciklusuk végén ki kell vonni a használatból. A „Korlátozott terjesztésű!" és a „Bizalmas!" minősítési szintű adatot tartalmazó adathordozót – annak érdekében, hogy a rajta tárolt minősített adat ne legyen helyreállítható – biztonságos adattörlési eljárást alkalmazó szoftverrel kell törölni. „Korlátozott terjesztésű!"

[41] Forrás: https://www.ia.nato.int/niapc/Product/Blancco---Data-Cleaner-version-4.8--HMG-_181 Letöltés:2023.04.03.

minősítési szintű adathordozót háromszoros, „Bizalmas!” minősítési szintű adathordozót hétszeres törlési-felülírási metódussal kell törölni. Az SSD meghajtókat ATA Secure Erase eljárással kell törölni. A biztonságos eljárással törölt adathordozó újra felhasználható.

Tehát a „Bizalmas!” és a „Korlátozott terjesztésű!” minősítési szintű adatot tartalmazó adathordozón feltüntetett minősítési szint alacsonyabb szintre megváltoztatható vagy megszüntethető, ha az azon tárolt minősített adat a jelenleg érvényes szabályok szerint legalább hétszeres illetve háromszoros felülírási eljárással kell törölni, így az információ a későbbiekben nem állítható vissza. A „Titkos!” és a „Szigorúan titkos!” minősítési szintű adatot tartalmazó adathordozón feltüntetett minősítési szint nem változtatható meg alacsonyabb minősítési szintre.(161/2010. Kormányrendelet, 2020)

Az olyan adathordozó, amelyet nem lehet engedélyezett módon újra felhasználni, alacsonyabb minősítési szintű jelzéssel ellátni vagy a minősítési jelzését megszüntetni, vagy amely a működőképességét elvesztette, a feltüntetett minősítési szintjének megfelelő engedélyezett eljárásokkal megsemmisíthető. A minősített adatot elektronikus rendszeren kezelő szerv az adathordozót – annak megsemmisítéséig – a feltüntetett minősítési szintnek megfelelően kezeli.

Tehát jogszabály alapján a „titkos” vagy „szigorúan titkos” minősítési jelöléssel ellátott adathordozók esetében törlési eljárástól függetlenül az adathordozót csak a minősítési szintnek megfelelő biztonsági tárolóban tárolják vagy fizikailag megsemmisítik.

A mágneses technológián alapuló adathordozókat erős mágneses tér segítségével, úgynevezett „degausser”[42]-el is meg lehet semmisíteni. A kereskedelemben forgalmazott degausserek olyan speciális, szigetelt és irodai környezetben használható berendezések, amelyek megfelelően erős mágneses mezőt generálnak ahhoz, hogy a behelyezett merevlemezen vagy más mágneses adathordozón tárolt adatokat véglegesen és helyreállíthatatlan módon megsemmisítsék az adathordozó mágneses felületének újrarendezésével. Egy degaussing ciklus jellemzően 5-20 másodpercig tart, ennyi idő szükséges az adathordozó felületének teljes átrendezéséhez. A degaussing tehát nem csupán megbízható, de rendkívül gyors eljárást is jelent, így vállalati környezetben és katonai alkalmazásra is hatékonyan használható. Telepíthető, mobil minősített adatkezelő rendszerek alkalmazása esetén egy degausser fontos része lehet egy vészhelyzeti megsemmisítési eljárásrendnek. A berendezések megbízhatóságát jelezheti

[42] Degauss – angol szó, jelentése: demagnetizál

egy független külső minősítés, egyes típusok például NSA/CSS minősítéssel is rendelkeznek. (Az NSA – National Security Agency). A mágnesezés végleges megsemmisítést jelent a merevlemezek esetében, mivel a bootoláshoz szükséges gyártói fájlok is törlődnek, valamint sérülhet az elektronika. A Magyar Honvédségnél ezen eszközök használata véleményem szerint indokolatlanul kihasználatlan. Alkalmazásukkal elsősorban műveleti területen fokozni lehet a műveleti biztonságot azáltal, hogy a megsemmisítési eljárás meggyorsításával és egyszerűsítésével csökkentjük a katonai adatok illetéktelen megismerésének a lehetőségét.

A nem mágneses technológiát használó adathordozók csak darabolással vagy erőteljes roncsolással semmisíthetők meg. SSD meghajtókat, mobiltelefonokat, USB kulcsokat és memóriakártyákat az adattárolásra használt alkatrészek apró mérete miatt csak apró részekre történő bontással vagy más speciális fizikai eljárással semmisíthetünk meg. SSD meghajtók megsemmisítésére alkalmas berendezések mind az SSD meghajtókat, mind a mobiltelefonokat, USB kulcsokat és memóriakártyákat képesek megbízhatóan megsemmisíteni.[43]

A minősített adat módosítása papír alapú adathordozók esetén lapok cseréjét jelentheti, amit természetesen azok az ügyintézők vagy azok helyettesítői végezhetnek, akik az módosítandó minősített adatot készítették.

A minősített adat módosítása elektronikusan tárolt adat esetében az adat általában a készítő személy által elérhető tárhelyen tárolódik és az ügyintéző csak a megfelelő felhasználó név/jelszó ismeretében férhet hozzá. A minősített adatokat elektronikusan kezelő rendszer jelszóházirendjét úgy kell kialakítani, hogy a fenti szabály érvényre jusson.

Természetesen a minősített adat módosítását minden esetben adminisztratív eljárásrend betartásával rögzíteni kell.

c. ***Rendelkezésre állás elve: annak biztosítása, hogy a minősített adat az arra jogosult személy számára szükség szerint elérhető és felhasználható legyen.***(2009 évi CLV törvény, 2022)

Papíralapú adathordozók esetén a rendelkezésre állás azt jelenti, hogy a 90/2009 Kormányrendeletben foglalt követelményeket úgy kell teljesíteni, hogy az ügyintézők a biztonsági tárolóból a minősített adatot át tudják venni és legyen az adatfeldolgozásra kijelölt, jogszabályban foglaltaknak eleget tevő helyszín.

[43] https://degausser.hu/gyakran-ismetelt-kerdesek/ Letöltés ideje:2023.04.05.

A rendelkezésre állással kapcsolatos feladatrendszerre az elektronikusan tárolt adatok estében az alapfogalmak ismertetésénél már részletesen kitértem.

Minősítés szükségessége:

Olyan információk előállítása, tárolása, továbbítása, amelyeket nem kívántak mindenki számára megismerhetően kezelni, amelyeket a legkülönbözőbb módszerekkel próbáltak elrejteni, védeni az illetéktelen szemektől, az emberiség harcaival egyidősek.

A Magyar államnak, mint a világ többi államának is vannak olyan adatai, információi, amelyek illetéktelen kezekbe kerülése, nyilvánosságra hozatala sérti az állam érdekeit, amelyek a következők lehetnek.

Magyarország:

- szuverenitása, területi integritása,
- alkotmányos rendje,
- honvédelmi, nemzetbiztonsági, bűnüldözési és bűnmegelőzési tevékenysége,
- igazságszolgáltatási, központi pénzügyi, gazdasági tevékenysége,
- külügyi vagy nemzetközi kapcsolatai,
- állami szerve illetéktelen külső befolyástól mentes, zavartalan működésének biztosítása.

Minősített adatot kezelni csak a Nemzeti Biztonsági Felügyelet által kiadott engedély alapján lehet akkor, ha az állami vagy közfeladat ellátásához nélkülözhetetlen.

A Magyar Honvédség a minősített adatok kezelését az ország honvédelmi tevékenységének keretein belül valósítja meg. Minősített adat létrehozására, minősítésre a honvédelemért felelős miniszternek van törvényben biztosított felhatalmazása.

A honvédelemért felelős miniszter a honvédelmi, a minősített adat védelmének szakmai felügyeletével kapcsolatos minősítési jogkörét belső szabályzatban az alárendeltségébe tartozó, vezetői megbízással rendelkező, illetve vezetői beosztásba kinevezett más személyre írásban átruházhatja. Ez a gyakorlatban azt jelenti, hogy általában az állományilletékes parancsnokok és helyetteseik jogosultak minősítési eljárás alapján „titkos” szintig adatok minősítésére.

Az adatoknak, így a minősítetteknek is számos megjelenési formája lehetséges. Jelen dolgozatomban a Magyar Honvédségnél kezelt adatok jellemző megjelenési formái alapján a minősített adatokat három nagy kategóriára osztom fel.

Papír alapú minősített adatok:

A papír alapú adattárolás az egyik legősibb információ tárolási eljárás. Dolgozatomban az egyéb eljárásokkal (bőrre, fára, állati felfújt hólyagra, stb) írással rögzített adatokat nem vizsgálom.

A történelmi háttértől most eltekintve, jelenleg a Magyar Honvédségben a papír alapú adattárolás lényege az, hogy az információt teljesen nyílt, olvasható módon rögzítik a papíron és az elkészült iratot, harcparancsot, jelentést, stb. védik fizikai védelmi eljárásokkal, személyzettel, adminisztratív eljárásrend kidolgozásával és betartásával.

A minősített adat kezelése során mindig egyértelműen felismerhetőnek kell lennie az adat minősített jellegének. A nemzeti minősített adat hordozóján vagy – ha arra nincs lehetőség – külön kísérőlapon fel kell tüntetni a minősítési szintet, az érvényességi időt, a minősítő nevét és beosztását (a továbbiakban együtt: minősítési jelölés).(2009 évi CLV törvény, 2022)

A papír alapú minősített adatok előállításának egyik legnagyobb nehézsége az a követelmény, amely szerint minősített adat kizárólag olyan rendszeren kezelhető, amely rendelkezik az NBF által kiadott, legalább a kezelni kívánt minősített adat minősítési szintjével megegyező szintű rendszerengedéllyel.(161/2010. Kormányrendelet, 2020)

A jogszabályban foglaltak szerint tehát azokat a számítógépeket, amelyeken a minősített adatot készítjük és azután kinyomtatjuk, hatósági eljárásrendben foglaltak szerint akkreditálni kell. A katonai szervezetnél levő asztali és laptop számítógépek közül csak azokon állítható elő minősített adat, amelyek rendelkeznek az NBF által kiadott rendszerengedéllyel.

A rendszerengedély jogszabályokban meghatározott fizikai, személyi, adminisztratív és elektronikus biztonsági követelmény teljesítése esetén adható ki, amelyeket a minősített adat elektronikus tárolásának vizsgálatánál fejtem ki részletesen.

Ha a követelményeknek megfelelő módon sikerült a minősített adatot kinyomtatni, akkor a továbbiakban folyamatosan védeni kell a bizalmasságát. Ez a gyakorlatban azt jelenti, hogy a minősített papír alapú adathordozókat jogszabályban foglalt, kategóriákba sorolt fizikai védelmi képességű biztonsági tárolóban tárolják. A nagy biztonságú tárolók minimum 300-400 kg súlyúak. Laktanyai elhelyezési körülmények között alkalmazásuk nehézség nélkül megoldható de hadműveleti körülmények között alkalmazásuk a szállítás nehézségei miatt speciális logisztikai igényeket támaszt.

A jelenlegi szabályozás szerint a papírokon a minősített adat nyílt, olvasható, látható formában kerül rögzítésre. Megkülönböztetése a nyílt adatokhoz képest annyi, hogy a

minősített adatok védelméről szóló törvényben foglalt irat alaki kellékeit kötelező alkalmazni, például a minősített adat minden oldalán alul és felül fel kell tüntetni a minősítés jellegét (nemzeti/NATO) és szintjét (korlátozott terjesztésű, bizalmas, titkos, szigorúan titkos).

A papír alapú minősített adatok szállítására hagyományos védelmi eljárásrendet alkalmaznak. A papírokat állami vagy eseti futár szállítja átlagos védőképességű táskában, általában önálló fuvarként szervezett gépjárműben. Az illetéktelen hozzáférést személyekkel szemben fegyver alkalmazásával hivatott a jogszabály védeni. Rendészeti, rendőri ellenőrzés esetén a nyílt parancs alkalmazásával biztosítható, hogy illetéktelen személy ne ismerhesse meg a szállított minősített adatokat. A papír alapú minősített adat tehát amikor nincs biztonsági tárolóba zárva, akkor jogszabály által előírt módon csomagolva fegyveres futárral szállítható egyik helyről (adminisztratív zónából) egy másikba. Béke időszakban ez a megoldás általánosan használt, alacsony kockázatú módszer.

Hadműveleti körülmények között, békétől eltérő állapotban viszont a fenti eljárás nagy kockázatúvá válik egyrészt az utak járhatóságának bizonytalansága, másrészt a szembenálló felek esetleges ellentevékenysége (tüzérségi tűz, futár elfogása, …) miatt. A technikai fejlettség jelentlegi szintje véleményem szerint lehetővé teszi a papír alapú minősített adatok elektronikus továbbítását (Fax) vagy kizárólag elektronikus alapú minősített adat tárolást, továbbítást, akár a legkisebb alegységek (raj, szakasz) szintjén is.

<u>Hang alapú minősített adatok</u>:

Értelmezésem szerint a hang alapú minősített adatok definiálása jogszabályi szinten azonosítható módon nem valósul meg. Papír alapú és digitális file formában létező, vagyis olvasható vagy egyértelműen beazonosítható adatok esetében a minősítési eljárás alapján, a minősített adat alaki kellékeit alkalmazva egyértelmű a kezelt adatok fajtája és minősítési szintje. Olyan szabályozás is létezik, amely egy bizonyos adatfajtára előre meghatározza a minősítési szintet. Például a telepített radar állomások által előállított és a légi vezetési szintekre továbbított adatokra általános érvénnyel előre megszabták a minősítés szintet. Véleményem szerint a hang alapú kommunikációt nem lehet vagy legalábbis nem könnyű klasszikus módon a minősített adatok közé besorolni. Ha egy parancsnok telefonon vagy rádión beszél egy másik parancsnokkal, a beszélgetés során elhangzó információ minősítési szintjét a MAV törvény szerint csak akkor lehet egyértelműen besorolni, ha a beszélő felek egy már minősített adatot (papírt, képernyőképet,…) olvasnak fel hangosan. Ez nem túl életszerű. Amennyiben

hadműveleti helyzetet, logisztikai igényt, szállítást, táboráthelyezést, stb. egyeztetnek, akkor az elhangzó információk, adatok jogszabály szerinti minősítési szintjét szerintem nem lehet egyértelműen meghatározni. Jelenleg az infokommunikációs rendszerek tervezésekor a hadműveleti tisztek döntik el, melyik vezetési szintet milyen mértékben tartanak szükségesnek védeni, vagyis milyen minősítési szintű adat továbbításra van szükség. Nyilvánvaló, hogy a lövészraj belső rádióhálójában elhangzó információk nyilvánosságra kerülése, ellenség tudomására jutása esetén nem okozna akkora kárt mint például a dandárparancsnok és az elöljáró hadászati –hadműveleti vezető közötti eszmecsere. Tapasztalatom és kutatásaim alapján kijelenthetem, hogy a vezetési szintek és a közöttük létesítendő rádiókapcsolat védelmi szintjére vonatkozóan nincs egységes, kötelezően betartandó szabályozás.

Továbbiakban áttérek a hang alapú kommunikáció technikai megvalósítására.

A hang alapú minősített adattovábbítás értelmezésem szerint két további altípusra bontható:

- Telefonos kommunikáció:

  Parancsnokok egymás közötti közvetlen kommunikációjának biztosítására szolgál. Elsősorban rövid, bizalmas jelentések, beszámolók megtételére, egyszerű parancsok fogadására alkalmas. Egy jellemző, még rendszerben levő, de már sokat bizonyított eszköz: A TCE 500/B egy asztali telefon formátumú rejtjelzőeszköz biztonságos hang- és adatátvitelhez.

  Végpontok közötti titkosítást biztosító kommunikációt biztosít a felhasználók között bármilyen típusú telefonhálózaton. Használata engedélyezett „Titkos” szintű kommunikációig.

  Minden TCE 500/B rendelkezik egy használható helyi adatinterfésszel faxkészülékek, PC-k és egyéb digitális interfésszel rendelkező terminálok csatlakoztatásához.

  Az adatkommunikáció akár 14 400 bit/s adatátviteli sebességgel valósul meg, és lehetőség van hang- és adatcserére egyidejűleg.(*TCE 500B*, é. n.) Előnye, hogy szinte bármilyen típusú kommunikációs csatornán képes működni. Hátránya a viszonylag alacsony átviteli sebesség.

  A jelenlegi fejlesztések inkább a VOIP[44] technológia felé tolódnak. A technológia célja két vagy több ember között valós idejű, élő beszéd- vagy videókapcsolat

[44] VOIP- Voice Over Internet Protokol

nyújtása. Példaként említhető civil szférában a Skype vagy Viber nevű applikáció. Jelenleg a Honvédség legfelsőbb vezetői állománya nagy hangsúlyt fektet a videokonferencia rendszer alkalmazására. Sajnos többnyire nyílt, nem minősített kommunikációs eszközrendszer felhasználásával. A VOIP rendszer megvalósítása egy már üzemelő, minősített adat feldolgozására akkreditált hálózat esetén a hálózat minősítési szintjével megegyező szintű információcserét tesz lehetővé. Véleményem szerint ez már a jelen, további fejlesztések, engedélyeztetések után pedig a Honvédség jövőbeli minősített beszéd (voice) kommunikációjának technológiája.

- Rádiókommunikáció:

  A katonai rádiókommunikáció szinte egyidős a rádió feltalálásával. Alapvetően az amplitúdó modulált (AM)[45] jelekkel kezdődött a vezeték nélküli beszédátvitel. Egyszerű felépítés, kis sávszélesség, gyenge hangminőség jellemezte. Ezt követte a frekvencia modulált (FM)[46] technológia feltalálása. A hangminőség sokat javult, de már nagyobb sávszélességre volt szükség a használatához. Katonai szempontból nagy változást hozott az úgynevezett frekvencia ugrásos (Hopping) rádiókommunikáció kidolgozása. A frekvenciaugrásos szórt spektrumú rádió adás-vétel egy olyan módszer, amelyben a rádióhullámok felváltva használnak több csatornát elosztva a frekvenciasávon az adó és a vevő által ismert álvéletlen szekvenciával. A frekvencia váltási időtartam a lassútól (100 ugrás/sec) a gyors (akár 4000 ugrás/sec) felé tartva egyre nagyobb kihívást jelent a kommunikációt lefogni, megzavarni vagy lehallgatni szándékozó ellenséges szándékú erőknek.

  Információbiztonsági szempontból már a szórt spektrumú ferkvenciaugrásos adás/vételi mód is nyújt biztonságot, mert hagyományos technikai eszközökkel ez a kommunikáció már nem hallgatható le és igen nehezen zavarható. Ennek ellenére a minősített adatok biztonságáért felelős NATO és nemzeti hatóságok, így Magyarországon a Nemzeti Biztonsági Felügyelet is csak olyan rádióadóvevő eszközökkel engedélyezi minősített adat továbbítását, amelyik eszköz rendelkezik rejtjelző részegységgel. A részegység vizsgálata alapján a hatóság írásos engedélyt ad ki arról, hogy a rádióeszközön keresztül milyen minősítési szintű adatokat szabad továbbítani.

[45] AM Adott frekvenciájú jel amplitúdóját változtatják a beszédinformáció függvényében.
[46] FM Adott sávon

2.4.Nemzeti és NATO adatok minősítési eljárásrendje .

A minősített adatok minősítési eljárásrendjét alapvetően a 2009 évi CLV törvény szabályozza.

A nemzeti minősített adatok kezelésére vonatkozó részletes szabályozását a 2.3.2 fejezetben részletesen kifejtettem. A törvény érintőlegesen a NATO minősített adatok, mint külföldi minősített adatok kezelésére is intézkedik.

külföldi minősített adat:

„megjelenési formájától függetlenül az Európai Unió valamennyi intézménye és szerve, továbbá az Európai Unióképviseletében eljáró tagállam, a külföldi részes fél vagy nemzetközi szervezet által készített és törvényben kihirdetett nemzetköziszerződés vagy megállapodás alapján átadott olyan adat, amelyhez történő hozzáférést az Európai Unió intézményei és szervei, az Európai Unió képviseletében eljáró tagállam, más állam vagy külföldi részes fél, illetve nemzetközi szervezet minősítés keretében korlátozza”. (2009 évi CLV törvény, 2022)

A fogalmi meghatározásnál a nemzetközi szervezetek között a NATO külön nem kerül említésre, szemben az EU.-val. A törvény a NATO-val kapcsolatban egyértelműen csak a minősítési szinteket állapítja meg. A következő, összetett módon megfogalmazott bekezdés szerint külföldi minősített adat lehet például a következő is:

„Magyar Honvédség nemzetközi műveletei és gyakorlatai keretében keletkezett, illetve felhasznált olyan adat, amelyhez történő hozzáférést a műveletben résztvevő felek – a művelet vagy gyakorlat követelményei szerinti minősítéssel – korlátozzák, attól függetlenül, hogy a részes felek által képviselt államokkal Magyarországnak van-e a ba) alpontban foglaltaknak megfelelő megállapodása a minősített adat védelmére és cseréjére, és a minősített adat kezelésére vonatkozó rendelkezéseket a Magyar Honvédség, illetve a műveletet vagy a gyakorlatot irányító más részes fél határozza meg. Nemzetközi gyakorlat vagy művelet esetén tehát vagy van egy a műveletben részt vevők között a művelet vagy gyakorlat során keletkezett minősített adatok kezelésére vonatkozólag nemzetközi egyezmény, vagy a művelet szervezéséért felelős nemzet információbiztonság jogi hátteréért felelős szakembereknek kell azt meghatározni és valamennyi részt vevővel elfogadtatni.”(2009 évi CLV törvény, 2022)

A fenti jogszabályok alkalmazására nagyon jó példa a nemzetközi erők Afganisztáni tevékenysége során alkalmazott eljárásrend. Afganisztánban olyan koalíciós erők

tevékenykedtek közösen, amelyek nem mindegyike volt NATO tag (például Oroszország)

A tevékenység közös elnevezése „ISAF”[47] lett. A műveletek során ISAF minősített adatok keletkeztek, melyek kezelésében a részt vevő feleknek külön szerződésben kellett egyetértenie.

