ZRÍNYI MIKLÓS
NEMZETVÉDELMI EGYETEM
HADTUDOMÁNYI DOKTORI ISKOLA

Kerti András alezredes

A vezetési és információs rendszer technikai alrendszerének vizsgálata különös tekintettel a minőségbiztosításra és az átvitelbiztonságra

doktori (PhD) értekezés

Tudományos témavezető:

Prof. Dr. Rajnai Zoltán mk. ezredes
egyetemi tanár

Budapest, 2010

Tartalom

Bevezetés

A korszerű hadviselés, a korszerűen felszerelt haderő sikeres tevékenységének egyik legfontosabb eleme, hogy rendelkezzen hatékony, a feladatok végrehajtását biztosító és támogató vezetési és irányítási rendszerrel. Ez a rendszer nem nélkülözheti a hatékony irányítási filozófiákat éppúgy, mint a vezetéshez szükséges technikai eszközök modernségét, fejlettségét, a béke- és a békeállapottól elérő helyzetek gyors változásához szükséges reagálási idő alkalmazkodását a vezetésben.
A 21. század technikai eszközeinek gyors fejlődése, a nagypontosságú fegyverek jelenléte, a kommunikációs és informatikai, az információs forradalom időszaka új vezetési elveket kíván, melyek szoros összefüggést feltételeznek, harmonizálnak a technikai rendszerek megfelelésével.

A Magyar Honvédség a vezetési és információs rendszer üzemeltetésével a haderő alkalmazkodási képességének feltételeit biztosíthatja akkor, amikor a missziós szerepvállalások fokozódásának idején egyrészt a külszolgálaton lévő kontingensek irányítási rendszerét igazítja a vezető nemzet szerepét ellátó parancsnokság rendszeréhez, másrészt a honi területen lévő csapatainak vezetési és irányítási rendszerét saját nemzeti érdekeinek védelme érdekében fenntartja. A két rendszer sok esetben eltérő vonásokat, jellemzőket hordoz, hiszen a missziós tevékenységek országhatárainktól távol folynak, a vezetés és irányítás elvi és technikai feltételei kompatibilitási hiányosságokat nem szenvedhetnek, vagyis a más nemzetek által alkalmazott elveket és módszereket éppúgy kell tudni alkalmazni, mint a kontingens belső működését biztosító, nemzeti szinten begyakorolt és elfogadott irányítási mechanizmust és technikai eszközrendszert. E területeken a rendszerek elsődleges feladataként kell meghatározni, hogy a modern technológián alapuló vezetéstechnikai eszközök biztosítsák a reális idejű információhalmazokat a parancsnok, a döntéshozók részére, másrészt vezetési elveinknek megfelelő technikai eszközpark álljon rendelkezésre a műveletek, missziós tevékenységek, békeműveletek speciális feladatainak végrehajtásához.

Feladataink végrehajtásának nem lehet azonban egyetlen feltétele a technikai eszközpark, a korszerű eszközrendszer, hanem az irányítási mechanizmus helyzetekhez adaptált működtetése is feltételét képezi a sikereknek. A feladatrendszerek változása, a technológia fejlődése maga után vonja a vezetési és irányítási rendszerek változtatását, módosítását, hiszen ez alapfeltételként jelentkezik a korszerűség, a hatékonyság realizálásának szintjén.

„*Napjainkban a szakmai közösségen belül a legtöbb polémia technikai részletkérdésekről folyik, ugyanakkor döntően az információs rendszer egyes alkotóeleme összetevőinek részletkérdéseiről, és nem a rendszer egészéről vitázunk. Természetesen itt is igaz az a mondás, hogy az ördög a részletekben lakik, a részletek lehetőségei azonban napjainkban szinte kezelhetetlenek. Ezért fontos, hogy találjunk egy fő irányvonalat, szakmai rendezőelvet, amihez hozzárendeljük a részleteket*."[1.] – írja doktori értekezésében Ternyák István, akinek gondolatmenetével egyetértek, és dolgozatom megírásához vezérelvként fogadok el. E gondolatsort kiegészítve egyrészt csapattapasztalataimmal másrészt kutatásaimmal megállapítottam, hogy az elmúlt mintegy 8-10 éves időszakban, több tudományosan megalapozott publikáció - *cikk, tanulmány, doktori értekezés* - készült a kommunikációs és informatikai szakterületekről, amelyek azonban megítélésem szerint csak technikai részterületeket érintettek, a teljes rendszer szabályozását, mint egységes területet azonban nem vizsgálták. Ehhez a vizsgálati körhöz hozzájárul az is, hogy egységes és hatályba léptetett szabályzatot kutatásaim lezárásáig, 2009 decemberéig sem a hazai, sem a szövetségesi rendszerben nem találtam. Igaz ez még akkor is, ha léteznek rész-dokumentumok a terület szabályzására, mint a NATO információ biztonságát meghatározó dokumentum, az MH Informatikai szabályzata, vagy éppen a 2009-ben megjelent MH Információbiztonsági politikája is. Alapvető problémaként látom tehát, hogy a korszerű hadviselés és a megváltozott feladatrendszerhez adaptált vezetési és irányítási filozófiát egységesítő szabályzás, fogalomrendszer és a technikai (technológiai) háttér összhangja hiányzik

Alapvető kutatási célkitűzések

1.) Kiindulva abból a tényből, hogy NATO-csatlakozásunk óta a felsőszintű szabályozás keretei - *a vezetési és irányítási rendszerek egyik alappillérét képező* -hírrendszer teljes egészére nézve hiányoznak, valamint kutatásaim lezárásáig a

szakmai felső vezetés a híradó, informatikai és információbiztonság területén megosztott, célként tűztem ki a témakörben született tudományos igényű publikációk, jogszabályok, és az államirányítás egyéb jogi eszközeinek, a nyílt formában elérhető szabályzatok, és nyílt forrásból származó NATO-dokumentumok feltárását, elemzését.

2.) A hírrendszert, mint a vezetési és irányítási rendszer technikai alrendszerét vizsgálva megállapítsam, hogy az elmúlt egy évtized alatt az alrendszer terminológiája, elemei és viszonyrendszere megváltozott-e, és amennyiben szükséges, az új elveknek és eljárásoknak megfelelően adaptációval, vagy szintetizálással egészítsem ki a korábbi elvrendszert. Ennek érdekében a feldolgozott dokumentumok alapján bemutassam, hogy a különböző szakirodalmak milyen modellek mentén vizsgálják, illetve tervezik, szervezik a vezetési és információs rendszer technikai alrendszerét (VIRTAR).

3.) A technikai alrendszerek funkciórendszerét, működőképességének hatékonyságát a minőség és a minőségirányítási rendszer alapvetően determinálja, ezért szükségesnek tartom annak bemutatását és vizsgálatát, hogy egy minőségirányítási szabványcsalád (pl.: az MSZ/EN ISO 9001:2009 és a hozzá kapcsolódó szabványok) milyen mértékben alkalmazható a VIRTAR vezetési és irányítási valamint szabályozási folyamatainak kidolgozásában.

4.) A vezetési és információs rendszer technikai alrendszerének elemei közül a legfontosabbként meghatározható átviteli utak szerepe a rendszer működése és szolgáltatásainak biztosítása szempontjából kiemelt fontossággal bír. Az átviteli út biztonsági kérdéseinek vizsgálta tehát olyan rendszer szintű funkcionalitást feltételez, mely biztosíthatja az információk hiteles és védett továbbítását a vezetési és információs rendszerekben, ezért értekezésemben be kívánom mutatni az átviteli út biztonságának szükségességét, valamint az információbiztonsági szabványok alkalmazásával javaslatokat dolgozzak ki az átviteli út biztonsága és incidenskezelése tekintetében.

Kutatói hipotézisek

1.) Az elmúlt időszakban végrehajtott missziós feladatok híradása nem a tábori hírrendszerre épült.

A kilencvenes évek elejéig a katonai stratégiákból fakadóan a katonai híradó rendszerekben elsődleges kiemelt szerepe volt a tábori hírrendszernek, amelynek

fejlődése a Magyar Honvédségben a rendszerváltáskor megállt. Az 1990-es évek közepétől napjainkig az MH csapatai több külföldi missziós feladatot is ellátták, amelyeknek híradó-. Információs- és adatátviteli feladatit csak kisebb részben oldották meg a meglévő, rendszeresített tábori eszközökkel. A kifejezetten missziók igények kiszolgálására kifejlesztett híradó-komplexumok nem tekinthetők „hadi" eszközöknek, mert a mobilitásuk és egyéb paramétereik (rázkódás-, por-, vízállóképességük, stb.) nem teszik őket erre alkalmassá. Ezek az eszközök inkább csak az állandó hírrendszer ideiglenes, kihelyezett részének tekinthetők.

2.) Az infokommunikációs szabályozás nem teljes körű

Az előző pontban felvázoltak azonban nemcsak technikai problémákat vetnek fel, hanem szervezésieket is. A tervezéssel és szervezéssel foglalkozó szakállomány nem volt képes autodidakta módon olyan hipotetikus kérdésekkel foglalkozni, mint a tábori vezetési és információs rendszer szervezési és megvalósítási kérdései. A vezetés és információs rendszer technikai megvalósítását három fő tárgy köré lehet csoportosítani:

- az adatok feldolgozása és tárolása (informatika),
- az adatok megjelenési formáinak (hang, kép, mozgókép, stb.) átvitele,
- és a két rendszer biztonsági kérdései.

Jelenlegi szabályozásban egy 1993-ban kiadott és érvényben levő szabályzat[1], valamint a 2009 októberében megjelent Magyar Honvédség Információbiztonsági Politikája játszi szerepet. Híradás tekintetében vannak a részterületeket érintő szabályozások, mint például az egységes digitális rádió-távközlő rendszerről, a frekvenciagazdálkodásról, de nincs teljes „infokommunikációs" szabályzat, és sajnos ez idáig még az igény felmerülése sem tapasztalható a három szakterület egységes elv alapján történő szabályozásra.

3.) A hírrendszer vezetésének korábbi felső szintű elvei, módszerei aktualizálva megfeleltethetők napjaink VIRTAR rendszerének vezetésére, irányítására

[1] Ált/210

Az elmúlt tizenöt év missziós feladatai sikeresek voltak, melyeket nem lehetett volna végrehajtani az infokommunikációs rendszer megfelelő tervezése, szervezése, és működtetése nélkül. Ez megítélésem szerint a felső szintű központi szabályozás hiányossága ellenére csak úgy volt lehetséges, hogy a tervező és üzemeltető állomány szakmai tudása kiemelkedő szintű volt, az alkalmazók a tanult elveket helyesen alkalmazták. Számomra ebből a tényből az következik, hogy bár az elmúlt évek változásai jelentősek voltak, a szakterületek korábbi elveit adaptálni lehet a megváltozott körülményekre is, azokat nem elvetni, hanem megújítani kell. Szintén figyelembe kell venni azt a jelentős körülményt is, hogy a polgári életben az információ-technológiában lényeges, minőségi változások mentek végbe, melynek hatásait jelentősek a hírrendszerre nézve. Ilyen kiemelkedő hatásnak tartom a polgári élet szabványosítási törekvéseit, amelyek a Magyarországon is elfogadott nemzetközi szabványokban, és tárcaközi ajánlásokban csúcsosodik ki.

Kutatásaim tárgyának meghatározása

Kutatásaim során megvizsgáltam a **vezetési és információs rendszer** (VIR) **felépítését, valamint annak alrendszerei által gyakorolt hatásait** a kiszolgálására létrehozott infokommunikációs hálózatra, mely a technikai alrendszert képezi. Ezeket a vizsgálatokat az érvényben levő jogszabályokra, az államirányítás egyéb jogi eszközeire, az érvényben lévő szabályzatokra, tudományos munkákra valamint a Magyarországon is elfogadott nemzetközi szabványokra alapoztam.

A vezetési és információs rendszer technikai alrendszere (VIRTAR) jelenlegi szabályzási környezetének vizsgálata kapcsán különös figyelmet fordítottam arra, hogy **a szabályozási rendszerünket összevessem a szövetségi rendszer szabályzási struktúrájával**.

Megvizsgáltam a polgári életben elfogadott szabványosítási törekvések alkalmazási lehetőségét a VIRTAR vezetés-irányítási folyamatában.

Áttekintettem a **vezetési és információs rendszer információbiztonsági kérdéseit**, kutatásaimat **az átviteli út biztonságára**, mint a leginkább katonai, és legkevésbé kidolgozott szakterületre fókuszáltam.

Nem tekintettem a kutatás tárgyának

1.) **A polgári életben befejezettnek tekintett informatikai és távközlő (híradó) eszközök konvergenciáját.** Az elektronikus számítógépek kifejlődésével egy időben felmerült a feldolgozott adatok továbbításának a problémája is, mivel a kezdeti időkben az akkor még analóg híradó vonalak nem, illetve csak nagy technikai nehézségek árán voltak alkalmassá tehetők a digitális jelek továbbítására. Ebből kifolyólag a híradó és az informatikai technológia külön-külön fejlődött, és a híradó hálózatokban is teret kezdett hódítani a digitalizáció, a konvergencia, amely során megindult a két terület közötti közeledés. A véleményem szerint ez a konvergencia a polgári életben mára már befejeződött, amit a digitális átállás szabályairól szóló jogszabályok[2], valamint – *többek között* – az is bizonyít, hogy a háztartások jelentős részében egyetlen szolgáltató nyújthatja a TV, az Internet és a vezetékes telefonszolgáltatást, vagy az is, hogy az új típusú mobiltelefonokon már mindezek a szolgáltatások elérhetők. Bár a technikai lehetőségek adottak, a tábori hírrendszerek ezt a fejlődést hazai szinten visszavezethetően nem követték.

2.) A vezetési és információs rendszer megvalósításának technikai részleteit csak olyan mértékben tekintettem át, amely témám kidolgozásához elengedhetetlenül szükséges.

3.) **Az informatika és híradás egymáshoz való viszonyával, illetőleg konvergenciájukkal összefüggő technikai és definíció szintű összehasonlító vizsgálatokat** nem tárgyalom, mert megítélésem szerint ez a polgári életben már megtörtént, a védelmi kommunikációs hálózatok és a polgári hálózatok közötti kapcsolatok, és a szolgáltatóktól igénybe vehető lehetőségek azt mutatják, hogy a védelmi szférának is követnie kell ezt az irányvonalat, más alternatíva nem merülhet fel.

4.) Nem tekintettem a vizsgálatok tárgyának **a Magyar Honvédség tábori híradó és informatikai hálózatainak technikai elemzését**, elmaradottsági szintjének (lemaradásának), továbbfejlesztésének lehetséges irányait, a polgári hálózathoz történő csatlakoztatásának technikai megoldásait.

[2] Mint például: 2007. évi LXXIV. törvény a műsorterjesztés és a digitális átállás szabályairól.

Kutatásaim fő bázisai

A témába kidolgozott doktori (egyetemi doktori, kandidátusi, PhD) disszertációk, amelyeket alapvetően az Oktatási és Kulturális Minisztérium hivatalos doktori adatbázisából (www.okm.hu/phd), valamint a Zrínyi Miklós Nemzetvédelmi Egyetem honlapjáról töltöttem le.

A hivatkozott és feldolgozott NATO-dokumentumokat nyílt forrásokból, hivatalos kiadványokból és az Internetről letöltve szereztem be. Azok a jogszabályi utalások, hivatkozások, melyek dolgozatom törzsanyagában fellelhetőek a Honvédelmi Minisztérium, valamint a Magyar Közlöny hivatalos kiadványaiból erednek. Az értekezésemben felhasznált és idézett magyar és nemzetközi szabványokat a HM Fejlesztési és Logisztikai Ügynökség biztosította részemre, míg a kormányközi ajánlásokat, az Informatikai Tárcaközi Bizottság ajánlásait, a Közigazgatási Informatikai Bizottság ajánlásait a bizottságok hivatalos honlapjáról töltöttem le. Az anyaggyűjtés és -feldolgozás során törekedtem a lehető legfrissebb ismeretanyagok beszerzésére. Dolgozatom lényegi elkészülte után azokat a fontosabb forrásanyagokat, amelyek esetlegesen változhattak ismételten áttekintettem, frissítettem, így várhatóan azok az eljárás időszakában is hatályban lesznek. **Az anyaggyűjtést 2009. decemberében zártam le.**

Az idegen nyelvű hivatkozásokat saját fordításomban közlöm, a hitelesség érdekében ezeket a hivatkozás megjelölésén túl eredeti szövegként lábjegyzetben közzé teszem.

Értekezésemben minősített, illetve nem nyilvános információt nem használtam fel, az adatgyűjtést kizárólag nyílt és nyilvános adatokra alapoztam, nem vizsgáltam azonban azt, hogy a nyílt források, mint például az Internetre felkerülő adatok és tények, publikációk hordoznak-e „érzékeny" információkat.

1 Vezetési és információs rendszer

Az 1990-es évek első felében és még napjaink általános katonai gondolkodásában is egy le nem zárult paradigmaváltás[3] figyelhető meg, amely érinti a hadsereg társadalomban betöltött szerepét, feladatait, a hadtudományi kutatások irányainak és tartalmának változását, melyet determinánsan a polgári élet kutatási területeihez történő közeledés jellemez. A változás lényegét három fő okban látom:

- Hadikultúra váltás

A Varsó Szerződés (VSZ) felbomlása és a kedvező politikai folyamatok eredményeként hazánk NATO-tagsága nem egyszerűen az egyik szervezetből a másikba történő „átállásként" jelent meg.. Míg a VSZ-tagállamainak katonái a mozgás centrikus hadikultúra hadművészetét gyakorolták, a NATO katonai gondolkodói az anyag centrikus hadikultúra hívei voltak.[4]

- Terminológiaváltás

NATO-tagságunkkal a terminológiai, eljárásbeli változások nem csak az új „szövetségi nyelv" változását, hanem egy új kifejezés-rendszer, fogalomértelmezési szükségességet is magukkal hoztak. Az új definíciók jelentéseinek, tartalmának egységes értelmezése, vagy annak hiánya felületesen nem annyira szembetűnő jelenség, hiszen nagyon sok kifejezés hasonló tartalommal bír, azonban a két különböző „iskolán" (szövetségi rendszerben) felnőtt szakembergárda esetében, ha nem is teljesen eltérő, de esetenként nem is egymással azonos fogalmakat ért ugyanazon definíció alatt. Ilyen például a szakterületemről vett „információ technológia" amely jelenthet akár információ-feldolgozó eszközt (akár elektronikus akár nem), más számára azonban csak a szűken vett informatikai eszközparkot, eljárási módszert, megvalósítási lehetőséget jelenhet. Vagy másik példaként említhetném a kommunikáció kifejezést, ami technológiai szemléletű egyének

[3] A paradigma egy adott időszakban az adott tudomány művelői között kialakult és intézményesült közmegegyezés arról, hogy mi az adott tudomány tárgya, feladata, hol húzódnak a tudományosan érvényes ill. érvénytelen kérdésfeltevések közötti határok, ill. mely feltételek mellett lehet valamely álláspontot egyáltalán tudományon belülinek elfogadni.

[4] A hadikultúrákról részletesebben olvashatunk például: Kőszegvári Tibor: A hadtudomány fejlődése az ókortól a 21. századig. Egyetemi jegyzet Budapest 2008.

számára a kommunikációs rendszert, annak technikai és személyi feltételeit, más számára egy megjelenési lehetőséget jelent a külvilág felé.

- Alapvető feladat váltás

A rendszerváltás előtt egy „bipoláris" világban éltünk, amelynek alapvető katonapolitikáját a két fél szembenállása határozta meg, amelyben az I. és II. világháborúra is jellemző frontális jellegű hadműveleti és harcászati feladatokat vizionáltunk. Napjaink katonapolitikai, biztonságpolitikai szakértőinek és Magyarország hivatalos álláspontja szerint is: „A Magyar Köztársaságot belátható időn belül hagyományos jellegű fegyveres támadás veszélye nem fenyegeti, bekövetkezése hosszabb távon is alacsony valószínűségű."[2.] Ebből is következtetve a Magyar Honvédség elsősorban a nemzetközi szerepvállalásra, a különböző missziós feladatokra készül fel. Megítélésem szerint tehát a napjainkban a magyar katonai terminológiában keverednek a különböző, a rendszerváltás előtti és utáni fogalmak, definíciók meghatározások és azok értelmezése, nincs letisztult kép, kialakult azonos hivatalos szemlélet. A vezetési és információs rendszerek tekintetében a tisztánlátást tovább nehezítő tényezőnek tartom a bekövetkezett technikai-technológiai fejlődést, az informatikai és híradó rendszerek között végbe ment konvergenciát.

1.1 A vezetési és információs rendszer

A Vezetési és információs rendszerekkel kapcsolatos alapfogalmak megjelenését, kialakulást Fekete Károly tudományos jelleggel már feltárta doktori értekezése 1.1 fejezetében, [3.] ezért ezzel a továbbiakban csak akkor foglakozom, ha annak a tartalmát témám megértése szempontjából szükségesnek tartom. Értekezésem első részéhez alapproblémaként kezelem, hogy nincs egységesen kialakult és letisztult fogalom rendszerünk, amit a technikai rendszert tervező, szervező és használó állomány formálisan is egységesen értelmezne. Többször tanúja voltam szakmai vitájának, amely véleményem szerint csak azért alakult ki, mert egyes fogalmakat nem egyformán értelmeztek.[5] Álláspontomat ugyancsak alátámasztja Dr. Kassai Károly is az információ biztonsággal kapcsolatban:"… fogalmi keveredések, zavarok olvashatók a katonai lexikonokban is, melynek oka az új és a régi fogalmak ötvözése, illetve az angol kifejezések fordítási és honosítási

[5] A konkrét példaként hozom fel az „Information Assurance" és az "IT" fogalmak.

szándéka."[13.][4.] A fentieken túl egyes kifejezések az idők folyamán változhatnak is. E szempontból követendő példaként emelem ki azt a NATO-gyakorlat, amely szerint évente megtörténik a jelentősebb kifejezések felülvizsgálata, és ez alapján új kifejezés és rövidítés gyűjtemény kerül kiadásra.[6] A vázolt gondolatmenetből kiindulva: ahhoz, hogy a vezetési és információs rendszer vizsgálatát elvégezzem, fontosnak tartom definiálni a vezetési információs rendszert.

1.1.1 A vezetési és információs rendszer fogalma és felépítése

A vezetési és információs rendszer vizsgálatánál tisztáznom szükséges néhány alapfogalmat. A legfontosabb definíció-kategóriának a vezetést[7] tartom.

„A katonai vezetés az adott időszakban érvényben lévő, az ország védelmi helyzetére vonatkozó törvényi szabályozás, és a bevezetett rendszabályok alapján megvalósuló békevezetés, vagy háborús vezetés, az alárendeltek befolyásolásának folyamata a feladat eredményes végrehajtása érdekében. Lényege a parancsnoki akarat és szándék megvalósítása."[5.]

Hogyan mi módon fogja a parancsnok végrehajtani az alárendeltek befolyásolását? A vezetési rendszerrel, mely:

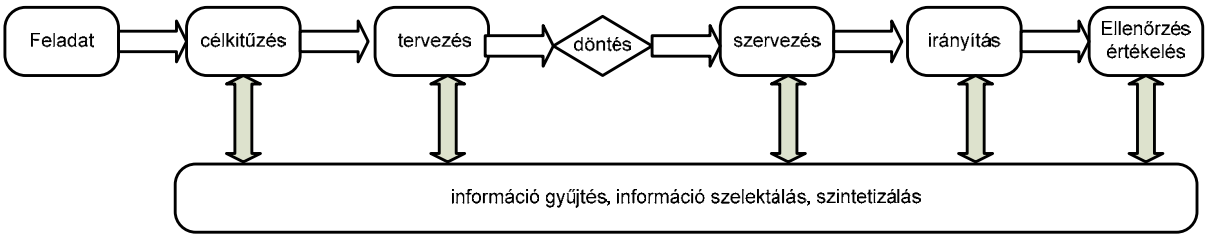
„Egy szervezeten belül a vezetés folyamatai, a vezetési módszerek és vezetési eszközök együttese". [6.] A vezetési rendszer felépítése tehát a parancsnok feladata, melynek kialakítását vezetési ismereteire, a vezetési módszerére vonatkozó elképzelések alapján határoz meg. „ A katonai vezetés akkor tölti be szerepét, ha azt felkészült és az egyszemélyi felelősséget vállaló parancsnokok (vezetők) gyakorolják, akik a módszerek, eljárások, vezetési stílusuk megválasztását, a végrehajtók motiválását a körülményekhez igazítják"[6.]. A definíció alapján meghatározhatjuk a vezetés részterületeit is, melyek: **„**információ gyűjtés, információ szelektálás, szintetizálás, célkitűzés, tervezés, döntés, szervezés, irányítás, ellenőrzés és eredménymérés (értékelés)"[5.].

Alapvetően jónak és elfogadhatónak tartom a megfogalmazást, azonban véleményem szerint két terület nem tűnik ki belőle: az egyik, hogy hiányzik a feladat-orientált jelleg beépülése a definícióba, vagyis a tevékenység meghatározásának feladata, joga, amit vagy az elöljárótól kap a parancsnok (mint például egy harcászati

[6] AAP 6, AAP 15, AAP 42.

[7] A vezetéstudomány és ezen belül a katonai vezetéstudomány külön szakterület, melynek a vizsgálatához az Összhaderőnemi doktrína fejezeteit veszem alapul.

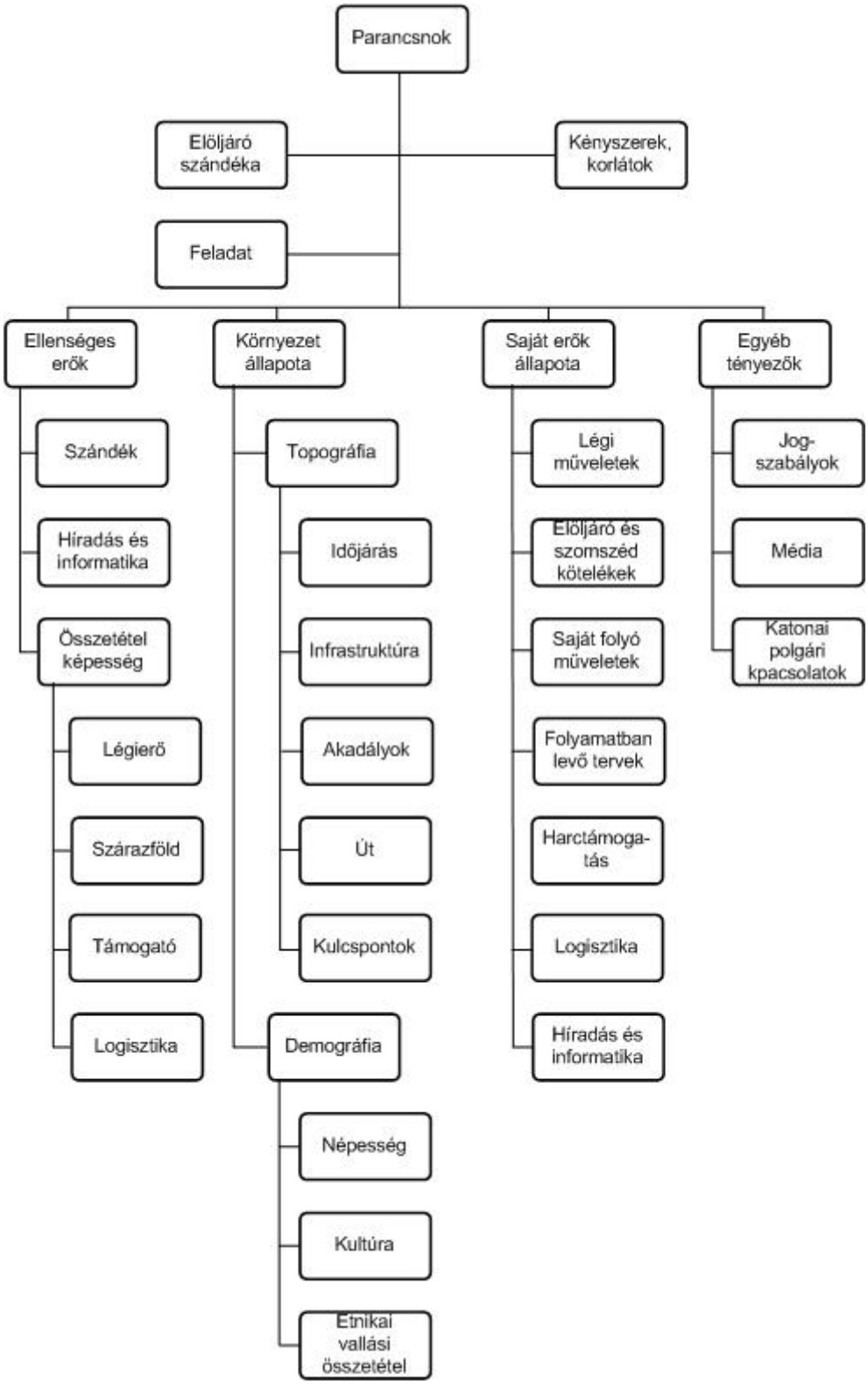
feladat), vagy az alaprendeltetéséből fakadóan kell megoldania (kiképzési, vagy fenntartási feladatok). Másrészt az idézett fogalomrendszer teljesen lineárisnak mutatja be a folyamatot, pedig a résztevékenységek egymásra hatása és visszahatása jelentős szerepet tölt be a vezetés folyamatában. Például, ha szervezésnél kiderül, hogy olyan gátló tényezők, akadályok merülnek fel, amelyek lehetetlenné teszik, vagy csak aránytalanul nagy áldozatokkal vállalható a célkitűzés megvalósítása, akkor az egész vezetési folyamatot át kell tekinteni, és új célkitűzéseket, terveket stb. kell készíteni. Másik példaként hozom fel az ellenőrzés és eredmény-mérés eseteit, amikor az észlelt negatív információk alapján lehet, hogy a szervezési és a tervezési folyamatot kell korrigálni. Az egész folyamat mozgatórugója tehát megítélésem szerint az információáramlás[8]. Egyrészről a vezetői folyamat is felfogható a különböző információk továbbításának, amikor tervek, utasítások, intézkedések eljuttatása az érintett feleknek, másrészt a végrehajtásról történő visszacsatolást, a tervezést és a szervezést is a különböző információkkal alá kell alátámasztani. A bemutatott folyamatokat, vagyis a vezetési és információs rendszerben végbemenő folyamatokat az 1. ábra segítségével kívánom szemléltetni.



1. ábra A vezetési és információs rendszer folyamatai

Ugyancsak nagyon fontos kérdésnek tartom azt is megvizsgálni, hogy milyen típusú információk gyűjtése szükséges, melyeket kell szelektálni és szintetizálni. Erre a kérdésre a parancsnok információs igényei adják meg a választ amit a **Hiba! Érvénytelen könyvjelző-hivatkozás.** szemléltet.

[8] Az információ olyan ismeretanyagot jelent, amelyet bármilyen formában továbbítani lehet. 2000. évi IV. törvény.



2. ábra A parancsnok információ követelményei

forrás: [1.]

Fontos megválaszolni tehát azt a kérdést, hogy a szükséges információkat ki és mi módon fogja szolgáltatni a vezetési rendszer számára. A válasz megadására Gorza Jenő is kísérletet tesz értekezésében. [7.] Válaszában a problémát abban

látom, hogy ő kifejezetten az adatfeldolgozás szemszögéből, a felső vezetés számára készített KGIR rendszer felépítése alapján modellezte az információ-szolgáltatást (3. ábra). Megítélésem szerint alapnak kell tekinteni, hogy a vezetési szintek információs igénye azonos, ezért az általa leírt haderő tervezési információs rendszer legfeljebb a középvezetői szint felett jelenik meg. Ennek példája a személyügyi adatgyűjtő rendszer, mely a parancsnoknak többek között harcértéki adatok szolgáltatásával válik szükségessé a hadműveletek során.

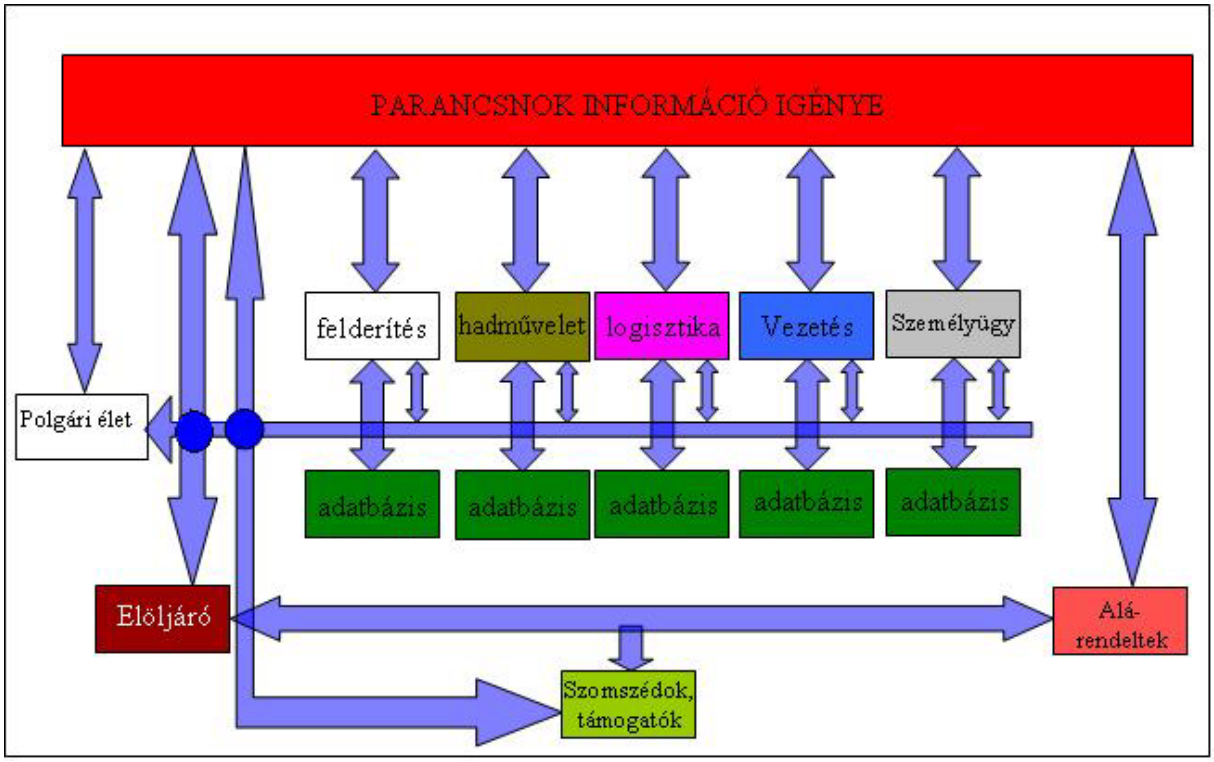
3. ábra A funkcionális alrendszerek és a vezetési információs rendszer viszonya Gorza Jenő szerint

Forrás: [15.][7.]

A hivatkozott ábra és szöveg pontosítását és értelmezését azonban fontosnak tartom. Egyrészről a szerző kifejezetten „nagy gépes” rendszerben gondolkodott, és ebben egy nagy összefüggő adatbázist, mint információ szolgáltatást képzelt el, viszont a jelenlegi hálózati elrendezésben az általa funkcionális rendszereknek nevezett elemek a parancsnoksági szinten saját (külön) adatbázissal rendelkeznek. Természetesen ez nem zárja ki a Gorza Jenő által leírt és megvalósított rendszert, ezek azonban csak az országos szintű feladatok ellátása során a legmagasabb vezetési szinten jelennek meg.

Másik pontosításként emelem ki, hogy az általa vázolt sémában az adatbázis fix rendszernek tűnik, nincs ki- és bemeneti relációja, pedig véleményem szerint ez is az idő függvényében dinamikusan változó elem. Ez biztosíthatja csak, hogy a

felhasználók az új, friss adatokat kaphatják az elöljárótól, az alárendelttől és saját törzsük más szakirányú munkatársaitól, vagy éppen a szomszéd és támogató alakulatoktól, valamint a külső (civil) környezetből. Ezért, figyelembe véve és továbbgondolva Ternyák István által közölt információ követelményeket és a Gorza-féle struktúra alapjait, meggyőződésem, hogy a 4. ábra jobban fejezi ki a vezetési és információs rendszer elemeit és annak kapcsolatait.