Létezett olyan adatkezelési kategória is, amelyben meglévő szervezet bizonyos, meghatározott minősített adatát engedélyezték az ISAF erők tagjainak adatkezelésre. pl ”NATO Confidental relase to ISAF” minősítési jelöléssel.

Ez azt jelentette, hogy az ilyen jelöléssel ellátott adatokat egyéb jogszabályi megfelelőségek teljesítése esetén, amennyiben a feladat ellátásához nélkülözhetetlen volt, át lehetett adni az ISAF műveletekben részt vevő, de nem NATO tagországok tagjainak is.

A fenti jogszabályokat és értelmezésüket azért fejtettem ki részletesen, mert véleményem szerint a NATO minősített adatok kezelésének szabályait nemzetközi szinten meghatározó jogi háttér egy sok tapasztalaton alapuló, műveletek végrehajtását rugalmasan támogató rendszer. A nemzeti minősített adatok kezelése néhány lényeges pontban, véleményem szerint katonai feladatok ellátása esetén hátrányára, eltér a NATO szabályozástól.

Minősített adat létrehozása:

Nemzeti minősített adat létrehozása csak a 2009 évi CLV törvény korábban részletesen tárgyalt szabályai szerint lehetséges. A szabályozás egyik leglényegesebb eleme, hogy adat minősítésére csak arra feljogosított személyek jogosultak A jogosult személyek köre szűk. Béke időszakban laktanyai elhelyezési körülmények között elegendő lehet azonban műveletek végrehajtása során az egységek alegységekké tagolódása esetén nem minden települési helyre vagy harcálláspontra jut olyan személy, aki jogosult az adat minősítésére.

Tehát egy kisebb önálló alegység akár hazai akár külföldi alkalmazás esetén jogszabályi előírások miatt önállóan nem képes egy adat minősítésére, ezáltal az adat kezelésével kapcsolatos fizikai, személyi, adminisztratív és elektronikus információvédelmi szabályok érvényesítésére sem.

NATO minősített adat létrehozásának folyamatát a 2009 évi CLV törvény nem szabályozza részletesen.

[47] ISAF – International Security Assistant Forces – Nemzetközi biztonsági segítségnyújtó erők.

A NATO minősített adatok kezelésére vonatkozó, a NATO valamennyi tagországában egyaránt érvényes általános szabályozó, a C-M(2002)49[48] és a részterületekre, végrehajtásra vonatkozó AC/35-D direktívák. A szabályozókat a NATO minősített adatok biztonságáért felelős szervei rendszeresen frissítik, a változásokról a tagországokat rendszeresen tájékoztatják. Ezen jogszabályok előírják a NATO minősített adatok kezelésével kapcsolatos, a tagországokban egységesen értelmezendő védelmi intézkedéseket a személyi, fizikai, adminisztratív és elektronikus információvédelem szempontjából. Nem adnak egységes iránymutatást a minősített adat keletkezésére és a minősítési eljárásra vonatkozóan.

Személyes tapasztalatom és kutatásaim alapján kijelentem, hogy a NATO minősített adatok keletkezésével és a minősítési eljárás rendjével, minősítő személyével kapcsolatban nemhogy a tagországok nem egységesek, de még a Magyar Honvédségen belül is az egymástól eltérő jogszabályértelmezések alapján különböző „napi gyakorlat" létezik.

A NATO műveletek kapcsán keletkező minősített adatokkal kapcsolatos személyes tapasztalatom, hogy a NATO minősített adatokat elektronikusan kezelő rendszerekben (NIAR, BICES[49],…) minden felhasználó, rendfokozatra és beosztásra való tekintet nélkül képes létrehozni NATO minősített elektronikus adatot.

Ezen eljárásrend alkalmazása a nemzeti minősített adatokra nagyban megnövelné a kikülönített alegységek adatok továbbításának védelméhez alkalmazható eljárásrendjének lehetőségeit. Lehetővé válhat például, hogy egy éjszakai ügyeletben szolgálatot teljesítő altiszt önállóan küldhessen nemzeti minősített jelentést védett informatikai rendszeren keresztül a szolgálati elöljárójának, az adminisztrációs eljárással járó késlekedés nélkül.

Fentiek alapján javaslom a nemzeti minősített adatok létrehozásával és továbbításával kapcsolatos szabályozás módosítását olyan módon, hogy önálló alkalmazás esetén alegységek állománya is minősítő személye nélkül hozhasson létre egy zárt informatikai rendszerben minősített elektronikus adatot. A vonatkozó szabályrendszer kidolgozáshoz

[48] This document is the result of a major and comprehensive review of the NATO Security Policy and its supporting directives, as approved by the Security Committee. - Ez a dokumentum a NATO Biztonságpolitikája és az azt támogató irányelvek fő elemei átfogó felülvizsgálatának eredménye, a NATO Biztonsági Tanács által jóváhagyott módon.

[49] NIAR- NATO Iroda Automatizálási Rendszer, BICES- Battlefield Information Collecting and Exploitation System

véleményem szerint mindenképpen létre kell hozni egy elméleti ismeretekkel és gyakorlati tapasztalatokkal rendelkező szakcsoportot. Kiemelten fontos a korábbi nemzeti és NATO katonai műveletek , gyakorlatok minősített adatkezelésre vonatkozó tapasztalatainak a feldolgozása.

2.4.1.Új adatvédelmi osztály szükségessége röviden és részletesen.

Magyarországon jelenleg az adatokat információbiztonsági szempontból két csoportra bonthatjuk.

Az egyik csoport a nyílt információk halmaza. Ebből áll a Honvédség adatállományának több mint 99 százaléka. Ezeket az adatokat tovább kategorizálhatjuk publikus és nem nyilvános kategóriára. A publikus adatok mindenki számára megismerhetőek, mint például a toborzó irodák által a katonának jelentkező személyeknek átadott információ a leendő munkájukról. A nem nyilvános adatok a Honvédség működése során keletkező olyan adatok, amelyeket nem szükséges minősítéssel védeni. Ezen adatok élveznek bizonyos mértékben, jogszabály által meghatározott védelmet.

Az általam feltárt egyik probléma itt az, hogy a nem nyilvános adatokat nem védhetjük minősített adatok védelmére szolgáló (rejtjelző) eszközökkel, ezt a Magyar Honvédség rejtjelszabályzata tiltja. Sajnos az erre vonatkozó szabályt nem idézhetem itt, mert a teljes rejtjelszabályzat minősített adat.

Ha egy adatot az elektronikus továbbítás során a felfedés, lehallgatás, megváltoztatás elleni védelem elemeként rejtjelzéssel szeretnénk védeni, azt az adatot jelenleg előtte minősíteni kell.

A probléma másik eleme pedig a minősített adatok védelméről szóló törvény és Kormányrendeletek szigorú előírásai.

Ha a műveleti területen két harcjármű vagy kisebb gyalogos katonai egység, járőr kommunikál egymással az őket közvetlenül irányító harcállásponttal, jelen szabályok szerint a továbbított adatokat kezelhetjük nyílt adatként vagy minősített adatként, az adatgazda döntése alapján. Ha a továbbítandó adatok nyílt kategóriába tartoznak, a rendszert **nyíltként** kezeljük, nem alkalmazunk rejtjelző eszközöket. A rendszer tervezését, működtetését nem kötik a merev jogszabályok, viszont sérülékeny, lehallgatható, a továbbított adatok harmadik fél által módosíthatók. Ezek a veszélyek különösen fennállhatnak ha a műveleteket az országhatárhoz közel kell végrehajtani, ahol akár a kisebb teljesítményű (kézi)rádiók rádióhullámai is a szomszédos ország általunk

nem ellenőrzött területét is elérhetik. A Honvédségnek pedig valós katonai műveleteket nagy arányban éppen a határaink mellett kell végrehajtania.

Másik lehetőség, hogy az infokommunikációs rendszeren továbbított adatokat minősítettként kezeljük, **minősítjük.** A rendszer jogszabályi előírások alapján, kötelezően rejtjelző eszközökkel védetté, biztonságossá válik. De a jogszabály megköveteli a minősített adatok védelmével kapcsolatos személyi, fizikai, adminisztratív feltételek maradéktalan teljesítését is, beleértve a rendszernek a Nemzeti Biztonsági Felügyelet előzetes hatósági engedélyeztetési eljárás lefolytatását is. Ennek a lebonyolítása sok éves személyes tapasztalatom alapján szinte esélytelen. Amint az információvédelemért felelős szakember tájékoztatja a döntésre jogosult elöljárót arról, hogy a minősített adatok kezelése milyen kiegészítő intézkedéseket és védelmi rendszabályokat igényel, a döntésre jogosult elöljárók eddigi tapasztalatom alapján mindig úgy döntöttek, hogy az alakulat által a művelet során kezelni kívánt adatok nem minősítettek.

(Természetesen léteznek speciális, kikülönített, pl. NATO kötelékbe ideiglenesen felajánlott alegységek, amelyek belső kommunikációs rendszereit részben minősíteni kellett, de ezek éves előzetes felkészülést, egyeztetést igényeltek és a jogszabályi feltételeknek való folyamatos megfelelés nagy odafigyelést és erőfeszítést igényel a rendszer működéséért felelős személyektől. Ez véleményem szerint váratlan feladat elrendelése esetén azonnal kialakított hadrendi elemek esetén nem releváns.)

Az általam javasolt új adatvédelmi osztály lényege a következő.

A Magyar Honvédség belső szabályozóban, csak saját hatáskörben létrehozza az adatkategóriát. Az ilyen adatot jól látható módon, akár a minősített adatok alaki kellékeinek megfelelően meg kell különböztetni pl. ”Műveleti információ” jelöléssel. A szabályozóban meg kell határozni, hogy ki jogosult az adat kategorizálásra. Itt lehetőség van a minősített adatokkal szemben, hogy kikülönített csoport parancsnoka, ügyeleti szolgálat vezetője tehát a műveletben folyamatosan részt vevő személy besorolhassa az adatot. A szabályozóban meg kell határozni, ki ismerheti meg ezeket az adatokat. Itt, szemben a minősített adatokkal, ahol nemzetbiztonsági szolgálat szakvéleménye alapján adható engedély, lehet egy adott műveletben részt vevő alegység teljes állománya.

Meg kell határozni a fizikai védelmi rendszabályokat, amelyeket a művelet jellegének megfelelően, de nem feltétlenül a vonatkozó kormányrendelet betűi szerint kell kialakítani.

Egyik legfontosabb változás a jelenlegi helyzethez képest, hogy ezek az adatok továbbíthatók rejtjelző eszközök alkalmazásával. A rejtjelző eszközökben használt rejtjelkulcsoknak ebben az esetben nem kell minősítettnek lenniük. Előzetes kockázatelemzés és rejtjelbiztonsági ellenőrzés alapján lehetségesnek tartom azt is, hogy gyors elévülésű információk kezelésekor, mint például mozgó járművek, járőrök jelenlegi helyzete, a jelenleg használt Harris rádiók saját, beépített kódgenerátorával előállított kulcs használata is elegendő lehet.

Ezek a változtatások lehetővé teszik a műveletet végrehajtó állomány számára, hogy információvédelmi intézkedéseket foganatosítsanak a megvalósíthatóság szintjén, elősegítve ezzel az eddig kényszerűségből nyílt módban kezelt műveleti adatok védelmét. Ezek az adatok elsősorban harcászati, végrehajtói szinten keletkező adatok, nem helyettesíthetik a meglévő vagy tervezett, minősített adatokat kezelő infokommunikációs rendszereket. Érkezett vagy meglevő minősített adatok tárolására, továbbítására nem lehetnek feljogosítva. A minősített adatok kezelésére feljogosított rendszerek általában magasabb szintű harcálláspontok részelemei, ahol megfelelő eszközrendszer szakembergárda és idő áll rendelkezésre a jogszabályok által meghatározott védelmi intézkedések folyamatos biztosítására. A harcászati szintű elemek ebből csak egy-egy végponti munkaállomást, rádiót üzemeltetnek, amely feladat végrehajtható számukra.

Elgondolásom szerint a rejtjelkulcsot igénylő fenti feladatokat a meglévő, egységekben, alegységekben rendszeresített rejtjelző szakállomány bázisán, szükség esetén létszámukban bővítve a legcélszerűbb végrehajtani.

2.5.Összefoglalás, következtetések:

- Jelen fejezetben értelmeztem a Nemzeti stacioner rendszerek elemeit: A Magyar Honvédség Műveleti Vezetési Rendszert, A MH Kormányzati Célú Elkülönült Hírközlő Hálózatot, Honvédelmi Katasztrófavédelmi Rendszert, a NATO stacioner hírhálózat szervezésének, üzemeltetésének alapjait.
- Megvizsgáltam a katonai műholdas rendszerek működtetésének szervezési és technológiai alapjait. különös tekintettel a szembenálló felek műholdak működését zavaró, megszakító vagy megsemmisítő lehetőségeire.
- Elemeztem a Magyar Honvédségben jelenleg telepíthető hírrendszer és a kiépített, stacioner hírrendszer működtetésének alapjait.
- Az infokommunikációs rendszerek szolgáltatásai, biztonsága, telepíthetősége és üzemeltetése összehasonlítása alapján javaslatot tettem a jövőbeli felhasználás

optimális irányára: véleményem szerint jelenleg a legésszerűbb megoldás egy már működő műholdas infokommunikációs rendszer szolgáltatásának a bérlése.

- Vizsgáltam a katonai műveletekkel összefüggésben keletkező, nem minősített adatok védelmének jelenlegi jogszabályi hátterét. Értelmeztem a jogszabályok lehetséges alkalmazhatóságát telepíthető infokommunikációs eszközök alkalmazása esetén. Véleményem és tapasztalatom szerint csak a nemzeti jogszabályi meghatározások pontosításával, a rádióforgalmazási eljárásrendek alapján kidolgozott cselekvési változatok és felhasználóbarát segédletekkel válhat képessé a KNBSZ hatósága a jogszabályban foglalt kötelmei teljesítésére és ami ennél is fontosabb, válhat rugalmasabbá a katonai műveletek tervezésének infokommunikációs vetülete.
- Elemeztem a PKI (Nyílt kulcsú infrastruktúra) alkalmazásának lehetőségeit a Magyar Honvédségnél. A PKI technológia lehetővé teszi, hogy a digitális aláírás szolgáltatás mellett az adatok digitális tárolása vagy továbbítása esetén a készítő személy vagy szervezet privát kulcsával magát az egész dokumentumot titkosítsa. Ez a védelem ugyan nem felel meg a minősített adatok továbbítására előírt elektronikus védelmi intézkedések szintjének, tehát minősített adatokat ilyen módon nem továbbíthatunk, de a Magyar Honvédség működéséhez szükséges nem minősített adatokat, amelyek az adatok több mint 99% át teszik ki, hatékonyan, további anyagi erőforrások lekötése nélkül védhetnénk ezzel az eljárásrenddel.
- Összehasonlító elemzést végeztem a nemzeti illetve NATO minősített adatok védelméről szóló jogszabályok azonos és eltérő szabályairól, jogértelmezéséről. Nemzeti minősített adat létrehozása csak a 2009 évi CLV törvény korábban részletesen tárgyalt szabályai szerint lehetséges. A szabályozás egyik leglényegesebb eleme, hogy adat minősítésére csak arra feljogosított személyek jogosultak A jogosult személyek köre szűk. Béke időszakban laktanyai elhelyezési körülmények között elegendő lehet azonban műveletek végrehajtása során az egységek alegységekké tagolódása esetén nem minden települési helyre vagy harcálláspontra jut olyan személy, aki jogosult az adat minősítésére.
- A személyi biztonsági tanúsítványok meglétének ID card színével történő jelölése véleményem szerint ötletes és békétől eltérő állapotban is gyors, szakszerű ellenőrzést jelenthet, alkalmazását egy egységes értelmezés érdekében

szabályrendszerben történő rögzítést követően javaslom. Az elvégzett kutatások és szakmai tapasztalataim alapján meglátásom szerint a kiképzési tervekben nem fordítanak kellő figyelmet a minősített adatok telepíthető körülmények közötti kezelésének gyakorlására, ami során pedig felszínre kerülnek az esetleges problémák, megoldandó részfeladatok valamint a minősített adat előállításában, tárolásában, továbbításában a kidolgozó állomány tapasztalatokra tehet szert.

- Javasoltam egy sok területen már használt de a Magyar Honvédségnél még nem elterjedt technikai eszköz alkalmazásának széleskörű bevezetését. A Degausserek megfelelően erős mágneses mezőt generálnak ahhoz, hogy a behelyezett merevlemezen vagy más mágneses adathordozón tárolt adatokat véglegesen és helyreállíthatatlan módon megsemmisítsék az adathordozó mágneses felületének újra rendezésével. Alkalmazásukkal elsősorban műveleti területen fokozni lehet a műveleti biztonságot azáltal, hogy a megsemmisítési eljárás meggyorsításával és egyszerűsítésével csökkentjük a katonai adatok illetéktelen megismerésének a lehetőségét.
- Értelmeztem a minősített adatok kezelésére vonatkozó jogi szabályozást, amelyben megállapítottam, hogy a hang alapú minősített adatok definiálása jogszabályi szinten azonosítható módon nem valósul meg. Javaslatom szerint a jogi szabályozás kialakítása mellett technikailag az a legegyszerűbb és használható eljárásrend, ha a külföldi katonai műveletek adatforgalmát hang kommunikáció továbbítása esetén is minden esetben rejtjelző eszközök alkalmazásával valósítjuk meg.
- Összehasonlítottam a NATO és nemzeti minősített adatok keletkezésével, minősítési eljárás rendjével kapcsolatos logi szabályozást és a szabályozás napi gyakorlati végrehajtását. Személyes tapasztalatom és kutatásaim alapján kijelentem, hogy a NATO minősített adatok keletkezésével és a minősítési eljárás rendjével, minősítő személyével kapcsolatban nemhogy a tagországok nem egységesek, de még a Magyar Honvédségen belül is az egymástól eltérő jogszabályértelmezések alapján különböző „napi gyakorlat” létezik. Javaslatot tettem a nemzeti minősített adatok elektronikus kezelésének eljárásrendje módosítására a NATO hasonló rendszerek mintájára.
- Elemeztem a nem minősített adatok védelmével kapcsolatos jelenlegi korlátokat. Kutatási eredményeim valamint saját tapasztalataim alapján javaslatot tettem egy

új adatvédelmi osztály létrehozására, amely jelentősen hozzájárulhat a katonai műveletek infokommunikációs rendszerein kezelt adatok illetéktelen személy általi megismerésével szembeni védelmének a növeléséhez. Javaslatot tettem a nem minősített adatok jogi korlátok miatti sebezhetőségének csökkentésére jogi és technikai megoldások alkalmazásával.

3. A katonai műveletek infokommunikációs támogatásának lehetőségei nem katonai információs infrastruktúra alkalmazásával

A katonai műveleteket, beleértve a békeidőben végrehajtásra kerülő kiképzési feladatokat és a Honvédség feladatrendszeréből adódó béke és háborús műveleteket is, a jelenlegi, számtalan polgári infokommunikációs rendszer alkalmazó világban nehezen megvalósítható, és nagy erőforrások folyamatos biztosításával megoldható feladat a műveletek kizárólag katonai infokommunikációs eszközrendszerrel való támogatása.

Az infokommunikációs eszközrendszerek fenntartásának anyagi és emberi erőforrásai még a legnagyobb hadseregeknél is végesek, ezért működésük során különböző mértékben, szervesen támaszkodnak a polgári hálózatok szolgáltatásainak igénybevételére.

Lényeges, hogy a polgári célú hálózatok katonai alkalmazása esetén milyen elveket, jogszabályokat és elvárásokat fogalmazunk meg az igénybe venni kívánt rendszerrel és annak szolgáltatójával szemben. A nem katonai rendszereket két csoportra osztva kívánom tárgyalni.

Az első csoport a Kormányzati célú, de nem kifejezetten katonai alkalmazású infokommunikációs rendszerek halmaza. Ezek a hálózatok szigorú törvényi feltételek szerint kötelesek működni, szolgáltatásokat biztosítani. Költségvetési forrásból működnek, tehát a beszerzési, üzemeltetési feltételeik pénzügyi szempontból is jogszabály által szabályozott. Elsősorban az országhatáron belüli katonai műveletek infokommunikációs támogatására vezetők igénybe.

A második csoportba sorolom az egyéb, nem kormányzati jellegű infokommunikációs hálózatokat, amelyek üzleti alapon szolgáltatnak, természetesen honvédelmi érdekből, bizonyos feltételek teljesülése esetén kötelező szolgáltatásokat is kell nyújtaniuk.

Akár kormányzati célú, akár kereskedelmi jellegű szolgáltatót vizsgálunk, minden esetben fontos követelmény, hogy az adatkezelés során elkerülhető legyen adatvédelmi incidens bekövetkezése. Az **adatvédelmi incidens** a GDPR 4. cikk 12. pontja értelmében a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését (rendelkezésre állás sérülése), megváltoztatását (integritás sérülése), jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést (bizalmas jelleg sérülése) eredményezi.(*NAIH.hu,* 2023)

A Nemzeti Infokommunikációs Stratégia utódjaként 2022 decemberében a Miniszterelnöki kabinetiroda kiadásában megjelent a „Nemzeti Digitalizációs Stratégia”

A stratégia kiemeli, hogy létrehozták a Szabályozott Tevékenységek Felügyeleti Hatóságát (SZTFH), amely Az Európai Unió által kidolgozott kiberbiztonsági tanúsítási rendszer hazai elemeként a 2022. január 1-jétől a Szabályozott Tevékenységek Felügyeleti Hatóságáról szóló 2021. évi XXXII. törvény és az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény módosításának eredményeként a Szabályozott Tevékenységek Felügyeleti Hatósága (a továbbiakban: SZTFH) került kijelölésre a nemzeti kiberbiztonsági tanúsító hatósági feladatok elvégzésére. A hazai kibervédelem részeként a Hatóság látja el a digitális termékek kiberbiztonságát tanúsító hatósági feladatokat, illetve a kiberbiztonság erősítése területén az SZTFH további fő prioritása a kiberbiztonsági tudatosság növelése, azaz a kibertérben megjelenő fenyegetések széles körben történő megismertetése, valamint az állampolgárok online térben történő biztonságos eligazodásának segítése. A szervezet munkája is hozzájárul ahhoz, hogy kereskedelmi, civil infokommunikációs hálózatok alkalmazásakor az adatkezelés során minimálisra csökkenjen az adatvédelmi incidens bekövetkezésének lehetősége.