4. ábra A vezetési információs rendszer felépítése

Az ábrából látszik, hogy a parancsnok számára a különböző információkat alapvetően az elöljáró és alárendeltjei, valamint a törzs különböző beosztású tagjai saját adatbázisaikra és információs kapcsolataikra támaszkodva szolgáltatják. Az ellenségre és a környezetre vonatkozó adatokat a felderítési rendszer, a saját erőkre vonatkozó adatokat a hadműveleti, logisztikai, és személyügyi rendszer, a saját csapatok vezetését a híradó és informatikai rendszer biztosítja. Természetesen ezek az alrendszerek akár még kisebb alrendszerekre is bonthatók, attól függően, hogy milyen mélységben és céllal kívánjuk vizsgálni a rendszert. Az, hogy ezeknek az információs alrendszereknek mi az adattartalma, nagy részben függ a feladat jellegétől, a parancsnok szándékától és a törzs szervezetétől. A törzs szervezete függ az alegység, illetve egység alaprendeltetésétől és nagyságától, valamint attól, hogy a különböző szervezeti elemeket a kötelék vezetése mely szervezetei elemben

tervezi alkalmazni. E meghatározások működésmechanizmusát egyszerű belátni, ha például egy század, illetve a dandár vezetési rendszerét vetjük össze, vagy ha a frekvencia menedzsment feladatainak változását vizsgáljuk a különböző szervezetek között, amelyet Ternyák István is elemez doktori értekezésében [1.]. Egyértelműnek tűnik tehát azon tény, amely szerint minél magasabban helyezkedik el a parancsnok a vezetési struktúrában, annál több információra van szüksége előírt feladata megfelelő végrehajtásához.

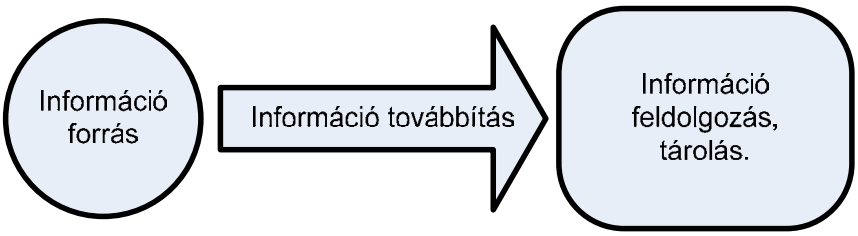
Azt viszont már nehezebb belátni, hogy bármely szinten elhelyezkedő parancsnoknak ugyan olyan fajta információkra van szüksége csak más, esetleg „kisebb" adattartalommal. Abban az esetben, amikor a szakaszparancsnok parancsot kap elöljárójától az egyértelműen vezetési és irányítási információnak minősül, amikor viszont figyelembe veszi alegysége lőszerkészletét, az már logisztikai információ, ha azonban az ellenségről megfigyeléseket gyűjt, az felderítési információ. Természetesen ezeknek az információknak a nagysága egység és magasabb egység szinten már azt eredményezheti, hogy nem elég egyetlen ember a feldolgozásukhoz, hanem több emberből álló törzs összehangolt munkájára van szüksége a parancsnoknak az információk szakszerű szolgáltatása érdekében. Azonban bármilyen nagy is a törzs, annak feladata, hogy a parancsnok számára a szükséges információkat előállítsa a feladat végrehajtása érdekében. Vagyis megállapíthatjuk, hogy az információt szolgáltató alrendszer a törzs szakbeosztású személyzete (felderítő, kiképző, hadműveleti, humán stb.).

Kérdésként merülhet fel, hogy az információk milyen módon jutnak el a megfelelő entitásokhoz? A jelentések, adatok, üzenetek címzettekhez történő eljuttatását és megfelelő feldolgozását a vezetési és információs rendszer számára szolgáltatást nyújtó ***híradó és informatikai rendszer*** feladata. Más szóval **a híradó és informatikai rendszer a vezetés és információs rendszer technikai alrendszere**.

Összegezve az eddigi definícióhalmazt megállapítható, hogy a vezetési és információs rendszer elemei közé sorolható az annak működtetésére vonatkozó **elvek, elgondolások**, az **információkat szolgáltató alrendszer**, valamint az információk áramlását, feldolgozását és tárolását biztosító **technikai alrendszer**.

1.2 A vezetési és információs rendszer technikai alrendszerének feladatai

A technikai alrendszer alapvető feladatait az 5. ábra mutatja be. Ezen az ábrán bemutatott modell alkalmazható a legkisebb részegységektől a teljes rendszer leírására, a számítógép belső architektúrájától az NII-ig[9]. Ugyanezzel a sémával ki lehet fejezni olyan bonyolultabb feladatokat mint a rendelkezésre bocsátás és az információ szolgáltatás, ezekben az esetekben az információforrás a számítógépben tárolt információ, a tárolás helye a megjelenített periféria (nyomtató, képernyő stb.) és az információ továbbítást a számítógép belső struktúrája biztosítja, példákat lehetne tovább folytatni.



5. ábra. A vezetési és információs rendszer technikai alrendszerének feladatai

Forrás: szerző

Az információs társadalom és így az információs társadalom hadseregének az egyik legnagyobb kihívása az információk biztonságának egy, a költségek és a lehetséges károk közötti arányos megvalósítása.

„Az információvédelmi mechanizmusok az információs infrastruktúra minden területére beépülve, egymással együttműködve fejtik ki hatásukat.”[4.]

Az általam információforrásként jelölt részegység a rendszer legkevésbé meghatározható eleme, amely minden egyes esetben más és más lehet, például lehet egy szenzor adata, egy felderítő jelentés, vagy éppen lehet egy másik információs rendszer. Fontos viszont, hogy ez az információforrás mennyire van az ellenőrzésünk alatt. Előfordulhat, hogy teljesen, részben, illetve teljesen független tőlünk. Éppen ezért az általam vázolt struktúrában az információbiztonság nem teljesen fedi le az információforrást, csak olyan mértékben garantálhatjuk az információforrás információinak biztonságát és megbízhatóságát, amilyen mértékben ellenőrzésünk alatt tartjuk.

[9] Hálózati és információs infrastruktúrák (networking and information infrasructures; NII).

Az információforrások az általuk szolgáltatott adatok jellegét tekintve a vezetés és információs rendszer technikai alrendszere szempontjából alapvetően kétfélék lehetnek: analóg és digitális jeleket szolgáltatók. Az analóg jelek lehetnek, mozgó- és állóképek, beszéd, írás. A digitális jeleket szolgáltató információs források lehetnek különböző szenzorok, illetve egy másik információs rendszer adatai is.

Mivel az információforrás majdnem minden esetben konkrét elemzést kíván ezért a továbbiakban nem kívánok az értekezésemben foglalkozni vele, elfogadom a hadtudományban elterjedt kategóriákat.[10]

A vezetési és információs rendszereket kiszolgáló technikai alrendszer általános elfogadott megnevezése jelenleg Híradás és Informatika Rendszer. *Értekezésemben, ahol ez lehetséges, tudatosan kerülöm ezt az elnevezést, ami nem azt jelenti, hogy új terminológiát szeretnék bevezetni, hanem azt, hogy a részegységek besorolása nem egyértelmű az informatikai és híradóeszközök konvergenciájának következtében. Vagyis a Vezetési és Információs Rendszer Technikai Alrendszere (VIRTAR) a vezetés és az információ szolgáltatás érdekében telepített információ és adat továbbító, feldolgozó és tároló eszközök (hardver és szoftver) és az őket telepítő és üzemeltető személyi állomány összessége.*

Az információtovábbítást, valamint a feldolgozást-tárolást végrehajtó egységek feladatait – *véleményem szerint a szakmai közösség által elfogadottan* – Ternyák István fogalmazta meg értekezésében a következőképpen: „Az a tudomány, amely az információk keletkezésének, kezelésének és felhasználásának elméleti és gyakorlati megvalósításával és eszközrendszerével foglalkozik az informatika. Az információs rendszer „nyersanyagait" azonban nemcsak felhasználni – feldolgozás, tárolás, megjelenítés, elosztás, stb. -, hanem továbbítani is kell. A rendszer, amely a különböző formában megjelenő híreket, adatokat, stb. továbbítja a híradó rendszer." [16.]

Ebből a megfogalmazásból azt a következtetéseket vonhatunk le, hogy a faxberendezések (papír alapú dokumentumok átalakítása elektronikus jelekké) és telefonok (szóbeli közlések átalakítása) ugyan olyan végberendezések, mint a számítógépek. Tapasztalataim szerint a Magyar Honvédségben uralkodó jelenlegi nézet szerint a telefon és a fax berendezések, valamint az őket összekötő hálózatok

[10] Ezeket az elfogadott kategóriákat például a Hadtudományi lexikonban lehet megtalálni.

a híradó rendszer részei, míg a számítógépek, a hozzájuk tartozó szoftverek és az őket összekötő hálózatok pedig az informatikai rendszer részei. Véleményem szerint ezen, egységesnek nem tekinthető álláspont a honvédségi eszközök különböző rendszereinek fejlettségi viszonyaiban keresendő. Meglátásom szerint a polgári életben az évek során sokat emlegetett informatikai és híradó rendszerek konvergenciája befejeződött. A polgári rendszerekben a különböző szolgáltatók egymással versenyezve ajánlanak komplex szolgáltatásokat, amelyekben bennfoglaltatik mind az infrastruktúra mind a tartalom is. A legújabb mobil készülékekkel pedig már képesek lehetünk az internetezésre és tévénézésre is a telefonáláson kívül. Miután hazánkban megfordult azon trend, amely szerint a katonai fejlesztést követi a civil fejlesztés, előzőekben ismertetett folyamat mérvadónak is tekinthető.

„A hadiiparra eddig jellemző trendek megfordultak, és ma már elsősorban nem a védelmi szféra termeli ki a kommunikációs és informatikai eszközök újabb generációját, hanem azok a polgári életben előbb megjelennek, mint a katonai alkalmazásokban. A kommunikációs eszközök gyors fejlődésével a védelmi szféra csak úgy képes lépést tartani, hogy rendszereikben a polgári életben megvásárolható termékek széleskörűen kerülnek alkalmazásra” [12.]

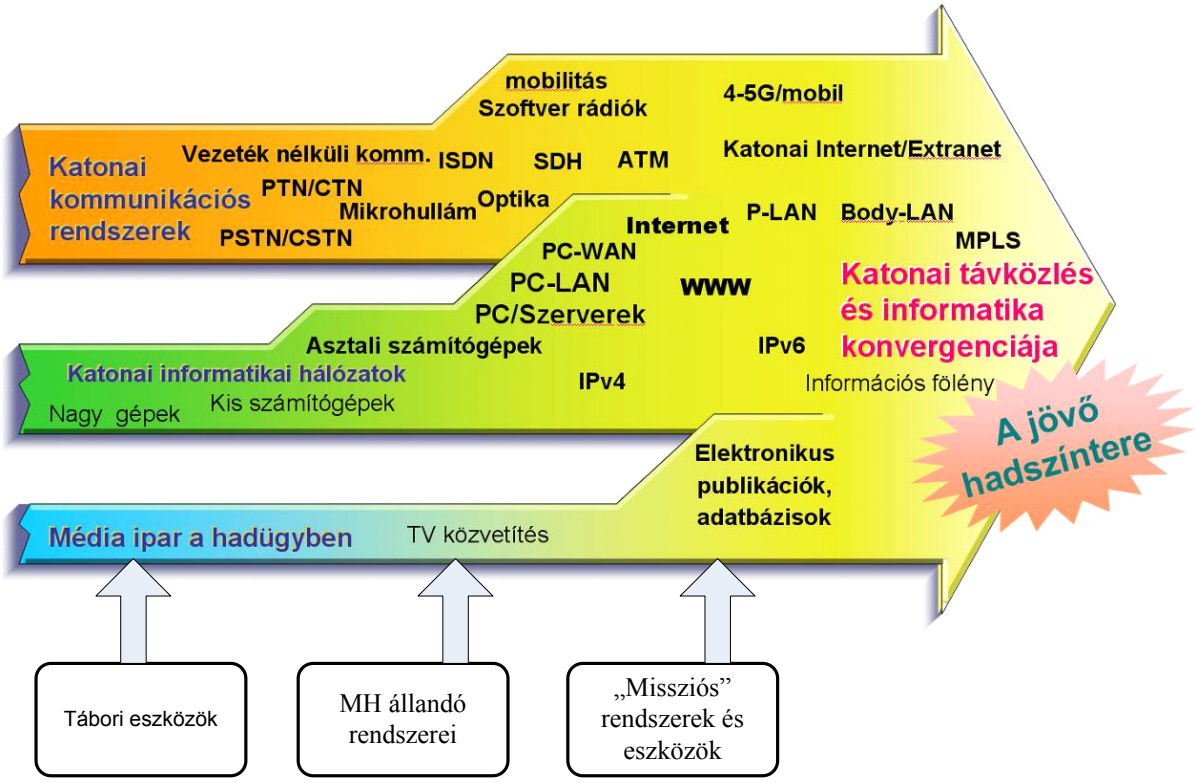
A honvédségi híradó és informatikai rendszerek konvergenciájára két alapvetően különböző modellt találtam kutatásaim során. Az egyik szerint mindig is megmarad valamiféle különállás a két rendszer között, a másik teljes összeolvadást ígér. Az első vélemény képviselője többek között Gorza Jenő, aki azt írja:

„Ugyanakkor a konvergencia véleményem szerint kizárólag az infrastruktúra területén értelmezhető, nem terjeszthető ki az alkalmazásokra.” [15.]

A másik vélekedésre példa Fekete Károly víziója, amelyet a 6. ábra mutat be. A fenti, polgári életre vonatkozó tények ismeretében ez az utóbbi az, amelyet az évek igazoltak. A következő ábrát kívánom felhasználni arra, hogy bemutassam a különböző MH szintű rendszerek eltérő fejlettségi szintjét. Véleményem szerint jelenleg három különböző szintű rendszerről beszélhetünk.

Az első az állandó telepítésű technikai alrendszer, amely a legfejlettebbnek tekinthető, összeköttetésben van a többi kormányzati rendszerrel. Esetükben már a tartalomszolgáltatás is kialakulóban van, erre példa megítélésem szerint a 74/2008.

(HK 15.) HM utasítás[11], amely gyakorlatilag egy olyan adatbázis létrehozását rendeli el, amely a legjobb gyakorlatok tapasztalatait dolgozza fel, mint tanulságokat.



6. ábra Katonai kommunikációs platformok fejlődése

Forrás:[13.]

A harmadik fejlettségi szinten a tábori rendszer található, amely a végbement politikai és gazdasági változások hatására megrekedt az 1980-as évek technológiai szintjén. Ezen megállapítást még akkor is reálisnak tartom, ha figyelembe vesszük az új URH rádiókat és a hozzánk egyéb úton (támogatásként) beérkezett RH eszközöket. Hiába érkeztek meg ezek az eszközök, hiszen nem illeszthetők a saját rendszerünkhöz, attól mintegy elkülönülve léteznek. Ebből adódóan nem létezik egy teljes, a mai kornak megfelelő komplex tábori rendszer, amely a vezetés és irányítási rendszerek technikai alrendszereként működhetne.

A második fejlettségi szint egy kis magyarázatra szorul. Az 1990-es évek közepétől hazánk részt vesz különböző missziókban és valószínűsíthető, hogy ezeket a missziókat nem lehetett volna sikeresen végrehajtani megfelelő vezetés és irányítási rendszer nélkül. Azonban a missziók vezetés és információs rendszerének technikai alrendszere szerintem nem tekinthető sem állandó rendszernek, sem tábori

[11] 74/2008. (HK 15.) HM utasítás A Magyar Honvédség műveleti tapasztalat-feldolgozó rendszere kialakításáról és működtetéséről.

rendszernek. Egyértelműnek tűnik számomra, hogy állandó rendszernek azért nem, mert az országtól távol, ideiglenesen üzemeltették, üzemeltetik ezeket a rendszereket. Tábori rendszernek viszont azért nem, mert ezek a hír-, és informatikai központok a misszió kezdetén letelepítésre és a misszió végén pedig elbontásra kerültek, közben nem kellett őket mozgatni, áttelepíteni mint egy „klasszikus" hadművelet során. Ennek következtében a fejlettségük is a kettő között van. Leszögezhető, hogy az MH-ba bekerült legjobb minőségű tábori eszközök kerültek összeépítésre a kereskedelemben kapható berendezésekkel.

Természetesen minél előrehaladottabbak a rendszerek fejlettsége, annál nehezebb elkülöníteni az „informatikai rendszert" a „híradó rendszertől". Véleményem szerint a vezetés és irányítás technikai alrendszerének fogalmát mint híradó és informatikai rendszert az Összhaderőnemi Doktrína fogalmazza meg helyesen:

„A híradó és informatikai rendszer magába foglalja a híradó és informatikai eszközállományt (hardver), az eszközöket működtető rendszer- és az alkalmazói feladatok ellátását elősegítő alkalmazói szoftvereket, az üzemeltetési és alkalmazási eljárásokat, a rendszerben rögzített, illetve továbbított adatokat, valamint az üzemeltető személyi állományt." [14.]

A megfogalmazásból pontosan kitűnik, hogy a híradó és informatikai rendszer egymástól elválaszthatatlan, azonban ezen előremutató definíció elfogadottságának magyar katonai körökben megnyilvánuló hiányát jelzi, hogy a Honvédelmi Minisztérium szervezetében jelenleg csak az informatikai szakterület képviselteti önmagát önálló szervezeti egységként (Informatikai és Információvédelmi Főosztály). [16.][12]

[12] A megfogalmazás csak az adatgyűjtés időszakára vonatkozik mert azóta ez a helyzet megváltozott.

1.3 A vezetési és információs rendszere technikai alrendszerének felépítése

1.3.1 A technikai alrendszer „hagyományos modellje”

A vezetési és információs rendszere technikai alrendszerének (VIRTAR) felépítésére, szerkezetének bemutatására a szakirodalomban nem találtam a teljes rendszert bemutató modellt, a korban legfiatalabb felépítési rendszert Rajnai Zoltán mutatta be a Doktori értekezésében[11.]

Amikor a VIRTAR itt bemutatott modellje kialakult, akkor ezt gyakorlatilag csak a hírrendszer jelentette és a számítógépes környezet még nem létezett, legfeljebb egyedi nagygépek álltak rendelkezésre,[13] valamint a hadászati elgondolás szerint csak szimmetrikus hadműveletekre[14] kellett felkészülnünk.

A vezetési pontok hírközpontjai

„A vezetési pont hírközpontja a vezetési pont szerves részét képezi. Rendeltetése az itt tevékenykedő parancsnok és törzs híradási igényeinek biztosítása a hírhálózatok felhasználásával. Összetételét az adott katonai szervezet szintje, a vezetési pont rendeltetése és a rendelkezésre álló híradó erők és eszközök határozzák meg.” [59.]

A közvetlen összeköttetések híradó vonalai

Azokat az összeköttetéseket sorolhatjuk ide, amelyek a parancsnoktól parancsnokig közvetlenül biztosítanak kapcsolatot, illetve azokat a hírközpontokat összekötő vonalakat, amelyek valamely szervezési meggondolás miatt az alap-hírhálózatot megkerülve kerülnek létesítésre. Ezekre tipikus példák voltak a rádió hírhálózat elemei.

Az alap hírhálózatok

„Az alap hírhálózat a hírrendszer azon része, mely alaphírközpontokból, az azokat összekötő híradó vonalakból áll és biztosítja a híradás (információcsere) feltételeit két vagy több vezetési szint részére.”[11.]

---

[13] Ezekről a nagygépekről a [15.]-n lehet többet megtudni.

[14] Szimmetrikus hadművelet, amikor a szemben álló felek, harcértéke, technikai felkészültsége, (közel) azonos.

A híradó tartalék

„A hírrendszer elemenként létrehozott híradótartaléknak nevezzük azokat a híradó erőket és eszközöket, amelyek a hírrendszer megbontása nélkül használhatók fel a veszteségek pótlására, a hírrendszer kiegészítésére, vagy az alárendeltek megerősítésére.” [59.]

Futár és tábori posta hírhálózat

A futár és tábori posta hírhálózat a legrégebbi és esetenként egyetlen eleme a hírközlésnek. Feladata az írott, és egyéb módon[15] rögzített információk eredeti formában történő továbbítása.

A híradás vezetési rendszere

A híradást tervező-szervező és vezető szervek folyamatos ráhatása a hírrendszer üzemeltetésére, az alárendeltek tevékenységére, valamint a híradó erők és eszközök célszerű alkalmazására a mindenkori helyzetnek megfelelően.

Híradó anyagi- technikai biztosítás rendszere

Híradó anyagi-technikai (logisztikai) biztosítás rendszerének feladata a technikai eszközök biztosítása, azok javítása, technikai kiszolgálása. A hírrendszer legellentmondásosabb része, mert bár a hírrendszer érdekében tevékenykedik feladatai egyértelműen a logisztika tárgykörébe tartozik. Dr. Sándor Miklós már 1999-ban így vélekedett:

„A híradó anyagi-technikai biztosítás csak és kizárólagosan a postaszabványú hírközlő eszközökre értelmezhető. A tábori, hadinomenklatúrás eszközök anyagi-technikai biztosítása a rendszerbe állítástól rendszerből történő kivonásig az elektrotechnikai szolgálatfőnökség feladata.” [18.]

A „hagyományos modell” kritikája

A hírrendszer kritikájaként az alábbi megállapításokat tehetjük:

- A híradás és az informatikai eszközök konvergenciája technikai szinten végbe ment, egymástól elválaszthatatlan egységet alkotnak. Ugyanakkor a Magyar Honvédség tábori híradó és informatikai eszközparkja

[15] Például CD-n, DVD-, Nyomtatott képen.

esetében, a meglévő technikai eszközök szintjén ez még nem történt meg.

- A NATO jelenleg a hálózat nyújtotta képességek kifejlesztésén dolgozik, amelynek adaptálása a magyar katonai vezetésnek is az egyik legfontosabb feladata.
- A jelenlegi katonai gondolkodásunkban a szimmetrikus hadviselés lehetősége ha nem is szűnt meg, de jelentősen háttérbe szorult. A csapatok elsősorban a különböző missziók végrehajtására és természeti katasztrófák leküzdésének támogatására készülnek fel.

1.3.2 A VIRTAR jelenlegi helyzete

A „hagyományos" modellnek az elavultsága ellenére is van egy nagy előnye, mégpedig az, hogy egységes egészként szemléli a rendszert. Az 1990-s évek elejétől a katonai munka területén is megjelentek a személyi számítógépek amelyeket az ezredforduló idején elkezdtünk helyi hálózatokba szervezni és jelenleg a legtöbb helyen a helyi hálózatok egy egységes országos hálózatban tudnak működni. A honvédségi VIRTAR tábori, missziós és állandó rendszerének fejlettségét az 6. árán mutattam be. Összegzésképpen megállapítható, hogy a katonai rendszerekben a híradás és az informatika konvergenciája még nem fejeződött be, ami kettőséget mutat minden rendszerelem tekintetében.

A VIRTAR vezetése

Bár a vezető szervek feladata és felelőssége, ezzel együtt eszközparkja is kibővült, de ezzel nem változott alapvetően a híradás vezetési rendszere, a szakmai irányítás továbbra is meghatározza a rendszer alkalmazhatóságát. Az adat gyűjtési időszakom lezárása után, 2010. február 20-án megalakult a Honvéd Vezérkar Főnök alárendeltségében a HM Híradó, Informatikai és Információbiztonsági Főosztály amely már a nevével is mutatja a VIRTAR szakmai vezetésének kettősségét (híradó és informatikai). A vezetési rendszer feladatait lehetőségét a későbbiekben még tárgyalom.

Vezetési pontok belső struktúrája

A végberendezések és a külső összeköttetések biztosítása a nyolcvanas években teljesen homogén volt (csak híradó eszközök voltak). A jelenlegi

rendszereinkben külön híradó és külön informatikai rendszerek vannak, amelyek felesleges redundanciát okoznak, hiszen külön-külön ki kell építeni mindkét rendszer hálózatát, külön kapcsoló elemek és központok szükségesek.

A végberendezések jellege is megváltozott, mára már teljesen kikoptak az állandó telepítésű és a missziós rendszerekből a géptávíró vonalak, valamint berendezések. A fax berendezések jelenleg még üzemelnek, de a polgári életben látható tendenciák szerint a jelentőségük csökkenni fog[16], szerepüket átveszik a különféle elektronikus üzenetküldési rendszerek. A laptopokat beépített, webkamerával, mikrofonnal, és hangszórókkal árulják, ami azt is jelentheti, hogy egyetlen hardver elem (a laptop), helyettesítheti az eddig több végberendezés (telefon, VTC, fax, számítógép) szerepét, amennyiben megfelelő szoftvertámogatást nyújtunk számára.

A tábori rendszerek híradó eszközei megmaradtak a nyolcvanas évek szintjén, és jelenleg nincs a rendszerünkben kifejezetten tábori informatikai eszköz sem. A személyes tapasztalataim alapján, amelyeket a különböző gyakorlatok megszervezésében és végrehajtásában szereztem, jelenlegi helyzetben a törzsek állománya előszeretettel használja az információtovábbítás céljára a saját tulajdonú és szolgálati mobiltelefonjait. Nagyon nehéz az állományt rávenni, a nehézkesen működő és gyenge minőségi mutatókkal rendelkező tábori híradó eszközök használatára. Ebből kifolyólag sokan (nem híradó és informatikai szakállomány) megkérdőjelezi a tábori eszközök fejlesztésének szükségességét. Mondván: minek a sok fejlesztés ha elég egy mobil telefon is. Az informatikai hálózatok kiépítésére a csapatok informatikusa a meglévő, általában asztali számítógépeket telepítik, amelyek nem a gyakorlótér körülményeihez lettek kitalálva, és ez miatt nagyon gyakori a meghibásodás.

A VIRTAR területlefedő rácsrendszere (alap hírhálózatok)

Az állandó VIRTAR nagytávolságú összeköttetéseit, a különböző stacioner gerinchálózatok képezik, amelynél szintén jelentkezik a híradó és informatikai kettősség.

[16] Például a Zrínyi Miklós Nemzetvédelmi Egyetemen a hagyományos fax berendezéseket felváltotta, a számítógépről üzemeltetett *fax szerver.*

A tábori területlefedő hírrendszer elemei jelenleg megtalálhatók a 43. Vezetés Támogató Ezred kötelékében, azonban ezekhez informatikai eszköz, hatásosan nem csatlakoztatható, vagyis a országos informatikai hálózat képzésére nem alkalmasak.

A Dr. Rajnai Zoltán által tudományos igényességgel bemutatott alap hírhálózati rendszer [11.] koncepciója ugyan nem évült el, néhány pontosítás azonban mára már szükségessé vált.

A legszembetűnőbb változás az állandó telepítésű rendszerek esetében látható. Az értekezés megírásakor, 2001-ben Magyarországon a különböző kormányzati szervezetek külön, saját igény szerinti zártcélú hálózatokat üzemeltettek. Napjainkban megmaradt ugyan a Magyar Honvédség zártcélú hálózata, azonban a jogszabályilag előírt különböző feladatok, mint például az ügyfélkapu működtetése miatt egyre több szállal kapcsolódik a kormányzati gerinchálózathoz. Megítélésem szerint ezért az MH zártcélú hálózata és EKG[17] hálózat közelít egymáshoz. Nem tartom elképzelhetetlennek, hogy a jövőben a kettő összeolvad. Ez viszont nem elsősorban technológiai, hanem szakmapolitikai döntés kérdése. Többek között ezt a folyamatot elemezte doktori értekezésében Pándi Erik is, aki jogszabályi oldalról mutatta be az összeolvadás folyamatát. [26.] Megállapítása szerint a zártcélú hálózatokról szóló 50/1998. (III.27.) Korm. rendelet „kusza" fejlődéstörténete[18] jól bizonyítja a technológiai összeolvadás tényét.

Az viszont már technológiai kérdés, hogy a meglévő nemzeti hálózatunkhoz hogyan tudunk csatlakozást biztosítani a szövetséges csapatok részére, mint a befogadó nemzeti támogatás egyik része, amennyiben a NATO csapatoknak feladatukat hazánk területén kell végrehajtaniuk.

A tábori alap hírhálózatok tekintetében véleményem szerint megváltozott a hadműveleti helyzet is. Megjelenésük idején bármelyik, Rajnai Zoltán által bemutatott rendszerről is legyen szó, egy a területet elfoglaló és megtartó frontális hadműveleti képességekre alapoztak a stratégák. A jelenlegi missziók tapasztalata viszont az, hogy különböző szomszédos alakulatok egymástól több tíz kilométerre levő bázisokon állomásoznak és onnan kiindulva végzik a feladatukat.

[17] Elektronikus Kormányzati Gerinchálózat.
[18] A jogszabály, megalkotása óta több mint tizenöt alkalommal került módosításra.

A terület lefedő hírrendszereknek az előnyük, hogy a csomópontjaikhoz több vezetési pont is tud csatlakozni, ezáltal elkerülhetjük a híradó vonalak újólagos telepítését csapatmozgások esetén. Ez az előny azonban akkor ha vezetési pontok nem folyamatosan, hanem szigetszerűen egymástól nagy távolságra helyezkednek el hátránnyá válhat, ha csak azért kell fenntartani a csomópontokat, hogy a messzebb levő csomópontok számára biztosítsák az összeköttetést, ugyanakkor azokhoz senki sem csatlakozik, Könnyen belátható, ez gazdaságtalan erőforrás-kezelést jelent.

Az általam taglalt probléma megnyugtató rendezéséhez megítélésem szerint katonai felsővezetői szintű döntés, vagy kormányzati politikai döntés szükséges, amely nem is kifejezetten a híradásra, hanem sokkal inkább a Magyar Honvédség feladataira vonatkozik. Hogy ez mennyire nem egyszerű kérdés álljon itt két idézet a nemzeti katonai stratégiából:

„A haderő szervezetét, felszerelését, infrastruktúráját, működési elveit és fejlesztését a biztonsági környezetből, kihívásokból levezetett célok és feladatok határozzák meg. Döntő hatást gyakorol a haderő transzformációjára a várható alkalmazási környezet, a legvalószínűbb feladat, a hadviselés elveinek módosulása, valamint a szövetségi és európai uniós igények” [2.]

„Bár a Szövetség elleni nagyméretű hagyományos agresszió esélye minimális, meg kell őriznünk a magas intenzitású műveletekben való részvétel képességét, annak érdekében, hogy képesek maradjunk a nagyobb kihívást jelentő hagyományos kockázatok kezelésére is. A Magyar Honvédség képességeit és struktúráját a legvalószínűbb műveletek figyelembevételével kell fejleszteni, és a legmagasabb követelményekkel járó feladatok ellátására kell felkészíteni.” [76.]

Az első esetben ez azt jelenti, hogy tapasztalati alapon az MH által eddig végrehajtott missziós feladatokból kell kiindulni. Ebben az esetben nem kell „erőltetnünk” a terület lefedő rendszer létrehozását, hanem a jól bevált „missziós konténereket” kell továbbfejleszteni.

A második esetben viszont a „legmagasabb követelmények” miatt ki kell alakítanunk a NATO követelmények szerinti területlefedő hírrendszert.

Közvetlen összeköttetések

Az elmúlt tíz évben nem vettem részt olyan gyakorlaton ahol, az alap hírhálózatok telepítésre kerültek volna, vezetési pontok hírközpontjai közvetlen összeköttetések felhasználásával biztosították az összeköttetést. A technikai színvonalukra ugyan az jellemző az hírhálózatra, informatikai vonalak biztosítására nem alkalmasak. Az informatika hálózatok összekapcsolását a szakállomány a meglévő stacioner központok felhasználásával oldotta meg.

A közvetlen összeköttetéseket megvalósító rádiórendszerek az MRR rádiók kivételével elavultak, hálózatképzésben szintén nem játszanak szerepet.

Futár és tábori posta hírrendszer

A béke időszakban a futár szolgálat feladatait a országosan az IRM látja el, a missziókná ezt a feladatot egyedi futárok veszik át. Meg kell azonban jegyeznem azt is, hogy ezen hálózat szerepe egyre csökken és tovább is fog csökkenni, amennyiben megvalósul az elektronikus küldemények hitelesítése,[19] ugyanis ebben az esetben már nem lesz szükség az eddigi az egyetlen hitelesként elfogadott eredeti, a kiadmányozási joggal rendelkező által aláírt, papíralapú dokumentum továbbítására. Valószínűsíthető azonban, hogy mindig lesznek olyan küldemények, amelyeket eredeti formában kell továbbítani a különböző felhasználóknak.

Az anyagi technikai biztosítás rendszere

A híradó és informatikai anyagi-technikai biztosítás rendszere jelenleg a logisztikai szervezetek feladatkörébe tartozik, mely azonban csak akkor működhet a rendeltetésének megfelelően, ha szoros együttműködés alakul ki a híradó és informatika vezetési rendszer és a logisztika vezetési rendszere között.

1.3.3 A NATO hálózat nyújtotta képességek (NNEC)

„2002 novemberében a NC3B ülésén a NC3B tagjai egyetértettek abban, hogy szükség van kifejleszteni egy NATO vonatkozású koncepciót, amely olyan nemzeti kezdeményezésekre épül, mint az USA hálózatközpontú hadviselés és az UK

[19] Az ezt megvalósító elektronikus aláírást biztosító rendszer a NATO szerveinél már kialakításra került, a MH-ban jelenleg kialakítás alatt van.

hálózat alapú képességek. Ezt a NATO koncepciót úgy nevezik, hogy NATO hálózat nyújtotta képességek".[20][19.]

Vagyis a NATO kommunikációs és információs infrastruktúráját meghatározó NC3B 2002 óta megkezdte a hálózatos rendszer kiépítésének tervező és szervező munkáját. Az ezzel kapcsolatos eredmények nem mindegyike kerül publikálásra, ezért a nagyközönség számára „láthatatlan" marad. A látható rész az interneten is közzétett „Allied Data Publication 34 (ADatP-34) NATO C3 Technical Architecture Implementation Handbook[21]" Maga a kézikönyv több kötetből áll, és folyamatosan előírt időrend szerint fejlesztik.

A NATO kezdeményezésétől függetlenül már többen leírták a kommunikációs rendszer hálózat alapú továbbfejlesztésének szükségességét. Erre példa Dr. Rajnai Zoltán doktori értekezése 2001-ből, amelyben azt írja:

„Napjainkban a haderőkben tevékenykedő törzsek és egységek, alegységek vezető állománya, a feladatok kidolgozásában és végrehajtásában közreműködők munkájuk során különböző irodai alkalmazású kommunikációs eszközöket (számítógépek, távközlő berendezések), rendszereket (LAN, strukturált hálózatok, stb.) használnak. Ezen törzsek, parancsnokok jogos elvárása, hogy hadműveleti feladatok előkészítése, kidolgozása és végrehajtása során a hadműveleti területen is képesek legyenek hasonló, esetenként még több szolgáltatás és adatbázis igénybevételére, mint béke elhelyezési körleteikben, helyőrségeikben."[20.]

Azonban nem csak a NATO, valamint tudományos oldalról, hanem kormányzati oldalról is megtörtént az új igényeket megvalósító képességek kialakítása szükségességének megfogalmazása:

„A fejlesztési feladatok fontossági sorrendjét a Magyar Honvédség professzionális, valamint a műveleti területre telepíthető, ott együttműködésre és működőképességének fenntartására alkalmas (expedíciós) jellegének erősítése határozza meg. Ezen belül az irányítási-vezetési-rendszerek fejlesztésének folytatása úgy, hogy azok illeszthetőek legyenek a kialakítandó hálózat alapú hadviselés képességhez."[21.]

---

[20] „At their meeting in November 2002, the NATO C3 Board (NC3B) agreed that there was a need to develop a NATO concept to adapt national initiatives such as the U.S. Network-Centric Warfare (NCW) and the U.K. Network Enabled Capability (NEC) to the NATO context. This NATO concept is referred to as "NATO Network Enabled Capability" (NNEC).