3.1 Kormányzati, közszolgálati célú rendszerek, információvédelmi eljárásrendek, alkalmazhatóságuk katonai igénybevételre.

Az állami és önkormányzati szervek infokommunikációs rendszereit információbiztonsági szempontból a 2013. évi L. törvény (a továbbiakban: Ibtv.) szerint kell tervezni és üzemeltetni.

Az állami szervek kategóriába a Magyar Honvédség is beletartozik. Mint korábban kifejtettem, a Honvédség nyílt adatainak kezelése során eleget kell tennie az Ibtv..-ben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet előírásainak is.

A rendelet részletes feltételrendszerben foglaltak teljesítése alapján biztonsági osztályokba sorolja az infokommunikációs rendszereket. A Magyar Honvédség nyílt infokommunikációs rendszereinek meg kell felelnie a 4. vagy 5. biztonsági kategóriához előírt követelményeknek.

Magyarországon az állami, kormányzati és a honvédelmi tevékenységet végrehajtó szervezeteinek infokommunikációs hálózatai jogszabály előírások alapján egyre inkább egységes rendszert alkotnak, bár egyes elemei külön – külön önálló üzemeltetés alatt állnak, bizonyos részei pedig egymáshoz kapcsolódnak. A jogszabályok alapján

felügyeleti szerveik is különbözőek. Az állami és önkormányzati szervek információbiztonsági felügyeletét általánosságban a Nemzeti Kibervédelmi Intézet látja el. De például a Magyar Honvédség nyílt infokommunikációs rendszereit külön jogszabály alapján a Katonai Nemzetbiztonsági Szolgálat felügyeli.

A fentiekkel kapcsolatos álláspontomat már megfogalmaztam az Adatok bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása katonai információs rendszerek alkalmazása esetén című cikkemben:" A katonai nyílt adatkezelő rendszerek üzemeltetéséhez szükséges jogszabályi háttér rendelkezésre áll, ezen a területen is növelhető az elektronikai adatkezelő rendszerek kapacitása nem katonai adatkezelő rendszerek, pl. internet igénybevételével, természetesen a szükséges védelmi rendszabályok és eljárások alkalmazásával. A rendszerekben kezelt adatok hozzáférhetősége nincs szigorúan szabályozva, a rendszer elemei csatlakozhatnak nem katonai célú infokommunikációs hálózatokhoz is, ha a rendszer üzemeltetése más módon nem oldható meg. Javaslom ennek a területnek a további vizsgálatát."(Megyeri Lajos, 2016)

A cikk megjelenése óta természetesen történtek előremutató kezdeményezések, például harcászati rádióhálók chat programjai terén de a fejlesztés még nem ért véget.

3.1.1.Stacioner elemek, információvédelmi eljárásrendek, alkalmazhatóságuk katonai igénybevételre:

A kormányzati célú hírközlési hálózatok a 346/2010. (XII. 28.) Korm. rendeletben foglaltak szerint a következők:

a) Nemzeti Távközlési Gerinchálózat (NTG);

b) Egységes Digitális Rádiótávközlő Rendszer (EDR)[50];

c) Zártcélú Rendészeti Hálózat;

d) Köznet;

e) K-600/KTIR Hírközlési és Informatikai Rendszer.

Összetett feladatrendszeréből adódóan a Magyar Honvédség infokommunikációs hálózata mind a felépítésében, mind üzemeltetésében nagymértékben eltér a többi kormányzati hálózattól. Bár a kormányzati célú rendszerek egyik elkülönített eleme a

[50] *egységes digitális rádiótávközlő rendszer (EDR):* a Schengeni Megállapodás Schengenben, 1990. június 19-én aláírt Végrehajtási Egyezményének 132., illetve 44. cikkében meghatározott követelményeket kielégítő digitális, nyalábolt (trönkölt), kormányzati célú rádióhálózat.(346/2010 Korm. rendelet, XII.28.)

Magyar Honvédség hálózata, de részben függetlenül működik tőle. A hálózat beintegrálását a kormányzati rendszerbe egy kapcsolódási felületen biztosítja.

A fenti felsorolásból a Honvédség igénybe veszi az NTG, az EDR és szükség esetén a K-600/KTIR szolgáltatásait.

a. Nemzeti Távközlési Gerinchálózat

A Nemzeti Távközlési Gerinchálózaton belül elkülönült hírközlési tevékenység végzésére jogosult a Hazai Titkosszolgálatok, a Terrorelhárítási központ és a Diplomáciai testületek mellett a Magyar Honvédség, amely jogszabályban rögzített jogosítványa alapján működteti a Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózatát (MH KCEHH). Ennek igénybevételével üzemelteti a nyílt infokommunikációs hálózatát és a nem nyilvános, helyhez kötött szolgáltatásait[51] is.

Törvény vagy kormányrendelet eltérő rendelkezése hiányában kormányzati célú hírközlési tevékenységet kizárólag a kormányzati célú hírközlési szolgáltatók és az elkülönült hírközlési tevékenység végzésére jogosultak végezhetnek.

A kormányzati célú hírközlési szolgáltató az egységes digitális rádiótávközlő rendszer kivételével a Nemzeti Infokommunikációs Szolgáltató Zártkörűen Működő Részvénytársaság, továbbiakban NISZ.

A jogszabály a folyamatos és rugalmas üzemeltetés érdekében a fent leírtaktól eltérően lehetőséget ad más szolgáltató igénybevételére a következők szerint.

Az elkülönült hírközlési tevékenység végzésére jogosult szerv a Magyarország területén belüli felhasználói vagy hálózati hozzáférési pontok vonatkozásában a kormányzati célú hírközlési szolgáltatón kívül más elektronikus hírközlési szolgáltatót az alábbi esetekben vehet igénybe: Az elkülönült hírközlési tevékenység végzésére jogosult más adatátviteli hálózathoz az NTG-n kívül is csatlakozhat, ha ez az elkülönült hírközlési tevékenység végzésével összefüggő feladatainak ellátásához szükséges, és az NTG-n keresztül történő csatlakozás e feladatainak ellátását hátrányosan befolyásolná.(346/2010 Korm. rendelet, XII.28.)

[51] *nem nyilvános, helyhez kötött telefonszolgáltatás:* a helyhez kötött előfizetői végponton keresztül igénybe vehető, kormányzati célú hálózaton nyújtott olyan, kizárólag e rendeletben meghatározott szervek, szervezetek vagy személyek által igénybe vehető elektronikus hírközlési szolgáltatás, amely belföldi vagy nemzetközi számozási tervben szereplő hívószám vagy hívószámok segítségével közvetlenül vagy közvetve lehetővé teszi belföldi vagy belföldi és nemzetközi hívások kezdeményezését és fogadását, és amely nem minősül mobil rádiótelefon szolgáltatásnak.(346/2010 Korm. rendelet, XII.28.)

Tehát a jogalkotó preferálja a NISZ által nyújtott szolgáltatások igénybevételét, a jogszabály azonban lehetővé teszi, hogy a NISZ által nem nyújtott szolgáltatások tekintetében harmadik fél nyújtson szolgáltatást az infokommunikációs rendszer felhasználói részére. Értelmezésem szerint ez azt jelenti, hogy a NISZ által lefedett szolgáltatási körben, Magyarországon kereskedelmi szolgáltatók igénybevételére a jogszabályi tiltás miatt kevés az esély. A lehetőségek az új szolgáltatások esetében jöhetnek szóba, ami véleményem szerint például a műholdas infokommunikációs szolgáltatás lehet. Ezen kívül telepíthető körülmények között és missziós katonai feladatok támogatása esetén nincs törvényi akadálya a polgári, kereskedelmi szolgáltatások igénybevételének.

b. EDR szolgáltatás:

(EDR): a Schengeni Megállapodás Schengenben, 1990. június 19-én aláírt Végrehajtási Egyezményének 132., illetve 44. cikkében meghatározott követelményeket kielégítő digitális, nyalábolt (trönkölt), kormányzati célú rádióhálózat.(346/2010 Korm. rendelet, XII.28.)

Tehát az EDR egy olyan kormányzati célú rádióhálózat, amelyet nemzetközileg elfogadott szabványok alapján állami és önkormányzati szervek készenléti szolgálatai infokommunikációs támogatása céljából hoztak létre. A rádióhálózat az egységes szabványoknak köszönhetően akár nemzetközi viszonylatban is biztosíthat összeköttetést.

Az EDR a TETRA technológiára épül, mely egy, a professzionális felhasználói igények kielégítésére alkalmas mobil hírközlő rendszer, szelektív és csoportkommunikációs beszéd és adatátviteli szolgáltatásokkal

A TETRA rendszer által nyújtott szolgáltatások – más hírközlő rendszerhez hasonlóan – három csoportba sorolhatók. A teleszolgáltatások a végfelhasználói rádióterminál segítségével vehetők igénybe (pl. beszédhívás), míg a hordozószolgáltatások eléréséhez valamilyen külső berendezés csatlakoztatására van szükség (pl. számítógép, GPS vevő). A kiegészítő szolgáltatások a teleszolgáltatásokat (vagy azok igénybevételének módját) változtatják meg, illetve egészítik ki.(Kardos, 2021)

A kormányzati célú hírközlési szolgáltató többszintű hierarchia szerint az EDR egységes infrastruktúráján biztosítja a VPN[52]-ekhez való hozzáférést, elbírálja a felhasználók VPN-jeinek erőforrásigényeit és meghozza az ezzel kapcsolatos döntéseket

Az EDR üzemeltetési szabályzat alapján ellátja az EDR VPN hálózat menedzsment feladatait, és biztosítja a VPN menedzsment központ működését, kialakítja, menedzseli és nyilvántartja a VPN gazda szervezeteket, valamint biztosítja a VPN-ek közötti együttműködést, szükség esetén létrehozza a különböző VPN gazda szervezetek által felügyelt felhasználók közötti együttműködési forgalmi csoportokat.

A Magyar Honvédség önálló EDR VPN.-nel rendelkező, közös hálózatot alkotó szervezetei:

- Magyar Honvédség katonai szervezetei
- A honvédelemért felelős miniszter által vezetett minisztérium.
- A honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvény egyes rendelkezéseinek végrehajtásáról szóló 290/2011. (XII. 22.) Korm. rendelet 16. § (2) bekezdésében meghatározott szerveknél a honvédelemmel foglalkozó szervezeti egységek
- NAMPO (NATO Támogatási Ügynökség, Légiszállítást Kezelő Programiroda)

Tehát a szolgáltatás igénybevételével a Magyar Honvédség szinte valamennyi szervezeti eleme kommunikálhat egymással.

A szolgáltatás előnye, hogy igénybevétele egyszerű, az alkalmazott mobil készülékek felhasználói igénybevétele kevesebb, mint 1 nap alatt elsajátítható. A szervezeti elemek gyorsan, könnyen összekapcsolhatóak a VPN lefedettségi területén.

A szolgáltatás hátrányai:

- Honvédségtől független, polgári kormányzati célú hírközlési szolgáltató, (Pro-M Zrt) üzemelteti. Ez megnehezíti a rendszer művelettől függő, gyors átalakítását. Általam nem ismert továbbá katonai szempontból a rendszer felderíthetősége, lehallgathatósága, zavarhatósága sem.
- Jelenleg csak nyílt üzemmódban üzemel, ezért minősített adatot semmiképpen nem, szabad rajta továbbítani.

[52] VPN: valamely VPN gazda szervezet irányítása és felügyelete alá tartozó, a felhasználó szempontjából önálló, zárt hálózatként viselkedő, úgynevezett virtuális magánhálózat

- Mivel stabilan kiépített központokból és vezetéknélküli hálózatokból áll, használatának szigorúan kötött földrajzi korlátai vannak.

A rendszer katonai műveletekre így csak korlátozottan alkalmazható.

EDR VPN felhasználó szervezetek a Magyar Honvédség mellett a teljesség igénye nélkül:

- Országos Rendőr-főkapitányság,
- Nemzeti Adó- és Vámhivatal,
- Országos Katasztrófavédelmi Főigazgatóság,
- Országos Környezetvédelmi, Természetvédelmi és Vízügyi Főigazgatóság,
- Országos Mentőszolgálat,
- OMSZ Légimentő Kht.,
- Büntetés-végrehajtás Országos Parancsnoksága,
- Nemzeti Adó és Vámhivatal,
- Nemzetbiztonsági Szakszolgálatok.

A VPN gazda szervezetek teljes listáját a 346/2010 Kormányrendelet 3.- számú melléklete tartalmazza.

Az EDR rendszer kialakításának célja az állami és közfeladatot ellátó szervezetek készenléti szolgálatai számára közös infokommunikációs hálózat létesítése. Jelenlegi kihasználtsága a felhasználók nagy száma valamint a megváltozott felhasználói igények miatt elérte a határait. Az adatkommunikáció iránt megnövekedett igények miatt az üzemeltető Pro-M Zrt. mint készenléti célú hírközlési szolgáltató keresi azokat a lehetőségeket, amelyek a TETRA technológia további fenntartásával a 2020 utáni technológiaváltásra felkészülve biztosítják a készenléti felhasználók nagysebességű adatátviteli igényeinek kiszolgálását.[53]

Az EDR rendszernek jelenleg nem célja a Magyar Honvédség Telepíthető híradó hálózatának infokommunikációs elemeit helyettesíteni és kutatásom szerint a jelenlegi formájában technikailag sem tudná ezt a támogatási feladatot ellátni.

c) Zártcélú Rendészeti Hálózat;

A fizikailag önálló Zártcélú Rendészeti Hálózat (zRH) egy technikai megoldással az Elektronikus Kormányzati Gerinchálózat (EKG) virtuális kiegészítő gerinchálózatát, annak melegtartalékát is képezi, egyben az EKG is nyújthat szolgáltatást a zRH-nak oly módon, hogy a két hálózat önállóan felügyelhető, működésük egymást nem befolyásolja.

[53] https://www.pro-m.hu/Hirek/2019/ProMNews/ Letöltve: 2023.04.19.

d) Köznet;

A KÖZNET szélessávú internet és levelezési szolgáltatást biztosít az információs társadalommal összefüggő szolgáltatást térítésmentesen, nem kereskedelmi célból nyújtó jogi személy, jogi személyiség nélküli szervezetek számára (Teleházak, eMagyarország pontok) A projekt Európai Uniós és Magyar költségvetési forrásból informatikai eszközrendszert és szolgáltatásokat fejleszt az Információs társadalom kialakulásának elősegítésére. Olyan nyilvános közösségi hozzáférési pontok hálózatát hozza létre, amely elsősorban a hátrányos helyzetű kistelepüléseken teszi elérhetővé az internet-elérést.

A fentiekből adódóan, a KÖZNET Kormányzati infokommunikációs hálózat, katonai célú igénybevételére véleményem szerint csak végszükség esetén és esetlegesen kerülhet sor.

e) K-600/KTIR Hírközlési és Informatikai Rendszer.

A 346/2010. (XII.28.) Korm rendelet alapján a „K-600/KTIR Hírközlési és Informatikai Rendszer a Honvédelmi Tanács és a Kormány speciális működési feltételeinek, valamint a Magyarország védelmi igazgatási szervei által folytatott döntés-előkészítés és döntéshozatal informatikai támogatását biztosító, kormányzati célú hálózatnak minősülő hírközlési és informatikai rendszer”. A K-600/KTIR Hírközlési és Informatikai Rendszer (K600/KTIR) hírközlési és informatikai vezetési rendszer kormányzati szinten, amely feladata a Honvédelmi Tanács és a Kormány infokommunikációs (távközlési és informatikai) támogatása feltételeinek biztosítása. A rendszerrel kapcsolatos fő irányító szerv az MH Védelmi Hivatal (MH VH), amely az üzemeltetési irányvonalat is meghatározza a rendszerrel kapcsolatban. A K-600/KTIR a védelmi igazgatás kiszolgálását biztosított ellátni, biztosítja az informatikai platformot és támogatást a védelmi igazgatás különböző szintű szervezetei részére. A rendszer működtetéséért a NISZ felelős a HM VH követelménytámasztásának figyelembevételével. A rendszer a teljes országot lefedi szolgáltatással, nagy sebességű, korszerű távközlési és informatikai összeköttetéseket biztosítva az adott szervezetek, minisztériumok és védelmi bizottságok között. A rendszer szolgáltatásai (szoftverek, adatbázisok, térinformatikai szolgáltatások, VTC, EDR) és annak fejlesztése teszi lehetővé, hogy minősített esetben a teljes szintű (teljes spektrumú) vezetés megvalósuljon. (Farkas, 2016)

Mindezekből is jól látszik, hogy az országhatáron belüli katonai műveletek sikeres végrehajtásakor a K-600/KTIR rendszernek jelentős szerepe lehet, mivel a feladatok végrehajtásának irányítását megfelelően képes támogatni.

3.2 Kereskedelmi célú rendszerek, információvédelmi eljárásrendek, alkalmazhatóságuk katonai igénybevételre:

A kormányzati célú hírközlési szolgáltató és az elkülönült hírközlési tevékenység végzésére jogosult a kormányzati célú hírközlési tevékenység érdekében a nem kormányzati célú elektronikus hírközlési szolgáltatóval előfizetői-, összekapcsolási-, hálózati- vagy közös eszközhasználatra vonatkozó szerződést köt.

Az auditált elektronikus információs rendszereket és eszközöket, nemzetközi egyezmények vagy nemzetközi szabványok alapján, illetve az ezeken alapuló hazai követelmények vagy ajánlások alapján üzemeltetik.(55/2013 HM rendelet, é. n.)

Jelenleg Magyar Honvédség Kormányzati Célú Elkülönített Hírközlési Hálózata többségben polgári szolgáltatótól bérelt szolgáltatás formájában üzemel.

A bérelt kommunikációs csatornák alkalmazhatóságát katonai jellegű adatok továbbítására információbiztonsági szempontból jelenleg a Katonai Nemzetbiztonsági Szakszolgálat ellenőrzi. A biztonságos működéshez szükséges követelményeket a 41/2015 BM rendelet *Védelmi intézkedési katalógus*a tartalmazza. A bérelt kommunikációs csatornák használatakor a rendeletben foglaltakat a katonai műveletek infokommunikációs támogatását nyújtó szervezeteknek, állományának kötelező betartani. Véleményem szerint a fenti biztonsági környezet megfelel az általános, adminisztratív jellegű adatok kezeléséhez, melyek a Magyar Honvédség védelmi képességeit nem befolyásolják.

3.2.1. Polgári műholdas szolgáltatások igénybevétele

A jelenleg Magyarországon használt műholdas szolgáltatást Tóth doktori értekezésében a következők szerint írta le: „A Magyar Honvédségben jelenleg polgári szolgáltatóktól bérelt műholdas rendszerek kerülnek alkalmazásra, melyek jellemzően VSAT[54]-szolgáltatásokat alkalmaznak, így biztosítanak közel valós idejű folyamatos hang- és adatkapcsolatot. A VSAT-hálózatok világméretű működését geostacionáris távközlési mesterséges holdak biztosítják, melyeket az Egyenlítő fölött, 35 786 km magasságban helyeznek pályára. Mivel ezek a holdak látszólag együtt forognak a Földdel, a földfelszínnek ugyanazon területét sugározzák be. Így a földi szegmens antennáinak nem kell holdkövető elektronikával és mechanikával rendelkezni.

Az adatátviteli csatornán elérhető hálózati szolgáltatások:

[54] VSAT - Very Small Aperture Terminal – nagyon kicsi fókuszfelületű terminál

intranet hozzáférés;
• videó konferencia;
• központi szerver elérése (pl. adatközpont);
• beszéd célú adatátvitel (telefonközpontok kihelyezése, VolP, stb.);
• dedikált vagy dinamikus (ügyfél hálózatán belül) nagysebességű IP virtuális magánhálózat összeköttetések;
• backup hálózatok;
• helyi szervezetek elérésének biztosítása”
(Tóth, 2015)

A csatornaszámok, technikai paraméterek a technológia fejlődésével és az igények változásával módosulhat, de a szolgáltatások jelenleg is a fenti felosztás szerint érhetők el.

A nagyon kis apertúrájú hálózat egy elosztóközpontból (hub) és a mesterséges holdakkal összeköttetésben álló számos terminálból, VSAT-állomásból áll. A terminálok antennáinak átmérője 1,2– 2,4 m. A földi hálózatokkal összehasonlítva a VSAT több jelentős előnnyel bír: alacsony működtetési költség, egyszerű karbantartás, a hálózat könnyű bővíthetősége további terminálokkal.

A VSAT-hálózat topológiája rendszerint csillag formáció, melyben a központi vezető állomás szerepét a Hub tölti be. A hálózatban a VSAT-terminálok a Hub által kiszolgált csomópontok. A csillag formáció nagyon rugalmas hálózat, könnyen lehetővé teszi a bővítését további terminálokkal, illetve egyszerűsítését azok kivonásával anélkül, hogy befolyásolnák a többi csomópont által nyújtott szolgáltatást.

A szolgáltatás jelenlegi igénybevételének egy jellemző formája a videokonferencia hívás. Személyes tapasztalatom, hogy az országhatáron kívüli, nemzetközi kötelezettségvállalás alapján szolgálatot teljesítő alegységek parancsnokai, de még az országon belüli különböző katonai szervezetek parancsnokai is rendszeresen VTC[55] eszközök és alkalmazások segítségével tesznek eleget ismétlődő jelentési kötelezettségeiknek.

Véleményem szerint ez a gyakorlat információbiztonsági szempontból nem mindig helyes. A jelenleg általánosan használt VTC eszközök és kommunikációs csatornák nem védettek rejtjelző eszközökkel, csak nyílt információ továbbítására engedélyezett a használatuk. Magas beosztású parancsnokok szóbeli jelentése alkalmával nem egyszerű az elhangzott adatok, információk szűrése. A szóbeli információ minősített vagy nyílt

[55] VTC - Video Teleconferencia – Videotelefon konferencia

adattá nyilvánítás problémakörét dolgozatom II. fejezetében is tárgyaltam, ezért itt csak annyiban térek ki rá, hogy a jogszabályok szerint minősített adat továbbításakor a kommunikációs csatornát védeni kell rejtjelző eszközökkel, amely esetben viszont a minősített adatkezelés egyéb személyi, fizikai és adminisztratív és elektronikus információvédelmi előírásait is alkalmazni kell. Ezen védelmi intézkedések hiányában a csatorna kizárólag nyílt adatok továbbítására lesz alkalmas. Az információbiztonsági képzettséggel nem rendelkező parancsnoki állomány figyelmét nyomatékosan fel kell hívni arra a tényre, hogy a VTC kommunikációs csatorna nem védett. Ettől kezdve a parancsok saját döntése, hogy milyen információt továbbít a rendszeren. Sajnos jelentések esetén gyakran szóba kerülnek technikai meghibásodások, feladat végrehajtását akadályozó tényezők, amelyekről megítélésem szerint nem helyes nyílt kommunikációs csatornán kommunikálni.

A kockázatok további növekedését eredményezi, amikor a VTC egyes végpontjait VSAT műholdas rendszer alkalmazásával valósítják meg. Az alkalmazott műholdak ún. „bent-pipe" átjátszók, vagyis a szolgáltatási terület bármely pontjáról beérkező rádiójelet a teljes területre visszasugározzák.(Attila Gulyás & Horváth, 2013)

Ez azt jelenti, hogy a VSAT jeleket egy kilométerekben mérhető átmérőjű foltnyi területre sugározzák le. Elsősorban külföldi alkalmazás esetén előfordulhat, hogy a lesugárzott jelek jóval vevőállomás környezetét körülvevő katonai táboron, központon, harcállásponton kívül is kiválóan fogható. A kommunikációt polgári szabványokban meghatározott módon, az ügyfelek privát zónája biztosítása érdekében védett, a nyílt adatokat a műholdas rendszeren és a kapcsolódó földi átviteli úton AES-256 IPsec2 titkosítással védi a szolgáltató. A hálózat titkosító kulcs azonban egyes információk szerint hozzáférhető.

„A Fox-IT nevű IT-biztonsági cég beszámolója szerint hardveres téren kevesebb mint 200 dollárnyi eszközre van szükség ahhoz, hogy vezetékmentes módon (maximum egy méteres távolságról) hozzáférhessenek az AES-256 titkosítókulcsokhoz."[56]

Bár az interneten található hír nem hitelesen dokumentált, általánosságban elmondható, hogy a kereskedelmi és az állampolgárok különleges személyi adatai védelmét biztosító titkosítási eljárások védelmi szintje nem éri el a nagyon szigorú szabályok szerint működő, kiválasztott személyekkel üzemeltetett, egyedileg gyártott rejtjelkulcsokat alkalmazó rejtjelzés védelmi képességi szintjét. Megfelelő technikai háttérrel és

[56] https://bitport.hu/200-dollarbol-megtortek-az-aes-256-titkositast letöltés ideje: 2023.05.19.

szakemberekkel rendelkező állam, csoport képes lehet a kereskedelmi forgalomban szabadon vásárolható VTC eszközök biztonsági protokolljainak feltörésére és az ott kezelt információk jogosulatlan megismerésére.

Ezért a rejtjelző eszközökkel nem védett kommunikációs csatornákon az illetéktelen megismerés esetén a honvédelem érdekeit hátrányosan befolyásoló információ kezelése, továbbítása tilos.

Napjaink egyik példája a szomszédos Ukrajnában zajló fegyveres konfliktushoz köthető. Sajnos a zajló műveletekről nehéz hiteles információkhoz jutni, többnyire különböző médiacsatornák által közölt valós vagy egymástól eltérő érdekek által elfordított hírekből tájékozódhatunk. Dolgozatomban itt mégis beidézek néhány ilyen hírt. Egyrészt, mert több különböző forrásból származnak, a hírcsatornákban hosszabb ideje jelen vannak érdemi cáfolat nélkül, és technikai jellegüknél fogva véleményem szerint a megvalósulásuk technológiailag lehetséges.

Másrészt mert a műholdas kommunikáció problémáinak egy jelenkori, gyakorlatban, élesben jelentkező ékes példáját láthatjuk ezen események tükrében.

Az tény, Elon Musk maga is megerősítette, hogy az ukrán polgárok humanitárius megsegítésére rendelkezésükre bocsátja az általa létrehozott Starlink[57] rendszer mozgatható termináljainak használatát. Természeresen nem ingyen, az Európai Unió vállalta, hogy szerződés alapján fizeti a költségeket. A publikus hírek szerint Ukrajnában mintegy 30 000 műholdhoz közvetlenül internetes hálózatra kapcsolható, az előfizetés függvényében akár 100Mb/s adatletöltési sebességgel működő hordozható terminál üzemel. Álszentség volna azt gondolni, hogy a gyakorlatilag minden más hálózati kommunikációját elveszített ukrán hadsereg ne venné igénybe a rendszer szolgáltatásait. Emiatt Oroszország többször is reagált az amerikai tulajdonos illetve az USA irányába. Végül újsághírek szerint Oroszország lépett:

„*A The Washington Post birtokába került titkos amerikai hírszerzési jelentés szerint Oroszország azon törekvése, hogy szabotálja az ukrán erők internet-hozzáférését azáltal, hogy a Starlink műholdműveleteket célozza meg… … Moszkva hónapokig kísérletezett Tobol elektronikus hadviselési rendszereivel annak érdekében, hogy megzavarja a*

[57] Elon Musk amerikai milliárdos, feltaláló egyik vállalata, a SpaceX újabb tízezer Starlink műholdas internetes terminált szállít Ukrajnának segítségül, ha a háború miatt újabb nagyszabású villamosenergia-kiesés történne - közölte Mihajlo Fedorov ukrán digitális átállási miniszter a Bloomberg hírügynökségnek nyilatkozva. forrás: https://www.portfolio.hu/global/20221220/elon-musk-ujabb-tizezer-starlink-terminalt-szallit-ukrajnanak-586236

Starlink ukrajnai adásait – állítja a szigorúan titkos értékelés, amelyet korábban nem hoztak nyilvánosságra.

A Starlink létfontosságúnak bizonyult az ukrán hadsereg számára, amely a kis hordozható terminálokra támaszkodik a csatatéren keresztüli kommunikációhoz és a hírszerzési adatok továbbításához. Nem világos, hogy az Ukrajnában jelentett Starlink leállások az orosz Tobol-kísérletek vagy az orosz erők által használt egyéb zavaró képességek, például a teherautóra szerelt Tirada-2 rendszer eredménye-e. Az elemzők legalább hét Tobol komplexumot azonosítottak Oroszországban, amelyek mindegyike a műholdak nyomon követésére használt létesítmények mellett található"[58]

Természetesem a Starlink üzemeltetői nem ismerték el, hogy a szolgáltatásaikat az Orosz erők képesek volnának korlátozni, a médiában „önkéntes" önkorlátozásról beszéltek, amelyről egy 2023 februárban megjelent hírben az alábbiak szerint nyilatkoztak : „Az Elon Musk által alapított SpaceX űrkutatási vállalat lépéseket tesz annak érdekében, hogy az ukrán haderő a továbbiakban ne használhassa drónok vezérlésére az általa Kijev rendelkezésére bocsátott Starlink műholdas internethálózatot. - *A Starlinket nem arra tervezték, hogy fegyverként használják* - húzta alá egy washingtoni konferencián Gwynne Shotwell, a SpaceX elnöke és operatív igazgatója. Shotwell elmondta, az ukrán haderő ezzel szemben olyan módon alkalmazza technológiát, amely nem volt része semmilyen megállapodásnak − utalt ezzel arra, hogy Kijev az ellenállás során oly sikeresnek bizonyuló pilóta nélküli rendszerek irányítására használja a Starlinket." [59]

A fenti cikkből látható, hogy a műholdas kommunikációs eszközök elleni harc már nyíltan is zajlik. Az elektronikai hadviselés eszközeinek használata véleményem szerint azért is került előtérbe, mert így a tevékenység kevésbé kézzelfogható, nehezen értelmezhető egy harmadik ország elleni támadásnak. A médiában ma is csak találgatják, hogy egyáltalán alkalmazásra kerültek e. Bár az Orosz illetékesek megemlítették a Starlink műholdak vagy azok földi szegmensének a fizikai megsemmisítése lehetőségét is, erre mindeddig nem került sor, vélhetőleg a várható diplomáciai következmények miatt. A háború kiszélesedése, több ország konfliktusba bevonása bizonyos határig Oroszországnak sem célja. Az Ukrajna felett átrepülő amerikai vállalat tulajdonában levő

[58] forrás: https://www.washingtonpost.com/national-security/2023/04/18/discord-leaks-starlink-ukraine/?fbclid=IwAR1YpPUtAHbTu9CWetH41OWmMDlySGS9fjkUVMCewCTuqIK67M4ynh-sxsA letöltés ideje: 2023.05.23.

[59] https://magyarnemzet.hu/kulfold/2023/02/bajban-az-ukranok-korlatozzak-a-hadero-starlink-internet-hasznalatat letöltés ideje 2023.06.11.

eszközök megsemmisítése diplomáciai szempontból problémás lehet, a földi terminálok pedig más országok, többek között NATO tagállamok területén vannak.

A fent említett, Elon Musk nevéhez köthető polgári műholdas rendszer, a „Starlink" használata ma már Magyarországon is bárki számára elérhető. Ahhoz, hogy elemzésem a rendszer magyar katonai alkalmazások használhatóságra számára értékelhető legyen, mindenképpen meg kell ismerkedni annak működésével. A leírás, amely a Starlink saját oldaláról származik, némileg marketing „ízű", de a benne szereplő adatok a valóságnak megfelelnek:

Bolygónk jelenleg legfejlettebb szélessávú műholdas internete.

A Starlink a világ első és legnagyobb műhold-konstellációja, amely alacsony Föld körüli pályát használ szélessávú internet biztosításához, amely képes streaming, online játékok, videohívások és egyebek támogatására.

A fejlett műholdak és felhasználói hardverek, valamint az űrtechnológia és az orbitális pályán végzett műveletek terén szerzett komoly tapasztalatainkkal párosulva a Starlink nagy sebességű, alacsony késleltetésű internetet biztosít a felhasználók számára a világ minden tájáról.

- Állandó hozzáférés a Világűrhöz:

A világ vezető (űrtechnológiai) kilövési szolgáltatójaként jelenleg a SpaceX az egyetlen műhold-üzemeltető, amely igény szerint képes saját műholdakat felbocsátani. A Starlink műholdak gyakori, alacsony költségű felbocsátásával folyamatosan frissítik a legújabb technológiát.

- Hogyan működik a Starlink:

A legtöbb műholdas internetszolgáltatás egyetlen geostacionárius műholdtól származik, amelyek 35 786 km-es körzetben keringenek a bolygó körül. Ennek eredményeként a felhasználó és a műhold közötti oda-vissza adatátviteli idő – más néven késleltetés – magas, ami szinte lehetetlenné teszi a streaming, az online játékok, a videohívások vagy más nagy adatátviteli sebességű tevékenységek támogatását.

A Starlink több ezer műholdból álló konstelláció, amelyek a Földhöz sokkal közelebb, körülbelül 550 km-re keringenek a bolygó körül, és lefedik az egész földgömböt. Mivel a Starlink műholdak alacsony pályán keringenek, a késleltetés lényegesen alacsonyabb – körülbelül 25 ms a 600+ ms-hoz képest.

- A „raj" műholdösszeállítása:

A Swarm műholdjai 450-550 km magasságban keringenek, teljes globális lefedettséget biztosítva. A műholdak gyöngysorként vannak szétszórva napszinkron pályasíkok

sorozatában. Ez a konfiguráció lehetővé teszi a műholdak számára, hogy megbízható globális hálózati lefedettséget tartsanak fenn.

- Alacsony költségen globális adattovábbítás:

A Swarm alacsony sávszélességű műholdkapcsolatot biztosít mindössze 5 USD/hó áron ultra-kis műholdak használatával alacsony pályán. A Swarm műholdak a Föld minden pontját lefedik, lehetővé téve az IoT-eszközök megfizethető működését bárhol.

- Önvezérlő, öntelepítő rendszer:

A Starlink az első kereskedelmi forgalomban kapható fázissoros antenna. A Starlink Kit mindent tartalmaz, amire szüksége van az internethez percek alatt, beleértve a Starlinket, a WiFi útválasztót, a kábeleket és a bázist. Önorientált, és percek alatt csatlakozik, amíg jól látja az eget.

A Starlink (antenna) ellenáll a szélsőséges hidegnek, melegnek, jégesőnek, havas esőnek, heves esőnek, viharos szélnek.[60]

Összességében tehát a Starlink rendszer egy olyan műholdas internet-hálózat, amelyet a SpaceX cég fejleszt ki és üzemeltet. A Starlink rendszer célja, hogy gyors, megbízható és olcsó internet-szolgáltatást nyújtson a világ bármely pontján. A Starlink rendszer katonai alkalmazásai között szerepelhetnek az eredeti szaknyelvi kifejezés szerinti „imagery", a „communications" és a „hosted payloads" területei, amelyek lehetővé teszik a kormányzati ügyfelek számára, hogy biztonságosan küldjenek és fogadjanak adatokat, képeket, videókat vagy más tartalmakat a műholdakon keresztül.

A Starlink rendszer katonai alkalmazásainak egyik előnye, hogy használja az „inter-satellite laser communications" technológiát, amely lehetővé teszi a műholdak közötti közvetlen adatátvitelt anélkül, hogy földi állomásokra lenne szükség. Ez növeli a hálózat sebességét, megbízhatóságát és ellenálló képességét a zavarásokkal vagy az ellenséges támadásokkal szemben.[61]

A Starlink rendszer katonai alkalmazásainak egyik kihívása, hogy megfeleljen a kormányzati követelményeknek és szabványoknak, valamint hogy integrálja a meglévő katonai kommunikációs rendszerekkel. A SpaceX már együttműködik több katonai szervezettel és vállalattal, mint például az Air Force Research Laboratory, a Ball

[60] forrás: https://www.starlink.com/technology letöltés ideje 2023.07.03.
[61] forrás:SpaceX unveils Starshield, a military variation of Starlink satellites (cnbc.com) letöltés ideje 2023.07.04.

Aerospace vagy az L3Harris Technologies, hogy tesztelje és fejlessze a Starlink rendszer katonai alkalmazásait[62].

A Starlink rendszer katonai alkalmazásai tehát nagy potenciállal bírnak a kibertérben zajló konfliktusok és versenyek során, de még sok munka és kutatás szükséges ahhoz, hogy teljes mértékben kihasználják a rendszer előnyeit és kezeljék a kockázatait.

Véleményem szerint a Magyar Honvédségnek a haderőfejlesztési törekvései során mindenképpen vizsgálnia kell a Starlink vagy azzal hasonló szolgáltatásokat nyújtó rendszer igénybevételének lehetőségeit a katonai műveletek infokommunikációs támogatása megvalósítása során. A jelenlegi feltételrendszer alapján az igénybevétel nem igényel aránytalanul nagy anyagi erőforrásokat. A rendszer tulajdonosa az Egyesült Államok állampolgára, NATO tagországként politikai jellegű ellenérdekeltség esélye igen csekély.

Véleményem szerint polgári infokommunikációs rendszer katonai alkalmazása esetén az érzékeny bár nem minősített, katonai jellegű adatok feldolgozása során minden estben szükséges a polgári rendszer saját, szabványokban meghatározott információbiztonsági protokolljainak betartása mellett egy „saját” , kifejezetten katonai szervezetek kizárólagos használatával létrehozott végponti titkosítás is.

A nem katonai információbiztonsági szakkifejezéssel „end to end titkosításnak” nevezett eljárás sokban hasonlít a katonai, minősített adatokat kezelő rendszerek információbiztonsági eljárásrendjéhez:

Az "end-to-end titkosítás" olyan kifejezés, amelyet az adatok védelmének egy bizonyos módszerére használnak. Az end-to-end titkosítás azt jelenti, hogy a kommunikáció során az adatok csak a küldő és a fogadó között vannak titkosítva és védve, és senki más nem tudja hozzáférni vagy olvasni azokat az útjuk során.

A hagyományos kommunikációs rendszerekben gyakran számos pont van, ahol az adatok áthaladnak, például szerverek vagy köztes eszközök (pl. útválasztók), amelyek potenciálisan hozzáférhetnek az adatokhoz. Az end-to-end titkosítás ezzel szemben a kommunikáció végpontjai közötti közvetlen titkosítást jelenti, ami azt eredményezi, hogy csak a feladó és a címzett tudja elolvasni az adatokat.

Ez a módszer nagyon fontos a bizalmas információk, például az üzenetek, fájlok vagy személyes adatok védelmében. Az end-to-end titkosítás biztosítja, hogy még akkor is, ha valaki illetéktelenül hozzáfér az adatokhoz a köztes pontokon, nem lesz képes elolvasni

[62]forrás: Air Force Considers SpaceX Starlink For Military Applications - SlashGear letöltés ideje 2023.07.04.

vagy megérteni azokat, mivel csak a végpontokon történő titkosítás és visszafejtés kulcsaival rendelkező felek képesek megfelelően kezelni az adatokat.

A kommunikációs alkalmazások, mint például az üzenetküldő alkalmazások és a videóhívó szolgáltatások, gyakran alkalmazzák az end-to-end titkosítást, hogy védelmet nyújtsanak a felhasználók számára a magánélet és az adatvédelem szempontjából. Ez növeli a felhasználók bizalmát az adott szolgáltatásban, mivel csak a résztvevők tudják, hogy mit kommunikálnak egymással.

Az Európai Unió az Orosz Ukrán konfliktus kapcsán felismerte a földi infokommunkációs rendszerek sérülékenységét, a műholdas ifokommunikációs rendszerekben rejlő stratégiai lehetőségeket, ezért egy európai műholdas rendszer létrehozásáról döntött.

Az IRIS² (Infrastructure for Resilience, Interconnection and Security by Satellite) a tervek szerint 2024-ben kezdi meg működését és fő célja, hogy természeti katasztrófák vagy válsághelyzetek esetén is biztonságos műholdas kommunikációt biztosítson az EU kormányzati felhasználóinak.[63]

Jelenlegi tervek szerint Magyarországon közös vállalatot hoz létre a 4iG Nyrt. az Antenna Hungária Zrt., valamint a NewSpaceIndustriesZrt. A bejegyzés alatt álló CarpathiaSatMagyar Űrtávközlési Zrt. (CarpathiaSatZrt.) létrehozásával az alapítók célja, hogy a társaság 2024-ben geostacionárius pályára állítsa és hosszú távon üzemeltesse Magyarország első kereskedelmi, valamint kormányzati és tudományos kutatási feladatokra is alkalmas műholdját.

Mindezek alapján elmondható, hogy a Magyar Honvédségnek még békeidőben kereskedelmi szabályok szerinti szerződések alapján kell szolgáltatásokat bérelnie mindaddig, amíg az Állam nem képes ezeket az infokommunikációs szolgáltatásokat megfelelő saját eszközrendszer megvásárlásával és üzemeltetésével kiváltani. A szerződések megkötésekor törekedni kell arra, hogy a technikai megfelelőség és megbízhatóság mellett lehetőleg honi, NATO vagy Európai Unió tagországa által nyújtott szolgáltatásokat vegyünk igénybe. A szerződések szövegében véleményem szerint fontos kikötés kell, hogy legyen a részfeladatok anyavállalattól való kiszervezésének részletes szabályainak a megfogalmazása is. Véleményem szerint a biztonság és folyamatos szolgáltatásnyújtás érdekében fontos kikötésnek kell lennie, hogy amennyiben technikailag lehetséges, bekerülési összegtől függetlenül preferáljunk és tilalmazzunk

[63] https://ictglobal.hu/rovid-hirek/az-eu-elinditja-sajat-kommunikacios-muholdhalozatat-a-biztonsagos-osszekottetes-erdekeben/

bizonyos országokban üzemelő bizonyos vállalkozásokat még akkor is, ha ez a szabadkereskedelem elveinek ellentmond. Ezt a véleményemet műholdas kommunikációs rendszerek esetében alátámasztja Gulyás és Horváth is, akik szerint:

„Politikai szempontból mérlegelendő ezzel kapcsolatban, hogy a rendszer működéséhez alapvetően szükséges műholdat fontos-e NATO-szövetségeseink felügyelete alatt tudni, vagy megelégszünk a piacon megvásárolható és üzletfelek között szokásos, szerződéses garanciákkal. Meg kell viszont jegyezni, hogy a katonai műholdak támadások elleni védettsége magasan felülmúlja a polgáriakét, annak ellenére is, hogy a polgári területen is történnek erre irányuló lépések. Ha fennáll annak esélye, hogy akár a hírrendszer földi elemeit, akár a műholdat fegyveres vagy elektronikai támadás éri, azoknak csak a katonai rendszerek képesek ellenállni"(Attila Gulyás & Horváth, 2013)

Természetesen az a legbiztonságosabb megoldás az, ha az ország saját erőből meg tudja valósítani a honvédelemhez szükséges katonai műveleteket támogató infokommunikációs rendszer műholdas – űr szegmensét is. Gulyás és Horváth véleménye szerint:

„Amennyiben viszont az a követelmény jelentkezik, hogy magas intenzitású katonai műveletek támogatására is alkalmas rendszerrel rendelkezzünk, ahhoz katonai távközlési műholdak és saját hub szükséges. Erre vonatkozóan az elmúlt évek során spanyol (XTAR-EUR), brit (Skynet) és olasz (SICRAL) rendszerekkel kapcsolatban érkeztek felajánlások. Ez azonban olyan jelentőségű és erőforrásigényű beruházás lenne, amihez évekig tartó, fókuszált felkészülés szükséges"(Attila Gulyás & Horváth, 2013)

Ez azonban véleményem szerint Magyarországtól gondosan megválasztott és hosszútávon ekvivalens irányelvek mentén tervezett fejlesztési erőfeszítést kíván. A fentieket Gulyás és Horváth 2013 – ban írta, az azóta eltelt 10 év alatt a műholdas kommunikáció irányába jelentős elmozdulás nem történt.