[21] http://194.7.80.153/website/book.asp?menuid=15&vs=3&page=ihb%2Findex.html.

Ennyi bevezető után felmerül az a jogos kérdés: tulajdonképpen mi is az NATO hálózat nyújtotta képesség (NNEC)? A kérdés megválaszolása csak első megközelítésben tűnik egyszerűnek, mert mindenki beszél róla, viszont az elérhető publikációk száma[22] korlátozott és a legtöbb csak ismétléséket tartalmaz. Ez sajnos akkor is igaz ha figyelembe vesszük, hogy a NATO a NNEC-nek külön honlapot tart fent az interneten.[23]

A NATO hivatalos megfogalmazásában a NNEC a következő[22.]:

„A NATO hálózat nyújtotta képességek (NNEC) a szövetség észlelő és technikai képessége, amely egyesítse a műveleti környezet alkotóelemeit a stratégiai szinttől (beleértve a NATO parancsnokságot is) a taktikai szintig a hálózati és információs infrastruktúrán keresztül[24].”

Azonban a NNEC nem kifejezetten csak katonai fogalom a NNEC koncepciójában az érdekelt felek[22.]:

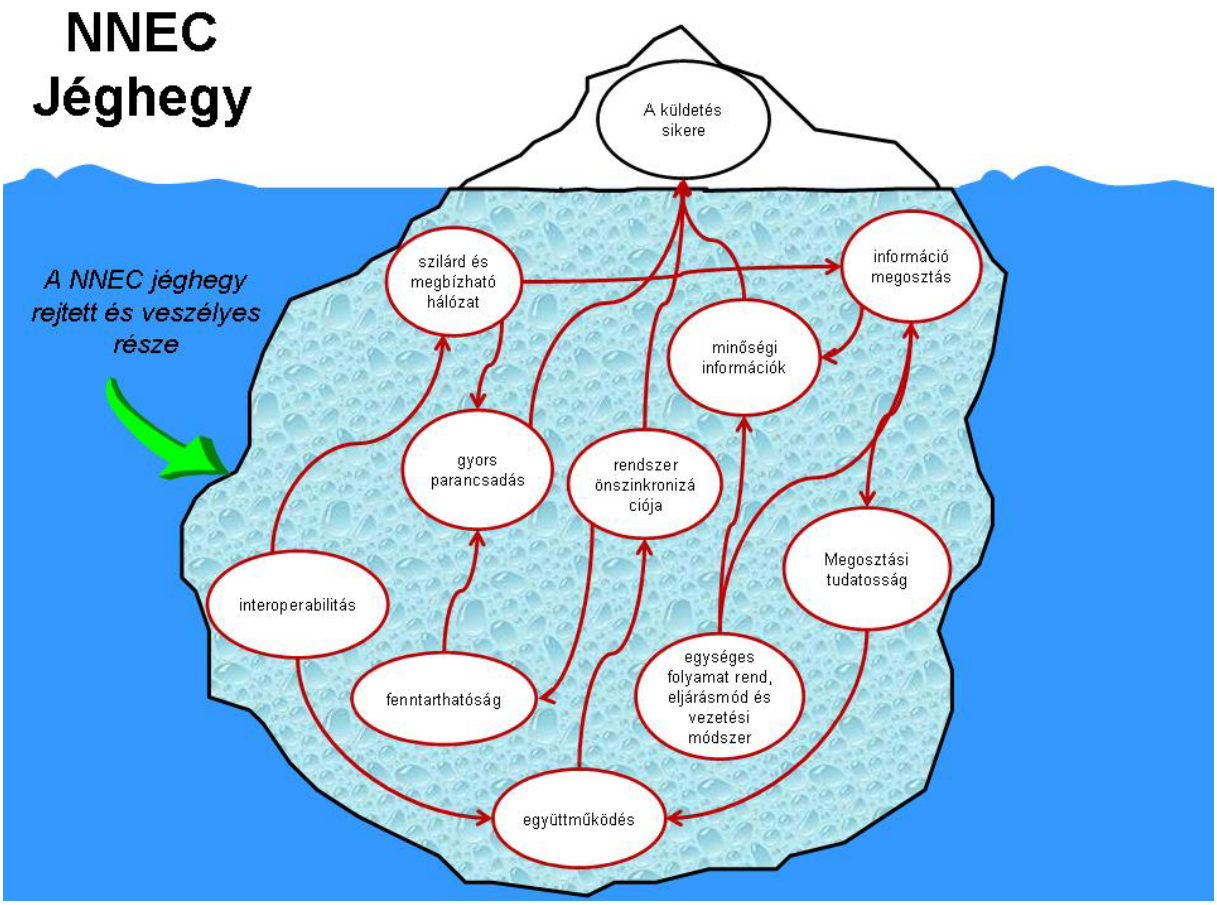
- a NATO szervezetei, a parancsnokságok, ügynökségek, civil és katonai szervezetei stb.
- A NATO-t alkotót nemzetek katonai és polgári szervezetei.
- A kutatás fejlesztés és a megvalósításában résztvevők, kutatóhelyek, egyetemek, iparvállalatok.
- A nem kormányzati szereplők, nemzetközi szervezetek.

A figyelembe véve a fentieket és feldolgozott irodalom alapján azonban úgy tudom a NNEC lényegét a legegyszerűbben megfogalmazni, hogy az információk hatásos és hatékony megosztásának a képessége, a missziók (feladatok) sikeres végrehajtása érdekében, a NATO-t alkotó nemzetek és a szervezetek között.

Megan Thum, a NATO Headquarters Supreme Allied Commander Transformation munkatársa a NNEC-et egy jéghegyhez (7. ábra) hasonlította amelynek a látható része a küldetés sikere a lényegi rész viszont víz felszíne alatt van és egy komplex rendszert tartalmaz amelynek a részei: Az információ

[22] Az elérhető publikációk alatt a nyílt publikációkat értem
[23] http://nnec.act.nato.int/default.aspx
[24] "NATO Network-Enabled Capability (NNEC) is the Alliance's cognitive and technical ability to federate the various components of the operational environment, from the strategic level (including the NATO HQ) down to the tactical levels, through a networking and information infrastructure (NII)."

megosztás, a szilárd és megbízható hálózat, a minőségi információk, a rendszer önszinkronizációja, az interoperabilitás, a fenntarthatóság, a gyors parancsadás, az együttműködés képessége, az egységes folyamat rend, eljárásmód és vezetési módszer.



7. ábra A NNEC „jéghegy”
Forrás: [23.]

A bemutatott ábrából látszik hogy a NNEC megvalósítása nem csak technológiai feladat. A technológia feladata, hogy támogassa a NNEC kialakítását, elősegítse az információkról a döntésekről a folyamatok gyorsaságáról szóló nézeteink fejlődését, valamint szükséges az együttműködés és valósidejű információközlés megvalósításához[22.].

Ruud van Dam a Holland Királyi Légierő vezérőrnagya egy 2006-ban tartott előadásán, a szükséges változtatásokat három egymással szoros összefüggésben levő terület köré csoportosította. Ezek a hálózat, az információ, és az emberi viselkedés amely tartalmazza a folyamatokat a szervezetet és az embereket. Vagyis az információ területén ki kell alakítani az információk egységét, a jelentések, parancsok, egyéb dokumentumok standardizálását, és ezek megfelelő továbbítási

metódusát, a szervezeteknél be kell vezetni az információ menedzsmentet. Az emberi viselkedés során egységesíteni kell a szervezeteket, a szervezetekben folyó munkát, a munkát meghatározó előírásokat, fejleszteni kell az emberek tudatosságát az egymásiránti bizalom, az információbiztonság, az információ felhasználás terén. A hálózat kialakítása során a feladat egy egységes elvek szerint létrehozott, szélessávú megbízható és megfelelő módon védett struktúra kialakítása.[24.]

Könnyen belátható, hogy ebből hatalmas munkából a VIRTAR állományának a legfontosabb feladata követelményeknek megfelelő hálózat megvalósítása és üzemeltetése.

Ruud van Dam a már idézett előadásában[24.] a NNEC kialakításához szükséges hálózatot úgy mutatta be mint a NATO hálózati és információs infrastruktúra kiegészítve a NATO nemzetek saját hálózati és információs infrastruktúrájával[25]. Véleményem szerint, figyelembe véve az előzőekben leírtakat is, figyelembe kell venni ezeken kívül még az egyéb szervezetek és a missziók hálózatát is. 8. ábra

8. ábra A NNEC létrehozásához szükséges hálózati struktúra vázlata

Fentieket összegezve mindenképpen feltehető a következő kérdés: milyen elemekből állhat össze a hálózat alapú vezetési és információs rendszer?

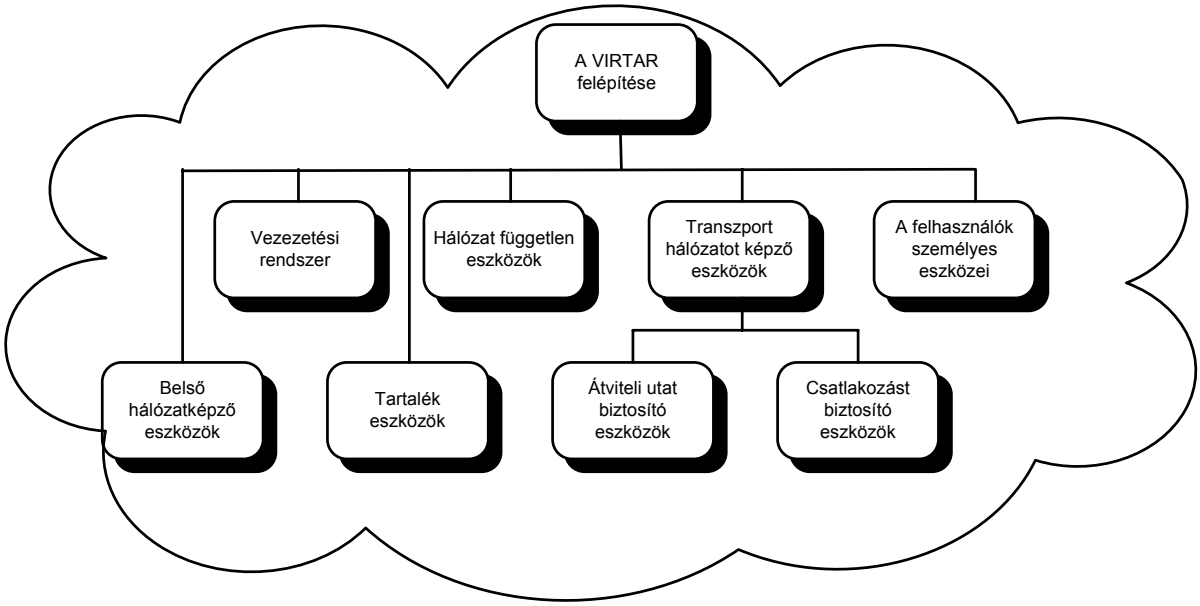
[25] NII = 'National NIIs' + NATO NII; NII = Networking & Information Infrastructure

Ahhoz, hogy a törzsben dolgozó tiszt el tudja látni a feladatát először is szüksége van saját eszközökre, nevezzük őket **felhasználói eszközök**nek**.** Ahhoz, hogy ezeket az egy vezetési ponton levő felhasználói eszközöket hatékonyan ki lehessen használni célszerű őket hálózatba kötni. A vezetési pont hálózatát megvalósító eszközöket nevezzük **belső hálózatképző eszközök**nek. A vezetési pontok is csak akkor tudnak hatékonyan működni, ha egymással összeköttetésben állnak és arra, hogy ezt megvalósítsuk a legjobb, ha egy mindent felölelő hálózatot használunk. Diffúzió szintjén ezt tekintem **transzport hálózatnak**, harcászati hálózatnak vagy országos hálózatnak, attól függően, hogy béke elhelyezési körletben, vagy feladat végrehajtáson van az alakulat. Ebben az időszakban ez a rendszer nem különbözik a NATO-leírástól, mert a felhasználói eszközök és a belső hálózatképző eszközök megfelelnek az „User domain", a harcászati hálózat pedig a „Network domain" szintjének. Azonban, hogy a rendszerünk működőképes legyen, szükség van két fontos elemre, a **hálózat független eszközök**re és a VIRTAR **vezetési rendszeré**re. Teljes mértékben egyetértek dr. Szöllősi Sándorral, aki azt írja: „Feltétlenül törekedni kell a lehető leghomogénebb technikai rendszer kialakítására, de nem szabad elhanyagolni a katonai feladatokból adódó sajátosságokat, követelményeket, lehetőségeket, melyek jelentősen eltérőek lehetnek a civil igényektől." [27.] Erre az igényre a legjobb választ a harcászati internet nyújtja:

„A harcászati internet leírható úgy is, mint egy integrált hadszíntéri kommunikációs hálózat, amely funkciójában hasonlóságot mutat a nyilvános internettel, annál is inkább, mivel infrastruktúrája az internet protokollok (IP) kommunikációján alapul. Kulcsfontosságú az a képesség – csakúgy, mint a nyilvános internetnél -, hogy az információ eljuthasson a hálózat bármely szegmensébe" [28.]

Az, hogy egy jövőbeni rendszer milyen technológiai kiépítésű lesz, véleményem szerint túlmutat értekezésem keretein, hiszen előre vetíti a polgári technológia térnyerését. Igaz ez a megállapítás a szabványosításra is, amely a technológia fejlődése után „kullog". A hálózati technológia szabványosítási törekvéseit és buktatóit például Andrew S. Tanenbaum is bemutatja könyvében.[29.]

1.3.4 A technikai alrendszer elemeinek részletes elemzése



9. ábra: A VIRTAR felépítése a NNEC megvalósításakor

- **felhasználói eszközök (végberendezések)**

A tendenciákat figyelembe véve a felhasználói eszközök közül lesznek olyanok, amelyek a felhasználó számára változatlanok lesznek, lesznek olyanok, amelyek eltűnnek és teljesen új eszközök kerülnek előtérbe. A legfontosabb közös tulajdonságuk várhatóan „plug and play”[26] eszközök kell, hogy legyenek. „A hadműveleti helyzetek gyors változása nem teszi tehát lehetővé a vezetési pontok hálózatainak hosszú idejű kiépítését és telepítését, konfigurálását, vagy áttelepítését, ezért ki kell alakítani a minimális telepítési idejű rendszert, a kezelők rövid idő alatti telepítési és konfigurálási feladatait, vagyis a lehető legnagyobb automatizáltságra kell törekedni.”[30.]

A rendszerből eltűnő eszköznek tartom a távíró és géptávíró (telefax) berendezéseket, valamint az ezeket felhasználó rejtjelző eszközöket. A telefax berendezések jelentősége az elektronikus levelezéssel egyre csökken, de véleményem szerint, a teljes eltűnésükkel a rendszerből egyelőre nem kell számolnunk.

A felhasználó számára változatlannak tűnnek például a telefonok, amelyek funkciója nem változik, viszont változik a rendszerhez való viszonyuk. A kereskedelemben már kapható IP alapú telefonok megjelenése a Magyar Honvédség

[26] Automatikusan induló eszközök, amelyek a rendszerhez történő csatlakozás után azonnal funkcionálnak.

tábori rendszereinél idő és pénz kérdése. Sajnos az évtized elejére végbe ment honvédségi telefonkorszerűsítési program, az összes elért eredménye ellenére, mára már korszerűtlen, gátolja az új rendszerek terjedését. Mindez mutatja a technológia gyors fejlődését, hiszen a korszerűsítés még be sem fejeződött, de már új technológiára történő átállás is napirenden lehetne.

A felhasználói eszközök leglátványosabban fejlődő tagjai a különféle számítógépek (asztali számítógép, laptop, PDA) és az ezekhez rendelhető felhasználói szoftverek. 2001-ben Rajnai Zoltán még csak az „irodai alkalmazású munkaállomások”-ról írt [31.] mára azonban ezek mellett már a speciális alkalmazások sora jelent meg a katonai alkalmazásokban. Ilyen speciális alkalmazásnak tekinthető példaképpen a vezetési és irányítási (C2)-, irodaautomatizálási-, térinformatikai-, automata jelentési-, döntés előkészítő szoftverek. Nagyon valószínűnek tartom, hogy a felhasználói eszközökért a minden egyes felhasználó saját maga fog felelni, ezeket az eszközöket nem a VIRTAR személyi állománya fogja telepíteni az adott települési helyeken. Ezt a következtetést a jelenlegi polgári életben átélt tapasztalataim alapján vontam le, ugyanis a jelenleg már sok olyan vállalat létezik, ahol az irodai dolgozók a megfelelő biztonsági lehetőségeket figyelembe véve, magukkal hordják a laptopjaikat és azon dolgoznak a kiküldetéseiken illetve akár otthon is. Ezekkel a személyes eszközökkel a VIRTAR üzemeltetőinek, nyilvántartási, ellenőrzési, rendszerbe történő beléptetési feladatokat kell végrehajtani.

Meglátásom szerint, minél alacsonyabb beosztású a parancsnok, annál kisebb és integráltabb a felhasználói eszköze. Jelenleg a kereskedelemben kapható PDA-k többsége rendelkezik mobil telefon, WiFI, Bleutooth, GPS funkcióval, processzoraik feldolgozó képességei megegyeznek a 2-3 évvel ezelőtti személyi számítógépek képességeivel, ami lehetővé teszi a speciális szoftverek futtatását. Ezek a lehetőségek képessé teszik az eszközt, hogy egy kisebb alegység, raj szakasz, esetleg század komplex vezetési eszköze legyen. A második öböl háborúban, az amerikai elit alakulatok szakaszparancsnokai már ilyen eszközzel vezették alegységeiket.

10. ábra Integrált vezetési pont
Forrás: [32.]

Természetesen a hierarchia magasabb szintjén levő a parancsnokok ezek mellett hagyományosnak mondható vezetési eszközöket is használnak, úgymint számítógép, telefon, fax. A **10. ábra** egy korszerű század, zászlóalj szintű integrált vezetési pont automatizált vezetési eszközeit mutatja be.

- **belsőhálózat képző eszközök**

A belső hálózat képző eszközöknek alapvetően kettős szerepük van, egyrészt a felhasználói eszközöket kell csatlakoztatni a harcászati vagy országos hálózathoz, másrészt a felhasználói eszközök egymás közötti kapcsolatát kell biztosítani. Véleményem szerint, ha már van két számítógépünk azt már célszerű hálózatba szervezni, mert egy hálózat nem csak a számítógépek összessége, hanem alkalmat ad több funkció egyesítésére, mint a közös munka, az adatbázisok megosztása, és hatékony kommunikáció. A belső hálózatok sajátossága kell, hogy legyen a megfelelő szintű adathozzáférés biztosítása is, lehetőség szerint tehát csak azokat az adatainkat osszuk meg, amelyekre másoknak is szükségük van. A számítógép hálózatok kialakításakor lehetőségünk van a fizikai összeköttetés mellett logikai összeköttetés létrehozására is, így egy számítógép több kisebb virtuális hálózat eleme is lehet egyszerre, így ezekben a rendszerekben az erőforrásokat másként oszthatja meg. Elképzelhető, hogy a Híradó és Informatikai Főnök számítógépe szerepelhet a törzsfőnök virtuális hálózatában mint beosztott, illetőleg egy időben lehet a híradó és informatikai hálózatban mint vezető. A virtuális hálózatok lehetősége megkönnyíti a telepítést, mert minden egyes végberendezés funkciójára

és fizikai elhelyezkedésére tekintet nélkül ugyan arra a hálózatképző elemre csatlakozhat és a hálózatok kialakítása központilag biztosítható.

A belső hálózatok kialakítására igénybe lehet venni vezetékes és vezeték nélküli eszközöket. Az új típusú vezeték nélküli eszközök, mint a Bluetooth, WiFi, vagy WiMAX biztosíthatják a végberendezések közötti hálózati kapcsolatot a hadműveleti területen menet közben és ideiglenes települési hely elfoglalása esetén. Véleményem szerint különösen béke elhelyezési és stacioner körletben a vezeték nélküli rendszereket ki kell váltani vezetékes, lehetőség szerint optikai eszközökkel, azok nagyobb zavarvédettsége és kisebb felderíthetősége miatt.

- **harcászati vagy országos hálózat**

A vezetési pontok belső hálózatainak kommunikációját a harcászati vagy az országos hálózat oldja meg attól függően, hogy a kötelékek hol teljesítik a feladataikat. Mindkét esetben a hálózat struktúrájában két alkotóelemet különböztethetünk meg, úgymint az átviteli vonalakat és a kapcsoló elemeket.

Attól függően, hogy a hálózatot milyen szervezet felügyeli feloszthatjuk, nemzeti-, missziós vagy harcászati, illetve szövetséges hálózatokra.

- **Hálózat független eszközök**

A hálózat független eszközök tervezése esetén fontos szempont, hogy nem szabad csak a hálózat nyújtotta képességekre támaszkodnunk, szükségünk van olyan rendszerekre, amelyek a hálózat nyújtotta szolgáltatások nélkül is üzemképesek maradhatnak.

2009. január 25-én egy dunántúli építkezésen véletlenül átvágták a Magyar Telekom Nyrt. által üzemeltetett internet kábelt, melynek következményeként többórás üzemszünet állt be a cég országos hálózatában. Ebből a számunkra levonható következtetés az, hogy még egy jól megtervezett és kivitelezett hálózat sem sérthetetlen.

Ilyen közvetlen összeköttetéseket biztosító eszközök lehetnek a nagytávolságú kapcsolatokat biztosító rövidhullámú rádiók, illetőleg a mikrohullámú műholdas berendezések. Alapesetben ezek az eszközök is részt vehetnek a hálózat kiépítésében, mint kerülő irányok, még abban az esetben is, ha ez a képességük a

korlátozott sávszélességük miatt nem jelentős (pl.: RH rádiók). Viszont adott esetben ez a korlátozott sávszélességű összeköttetés is létfontosságú lehet.

- **Tartalék eszközök**

A tartalék eszközök olyan eszközök amelyek a a rendszer megbontása, áttervezése nélkül alkalmazhatók a meghibásodott eszközök cseréjére. A rendszer elemek fontosságának, illetve az elviselhető kiesés függvényében, lehetnek „hideg" illetve „meleg" tartalék eszközök. A „hideg" tartalék amikor a meghibásodott eszköz kiszerelése után cseréljük ki őket, a rendszer elviseli ezt az idő kiesést. A „meleg" tartalék eszközök, folyamatosan, mintegy párhuzamosan működnek és a meghibásodás esetén azonnal át tudjuk terhelni a feladatokat a tartalék eszközökre, ez abban az estben fontos, amikor az időkiesést minimális szinten kell tartanunk.

- **VIRTAR vezetési rendszere**

Minél bonyolultabb egy rendszer, annál nehezebb a tervezése és létesítése, bonyolult a kapcsolatok fenntartása, a hálózat áttekintése és az elvárt szintű üzemeltetése. A „klasszikus" értelemben vett híradó irányítópontok és híradó ügyeletesi rendszer feladatai nagymértékben változtak és véleményem szerint sok esetben át is alakultak. A VIRTAR vezetési rendszere a következő fejezetben kerül feldolgozásra.

- **A minősített adatfeldolgozás a VIRTAR-on**

Napjaink katonai gondolkodásában nagyon sokan összekeverik a biztonságos átviteli utakat a minősített adatokat feldolgozó rendszerekkel. Véleményem szerint nagyon fontos a megkülönböztetés, mert minden egyes rendszernek és hálózatnak vannak, kell, hogy legyenek biztonsági funkciói, amelyek „szigorúsága" függ a feldolgozott adatok minősítési szintjétől.

A minősített adatfeldolgozó rendszerek követelményei a NATO rendszerekre nagyon pontosan rögzítettek, azokat évente felülvizsgálják és ha szükséges módosítják. Ezen rendszerek létrehozására alapvetően két módszer létezhet, az egyikben létrehozunk számukra egy külön hálózatot: „A gerincrendszer stacioner lokális hálózatainak kialakítása tulajdonképpen három hálózat létrehozását jelenti. A három elkülönülő hálózat általános értelemben a meglévő adatminősítési szintekhez kapcsolódik. Az elkülönítve létrehozandó hálózatok a következők:

- titkos hálózat (minősített adatok kezelésére),
- Internet hozzáférést biztosító hálózat,
- nyílt (honvédségi Intranet) hálózat.” [15.]

Ugyan ezt a szerintem elavult vélekedést fejezi ki a MHPK VKF 81/1997 intézkedése az Internet igénybevételével kapcsolatos titokvédelmi és adatbiztonsági rendszabályok betartásáról:

„2. Az Internetre ideiglenesen vagy állandó jelleggel rákapcsolt számítógépen az államtitokról és a szolgálati titokról szóló 1995. évi LXV. törvény 3. és 4. §-aiban meghatározott állam- és szolgálati titkot képező, továbbá a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény 19. § (3) bekezdés a) pontjára figyelemmel és a honvédelmi vonatkozású szolgálati titokkörről szóló 11/1995. (XI. 14.) HM rendelet mellékletében meghatározott különös adatfajtákkal kapcsolatos - az MH-ra vonatkozó és a szolgálati tevékenységgel összefüggő - nyílt, illetve belső használatra készült nem nyilvános adatok tárolása tilos!

3. Tilos az Internetre olyan számítógép rákapcsolása, amely olyan lokális hálózat tagjaként üzemel, amelynek szerverén vagy más munkaállomásain a 2. pontban meghatározott adatokat tárolnak. Az Internet igénybevételére fizikailag elkülönített számítógépet vagy lokális hálózatot kell használni” [34.]

Azonban ha tovább gondoljuk Gorza Jenő véleményét és a VKF intézkedését akkor a szövetségi rendszereinkben, akkor könnyen belátható, hogy legalább öt rendszert kellene szerveznünk, a fenti hármat ki kell egészíteni a NATO, valamint EU minősített hálózatokkal.

Belátható, hogy ebben az esetben minden olyan munkahelyre ahol, több hálózatot is használnak, a használt hálózatok számának megfelelő külön számítógépet és a hálózatokhoz tartozó aktív és passzív elemeket kell rendszeresíteni. Ez még akkor is hatalmas kiadást jelent ha korlátozzuk a felhasználók számát a hálózatokban.

Az is belátható hogy, ha mind az öt hálózatot külön kiépítjük milyen hatalmas ráfordítást igényel. Éppen ezért főként a hadműveleti területen, ahol a kiépítésnek nem csak anyagi de idő korlátjai is vannak, lehetőség szerint egy hálózaton kelljen

építeni és a felhasználónak egyetlen gépen legyen lehetősége elérni az összes használni kívánt hálózatot.

Annak a megoldását, hogy hogyan lehet megoldani a különböző minősítésű hálózatok összekapcsolását az NC3A munkatársai mutatták be 2008 novemberében a „Communications" magazinban.[35.] Az egy munkahely –egy gép elvét angolul: „one box, one wire" (OB1) több cég is kínálja a különböző hirdetéseiben. Természetesen, ahhoz hogy ezeket az eszközöket alkalmazhassuk az illetékes akkreditáló hatósággal előzetesen véleményeztetni, illetve akkreditáltatni kell.

.

1.4 Összegzés, következtetések

A katonai hívatás a feladata a különféle, akár béke akár missziós feladatok eredményes végrehajtása, amelyet a parancsnok mint egyszemélyi vezető döntései alapján hajtanak végre. A parancsnok döntéseihez megfelelő minőségű és mennyiségű információ szükséges. Ezeket az információkat a parancsnok számára az elöljáró, az alárendeltjei valamint a törzsének különböző beosztású tagjai, a saját adatbázisaikra és információs kapcsolataikra támaszkodva szolgáltatják. Az ellenségre és a környezetre vonatkozó adatokat a felderítési rendszer, a saját erőkre vonatkozó adatokat a hadműveleti, logisztikai, és személyügyi rendszer, a saját csapatok vezetését a híradó és informatikai rendszer biztosítja. Természetesen ezek az alrendszerek akár még kisebb alrendszerekre is bonthatók, attól függően, hogy milyen mélységben és céllal kívánjuk vizsgálni a rendszert. Az, hogy ezekben az információs alrendszereknek mi az adattartalma, függ a parancsnok szándékától és a törzs szervezetétől. A törzs szervezete függ az alegység, illetve egység alaprendeltetésétől és nagyságától, valamint attól, hogy a különböző szervezeti elemeket a kötelék vezetése mely szervezetei elemben képzeli el.

Az egész folyamat mozgatórugója az információáramlás, egyrészről a vezetői folyamat is felfogható a különböző információk továbbításának: tervek, utasítások, intézkedések eljuttatása az érdekelt feleknek, másrészt a végrehajtásról történő visszacsatolást, a tervezést és a szervezést is a különböző információkkal alá kell támasztani.

Az, hogy ezek a jelentések, adatok, üzenetek eljussanak a címzettekhez, és megfelelően feldolgozásra kerüljenek, a vezetési és információs rendszer számára szolgáltatást nyújtó híradó és informatikai rendszer feladata. Más szóval a híradó és informatikai rendszer a vezetés és információs rendszer technikai alrendszere.

Az információt szolgáltató alrendszer és a technikai alrendszer elválaszthatatlan. A vezetési funkció nem értelmezhető, ha a parancsokat, utasításokat, és az őket alátámasztó információkat nem tudjuk eljuttatni a feladótól a címzettig, illetve ezek nélkül a továbbítandó adatok nélkül a technikai alrendszer oka fogyottá válna.

Jelenleg a katonai infokommunikációs terminológiánkban nincs egységesen kialakult és letisztult fogalom rendszerünk, amit a szakember gárda formálisan, vagy informálisan de egységesen értelmezne. Fogalmi keveredések, zavarok olvashatók a katonai lexikonokban is, melynek oka az új és a régi fogalmak ötvözése, illetve az angol kifejezések fordítási és honosítási szándéka. Ezért, hogy a különböző értelmezésbeli problémákat elkerüljem a dolgozatomban a híradó és informatika rendszert a feladatából adódóan Vezetési és Információs Rendszer Technikai Alrendszere (VIRTAR)ként emlegetem. Vagyis a VIRTAR a vezetés és az információ szolgáltatás érdekében telepített információ és adat továbbító, feldolgozó és tároló eszközök (hardver és szoftver) és az őket telepítő és üzemeltető személyi állomány összessége.

A VIRTAR felépítésére, szerkezetének bemutatására a szakirodalomban nem találtam a teljes a kor színvonalán álló modellt. A legfiatalabb a hagyományosnak számító modell keletkezésekor gyakorlatilag ez csak a hírrendszert jelentette és a számítógépes környezet még nem létezett, legfeljebb egyedi nagygépek álltak rendelkezésre. A „hagyományos modell” alkalmazása a jelenlegi és a jövőbeli rendszerek leírására nem alkalmazható mert:

- A híradás és az informatikai eszközök konvergenciája a polgári életben végbe ment, egymástól elválaszthatatlan egységet alkotnak.
- A NATO jelenleg a hálózat nyújtotta képességek kifejlesztésén dolgozik, amelynek adaptálása a magyar rendszerekre számára is elengedhetetlen.

- A jelenlegi katonai gondolkodásunkban a szimmetrikus hadviselés lehetősége ha nem is szűnt meg, de jelentősen háttérbe szorult. A csapatok elsősorban a különböző missziók végrehajtására és természeti katasztrófák leküzdésének támogatására készülnek fel.

A „hagyományos” modellnek az elavultsága ellenére is van egy nagy előnye, mégpedig az, hogy egységes egészként szemléli a rendszert. Az 1990-s évek elejétől a katonai munka területén is megjelentek a személyi számítógépek amelyeket az ezredforduló idején elkezdtünk helyi hálózatokba szervezni és jelenleg a legtöbb helyen a helyi hálózatok egy egységes országos hálózatban tudnak működni. Azonban a katonai rendszerekben a híradás és az informatika konvergenciája még nem fejeződött be, ami kettőséget mutat minden rendszerelem tekintetében.

A jövő katonai konfliktusainak az információ áramlását, az információk minőségét mennyiségét és elosztását a „NATO hálózat nyújtotta képességek NNEC” koncepciója fogja meghatározni.

A NATO hálózat nyújtotta képességek (NNEC) a szövetség észlelő és technikai képessége, amely egyesítse a műveleti környezet alkotóelemeit a stratégiai szinttől (beleértve a NATO parancsnokságot is) a taktikai szintig a hálózati és információs infrastruktúrán keresztül. Egyszerűbben fogalmazva, az információk hatásos és hatékony megosztásának a képessége, a missziók (feladatok) sikeres végrehajtása érdekében, a NATO-t alkotó nemzetek és a szervezetek között.

A NNEC koncepció érzékeltetéséhez a legjobb a jéghegy hasonlat ahol NNEC jéghegy látható része a küldetés sikere a lényegi rész viszont víz felszíne alatt van és egy komplex rendszert tartalmaz, amelynek a részei: Az információ megosztás, a szilárd és megbízható hálózat, a minőségi információk, a rendszer önszinkronizációja, az interoperabilitás, a fenntarthatóság, a gyors parancsadás, az együttműködés képessége, az egységes folyamat rend, eljárásmód és vezetési módszer. Tehát a NNEC megvalósítása nem csak technológiai feladat. A technológia feladata, hogy támogassa a NNEC kialakítását, elősegítse az információkról a döntésekről a folyamatok gyorsaságáról szóló nézeteink fejlődését, valamint szükséges az együttműködés és valósidejű információközlés megvalósításához[22.].

Azonban a NNEC nem kifejezetten csak katonai fogalom a NNEC koncepciójában az érdekelt felek a NATO szervezetei, a parancsnokságok, ügynökségek, civil és katonai szervezetei, a NATO-t alkotót nemzetek katonai és polgári szervezetei, a kutatás fejlesztés és a megvalósításában résztvevők, kutatóhelyek, egyetemek, iparvállalatok, nem kormányzati szereplők, nemzetközi szervezetek.

A VIRTAR tervezésében, üzemeltetésében résztvevők számára az a legfontosabb kérdés, hogy a NNEC megvalósításához szükséges rendszer hogyan fog felépülni. A kutatásaim során arra a következtetésre jutottam, hogy a VIRTAR a következő elemekből kell hogy álljon:

- **felhasználói eszközök (végberendezések)**

Amelyek közvetlenül a felhasználó használatában, felügyelete alatt kell hogy legyenek, ezeket az eszközöket valószínűleg maguk a felhasználók fogják az adott települési helyre szállítani azonban a VIRTAR üzemeltetőinek kell gondoskodniuk a rendszerbe történő biztonságos beléptetésről.

- **belsőhálózat képző eszközök**

A belső hálózat képző eszközöknek alapvetően kettős szerepük lesz, egyrészt a felhasználói eszközöket kell csatlakoztatni a harcászati vagy országos hálózathoz, másrészt a felhasználói eszközök egymás közötti kapcsolatát kell biztosítani. A belső hálózatok sajátossága kell, hogy legyen a megfelelő szintű adathozzáférés biztosítása is, lehetőség szerint tehát csak azokat az adatainkat osszuk meg, amelyekre másoknak is szükségük van. A számítógép hálózatok kialakításakor lehetőségünk van a fizikai összeköttetés mellett logikai összeköttetés létrehozására is, így egy számítógép több kisebb virtuális hálózat eleme is lehet egyszerre, így ezekben a rendszerekben az erőforrásokat másként oszthatja meg.

- **harcászati vagy országos hálózat**

A vezetési pontok belső hálózatainak kommunikációját a harcászati vagy az országos hálózat oldja meg attól függően, hogy a kötelékek hol teljesítik a feladataikat. Mindkét esetben a hálózat struktúrájában két alkotóelemet különböztethetünk meg, úgymint az átviteli vonalakat és a kapcsoló elemeket.

Attól függően, hogy a hálózatot milyen szervezet felügyeli feloszthatjuk, nemzeti-, missziós vagy harcászati, illetve szövetséges hálózatokra.

- **Hálózat független eszközök**

A hálózat független eszközök tervezése esetén fontos szempont, hogy nem szabad csak a hálózat nyújtotta képességekre támaszkodnunk, szükségünk van olyan rendszerekre, amelyek a hálózat nyújtotta szolgáltatások nélkül is üzemképesek maradhatnak.