A Honvédség infokommunikációs fejlesztéséért is felelős Gerőfi 2017.-ben ezt írta:

Az MH telepíthető híradó-informatikai rendszer fejlesztése, digitális alapokra helyezése, az alakulatok infokommunikációs képességeinek hálózatba szervezése folyamatban van, a század szintű korszerű híradó-informatikai rendszer kialakítása a csapatok többségénél megvalósult.

Az elkövetkező tíz év fejlődési iránya a sokfunkciós, mobil, könnyen kezelhető, komplex infokommunikációs szolgáltatások irányába mutat, amely magában foglalja a mozgókép, a hang, az írásos és egyéb adatok integrált kezelését, a sokszereplős kommunikáció

egyidejű megvalósítását, az automatikus információkeresést és adattársítást. .(Gerőfi, 2017)

A fenti idézet megmutatja, hogy fejlesztési források rendelkezésre állása esetén sem gondolkodtak az infokommunikációs rendszer műholdas kommunikáció irányába való fejlesztéséről. Ennek oka véleményem szerint az lehetett, hogy egyrészt égető szükség volt a meglévő elavult infokommunikációs rendszerek a NATO tagországokhoz hasonló szintre emeléséhez másrészt hazánkban a katonai műholdas rendszerek infrastruktúrális alapja sincs meg ezt a képességet nulla szintről kell felépíteni. Jelenleg az Európában megteremtődött feszült politikai helyzet és fegyveres konfliktusok okán ismét előtérbe került a magyar haderő fejlesztése. Határozott véleményem, hogy a műholdas kommunikációs rendszerek kialakítása és alkalmazása megkerülhetetlen, elengedhetetlen feladat a katonai műveletek korszerű infokommunikációs támogatása céljából.

A műholdas szolgáltatások igénybevétele mellett természetesen szükség van a földi szegmens igénybevételére, fejlesztésére is. A Honvédség jelenleg a honi kiképzési és műveleti feladatai ellátása során elsősorban a Kormányzati infokommunikációs rendszerekre és polgári szolgáltatóktól bérelt szolgáltatásokra támaszkodik. Ennek előnye, hogy a bérelt szolgáltatások rendelkezésre állását nem katonai erőforrásból kell megoldani. Ez az előny azonban hátránnyá is válhat azáltal, hogy a katonai műveletek begyakorlásának végrehajtása során az infokommunikációs támogatást nyújtó szakállomány nem a gyakorlat által elvárt tábori feltételrendszerek között dolgozik, hanem „könnyített üzemmódban”. A szakállomány nem biztos, hogy kellő jártasságot szerez a műveletek infokommunikációs támogatásának kizárólag a telepíthető rendszerek alkalmazásával végrehajtott gyakorlati fogásaiból.

Véleményem szerint a honi kiképzési feladatok végrehajtása során nagyobb súlyt kellene fektetni a telepíthető rendszerek által gyakorlatok időtartamára biztosított infokommunikációs rendszerek használatára Ezzel ellentétben Határon kívüli nemzeti érdekből végrehajtandó műveletek támogatása esetén nyomatékosan előnyben részesíteném polgári infokommunikációs rendszerek földi szegmensét is, a nyílt, nem nyilvános adatok kezelése esetén is végponti rejtjelző eszközök alkalmazásával.

3.3.Nem minősített adat továbbítása polgári infrastruktúra igénybevételével:

Jelen szabályozás szerint a nem minősített adatokat kezelésük, továbbításuk során nem védhetjük rejtjelzéssel. Ezen adatok biztonságát a polgári infokommunikációs hálózatok egyéb védelmi protokolljai teremthetik meg.

Legelterjedtebb adatvédelmi eljárásrend az aszimmetrikus, más néven nyilvános kulcsú (PKI = Public Key Infrastructure) titkosítás. Ennek lényege, hogy „a kódolás és dekódolás nem egy, hanem két különböző, szorosan egymáshoz tartozó, de egymásból nem kikövetkeztethető kulcspár segítségével történik. Az ún. Diffie-Hellman kulcscsere eljárás és az RSA algoritmus kombinációjaként lehetővé vált - polgári célú felhasználásra is - titkosított üzenetek küldése anélkül, hogy a kommunikációban részt vevő feleknek előre meg kellett volna állapodniuk egy meghatározott kulcsban. Az eljárás során az egyik kulcs ténylegesen titkos (magánkulcs), míg a másik bárki számára megismerhető (nyilvános kulcs). Amennyiben az eljárást titkosításra szeretnénk használni, akkor a címzett fél nyilvános kulcsával végezhető el a küldendő dokumentum kódolása, a fogadó fél pedig saját magánkulcsával dekódolja az üzenetet. Ellenben, ha aláírásra (azaz egy adott dokumentum hitelesítésére) használjuk az eljárást, akkor az aláíró a magánkulcsával kódolja a közlésre szánt dokumentumot (illetve egy abból készült digitális lenyomatot), amelyet a címzett a feladó (aláíró) nyilvános kulcsával dekódolhat, és ellenőrizheti a kapott dokumentum hitelességét”(Szádeczky, Tamás és mtsai., 2017).

Amíg a szimmetrikus titkosításnál, (amelyet a katonai rendszerek rejtjelzésre használnak), minden végponton egyforma kulcsot használunk, amelyet el is kell juttatni a felhasználás helyére, addig a PKI alkalmazásoknál egy újként jelentkező végpont is biztonságos kapcsolatot tud létesíteni egy előre ismert másik ponttal, annak nyilvános kulcsa segítségével. Ez a védelem matematikailag akár elegendő is lehetne egy katonai, nem minősített adat védelméhez.

De van egy nagy probléma, nevezetesen a nemzetállamok titkosítással kapcsolatos jogi szabályozása:

„Az 2015. évi CCXXII. törvény 97. § (2) bekezdésében továbbra is találkozunk a korábbi Eat.[64] 13. § (4) bekezdés[20] azon korlátozó rendelkezésével, miszerint a "tanúsítvány alanya az elektronikus aláírás vagy bélyegző létrehozásához használt adatot kizárólag elektronikus aláírás, illetve bélyegző létrehozására használhatja, betartva a tanúsítványban jelzett esetleges egyéb korlátozásokat is", e rendelkezés "nemzetbiztonsági érdekből nem teszi lehetővé az aláírás létrehozó adatnak (magánkulcsnak) titkosítás céljából történő felhasználását.”"(Szádeczky, Tamás és mtsai., 2017)

[64] az elektronikus aláírásról szóló 2001. évi XXXV. törvény

Tehát a jogszabályok a terrorellenes harc és a bűnüldözés hatékonyságának növelése érdekében korlátozzák a polgári infokommunikációs hálózatok titkosítási képességeit. Ezen kívül, amennyiben a szolgáltató mégis hatékonyan védi az ügyfelek adatainak a biztonságát, a jogszabályok a következőkre kötelezik őket:

„Az az alkalmazásszolgáltató, aki titkosított kommunikációt biztosító szolgáltatást nyújt, köteles az ilyen alkalmazás igénybevételével továbbított küldeményekkel, közlésekkel kapcsolatosan keletkező vagy kezelt, (2) bekezdés szerinti metaadatokat azok keletkezésétől számított 1 évig megőrizni.

(2) A külső engedélyhez kötött titkos információgyűjtésre jogosult szerv megkeresése esetén a titkosított kommunikációt biztosító szolgáltatást nyújtó alkalmazásszolgáltató

a szolgáltatás típusát;

b) a szolgáltatás előfizetőjének vagy felhasználójának

ba) a szolgáltatás igénybevételéhez szükséges azonosító adatait, a szolgáltatás igénybevételének dátumát, kezdő és záró időpontját;

bb) a regisztrációhoz használt IP-címét és portszámát;

bc) az igénybevételnél használt IP-címét és portszámát;

c) a felhasználói azonosítót

köteles átadni.(2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről, 2022)

A fenti jogszabályok alapján a polgári infokommunikációs rendszerek folyamatosan kötelesek a kezelt adatokkal kapcsolatosan metaadatokat gyűjteni.

Különböző jogszabályok alapján a következő szervek jogosultak a végponti felhasználók tudta és beleegyezése nélkül információt gyűjteni:

- a rendőrség az Rtv. 63. § (4) bekezdése alapján;
- a NAV a NAV tv. 51. § (4) bekezdése alapján és
- az ügyészség a Be. alapján.
- a rendőrség terrorizmust elhárító szerve a Terrorelhárítási Központ (a továbbiakban: TEK),
- a rendőrség belső bűnmegelőzési és bűnfelderítési feladatokat ellátó szerve az NVSZ.
- Alkotmányvédelmi hivatal
- Információs Hivatal

- Katonai Nemzetbiztonsági Szolgálat

Az ismertetett lehetőségek Magyarországon érvényesek, de az Uniós jogharmonizáció elveinek alapján az Európai Unió tagországaiban hasonló jogi szabályozásnak kell lennie. Biztos vagyok benne, hogy egy külföldön végrehajtandó katonai művelet esetén bármely érdekeinkkel szembenálló nemzet arra jogosult döntéshozói legálisnak minősíthetik bármely polgári infokommunikációs rendszer fentiek szerinti ellenőrzését. Ez pedig, ha kizárólag a szolgáltatók védelmi eljárásrendjére támaszkodunk katonai nyílt adataink továbbításakor, azok kompromittálódásához fog vezetni. Ezt egyetlen módon kerülhetjük el. Külföldi alkalmazás esetén az infokommunikációs rendszereinket, amennyiben polgári infrastruktúra is érintett az adatok feldolgozásában, rejtjelzéssel kell védenünk.

3.4. Rejtjelzés

3.4.1..Rejtjelzés szükségessége és lehetőségei:

A rejtjelzés fogalmát sokféleképpen lehet magyarázni. Dolgozatomban az érvényben levő jogszabályban foglaltat idézem: „minden olyan tevékenység, eljárás, amelynek során valamely minősített adatot abból a célból alakítanak át, hogy annak eredeti állapota a megismerésére illetéktelenek számára rejtve maradjon és ennek következtében a minősített adat minősítés nélküliként kezelhető legyen, valamint a rejtjelzett adat eredeti állapotba történő visszaállítása.” (161/2010. Kormányrendelet, 2020)

A jogszabály fogalomi meghatározása véleményem szerint nem teljes. A definíció szerint a rejtjelzés minősített adat átalakítása. Az átalakító eszközt nevezzük rejtjelző eszköznek, a teljes eljárásrendet, a személyi, fizikai, adminisztratív, elektronikus információvédelmi feltételrendszer biztosításával nevezhetjük precízebben rejtjelzésnek A fogalmi meghatározás önmagában nem elegendő a rejtjelzés szükségességének megállapításához és a rejtjeltevékenység megismeréséhez.

A szükségesség minden esetben bizonyos, közfeladat ellátása céljából – lásd honvédelem – keletkezett adatok védelme. Jelenleg a Magyar Honvédségnél rejtjelzést csak a minősített adatok védelmében alkalmazunk, elektronikusan továbbított adatok védelmének biztosítására.

A rejtjeltevékenységet folytató szerv a minősített adatot rejtjelzéssel védi, ha vezetékes vagy vezeték nélküli adatátviteli rendszerben történő továbbítás során az adat a minősített adatot elektronikus rendszeren kezelő szerv által ellenőrzött területen kívülre kerül vagy amennyiben egy adott rendszeren belül a szükséges ismeret elvének betartása rejtjelzéssel oldható meg.(161/2010. Kormányrendelet, 2020)

Gyakorlatilag a vezetékes adatátviteli rendszerben akkor kötelező a jogszabály értelmezésében rejtjelezni az adatokat, ha azok az általunk ellenőrzött területet elhagyják. Ezt a területet, mint fentebb már említettem, adminisztratív zónának nevezik és béke időszakban megegyezik a laktanya külső kerítésével, műveletek esetén pedig a tábor, harcálláspont élőerővel védett határain belüli területet jelenti.

A minősített adat rejtjelzett formája minősítés nélküliként kezelhető és nyílt csatornán is továbbítható, amennyiben rendszerengedéllyel rendelkező rejtjelző eszköz alkalmazásával történt a rejtjelzés és a rejtjeltevékenységre vonatkozó szabályokat és előírásokat maradéktalanul betartották. Tehát, ha rejtjelző eszköz alkalmazásával alakítunk át egy minősített adatot, akkor azt az adatot tovább, más módon már nem kell védeni. Nem csak zárt, katonai kommunikációs csatornán továbbítható, hanem bármely polgári szolgáltató hálózatán, akár interneten is. Természetesen békeidőszakban törekszünk rá, hogy a minősített adatok is zárt belső hálózaton kerüljenek továbbításra, de dolgozatom egyik vizsgálandó területe éppen az, hogy ennek hiányában hogyan, milyen csatornán, milyen eszközrendszerrel továbbíthatóak a rejtjelzett minősített adatok.

A rádióeszközök minősített adattovábbításának szabályrendszerével, lehetőségeivel fentebb részletesen foglalkoztam. Itt részletesen az informatikai eszközök segítségével létrehozott minősített adatkezelő hálózatok biztonságára szeretnék fókuszálni. Az információ áramlás, globális szinten megvalósuló adatfeldolgozás megvalósítására legáltalánosabbak és legelterjedtebbek a minősített számítógépes hálózatok. A hálózatok architektúrája megegyezik a nyílt adatok feldolgozására létesített számítógépes hálózatokkal. A különbség az, hogy a minősített adatokat feldolgozó hálózatok végpontjait, szerver számítógépeit, perifériáit jogszabály által meghatározott személyi, fizikai, adminisztratív és elektronikus információvédelmi szabályrendszereket betartva kell használni a rendszer teljes életciklusában. Az életciklus magában foglalja a rendszer létrehozására vonatkozó döntéstől a tervezést, a fejlesztést, a beszerzést, a telepítést, az üzemeltetést, a továbbfejlesztést és a módosítást, a rendszer egyes elemeinek vagy egészének a kivonását és megsemmisítését. Az életciklus állomásokban a minősített adatkezelő rendszer működése során a szabályok betartásáért felelős személyeket kell kijelölni (megbízni vagy kinevezni). Minden munkaállomás védelmére rendszer biztonsági felügyelőt és rendszeradminisztrátort kell alkalmazni. A rendszer biztonsági felügyelő felelős a munkaállomások biztonságos és szabályos üzemeltetését biztosító szabályrendszer kidolgozásáért, a rendszert igénybe vevő felhasználók a rendszer szolgáltatásainak igénybevételi szabályainak megismertetéséért. A

rendszeradminisztrátor informatikusként működteti a számítógépeket, programokat telepít, vírus adatbázist frissít, felhasználókat segít a rendszerhez történő hozzáférésben , biztonsági mentéseket készít.

A szabályrendszernek való megfelelést úgynevezett akkreditációs eljárás során vizsgálja meg a Nemzeti Biztonsági Felügyelet. Amennyiben az akkreditációs eljárás végén a Hatóság jogszabályok szerint biztonságosnak ítéli az informatikai hálózatot, egyenként kiadja a hálózat munkaállomásaira és szervez eszközeire egyenként vonatkozó rendszerengedélyt.

A rendszerengedély a minősített adatot kezelő szerv által üzemeltetett rendszer üzemeltetésére, módosítására, valamint rendszerek összekapcsolására a Nemzeti Biztonsági Felügyelet (a továbbiakban: NBF) által lefolytatott engedélyezési eljárást követően kiadott határozat, amely meghatározza a rendszer által kezelhető minősített adat legmagasabb minősítési szintjét, valamint a kérelmező szervezet számára meghatározott rendszerben és telepítési helyen engedélyezi a kérelemben azonosított rejtjelző eszköz működtetését. Tehát az engedély egy telepítési helyre vonatkozik. A több helyőrségben, városban, országban települt, de egy rendszerhez tartozó rendszer elemeit külön – külön kell engedélyeztetni. Nagy odafigyelést igényel a rendszerengedélyek érvényességének megőrzése. A rendszerengedély ugyanis 3 évig érvényes. A rendszer működésének meghosszabbítására irányuló kérelmet a rendszerengedély érvényességi idejének lejárta előtt legalább 30 nappal kell kezdeményezni. A rendszerengedély meghosszabbításának kérelme az adott minősített adatkezelő rendszer rendszer biztonsági felügyelőjének a feladata.

Ha egy munkaállomás vagy helyi hálózat rendszerengedélye lejár, akkor azon a rendszeren a továbbiakban, újabb akkreditációs eljárás eredményeként szerzett új rendszerengedély beszerzéséig minősített adat nem kezelhető. Ebben az esetben sérül a jogszabály által előírt rendelkezésre állás szolgáltatás.

Ha egy települési helyen több különböző minősített adatkezelő rendszert üzemeltetünk, célszerű az engedélyeztetési eljárást úgy lefolytatni, hogy a rendszerengedélyek érvényességi ideje ugyanaddig a naptári napig tartson. Így könnyebben szervezhető az egységes újra akkreditálás biztosítása.

Az informatikai hálózat adatkezelése során a minősített adatok adminisztratív zónán kívülre való továbbítása esetén van egy nagyon fontos szabály. A továbbítandó adatokat még az adminisztratív zónán belül rejtjelezni kell. Így biztosítható, hogy a továbbiakban az adatokat nyíltként kezelve, nyílt csatornán továbbíthassuk.

A rejtjeltevékenységet folytató szerv rejtjeltevékenysége során csak olyan rejtjelző eszközt alkalmazhat, amelyre vonatkozóan az NBF rendszerengedélyt adott ki.
Nemzeti minősített adat rejtjelzésére csak olyan rejtjelző eszköz alkalmazható, amelynek fejlesztője, illetve gyártója rendelkezik a minősített adat kezeléséhez szükséges, jogszabályban meghatározott személyi és tárgyi feltételekkel, és amely szerv esetében az NBF a rejtjelző eszközre vonatkozóan – a létrehozására vonatkozó döntéstől a tervezést, a fejlesztést, a beszerzést, a telepítést, az üzemeltetést, a továbbfejlesztést és a módosítást is érintően, a rendszer egyes elemeinek vagy egészének a kivonásáig és megsemmisítéséig – megbízhatóan meggyőződött arról, hogy nem áll fenn a bizalmasság elve sérülésének veszélye. (161/2010. Kormányrendelet, 2020)
Szerencsére a jogszabály alkotók gondoltak arra az esetre, ha a rejtjelzés csak külföldi gyártású eszközön valósulhat meg:
Nemzeti minősített adat rejtjelzésére külföldi eszköz csak akkor alkalmazható, amennyiben a bekezdésben meghatározott rejtjelző eszköz nem áll rendelkezésre, vagy a katonai műszaki követelmények nem teszik lehetővé külön nemzeti és külföldi rejtjelző eszköz együttes alkalmazását katonai műveletekben.(161/2010. Kormányrendelet, 2020)
Ez a jogszabály nagyon fontos lehet katonai műveletek infokommunikációs tervezésénél. Lehetővé teszi, hogy egy olyan műveletben, ahol nemzeti és NATO minősített adat továbbítása érdekében rejtjelző eszközöket alkalmazunk, a nemzeti minősített adatokat is védhetjük a megfelelő NATO engedélyekkel rendelkező eszközeinkkel, nem kell külön, más típusú nemzeti rejtjelző eszközt telepítenünk. A homogén eszközrendszer alkalmazása egyszerűsíti az üzemeltetést. Nem kell több eszköztípusra képezni a rejtjelző szakállományt, könnyebbé válik az eszközök karbantartása, esetleges javítása, cseréje is. Nemzeti minősített adat IP alapú továbbításának rejtjelzésére jelenleg nemzeti eszköz híján a NATO által, megfelelő ellenőrzési eljárások eredményeként kiadott engedély alapján megbízhatónak minősített eszközöket használhatunk. A nemzeti adatok védelmét ebben az esetben a hazai gyártású rejtjel kulcsok alkalmazása jelenti.

3.4.2. Rejtjelző eszközök:

Jelen pillanatban a NATO tagállamokban a minősített informatikai adatkezelő rendszerek adatforgalmának védelmére egyik legelterjedtebb a Norvég gyártmányú TCE 621 IP chripto eszközcsalád. A különféle típusváltozatok hazai alkalmazásában is jelentős tapasztalatokkal rendelkezünk. Az eszközeik a technológia fejlődése és a felhasználói igények alapján folyamatosan fejlődnek.

Dolgozatomban megfogalmazott javaslatom, hogy a jövőben katonai műveletek külföldi végrehajtása során a műveleteket támogató, nem minősített katonai jellegű adatokat kezelő infokommunikációs rendszereket is védjük rejtjelzéssel.

Hipotézisemnek a műveleti biztonsági indokok mellett van egy kifejezetten technológiai jellegű támogató eleme is.

Az informatikai eszközök fejlődésével párhuzamosan a rejtjelző eszközök is folyamatosan fejlődnek. Ennek az oka, hogy a fejlett IP alapú rejtjelző eszközök tulajdonképpen egy speciális felépítésű és funkciójú célszámítógépként is értelmezhetőek. A katonai jellegű adataink védelméről szóló jogszabályok megalkotásakor ezek az eszközök még viszonylag lassú, maximum 1 Mbit/sec adat átviteli képességgel rendelkeztek.