Ilyen közvetlen összeköttetéseket biztosító eszközök lehetnek a nagytávolságú kapcsolatokat biztosító rövidhullámú rádiók, illetőleg a mikrohullámú műholdas berendezések. Alapesetben ezek az eszközök is részt vehetnek a hálózat kiépítésében, mint kerülő irányok, még abban az esetben is, ha ez a képességük a korlátozott sávszélességük miatt nem jelentős (pl.: RH rádiók). Viszont adott esetben ez a korlátozott sávszélességű összeköttetés is létfontosságú lehet.

- **VIRTAR vezetési rendszere**

A VIRTAR egyik legfontosabb tulajdonsága kell hogy legyen a rugalmasság, azaz a körülményekhez való alkalmazkodás képessége, ez a képesség elképzelhetetlen a megfelelő szintű vezetés nélkül, a vezetésnek folyamatosan figyelemmel kell kísérni a rendszert és szükség esetén beavatkozni, illetve tervezni a kialakítandó hálózatot.

Napjaink talán a legfontosabb kihívása a biztonságos infokommunikáció a katonai gondolkodásában nagyon sokan összekeverik a biztonságos átviteli utakat a minősített adatokat feldolgozó rendszerekkel. Azonban nagyon fontos a megkülönböztetés, mert minden egyes rendszernek és hálózatnak vannak, kell, hogy legyenek biztonsági funkciói, amelyek „szigorúsága” függ a feldolgozott adatok minősítési szintjétől. Jelenleg a különböző szigorúságú (különböző minősítéssel rendelkező adatokat feldolgozó) rendszerek számára külön hálózatokat üzemeltetünk. Belátható, hogy ebben az esetben minden olyan munkahelyre ahol, több hálózatot is használnak, a használt hálózatok számának megfelelő külön számítógépet és a hálózatokhoz tartozó aktív és passzív elemeket kell rendszeresíteni. Ez még akkor is hatalmas kiadást jelent ha korlátozzuk a felhasználók számát a hálózatokban. Az is belátható hogy, ez milyen hatalmas ráfordítást igényel. Éppen ezért főként a hadműveleti területen, ahol a kiépítésnek

nem csak anyagi de idő korlátjai is vannak, lehetőség szerint egy hálózaton kelljen építeni és a felhasználónak egyetlen gépen legyen lehetősége elérni az összes használni kívánt hálózatot.

A fejezetben foglaltakat mérlegelve az alábbi következtetéseket vonom le:

1) A vezetési funkció nem választható el a vezetés technikai alrendszerétől, amelyből következik, hogy az információt szolgáltató alrendszer és a technikai alrendszer egymástól szintén elválaszthatatlan;

2) A NATO és így a Magyar Honvédség előtt álló fontos feladat a hálózat nyújtotta képességek megteremtése;

3) A Hálózat nyújtotta képességek kialakítása nem elsősorban technikai feladat, de a jelenlegi VIRTAR átalakítása szükséges. A VIRTAR felépítése felhasználói eszközök (végberendezések) belsőhálózat képző eszközök, harcászati vagy országos hálózat, Hálózat független eszközök, VIRTAR vezetési rendszere, elemcsoportokat kel, hogy tartalmazza.

4) A VIRTAR személyi állománya előtt álló egyik legnagyobb kihívás a biztonságos rendszer megteremtése, azonban szakítani kell a meglévő hagyományokkal, és lehetőség szerint egy munkahelyhez csak egy felhasználói eszközt kell rendelni, és azon kell biztosítani a különböző hálózatok biztonságos elérését.

2 Vezetési és információs rendszer technikai alrendszerének irányítása

A vezetési és információs rendszer technikai alrendszerének (VIRTAR) irányítás nem lehet más, nem alkalmazhat más módszereket, mint a Magyar Honvédség, másképpen fogalmazva a VIRTAR irányításának szervesen integrálódnia kell a honvédség irányításába. Ezért mielőtt a VIRTAR irányításával foglakoznánk, át kell tekinteni a Magyar Honvédség irányítási rendjét.

2.1 A Magyar Honvédség irányítása

Hazánkban az alapvető kérdések fundamentumaként az Alkotmány szolgál, amely e kérdéskört tekintve a következőképpen fogalmaz:

„A Magyar Honvédség irányítására - ha nemzetközi szerződés másként nem rendelkezik - az Alkotmányban meghatározott keretek között kizárólag az Országgyűlés, a köztársasági elnök, a Honvédelmi Tanács, a Kormány és az illetékes miniszter jogosult.” [36.]

Az Alkotmány tehát rögzíti a legfelsőbb szintű, alapvető irányítási jogosultságokat, amely mellett a Magyar Honvédségről szóló törvény részletezi a feladat- és hatásköröket. A törvényben a Magyar Honvédség irányításáról és vezetéséről a IX. fejezet rendelkezik. A jogszabály tisztázza a szolgálati elöljáró, hivatali felettes, illetve szakmai elöljáró, szakmai felettes fogalmát, és meghatározza jogosultságaikat:

„93. § (1) Az általános hatáskörű elöljáró, illetőleg felettes: a szolgálati elöljáró, illetőleg hivatali felettes, a neki alárendelt katonák: a szolgálati, illetőleg hivatali alárendeltek. …..

94. § (1) Az olyan elöljáró, illetőleg felettes, aki csak a saját szakterületén van felruházva rendelkezési jogkörrel: szakmai elöljáró, illetőleg szakmai felettes, akikre vonatkozóan rendelkezési jogkörrel rendelkezik - állományviszonyuktól függetlenül - szakmai alárendeltek.

(2) A különböző vezetési szinteken a szakmai elöljáró gondoskodik az elöljárói döntéseknek megfelelő szakmai feladatok végrehajtásáról. A szakterületi vezetők vezetői jogosultságait hatásköri szabály, illetve a szolgálati elöljáró állapítja meg.” [37.]

A fejezet meghatározza még a Magyar Honvédség felső szintű irányítását és vezetését, amelyet rendkívüli állapot idején a Honvédelmi Tanács „béke” időszakban a honvédelmi miniszter hajt végre:

„(2) Rendkívüli állapot idején a Honvédség legfelsőbb irányító szerve a Honvédelmi Tanács.

(3) A honvédelemért felelős miniszter önállóan gyakorolja a törvényben meghatározott hatáskörét, az Országgyűlés és a Kormány döntései szerint irányítja és vezeti a Honvédséget.” [38.]

A törvény a vezetés és irányítás szempontjából még két fontos hivatali (parancsnoki) beosztást említ, úgymint a Honvéd Vezérkar főnökét (101. §), valamint a szakirányításért felelős honvédelmi miniszter által kijelölt személyt, aki a Honvédelmi Minisztérium hivatali szervezetének a vezetője, de akinek a beosztását a szövegezés nem nevesíti (100. §). E jogkört a 2134/2006. (VII. 27.) Korm. határozat[27] 3. pontja a kabinetfőnök hatáskörébe utalja. A két személy együttműködési kötelezettségét a törvény a 100. § (4) és a 101. § (5) bekezdése írja elő.

A Honvéd Vezérkar főnöke:[28]

„f) közreműködik a Honvédség feladatainak teljesítése szempontjából fontos közlekedési és hírközlő hálózat, valamint a légi, sugárfigyelő, jelző- és riasztási rendszerek működőképességének biztosításában,

k) a parancsnokságok, csapatok békeidőszaki vezetési rendszere működésének biztosítása érdekében tervezi, szervezi a híradással, az informatikával és a vezetés egyéb területeivel kapcsolatos feladatokat,” [37.]

Az „f)” pontban szereplő rendszerek esetében nem tekinthető egyértelműnek az, hogy milyen módon és kivel kell a közreműködést végrehajtani.

A „k)” pont is fel vet egy kérdést. Amennyiben a vezérkari főnök csak a csapatok békeidőszaki vezetési rendszer működése érdekében tervez és szervez, akkor ki tehető felelőssé a minősített időszak vezetési rendszeréért? Ezen felül, véleményem

[27] 2134/2006. (VII. 27.) Korm. határozat a Magyar Honvédség irányításának és felsőszintű vezetésének rendjéről.
[28] A dolgozat szempontjából a többi közül kiemelve.

szerint a szabályozás ellentmondásban áll a 2134/2006. (VII. 27.) Korm. határozat 4. pontjával amely szerint:

„A jogi szakállamtitkár szakirányítja a jogi, informatikai és információvédelmi, ügyviteli, tárca szintű ellenőrzési, valamint a hatósági tevékenységet." Mivel „A Honvéd Vezérkar főnök a miniszter legfőbb katonai tanácsadója, a szakállamtitkárokkal azonos egyeztetési jogok illetik meg." [40.] A két azonos szintű vezető közül a két dokumentum alapján nem állapítható meg, hogy ki a felelős a tárca informatikai munkájáért.

A törvény 102-103. §-ai a katonai szervezetek középszintű irányítását a középszintű irányító szervek vagy más magasabb szintű parancsnokságok élén álló parancsnokok, a katonai szervezetek vezetését a szervezet parancsnokának hatáskörébe utalják. A parancsnok szolgálati hatásköre kiterjed az általa vezetett katonai szervezet működésének minden területére.

A szakirányításról a 2134/2006. kormányhatározat 7. pontja rendelkezik: „A szakállamtitkárok és a kabinetfőnök szakmai felettesei a Magyar Honvédség szakterületükhöz tartozó állományának, a szakirányítási feladataikat főosztályvezető útján vagy közvetlenül, jogszabályban vagy az állami irányítás egyéb jogi eszközeiben rögzítettek szerint látják el. A Honvéd Vezérkar főnök vezeti továbbá a Honvéd Vezérkart és a Magyar Honvédség hadrendjébe tartozó katonai szervezeteket, szolgálati elöljárója (hivatali felettese) azok személyi állományának. Felelős az alárendelt szervezetek - jogszabályok, az állami irányítás egyéb jogi eszközei és a belső rendelkezések előírásai szerinti, a szakirányítás keretein belül történő – vezetéséért". [40.]

2.2 A kiadványok, mint a vezetés eszközei

A vezetés eszközeit szintén a jogszabályokban és az államirányítás egyéb jogi eszközeiben találhatjuk meg a honvédelmi törvény alapján. Ezek alapján:

- A honvédelmi miniszter

„… rendelettel és az állami irányítás egyéb jogi eszközeivel szabályozza a honvédelmi feladatok végrehajtását", amelyet az 52. § f) pontja fogalmaz meg. A miniszteri utasítás tartalmát a 109. § rögzíti: „Miniszteri utasításban (az állami irányítás egyéb jogi eszköze) kell meghatározni a miniszter irányítása és vezetése alá tartozó szervezetek tevékenységére vonatkozó szabályokat."

- A Honvéd Vezérkar főnöke

„ a vezetési hatáskörében parancsot, intézkedést és szakutasítást ad ki.” (101. §).

- A hivatali felettes

„egyedi utasítással érvényesíti az akaratát alárendeltjeivel szemben. Részükre a hatáskörébe tartozó és jogszabály által nem tiltott bármilyen utasítást kiadhat.” (109. § (2) bek.).

A legfelsőbb szinten az egyéb belső rendelkezésekről szintén a honvédelmi törvény rendelkezik:

- Szakutasítás

„Szakutasításban kell meghatározni a Honvédség szakmai feladatai ellátásának alapvető szabályait, valamint a haditechnikai eszközök és anyagok üzemeltetésével, karbantartásával, javításával kapcsolatos szakmai-technikai szabályokat.”

- Intézkedés

„Intézkedésben állapíthatók meg egyes rendszeresen ismétlődő tevékenységek végrehajtásának szakmai, technikai vagy eljárási szabályai, ideértve a katonai szervezetek működési rendjének és a személyi állomány mindennapi tevékenységének általános rendezést igénylő kérdéseit.” (110. §)

A további kiadványokról a 93/2006. (HK 18.) HM utasítás[29] rendelkezik, amely alapján rendelkezésünkre áll:

- szolgálati könyv (szabályzat és alapdoktrína), valamint
- főnökségi kiadvány:

Amely lehet doktrína, állandó működési eljárások, szövetségi, illetve NATO egységesítési dokumentumok (STANAG, AP stb.), szakutasítás, műszaki leírás, lőtáblázat, kiképzési program, tankönyv, kézikönyv, módszertani és tansegédlet, jogszabályok vagy belső rendelkezések gyűjteménye, ár- és cikkjegyzék, hasonló rendeltetésű külföldi katonai és védelmi kiadványok fordítása, valamint szolgálati könyvnek nem minősülő, de a szabályozott tevékenységet elősegítő egyéb kiadvány.

[29] 93/2006. (HK 18.) HM utasítás a szolgálati könyvek és a főnökségi kiadványok kiadásának rendjéről.

Vizsgálataim alapján megállapítottam, hogy jogszabály nem rendelkezik a különböző kiadványok egymáshoz való viszonyáról, sőt az egyes kiadványok tartalmáról sem. Így például nem tisztázott az sem, hogy mit kell tartalmaznia a szabályzatnak és mit az alapdoktrínának, mi a különbség a kettő között, milyen tárgyban kell őket kiadni. Ezen túlmenően a felsorolás nem is tekinthető teljesnek, mert hiányzik a rendszerből a stratégia.[30]

Véleményem szerint ebben a rendszerben is látszik az a tétovaság, amely a NATO tagságunkból adódik, átvettünk bizonyos dolgokat, de a régieket se mertük elvetni, átnevezni.

Továbbbonyolítja helyzetet a a 74/2008. (HK 15.) HM utasítás amelynek a célja egy új egységes rendszer kialakítása. Ennek az új rendszernek a feladata

„A műveleti képességek alakítása, a műveletek sikeres végrehajtása, a műveletekre való felkészülés és a kiképzés hatékonyságának növelése, a vezetői kontroll erősítése, a belső eljárásrend, az együttműködés rendszerének és a különböző vezetői szinteken jelentkező egyéb katonai feladatok végrehajtásának hatékonysága folyamatos javítása érdekében tapasztalat feldolgozó-rendszer kialakítása és működtetése.” [45.]

A rendszer céljával teljesen egyetértek, a probléma véleményem szerint az, hogy ismételten átvettünk egy működő rendszer egyetlen darabját mindenféle kritikai észrevétel nélkül. A tapasztalat-feldolgozó rendszerben tetten érhető az amerikai precedens rendszer, amely azt jelenti, hogyha már volt ilyen tapasztalatunk, akkor azt alkalmazzuk is. Ez még alapvetően nem lenne baj, azonban az utasítás nem rendelkezik arról, hogy a tapasztalati rendszer hogyan illeszkedik a már meglévő vezetési rendszerünkhöz. Az előzőekben már említett kaotikus rendszert tovább bonyolítja, amennyiben e rendszer – *már meglévőhöz való viszonyát* – nem rendezzük megfelelőképpen. Felmerülhet továbbá a kérdés, hogy a meglévő, a még ki nem vont nemzeti, vagy a NATO által kiadott dokumentumot használjuk, vagy csak egyszerűen alkalmazzuk a tapasztalat-feldolgozó rendszer adatait.

[30] Pedig HM utasítás rendelkezik pl.: az informatikai stratégiáról: 141/2006. (HK 2/2007.) HM utasítás a Magyar Honvédség Informatikai Stratégiájának kiadásáról.

A felvázolt probléma azonban nem csak a nemzetünk sajátja az is mutatja, hogy a szövetségesi rendszerünkben kiemelt feladatként kezelik a különböző területek interoperabilitási kérdéseit, amelyek a különböző kiadványokban öltenek formát:

„Egyetértésben a Szövetség politikájával, a nemzeti és NATO hatóságok elkötelezettek, hogy kifejlesszék, elfogadják és megvalósítsanak fogalmakat, doktrínákat, folyamatokat és mintákat amelyek képessé fogják őket tenni, hogy elérjék és fenntartsák az interoperabilitást. Ez a kompatibilitás, felcserélhetőség, azonosság szükséges szintjének létesítését igényli hadműveleti, eljárási, anyagi technikai és adminisztratív területen” [31] [41.]

Vagyis adminisztratív területen, a szabályzók kiadásakor is törekednünk kellene az interoperabiltiás megvalósítására. Erre a felsőszintű akarat meg van az egyik irányból, amikor a NATO előírások hazai alkalmazásának kérdéseit érintjük[32]. A másik irányból tekinthető problémának azon tény, amely szerint saját előírásainkat kellene úgy kidolgozni, hogy azok megfeleljenek a NATO követelményeknek, azonban a megvalósítás elrendelésére nem találtam utalást sem a jogszabályok, sem az államirányítás egyéb jogi eszközei között.

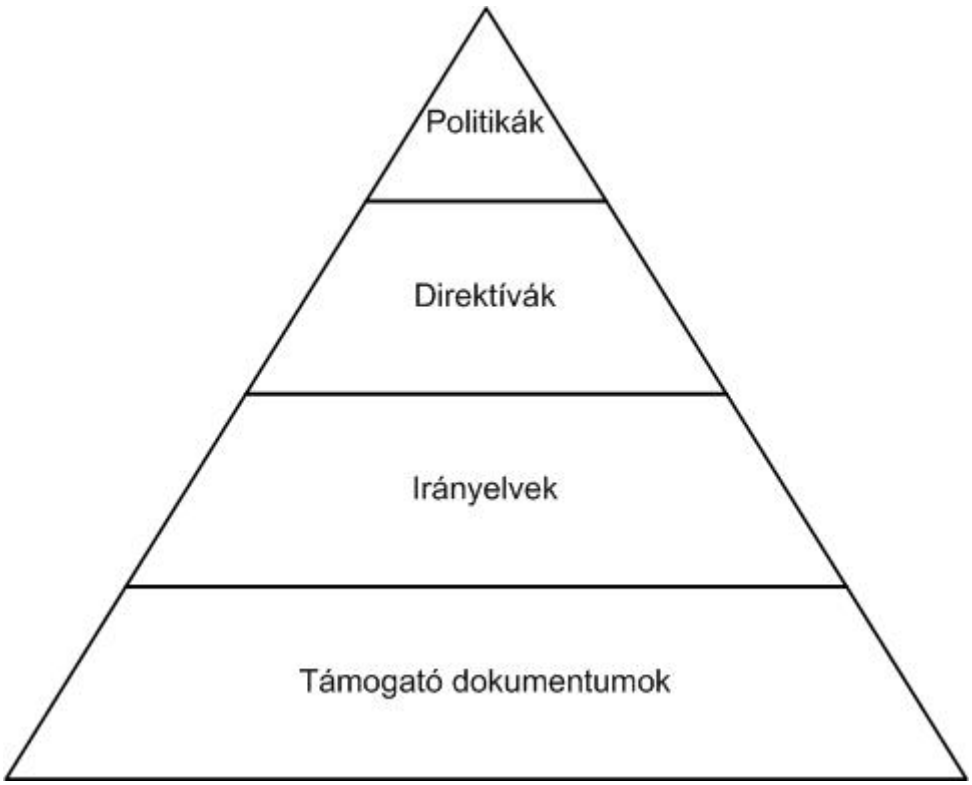
A különböző szakterületek szabályozását előíró NATO dokumentumok legtöbbje beleilleszthető egy négyes sémába, amelynek az elemei a politikák, direktívák, irányelvek, valamint egyéb támogató dokumentumok. Az egymásra épülés sémáját a 11. ábra mutatja be. Amennyiben a vezetési és rányitási dokumentumainkat kompatibilisé akarjuk tenni a NATO-éval két lehetőségünk van:

- A jelenlegi rendszert teljesen felülbírálva, a NATO terminológiát alkalmazzuk, amely azonban nagyon nagy, egyszer elvégzendő munkát jelent;
- A jelenlegi rendszert meghagyjuk, viszont a már meglévő belső utasításainkat megfeleltetjük a NATO ekvivalens dokumentumaival. A feladat végrehajtása nem tekinthető egyszerű feladatnak, mert vannak

[31] “In accordance with Alliance policy, national and NATO authorities are encouraged to develop, agree and implement concepts, doctrines, procedures and designs which will enable them to achieve and maintain interoperability. This requires the establishment of the necessary levels of compatibility, interchangeability or commonality in operational, procedural, materiel, technical and administrative fields.”.

[32] 1/2000. (HK 2.) HM utasításaz egységesítési, szabványosítási tevékenységről és a NATO egységesítési dokumentumok kezeléséről és feldolgozásáról.

olyan szabályzataink, amelyek nem csak egy NATO dokumentum szintnek felelnek meg hanem többet is felölelhetnek.



11. ábra NATO dokumentumok egymásra épülése

2.3 VIRTAR irányítása

Amint azt az előző fejezetben láttuk a jogszabályokból és az állami irányítás egyéb jogi eszközeiből nem egyértelmű, hogy VIRTAR három alrendszeréből (híradás, informatika, információbiztonság) ki tehető felelőssé az informatikáért. E mellett megállapítható, hogy a híradás és az információvédelem, mint szakterület más-más szolgálati személy felelősségi körébe van utalva.

Megítélésem alapján a három alapterület szakirányítását egy szolgálati személynek kellene végeznie.

A szakirányítást végző személy, illetve szervezet feladatai a következőképpen foglalható egybe:

„Szakterületén a szakmai felettes vagy elöljáró:

a) belső rendelkezéseket ad ki a jogszabályok és az állami irányítás egyéb jogi eszközei végrehajtására;

b) intézkedik a szakmai tevékenység végrehajtásával kapcsolatban, a közvetlenül alárendelt szervezetek, illetőleg a Magyar Honvédség szaktevékenységet ellátó szerveire vonatkozóan;

c) feladatkörébe tartozó információkat ad és kér;

d) szakterületének körébe tartozó jogszabályokat és döntéseket készít elő;

e) véleményezési jogot gyakorol;

f) ellenőrzi az alárendelt szakmai szervezetek tevékenységét, illetőleg - a miniszter nevében és megbízásából - az alárendelt katonai szervezetek parancsnokainak és más szolgálati elöljáróinak szakmai tevékenységét;

g) a szakterületéhez tartozó, általa irányított tevékenység egységes gyakorlatának kialakítása érdekében dönt a végrehajtás során felmerült vitás kérdésekben, illetőleg állásfoglalás kiadásával biztosítja a szakmai feladatok egyöntetű végrehajtását.” [40.]

A VIRTAR szakmai vezetése azonban egy nagyon fontos dologban különbözik a többi szakmai tevékenységben méghozzá abban, hogy nem csak a szakmai alárendeltek feladatait kell vezetnie, hanem felügyelnie kell egy működő rendszert is. Erről az összhaderőnemi doktrína a következőket írja:

„A híradó és informatikai rendszer vezetése magában foglalja a hadműveleti és az üzemeltetést irányító funkciókat. A hadműveleti vezetés a rendszer tervező-szervező tevékenységét foglalja magában és a híradó és informatikai irányító pontról történik. A rendszer üzemeltetésével (fenntartásával, kiszolgálásával) kapcsolatos tevékenység a hálózat-felügyeleti központból valósul meg;”[45.]

Figyelembe véve azonban azt, hogy a jelenleg is üzemelő mindkét hálózatunk (híradó, valamint az informatikai) is IT alapú, illetőleg a NATO szakemberei gyakorlatilag már csak a hálózat nyújtotta képességekben gondolkodnak, a Magyar Honvédségben is szükséges létrehozni a számítógép veszélyjelző és incidenskezelő központot, NATO terminológiát használva CIRC[33]-et.

[33] Computer Incident Response Center.

2.4 Javaslat a VIRTAR tervező és szervező munka irányításának kialakítására a magyar és nemzetközi szabványok alapján

Számomra, mint aki alapvetően a katonai viselkedésre és szakmára az elmúlt érában szocializálódtam nagyon furcsa, hogy alapvető szabályzatok jelentős késéssel kerülnek kiadásra. Ilyen alapvető szabályzatnak (direktívának) tartom a VIRTAR szabályzatát, amely leírná az alapvető feladatokat, folyamatokat a tervező és végrehajtó állomány számára.

Véleményem szerint a Magyar Honvédség előtt álló fejlesztési feladatok, hálózatközpontú környezetben való alkalmazás képessége megköveteli a VIRTAR korszerű szemléletű vezetését. A különböző szervezetek vezetési egységesítésére több megoldási javaslat és könyvtárnyi szakirodalom született, amellyel hely hiányában most nem kívánok foglalkozni.[34] Bármiféle vezetési rendszert is alakítunk ki célszerű azt írásban rögzíteni. Erre azért is szükség lehet, mert az elmúlt évek tapasztalatai alapján kijelenthető, hogy mindenféle szervezeti egységben, így az irányítást végrehajtó szervezetekben is nagy a fluktuáció, így egy leírt módszer esetében nem kell minden kidolgozói és alkalmazói munkát előröl kezdeni.

Az előzőző fejezetben láthattuk, hogy a NATO és így a Magyar Honvédség elött álló egyik legnagyobb feladat a hálózat nyújtotta képesség kialakítása, így azt is láthattuk, hogy ez nem csak kifejezetten katonai feladat, ebben részt fognak venni a különböző kutató bázisok, és polgári szervezetek is. Azt is bemutattam, hogy az egyik kiemelt feladat, az egységes vezetési szemlélet kialakítása. A különböző nemzeteknek és szervezeteknek jelenleg nincs egységes vezetési rendszerük, ami lehet a polgári életben már bevált nemzetközi szabványokon alapuló vezetési rendszer.

A híradó és informatikai rendszerekben a szakterületektől függően az alábbi szabványokat érdemes figyelembe venni:

- MSZ EN ISO 9001 Minőségirányítási rendszerek.
- MSZ EN ISO 14001:2005 Környezetközpontú irányítási rendszerek.
- MSZ ISO/IEC 20000:2007 Informatika. Szolgáltatásirányítás.

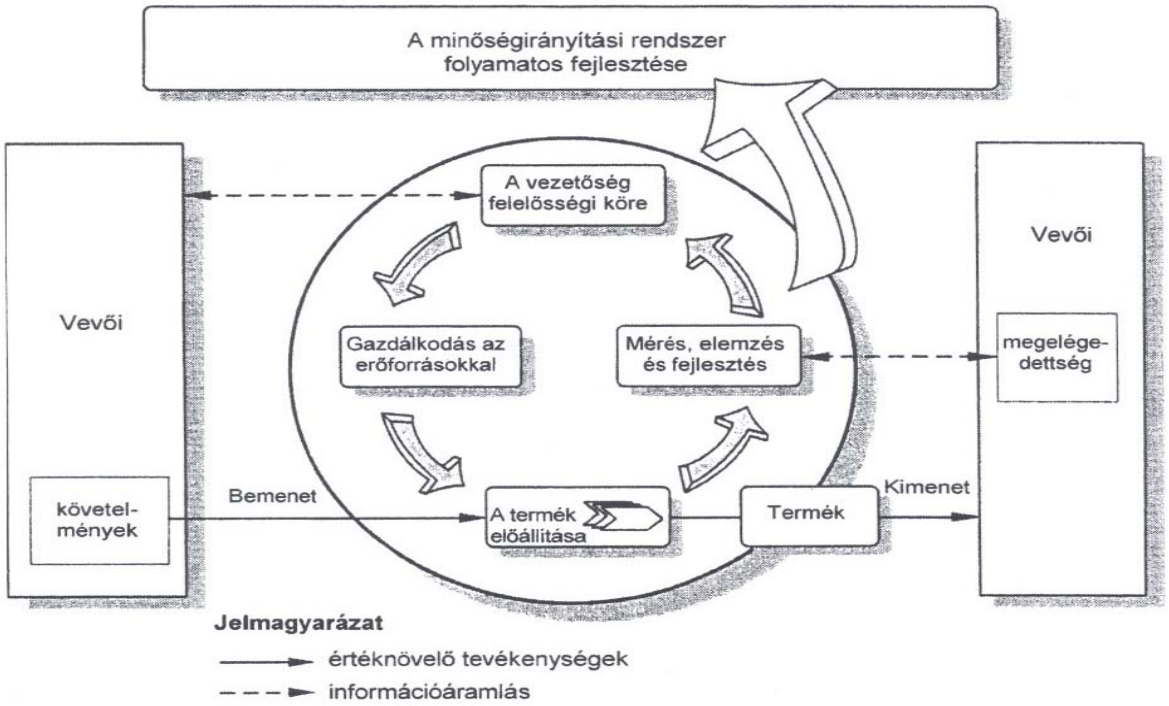
[34] A témában megszületett nemzetközi ajánlásokat nagyon jól összefoglalja Husi Géza a doktori értekezésében: Minőségmenedzsment-rendszerek módszereinek alkalmazása a Magyar Köztársaság rendőrségénél Doktori (PhD) értekezés 2006. BUDAPEST.

• MSZ ISO/IEC 27001:2006 Informatika, biztonságtechnika, az információbiztonság irányítási rendszerei.

A felsorolt szabványok mindegyike a folyamatszemléletű megközelítést, a PDCA[35] modellt alkalmazza előírásaihoz. Ahhoz hogy mit jelent a folyamat szemléletű megközelítés, a 9001-s szabvány mutatja be a lehető legjobban.

„Ahhoz, hogy egy szervezet eredményesen és hatékonyan tudjon működni, meg kell határoznia és irányítania kell számos, egymással összefüggő folyamatot. Bármely tevékenység, amely erőforrásokat használ, és amelyet úgy irányítanak, hogy bemeneteket kimenetekké alakítson át folyamatnak tekinthető. Az egyik folyamat kimenete gyakran egyben a következő folyamat közvetlen bemenetét is jelenti.” [48.]

Szintén a szabvány mutatja be legjobban a PDCA modellt:



12. ábra Folyamatszemléletű irányítási rendszer modellje

Forrás: [49.]

[35] Tervezés, végrehajtás, ellenőrzés, beavatkozás.

A modell alapján meghatározhatók:

Tervezés (**P**lan): azoknak a céloknak és folyamatoknak a megállapítása, amelyek a követelményeknek és a szervezetpolitikájának megfelelő eredmények eléréséhez szükségesek.

Végrehajtás (**D**o): a folyamatok bevezetése.

Ellenőrzés (**C**heck): a folyamatok és a termékek (szolgáltatások) figyelemmel kísérése és összehasonlítása a politikával, a célokkal és a termékre vonatkozó követelményekkel, valamint az eredmények bemutatása.

Intézkedés (**A**ct): intézkedések megtétele a folyamat működésének folyamatos fejlesztésére.

A szabványok tartalmi struktúrája egységes, a MSZ ISO/IEC 20000:2007 szabvány kivételével. Ezen egységességet szemlélteti például a „Biztonságtechnikai" szabvány mellékletét képező táblázat, amely a megmutatja a szabványok egymás közötti viszonyát. A 9001 és 14001 szabvány megítélésem szerint a vezetés szempontjából ekvivalens, csak a nézőpontjaik különböznek. A kettő közötti választást indokolja, hogy a NATO a minőségügyi publikációinak AQUAP[36]-oknak az alapjául is a 9000-s szabványcsaládot választotta.

Javaslatom szerint a VIRTAR általános vezetési alapszabályzatát/doktrínáját, az általános követelményi rendszert célszerű a 9000-s szabványcsalád előírásai szerint kidolgozni. A kidolgozott általános vezetési szabályzat alapján a híradó, valamint az informatikai szakterületek a 20000-es szabványcsalád, az információbiztonság szakterület a 27000-es szabványcsalád előírásait figyelembe véve dolgozhatnák ki az alapdokumentumaikat. Továbbiakban szeretném bemutatni, hogy melyek azok az alapelvek, amelyek mentén szükséges kifejleszteni a VIRTAR általános vezetési alapdoktrínáját, amely a későbbiekben alapja lehet a szabványcsaládokkal együtt a többi részterület alapdokumentumainak. (A részterületek doktrínáinak kidolgozása meghaladná a disszertációm kereteit ezért ezeknek a kidolgozásával nem kívánok foglalkozni.)

[36] Allied Quality Assurance Publications (AQAP).

2.4.1 A 9000-s szabványcsalád

A minőségirányítási szabványcsalád alkalmazása a közszférában és ezen belül az információs rendszerekben nem új keletű, amelyet bizonyít az Informatikai Tárcaközi Bizottság (ITB) 1996-ban kibocsátott 9-es számú ajánlása.

A 9000-es szabványcsalád eredetileg termelő szervezetek számára került kifejlesztésre, azonban a továbbfejlesztések alkalmával megállapításait általánosították annak érdekében, hogy azok mindenfajta szervezetre alkalmazhatók legyenek: „Az ebben a nemzetközi szabványban meghatározott minden követelmény általános, azzal a céllal, hogy minden szervezetre alkalmazhatók legyenek, azok típusától. méretétől és az általuk előállított termékfajtáktól függetlenül.” [47.]

A minőségirányítás alatt tehát olyan folyamatokat értünk, amely „…szisztematikus módon garantálja azt, hogy a tevékenységek az előzetes tervek szerint folyjanak és eképpen lényegében két részből áll: mit tegyen a szervezet és hogyan tegye azt.” [50.] A minőségirányítási rendszer pedig a „…a minőségirányítás megvalósításának az eszköze. Magában foglalja a minőség megvalósításában alkalmazott szervezeti struktúrát, felelősségeket, eljárásokat, folyamatokat és erőforrásokat”. [52.] Figyelembe véve ezen megállapításokat, valamint azon állítást, amely szerint „…a minőségirányítás rendszerének keretdokumentációját az intézményben felgyűlt tapasztalatok alapján kialakított belső szabványok, szabályzatok alkotják.” [51.], nagyon fontosnak tartom annak kimondását, hogy a minőségirányítás nem egy teljesen új rendszer kidolgozását jelenti, hanem a meglévő felhalmozott tudásbázisnak szab egyfajta keretet. Sajnos a tapasztalataim, a különböző szervezetek minőségüggyel foglalkozó szakembereivel való konzultációk alapján levont következtetéseim azt mutatják, hogy sok esetben a minőségügy önálló életet kezd élni és szinte teljesen függetlenné válik a szervezettől. Éppen ezért, nagyon fontosnak tartom, hogy egy termék vagy szolgáltatás minőségét a szervezetben dolgozó, szolgáló emberek biztosítsák. Ezen túl fontos, hogy velük értessük meg, leegyszerűsítve a minőségirányítás nem más, mint a legjobb gyakorlat írásba foglalása. A minőségügyi célok megvalósítása elképzelhetetlen a résztvevők tudatos közreműködése nélkül.

Az ITB 9-es ajánlása a minőségirányítási rendszer kialakításának folyamatát három fő fázisra osztja, ezek:

- Első fázis: A minőségirányítási rendszer meghatározása, ami alapvetően egy hatáselemzés és tényfeltárás elvégzését jelenti, amely meghatározza a szervezet „egészségi állapotát”.
- Második fázis: A minőségirányítási rendszer kialakítása, amelynek során költséghatékony „terápiát” alkalmaznak és kiképzik a munkatársakat a „megelőzés technikáira” annak érdekében, hogy a szervezet „állapota” javuljon vagy legalábbis ne romoljon.
- Harmadik fázis: A minőségirányítási rendszer javítása, amely a folyamatos önjavítást célozza meg a vevőktől, illetve a gazdálkodásból származó haszon növelése érdekében.

Ezt a három fázist az ajánlás összesen további nyolcvanhat feladatra bontja. Természetesen, ha valaki be akar vezetni egy minőségirányítási rendszert nem kötelező követni ezt a felosztást, a számokkal csak a tennivalók mennyiségét szerettem volna bemutatni. A minőségirányítási rendszert csak a rendszerben dolgozók, illetve a rendszert teljesen átvizsgáló szervezetek, vagyis csak azok, akik teljes rálátással vannak a rendszerre, tudnak eredményesen kialakítani. Ebből kifolyólag ebben a fejezetben csak arra vállalkozom, hogy az ajánlás szerinti megvalósíthatósági-, és szerintem az ettől elválaszthatatlan előzetes elemzést elvégezzem.

2.4.2 Minőségügyi megvalósíthatósági elemzés

A megvalósíthatósági elemzés során az olyan kérdésekre kell keresni a választ, amely válaszokat ad a minőségirányítási rendszer hasznosságát, lehetőségeit, kockázatait, korlátozásait illetően. Fontos megbecsülni a ráfordítás nagyságát is. A megvalósíthatósági/előzetes elemzésnek a részletesebb célja lehet, hogy megállapításra kerüljön:

- A javasolt minőségügyi kezdeményezés terjedelme és mérete, valamint a megvalósítás esetleges szakaszolása.
- Megállapítani, hogy van-e minőségirányítási rendszer, ha igen, az milyen mértékben valósult már meg és kielégíti-e a vevők és a szervezet igényeit.

- A jelenlegi irányelvek és eljárások eredményessége a minőség elérésében, beleértve az ISO 9001-gyel történő összehasonlítást.
- A minőségügyi célok és célkitűzések megértése és az irántuk való elkötelezettség a személyzet részéről.
- A minőségügyi költségek értékelése, valamint a minőségirányítási rendszer megvalósítási és irányítási költségének becslése.
- A megvalósítás prioritásai és alternatívái a kockázat, a veszteség, a haszon és a vevők elégedetlenségének tekintetében.
- Meghatározni e célkitűzések eléréséhez szükséges fejlesztéseket.
- Felmérni a minőségügyi képzésre vonatkozó igényeket.

Legelőször azonban tisztázni szükséges az alapvető fogalmakat, úgymint ***(be)szállító, szervezet, vevő.*** Véleményem szerint, a minőségirányítási rendszert a teljes VIRTAR vezetési rendszerére kell ki dolgozni.

A VIRTAR egészét tekintve szervezetnek a vevő kifejezés megfelel VIRTAR-t felhasználók körével, különös tekintettel a vezetőkre, parancsnokokra. A beszállítók a különféle technikai eszközöket a Magyar Honvédség részére felkínáló, eladó gyártók, valamint a különféle szolgáltatást biztosító szolgáltatók.

A második ilyen értelmezendő fogalom a folyamat, amely „…alatt a tevékenységek egy olyan sorozatát értjük, amelynek során jól meghatározott bemeneteknek terv szerinti kimenetekké való átalakítása történik meg. A folyamat egy vagy több műveletet, illetve eljárást alkalmazhat”. [53.] Ez alapján a VIRTAR vezetésében az alábbi folyamatok lehetségesek:

- Tervezési folyamatok:
  - Gyakorlatok, missziók VIRTAR-jának megtervezése.
  - A működő VIRTAR továbbfejlesztésének tervezése.
- Olyan üzemeltetési problémák kezelése, amelyek meghaladják az üzemeltető szervezet lehetőségeit.
- Oktatási feladatok tervezése, szervezése.
- Ellenőrzési feladatok.

- Beszerzési feladatok.

A javasolt minőségügyi kezdeményezés terjedelme és mérete, valamint a megvalósítás esetleges szakaszolása

A VIRTAR vezetése érdekében megvalósítandó minőségügyi rendszernek át kell fognia a teljes vezetési rendszert. Oly módon kell kialakítani, hogy megfelelő alapot adjon a szakterületek vezetési dokumentumainak kialakításához. Nem tartom célszerűnek a rendszer bevezetésének szakaszolást, mert a bevezetési munka elhúzódást jelentené haszon nélkül. A bevezetésre kerülő rendszer nagy valószínűséggel nem lesz tökéletes, erre a későbbi javító folyamatok során kell törekedni, de ez nem a szakaszolást jelenti hanem a minőségügyi rendszer sajátja.

Megállapítani, hogy van-e minőségirányítási rendszer, ha igen, az milyen mértékben valósult már meg és hogy kielégíti-e a vevők és a szervezet igényeit

Az első megközelítés alapján jelenleg nincs minőségirányítási rendszer a VIRTAR irányításában, azonban véleményem szerint ez így csak a tények sarkítása. Minden dolgozó, aki a fentebb felsorolt folyamatokban részt vesz, végez minőségügyi munkát csak legfeljebb nincs tudatában ennek. A véleményemet arra alapozom, hogy az elmúlt évek gyakorlatainak, illetve misszióinak vezetési és információs rendszere az elvárásoknak megfelelően került megtervezésre és üzemeltetésre. Amikor valamely ügyintéző az előző tapasztalataira alapozva, netán az elkövetett hibákat javítva végrehajt egy új feladatot „minőségügyi feladatot” lát el. Amennyiben létezik egyfajta legjobb gyakorlat, helyette nem kell újat kitalálni, csak a szabvány szerint dokumentálni kell.

A jelenlegi irányelvek és eljárások eredményessége a minőség elérésében, beleértve az ISO 9001-gyel történő összehasonlítást

Annak ellenére, hogy a katonai szakterminológia sok esetben nem egyezik az ISO 9000 szabványcsalád terminológiájával nagyon sok olyan feladat van, amely a honvédségi munkában már létezik, ezeket csak be kell illeszteni a kialakítandó minőségügyi rendszerbe. Ilyenek például a dokumentumkezelés. A 9001-es szabvány előírásai a dokumentumkezelésről:

„4.2.3.A dokumentumok kezelése

A minőségirányítási rendszer számára szükséges dokumentumokat ellenőrzés alatt kell tartani. A feljegyzések a dokumentumok sajátos típusát jelentik, és a 4.2.4. szakasz követelményei szerint kell azokat kezelni….

4.2.4. A feljegyzések kezelése

Feljegyzéseket kell készíteni, és ezeket meg kell őrizni, hogy bizonyítékul szolgáljanak arra, hogy a minőségirányítási rendszer megfelel a követelményeknek és eredményesen működik. A feljegyzések maradjanak olvashatók, legyenek könnyen azonosíthatók és kikereshetők. Dokumentált eljárást kell bevezetni a feljegyzések azonosításának, tárolásának, védelmének, kikeresésének, megőrzési idejének és selejtezésének szabályozására." [47.]

Ezeknek az előírásoknak teljes mértékben megfelel az érvényben levő a „Honvédelmi Minisztérium és a Magyar Honvédség Titokvédelmi és Ügyviteli Szabályzata (ált/3)", illetve a „Magyar Honvédség Egységes Iratkezelési Szabályzata (ált/40)" által előírt követelményrendszer. Mindkét szabályzat olyan, a szabvány által megkövetelt, dokumentált eljárás rendet biztosít, amely a helyes és következetes alkalmazásuk esetén megfelel a minőségirányítási rendszer számára.

„8.2.2. Belső audit

A szervezet végezzen tervezett időszakonként belső auditokat….". [47.]

Az auditoknak, amelyek tulajdonképpen egyfajta ellenőrzések, a lefolytatása az egyik legjobban szabályozott szakterülete a Magyar Honvédségnek. Ennél a pontnál sem kell új dolgokat megalkotni, csak figyelembe kell venni a következő előírásokat:

- 86/2008. (HK 17.) HM utasítás a folyamatba épített előzetes és utólagos vezetői ellenőrzési rendszer kialakításával kapcsolatos feladatokról
- 103/2007. (HK 18.) HM utasítás a külföldi szolgálatot teljesítők ellenőrzési rendjéről
- 95/2007. (HK 17.) HM utasítás a folyamatba épített előzetes és utólagos vezetői ellenőrzési rendszer kialakításával kapcsolatos feladatokról szóló 114/2005. (HK 1/2006.) HM utasítás módosításáról
- 81/2007. (HK 15.) HM utasítás a HM fejezet államháztartási belső ellenőrzési rendjének szabályairól, és a HM fejezet egységes államháztartási belső ellenőrzési kézikönyvének kiadásáról

- 52/2007. (HK 11.) HM utasítás a honvédelmi tárca ellenőrzési rendjéről

A példákat lehetne folytatni, de itt csak lényeget szerettem volna bemutatni, másrészt a VIRTAR irányítási munkáiban előfordulnak nem publikus utasítások is. A meglévő utasítások beépítése a minőségügyi rendszerbe a kialakítási munkafázis része és a kialakításban résztvevők feladata.

A minőségügyi célok és célkitűzések megértése és az iránt uk való elkötelezettség a személyzet részéről

Véleményem szerint a minőségügyi rendszer bevezetésének legkritikusabb területe az, hogy a szervezet személyzete megértse a célokat. Amennyiben nem sikerül mozgósítani az állományt a feladat végrehajtására, abban az esetben a rendszer bukásra van ítélve. Ebben az esetben valószínűleg el fognak készülni a szükséges dokumentumok, de azoknak a „legfontosabb" célja az lesz, hogy legyen, így a minőségügy l'art pour l'art célúvá válik. A folyamatoktól ezért teljesen elkülönült önálló életet fog élni és a célkitűzései nem fognak megvalósulni. Ezért mindenképpen fontos, hogy megértessük a személyzettel, hogy mi az amiért a jelenben többletmunkát kérünk, miért kell továbbképzéseken részt venniük és az hogyan térül meg számukra a jövőben.

A minőségügyi költségek értékelése, valamint a minőségirányítási rendszer megvalósítási és irányítási költségének becslése.

A VIRTAR minőségügyi költségei alapvetően két részre bonthatók. A minőségüggyel legfelsőbb szinten foglalkozók minőségügyi tanfolyamainak költségére, valamint a személyzet többi tagjának a bevezetéskor szükséges plusz munkájára, illetve az ezzel kapcsolatos továbbképzések miatti munkaidő kiesésre. Nem látom célszerűnek ebben az esetben, hogy a minőségügyi rendszer kialakítását egy külsős céggel valósítsák meg, mert egyrészről a rendszerben dolgozók sokkal jobban át tudják látni a saját feladataikat, másrészről egy ilyen folyamatelemzés a külsős cégnek többlet erőforrást és így számunkra többletköltséget okozna. Harmadrészt a kezelt adatok érzékenysége miatt nem is biztos, hogy a megfelelő betekintési követelményeknek a külsős cég eleget tud tenni.

A megvalósítás prioritásai és alternatívái a kockázat, a veszteség, a haszon és a vevők elégedetlenségének tekintetében

Bár véleményem szerint a minőségügyi rendszert nem fokozatosan, hanem egyszerre célszerű bevezetni, azért a különböző prioritásokat előnyben kell részesíteni. Azt, hogy melyek ezek a prioritások mindig az adott munkafázis dönti el. Példának okáért, abban az esetben, amikor a Magyar Honvédség szervezetei egy missziós feladatra készülnek, akkor a prioritást az adott misszió VIRTAR-jának a megtervezése és megszervezése jelenti. Amennyiben ez az időszak egybe esik a minőségügyi rendszer bevezetésével, akkor erre kell fókuszálni. Másik példa lehet az is, amely során ha semmilyen egyéb feladat nincs, akkor a prioritást a működő VIRTAR továbbfejlesztésének tervezése, kell hogy kapja.[37] Tisztázni szükséges, hogy milyen hasznok származhatnak a rendszer bevezetéséből. Véleményem szerint a vezetés számára a következők jelenthetik a hasznot (az ITB 9-es ajánlásával összhangban):

- jobb lehet a vertikális és horizontális irányú kommunikáció,
- nagyobb hangsúly kerül a vevővel történő kapcsolattartásra,
- a csoportok között javul a kapcsolat,
- a munkatársak nagyobb mértékben érzik magukat késztetve és képesítve javító célzatú indítványok megtételére,
- a szervezeten belüli súrlódások csökkennek,
- a kétértelműségek és félreértések előfordulása csökken,
- jobb lesz a vezetés,
- a szervezeti célkitűzések és a vevők igényei tisztábbak lesznek,
- a vezetés és a dolgozók hozzáértőbbek és motiváltabbak lesznek,
- a képzési igények és a szükséges képzettség meghatározása javul,
- az egész szervezetben nagyobb hangsúly helyeződik a minőségre,

[37] Ilyen példa például a Nemzetvédelmi Egyetem minőségügyi rendszerének szervezése, ahol is először az oktatás minőségügyi rendszerének a kidolgozását hajtottuk végre, a kutatás-fejlesztés minőségügyi rendszerének a kidolgozása a későbbiekben fog megtörténni.

- a szolgáltatások nyújtása, illetve a termékek előállítása szisztematikusabb lesz,
- a veszteség (felesleges munka, az átdolgozásból adódó munka) megelőzésére irányuló törekvések hatékonyabbá válnak,
- az erőforrások tervezése és felügyelete javul,
- a felelősségek, hatáskörök és megbízások tisztábbak lesznek,
- az együttműködési készség javul,
- csökken a veszélye a nem kívánt kötelezettségvállalásnak,
- a teljesítményre és a trendekre vonatkozó információk pontosabbakká válnak,
- a munkatársak kinevezése, beosztása rugalmasabbá válik,
- rövidebb idő szükséges a munkavégzéssel kapcsolatos információk feldolgozásához és felhasználásához,
- javul a lényegi információkhoz való hozzáférés.

A VIRTAR irányítását végző szervezetnek a minőségügyi rendszer megvalósításakor a alábbi kockázati tényezőkkel kell számolnia:

- a teljes költség figyelmen kívül hagyása (fel nem ismerése) és itt kifejezetten a rendszer bevezetésekor szükséges többlet munkaigény alábecsülése,
- a szervezet munkatársaira háruló többletmunka átmeneti megnövekedése,
- az erőforrások helytelen elosztása,
- a folyamatban lévő munkákra gyakorolt hatás,
- a minőségirányítási kezdeményezés nem megfelelő irányítása,
- a szervezet kultúrájára gyakorolt negatív hatás.

Összességében a legnagyobb kockázatot az jelenti, ha minőségügyi rendszer csak „papíron” működik, mert ekkor a bevezetésére fordított ráfordítások csak plusz

kiadást jelentenek, és a rendszer nem hogy segítené, de gátolja a szokásos munkarendet.

Meghatározni e célkitűzések eléréséhez szükséges fejlesztéseket

Megítélésem szerint a VIRTAR vezetésében kifejlesztendő minőségügyi rendszer jelentős fejlesztéseket nem igényel, a legjelentősebb feladat a kapcsolódó dokumentáció kialakítása.

Felmérni a minőségügyi képzésre vonatkozó igényeket

Véleményem szerint a kialakításra tervezett rendszerben az ajánlásokkal ellentétben nem szükséges külön, csak a minőségüggyel foglalkozó menedzsmentet létrehozni, hanem a meglévő személyzet között kell szétosztani a feladatokat. E metódus eleinte többlet terhet ró az érintettekre, de a jól működő rendszer ezt később megtéríti. A minőségügyi rendszer legfontosabb eleme a vezetés elkötelezettsége, ezért a minőségügyért felelős vezetőt is a rendszer lehetőség szerinti legmagasabb pontján kell kijelölni. Ez a vezető lehet a VIRTAR irányításért egy személyben felelős vezető közvetlen, intézkedésre jogosult helyettese. A minőségügyi vezető képzését pedig mindenképpen végre kell hajtani a lehető legjobb minőségben. E képzést nem lehet megoldani önképzés keretében, erre mindenképpen a képzésre akkreditált céget, iskolát kell igénybe venni. A személyzet további képzését ennek, a már jól felkészült vezetőnek kell megszervezni. Elengedhetetlennek tartom a képzést, de ennél is fontosabb lehet a személyzet megnyerése a feladathoz, vagyis az, hogy megértsék a rendszer bevezetésének szükségességét.

A megvalósíthatósági elemzésemet tekintve összességében megállapítható, hogy a VIRTAR irányítási keretrendszerét ki lehet dolgozni a 9000-es szabványcsalád alapján, azonban ez a kidolgozás erőforrásokat igényel, amelyek a felső vezetés képzési költségeiben, a dolgozók kiképzésében, valamint a kidolgozói munkára fordítandó többlet munkaidő igényben rejlenek. A minőségügyi rendszerből adódó előnyök azonban csak akkor realizálódhatnak, ha a vezetési rendszerben dolgozók megértik a minőségügyi rendszer folyamatait, azok szükségességét, és nem csak egy felesleges, a munkájukat növelő feladatot látnak benne. A legnagyobb kockázat tehát az, ha minőségügyi rendszer öncélúvá válik.

2.5 A VIRTAR üzemeltetésével kapcsolatos tevékenységek. A hálózat felügyelet és a számítógépes incidenskezelő központ feladatai.

Mint arról már a 2.3 fejezetben volt szó, a híradó és informatikai rendszer vezetése magában foglalja a hadműveleti és az üzemeltetést irányító funkciókat is. És arról is volt szó, hogy az üzemeltetést irányító funkciók két részből kell, hogy álljanak, a hálózat felügyelet valamint a veszélyjelző és incidenskezelői feladatokból. A továbbiakban ennek a két területnek a feladatait vizsgálom meg.

2.5.1 Hálózat felügyelet feladatai:

Ezt a feladatot jelenleg a MH Támogató Dandár keretében működő Hálózat Felügyeleti Központ látja el, amelynek a deklarált feladata: [43.]

„Az MH zártcélú híradó és informatikai hálózatának központiüzem-felügyelete, menedzselése, a menedzsmentrendszer üzemeltetése, a szerviztevékenység központi irányítása, országos szintű műszaki nyilvántartás vezetése;”. [42.]

Ami részletesen az alábbiakat jelenti:

- Szoftveres és hardveres frissítések végrehajtása

A tesztkörnyezetben előzetesen tesztelt verziófrissítések, verziócserék nyomon követése. Vírusinformációk frissítésének telepítése, hálózati vírusellenőrzés lefuttatása. A vírusellenőrzésről készült REPORT-ok archiválása, gyűjtőzése, szükség esetén visszakeresése Szoftverfrissítések, biztonsági frissítések telepítésének végrehajtása, dokumentálása.

- A rendszer felügyelete

A rendszer aktív hálózati elemeinek rendszer-felügyeleti eszközök segítségével történő folyamatos ellenőrzése, az esetleges változások okainak kiderítése, szerverek felügyelete, tűzfalak működésének ellenőrzése, hálózati elemek, aktív eszközök IP címének folyamatos, naprakész nyilvántartása, az ezzel kapcsolatos adatok pontosítása, szerverek elérhetőségének, a szolgáltatások hozzáférhetőségének vizsgálata. Az eredmény függvényében a szolgáltatások rendszergazdájának értesítése.

- Kapcsolattartás

Folyamatos kapcsolattartás a szerződéses polgári és a katonai szolgáltatók, a katonai szervezetek együttműködő informatikai állományával.

- Működőképesség ellenőrzése, hibák javítása

Az informatikai és híradó hálózatok működőképességének ellenőrzése, a felmerülő hibák gyors és szakszerű elhárítása. A hibabejelentések fogadása, a szükséges adatok rögzítése. A hibaelhárítással kapcsolatos tapasztalatok kiértékelése és bevezetése az adatbázisba. A hibák jövőbeni bekövetkezésére utaló előjelek, hibajelenségek figyelemmel kísérése (pl.: rendellenes, kiszámíthatatlan működés) és javaslattétel a megelőzésre. A szolgálatellátás ideje alatt detektált rendellenességek okainak pontosítása a területileg illetékes informatikai szakállomány segítségével.

- Híradó és informatikai támogatás végrehajtása

A külföldi és hazai gyakorlatok, a missziók informatikai és híradó biztosítási feladatainak támogatása.

- A naplófájlok kezelése

Naplófájlok rendezése típus szerint (alkalmazás, biztonsági, rendszer), időszakonkénti archiválása.

- Véleményezés, bedolgozás

Az MH zártcélú híradó és informatikai hálózatának üzemeltetésével, szolgáltatások igénybevételével kapcsolatos szabályozó okmányok előkészítése, a hálózatgazda jóváhagyásával történő kiadása. Az MH zártcélú híradó és informatikai rendszerei fejlesztési és beruházási terveinek előkészítésében való részvétel, adatszolgáltatás biztosítása;

- Tudakozó és help desk

2.5.2 Számítógépes incidenskezelő központ (CIRC) feladatai :

Véleményem szerint akkor, amikor meghatározzuk a CIRC feladatait nem kell nóvumokat kreálni, elég ha a Magyar Honvédség szervezetére adaptáljuk az országos hatókörrel működő CERT-Hungary Központ feladatait amelyek így a következők lehetnek [44.]:

- Jelzések és figyelmeztetések adása

Ez a szolgáltatás olyan információk elterjesztését jelenti az alakulatok és szervezetek üzemeltetői felé, amelyekben a CIRC leír egy támadást, biztonsági rést, behatolás figyelmeztetést, illetve vírustámadást és egyúttal megoldási javaslatot tesz a probléma megoldására. A jelzések, figyelmeztetések és tanácsok a jelzett problémákra válaszul kiküldött reakciók, amelyek segítségével értesítik a szervezeteket a veszélyekre és megoldási javaslatot adnak, illetve visszaállítási lépésekre tesznek javaslatot az érintett rendszerek számára.

- Értesítések a szervezeteknek

Az értesítések magukba foglalják többek között a behatolási figyelmeztetéseket, sérülékenység figyelmeztetéseket és a biztonsági tanácsokat. Az értesítéseken keresztül a CIRC informálja a védett szervezeteket a közép- és hosszú távú hatással bíró új fejlesztésekről, valamint az újonnan észlelt sérülékenységekről és behatoló eszközökről. Az értesítések segítségével a szervezetek felkészülhetnek, hogy megvédjék a rendszereiket és hálózatukat az új kártékony informatikai termékektől, mielőtt azokkal bárki támadást indíthatna.

- Biztonsággal kapcsolatos információk terjesztése

A központ ezzel a szolgáltatással a védett szervezetek számára nyújt olyan átfogó, hasznos és könnyen kereshető információkat, amelyek segítségével növelhető a biztonság a szervezeteknél.

- Incidenskezelés

A biztonsági incidens lehet illetéktelen hozzáférés egy számítógépes rendszer adataihoz, szolgáltatásmegtagadásos támadás, vírus a számítógépeken, szoftver sérülékenység vagy egyéb a számítógépes rendszerek biztonságát fenyegető tevékenységek, kódok vagy hibák. Az incidenskezelés szolgáltatás során a CIRC megkapja, értékeli, analizálja a jelentett incidenseket és azokra reagál. Az egyes lehetséges intézkedések lehetnek:

- A behatoló aktivitása által érintett, illetve fenyegetett rendszer, vagy hálózat védelme érdekében való beavatkozás,
- Megoldások biztosítása, vagy stratégia kidolgozása a releváns figyelmeztetések függvényében,

- Behatolók aktivitásának keresése és figyelése a hálózat más szegmenseiben,
- Hálózati forgalom figyelése és szűrése,
- Más intézkedések és módszerek kidolgozása.

- Sérülékenység kezelés

A sérülékenység kezelési szolgáltatások során a CIRC információkat és jelentéseket kap a hardver és szoftver sérülékenységekről, analizálja a sérülékenységek természetét, mechanizmusát és a hatásait. Megoldási stratégiákat fejleszt a sérülékenységek detektálására és javítására.

- Kártékony informatikai termékek kezelése, jelentése a szervezeteknek.

Kártékony informatikai termékek mindazok a fájlok, objektumok és kódok, amelyek nagy valószínűséggel az informatikai rendszerek, illetve hálózatok elleni próbálkozások, vagy támadások segédeszközei, illetve maradványai. Ezek lehetnek többek közt vírusok, trójai programok, férgek, kiaknázó „scriptek” és segédeszközök. A CIRC információkat és másolatokat kap ezekről a kártékony informatikai termékekről, majd átvizsgálja őket. A vizsgálat során analizálja a természetüket, mechanizmusukat, verziójukat és használatuk módját, majd válaszadási stratégiát fejleszt ki detektálásukra, eltávolításukra és az ellenük való védekezésre.

2.6 A VIRTAR vezetési szintjei

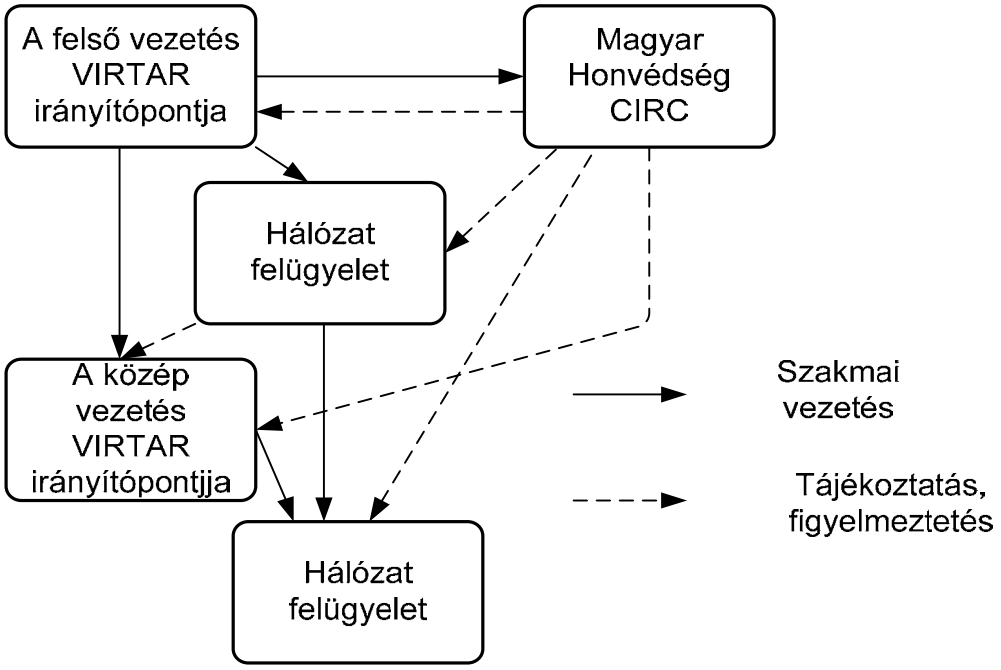
Nagyon fontos kérdésnek tartom annak eldöntését, hogy a fentiekben tárgyalt vezetési funkciók milyen szinteken kell, hogy megjelenjenek. Véleményem szerint a békevezetésnek nem szabad különbözőnek lenni a „hadműveleti” vezetéstől ezért azt a kérdést, hogy milyen szinteken kell létrehozni a különböző vezetési elemeket, az összhaderőnemi doktrína határozza meg:

„a híradó és informatikai rendszerek vezetése érdekében a katonai felső vezetés és a középszintű vezető szerv állít fel és működtet híradó irányító és hálózat-felügyeleti szolgálatokat;” [45.]

Ezeket a vezetési elemeket azonban, mint ahogy bemutattam, ki kell egészíteni az MH CIRC-cel. A bemutatott feladataiból azonban könnyen belátható, hogy

elegendő egyetlen szinten, a felső vezetés szintjén létrehozni, az alsóbb szinteken létrehozásra kerülő Incidenskezelő központok csak felesleges redundanciát vinnének a rendszerbe.

Az így létrejövő vezetési rendszert a 13. ábra mutatja.



13. ábra A VIRTAR vezetési rendszer

2.7 Összegzés, következtetések

A vezetési és információs rendszer technikai alrendszerének (VIRTAR) irányítása nem lehet más, nem alkalmazhat más módszereket, mint a Magyar Honvédség általános vezetése, vagyis a VIRTAR irányításának szervesen integrálódnia kell a honvédség vezetési struktúrájába. Jelenleg a Magyar Honvédség vezetését a szolgálati elöljárói, illetve a szakmai vezetés jellemzi. A vezetés eszközei a különböző kiadványok.

Azonban a nyílt formában elérhető dokumentumok alapján, nehezen látható át a vezetési rendszer elemeit képező dokumentumok (utasítások, szabályzatok, főnökségi kiadványok, doktrínák stb.) struktúrája, az egymáshoz való viszonyuk kiszámíthatatlan. Ez a legnagyobb problémát azért jelenti, mert nehéz őket a szövetségi rendszerünk által megkövetelt sémába illeszteni őket, vagyis

adminisztratív területen, a szabályzók kiadásakor is törekednünk kell az interoperabiltiás megvalósítására. A különböző dokumentumok kidolgozásakor elkötelezetteknek kell, lennünk, hogy kifejlesszük, elfogadjuk és megvalósítsunk fogalmakat, doktrínákat, folyamatokat és mintákat, amelyek alapján elérjük és fenntartsuk az interoperabilitást. Ez a kompatibilitás, felcserélhetőség, azonosság szükséges szintjének létesítését igényli hadműveleti, eljárási, anyagi technikai és adminisztratív területen is.

A különböző szakterületek szabályozását előíró NATO dokumentumok legtöbbje beleilleszthető egy négyes sémába, amelynek az elemei a politikák, direktívák, irányelvek, valamint egyéb támogató dokumentumok. Amennyiben a vezetési és irányítási dokumentumainkat kompatibilissé akarjuk tenni a NATO-val, két lehetőségünk van:

- A jelenlegi rendszert teljesen felülbírálva, a NATO terminológiát alkalmazzuk, amely azonban nagyon nagy, egyszer elvégzendő munkát jelent;
- A jelenlegi rendszert meghagyjuk, viszont a már meglévő belső utasításainkat megfeleltetjük a NATO ekvivalens dokumentumaival. A feladat végrehajtása nem tekinthető egyszerű feladatnak, mert vannak olyan szabályzataink, amelyek nem csak egy NATO - dokumentum szintnek felelnek meg, hanem többet is felölelhetnek.

A VIRTAR vezetése a szakmai vezetés körébe tartozik. Megállapítható azonban, hogy a három szakterület, úgymint az adatfeldolgozás, az adattovábbítás, illetve az adatbiztonság vezetése nincs egy kézben, a közöttük levő viszonyok jogszabályilag nem rendezettek. Megítélésem alapján a három alapterület szakirányítását egy szolgálati személynek kellene végeznie.

A VIRTAR szakmai vezetési rendszerét megvizsgálva észrevehetjük, hogy a többi szakmai vezetési rendszertől van egy jelentős eltérés is, ami nem más mint az, hogy a szakmai vezetésnek folyamatosan felügyelnie kell egy működő rendszert is.

A VIRTAR irányítási dokumentumrendszerében tovább bonyolítja a helyzetet, hogy az egyetlen érvényben levő szabályzat is elavult. Igaz, annak ellenére, hogy nincs egységes szabályzat az élet nem állt meg, így mind a VIRTAR, mind annak

irányítása is működőképes volt, aminek legjobb példája a Magyar Honvédség által végrehajtott missziós feladatok. Ezek nem lehettek volna sikeresek a megfelelő szintű és biztonságos híradó és informatikai támogatás nélkül. Ennek ellenére szükség van a mindhárom szakterületet átfogó dokumentumrendszer kialakítására.

Véleményem szerint a Magyar Honvédség előtt álló fejlesztési feladatok hálózatközpontú környezetben való alkalmazás képessége megköveteli a VIRTAR korszerű szemléletű vezetését. Bármiféle vezetési rendszert is alakítunk ki, célszerű azt írásban rögzíteni. Erre azért is szükség lehet, mert az elmúlt évek tapasztalatai alapján kijelenthető, hogy mindenféle szervezeti egységben, így az irányítást végrehajtó szervezetekben is nagy a fluktuáció, ezért egy leírt módszer esetében nem kell minden kidolgozói és alkalmazói munkát előröl kezdeni.

Az Magyar Honvédség előtt álló egyik legnagyobb feladat a hálózat nyújtotta képességek kialakítása, azt is láthattuk, hogy ez nem csak kifejezetten katonai feladat, ebben részt fognak venni a különböző kutató bázisok, és polgári szervezetek is. A különböző nemzeteknek és szervezeteknek jelenleg nem egységes a vezetési rendszerük, az egységesítés eszköze lehet a polgári életben már bevált nemzetközi szabványokon alapuló vezetési rendszer.

A dolgozatomban megvizsgáltam annak lehetőségét, hogy a polgári életben alkalmazott minőségirányítási szabványcsalád alkalmazása mennyire lehetséges erre a feladatra. A 9000-es szabványcsalád eredetileg termelő szervezetek számára került kifejlesztésre, azonban a továbbfejlesztések alkalmával a megállapításait általánosították annak érdekében, hogy a szabványban meghatározott követelmények minden szervezetre alkalmazhatók legyenek, azok típusától. méretétől és az általuk előállított termékfajtáktól függetlenül.

A minőségirányítás alatt olyan folyamatot értünk, amelyek szisztematikus módon garantálják azt, hogy a tevékenységek az előzetes tervek szerint folyjanak és ekképpen lényegében két részből állnak: mit tegyen a szervezet és hogyan tegye azt. A minőségirányítási rendszer pedig a minőségirányítás megvalósításának az eszköze, magában foglalja a minőség megvalósításában alkalmazott szervezeti struktúrát, felelősségeket, eljárásokat, folyamatokat és erőforrásokat.

A minőségirányítás rendszerének keretdokumentációját az intézményben felgyűlt tapasztalatok alapján kialakított belső szabványok, szabályzatok alkotják,

ezért nagyon fontos, hogy a minőségirányítás nem egy teljesen új rendszer kidolgozását jelenti, hanem a meglévő, felhalmozott tudásbázisnak szab egyfajta keretet. Nagyon fontos viszont, hogy a szervezetben dolgozó emberekkel értessük meg, hogy leegyszerűsítve a minőségirányítás nem más, mint a legjobb gyakorlat írásba foglalása. A minőségügyi célok megvalósítása elképzelhetetlen a résztvevők tudatos közreműködése nélkül.

A megvalósíthatósági elemzésemet tekintve összességében megállapítható, hogy a VIRTAR irányítási keretrendszerét ki lehet dolgozni a 9000-es szabványcsalád alapján, azonban ez a kidolgozás erőforrásokat igényel, amelyek a felső vezetés képzési költségeiben, a dolgozók kiképzésében, valamint a kidolgozói munkára fordítandó többlet munkaidő igényben rejlenek. A minőségügyi rendszerből adódó előnyök azonban csak akkor realizálódhatnak, ha a vezetési rendszerben dolgozók megértik a minőségügyi rendszer folyamatait, azok szükségességét, és nem csak egy felesleges, a munkájukat növelő feladatot látnak benne. A legnagyobb kockázat tehát az, ha minőségügyi rendszer öncélúvá válik. Vagyis a rendszer működőképessége nem a ráfordítások nagyságától függ, hanem attól, hogy a rendszerben tevékenykedő szakemberek mennyire értik meg és fogadják el a minőségügyi rendszert.

Ezt az irányítást a vezetés jelenleg a hálózat-felügyeleten keresztül gyakorolja. Ebben a fejezetben bemutattam, hogy a technikai fejlődés magával hozott olyan negatív változásokat is, amelyek indokolttá teszik a hálózat-felügyelet mellett a Magyar Honvédségben is létrehozni a számítógép veszélyjelző és incidenskezelő központot (CIRC). Ebben a fejezetben bemutattam továbbá a hálózat-felügyelet és az incidenskezelő központ viszonyrendszerét és áttekintettem mindkettő feladatkörét.

A Hálózat Felügyeleti Központ feladatai közé tartozik a szoftveres és hardveres frissítések végrehajtása, a rendszer felügyelete, folyamatos kapcsolattartás a szerződéses polgári és a katonai szolgáltatók, a katonai szervezetek együttműködő informatikai állományával, működőképesség ellenőrzése, hibák javítása, a külföldi és hazai gyakorlatok, a missziók informatikai és híradó biztosítási feladatainak támogatása, a naplófájlok kezelése, a tudakozó és help desk szolgáltatás üzemeltetése

Számítógépes incidenskezelő központ (CIRC) feladatai: jelzések és figyelmeztetések adása, olyan információk elterjesztése amelyekben a CIRC leír egy

támadást, biztonsági rést, behatolás figyelmeztetést, illetve vírustámadást és egyúttal megoldási javaslatot tesz a probléma megoldására. Értesítések a szervezeteknek, amelyek többek között a behatolási figyelmeztetéseket, sérülékenység figyelmeztetéseket és a biztonsági tanácsokat. Kártékony informatikai termékek kezelése, jelentése a szervezeteknek.

A békevezetésnek nem szabad különbözőnek lenni a „hadműveleti" vezetéstől ezért a VIRTAR különböző szintű vezetési elemeit, a katonai felső vezetés és a középszintű vezető szerv keretei között kell működtetni. A CIRC bemutatott feladataiból azonban könnyen belátható, hogy ezt az elemet elegendő egyetlen szinten, a felső vezetés szintjén létrehozni, az alsóbb szinteken létrehozásra kerülő Incidenskezelő központok csak felesleges redundanciát vinnének a rendszerbe.

A fejezetben foglaltakat mérlegelve az alábbi következtetéseket vonom le:

1) A vizsgálat időszakát tekintve kijelenthető, hogy a VIRTAR három alapvető szakterületét illetően a vezetés egységessége nem valósult meg, a szakterületi viszonyrendszer korrekt rendezése nem teljesült;

2) A technológiai fejlődés következtében megváltozó szövetségesi alkalmazási lehetőségek hazánk tekintetében is előre vetítik a számítógép veszélyjelző és incidens központ (CIRC) megszervezésének és működtetésének szükségességét;

3) A VIRTAR vezetésének kialakítását célszerű a megfelelő szabványcsaládra, valamint bevált gyakorlatokra alapozva végrehajtani.