Jelenleg a Honvédségnél is rendszeresített alapvetőnek számító rejtjelző eszköz, a TCE 621/C már 1 Gbit/sec adatátviteli sebességre is képes. Ez a fejlődés technológiai alapot biztosít egy katonai szervezet valamennyi infokommunikációs igényének egyidejű kiszolgálására, hipotézisem , gyakorlati életben történő implementálásához

A TCE 621/C főbb tulajdonságai:

A TCE 621/C egy gigabites IP-titkosító eszköz, amely minden NATO biztonsági szintre jóváhagyott. Elektromos és optikai Ethernet interfésszel is elérhető. Ez a CCI titkosítóeszköz NATO Secret algoritmust (A típusú) használ, és teljes mértékben együttműködik a NICE-vel (NATO IP Crypto Equipment). A TCE 621/C távolról felügyelhető egy TCE 671-ről (SMC) vagy helyileg az előlapról. A TCE 621/C szoftveresen újraprogramozható.

Alkalmazások:

• Biztosítja a végponti alkalmazású rendszereket és LAN-okat statikus és mobil IP-hálózatokban

• Ideális VTC és VOIP biztosítására.

• Minden valós idejű alkalmazás.

Főbb jellemzői:

• Jóváhagyva a NATO CTS (Nato szigorúan titkos) szintig

• Full duplex 1 Gigabit Ethernet hálózat

• Biztonságos csoportos küldés

• Gyors eszközindítást tesz lehetővé

• Belépés-szabályozás végrehajtása

• Átjárható a hálózati szolgáltatások számára

• NAT és SNMP informatikai biztonsági szolgáltatások támogatása.

• IPSec ESPv1 biztonsági protokoll

Interoperabilitás:

• Együttműködik a TCE 621, TCE 621/B, TCE 621/B Dual, TCE 621 /C Dual és TCE 621/M szabványokkal

• 1 Gbit/s Ethernet interfész

• Támogatja az IPv4-et és az IPv6-ot is

• Távoli felügyelet a TCE 671-ről (SMC)

• Kompatibilis a KOI-18 és DTD kompatibilis kulcsbetöltő eszközökkel.[65]

A jellemzőkből kitűnik, milyen tulajdonságai miatt ilyen népszerű az eszköz. A jelenleg legújabb verzió 1 Gbit/ sec átviteli sebességet tud biztosítani. Ez a sávszélesség elegendő lehet például videokonferencia valós idejű rejtjelzésére is. Az eszközcsalád nagy előnye, hogy a korábbi típus verziókkal kompatibilis tehát egy folyamatosan fejlődő hálózat esetén nem kell a hálózat régebbi elemeit azonnal cserélni a működőképesség fenntartásához. Támogatja a VOIP hangkommunikációs eszközök használatát, amelyek véleményem szerint hamarosan le fogják váltani a régebbi típusú beszédrejtjelző eszközöket. Kiválóan alkalmas belső alhálózatok és egyszerű végponti számítógépek kommunikációjának védelmére is. Hagyományos, papír alapú és modernebb, digitálisan tárolt rejtjelkulcs betöltő eszközök használatát egyaránt támogatja.

A rejtjelző eszközök és a CCI rádiók rejtjelzett kommunikációjának biztosításához az eszközökön kívül minden esetben szükség van úgynevezett rejtjelkulcsra is.

Amennyiben rejtjelző eszközzel nem minősített adatokat védünk, a jelenleg rendelkezésre álló technológiával a rejtjelző eszközök részére a minősített adatok védelmét szolgáló rejtjelkulccsal technikai szempontból teljesen azonos rejtjelkulcsokat minden módosítás nélkül gyárthatunk. A különbség csak az elkészült rejtjelkulcsok nyilvántartásba vételével kapcsolatos adminisztratív eljárás, amely ebben az esetben a minősített adatkezelő rendszer védő rejtjelkulcsok adminisztrálásánál akár lényegesen egyszerűbb is lehet.

A vonatkozó jogszabály szerint *rejtjeltevékenység:* a rejtjelzés, valamint az azzal összefüggő rejtjelző eszköz fejlesztése, gyártása, javítása, értékesítése, az ezekkel kapcsolatos kiképzés, a rejtjelkulcs gyártása, megsemmisítése, az ezekkel kapcsolatos ügyvitel, továbbá a felsoroltak biztonságához közvetlenül kötődő feladatok ellátása.(161/2010. Kormányrendelet, 2020)

[65] Forrás: https://www.ia.nato.int/niapc/Product/TCE-621-C_170 Letöltés ideje: 2023.04.04.

Tehát a rejtjelkulcsok tárolása, továbbítása, rádió vagy rejtjelző eszközbe való betöltése egyértelműen rejtjeltevékenység, tehát csak rejtjelző szakbeosztású, érvényes rejtjelhozzáférési engedéllyel rendelkező személy hajthatja végre. Békeidőszakban, állandó elhelyezési körülmények között ez általában megoldott, mert a szigorú szabályozás érvényre juttatása az állományilletékes parancsnok felelőssége, aki szakközegei útján gondoskodik a szükséges személyi feltételek folyamatos biztosításáról. Műveleti vagy missziós körülmények között nagy odafigyelést és előre tervezést igényel a feltételeknek való megfelelés, különös tekintettel a nagyobb darabszámú CCI rádiót minősített információ továbbítására alkalmazó alegységek esetén. Az eljárást tovább bonyolítja az a szabály, hogy a minősített adatok jogszabályoknak megfelelő védelme érdekében a rejtjelkulcsokat az eszközökben előre meghatározott időközönként, periódus alapján cserélni kell. A kulcsváltást úgy kell végrehajtani, hogy az infokommunikációs hálózat folyamatos rendelkezésre állása a kulcs váltása közben ne sérüljön, a végpontok folyamatosan képesek legyenek egymással rejtjelzett kommunikációt folytatni. A rejtjelző eszközök a nagy biztonságú és nagy átviteli sebességet lehetővé tevő szimmetrikus rejtjelzési modell alapján működnek szerte a világon. Ennek az eljárásnak a számos előnyével szemben van egy nagy odafigyelést igénylő részművelete, a kulcsellátás. A szimmetrikus rejtjelzés elméleti és gyakorlati alapja, hogy az egymással kapcsolatban álló rejtjelző eszközöknek azonos rejtjelkulcsot kell használniuk. Egy nagy megoldandó feladat, hogy ezek a rejtjelkulcsok ott legyenek a rejtjelző eszközök közelében, megfelelő fizikai és személyi biztonsági feltételek között tárolva. Ennek a biztosítása műveleti, missziós körülmények között komoly kihívást jelent az információvédelemért felelős szakállománynak. Hosszabb külföldi alkalmazás esetén a folyamatos rejtjelkulcs ellátás érdekében még diplomáciai futárszolgálat közreműködésére is szükség lehet.

A Magyar Honvédség jelenleg két általános rendeltetésű rádiócsaládot használ, amelyek alkalmasak rá, és ami legalább ennyire fontos, hatósági engedéllyel is rendelkeznek hozzá, hogy rajtuk keresztül minősített adatokat továbbítsanak. Ezek a Harris és a Konsberg rádiócsaládok rejtjelző részegységgel szerelt eszközei. A haderőfejlesztés jelenleg ismert szakaszában a Honvédség a jövőben egy harmadik, Elbit tipusú rádiócsaládot szándékozik rendszerbe állítani. Ezek a rádiók technológia szempontjából korszerűnek tekinthetők. Természetesen beépített rejtjelző részegységegel rendelkeznek. Rejtjelző szempontból alkalmazásuk, annak minden előnyével és hátrányával teljesen megegyezik a jelenleg rendszesített Harris és Konsberg rádiócsaládd al. Minősített adatok

továbbítása szempontjából alkalmazásukat még egy rejtjelző eszköz rendszeresítési eljárásnak meg kell előznie, amit a Nemzeti Biztonsági Felügyelethez benyújtott kérelem (és tekintélyes mennyiségű egyéb dokumentum) indíthat majd el és akár évekig is tarthat. A rejtjelkulcsok vagy papír alapon állnak rendelkezésre egy lyukszalag formájában vagy digitálisan tároljuk elektronikus kulcstároló eszközben. Ha a rejtjelkulcs papír alapon műanyag dobozba zárva áll rendelkezésre, mindenképpen szükség van egy olyan átalakító eszközre, amely a lyukszalag formátumot digitális jelsorozattá alakítja át. Ezek az eszközök nem tárolják el a rejtjelkulcs adatait. A papír alapú rejtjelkulcs tárolás előnye, hogy ellenáll mindenféle elektronikus zavaró vagy impulzusfegyver alkalmazásának. Egy kulcsszakasz használatával lehetőség van egyetlen rejtjelkulcs használatára, a jelenlegi és jövőbeli rejtjelkulcsokat egymástól fizikailag könnyű elválasztani. Hátránya, hogy fizikailag könnyen megsemmisülhet pl. tűz vagy kisebb robbanás hatására A kulcsadatok papíron, lyukak és „nem lyukak” váltakozásával vannak rögzítve. Felhasználását vagyis rejtjelző eszközbe való betöltését követően igen rövid időn belül kötelező megsemmisíteni. A megsemmisítést jelenleg vészhelyzeti megsemmisítés kivételével két főnek kell végrehajtania és papír alapon dokumentálni kell.

Bár a modern technológia egyértelműen a digitálisan tárolt kulcsok használata felé tolódik, harcászati alkalmazásra és rendkívüli tartaléknak véleményem szerint még sokáig alkalmaznunk kell papír alapú rejtjelkulcsokat is.

A rejtjelkulcsok digitális tárolása különböző típusú kulcstároló eszközökkel történhet. Az eszközök legfőbb előnye, hogy egy eszköz több rejtjelkulcs egyidejű tárolására alkalmas. A kulcstároló eszközök a technológia fejlődésével együtt változtak. Az egyik legrégebbi kulcstároló eszköz a KYK 13 NATO kódnevű eszköz, amelynek alapvető adatai az alábbiak.

A KYK-13 egy kisméretű elektronikus adatátviteli eszköz, amelyet elsősorban a hadseregek használnak kriptográfiai adatok tárolására. Elterjedt neve Transmission Encryption Keys (TEK) és az USA fejlesztette ki. A KYK-13 nagyon népszerű az egyszerűsége, kis mérete és könnyű használhatósága miatt. A belső memóriában összesen 6 rejtjel kulcs tárolható egyszerre. A KYK-13 univerzális, a legkülönfélébb rejtjelző eszközökkel képes együttműködni kulcsbetöltéshez.

A KYK-13-t az 1980-as években építették, és már több mint 40 éve szolgál. Számos újabb kulcsbetöltő követte, mint például a CYZ-10, a PYQ-10 és a Secure DTD2000 rendszer (SDS), de mindegyikből hiányzott a KYK-13 egyszerűsége. A KYK-13-at még ma is széles körben használják. Az egyetlen igazi hátránya az, hogy a legújabb biztonsági

protokollokat nem támogatja, de a jelenleg hazánkban széles körben használt rejtjelző eszközökhöz és rádióberendezésekhez azonban még kompatibilis.[66]Az eszköz egyszerűségét jellemzi, hogy összesen két kapcsoló és két csatlakozó van rajta. Kivitele robosztus, vízbe merülésnek, elejtésnek, rázkódásnak sérülés és kulcsadat vesztés nélkül ellenáll.

Jelenleg több, önálló operációs rendszerrel is rendelkező kulcsbetöltő eszköz rendelkezik NATO által kibocsátott engedéllyel rejtjel kulcs tároláshoz, betöltéshez. A modernebb eszközök saját képernyővel rendelkeznek sok funkcióval, például log file.-ban eltárolhatják az eszközben végbement valamennyi eseményt. Kulcs tároló kapacitásuk is sokszorosa a korábbi kulcsbetöltő eszközöknek. Használatuk béke elhelyezési körülmények között, nagyobb mennyiségű kulcsadat koordinálásáért felelős rejtjelszervezeteknél előnyös lehet.

Hátrányuk, hogy az összetett funkciókból adódóan használatukhoz hosszabb, akár több napos felkészítés szükséges. A legtöbb típusuk fizikailag sérülékenyebb a KYK-13.-nál. Tapasztalatom alapján műveleti, missziós alkalmazásra ahol a technikai feltételek megengedik, a továbbiakban is a bevált, egyszerű és strapabíró KYK-13-at ajánlom használatra.

A rejtjel kulcsok különböző kategóriákba sorolhatók, funkciótól és minősítéstől függően. Funkció szerint megkülönböztethetők aszerint, hogy melyik típusú eszközben kerülnek felhasználásra és hogy az eszközben mi a konkrét feladatuk (kulcs védő kulcs, tranzit kulcs csoport kulcs, stb). Minősítés szerinti megkülönböztetés azt jelenti, hogy a kulcs gyártásakor meghatározzák, hogy milyen minősítési szintű rendszert kell majd védeni a rejtjel kulcs alkalmazásával és magát a rejtjelkulcsot is ennek megfelelően minősítik.

Léteznek nem minősített rejtjel kulcsok is, amelyeket kiképzések, gyakorlatok alkalmával lehet felhasználni.

A kulcsbetöltő eszközök tárolására szigorú szabályok vonatkoznak. Üresen tárolásuk, szállításuk feltételei megegyeznek a CCI rádiók tárolásával és szállításával szemben támasztott, fentebb már részletesen tárgyalt követelményeknek.

Ha az eszközbe rejtjel kulcsot töltenek, az eszköz tárolását, szállítását és alkalmazását olyan biztonsági feltételek betartásával kell végrehajtani, amilyen intézkedések arra a minősítési szintű minősített adatra vonatkoznak, amilyen szintű a rejtjel kulcs minősítése.

[66] forrás: https://www.ia.nato.int/niapc/Product/KYK-13_21 Letöltés ideje: 2023.04.07.

Fontos, hogy a felhasználó rendszer használata nem minősül rejtjeltevékenységnek, ha a minősített adatok kezelése vagy továbbítása olyan informatikai rendszeren történik, amelyben a rejtjelző eszköz, rejtjelző szoftver vagy rejtjelző eljárás is telepítésre került és a rendszer biztonsági beállítása nem teszi a felhasználó számára lehetővé a rejtjelzés biztonsági beállításainak módosítását vagy a minősített adatok rendszerben történő kezelése vagy továbbítása során a rendszerben alkalmazott rejtjelzés kiiktatását.(161/2010. Kormányrendelet, 2020) Ezt azért fontos meghatározni, mert a rejtjelző részegységet tartalmazó rádiók (CCI) nagy arányú elterjedésével olyan személyek, felhasználók, híradó katonák kézben, háton, gépjárműbe beépítve használják az eszközöket, akik nem rejtjelző beosztásúak. Ezzel a kitétellel tehetjük meg azt, hogy a rádióeszközök kezelőinek nem kell a rejtjelző szakállománnyal megegyező valamennyi személyi biztonsági feltételekkel rendelkezniük a rádióeszközök használata során. A rejtjelzés egyik alapelve, a minimalizálás elve is azt határozza meg, hogy a rejtjelző szervezet létszáma ne legyen nagyobb, mint amekkora a szabályos működés folyamatos biztosításához szükséges.

Az eszközök használatánál fontos szabály, hogy a rejtjelkulcs betöltését viszont csak rejtjel hozzáférési engedéllyel rendelkező személy hajthatja végre. Ez nem kis feladat egy összfegyvernemi alegység végrehajtó állományánál, ahol esetenként akár több tíz vagy száz eszközt kell a gyakorlótéren vagy hadműveleti területen rejtjelkulccsal feltölteni.

A technikai eszközzel szemben követelmény, hogy a betöltött rejtjelkulcsot az eszközből a felhasználók semmilyen módszerrel ne tudják kinyerni. Ennek biztosítására például a Konsberg rádiók ellenőrző matricával is rendelkeznek. A matrica sérülése jelzi, ha valaki megbontotta a rádióberendezést. Ezeket az eszközöket azért sem szabad kellő szakértelem és műhelyfelszerelés nélkül szétszedni, mert a rádió a katonai szabvány szerinti vízállóképességét is elveszítheti.

3.4.3. A rejtjelzés helyszínei:

Az elektronikusan kezelt minősített adatokkal kapcsolatban nagyon fontos, általam elemezni kívánt terület, az üzemeltetés helyszíne.

A rejtjeltevékenység végzésének helyszínével szemben támasztott követelményeket jogszabály szabályozza. Szerencsére a béke elhelyezési és a gyakorlatok, katonai műveletek támogatása érdekében végzett rejtjeltevékenység esetén különbözőek a helyszínekkel szemben támasztott követelmények. Általános érvényű szabály, hogy a

rejtjeltevékenységet folytató szerv a rejtelző eszközök, módszerek üzemeltetésével, tárolásával, valamint fejlesztésével, gyártásával kapcsolatos helyiségek fizikai biztonságának kialakításakor biztosítja, hogy a rendszer rejtjelzéssel kapcsolatos elemeihez felügyelet nélkül kizárólag olyan személy férhessen hozzá, akinek a munkaköre ellátásához az feltétlenül szükséges, más személy hozzáférését korlátozza, még akkor is, ha rendelkezik a megfelelő szintű személy biztonsági tanúsítvánnyal.(161/2010. Kormányrendelet, 2020)

A **stacioner,** minősített adatokat feldolgozó számítógépes hálózatok munkaállomásainak működését támogató rejtjelző eszközöket békeidőszakban szinte kizárólag I. osztályú biztonsági területen telepítik. A helységben állandóan, 0-24 órában működnek a rejtjelkulccsal feltöltött rejtjelző eszközök. Munkaidőn túl felügyelet nélkül üzemelnek. Az eszközöket a biztonsági terület fizikai védelmi rendszere (ajtó, ablakrács, erős falak, mozgásérzékelők, nyitásérzékelők, elektronikus riasztó rendszer) az élőerős őrzéssel kombinálva védi az illetéktelen hozzáférési kisérletektől. A helységbe állandó belépést biztosító technikai megoldást – általában chipkártyát – csak az oda beosztott rejtjeltevékenységet folytató szakállomány részére szabad biztosítani. A rejtjelző eszközöket a lehető legközelebb kell telepíteni azokhoz a munkaállomásokhoz, amelyeknek a védelmét ellátják. Erre azért van szükség, mert a rendszer egyik legsebezhetőbb pontja az a kommunikációs csatorna, amelyik a végponti számítógépet a rejtjelző eszközzel összeköti. Ezen a szakaszon az információ „védtelenül" halad a csatornában. Ez az oka annak, hogy a Nemzeti Biztonsági Felügyelet erre a szakaszra csak optikai kábelen való információtovábbítást engedélyez. Az optikai kábelnek ugyanis nincs elektromágneses kisugárzása és „megcsapolása", lehallgatása a jelenleg rendelkezésre álló eszközök technikai szintjén szinte lehetetlen. A kábelt még így is védett csatornában kell vezetni és a kábelvezető csatorna épségét rendszeresen ellenőrizni kell. Állandó telepítésű eszközök esetében a jogszabályoknak megfelelő üzemeltetés a fenti jogszabályok által meghatározottak szerint telepített rendszerekkel egyszeri anyagi ráfordítással hosszú távra megoldott lehet. Természetesen a rendszert arra kijelölt személyeknek a teljes életciklusában menedzselni kell.

A rejtjeltevékenység végzéséhez rendszerengedélyre van szükség, amely a Nemzeti Biztonsági Felügyelet által lefolytatott engedélyezési eljárást követően kiadott határozat, amely a kérelmező szervezet számára meghatározott rendszerben és telepítési helyen engedélyezi a kérelemben azonosított rejtjelző eszköz működtetését. A rendszerengedély kérelemben részletes helyszínrajzokat kell a rejtjelző eszközök elhelyezéséről, a

helységben kiépített kábelezések vonalvezetéséről, a tápvonalak elhelyezkedéséről. Az üzemeltetés során a helyszínrajzban rögzített üzemeltetési környezetet tilos megváltoztatni.

A rejtjeltevékenységet folytató szerv az állandó telepítésű rejtjelző eszköz áthelyezése előtt az NBF-et a tervezett változtatásról tájékoztatja. Amennyiben a rejtjelző eszköz biztonsága megköveteli vagy működtetési szabályzata és kezelési utasítása ezt előírja, a rejtjeltevékenységet folytató szerv új rendszerengedélyt kér.(161/2010. Kormányrendelet, 2020)

A nagyobb nehézséget véleményem szerint a kiképzési célból **gyakorlatokon** vagy **katonai műveletek** infokommunikációs támogatása céljából üzemelő számítógépek és rejtjelző eszközök telepítése jelenti. Szerencsére a jogszabály lehetővé teszi, hogy telepíthető körülmények között eltérjünk a stacioner rendszerek üzemeltetéséhez előírt fizikai védelmi intézkedésektől. A 161/2010 kormányrendelet korábban már idézett 28. § (3) szerint a szervezet biztonsági vezetője által meghatározott védelmi intézkedések alkalmazásával minősített adat biztonsági területen kívül is feldolgozható.

A Kormányrendelet 22. § (7) szerint a nemzeti minősített adatot kezelő elektronikus rendszert biztonsági területen kívül, adminisztratív zónában, a biztonsági vezető által megjelölt helyszínen, kizárólag személyes felügyelet alatt lehet üzemeltetni.

A rejtjeltevékenység telepíthető körülmények közötti végzésére az MH Központi rejtjelfelügyelete az általa kiadott Magyar Honvédség rejtjelszabályzatában (Rj/41) részletesen szabályozta az üzemeltetés fizikai, adminisztratív és elektronikus biztonsági feltételeit. Sajnos a szabályzat minősített, így annak tartalmát jelen dolgozatomban nem áll módomban vizsgálni. A rejtjeltevékenységért felelős és a feladatokat végrehajtó állomány a részletszabályozásra támaszkodva hatékonyan és biztonságosan végre tudja hajtani a rendszer üzemeltetéséből rájuk szabott feladatokat.

A törvények és Kormányrendeletek mellett a rejtjeltevékenység valamennyi helyszínére kell egy helyi szabályozót, helyi rejtjelszabályzatot készíteni, amely a magasabb szintű szabályozást kiegészítve, pontosítva biztosítja a helyi rejtjeltevékenység végzésével kapcsolatos valamennyi részlet azonosítását. A rejtjelző eszközök kezelésének, őrzésének, szállításának, javításának, az azokkal folytatott rejtjelző munka ellátásának biztonsági követelményeit a rejtjeltevékenységre vonatkozó biztonsági dokumentáció tartalmazza. A rejtjelző eszközhöz kiadott speciális biztonsági követelményeket az eszközhöz kiadott működtetési szabályzat tartalmazza.

A fenti elemzésekből látható, hogy a rejtjeltevékenységet több szigorú jogszabályi előírás alapján, nagyon szűkre szabott keretek között lehet szabályosan üzemeltetni. Ennek oka, hogy a rejtjelzett adatok esetleges illetéktelen személy általi visszafejtése, az általunk védeni kívánt információ velünk szembenálló katonai szervezet tudomására jutása a szembenálló felet harcászati, hadműveleti vagy akár hadászati jelentőségű előnyhöz juttatná, a kompromittálódott információ jellegétől függően. A szigorú szabályozás egy ilyen incidens megakadályozása érdekében került kialakításra.

Telepíthető körülmények között a végponti munkaállomások biztonságos üzemeltetéséért felelős beosztottak már nincsenek olyan szerencsés helyzetben, mint a rejtjelző szakállomány. A Kormányrendelet ugyan megteremti a lehetőséget a biztonsági terület terepen történő kiváltására, részletszabályozást viszont csak annyiban biztosít, hogy a Biztonsági területen kívül a rendszer csak folyamatos személyes felügyelet mellett működhet. A konkrét védelmi intézkedések meghatározásának felelősségét a rendszer üzemeltetéséért felelős Biztonsági vezetőkre hárítja. Véleményem szerint a Biztonsági vezetők döntő többsége nincs szakmailag felkészülve a rendelet adta lehetőség információbiztonsági szempontból biztonságosnak nevezhető kihasználására. Álláspontomat az alábbiakkal támasztom alá.

A minősített adatot elektronikus rendszeren kezelő szerv biztonsági vezetőjével szemben támasztott követelmény, hogy felsőfokú végzettséggel rendelkezzen, minősített adatok kezelésének vagy védelmének területén szerzett legalább egy év szakmai gyakorlattal rendelkezzen vagy a Nemzeti Közszolgálati Egyetemen a minősített adat védelméről szóló törvény és a 90/2010 Kormányrendelet ismeretéből, gyakorlati alkalmazásából sikeres vizsgát tegyen. A Biztonsági Vezetők általában a katonai szervezet törzsfőnökei vagy parancsnokhelyettesei. Törzsmunkájuk során kezelnek minősített adatot, így a jogszabályban foglaltaknak az egy év szakmai gyakorlat meglétével felelnek meg. Gyakorlati ismereteik csak a legritkább esetekben terjednek ki gyakorlatok vagy katonai műveletek elektronikusan kezelt minősített adatai biztonságának menedzselésére és ha igen, gyakorlati tapasztalataik a helyszíntől, esetleg a műveletben részt vevő szövetséges erők eltérő jogértelmezéséből fakadóan nem egységesek.

A nemzeti minősített adatot kezelő elektronikus rendszert biztonsági területen kívül, adminisztratív zónában, a biztonsági vezető által megjelölt helyszínen, kizárólag személyes felügyelet alatt lehet üzemeltetni. Nemzeti „Titkos!" vagy „Szigorúan titkos!" elektronikus rendszer esetén a rendszer elemeinek meg kell felelnie a TEMPEST követelményeknek.

3.4.4.TEMPEST

Elektronikus információfeldolgozásra alkalmazott eszközöknél minden esetben fellép elektromágneses kisugárzás. Ezen kisugárzott jelek terjednek az éterben, és a sugárforrástól való elegendően kicsi távolság esetén átsugárzódnak a helység vezető anyagú elemeire (pl. fém fűtéscső, klíma berendezés fém alkatrészei) és továbbítódnak az infokommunikációs eszközhöz galvanikusan csatlakozó vezetőkön is. A hullámterjedés folyamatosan csillapítódik, jelfeldolgozás szempontjából hasznos jelnek a sugárforrástól való maximális távolsága több tényezőtől is függ, például az információt kezelő eszköz funkciójától, annak telepítésétől, fizikai biztonsági rendszabályoktól, az elektromágneses hullámterjedés környezeti feltételeitől. Ezért számos technikai rendszabályt kell alkalmazni a számunkra információbiztonsági szempontból veszélyes kisugárzás hatótávolságának csökkentésére. Mivel minden elektromos működésű eszköz bocsát ki magából elektromágneses jeleket, a fizikai jelenség lehetővé teszi, hogy megfelelő eszközök alkalmazásával a kisugárzott jelekből reprodukálható legyen az eszközön kezelt eredeti adat vagy annak egy része. Minősített adat elektronikus úton történő kezelése esetén a kompromittálódás elleni védelem egyik fő feladata a minősített adatot hordozó elektromágneses kisugárzás minimális szintre történő csökkentése, ami megnehezíti illetve megakadályozza az adat reprodukálhatóságát, annak illetéktelen kezekbe jutását. E módszer és a rá vonatkozó szabályok összefoglaló neve a TEMPEST.[67] A TEMPEST röviden: a „Titkos!" és „Szigorúan titkos!" minősítési szintű nemzeti minősített adat, valamint a „Bizalmas!" vagy magasabb minősítési szintű külföldi minősített adat bizalmasságának védelme érdekében kialakított biztonsági intézkedések – amelyek kiterjednek az elektromos és adatkábelek vonalvezetésére, a rendszer környezetében alkalmazható berendezésekre, árnyékolástechnikai megoldásokra, valamint csökkentett kisugárzású eszközökre – együttese, amelyet a rendszer valamennyi eleme vezetett és elektromágneses kompromittáló kisugárzásának csökkentése érdekében alakítottak ki. (161/2010. Kormányrendelet, 2020)

[67] forrás: https://www.nbf.hu/hasznos-informaciok/tempest/ letöltés ideje:2023.04.14.

Stacioner infokommunikációs rendszer esetén a TEMPEST követelményeknek való megfelelésre a rendszerelemeket akkreditálásra felkészítő szakállomány előre tervezhető időbeosztással, az akkreditáló Hatóság (NBF) által pontosan megszabott feltételek ismeretében tudja előkészíteni.

Az NBF a nemzeti TEMPEST hatóság feladatainak keretén belül:

a) a kompromittáló kisugárzás elleni védelem tekintetében felügyeletet és ellenőrzést gyakorol;

b) meghatározza és a minősített adatkezelést végző szervek részére elérhetővé teszi a TEMPEST biztonsági követelményeket;

c) ellenőrzi a rendszer és működési környezete TEMPEST megfelelőségét;

d) TEMPEST vizsgálatokat, méréseket végez;

e) a TEMPEST mérések alapján zónába sorolja a rendszer környezetét.

A fenti feladatokat technikai jellegükből adódóan elsősorban állandó telepítési helyszínen lehet maradéktalanul megvalósítani. A biztonsági területen telepítendő, minősített adatokat feldolgozó munkaállomások esetén, amennyiben a rendszer minősítési szintje alapján jogszabály előírja, a Hatóságnak TEMPEST mérést kell végeznie. A mérésről hiteles jegyzőkönyvet készít, amelyben egyértelműen meghatározza a helyszín zónába sorolását. A zóna besorolás alapján meghatározható, hogy a rendszer telepítési helyén milyen TEMPEST védelmi képességű infokommunikációs eszköz működése engedélyezhető.

Az eszközkiválasztás lehetőségeit tartalmazó táblázatot, illetve a telepítési előírásokat a minősített adatot feldolgozó rendszereknél alkalmazott eszközök, berendezések kiválasztására, telepítésére és üzemeltetésére vonatkozó, a Korm. rendelet 4. § (4) bekezdés b) pontjának felhatalmazása alapján készített „TEMPEST Biztonsági Követelmények-2” dokumentum tartalmazza. A dokumentum a NATO SDIP[68] 27-30 szabályozókban foglalt információk felhasználásával készült, melyek között minősített adat is van. A Hatóság által követelményként megszabott, táblázatban rögzített adatok így minősítettek, nyilvános forrásból nem érhetőek el, jelen dolgozatban sem jeleníthetők meg.

A táblázat lényegében azt tartalmazza, hogy a minősített adatkezelő infokommunikációs eszközöket az adminisztratív zóna határától (lásd: laktanya kerítés) befelé mért távolsága alapján milyen TEMPEST védelmi képességű eszközök alkalmazásával lehet

[68] NATO SDIP – NATO SECAN Doctrine and Information Publication
SECAN –Security and Evaluation Agency

szabályosan üzemeltetni. Egy ilyen módon kialakított rendszert viszonylag ritkán kell átalakítani. Az adminisztratív zóna határa és a területen belüli, a mérési eredményt befolyásoló tereptárgyak ritkán változnak meg. (Ha mégis, akkor ismételt TEMPEST mérést kell végezni a biztonságos üzemeltetés érdekében.)

Állandó telepítésű minősített adatkezelő rendszerek esetében fontos szerepe van a szándékos és véletlen vezetők vizsgálatának is. Az adatkezelés helyszíneiről részletes helyszínrajzot kell készíteni, amelyen valamennyi fémes vezetőt (fűtéscső, tápkábel, klímaberendezés fém részei,…) és minden infokommunikációs berendezést, a működtetéshez szükséges kábelek pontos vonalvezetésével ábrázolni kell. A Hatóság az engedélyeztetési eljárás során a rajzokat is vizsgálja.

A felesleges vezetékeket, vezetőket el kell távolítani a falakból, padlóból, mennyezetből. A szükséges vezetőket (fűtéscső, fémkeretek, klímaberendezés fém részei) potenciálját földkábellel a talajba le kell vezetni. A Hatóság a kompromittáló kisugárzás csökkentése érdekében megszabhat technikai rendszabályokat, például tápszűrők alkalmazását, speciális védőföldelés vagy speciális árnyékolás beépítését.

A rendszer akkreditálása előtt az állományilletékes parancsnoknak írásban ki kell jelölnie a helyszínre vonatkozóan egy úgynevezett „TEMPEST" felelőst. A felelősnek el kell készítenie a „A kompromittáló kisugárzás elleni védelemért felelős személy nyilatkozatát" amelyben a kijelölt személy azonosítja a teljes elektromágneses környezetet, felelősséget vállal annak jogszabályok szerinte megfelelőségéért. Ha a Hatóság a helyszínen telepített minősített adatkezelő hálózatra kiadja a rendszerengedélyt, a helyszínrajzban rögzített elektromágneses környezetet megváltoztatni csak az engedélyező hatóság egyetértésével szabad.

A stacioner hálózatok hosszú időn keresztül, folyamatosan ugyanazon a települési helyszínen működnek, ezért illetéktelen megismerési kísérletekkel szemben sokkal sebezhetőbbek, mint a mozgó vagy ideiglenesen telepített adatkezelő hálózatok.

Az illetéktelen személyeknek itt több idejük, lehetőségük van a rendszer esetleges gyenge pontjainak azonosítására, rejtett megközelítésére.

A rendszer infokommunikációs elemeinek a kezelt adatok minősítési szintjétől függően TEMPEST tanúsítvánnyal kell rendelkeznie. Ezek speciális árnyékolástechnikai követelmények (NATO SDIP-27/x) szerint tervezett, gyártott és a nemzeti biztonsági hatóságok tanúsítványával ellátott csökkentett kisugárzású, un. TEMPEST Level A, B, vagy C minősítésű eszközök. Az „A" minősítésű eszköz rendelkezik elektromágneses jelek nem szándékos kisugárzásának tekintetében a lenagyobb védelmi képességgel. A

feladatok rejtjelző támogatása könnyebben megvalósítható az általunk IP jelek rejtjelzésére használt TCE 600 sorozatú rejtjelző eszközökkel, mert ezek a típusok level „A” TEMPEST minősítéssel rendelkeznek.

Amennyiben a minősített adatot kezelő rendszer elemeit telepíthető körülmények között kell telepíteni, a telepítési feltételek megállapítása nem teljesen azonosak a stacioner rendszerek biztonsági feltételeivel.

Telepíthető elhelyezés esetén helyszíni TEMPEST mérés végzésére jelen technikai feltételek mellett a katonai műveletek dinamikáját is figyelembe véve általában nincs lehetőség. Mivel épített infrastruktúra elemek árnyékoló hatása sem érvényesül, ezért terepen általában a műveletek során kezelt minősített adatok legmagasabb minősítési szintjének megfelelő Tempest besorolású adatfeldolgozó eszközt, legtöbbször „TEMPEST” laptop számítógépet alkalmaznak. A hatóság az eszköz TEMPEST kategóriájának függvényében, általa megvizsgált általános telepítési rajz alapján ad engedélyt a minősített adat kezelésére. Az általános telepítési rajzon fel kell tüntetni, hogy a minősített adatot kezelő eszköztől milyen távolságra kell az adminisztratív zóna (ellenőrzött terület) határait megszabni, milyen módon védik a terület határait (kerítés, élőerő). Fontos az infokommunikációs rendszerben használt kábelek elvezetéseinek a pontos, egymáshoz képesti távolságának meghatározása. Az adatfeldolgozás során el kell különíteni a védendő (Red) és a már védett (Black) információkat feldolgozó részelemeket, kábeleket is.

3.5. Összegzés, következtetés:

- Jelen fejezetben azonosítottam és összehasonlítottam a Magyar Honvédség által jelenleg béke körülmények között használt Kormányzati célú infokommunikációs hálózatokat. Elemeztem a felhasználhatóságukat jogszabályi keretek adta lehetőségek és hatékonyság szempontjából.
- Megvizsgáltam a kereskedelmi célú infokommunikációs rendszerek felhasználhatóságát katonai műveletek infokommunikációs támogatásához, különös tekintettel a rendelkezésre állás és adatok biztonságos kezelése perspektívájából. Részletesen elemeztem a véleményem szerint minden releváns szempontból legalkalmasabb kommunikációs eljárás, a műholdas kommunikáció alkalmazhatóságának reális lehetőségeit. Véleményem szerint a Magyar Honvédségnek a haderőfejlesztési törekvései során mindenképpen vizsgálnia kell a Starlink vagy azzal hasonló szolgáltatásokat nyújtó rendszer igénybevételének

lehetőségeit a katonai műveletek infokommunikációs támogatása megvalósítása során.

- Ismételten hangsúlyoztam, hogy nem minősített, katonai jellegű adatok feldolgozása során minden estben szükséges a polgári rendszer saját, szabványokban meghatározott információbiztonsági protokolljainak betartása mellett egy „saját” , kifejezetten katonai szervezetek kizárólagos használatával létrehozott végponti titkosítás is.
- Elemeztem a Magyar Honvédségnél használt, Hatóság által engedélyezett rejtjelzési eljárásrendek sajátosságait nyílt források felhasználásával, olyan mértékben, amelyben a dolgozat bárki általi hozzáférhetősége engedte.
- Elemeztem a nem minősített adatokat rejtjelző eszköz közreműködésével kezelő infokommunikációs rendszer felépítésének technikai lehetőségét. Javaslatom szerint jelentős erőforrás igénybevétele nélkül alkalmazható a jelenleg a Honvédségnél is rendszeresített alapvetőnek számító rejtjelző eszköz, a TCE 621/C amely 1 Gbit/sec adatátviteli sebességre is képes. Ez a korábbi hasonló eszközökhöz képest nagyobb átviteli sebességre képes eszköz technológiai alapot biztosít egy katonai szervezet valamennyi infokommunikációs igényének egyidejű kiszolgálására, hipotézisem gyakorlati életben történő implementálásához.

Összefoglaló

Dolgozatomban a fentiekben értékeltem a rendelkezésre álló nyílt forrásokból kutatható NATO és hazai doktrínák infokommunikációs támogatással kapcsolatos szabályozási rendszerét, különös tekintettel az információbiztonsági követelményekre, ajánlásokra.

Az **első fejezetben** megállapítottam, hogy a NATO szövetségi infokommunikációs eszközrendszerei mellett, nemzeti érdekből, saját erőből tervezni és üzemeltetni kell a Magyar Honvédség katonai műveleteinek támogatásához szükséges infokommunikációs rendszereket, melyek nemzetközi szabványok szerint a működésük teljes spektrumában kompatibilisek egymással.

Megállapítottam, hogy a nem nyilvános adatok védelme erősen korlátozott. Az adatkezelés személyi, fizikai, adminisztratív és elektronikus információvédelmi feltételrendszere meg sem közelíti a minősített adatok kezelésénél alkalmazott védelmi rendszabályokat, eljárásrendeket. Véleményem szerint katonai műveletek végrehajtása során különösen külföldi alkalmazás esetén, amikor nem hazai információs infrastruktúrát veszünk igénybe adataink továbbításakor, a továbbítandó adatok védelméhez a hatályos jogszabályok alapján előírt szabályrendszer és védelmi eljárási rend nem elegendő.

Megvizsgáltam a hozzáférések hitelesítéséhez szükséges hitelesítési eljárásrend változásának a lehetőségét. Véleményem szerint a jövőben az egyre bonyolultabb jelszavak fejben tartásának követelménye teljesítése folyamatosan nehezedik, ezért a biometrikus azonosítás előtérbe kerülhet a személy hitelesítési folyamatban. Ennek jelenleg egyik akadálya a biometrikus azonosítók tárolásának GDPR szabályozása.

Az adatkezelési folyamat részelemeként vizsgáltam az infokommunikációs rendszerekben tárolt adatok tárolási helyének jelentőségét. Véleményem szerint a tárolás helye döntő fontosságú az infokommunikációs rendszerek rendelkezésre állási képességének biztosításához. A helyben tárolt adatokhoz lehet a leggyorsabban és biztonságosabban hozzáférni. Az információ távoli elérése bármilyen megvalósítás esetén magasabb technikai követelményeket, összetettebb eszközrendszer használatát igényli és az adatok továbbítása során nagyobb biztonsági kockázatokat is rejt.

A **második fejezetben** értelmeztem a Nemzeti stacioner rendszerek elemeit: A Magyar Honvédség Műveleti Vezetési Rendszert, A MH Kormányzati Célú Elkülönült Hírközlő Hálózatot, Honvédelmi Katasztrófavédelmi Rendszert, a NATO stacioner hírhálózat szervezésének, üzemeltetésének alapjait.

Megvizsgáltam a katonai műholdas rendszerek működtetésének szervezési és technológiai alapjait. különös tekintettel a szembenálló felek műholdak működését zavaró, megszakító vagy megsemmisítő lehetőségeire.

Elemeztem a Magyar Honvédségben jelenleg telepíthető hírrendszer és a kiépített, stacioner hírrendszer működtetésének alapjait.

Az infokommunikációs rendszerek szolgáltatásai, biztonsága, telepíthetősége és üzemeltetése összehasonlítása alapján javaslatot tettem a jövőbeli felhasználás optimális irányára: véleményem szerint jelenleg a legésszerűbb megoldás egy már működő műholdas infokommunikációs rendszer szolgáltatásának a bérlése.

Vizsgáltam a katonai műveletekkel összefüggésben keletkező, nem minősített adatok védelmének jelenlegi jogszabályi hátterét. Értelmeztem a jogszabályok lehetséges alkalmazhatóságát telepíthető infokommunikációs eszközök alkalmazása esetén. Véleményem és tapasztalatom szerint csak a nemzeti jogszabályi meghatározások pontosításával, a rádióforgalmazási eljárásrendek alapján kidolgozott cselekvési változatok és felhasználóbarát segédletekkel válhat képessé a KNBSZ hatósága a jogszabályban foglalt kötelmei teljesítésére és ami ennél is fontosabb, válhat rugalmasabbá a katonai műveletek tervezésének infokommunikációs vetülete.

Elemeztem a PKI (Nyílt kulcsú infrastruktúra) alkalmazásának lehetőségeit a Magyar Honvédségnél. A PKI technológia lehetővé teszi, hogy a digitális aláírás szolgáltatás mellett az adatok digitális tárolása vagy továbbítása esetén a készítő személy vagy szervezet privát kulcsával magát az egész dokumentumot titkosítsa. Ez a védelem ugyan nem felel meg a minősített adatok továbbítására előírt elektronikus védelmi intézkedések szintjének, tehát minősített adatokat ilyen módon nem továbbíthatunk, de a Magyar Honvédség működéséhez szükséges nem minősített adatokat, amelyek az adatok több mint 99% át teszik ki, védhetnénk ezzel az eljárásrenddel.

Összehasonlító elemzést végeztem a nemzeti illetve NATO minősített adatok védelméről szóló jogszabályok azonos és eltérő szabályairól, jogértelmezéséről.

A személyi biztonsági tanúsítványok meglétének ID card színével történő jelölése véleményem szerint ötletes és békétől eltérő állapotban is gyors, szakszerű ellenőrzést jelenthet, alkalmazását egy egységes értelmezés érdekében szabályrendszerben történő rögzítést követően javaslom. Az elvégzett kutatások és szakmai tapasztalataim alapján meglátásom szerint a kiképzési tervekben nem fordítanak kellő figyelmet a minősített adatok telepíthető körülmények közötti kezelésének gyakorlására, ami során pedig felszínre kerülnek az esetleges problémák, megoldandó részfeladatok valamint a

minősített adat előállításában, tárolásában, továbbításában a kidolgozó állomány tapasztalatokra tehet szert.

Javasoltam egy sok területen már használt de a Magyar Honvédségnél még nem elterjedt technikai eszköz alkalmazásának széleskörű bevezetését. A Degausserek megfelelően erős mágneses mezőt generálnak ahhoz, hogy a behelyezett merevlemezen vagy más mágneses adathordozón tárolt adatokat véglegesen és helyreállíthatatlan módon megsemmisítsék az adathordozó mágneses felületének újra rendezésével. Alkalmazásukkal elsősorban műveleti területen fokozni lehet a műveleti biztonságot azáltal, hogy a megsemmisítési eljárás meggyorsításával és egyszerűsítésével csökkentjük a katonai adatok illetéktelen megismerésének a lehetőségét.