3 A vezetési és információs rendszer biztonsága

„A kormányzati és üzleti szervezetek nagymértékben az információk használatára támaszkodnak üzleti tevékenységük irányítása során. Az információ és a szolgáltatások bizalmasságának, sértetlenségének, rendelkezésre állásának, letagadhatatlanságának, számonkérhetőségének, azonosíthatóságának és megbízhatóságának elvesztése igen káros hatással van a szervezet üzleti működésére. Következésképp az információk védelme és az informatikai rendszerek biztonságának menedzselése a szervezeten belül kritikus fontosságú.” [55.]

Az MSZ 13335-es szabványból citált idézet sehol sem olyan aktuális, mint a honvédségi rendszerekben, ahol adott esetben (konfliktusok, missziók) emberéletek és akár a küldetés sikere is múlhat az információbiztonságon. Az információbiztonság fontosságát a NATO tervezett híradó doktrínája is megerősíti:

„A biztonságos kommunikáció és adatátvitel lehetőségének megtestesítettnek kell lennie bárhol ahol katonai műveleteket, terveznek, illetve hajtanak végre.” [38] [58.]

3.1 Az információbiztonság szakterületei

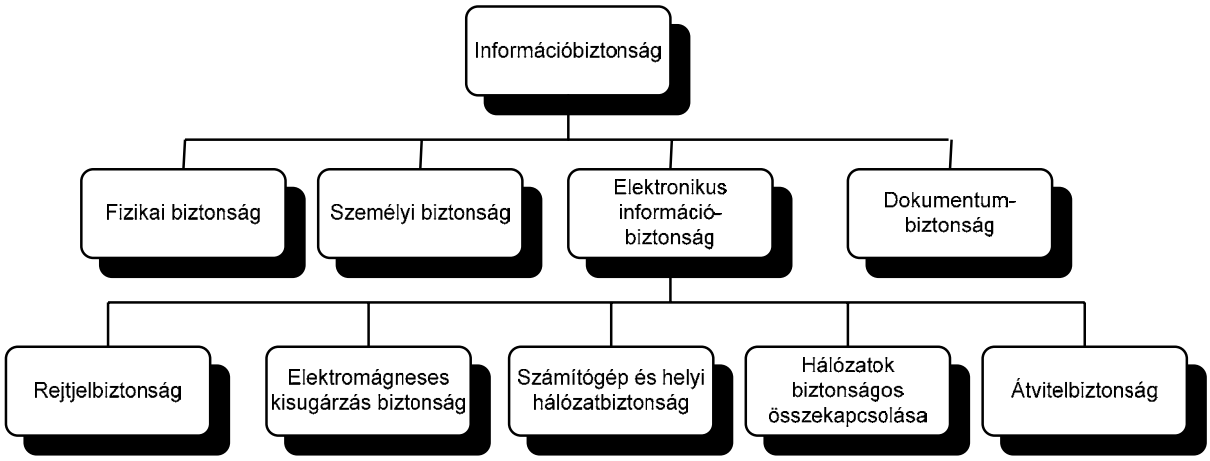
Az információbiztonsági feladatok szakterületekre bontásához többfajta modell létezik, amelyek közül a vizsgálatomhoz a NATO modellt választottam. Az információbiztonság NATO modelljét a „C-M(2002)49 Security Within The North Atlantic Treaty Organisation (NATO)” című dokumentum taglalja, amely a NATO-n belül a minősített információk védelmének alapdokumentuma:

„Az elektronikus információbiztonság a biztonsági rendszabályok alkalmazása annak érdekében, hogy megvédjük egyrészről a feldolgozott, tárolt vagy továbbított információt a kommunikációs, informatikai vagy más elektronikus rendszerben akár szándékosan, akár véletlenül bekövetkező bizalmasságának, teljességének és rendelkezésre állásának elvesztésétől, másrészről a rendszert a bizalmasságának, teljességének és rendelkezésre állásának elvesztésétől. Mindezt tesszük annak érdekében, hogy elérjük a minősített információ bizalmasságának, sértetlenségének, rendelkezésre állásának biztonsági célját a kommunikációs, informatikai és más elektronikus hálózatokban, amelyekben feldolgoznak, tárolnak, illetve továbbítanak információkat. Célunk kiegyensúlyozottan alkalmazni a biztonsági rendszabályokat

[38] „Secure communications and data transfer capabilities should be incorporated wherever military operations are planned or executed.”.

(fizikai, személyi, dokumentum és elektronikus információbiztonság) annak érdekében, hogy megalkossuk a biztonsági környezetet, amelyben a kommunikációs, informatikai és más elektronikus hálózatok működhetnek.” [56.][39]

„… az elektronikus információbiztonság technikai és megvalósítási szempontjai (amely magában foglalja a számítógép és helyi hálózat (LAN) biztonságot, a hálózatok biztonságos összekapcsolását, a rejtjelbiztonságot, az átvitel biztonságot, és a kisugárzás biztonságot).”[57.][40]



14. ábra Az Információbiztonság szerkezete a C-M(2002) 49 alapján

A NATO tehát az információbiztonság feladatait négy fő kategóriába osztja:

- fizikai biztonság,
- személyi biztonság,
- dokumentum biztonság,
- elektronikus információbiztonság.

Az elektronikus információbiztonság feladatai további öt feladatcsoportba oszthatók:

- számítógép és helyi hálózat (LAN) biztonság,

[39] „INFOSEC is the application of security measures to protect information processed, stored or transmitted in communication, information and other electronic systems against loss of confidentiality, integrity or availability, whether accidental or intentional, and to prevent loss of integrity or availability of the systems themselves. In order to achieve the security objectives of confidentiality, integrity and availability for classified information stored, processed or transmitted in communication, information and other electronic systems, a balanced set of security measures (physical, personnel, security of information and INFOSEC) shall be implemented to create a secure environment in which to operate a communication, information or other electronic system.

[40] „INFOSEC technical and implementation aspects (including computer and local area network (LAN) security, interconnection of networks security, cryptographie seçurity, transmission security, and emission security).”

- hálózatok biztonságos összekapcsolása,
- a rejtjelbiztonság,
- elektromágneses kisugárzás biztonság vagy másképpen kompromittáló kisugárzás biztonság,[41]
- átvitelbiztonság.

A biztonsági részterületek egymáshoz való viszonyát a 14. ábra szemlélteti. A négy elem között *fontossági sorrendet, alá-fölérendeltségi viszonyt nem lehet meghatározni.*

3.1.1 Az információbiztonsági szakterületek alapvető feladatai

A szakterületek nem szeparálhatók el egymástól, néhol bizonyos átfedések lehetségesek.[42] Az elektronikus információbiztonság két legrégebbi szakterülete a rejtjelbiztonság és az átvitelbiztonság (régi szakterminológiával élve híradóbiztonság) amelyeknek akkor van szerepük, ha az információ az ellenőrzött területen kívülre kerül. Mind a rejtjelbiztonság kérdéseivel, mind a többi három biztonsági területtel (számítógép és helyi hálózat (LAN) biztonság, a hálózatok biztonságos összekapcsolása, elektromágneses kisugárzás biztonság) a szakirodalom egyre bővülő tárháza foglalkozik,[43] azonban az átvitelbiztonság kérdésköre nagyrészt feldolgozatlan. Ebből kifolyólag ebben a fejezetben kifejezetten csak az átvitelbiztonsággal foglalkozom.

3.2 Átvitelbiztonság

Az átvitelbiztonság kérdésköre nagyrészt feldolgozatlan, amely véleményem szerint két okra vezethető vissza:

- a katonai hálózatokban az átviteli rendszerek nem csak homogén számítógépes hálózatokból állnak, mint a mai polgári architektúrák, hanem tartalmaznak a katonai innfokommunikációs hálózatokra jellemző eszközöket is (pl. különféle rádiók), és minden rendszerelem különböző

[41] A szakzsargonban az USA-ban használatos kódnéven említve TEMPEST
[42] Ilyen lehet például, a TEMPEST szobák érdekében végzendő Faraday kalitka kialakítása, amit célszerű az egyéb fizikai követelmények (rácsok, ajtók, stb..) kialakításakor elvégezni.
[43] Ezekre a szakirodalmakra példa a különböző szabványok, például a 27000-s szabványcsalád, 11770-s szabványok stb.

fenyegetettségekkel is szembenéz, ezért nehéz az egységes védelmi profil kidolgozása,

- a polgári életben a legtöbb szereplő az átviteli utat megvásárolja egy szolgáltatótól (pl.: Internet kapcsolat, mobiltelefonos szolgáltatás), így e rendszerek biztonságával a szolgáltatónak kell foglalkozniuk. A gyakorlat azt mutatja, hogy behatárolt azon szolgáltatóknak a száma, amelyek e kérdéskörrel foglalkozni tudnak. A katonai rendszerekben alapállapotban (békehelyzetben) is ilyen jellegű rendszerek dominálnak, azonban fel kell készülnünk olyan helyzetekre is amikor polgári cégek szolgáltatásait, vagy előre telepített zártcélú hálózatokat nem tudunk igénybe venni.

3.2.1 Az átviteli út és az átvitelbiztonság meghatározása

Ahhoz, hogy az átvitelbiztonság feladatait tisztázni tudjuk először is meg kell határozni az átviteli út és az átvitelbiztonság fogalmát. Első megközelítésben az átviteli út a transzport hálózatot[44] megvalósító eszközök összessége, azonban ha abból indulunk ki, hogy feltételezzük, az ellenség minden olyan összeköttetésünket értékelni és manipulálni tudja amelyet mi nem tartunk folyamatosan a felügyeletünk alatt akkor, azokat az összeköttetéseket is ide kell sorolni amelyek ugyan a belső hálózat összeköttetéseit valósítják meg, de az általunk ellenőrzött teret elhagyják, elhagyhatják. Ez alapján az átviteli út fogalma:

Az átviteli út mindazon hír, adat és információ továbbító csatornák (továbbiakban összeköttetések), jellegüktől és felépítésüktől, összetételüktől hosszúságuktól függetlenül amelyek, a szerepüket úgy töltik be, hogy közben az általunk ellenőrzött területet határain kívülre kerülnek vagy kerülhetnek.

Adaptálva az információbiztonság elveit, az átviteli út biztonság, vagy másképen az átvitel biztonság alapvető feladata:

Az információk rendelkezésre állásának, sértetlenségének, és bizalmasságának megőrzése az átviteli út folyamán, valamint az átviteli utat megvalósító eszközök rendelkezésre állásának, sértetlenségének biztosítása.

A fenti megfogalmazásból is látszik, hogy az átvitelbiztonság a híradó biztonságból fejlődött ki, ezért tekintsük át a vonatkozó szakirodalmat:

[44] A 9. ábra alapján.

„A HIRRENDSZER BIZTONSÁGA ÉS VÉDETTSÉGE olyan rendszabályok összessége, amelyek alkalmazásával egyrészt megakadályozható vagy jelentősen csökkenthető az ellenséges felderítés és rádióelektronikai zavarás hatékonysága, saját berendezéseink kölcsönös zavarása.

A hírrendszer biztonsága és védettsége feltételezi: a felderítés elleni védelem, az ellenséges rádiózavarás elleni védelem, és a kölcsönös rádiózavarás elleni védelem megszervezését és a rendszabályok komplex alkalmazását." [59.]

A meghatározásban a megjelenéskori technikai állapotot figyelembe véve, két hibát látok. Egyrészről csak kifejezetten a rádiós és kisugárzó eszközeinkre koncentrál az idézet, másrészről a veszélyeztető tényezőket sem tárja fel alaposan.

3.2.2 Az átvitelbiztonság feladatainak és folyamatainak meghatározása

Véleményem szerint egyrészről az átvitelbiztonság feladatainak és folyamatainak meghatározáshoz a kockázatkezelés végrehajtása a legjobb módszer. Másrészről a biztonsági ellenintézkedések minden esetben egyrészt valamiféle gátak az információ áramlás útjában, másrészt erőforrásokat emésztenek fel, éppen ezért a biztonsági ellenintézkedéseket gondosan, minden esetben az adott helyzetnek megfelelően, költség hatékonyan kell kivitelezni. Ahhoz, hogy ezt meg tudjuk tenni célszerű végrehajtanunk a VIRTAR kockázat elemzését és kockázat menedzsmentjét.

Az információs rendszerek kockázatkezelése az információbiztonság jelenleg egyik legjobban fejlődő részterülete, amely jelenleg nem mutat egységes képet a különböző szervezetek módszereiben. Az ISO és az IEC[45] 2008 júniusában kiadta a 27005-ös szabványát és ezzel egyrészt korszerűsítette a kockázatkezelés szemléletmódját, másrészt a 13335-ös szabványcsalád első négy tagját hatálytalanította. Ez a korszerűsítési folyamat azonban még nem fejeződött be az összes információbiztonsággal foglalkozó szervezetnél. Erre egy példa a szintén 2008 júniusában megjelent Közigazgatási Informatikai Bizottság 25. számú ajánlása (Magyar Informatikai Biztonsági Ajánlások című ajánláskötete), amely még a 13335-

[45] Az ISO (International Organization for Standardization – Nemzetközi Szabványügyi Szervezet) és az IEC.
(International Electrotechnical Comission – Nemzetközi Elektrotechnikai Bizottság) együtt világméretű, szabványosításra szakosodott intézményrendszert alkotnak.

ös szabványcsalád szerinti kockázatkezelést alkalmazza, valamint az ENISA,[46] ami diplomatikusan nem tesz különbséget a különböző kockázatkezelési módszerek között, viszont a honlapján lehetőséget nyújt ezek összehasonlítására.[47]

A NATO hivatalos biztonságpolitikája minderről ezt írja:

„- a biztonsági kockázat menedzsment a NATO polgári és katonai testületeinél kötelező, amelynek az alkalmazása a nemzeti rendszereknél javasolt"[48] [65.]

A különböző NATO információbiztonsági dokumentumok közötti kutatásaim során arra a következtetésre jutottam, hogy a NATO – bár kötelezővé teszi a kockázatelemzést és előírja, hogy mikor kell végrehajtani azt – a módszer kiválasztását a kockázatkezelést végrehajtó szervezetre bízza.

A Magyar Honvédség hivatalos információbiztonsági politikája pedig a következőket rögzíti:

„A kockázatelemzést

a) minősített adatokat kezelő rendszer, több szervezet által közösen használt vagy üzemeltetett rendszer, MH-szintű rendszer esetében kötelezően,

b) egyéb adatkezelő rendszerek esetében a NATO, EU, nemzeti elektronikus adatkezelésre feljogosított rendszerek felügyeletét ellátó hatóság, illetve az információvédelem szakmai felügyeletét ellátó honvédelmi szerv döntése szerint kell végrehajtani." [66.]

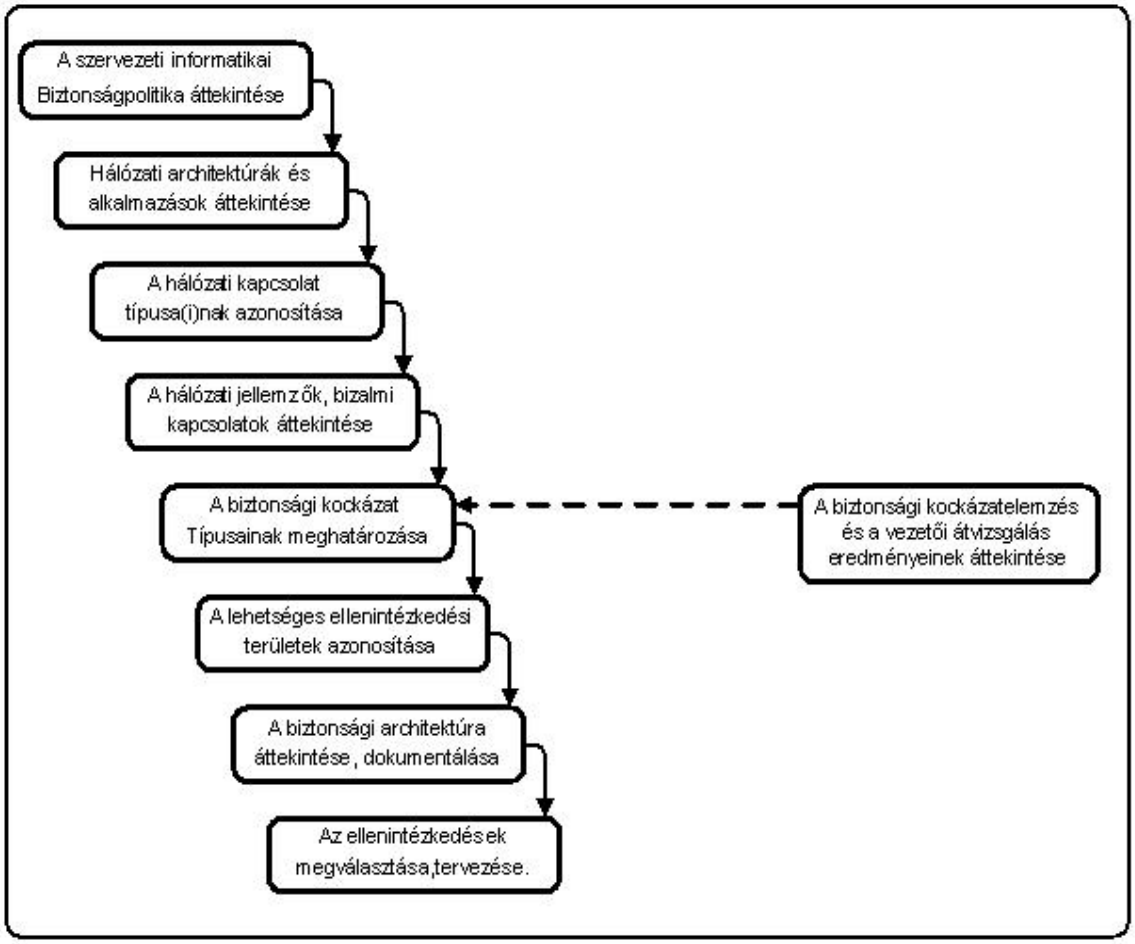
A fentiek alapján a kockázatkezelési folyamatot az átviteli utak tekintetében végre kell hajtani, mivel kezelt adatok minősítési szintjétől függetlenül az átviteli utakat több szervezet használja (elöljáró-alárendelt).

Mivel jelenleg két érvényben levő szabvány foglalkozik az információs hálózatok kockázat menedzsmentjével, amelyek metodikája más vizsgáljuk meg az általuk leírt munkafolyamatokat:

A ISO/IEC 13335-5 szabvány munkafolyamatait a **15. ábra** szemlélteti:

---

[46] ENISA -European Network and Information Security Agency Európai Hálózat- és Információbiztonsági Ügynökség Az Európai Parlament és a Tanács 460/2004/EK rendelete alapján létrehozott európai iformációbiztonsági szervezet.
[47] http://rm-inv.enisa.europa.eu/comparison.html (2009-12-29).
[48] security risk management shall be mandatory within NATO civil and military bodies. Its application within NATO nations shall be optional;



15. ábra Az ISO/IEC 13335-5 szabvány által bemutatott munkafolyamat
Forrás: [60.]

A kockázatkezelés azonban csak akkor lehet eredményes, ha ez nem egyszeri, hanem periodikus folyamat. Ezért a kockázatelemzés eredményeit időről időre felül kell vizsgálni és ha új kockázati tényező megjelenését tapasztaljuk újra kell tervezni az ellenintézkedéseket, illetve az egész kockázatkezelési folyamatot az új adatokkal meg kell ismételni. Szintén az eredményességet javíthatja, ha a kockázatokkal kapcsolatos információkat megosztjuk a kockázatkezelést végző szervezetekkel és ezeket a megosztott információkat felhasználjuk a kockázat menedzsmentben.

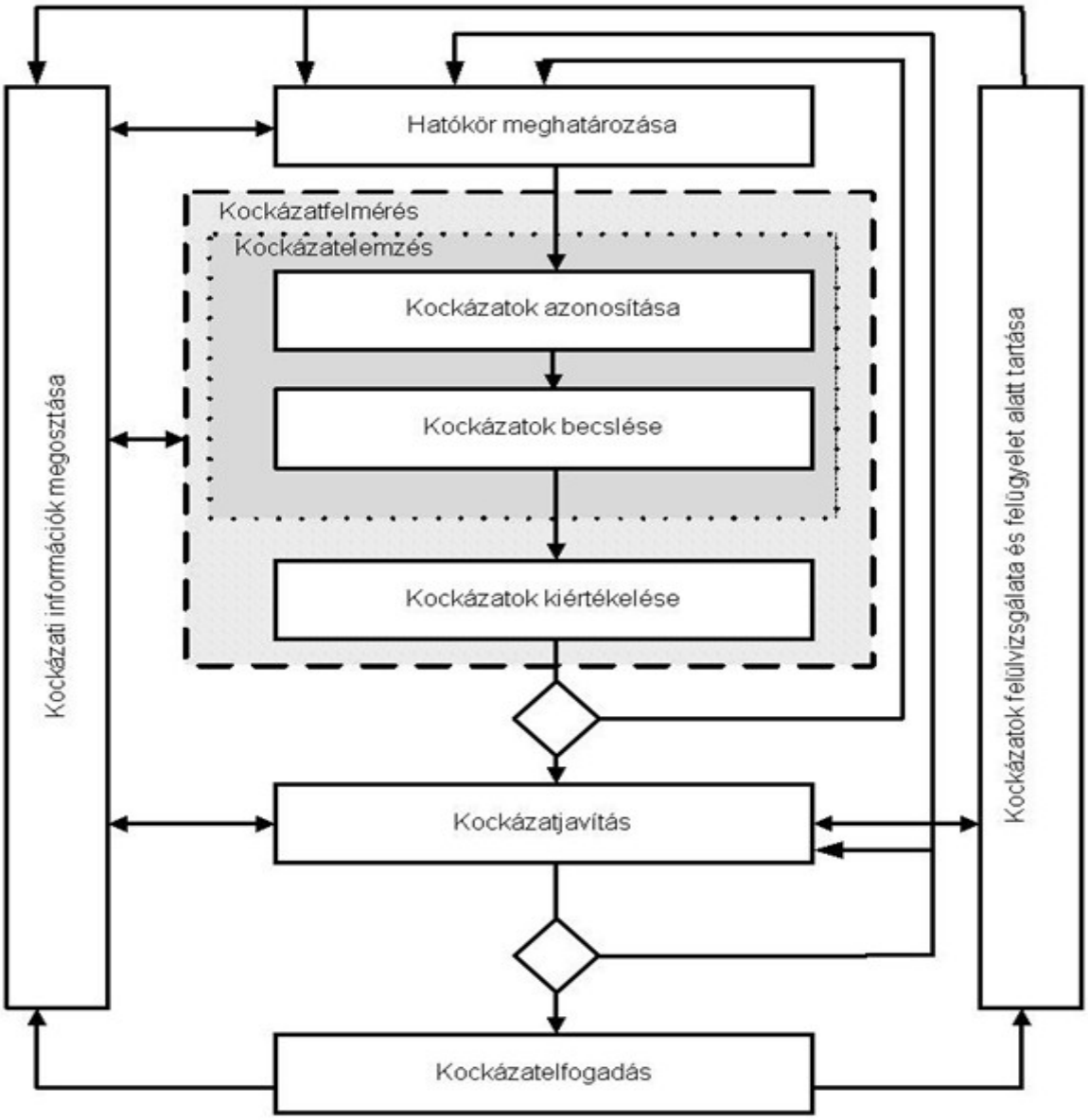
A szabvány által bemutatott folyamat azonban olyan, mintha a végrehajtott folyamat egyszeri cselekvés lenne, azonban a kockázatkezelés (vagy kockázatmenedzsment)[49] nem egy egyszeri cselekmény hanem egy folyamat, amelyet az információ feldolgozó rendszer és így az átviteli teljes életciklusa alatt

[49] Risk Management a MSZ ISO/IEC 27001 alapján a jelentése kockázatkezelés, kockázatmenedzselés, kockázatmenedzsment.

folyamatosan végre kell hajtani, amelyről például az információbiztonsági politika az alábbiakat írja:

„A kockázatelemzést az adatkezelő rendszer sajátosságainak, üzemeltetési környezetének figyelembevételével kétévente legalább egy alkalommal végre kell hajtani. Új kockázati tényező megjelenésekor a kockázatelemzést soron kívül el kell végezni.” [64.]

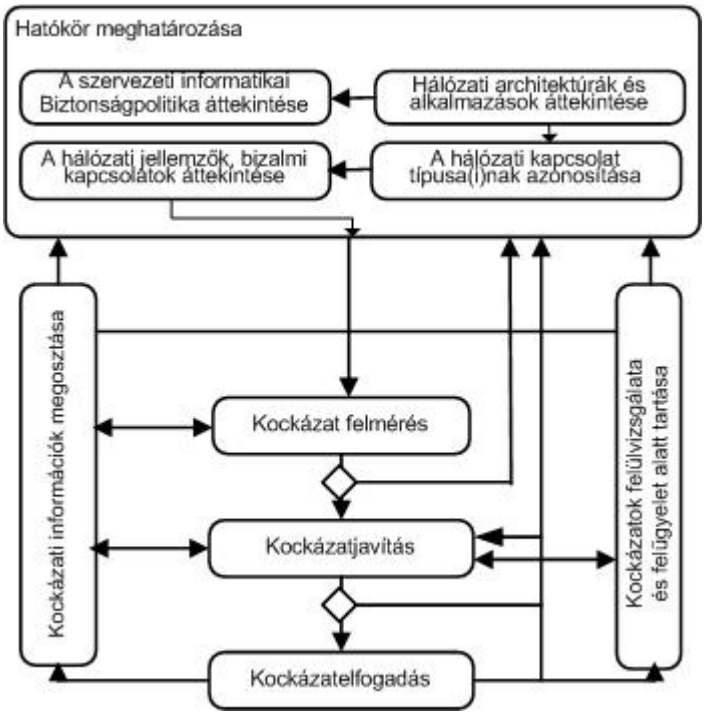
Ugyanezt a nézőpontot az MSZ ISO 27005 szabványból vett rajz (**16** ábra) is szemlélteti:



16. ábra A kockázatkezelés folyamata az ISO/IEC 27005 alapján

Forrás: [67.]

A véleményem szerint az átvitelbiztonsági kockázatok értékelésekor, vagyis az átvitelbiztonság meghatározásához a legfontosabb feladat a hatókör meghatározása. Az ISO/IEC 27005 szabvány véleményem szerint erre nem ad elegendő fogódzót ezért célszerűnek tartom a két szabvány munkafolyamatainak kombinációját alkalmazni. A 17. ábra egy olyan folyamatot mutat, amely a véleményem szerint egyrészről sokkal jobban megfelel az átviteli út biztonság kialakítási folyamatának, másrészről a két szabvány kombinációjával kaphatunk meg.



17. ábra Az átviteli utak biztonsági kockázatainak kiértékelési munkafolyamata

A kockázatfelmérés folyamatában a különböző folyamatok még további cselekvésekre bonthatók éppen ezért a továbbiakban csak vázlatosan fogom tárgyalni a különböző folyamatok tartalmát.

Annak érdekében, hogy a kockázatokat teljes mértékben azonosítani tudjuk a következő részfeladatokat kell végrehajtani:

- a vagyontárgyak azonosítása, amelyek közé a fizikai vagyontárgyakat, az információkat, a folyamatokat és a személyzetet sorolja a szabvány;
- fel kell mérni a valószínű fenyegetéseket, amelyek minden egyes esetben mások és mások lehetnek, de ha azonosak, akkor is hangsúlyuk különbözők;

- be kell azonosítani a már létező ellentevékenységeket és azonosítani kell a sebezhetőségeket, amelyeket a fenyegetések ki tudnak használni.

Amennyiben mindezeket a folyamatokat sikerült végrehajtanunk, akkor azonosítani tudjuk a kockázatok következményeit.

A kockázatok becslésénél figyelembe kell venni és ki kell értékelni az azonosított következmények hatásait a vizsgált rendszerre, illetőleg figyelembe kell venni az azonosított és kiértékelt következmények előfordulásának valószínűségét. A két eredményből megkapjuk a kockázatok szintjét.

A kiértékelésekor a kockázatok szintjének figyelembevételével egy olyan, lehetőleg sorba rendezett listát kapunk, amely megmutatja, hogy melyek azok a kockázatok amiket el tudunk fogadni és melyek azok amelyek ellen új ellenintézkedést kell bevezetnünk.

Az ellenintézkedések megválasztása után meg kell vizsgálni, hogy a fennmaradó maradványkockázatok elérik-e az elfogadható szintet avagy sem, természetesen amikor nem érik el ezt a szintet akkor új ellenintézkedéseket kell bevezetni.

3.3 A kockázatkezelés végrehajtása az átviteli út biztonság tekintetében

Az átviteli út kockázatelemzése csak abban különbözik az egyéb kockázatelemzésektől, hogy más hangsúlyt kapnak a sebezhetőségek és fenyegetések. Ezen megállapítás kifejezetten igaz akkor, amennyiben egy missziós vagy egy harci feladatot hajt végre az alakulat, ezért a továbbiakban erre az eshetőségre koncentrálva végzem a vizsgálatokat.

3.3.1 Az átvitelbiztonság hatókörének meghatározása

3.3.1.1 A szervezeti információbiztonság politika áttekintése

A jelenleg is érvényben levő MH információbiztonsági politika az átviteli út biztonságról a következőket írja: „Az elektronikus adatkezelő rendszerekben alkalmazott átviteli eljárásokat és biztonsági mechanizmusokat a kezelt adatok bizalmasságára, sértetlenségére és rendelkezésre állására vonatkozó követelmények szerint kell kialakítani.” [64.] Ebből az idézetből azonban nem derül ki,

hogy melyek ezek a követelmények, illetőleg az sem, hogy a jogalkotó az átviteli útbiztonságra, illetve az átviteli protokollokra gondol-e.

Ezek alapján fontos kérdésként merül fel, hogy mi lehet az információbiztonság feladata az átviteli út vonatkozásában. Első megközelítésben a C-M(2002)49-ből már citált idézet alapján a feladat az információk és a rendszer bizalmasságának, sértetlenségének, rendelkezésre állásának biztosítása. Véleményem szerint azonban bizonyos esetekben sokkal fontosabb, hogy a vezetés folytonosságát biztosítsuk:

„A vezetés folytonosságának fenntartása a vezetés egységének egyik alapvető feltétele, így a sikeres tevékenység alapja. Az erők alkalmazásának időszakában a vezetés megszűnése a kitűzött célok elérésének meghiúsulását okozhatja." [61.]

A NATO biztonságpolitikája erről a kérdésről a következőket fogalmazza meg:

„Kivételes műveleti körülmények idején a korlátozott, bizalmas, és titkos minősítésű információk továbbíthatók nyílt formában, mindegyik oknak tisztán fent kell állnia. A kivételes körülmények a következők:

- Küszöbön álló, vagy éppen aktuális krízis, konfliktus vagy háborús szituáció ideje alatt,
- amikor a kézbesítés sebessége nagy fontossággal bír, vagy megfelelő rejtjelző eszköz nem elérhető, és az elküldött információt nem lehet időben kihasználni, hogy ellenséges befolyást gyakoroljon a műveletre."[50] [57.]

Nem szabad azonban elfelejteni azt sem, hogy egy adott feladat esetében a legérzékenyebb információk a vezetési pont helye és a csapatok elhelyezkedése. Az elmúlt évek missziós feladatainak ellátás során a feladat jellegéből adódóan ez az információ teljesen nyíltnak számított, azonban egy tényleges harctevékenység során az ellenség legfontosabb célpontjai a saját csapataink vezetési rendszere lesz. Ebből kifolyólag a csapatok vezetését úgy kell kialakítani, hogy ne árulják el a vezetési pontok helyét, biztosítsák a rejtett vezetés lehetőségét.

[50] 21. Under exceptional operational circumstances, information classified NR, NC and NS may be transmitted in clear text provided each occasion is properly authorised. The exceptional circumstances are as follows :

(a) during impending or actual crisis, conflict, or war situations; and

(b) when speed of delivery is of paramount importance, or means of encryption are not available, and it is assessed that the transmitted information cannot be exploited in time to adversely influence operations.

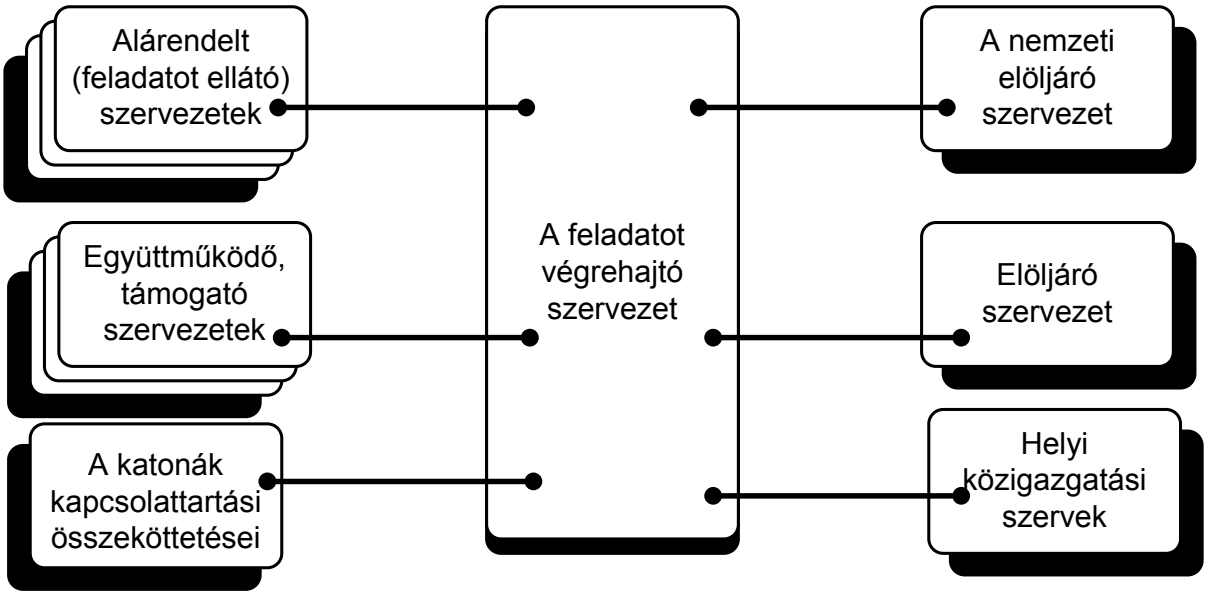
Összefoglalva az információbiztonsági politika átviteli út biztonságával foglakozó részben le kell szögezni, hogy az információvédelmi rendszabályoknak az átviteli út során biztosítaniuk kell a vezetés folytonosságát, amennyiben szükséges a rejtett vezetést, miközben megőrzik az információk és a rendszer sértetlenségét, bizalmasságát, és rendelkezésre állását.

3.3.1.2 A hálózati architektúrák és alkalmazások áttekintése

Véleményem szerint ahhoz, hogy a VIRTAR felépítését vizsgálni tudjuk célszerű áttekinteni a Magyar Honvédség alakulatai által végrehajtott missziók információs kapcsolatait. A missziót végrehajtó alakulatnak összeköttetésben kell lennie:

- az elöljáró szervezet törzsével, ahonnan gyakorlatilag a feladat végrehajtásához szükséges intézkedéseket, és egyéb információkat kapja;
- a hazai területen települt katonai vezető szervezettel, ami jelenleg a missziók esetében a Magyar Honvédség Műveleti Központ; [51]
- azokkal az alárendelt csapatokkal, szervezetekkel, amelyek a feladataikat nem a szervezet települési helyén hajtják végre. Ilyenek lehetnek például a különböző járőrök, illetve az iraki misszió idején a konvoj kisérések.