Értelmeztem a minősített adatok kezelésére vonatkozó jogi szabályozást, amelyben megállapítottam, hogy a hang alapú minősített adatok definiálása jogszabályi szinten azonosítható módon nem valósul meg. Javaslatom szerint a jogi szabályozás kialakítása mellett technikailag az a legegyszerűbb és használható eljárásrend, ha a külföldi katonai műveletek adatforgalmát hang kommunikáció továbbítása esetén is minden esetben rejtjelző eszközök alkalmazásával valósítjuk meg.

Összehasonlítottam a NATO és nemzeti minősített adatok keletkezésével, minősítési eljárás rendjével kapcsolatos logi szabályozást és a szabályozás napi gyakorlati végrehajtását. Személyes tapasztalatom és kutatásaim alapján kijelentem, hogy a NATO minősített adatok keletkezésével és a minősítési eljárás rendjével, minősítő személyével kapcsolatban nemhogy a tagországok nem egységesek, de még a Magyar Honvédségen belül is az egymástól eltérő jogszabályértelmezések alapján különböző „napi gyakorlat” létezik.

Elemeztem a nem minősített adatok védelmével kapcsolatos jelenlegi korlátokat. Kutatási eredményeim valamint saját tapasztalataim alapján javaslatot tettem egy új adatvédelmi osztály létrehozására, amely jelentősen hozzájárulhat a katonai műveletek infokommunikációs rendszerein kezelt adatok illetéktelen személy általi megismerésével szembeni védelmének a növeléséhez. Javaslatot tettem a nem minősített adatok jogi korlátok miatti sebezhetőségének csökkentésére jogi és technikai megoldások alkalmazásával.

A **harmadik fejezetben** vizsgáltam a Magyar Honvédség által jelenleg béke körülmények között használt Kormányzati célú infokommunikációs hálózatokat. Elemeztem a felhasználhatóságukat jogszabályi keretek adta lehetőségek és hatékonyság szempontjából.

Megvizsgáltam a kereskedelmi célú infokommunikációs rendszerek felhasználhatóságát katonai műveletek infokommunikációs támogatásához, különös tekintettel a rendelkezésre állás és adadok biztonságos kezelése perspektívájából. Részletesen elemeztem a véleményem szerint minden releváns szempontból legalkalmasabb kommunikációs eljárás, a műholdas kommunikáció alkalmazhatóságának reális lehetőségeit. Véleményem szerint a Magyar Honvédségnek a haderőfejlesztési törekvései során mindenképpen vizsgálnia kell a Starlink vagy azzal hasonló szolgáltatásokat nyújtó rendszer igénybevételének lehetőségeit a katonai műveletek infokommunikációs támogatása megvalósítása során.

Megállapítottam, hogy nem minősített, katonai jellegű adatok feldolgozása során minden estben szükséges a polgári rendszer saját, szabványokban meghatározott információbiztonsági protokolljainak betartása mellett egy „saját" , kifejezetten katonai szervezetek kizárólagos használatával létrehozott végponti titkosítás is.

Elemeztem a Magyar Honvédségnél használt, a Hatóság által engedélyezett rejtjelzési eljárásrendek sajátosságait nyílt források felhasználásával, olyan mértékben, amelyben a dolgozat bárki általi hozzáférhetősége engedte.

Elemeztem a nem minősített adatokat rejtjelző eszköz közreműködésével kezelő infokommunikációs rendszer felépítésének technikai lehetőségét. Javaslatot tettem egy jelentős erőforrás igénybevétele nélkül alkalmazható a jelenleg a Honvédségnél is rendszeresített alapvetőnek számító rejtjelző eszköz, a TCE 621/C szélesebb körű alkalmazására. Ez a korábbi hasonló eszközökhöz képest nagyobb átviteli sebességre képes eszköz technológiai alapot biztosít egy katonai szervezet valamennyi infokommunikációs igényének egyidejű kiszolgálására, hipotézisem , gyakorlati életben történő implementálásához.

Az új tudományos eredmények tömören megfogalmazva, számozott listába szedve:

1. A katonai infokommunikációs rendszerek felépítésének vizsgálatával és működő polgári infokommunikációs rendszerek elemzésével valamint a fentiek összehasonlításával bizonyítottam, hogy a jelenlegi infokommunikációs eszközpark bázisán kialakíthatók nem homogén, a katonai művelet jellegétől függően egyedileg kialakított infokommunikációs támogató rendszerek, amelyek lehetőség szerint markánsan támaszkodnak a műveleti területen elérhető polgári információs infrastruktúra elemekre.Polgári infokommunikációs rendszerek információbiztonságának elemzésével bizonyítottam és javaslatot tettem arra, hogy külföldi alkalmazás esetén a nem minősített adatok továbbítása során, az adatok bizalmassága megőrzése érdekében rejtjelző eszközöket alkalmazzunk.
2. Bizonyítottam, hogy az Egységeknél a katonai műveletekhez kapcsolódó részfeladatok tervezésének és azok végrehajtásának műveleti biztonságát az általam javasolt új eljárás megnöveli, amennyiben a Magyar Honvédségen belül megfelelő jogszabályi környezet megteremtésével létrehozunk egy új biztonsági osztályt, amelynek az adatkezelését a jelenleg minősített adatokat kezelő rendszerek technikai eszközrendszerével védünk, de az adat adminisztratív szempontból, a minősített adatok védelméről szóló törvényben[69] nem érintett, nem terhelik a minősített adatok védelmére előírt, a katonai műveletek végrehajtása során esetenként igen nehezen betartható szabályok.
3. Személyes tapasztalatom és kutatásaim alapján igazoltam és rámutattam arra a jelentős problémára, hogy a NATO minősített adatok keletkezésével és a minősítési eljárás rendjével, minősítő személyével kapcsolatban nemhogy a tagországok nem egységesek, de még a Magyar Honvédségen belül is az egymástól eltérő jogszabályértelmezések alapján különböző „napi gyakorlat” létezik Dolgozatomban bemutatott, általam elemzett jogszabályi előírások értelmezése folytán bizonyítottam, hogy a katonai műveletek végrehajtása során a tervező, szervező és végrehajtó tevékenységek hatékonyságát szignifkánsan megnöveli a nemzeti adatok minősítési eljárásának újragondolása, különös

[69] 2009 évi CLV törvény a minősített adatok védelméről.

tekintettel az ideiglenesen felállított, fegyveres műveletek végrehajtására kialakított alegységek tekintetében minősített adatot elektronikusan feldolgozó rendszerek alkalmazása esetén. Kutatásaim, elemzéseim és szakmai tapasztalatom alapján bizonyítottam, hogy a működőképesség érdekében, műveleti körülmények között, különleges jogrendben a katonai vonatkozású adatok minősítésére bővíteni kell a minősítésre jogosult személyek körét.

Javaslataim, gyakorlati felhasználhatóság:

- **Javaslom, hogy a Magyar Honvédség infokommunikációs** támogató képessége növelése, érdekében minden szintű vezetési pont működésének infokommunikációs támogatása céljából tervezze meg és hajtsa végre a rendelkezésre álló polgári műholdas infokommunikációs rendszerek használhatóságának tesztelését. Jelenleg működő, kis erőforrásból is megvalósítható lehetőség az amerikai polgári „Starlink" hálózat. Amennyiben megvalósul és az üzemeltető is beleegyezik, későbbiekben lehetőség lesz a „Starlink" fokozott biztonságú változatának, a „Starshield" hálózatnak a vizsgálatára, melyet a szolgáltató kifejezetten kormányzati infokommunikációs rendszerek támogatására tervez létrehozni. Továbbiakban, amennyiben megvalósul, javaslom az Európai Unió IRIS^2 és hazai 4iG által felbocsátandó műholdak kapacitásának katonai célú igénybevételének lehetőségeit is vizsgálni.
- **Javaslom,** hogy a műveleti biztonság növelése érdekében a külföldi katonai műveletek végrehajtása során a keletkezett nem minősített adatok továbbítására is rejtjelző eszközök alkalmazásával kerüljön sor.
- **Javaslom,** hogy alegységek önálló alkalmazása esetén minősített adatokat elektronikusan feldolgozó rendszerekben a feladat végrehajtásának biztonsága érdekében, NATO mintára valamennyi felhasználó készíthessen nemzeti minősített adatot.

- **Javaslom** a 2009 évi CLV törvény valamint a végrehajtására kiadott kormányrendeletek NATO minősítési eljárásrendjére vonatkozó részének felülvizsgálatát, kiegészítését.Javaslom a minősített dokumentumok minősítésénél, ahol indokolt, a bekezdésenkénti minősítés módszerét alkalmazni. Eddigi tapasztalataim alapján a minősített adatok kezelése során, az oktatás szempontjából mindenképpen hasznos lenne, ha a magyar szabályozási rendszer ebben a tekintetben is megegyezne az USA illetve a NATO szabályozással. Jelenleg ugyanis, ha egy tankönyv vagy szabályzat néhány oldalon tartalmaz szenzitív információkat, amiért az egész dokumentum minősítve van. Ez lényegesen megnehezíti a tankönyv további nem minősített információkat tartalmazó oldalainak a megismertetését azokkal a hallgatókkal, akikkel csak a kevésbé szenzitív információkat kellene megosztani.

Irodalomjegyzék:

41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. Évi L.törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre,termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozókövetelményekről, Pub. L. No. 41, 2015 BM rendelet (2018).

55/2013 HM rendelet a Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózatának békeidejű üzemeltetési és felügyeleti rendjéről, valamint a központilag biztosított szolgáltatások igénybevételének szabályairól.

65/2013. (III. 8.) Korm. Rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. Évi CLXVI. törvény végrehajtásáról.

90/2010 Kormányrendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről, (2010).

161/2010. (V. 6.) Korm. Rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól, Pub. L. No. 161, 2010 Kormányrendelet (2020).

187/2015. (VII. 13.) Korm. Rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról, Pub. L. No. 187, 2015 (2021).

346/2010. (XII. 28.) Korm. Rendelet a kormányzati célú hálózatokról, (XII.28.).

359/2015. (XII. 2.) Korm. Rendelet a honvédelmi létfontosságú rendszerelemek azonosításáról, kijelöléséről és védelméről.

2001. Évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről, Pub. L. No. 108, 2001 (2022).

2009. Évi CLV. törvény a minősített adat védelméről, Pub. L. No. 155, 2009 (2022).

2011. Évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról, Pub. L. No. 112, 2011 (2023). https://njt.hu/jogszabaly/2011-112-00-00

2012. Évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.

2013. Évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról, Pub. L. No. 50 (2023).

2021. évi CXL. Törvény a honvédelemről és a Magyar Honvédségről, Pub. L. No. 140, 2021 (2023).

Attila Gulyás, & Horváth, A. (2013). GONDOLATOK A NEMZETI VSAT-KÉPESSÉG FEJLESZTÉSÉRŐL. *Honvédségi Szemle*, *3*, 10.

Bérczes, A., & Pethő, A. (2014). *Kriptográfia*. Nemzeti Közszolgálati Egyetem Vezető- és Továbbképzési Intézet.

Deák, J. (2005). Napjaink és a jövő háborúja. *Hadtudomány*, *1*. https://www.mhtt.eu/hadtudomany/2005/1/2005_1_3.html

ELEKTRONIKUS BIZTONSÁGI KÖVETELMÉNYEK az állami szervezetek minősített adatot kezelő rendszereinek engedélyezéséhez és üzemeltetéséhez, Pub. L. No. 30710- 3/556/2021 (2021).

ELEKTRONIKUS BIZTONSÁGI KÖVETELMÉNYEK az állami szervezetek minősített adatot kezelő rendszereinek engedélyezéséhez és üzemeltetéséhez, Pub. L. No. 30710- 3/475- 2/2023 (2023).

Farkas, T. (2016). A KATASZTRÓFAVÉDELMI ÉS VÁLSÁGKEZELÉSI TEVÉKENYSÉGEK ÁLTALÁNOS ELEMZÉSE AZ IRÁNYÍTÁS ÉS AZ INFOKOMMUNIKÁCIÓS TÁMOGATÁS TÜKRÉBEN. *Hadmérnök*, *XI*(3).

Farkas, T. (2020). Védelmi infokommunikációs hálózatok és rendszerek – szakmai felkészítés. *Hadtudományi Szemle*, *13*(1), 37–48. https://doi.org/10.32563/hsz.2020.1.3

Farkas, T., & Hronyecz, E. (2018). Infokommunkiációs szakemberek a védelmi szférában: Szakirányú továbbképzés. *Műszaki Tudományos Közlemények*, *9*(1), 75–78. https://doi.org/10.33895/mtk-2018.09.14

Gerőfi, S. (2017). A Magyar Honvédség vezetéstámogató rendszere alkalmazásának lehetõségei a XXI. századi kihívások tükrében. *Hadtudomány*, *XXVII*(3–4), 10. https://doi.org/DOI 10.17047/HADTUD.2017.27.3–4.96

Haig, Zs., & Kovács, L. (2012). *Kritikus infrastruktúrák és kritikus információs infrastruktúrák* (o. 1–298). Nemzeti Közszolgálati Egyetem.

Haig Zs. (2022). Kibertéri kognitív befolyásolás az információs műveletekben. *Hadtudományi Szemle*, *15*(2), 115–130. https://doi.org/10.32563

Isaszegi, J. (2005). A honvédség részvétele a nemzetközi békeműveletekben – Tények, lehetőségek, tapasztalatok. *Hadtudomány*, *XV*, 4.

Jobbágy, S. (2017). A MAGYAR HONVÉDSÉG KORMÁNYZATI CÉLÚ ELKÜLÖNÜLT HÍRKÖZLŐ HÁLÓZATA. *Hadmérnök*, *12*(3), 273.

Kardos, T. Z. (2021). Az Egységes Digitális Rádió-távközlő Rendszer (EDR) továbbfejlesztési lehetőségei. *Rendvédelem*, *10*(3), 12–18. https://doi.org/10.53793/RV.2021.3.2

Kovács, Z. (é. n.). A Magyar Honvédség harcászati rádiócsalád fejlesztésének helyzete a Zrínyi Honvédelmi és Haderőfejlesztési Program tükrében. *Hadmérnök*, *XVII*(2), 187–203. https://doi.org/10.32567

Kovács L. (2018). *A Kibertér védelme*. Dialóg Campus.

MAGYAR HONVÉDSÉG ÖSSZHADERŐNEMI HÍRADÓ ÉS INFORMATIKAI DOKTRÍNA, (2013).

Magyar Honvédség Összhaderőnemi híradó és Informatikai doktrina, Hír/4 Honvédelmi Közlöny (2013).

Magyarország alaptörvénye, (2011).

Magyarország Nemzeti Katonai Stratégiája, Pub. L. No. 1393, Kormány Határozat (2021). https://njt.hu/jogszabaly/2021-1393-30-22

Magyarország Nemzeti Kiberbiztonsági Stratégiája, Pub. L. No. 1139, 2013 (2013).

Megyeri L. (2016). Adatok bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása katonai információs rendszerek alkalmazása esetén. *Katonai Műszaki Közlöny*, *26*(2), 59–66.

Megyeri L. (2017). Kockázatkezelés, tudomány vagy kuruzslás? *Hadmérnök*, *12*(3), 198–209.

Megyeri L. (2018a). Az ország egységes távközlő hálózatának (OTH) igénybevétele katasztrófavédelemre. *Honvédségi Szemle*, *146*(4), 103–112.

Megyeri L. (2018b). Elektronikus információs rendszerek biztonsági menedzsmentje. *Műszaki Katonai Közlöny*, *28*(2), 66–80.

Megyeri L. (2018c). Secure maintenance of electronic information systems in public service. *Hadmérnök*, *13*(2), 415–426.

Megyeri L. (2023). Fizikai biztonság. In *Új tipusú kihívások az infokommunikációban* (o. 159–180). Ludovika Egyetemi kiadó.

Megyeri L. (2021). *Arcfelismerő rendszerek alkalmazhatósága a COVID járvány előtt és a járvány szigorított körülményei között* [Tudományos szakmai konferencia]. Új típusú kihívások a biztonságban, Budapest.

MH Szárazföldi Haderőnemének Harcszabályzata IV rész. Szakasz, raj ,kezelőszemélyzet, honvéd, (2013).

Muha, L. (2008). Az informatikai biztonság egy lehetséges rendszertana,. *ZMNE BJKMF*, *XVII*(4), 137.

Muha, L. (2009). *INFOKOMMUNIKÁCIÓS BIZTONSÁGI STRATÉGIA*. *4*(1).

Muha, L., & Krasznay, C. (2018). *Az elektronikus információs rendszerek biztonságának menedzselése* (o. 132). NKE.

Nagyné, T. (2019). Hogyan irjunk informatikai biztonsagi szabalyzatot? *Hadmérnök*, *XIV*(3).

A NATO SZÁRAZFÖLDI CSAPATOK HíRADÓ ÉS INFORMATIKAI RENDSZEREI KAPCSOLATÁNAK MINIMÁLIS MÉRTÉKE STANAG 5048, Pub. L. No. 69-27/NATO, 38 (2006), A HONVÉDELMI MINISZTÉRIUM HONVÉD VEZÉRKAR KATONAI TERVEZO FOCSOPORTFONÖKSÉG kiadványa.

Papp, B., & Munk, S. (2021). A MH Tábori vezetési és irányítási (C2) szoftverrendszer (HUNTACCIS) integrációs feladatai 1. *Hadmérnök*, *16*(2), 205–2019. https://doi.org/10.32567/hm.2021.2.14

Porkoláb I. (2020). Az aszimmetrikus hadviselés adaptációja. *Dialóg Campus, KÖFOP-2.1.2-VEKOP-15-2016-00001*. https://tudasportal.uni-nke.hu/xmlui/static/pdfjs/web/viewer.html?file=https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/15904/576_aszimmetrikus_hadviseles.pdf?sequence=7&isAllowed=y

Resperger I. (é. n.). A VÁLSÁGKEZELÉS ÉS A HIBRID HADVISELÉS. *A közszolgáltatás komplex kompetencia, életpálya-program és oktatás technológiai fejlesztése, KÖFOP-2.1.1-VEKOP-15-2016-00001*.

Somodi, Z., & Kiss, Á. P. (2019). A hibrid hadviselés fogalmának értelmezése a nemzetközi szakirodalomban. *Honvédségi Szemle, 147*(6), 22–28. https://doi.org/10.35926/HSZ.2019.6.2

Szádeczky T. Gergely L, & Zámbó, Alexandra E. (2017). Titkosítás és jog – gondolatok a titkosításhoz kapcsolódó jogi szabályozásról. *INFOKOMMUNIKÁCIÓ ÉS JOG*. http://real.mtak.hu/id/eprint/64557

Szeleczki, S., & Farkas, T. (2022). A Magyar Honvédség harcászati infokommunikációs hálózatainak korszerűsítési irányelvei. *Hadtudomány, 32*(1), 74–92. https://doi.org/10.17047/HADTUD.2022.32.1.74

Szendy, I. (2017). A hadviselés, mint tudományelméleti és tudomány-rendszertani kategória. *Magyar Hadtudományi társaság, 3–4*.

Thomas, T. (2006). *Hálózati biztonság*. Panem.

Tóth, A. (2015). *A hálózat nyújtotta képességmegvalósításának lehetőségei aMagyar Honvédség kommunikációsrendszerében.* [Doktori értekezés, Nemzeti Közszolgálati Egyetem]. https://tudasportal.uni-nke.hu/xmlui/static/pdfjs/web/viewer.html?file=https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/12350/T%c3%b3th%20Andr%c3%a1s%20%c3%a9rtekez%c3%a9s?sequence=1&isAllowed=y

Tudnivalók az adatvédelmi incidensek kezeléséről. (2023, január 26). https://www.naih.hu/tudnivalok-az-adatvedelmi-incidensek-kezeleserol

Warsaw Summit Key Decisions. (é. n.). https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_02/20170206_1702-factsheet-warsaw-summit-key-en.pdf

Publikációs jegyzék:

- 1. Megyeri, Lajos: Fizikai biztonság

In: Tóth, András (szerk.) Új típusú kihívások az infokommunikációban
Budapest, Magyarország : Ludovika Egyetemi Kiadó (2023) 210 p. p. 159

- 2. Megyeri, Lajos ; Mógort, Krózser Terézia: Létfontosságú rendszerelemek védelmének kérdései a SARS-CoV-2 tükrében

In: Koltay, András; Török, Bernát (szerk.) Járvány sújtotta társadalom : A koronavírus a társadalomtudományok szemüvegén keresztül,Budapest,

- 3. Megyeri, Lajos: Biometric identification for security purposes

HÍRVILLÁM = SIGNAL BADGE International Scientific Conference on Military Information Security 2021 pp. 79-87

- 4. Megyeri, Lajos: Az ország egységes távközlő hálózatának (OTH) igénybevétele katasztrófavédelemre.

HONVÉDSÉGI SZEMLE: A MAGYAR HONVÉDSÉG KÖZPONTI FOLYÓIRATA No.4. pp. 103-112. , 10 p. (2018)

- 5. Megyeri, Lajos: Secure maintenance of eletronic information systems in Public service

HADMÉRNÖK XIII. No.2. pp. 415-426. , 12 p. (2018)

- 6. Megyeri, Lajos: Elektronikus információs rendszerek biztonsági menedzsmentje

MŰSZAKI KATONAI KÖZLÖNY XXVIII.No.2. pp. 66-80. , 15 p. (2018)

- 7. Megyeri, Lajos ; Farkas, Tibor:KOCKÁZATKEZELÉS, TUDOMÁNY VAGY KURUZSLÁS?

HADMÉRNÖK 12 : 3 pp. 198-209. , 12 p. (2017)

- 8. Megyeri, Lajos: Adatok bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása katonai információs rendszerek alkalmazása esetén

MŰSZAKI KATONAI KÖZLÖNY 26 : 2 pp. 59-65. , 7 p. (2016)

- 9. Megyeri, Lajos: A Magyar Honvédség nyílt és a polgári elektronikus információs rendszerek működtetésének azonos és eltérő szabályai

HÍRVILLÁM = SIGNAL BADGE 7 : 1 pp. 91-104. , 14 p. (2016)
HADMÉRNÖK 10 : 2 pp. 98-107. , 10 p. (2015)