[51] A Honvédelmi Minisztérium honlapja alapján ahol is a műveleti központ feladataként (többek között) az alábbiak szerepelnek: „A szövetségi vagy más nemzetközi alárendeltségbe átadott, illetve a béketámogató, válságkezelő és válságreagáló műveletekbe bevont katonai képességek szakmai támogatása, az alárendeltségébe utalt szervezetek és személyek irányítása,..” [62.].



18. ábra: Missziós alakulat kapcsolati rendszere

Természetesen a szervezetnek kapcsolatot kell fenntartania a szomszédos alakulatokkal és ha vannak, akkor a támogató alakulatokkal is. Ezek lehetnek más nemzeti szervezetek, szövetséges csapatok és ebbe a kategóriába kell sorolnunk a nem katonai szervezeteket is, amelyek ugyanabban a misszióban tevékenykednek (pl.: az ENSZ által delegált rendőri erők).

A misszió sikere érdekében a missziós csapatoknak el kell fogadtatni a misszió célját a helyi lakossággal, ezért mindenképpen összeköttetésben kell állniuk a helyi közigazgatási, illetve más civil szervezetekkel és helyi vezetőkkel.

Modern korunkban egy misszió sikere elképzelhetetlen a hazai közvélemény támogatása nélkül, ahhoz, hogy ezt a támogatást elnyerjük mindenképpen gondoskodnunk kell a misszióban szolgálatot teljesítő katonák hazai kapcsolattartási lehetőségeiről. Ez a feladat mind szervezési mind biztonsági szempontból nagy kockázatokat rejt, ezért fokozott gondossággal kell tervezni.

3.3.1.3 A hálózati kapcsolat típusainak azonosítása

A 13335-ös szabvány több kapcsolati típust felsorol az azonosításról szóló fejezetben [63.], amelyek közül az átviteli út szempontjából és az előző fejezetet figyelembe véve az alábbi kapcsolati típusok lehetségesek[52]:

[52] D*őlt betűvel a szabványszerinti* kapcsolatok, állóbetűvel a példákat írtam.

- *Kapcsolódás egy szervezet földrajzilag elkülönülő részei között,* pl.: a parancsnoki (helyi és nemzeti) kapcsolatok.
- *A szervezet telephelyei közti kapcsolatok és a távmunkát végző személyek kapcsolódásai*, pl.: az alárendeltekkel történő kapcsolattartás.
- *Kapcsolódás más szervezetekkel,* pl.: a helyi közigazgatási szervek, támogatók, együttműködőkkel történő kommunikációs csatornák.
- *Kapcsolódás nyilvános környezetekkel* pl.: a katonák kapcsolattartása a családjukkal.

3.3.1.4 A hálózati jellemzők, bizalmi kapcsolatok áttekintése

A VIRTAR-t elsősorban a hálózatok megvalósulása alapján célszerű csoportosítani. Ezek alapján kétféle hálózattípust lehet megkülönböztetni:

- a saját erőink által létesített hálózatok;
- szolgáltatótól bérelt hálózatok.

A szolgáltatótól bérelt hálózatokhoz sorolom a szövetséges csapatok által számunkra rendelkezésre bocsátott hálózatokat is. Ezen hálózatoknak az átviteli út biztonság szempontjából problémája, hogy a biztonsági tulajdonságait nem tudjuk megváltoztatni, azokat csak megrendelni és értékelni tudjuk. Természetesen más biztonsági osztályba sorolhatjuk és másképpen értékelhetjük a hálózatokat amennyiben egy NATO szövetséges vagy NATO által biztosított hálózatról van szó, másképpen ha egy polgári szolgáltatótól bérelt hálózatról van szó. Az első esetben a NATO biztonságpolitikájában leírtak szerint csak annyit kell tudnunk, hogy az engedélyező és jóváhagyó hatóság megfelelőnek találata-e hálózatot, illetve a 3.3 fejezetben említett kivételről van-e szó.

A második esetben a biztonsági értékelés nehezebb, de lehetséges. Tudnunk kell a szolgáltatóról hogyan kezeli a biztonságot, megfelel-e a különböző szabványoknak, netalán egy nemzetközi szabvány szerint auditált hálózatról van-e szó.[53] Amennyiben lehetőségünk van választani a szolgáltatók közül azt a szolgáltatót kell választani amelyik nagyobb garanciát nyújt az információbiztonság

[53] Ilyen a nemzetközileg is elfogadott információbiztonsági auditálást lehet kérni például az ISO 27001 szabvány alapján.

területén. A szolgáltatók és a szolgáltatások összehasonlításához szintén segítséget nyújthatnak a nemzetközi szabványok, mint például az MSZ ISO/IEC 15408 szabványcsalád.[54]

A saját szakcsapataink által megvalósított átviteli utak felosztása a biztonsági kockázataik szerint követi a technikai megvalósítási struktúrát, amely alapján megkülönböztethetünk vezetékes és vezeték nélküli, illetve vegyes kivitelezésűeket. Ezeket csoportokat szintén tovább lehet bontani. A vezetékes összeköttetések lehetnek optikai kábeles és hagyományos, fémes kábeles megoldások. A vezeték nélküli megoldások lehetnek rádióhálók, amelyeket a hullámhosszuk alapján kategorizálhatunk, pont-pont összekötetést megvalósító mikrohullámú és egyéb rádiórelé csatornák, EDR rendszerek, rádiótelefon és műholdas összeköttetések. Bár az utóbbi kettő - miután a Magyar Honvédség csak végberendezésekkel rendelkezik – inkább a bérelt hálózatok kategóriájába tartozik.

A szabvány a bizalmi kapcsolatok között a különböző szintű csoportok közötti kapcsolatokat érti és így az alábbi hálózatokat különbözteti meg:

- hálózat ismeretlen felhasználói csoportokkal;
- hálózat ismert, kizárólag a szervezeten belüli felhasználói csoporttal;
- hálózat ismert, zárt üzleti csoporton (több szervezeten) belüli felhasználói csoportokkal.

Véleményem szerint a katonai rendszerek átviteli út biztonságának szempontjából itt a különböző fontosságú kapcsolatokat kell beazonosítani, ennek okán elsősorban a vezetésfolytonosság biztosításában játszott szerepük szerint kell priorizálni az átviteli utakat (18. ábra szerint).

3.3.2 Az átviteli út kockázatainak felmérése

Vagyontárgyak azonosítása

„Éles” helyzetben, a vagyontárgyak felmérésekor véleményem szerint a folyamatok azok, amelyekre a hangsúlyt fektetni kell. Ezek között is a legfontosabb a vezetés-irányítási folyamat. Mindaddig, amíg a béke elhelyezési körletben általában

[54] MSZ ISO/IEC 15408 Informatika. Biztonságtechnika. Az informatikai biztonságértékelés közös szempontjai.

nem okoz különösebb gondot, ha a vezetés kisebb időszakra megszakad, azonban ennek a kockázatnak a megvalósulása a feladat végrehajtása során akár a küldetés sikertelenségét is okozhatja. Az, hogy a vezetés-irányítás után milyen fontossági sorrendben követik egymást a folyamatok (anyagi-technikai, összeköttetések, felderítési adat továbbítás, fegyverirányítás, stb.) mindig az adott feladattól függ és kifejezetten a parancsnok hatásköre eldönteni a sorrendiséget.

A folyamatok felmérése után tartom szükségesnek felmérni az összeköttetéseket megvalósító VIRTAR eszközrendszerét és az üzemeltető személyzetet. Nem tartom célszerűnek külön választani az eszközöket a személyzettől csak abban az esetben, amennyiben egy automatikusan üzemelő eszközről, például egy átjátszó pontról van szó.

Utoljára tartom célszerűnek felmérni az információs vagyontárgyakat, mert az átviteli utakat „Black" vonalaknak kell tekintenünk, azaz olyan vonalaknak ahol minősített adatot nem közlünk, illetve csak rejtjelezett formában. Azt azonban nem szabad elfelejtenünk, hogy a „mozaikból áll össze a kép", vagyis a sok minősítetlen adatból nagyon érzékeny információkat, fontos következtetéseket lehet levonni.

Fenyegetések azonosítása

A fenyegetések azonosításakor figyelembe kell venni a misszió elfogadottságát az adott földrajzi területen, azaz a lakosság támogatja-e a missziót vagy éppen ellenzi, számolni kell-e ellenséges ellentevékenységekkel, vannak-e ellenséges csapatok, illetve gerilla csapatok. Amennyiben ellenséges tevékenységgel kell számolnunk, akkor a legfontosabb kérdés, hogy az ellenségnek milyenek a technikai lehetőségei. Abban az esetben, amikor az ellenség technikai feltételei megegyeznek, vagy jobbak a sajátjainknál, akkor mindenképpen számolnunk kell a technikai felderítéssel, és a rádiózavarással. Nem szabad azonban figyelmen kívül hagyni az ellenfelet akkor sem, amennyiben a technikai fejlettsége elmarad tőlünk, mert az átviteli utak támadhatók hagyományos eszközökkel is. Ilyen hagyományos támadások lehetnek a különböző szabotázsok, a közművek rongálásai. Viszont nem szabad azt sem elfelejteni amire Kassai Károly hívta fel a figyelmet 2002-ben:

„A támadó információs műveletek során nemcsak a tárolt, feldolgozott vagy továbbított adatokat lehet támadni, hanem az infrastruktúrát, a rendszert vezérlő adatokat, a védelmi mechanizmusokat is, így nyilvánvaló, hogy a híradó és

informatikai rendszernek rengeteg olyan paramétere van, amelyet legalább olyan szinten kell védeni, mint az általuk kezelt adatokat.” [10.]

Sebezhetőségek azonosítása

Az átviteli utak sebezhetősége az átviteli utat megvalósító technikai eszközök tekintetében más és más. Minden egyes átviteli útra jellemző sebezhetőségek:

- az átviteli út megszakadása,
- a lehallgatás,
- a forgalom analízis,
- a megszemélyesítés (amikor az ellenség saját csapatainknak, vezetési pontunknak adj a ki magát)
- a dezinformálás.

Az átviteli utak tekintetében sebezhetőségek közé kell sorolnunk a letagadhatóságot is, ami azt jelenti, hogy a feladatot küldő az üzenet küldését, a fogadó viszont a vételét tudja tagadni. Azt is célszerű figyelembe venni, hogy azok a sebezhetőségek, amelyek egy átlagos polgári felhasználás során jelentősek lehetnek (pl.: porosodás), azok a katonai kivitelű berendezéseknél többnyire nem számottevőek. Ahhoz, hogy azonosítani tudjuk mind a sebezhetőségeket, mind pedig a fenyegetéseket, segítséget nyújthatnak a szabványok, amelyeknek a mellékletében egy sokoldalú lista is található.

Létező ellentevékenységek felmérése

Az átviteli utak tervezésekor figyelembe kell venni minden olyan ellentevékenységet, amelyeket jogszabályok és egyéb előírások tartalmaznak. Ezek lehetnek:

- a frekvencia menedzsment végrehajtása, amely a rádiós eszközöket a kölcsönös zavarás ellen védi és csökkentheti az ellenséges lehallgatást,
- a különböző fedőnevek, szolgálati közlések táblázatainak összeállítása,
- ezeken felül minden olyan intézkedést be kell vezetni amelyekkel, minimalizálhatjuk az ellenség lehetőségeit,

- meg kell szervezni a rádiós összeköttetések napszakhoz és évszakhoz viszonyított a terjedési tulajdonságokat figyelembe vevő frekvenciaváltásokat.

Szintén az ellenintézkedések közé sorolható azon szolgáltatások igénybevétele, amelyek esetében a szolgáltatási feltételekben meghatározzuk a maximális kiesési időtartamot, valamit az egy kiesési periódus maximális hosszát.

Meg kell vizsgálni, hogy az átviteli utak biztosításában résztvevő, a települési helytől távol eső objektumok (rádiórelé és mikrohullámú átjátszó állomások, rádiófelvevő pontok, rádió adócsoportok stb.) őrzés-védelmét hogyan lehet megvalósítani.

Szintén figyelmet kell fordítani arra, hogyan lehet megszervezni a letagadhatatlanságot, amelynek fogalmi rendszerét a Magyar Szabvány MSZ ISO/IEC 13888 fogalmazza meg:

„A letagadhatatlansági szolgáltatás célja, hogy létrehozzon, összegyűjtsön, elérhetővé tegyen és igazoljon bizonyítékokat egy igényelt eseményt vagy műveletet illetően, annak érdekében, hogy dönteni lehessen az esemény vagy művelet bekövetkezésére vagy be nem következésére vonatkozó vita esetén.” [68.]

Ennek a szolgáltatásnak a hagyományos megvalósítását jelenti a rádiós rendszerekben a forgalmi eseménynapló, de a modern rendszerekben a különböző digitális aláírások és időbélyegzők alkalmazásával lehet megoldani a problémát, amelyek használatáról többet megtudni a már említett szabványban lehet.

A kockázat bekövetkezési következményeinek azonosítása

Az átviteli út biztonság sérüléséből adódó következmények vizsgálatakor az összes átviteli utat figyelembe kell venni, mert ezek együttes hatása más lehet mint külön-külön, erősíthetik, illetve gyengíthetik egymást, vagyis az átviteli út minden összetevőjének kockázati tényezőit meg kell vizsgálni és ezt követően összesíteni kell a hatásukat.

A legrosszabb forgatókönyv következik be, amikor az ellenség az átviteli utak felhasználásával dezinformálja a szervezetet, számukra téves parancsokat továbbít. Közel hasonlóan negatív eredményt okozhat az is, amennyiben egy kiemelt időszakban tartósan megszakad a csapatok vezetése. Mélyreható következményei

lehetnek annak az esetnek is, amikor az átviteli utak technikai jellemzőinek felderítésével kiderítik a saját csapatok és vezetési pontok elhelyezkedését. Szintén negatív eseménynek minősül a minősített, illetve érzékeny adatok sikeres megszerezése, amelyet az ellenség az átviteli út biztonság hiányosságait kihasználva válik képessé realizálni.

Természetesen a negatív következmények sorrendisége az adott feladatnak megfelelően változhat, illetve lehetnek olyan következmények, amelyekkel nem is kell számolnunk. Ilyen példa lehet, ha a csapatok és a feladatuk közismert, így ekkor nem kell számolni a csapatok helyének felfedésével kapcsolatos kedvezőtlen következményekkel.[55]

A kockázatok becslése

A kockázatok becslésekor, az azonosítása során eredményül megkapott kockázat bekövetkezésének negatív következményeit összevetjük annak bekövetkezési valószínűségével és ebből az összevetésből megkapjuk a kockázatok „értékét". A polgári életben a kockázatok becslésénél alapvetően két fajta skálát szokásos használni, az egyiknél „beárazzuk" a következményeket különböző mutatók alapján, a másiknál nem foglakozunk különböző eszközeink árával, hanem az egymáshoz viszonyított értéküket skálázzuk be. Megítélésem alapján az átviteli út biztonság kockázatelemzésekor kimondottan nehéz lenne a különböző folyamatok árát megbecsülni, ezért mindenképpen a skálázás módszerét kell alkalmaznunk. Ezt a skálázásos módszert az információbiztonsági politika is előírja az alábbiak szerint:

„A fenyegetéseket, sebezhetőséget és az előfordulási valószínűséget rendszerszintű, általános kockázatelemzés esetében 1–5 közötti értékskála alkalmazásával, részletes vizsgálat esetén a használt módszertan szerinti szélesebb értéksála alkalmazásával kell megjeleníteni." [69.]

Mivel az átviteli utak biztonságáról van szó, adódik a kézenfekvő megoldás, hogy az összeköttetéseket az átviteli sávszélességgel jellemezzük. A sávszélesség szerinti értékelés esetében is lehetőség van arra, hogy az ötös skálát használjuk. Ebben az esetben a kockázatfelmérés megkezdése előtt rögzíteni kell, hogy milyen sávszélességhez mekkora skálaérték tartozik. A skálás értékelésnek meg van azon előnye, hogy ekkor az átviteli út kockázatai egyszerűen összemérhetők az egyéb

[55] Az elmúlt évek missziós feladatai majdnem mind ilyenek voltak.

infokommunikációs kockázatokkal. A sávszélességek abszolút értékben történő összemérésekor viszont egy precízebb vizsgálatot tudunk végrehajtani. Másik problémát okozhat az analóg és a digitális átvitel összehasonlítása, de ez is könnyen feloldható, ha alapul azt vesszük, hogy az analóg jel átviteléhez milyen digitális sávszélességre lenne szükség (pl.: a 4 kHz-s analóg jel átviteléhez 64 kbps).

A kockázatok kiértékelése

Miután a kockázatok becslése során megkaptuk a kockázatok értékét a kiértékelés során az értékük alapján nagyságrendi sorrendbe kell őket rendeznünk, amelyet követően meg kell határoznunk, hogy a feltárt kockázatok meglévő szintje milyen viszonyban áll az elfogadható kockázatok szintjével. Nincs semmi tennivalónk azokkal a kockázatokkal, amelyeknek a becsült értéke ez alatt a szint alatt marad.

Gyakorlatilag ennek a munkafolyamatnak az a célja, hogy a kockázati listából kiszűrjük azokat, amelyeket nem fogadhatunk el. Ehhez azonban nagyon gondosan kell megválasztanunk az elfogadható szintet. Nem tartom elfogadhatónak, ha jelentős valószínűsége lesz a vezetés megszakadásának, az ellenséges dezinformációnak, a minősített illetve érzékeny információk kiszivárgásának.

3.3.3 Kockázatjavítás

A kockázatjavítás során dönthetjük el, hogy milyen ellenintézkedéseket tegyünk a kockázatok lehetséges következményeinek csökkentésére. Az ellenintézkedések lehetnek olyanok, amelyekkel teljesen elkerüljük a kockázatokat, illetőleg csökkentjük az események bekövetkezésének hatását vagy elkerüljük a kockázat előfordulását, valamint olyanok, amelyekkel a kockázatok negatív következményeit áthárítjuk egy másik félre. Azt, hogy melyik ellentevékenységeket fogjuk alkalmazni az adott körülmények fogják eldönteni.

A kockázatjavítás során ki kell dolgozni azokat az ellenintézkedéseket, amelyeknek az értéke a kockázatok kiértékelésekor az elfogadható szint fölé került. Ezek az ellenintézkedések lehetnek technikai megvalósításúak és szervezésiek, valamint a kettő kombinációi.

A technikai ellenintézkedések közé tartozhat korszerűbb, szórt spektrumú vezeték nélküli berendezések, illetve rádiók alkalmazása, az átjátszó állomások szigorúbb őrzése, a vezetékes összeköttetések rejtett kiépítése.

A szervezeti intézkedések közé tartozhat az átviteli utak felhasználásának korlátozása, a felhasználók kategorizálása, gyakoribb frekvenciaváltások, vezetési táblázatok alkalmazása, a kiépített vezetékes összeköttetések járőrrel történő ellenőrzése.

Annak eldöntése, hogy milyen ellenintézkedéseket vezetünk be, függ attól, hogy milyen erőforrásaink vannak és milyen szinten kívánjuk megvalósítani az átvitel biztonságot.

3.3.4 Kockázatelfogadás

A kockázatok elfogadásának alapvetően két fajtája létezik. Az egyik esetében a kockázatelemzés folyamataként feltárt, kiértékelt és az ellenintézkedések érvénybe léptetésével olyan szintre csökkentettük a kockázatokat amelyek már további intézkedést nem igényelnek, vagyis az elfogadható szint alá kerültek.

A második esetben a kockázatok létezésének tudatában vagyunk, de valamilyen okból nem tudatosan nem intézkedünk a kockázat megszüntetésére. Ilyen ok lehet az időhiány például amikor minősített adatot tudatosan továbbítunk nyílt csatornán, hogy a nagyobb veszteséget elkerüljük.

Mindkét esetben azonban a kulcs szó a tudatosság, vagyis nem felelőtlenül abban bízunk, hogy a nem várt esemény nem következik be, hanem tudatában vagyunk a cselekedetünk teljes súlyával.

3.4 Incidenskezelés és vezetésfolytonosság tervezés

A végrehajtott, megfelelő szintű kockázatjavítás után a kockázatok csak a legritkább esetben szűnnek meg teljesen. A biztonsági állapot sehol nem annyira változékony mint egy katonai feladat végrehajtása során, ezért a biztonsági környezetet folyamatosan figyelemmel kell kísérni. A biztonságban bekövetkezett negatív történések hatásuk nagyságtól függően lehetnek:

- biztonsági események,
- biztonsági incidensek.[56]

A katonai műveletek legnagyobb súlyú biztonsági incidense a vezetés megszakadása. A vezetés megszakadásának legvalószínűtlenebb forgatókönyve az

[56] Magyar Szabvány MSZ ISO/IEC TR 18044 alapján.

egyszerre, hirtelen bekövetkező események hatása. Sokkal elképzelhetőbb, hogy több, akár egymástól független incidens sorozat eredményeként jutunk el addig, hogy a vezető szervek nem tudják vezetni csapataikat. Ebből az okfejtésből is látszik, hogy nagy hangsúlyt kell fektetni a VIRTAR információbiztonsági incidenskezelésére. Az információbiztonsági politika mindezekről a következő állásfoglalást adja:

„A nem kívánt események megelőzését, észlelését, bizonyítékok gyűjtését és a helyreállítási feladatok végrehajtását, valamint a biztonsági incidensek jelentésének és kezelésének rendjét az elektronikus adatok, adatkezelő rendszerek szolgáltatásainak és erőforrásainak bizalmassága, sértetlensége és rendelkezésre állása érdekében kialakított mechanizmusokkal és eljárásokkal kell biztosítani.” [70.]

Sajnos többet ebből a szabályzóból nem tudhatunk meg, ezért célszerű az incidenskezelésre vonatkozó MSZ 18044 szabványt adaptálni. Először is célszerű a fogalmakat tisztázni, amelyek az alábbiak:

„**Információbiztonsági esemény:** Az információbiztonsági esemény egy rendszer, egy szolgáltatás vagy egy hálózat állapotának azonosított előfordulása, amely az információbiztonsági szabályzat megszegését vagy a biztonsági ellenintézkedés hibáját, vagy egy addig nem ismert helyzetet jelez, amely biztonság vonzatú.” [71.]

„**Információbiztonsági incidens:** Információbiztonsági incidensre utal egyetlen vagy egy sorozat nem kívánt vagy nem várt olyan információbiztonsági esemény, amely bekövetkezésének jelentős az üzleti[57] műveleteket veszélyeztető és az információbiztonságot fenyegető valószínűsége van.” [72.]

A két fogalom természetesen a teljes infokommunikációs hálózatra vonatkozik, vagyis a mi esetünkben a teljes VIRTAR-ra. Egyértelműnek kell tekinteni azonban azt is, hogy az átviteli út információbiztonsági incidenskezelésének részévé kell válnia a VIRTAR incidenskezelésének. A különbség csak annyi, hogy nem a vírusfertőzések fogják jelenteni az eseményt, hanem példának okáért a rádióforgalmazás megszakadása a légköri jelenségek miatt, vagy vétlen vezeték szakadások, illetőleg átjátszó meghibásodások.

Az átviteli út incidensei közé kell sorolni minden, az ellenséges tevékenységre utaló cselekményt, úgymint:

[57] Természetesen az adaptáció után üzleti=katonai.

- berendezések támadása, rongálása,
- rádióforgalom zavarása, lefogása.

Szintén ebbe a kategóriába sorolom azokat az eseményeket, amelyek az átviteli utak sávszélességének jelentős csökkenését okozzák az okok eredetétől (természeti hatások, ellenséges támadások, saját csapatok tevékenysége, stb.) függetlenül.

3.4.1 Az incidenskezelési terv

Az incidensek kezelése lehet ad-hoc jellegű, amikor a szakembereink meglévő szaktudására támaszkodunk, azonban célravezetőbb, ha elkészítünk egy incidenskezelési tervet. Természetesen minden eshetőséget nem tudunk feldolgozni, mivel előfordulhatnak váratlan, eddig még nem tapasztalt események és incidensek, azonban egy meglévő terv sokat segíthet egy „éles" helyzetben.

Adaptálva az MSZ ISO/IEC TR 18044 szabvány 7. fejezetét véleményem szerint az információbiztonsági incidenskezelési tervnek az átviteli út vonatkozásában az alábbiakat kell tartalmaznia:

- áttekintés az információbiztonsági esemény észleléséről, bejelentéséről, a lényeges információk összegyűjtéséről, valamint arról, hogy hogyan használják fel ezt az információt az információbiztonsági incidensek meghatározására. Az áttekintésnek tartalmaznia kell az információbiztonsági események lehetséges típusainak összefoglalását, azok bejelentési módját, azt hogy mit jelentsenek, hol és kinek és tartalmaznia kell azt is hogyan kezeljék az információbiztonsági események teljesen új típusait;
- az információbiztonsági incidensek bejelentésének folyamatát (ki a felelős, mi a teendő az esemény észlelésekor, bejelentésekor);
- egy információbiztonsági esemény információbiztonsági incidenssé történő átminősítését követően végrehajtott tevékenységek összefoglalása. Ennek tartalmaznia kell a következőket:
    - az azonnali megteendő intézkedések;
    - az incidens forrásának azonosítása;

    - mikor, milyen esetekben kell azonnal jelenteni az incidenseket a törzsfőnöknek vagy a parancsnoknak;
    - a másodlagosan megteendő intézkedések;
    - a felelősségek rögzítése;
- az incidenskezelési tevékenység naplózási követelményei a későbbi elemzések számára, illetőleg az elektronikus bizonyítékok biztos megőrzésének biztosítása folyamatos megfigyeléssel;
- az információbiztonsági incidenseket követő és megoldásukat szolgáló tevékenységek, beleértve a tanulságok levonását, valamint az eljárások megjavítását is;
- az átviteli út rendszerdokumentációjának (beleértve az eljárásokat is) tárolási helye;
- az információbiztonsági incidenskezelés oktatásának és képzésének feladatai.

3.4.2 A vezetésfolytonosság

A vezetés folytonosságának fenntartása a vezetés egységének egyik alapvető feltétele, így a sikeres tevékenység alapja. Az erők alkalmazásának időszakában a vezetés megszűnése a kitűzött célok elérésének meghiúsulását okozhatja. A parancsnok a műveletek teljes időszakára köteles megszervezni a helyettesítését, a vezetés átvételének rendjét. A vezetés folytonosságának fenntartása érdekében a feladatokat az alárendeltek részére úgy kell meghatározni, hogy az összeköttetés megszakadása esetén is garantálja a kitűzött célok teljesítését.

A legjobban megvalósított információbiztonsági ellenintézkedések, a legkiválóbban végzett információbiztonsági incidenskezelés ellenére is bekövetkezhet, hogy a vezető szervek valamilyen objektív oknál fogva nem tudják irányítani, vezetni az alárendeltjeiket. A vezetés megszakadása nem minden esetben csak a VIRTAR-ben bekövetkezett nem kívánt események következménye lehet, hanem más jellegű is, például a vezető szervek vezetésre képtelenné válása a vezetési pont megsemmisítése, vagy a vezetői állomány fogságba esése

következtében. Ennél fogva a vezetésfolytonosság nem elsősorban a VIRTAR-t üzemeltető állomány feladata, amely a következőképpen került megfogalmazásra:

„**A vezetés folytonossága**: A vezetés folytonosságának fenntartása a vezetés egységének egyik alapvető feltétele, így a sikeres tevékenység alapja. Az erők alkalmazásának időszakában a vezetés megszűnése a kitűzött célok elérésének meghiúsulását okozhatja. A parancsnok a műveletek teljes időszakára köteles megszervezni a helyettesítését, a vezetés átvételének rendjét. A vezetés folytonosságának fenntartása érdekében a feladatokat az alárendeltek részére úgy kell meghatározni, hogy az összeköttetés megszakadása esetén is garantálja a kitűzött célok teljesítését.” [73.]

Gyakorlatilag az Összhaderőnemi Doktrínával megegyező a már felemlített MSZ ISO/IEC TR 18044 szabvány megfogalmazásai is, csak a megfelelő fogalmakat össze kell egyeztetni, vagyis ami a katonai életben vezetésfolytonosság az a szabványban folyamatos üzletmenet, amelyet az alábbi szemléltet:

„A folyamatos üzletmenet tervezése az a folyamat, amely biztosítja bármilyen váratlan vagy nem kívánt és a lényeges üzleti tevékenységek és az azokat támogató elemek folyamatosságát negatívan befolyásolni képes incidensek előfordulásakor az üzemszerű állapotba való visszatérést. A folyamatnak azt is biztosítania kell, hogy az üzemszerű állapotba való visszatérés a megkövetelt prioritásoknak és időbeliségeknek megfelelően legyen elérhető, aminek következtében valamennyi üzleti tevékenység és támogató elem az üzemszerű állapotba áll vissza.” [74.]

Mindkét idézetből látszik, hogy sem a vezetésfolytonosság, sem a folyamatos üzletmentet tervezése – *bár nagy szerepe van benne* – nem elsősorban az infokommunikációs rendszereket üzemeltető állomány feladata. Visszatérve a katonai alkalmazásokhoz, a vezetésfolytonosság biztosítása a parancsnok felelőssége. Az Összhaderőnemi Doktrínából az is következik, hogy az infokommunikációs összeköttetések teljes megszakadása sem feltétlenül jelenti egy katonai feladat kudarcát, ennek ellenére a VIRTAR üzemeltető állománynak mindent meg kell tennie azért, hogy a kor színvonalán álló, megfelelő sávszélességű csatornákat biztosítson a vezetés számára:

„Az állandó és tábori kommunikációs rendszerek üzemeltetése során az információs szükségletek fontosságával arányos helyreállítási műveletek, tartalék

eszközök és alternatív megoldások támogatják a szükséges kommunikációs képességek folyamatos fenntartását.” [75.]

Bár nem teljesen értek egyet az idézettel, mivel azonban a kommunikációs rendszerek helyreállítási műveleteiről ugyan beszél, de nem említi meg azt, hogy milyen, a helyreállítási műveleteket megelőző folyamatokra van szükség. Ezen túl, a kommunikációs rendszereket valójában leszűkíti az átviteli utakat megvalósító eszközökre, azonban ennek ellenére kiindulási alapnak tekinthető. Nézzük meg, hogy milyen folyamatokkal kell tisztában lennie az átviteli utat biztosító személyzetnek, hogy a feladatukat megfelelő módon tudják végrehajtani:

- ismerni kell az általános helyzetet, miután ez nagymértékben kihat az összekötetések szervezésére;
- tisztában kell lenni, hogy ki, mikor, kit vezet, mert ez meghatározza az adott helyzet prioritásait;
- tisztában kell lenni, hogy az adott helyzetben milyen az infokommunikációs hálózat, milyen kerülő utakat tud elérni;
- tudni kell, hogyan lehet adott esetben a hírrendszerben átcsoportosításokat végrehajtani a kevésbé fontos csatornáktól a fontosabbak felé és természetesen tudni kell felállítani egy fontossági sorrendet az átvinni kívánt információk között;
- tisztában kell lenni, hogy melyek azok a minimális kommunikációs szolgáltatások, amelyek még biztosítják a vezetésfolytonosság infokommunkációs feltételeit.

3.5 Összegzés, következtetések

Jelen fejezetben megvizsgáltam a VIRTAR információbiztonságának alapvető kérdéseit.

Az információ és a szolgáltatások bizalmasságának, sértetlenségének, rendelkezésre állásának, letagadhatatlanságának, számonkérhetőségének, azonosíthatóságának és megbízhatóságának elvesztése igen káros hatással van a szervezet üzleti működésére. Következésképp az információk védelme és az informatikai rendszerek biztonságának menedzselése a honvédségi rendszerekben,

ahol adott esetben (konfliktusok, missziók) emberéletek és akár a küldetés sikere is múlhat az információbiztonságon, kritikus fontosságú.

Az információbiztonság a NATO elveknek megfelelően négy fő kategóriába osztható amelyek: fizikai biztonság, személyi biztonság, dokumentum biztonság és az elektronikus információbiztonság. A négy elem között fontossági sorrendet, alá-fölérendeltségi viszonyt nem lehet meghatározni. Az elektronikus információbiztonság feladatai a számítógép és helyi hálózat (LAN) biztonság, hálózatok biztonságos összekapcsolása, a rejtjelbiztonság, elektromágneses kisugárzás, és az átvitelbiztonság. további feladatcsoportba oszthatók.

Az összes szakterület feladatai a szakirodalomban jól feldolgozottak, az átvitelbiztonság kivételével , amely két okra vezethető vissza: a katonai hálózatokban az átviteli rendszerek nem csak homogén számítógépes hálózatokból állnak, mint a mai polgári architektúrák, hanem tartalmaznak a katonai innfokommunikációs hálózatokra jellemző eszközöket is (pl. különféle rádiók), és minden rendszerelem különböző fenyegetettségekkel is szembenéz, ezért nehéz az egységes védelmi profil kidolgozása. A másik ok, hogy polgári életben a legtöbb szereplő az átviteli utat megvásárolja egy szolgáltatótól (pl.: Internet kapcsolat, mobiltelefonos szolgáltatás), így e rendszerek biztonságával a szolgáltatónak kell foglalkozniuk. A gyakorlat azt mutatja, hogy behatárolt azon szolgáltatóknak a száma, amelyek e kérdéskörrel foglalkozni tudnak. A katonai rendszerekben alapállapotban (békehelyzetbe) is ilyen jellegű rendszerek dominálnak, azonban fel kell készülnünk olyan helyzetekre is amikor polgári cégek szolgáltatásait, vagy előre telepített zártcélú hálózatokat nem tudunk igénybe venni.

Az átviteli út biztonság, vagy másképen az átvitel biztonság alapvető feladata, hogy az információk rendelkezésre állásának, sértetlenségének, és bizalmasságának megőrzése az átviteli út folyamán, valamint az átviteli utat megvalósító eszközök rendelkezésre állásának, sértetlenségének biztosítsa. És az átviteli út mindazon hír, adat és információ továbbító csatornák (továbbiakban összeköttetések), jellegüktől és felépítésüktől, összetételüktől hosszúságuktól függetlenül amelyek, a szerepüket úgy töltik be, hogy közben az általunk ellenőrzött területet határain kívülre kerülnek vagy kerülhetnek.

Átvitelbiztonság feladatainak és folyamatainak meghatározáshoz a kockázatkezelés végrehajtása a legjobb módszer. A kockázatkezelés azonban csak

akkor lehet eredményes, ha ez nem egyszeri, hanem periodikus folyamat. Ezért a kockázatelemzés eredményeit időről időre felül kell vizsgálni és ha új kockázati tényező megjelenését tapasztaljuk újra kell tervezni az ellenintézkedéseket, illetve az egész kockázatkezelési folyamatot az új adatokkal meg kell ismételni. Szintén az eredményességet javíthatja, ha a kockázatokkal kapcsolatos információkat megosztjuk a kockázatkezelést végző szervezetekkel és ezeket a megosztott információkat felhasználjuk a kockázat menedzsmentben.

Az átviteli utak kockázatelemzésének bemutatásához az érvényben levő ISO/IEC 13335-s és a az ISO/IEC 27005 szabvány egy fajta kombinációját választottam. Ez alapján, hogy a kockázatokat teljes mértékben azonosítani tudjuk, a következő részfeladatokat kell végrehajtani: a vagyontárgyak azonosítása, fenyegetések felmérés, a már létező ellentevékenységeket azonosítása, amelyek végrehajtása után azonosítani tudjuk a kockázatok következményeit.

A kockázatjavítás során dönthetjük el, hogy milyen ellenintézkedéseket tegyünk a kockázatok lehetséges következményeinek csökkentésére. Az ellenintézkedések lehetnek olyanok, amelyekkel teljesen elkerüljük a kockázatokat, illetőleg csökkentjük az események bekövetkezésének hatását vagy elkerüljük a kockázat előfordulását, valamint olyanok, amelyekkel a kockázatok negatív következményeit áthárítjuk egy másik félre. Azt, hogy melyik ellentevékenységeket fogjuk alkalmazni, az adott körülmények fogják eldönteni.

A kockázatok elfogadásának alapvetően két fajtája létezik. Az egyik esetében a kockázatelemzés folyamataként feltárt, kiértékelt és az ellenintézkedések érvénybe léptetésével olyan szintre csökkentettük a kockázatokat amelyek már további intézkedést nem igényelnek, vagyis az elfogadható szint alá kerültek.

A második esetben a kockázatok létezésének tudatában vagyunk, de valamilyen okból nem intézkedünk a kockázat megszüntetésére. Ilyen ok lehet az időhiány például amikor minősített adatot tudatosan továbbítunk nyílt csatornán, hogy a nagyobb veszteséget elkerüljük.

Mindkét esetben azonban a kulcs szó a tudatosság, vagyis nem felelőtlenül abban bízunk, hogy a nem várt esemény nem következik be, hanem tudatában vagyunk a cselekedetünk teljes súlyával.

A végrehajtott, megfelelő szintű kockázatjavítás után a kockázatok csak a legritkább esetben szűnnek meg teljesen. A biztonsági állapot sehol sem annyira változékony, mint egy katonai feladat végrehajtása során, ezért a biztonsági környezetet folyamatosan figyelemmel kell kísérni. A biztonságban bekövetkezett negatív történések hatásuk nagyságtól függően lehetnek biztonsági események és biztonsági incidensek.

Az incidensek kezelésének hatékony eszköze lehet az információbiztonsági incidenskezelési terv, amelynek az átviteli út vonatkozásában az alábbiakat tartalmaznia kell: áttekintés az információbiztonsági esemény észleléséről, bejelentéséről, a lényeges információk összegyűjtéséről, valamint arról, hogy hogyan használják fel ezt az információt az információbiztonsági incidensek meghatározására. Az áttekintésnek tartalmaznia kell az információbiztonsági események lehetséges típusainak összefoglalását, azok bejelentési módját, azt hogy mit jelentsenek, hol és kinek, és tartalmaznia kell azt is, hogyan kezeljék az információbiztonsági események teljesen új típusait.

A katonai műveletek legnagyobb súlyú biztonsági incidense a vezetés megszakadása. A vezetés megszakadásának legvalószínűtlenebb forgatókönyve az egyszerre, hirtelen bekövetkező események hatása. A vezetés folytonosságának fenntartása a vezetés egységének egyik alapvető feltétele, így a sikeres tevékenység alapja. Az erők alkalmazásának időszakában a vezetés megszűnése a kitűzött célok elérésének meghiúsulását okozhatja. A parancsnok a műveletek teljes időszakára köteles megszervezni a helyettesítését, a vezetés átvételének rendjét. A vezetés folytonosságának fenntartása érdekében a feladatokat az alárendeltek részére úgy kell meghatározni, hogy az összeköttetés megszakadása esetén is garantálja a kitűzött célok teljesítését.

A fejezetben foglaltakat mérlegelve az alábbi következtetéseket vonom le:

1) A VIRTAR-hoz kapcsolódó biztonsági területek kidolgozottsági foka az átvitelbiztonság részterületén tekinthető a legalacsonyabbnak.

2) Az átviteli út biztonság feladatrendszerét a nemzetközi szabványok adaptálása révén célszerű meghatározni;

3) A VIRTAR biztonságának fokozása érdekében incidenskezelési és vezetésfolytonossági tervet szükséges kimunkálni.

Összefoglalás, végkövetkeztetések

A Magyar Honvédségben 1993-ban lépett hatályba az Informatikai szabályzat (ÁLT/210), melyben az informatika - *mint az infokommunikáció különálló részterülete* - feladatait a kor technikai színvonalán rögzítette. Az azóta eltelt időszakra azonban a konvergencia meghatározó vonásai lettek jellemzőek, és a katonai infokommunikáció szabályozása nem volt képes követni az elmúlt több mint tizenöt évben végbement társadalmi, katonapolitikai és főleg technikai változásokat. A tudományos igényű publikációk, cikkek, tanulmányok, doktori értekezések többsége is általában csak a technikai megvalósításra, a technikai fejlődésre fordítottak figyelmet, nem kaptak a kérdés fontosságának megfelelő hangsúlyt a vezetési és információs rendszerek technikai alrendszerének területei (híradás, informatika, információbiztonság) és azok tervezési-szervezési kérdései.

Az értekezésemben a kapcsolódó nemzeti és NATO-dokumentumokra alapozva megvizsgáltam, a vezetési és információs rendszer, valamint a híradó és informatikai rendszerek közötti összefüggéseket és viszonyrendszereket azok kölcsönhatásait. Kutatásiam során megállapítottam, hogy a vezetési és információs rendszer (VIR) a parancsnok elgondolásának megfelelően, a feladat eredményes végrehajtása érdekében létrehozott szervezet és kapcsolatrendszer, amelynek legfontosabb feladata, hogy megfelelő információkkal lássa el a parancsnokot döntési mechanizmusának segítése érdekében. A VIR megállapításaim szerint nem más, mint a parancsnokságok és törzsek különböző szakbeosztású tisztjeinek összessége. Azonban ahhoz, hogy a törzsben dolgozó egyének munkájukat a parancsnok által elvárt szinten tudják végrehajtani szükségük van információ-feldolgozó és tároló- (informatikai), valamint információt továbbító (híradó) rendszerekre, eszközökre és kapacitásokra. A teljes információs rendszer minőségi mutatói nem hagyhatják figyelmen kívül a megfelelő információbiztonsági szintek megvalósítását. Vizsgálataim alapján bebizonyítottam, hogy az említett eszközrendszer nem más, mint a VIR technikai alrendszere (VIRTAR).

Úgy ítéltem meg, hogy a híradás és informatika konvergenciája a polgári életben napjainkra befejezettnek tekinthető, ezért fontosnak tartottam a VIRTAR

felépítésének, elemeinek és viszonyrendszerének vizsgálatát a felkutatott dokumentumok révén. Megállapítottam, hogy jelenleg nincs egységes nézőpont a rendszer felépítésére, a tudományos publikációk szerzői gyakorlatilag a polgári életben végbement konvergencia eredményeit nem rendszerben elemezték, hanem az informatika, vagy az átvitelt biztosító hírrendszer oldaláról. Ezen túlmenően megállapítottam, hogy a NATO-ban sincs egységes elfogadott álláspont a rendszer egészéről, az üzemeltett rendszert több (különböző) nézőpontból vizsgálják. A meglévő, illetve a továbbfejlesztendő rendszert legjobban leíró modellt egy 2001-ben készített doktori értekezésében találtam meg, azonban ekkor még a konvergenciát nem lehetett befejezett tényként kezelni. Az eddig elért kutatási eredményekre alapozva dolgozatomban bemutattam a VIRTAR célszerű felépítését és elemeinek feladatrendszerét a Magyar Honvédség hálózat nyújtotta képességének elérése utáni időszakra.

Kimutattam, hogy a VIRTAR fő területeinek nincs egységes szabályozási rendszere, ezért a hiány pótlására irányuló feladatot alapvetően vezetési feladatként kell kezelni, amelynek egyúttal illeszkednie kell a meglévő katonai vezetési funkciórendszerhez. Ennek érdekében értekezésem második részében megvizsgáltam, hogy napjainkban milyen metodikák alapján, milyen eszközrendszerrel irányítják a vezetők, a parancsnokok a Magyar Honvédség tevékenységét. Megállapítottam, hogy amíg a parancsnoki munka viszonylag jól szabályozott addig a szakmai munka nyílt forrásokra támaszkodva nem követhető. Bizonyítottam, hogy a Magyar Honvédségben keveredik az öröklött szabályzati struktúra a NATO szerinti policy-directive-guideline szisztémával, illetőleg tovább bonyolítja a helyzetet a polgári szférából érkező szabályozási rendszer is, melyet a vezetési és információs rendszer, mint külső tényezői halmazt nem hagyhat figyelmen kívül. Ez a keveredés jellemző a VIRTAR irányítására is, mert bár egységes szabályozás nincs, jogilag (jogszabályokkal és az állam irányítás egyéb jogi eszközeivel) azonban néhány részterület, úgymint frekvenciagazdálkodás vagy az EDR hálózat szabályozásra került.

Annak érdekében, hogy javaslatot tehessek a VIRTAR irányítására szükségszerűnek mutatkozott előzetesen megvizsgálni a vezetés érdekében ellátandó feladatok körét. Megállapítottam, hogy vezetési feladatokat egyrészt tervezési-szervezési feladatokra, valamint a mindennapi élet irányítására lehet

felbontani. Mindkét részfeladatot további részekre osztottam fel, így meghatároztam az állandó és ideiglenes rendszerek tervezési és szervezési elemeit. A napi élet irányítását a hálózat-felügyeleti munka feladataira, illetve a számítógépes incidenskezelő központ feladataira bontottam fel, és értekezésem ezen részében összehasonlítottam a napi élet irányításának e két részterületét.

Korunk társadalmi elvárása, hogy a hadsereg ne állam legyen az államban, hanem a társadalom szerves, integrált része. E gondolatból kiindulva megvizsgáltam annak lehetőségét, hogy a VIRTAR vezetési rendszerében milyen eljárásrend szerint lehetséges alkalmazni a polgári életben már elfogadott minőségirányítási szabvány előírásait. Megállapítottam, hogy a VIRTAR irányításának megszervezése a minőségirányítási szabvány alapján kimutatható előnnyel jár abban az esetben, amennyiben egyrészről a szakmai vezetés elfogadja annak mechnizmusát, másrészről a beosztott állománnyal sikerül a kitűzött célokat megértetni és megvalósíttatni. Amennyiben a minőségirányítási rendszer nem fogja elősegíteni a hatékonyság növelését, várhatóan a kvantitatív és kvalitatív mutatók csökkenésére kell számítani.

Kimutattam, hogy az információs rendszerek bármelyikéről is legyen szó, a legfontosabb feladat az információbiztonság megfelelő, az adott rendszerre jellemző megteremtése. Ebből eredően a NATO minősített információbiztonságának alapdokumentumára alapozva, a polgári életben meglevő szabványosítási törekvéseket szem előtt tartva a kutatások végrehajtása során áttekintettem a VIRTAR biztonsági kérdéseit.

A biztonsági kérdések elemzését követően megállapítottam, hogy a technikai információbiztonsági kérdéskörből az átviteli út biztonság vagy másképpen az átvitel biztonság, amely leginkább katonai szakterülete a biztonságnak, sem a polgári életet, sem a katonai rendszereket tekintve nem került teljes egészében kidolgozásra. Feltártam a kidolgozatlanság okait, és kutatásaimat az átviteli út meghatározására és a biztonságának megvalósítására fókuszáltam a Magyarországon is elfogadott nemzetközi szabványokra alapozva. A vonatkozó szabvány alapján bemutattam, hogyan lehet meghatározni az átviteli utat és struktúráit. Bizonyítottam a biztonsági intézkedések szükségességét, melyet a szakértők igazoltnak látnak, azonban a költségek és a szabad információ áramlás gátjai miatt az elfogadás alacsony szintű. Ezek miatt a fenyegetésekkel és a védendő

információkkal arányos védelem megvalósításának leginkább járható útja és eszköze a kockázatok felmérése. Az idevágó szabvány módszereit alkalmazva bemutattam hogyan célszerű az átviteli út tekintetében végrehajtani a kockázatok felmérését.

Megfogalmaztam, hogy a biztonság egy olyan állapot, amely csak egy bizonyos időpillanatra értelmezhető, ezért ha kidolgozásra kerül egy rendszer biztonsági intézkedéscsomagja, akkor a figyelmet a biztonságot befolyásoló eseményekre és az azokra adandó válaszintézkedésekre kell fordítani. A válaszintézkedések életbeléptetésére már előre fel kell készülni, amely a Magyar Honvédség tekintetében két fő feladat köré csoportosítható, egyrészről az információbiztonsági incidenskezelés, másrészről a vezetésfolytonosság köré. Az értekezés utolsó részében bemutattam mindazon feladatokat, amelyeket az incidenskezelés és a vezetésfolytonosság megfelelő tervezése érdekében kell végrehajtani.

Végkövetkeztetések:

Az értekezésben foglaltakat mérlegelve az alábbi végkövetkeztetéseket vontam le:

1) A vezetési funkció nem választható el a vezetés technikai alrendszerétől, amelyből következik, hogy az információt szolgáltató alrendszer és a technikai alrendszer egymástól szintén elválaszthatatlan, szerves egységet alkot. A VIRTAR leírását és megalkotását a nemzeti modell módszertana alapján célszerű végrehajtani.

2) Az információs társadalomban a haderő előtt álló egyik legnagyobb kihívás az információk biztonságának megvalósítása. A részterületek kidolgozottsági foka megfelelő az átvitelbiztonság kérdéskörének kivételével.

3) A vizsgálat időszakát tekintve kijelenthető, hogy a VIRTAR három alapvető szakterületét illetően a vezetés egységessége nem valósult meg, a szakterületi viszonyrendszer korrekt rendezése nem teljesült. A VIRTAR

kialakítását újabb megoldások keresése helyett célszerű a megfelelő szabványcsaládra, valamint a bevált gyakorlatokra alapozva végrehajtani.

4) Az átvitelbiztonság feladatrendszerét a nemzetközi szabványok adaptálása révén célszerű meghatározni. A VIRTAR biztonságának fokozása érdekében incidenskezelési és vezetésfolytonossági tervet szükséges készíteni.

Az értekezés tudományos eredményeinek tartom:

1) Tudományos módszerekkel feldolgoztam, elemeztem és értékeltem - *mindazon dokumentumot, jogszabályt, amely alapján meghatározhatóvá vált* - **a vezetési és információs rendszerrel és annak technikai alrendszerével szemben a hálózat nyújtotta képességek megvalósulása érdekében támasztható követelményeket.**

2) Kritikai szempontból elemezve a VIRTAR Magyar Honvédség szintű szakmai vezetését, **a hazai és nemzetközi szinten kidolgozott eljárások adaptációja révén meghatároztam a VIRTAR minőségbiztosításra épülő vezetési elveit.**

3) A kockázatelemzés módszerének felhasználásával kidolgoztam az információbiztonság átvitel-biztonsági részterületének feladatrendszerét.

Javaslat az értekezés hasznosítására

Értekezésemben megfogalmazottakat a VIRTAR fejlesztési stratégiájának kialakításához nélkülözhetetlennek tartom. A hazai szabványcsaládra adaptált technikai alrendszer minőségirányítási feltételrendszerének kidolgozása napirenden lévő feladat, a híradó szolgálat előtt álló fejlesztési feladatok végrehajtásához elengedhetetlen, ezért ajánlom a szakmai vezetés figyelmébe.

Kutatási eredményeimre alapozva a Tudományos Diákkörök részére ajánlom kiinduló forrásdokumentumként értekezésem anyagát, hiszen a hálózat nyújtotta képességek elérése, annak kutatása az alap- és mesterképzésben megkezdődött,

Eredményeimet az ösztöndíjas hallgatók és a mesterképzés szakmai szakirányain és specializációi célszerű bevezetni, mert a jövő tisztjeinek a minőségirányítás és a minőségi szolgáltatások szintjén is ismerniük kell azok elvárásait, megvalósításának lehetőségeit, módszereit.

Budapest, 2010. március 11.

Kerti András mk. alezredes

Hivatkozások

[1.] Ternyák István ezredes: NATO tagságunk hatása és következményei a magyar katonai információs rendszerre Doktori (PhD) értekezés Budapest 2003 107. oldal

[2.] 1009/2009. (I. 30.) Korm. határozat A Magyar Köztársaság Nemzeti Katonai Stratégiájáról 41 pont.

[3.] Fekete Károly mk. alezredes: A Magyar Honvédség állandó telepítésű kommunikációs rendszere továbbfejlesztésének technikai lehetõségei. Doktori (PhD) értekezés Budapest, 2003. 10-16 o.

[4.] Kassai Károly mk. alezredes: A magyar honvédség információvédelmének mint a biztonság részének feladatrendszere Doktori (PhD) értekezés Budapest 2007 36 o. 25 oldal

[5.] Magyar Honvédség Összhaderőnemi Doktrina 3. kiadás 53. oldal

[6.] ÁLT 27 Magyar Honvédség Összhaderőnemi Doktrína 2. kiadás 2007 80. oldal

[7.] Gorza Jenő: A Magyar Honvédség informatikai rendszerének fejlesztése, az

[8.] Nato Glossary Of Terms And Definitions AAP-6(2008) in: 2-C-9 2-C-11

[9.] A honvédelmi minisztérium hivatalos honlapja http://www.hm.gov.hu/honvedseg/a_magyar_honvedseg_feladata (2008-12-19)

[10.] Kassai Károly: A korszerű híradó és informatikai rendszer védelmi szempontú vizsgálatának egyes kérdései. Nemzetvédelmi Közlemények http://www.zmne.hu/tanszekek/kvt/digitgy/20022/vszt/kassai.html (2008-12-20)

[11.] Rajnai Zoltán mk. őrnagy:A tábori alaphírhálózat vizsgálata egyes NATO tagországok kommunikációs rendszereinek tükrében, Doktori (PhD) értekezés Budapest, 2001, 11. oldal

[12.] Rajnai Zoltán mk. őrnagy:A tábori alaphírhálózat vizsgálata egyes NATO tagországok kommunikációs rendszereinek tükrében, Doktori (PhD) értekezés Budapest, 2001, 99. oldal

[13.] Fekete Károly: Az egyes harcos katona jövőbeni személyi kommunikációja. Elemző tanulmány Budapest 2002 6. oldal

[14.] ÁLT 27 Magyar Honvédség Összhaderőnemi Doktrína 2. kiadás 2007 98. oldal

[15.] adatmodellezés szerepe a fejlesztési folyamatban Doktori (PhD) értekezés Budapest 2003

[16.] A honvédelmi minisztérium szervezeti és működési szabályzata 16. oldal

[17.] Allied joint doctrine for communication and information system AJP-6 second study draft internet letöltés: http://194.7.80.152/website/book.asp?menuid=15&vs=3&page=ihb%2Findex.html 2008.12.23

[18.] Dr. Sándor Miklós: A gépesített hadtest híradása. In. Új Honvédségi szemle 50. évfolyam 9. szám 1996. szeptember HU ISSN 1216-7436 33-39.oldal

[19.] NATO C3 Agency: Nato Network Enabled Capability Feasibility Study Executive Summary : Version 2.0

[20.] Rajnai Zoltán mk. őrnagy:A tábori alaphírhálózat vizsgálata egyes NATO tagországok kommunikációs rendszereinek tükrében, Doktori (PhD) értekezés Budapest, 2001, 72.oldal

[21.] 51/2007. (VI. 6.) Országgyülési határozat a Magyar Honvédség további fejlesztésének irányairól. 4. pont.
[22.] ACT Transformation Network Portal https://transnet.act.nato.int/WISE/Informatio
[23.] A NNEC hivatalos honlapja http://nnec.act.nato.int/pages/documents.aspx NNEC_BasicOverview_HighLevel Megan Thum
[24.] Major General Ruud van Dam Royal Netherlands Air Force HQ SACT, ACOS C4I and Director IS & NNEC előadása Internet letöltés: 2009. december 23. http://www.afcea.org/europe/html/documents/060525-AFCEA2006DraftV1.2.ppt MajGenvanDam_000.ppt
[25.] Gorza Jenő: A Magyar Honvédség informatikai rendszerének fejlesztése, az adatmodellezés szerepe a fejlesztési folyamatban Doktori (PhD) értekezés Budapest 2003 32.oldal.
[26.] Pándi Erik rendőr alezredes : A magyar kormányzati távközlés egységesítésének hatása a rendvédelmi-, katonai-, és közigazgatási kommunikációs rendszerek megszervezésére és irányítására Doktori (PhD) értekezés Budapest 2005
[27.] Szöllősi Sándor okl. mk. őrnagy: Konvergáló hálózatok fejlődési trendjei, a technikai alkalmazhatóság kérdései a Magyar Honvédség infokommunikációs rendszerében Doktori (PhD) értekezés Budapest 2007 30. oldal
[28.] Hóka Miklós mk. alezredes: A Magyar Honvédség harcászati rádiórendszerének kialakítási lehetőségei egyes NATO-tagországok rádiórendszereinek vizsgálata tükrében, Doktori (PhD) értekezés Budapest 2005 55.oldal.
[29.] Andrew S. Tanenbaum: Számítógép hálózatok 97-101. oldal.
[30.] Rajnai Zoltán mk. őrnagy:A tábori alaphírhálózat vizsgálata egyes NATO tagországok kommunikációs rendszereinek tükrében, Doktori (PhD) értekezés Budapest, 2001, 75.oldal
[31.] Rajnai Zoltán mk. őrnagy:A tábori alaphírhálózat vizsgálata egyes NATO tagországok kommunikációs rendszereinek tükrében, Doktori (PhD) értekezés Budapest, 2001,83. oldal.
[32.] Konsberg hivatalos honlapja: http://www.kongsberg.com/en/KDS/News.aspx
[33.] Gorza Jenő: A Magyar Honvédség informatikai rendszerének fejlesztése, az adatmodellezés szerepe a fejlesztési folyamatban Doktori (PhD) értekezés Budapest 2003 58. oldal.
[34.] MHPK VKF 81/1997 intézkedése az Internet igénybevételével kapcsolatos titokvédelmi és adatbiztonsági rendszabályok betartásáról
[35.] Geir Hallingstad and Sander Oudkerk: Protected Core Networking: An Architectural Approach to Secure and Flexible Communications. In: IEEE Communications Magazine november 2008 ISSN 0163-6804 pg.: 35-41
[36.] 1949. évi XX. Törvény: A Magyar Köztársaság alkotmánya 40/B § (3) bekezdés
[37.] 2004. évi CV. Törvény: a honvédelemről és a Magyar Honvédségről 93-94§.
[38.] 2004. évi CV. Törvény: a honvédelemről és a Magyar Honvédségről 95§.
[39.] 2004. évi CV. Törvény: a honvédelemről és a Magyar Honvédségről
[40.] 2134/2006. (VII. 27.) Korm. határozat a Magyar Honvédség irányításának és felsőszintű vezetésének rendjéről
[41.] NATO Handbook ISBN 92-845-0178-4 HB-ENG-0406 © NATO 2006
[42.] A HM Támogató Dandár rendeltetése internet letöltés: http://www.hm.gov.hu/honvedseg/magyar_honvedseg_tamogato_dandar
[43.] Farkas Tibor hadnagy előadása kommunikáció 2008. nemzetközi tudományos konferencia 2008. 10.17.
[44.] CERT-Hungary Központ honlapja http://www.certhungary.hu/
[45.] ÁLT 27 Magyar Honvédség Összhaderőnemi Doktrína 2. kiadás 2007 68. oldal

[46.] A honvédelmi miniszter 74/2008. (HK 15.) HM utasítása a Magyar Honvédség műveleti tapasztalat-feldolgozó rendszer kialakításáról és működtetéséről. 3.§ (1)
[47.] MSZ EN ISO 9001:2000 Minőségirányítási rendszerek 4. oldal
[48.] MSZ EN ISO 9001:2000 Minőségirányítási rendszerek 20. oldal
[49.] MSZ EN ISO 9001:2000 Minőségirányítási rendszerek 22. oldal
[50.] Informatikai Tárcaközi Bizottság (ITB) 9-s ajánlás: Minőségirányítás. 1. oldal
[51.] Informatikai Tárcaközi Bizottság (ITB) 9-s ajánlás: Minőségirányítás. 4. oldal
[52.] Informatikai Tárcaközi Bizottság (ITB) 9-s ajánlás: Minőségirányítás. 2. oldal
[53.] Informatikai Tárcaközi Bizottság (ITB) 9-s ajánlás: Minőségirányítás. 7. oldal
[54.] MSZ ISO/IEC 13888-1 Informatika. Biztonságtechnika. Letagadhatatlanság 1. rész: Általános ismertetés
[55.] MSZ ISO/IEC TR 13335-5 Informatika. Az informatikai biztonság menedzselésének irányelvei 5. rész: A hálózatbiztonság menedzselési útmutatója.
[56.] C-M(2002)49 Security Within The North Atlantic Treaty Organisation (NATO) Enclosure 'B" Internet letöltés: Nemzeti Biztonsági Felügyelet honlapja http://www.nbf.hu/anyagok/jogszabaly/C-M(2002)49.pdf
[57.] C-M(2002)49 Security Within The North Atlantic Treaty Organisation (NATO) Enclosure 'F" Internet letöltés: Nemzeti Biztonsági Felügyelet honlapja http://www.nbf.hu/anyagok/jogszabaly/C-M(2002)49.pdf
[58.] Allied joint doctrine for communication and information system AJP-6 second study draft Internet letöltés: http://194.7.80.152/website/book.asp?menuid=15&vs=3&page=ihb%2Findex.html 2008.12.23
[59.] Szakutasítás a szárazföldi csapatok híradásszervezés elveire és követelményeire (Tervezet) A Honvédelmi minisztérium kiadványa 1984 Budapest, 8. oldal
[60.] MSZ ISO/IEC TR 13335-5 Informatika. Az informatikai biztonság menedzselésének irányelvei 5. rész: A hálózatbiztonság menedzselési útmutatója
[61.] Magyar Honvédség Összhaderőnemi doktrína 78.oldal
[62.] A Magyar Honvédség Műveleti Központ feladata A Honvédelmi Minisztérium honlapja http://www.hm.gov.hu/miniszterium/mh_muvelet_iranyito_kozpont
[63.] MSZ ISO/IEC TR 13335-5 Informatika. Az informatikai biztonság menedzselésének irányelvei 5. rész: A hálózatbiztonság menedzselési útmutatója 10. fejezet
[64.] A honvédelmi miniszter 94/2009. (XI. 27.) HM utasítása a honvédelmi tárca információbiztonság politikájáról 22 §
[65.] C-M(2002)49 Security Within The North Atlantic Treaty Organisation (NATO) enclosure "B" Internet letöltés: Nemzeti Biztonsági Felügyelet honlapja http://www.nbf.hu/anyagok/jogszabaly/C-M(2002)49.pdf
[66.] A honvédelmi miniszter 94/2009. (XI. 27.) HM utasítása a honvédelmi tárca információbiztonság politikájáról 16 § (4) bekezdés
[67.] International Standard ISO/IEC 27005 First edition 2008-06-15 Information technology — Security techniques — Information security risk management 5. oldal
[68.] Magyar Szabvány MSZ ISO/IEC 13888-1 2005 Informatika. Biztonságtechnika. Letagadhatatlanság 9. oldal
[69.] A honvédelmi miniszter 94/2009. (XI. 27.) HM utasítása a honvédelmi tárca információbiztonság politikájáról 16 § (1) bekezdés
[70.] A honvédelmi miniszter 94/2009. (XI. 27.) HM utasítása a honvédelmi tárca információbiztonság politikájáról 22 § (6) bekezdés
[71.] Magyar Szabvány MSZ ISO/IEC TR 18044 Informatika. Biztonságtechnika. Az információbiztonsági incidensek kezelése 3.2 fejezet

[72.] Magyar Szabvány MSZ ISO/IEC TR 18044 Informatika. Biztonságtechnika. Az információbiztonsági incidensek kezelése 3.3 fejezet
[73.] Magyar Honvédség Összhaderőnemi doktrína 78.oldal
[74.] Magyar Szabvány MSZ ISO/IEC TR 18044 Informatika. Biztonságtechnika. Az információbiztonsági incidensek kezelése 3.1 fejezet
[75.] Magyar Honvédség Összhaderőnemi doktrína 118. oldal
[76.] 1009/2009. (I. 30.) Korm. határozat A Magyar Köztársaság Nemzeti Katonai Stratégiájáról 49 pont.
[77.] 1009/2009. (I. 30.) Korm. határozat A Magyar Köztársaság Nemzeti Katonai Stratégiájáról 12-16. pont
[78.] Szakutasítás a szárazföldi csapatok híradásszervezés elveire és követelményeire (Tervezet) A Honvédelmi minisztérium kiadványa 1984 Budapest, 11. oldal
[79.] 51/2007. (VI. 6.) OGY határozat Magyar Honvédség további fejlesztésének irányairól
[80.] Magyar Szabvány MSZ ISO/IEC 27001 Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények C melléklet
[81.] Magyar Szabvány MSZ ISO/IEC TR 13335-3 Informatika. Biztonságtechnika. Az informatikai biztonság menedzselésének irányelvei 3. rész C melléklet
[82.] Magyar Szabvány MSZ ISO/IEC TR 13335-3 Informatika. Biztonságtechnika. Az informatikai biztonság menedzselésének irányelvei 3. rész D melléklet

Felhasznált irodalom

Doktori értekezések

1. Fekete Károly mk. alezredes: A Magyar Honvédség állandó telepítésű kommunikációs rendszere továbbfejlesztésének technikai lehetőségei. Doktori (PhD) értekezés Budapest, 2003.
2. Ternyák István ezredes: NATO tagságunk hatása és következményei a magyar katonai információs rendszerre Doktori (PhD) értekezés Budapest 2003
3. Rajnai Zoltán mk. őrnagy:A tábori alaphírhálózat vizsgálata egyes NATO tagországok kommunikációs rendszereinek tükrében, Doktori (PhD) értekezés Budapest, 2001,
4. Kassai Károly mk. alezredes: A magyar honvédség információvédelmének mint a biztonság részének feladatrendszere Doktori (PhD) értekezés Budapest 2007
5. Gorza Jenő: A Magyar Honvédség informatikai rendszerének fejlesztése, az adatmodellezés szerepe a fejlesztési folyamatban Doktori (PhD) értekezés Budapest 2003
6. Pándi Erik rendőr alezredes: A magyar kormányzati távközlés egységesítésének hatása a rendvédelmi-, katonai-, és közigazgatási kommunikációs rendszerek megszervezésére és irányítására Doktori (PhD) értekezés Budapest 2005
7. Szöllősi Sándor okl. mk. őrnagy: Konvergáló hálózatok fejlődési trendjei, a technikai alkalmazhatóság kérdései a Magyar Honvédség infokommunikációs rendszerében Doktori (PhD) értekezés Budapest 2007
8. Hóka Miklós mk. alezredes: A Magyar Honvédség harcászati rádiórendszerének kialakítási lehetőségei egyes NATO-tagországok rádiórendszereinek vizsgálata tükrében, Doktori (PhD) értekezés Budapest 2005

9. Husi Géza Minőségmenedzsment-rendszerek módszereinek alkalmazása a Magyar Köztársaság rendőrségénél Doktori (PhD) értekezés 2006. Budapest

Jogszabályok, és az államirányítás egyéb jogi eszközei:

10. 51/2007. (VI. 6.) Országgyülési határozat a Magyar Honvédség további fejlesztésének irányairól
11. 50/1998. (III. 27.) Kormányrendelet a zártcélú távközlő hálózatokról
12. 74/2008. (HK 15.) HM utasítás A Magyar Honvédség műveleti tapasztalat-feldolgozó rendszere kialakításáról és működtetéséről
13. 1949. évi XX. Törvény: A Magyar Köztársaság alkotmánya
14. 2004. évi CV. Törvény: a honvédelemről és a Magyar Honvédségről
15. 2134/2006. (VII. 27.) Korm. határozat a Magyar Honvédség irányításának és felsőszintű vezetésének rendjéről
16. 93/2006. (HK 18.) HM utasítás a szolgálati könyvek és a főnökségi kiadványok kiadásának rendjéről
17. 141/2006. (HK 2/2007.) HM utasítás a Magyar Honvédség Informatikai Stratégiájának kiadásáról
18. 1009/2009. (I. 30.) Korm. Határozat a Magyar Köztársaság Nemzeti Katonai Stratégiájáról
19. 1/2000. (HK 2.) HM utasítás az egységesítési, szabványosítási tevékenységről és a NATO egységesítési dokumentumok kezeléséről és feldolgozásáról
20. A honvédelmi miniszter 40/2009. (V. 27.) HM utasítása a Nemzeti Katonai Stratégiában foglaltak végrehajtásával kapcsolatos feladatokról
21. A honvédelmi miniszter 74/2008. (HK 15.) HM utasítása a Magyar Honvédség műveleti tapasztalat-feldolgozó rendszer kialakításáról és működtetéséről
22. 86/2008. (HK 17.) HM utasítás a folyamatba épített előzetes és utólagos vezetői ellenőrzési rendszer kialakításával kapcsolatos feladatokról
23. A honvédelmi miniszter 94/2009. (XI. 27.) HM utasítása a honvédelmi tárca információbiztonság politikájáról.
24. 51/2007. (VI. 6.) OGY határozat Magyar Honvédség további fejlesztésének irányairól
25. 2007. évi LXXIV. törvény a műsorterjesztés és a digitális átállás szabályairól
26. 103/2007. (HK 18.) HM utasítás a külföldi szolgálatot teljesítők ellenőrzési rendjéről
27. 95/2007. (HK 17.) HM utasítás a folyamatba épített előzetes és utólagos vezetői ellenőrzési rendszer kialakításával kapcsolatos feladatokról szóló 114/2005. (HK 1/2006.) HM utasítás módosításáról
28. 81/2007. (HK 15.) HM utasítás a HM fejezet államháztartási belső ellenőrzési rendjének szabályairól, és a HM fejezet egységes államháztartási belső ellenőrzési kézikönyvének kiadásáról
29. 52/2007. (HK 11.) HM utasítás a honvédelmi tárca ellenőrzési rendjéről
30. MHPK VKF 81/1997 intézkedése az Internet igénybevételével kapcsolatos titokvédelmi és adatbiztonsági rendszabályok betartásáról

Szabályzatok, szabályzók

31. Nato Glossary Of Terms And Definitions AAP-6(2008) Internet letöltés: http://www.nato.int/docu/stanag/aap006/aap-6-2008.pdf 2008-12-16
32. ÁLT 27 Magyar Honvédség Összhaderőnemi Doktrína 2. kiadás 2007
33. Allied joint doctrine for communication and information system AJP-6 second study draft Internet letöltés: http://194.7.80.152/website/book.asp?menuid=15&vs=3&page=ihb%2Findex.html 2008.12.23.
34. Magyar Honvédség Egységes Iratkezelési Szabályzata (Ált/40)
35. Honvédelmi Minisztérium és a Magyar Honvédség Titokvédelmi és Ügyviteli Szabályzata (Ált/3)
36. ÁLT 210 MH Informatikai Szabályzata
37. Nato Quality Assurance Requirements For Design, Development And Production AQAP 2110, Internet letöltés: http://www.nato.int/docu/stanag/aqap2110/aqap2110e.pdf 2009-10-17
38. Szakutasítás a szárazföldi csapatok híradásszervezés elveire és követelményeire (Tervezet) a Honvédelmi minisztérium kiadványa 1984 Budapest

Szabványok

39. MSZ EN ISO 9001:2000 Minőségirányítási rendszerek
40. MSZ ISO/IEC 13888-1 Informatika. Biztonságtechnika. Letagadhatatlanság 1. rész: Általános ismertetés
41. MSZ ISO/IEC TR 13335-5 Informatika. Az informatikai biztonság menedzselésének irányelvei 5. rész: A hálózatbiztonság menedzselési útmutatója.
42. Magyar Szabvány MSZ ISO/IEC 15408 Informatika. Biztonságtechnika. Az informatikai biztonságértékelés közös szempontjai
43. Magyar Szabvány MSZ ISO/IEC 13888 Informatika. Biztonságtechnika. Letagadhatatlanság
44. Magyar Szabvány MSZ ISO/IEC TR 18044 Informatika. Biztonságtechnika. Az információbiztonsági incidensek kezelése
45. Magyar Szabvány MSZ ISO/IEC 27001 Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények
46. Magyar Szabvány MSZ ISO/IEC 17799 Informatika. Biztonságtechnika. Az információbiztonság irányítási gyakorlatának kézikönyve
47. International Standard ISO/IEC 27005 First edition 2008-06-15 Information technology — Security techniques — Information security risk management

Könyvek, cikkek, honlapok, ajánlások

48. Kassai Károly: A korszerű híradó és informatikai rendszer védelmi szempontú vizsgálatának egyes kérdései Nemzetvédelmi Közlemények http://www.zmne.hu/tanszekek/kvt/digitgy/20022/vszt/kassai.html (2008-12-20)
49. Fekete Károly: Az egyes harcos katona jövőbeni személyi kommunikációja. Elemző tanulmány Budapest 2002
50. NATO C3 Agency: Nato Network Enabled Capability Feasibility Study Executive Summary : Version 2.0 Internet letöltés: 2006.11.13 http://www.mdn.gov.pt/defesa/estretura/organigrama/DGAED/DGAED_pdf

51. Allied Data Publication 34 (ADatP-34) NATO C3 Technical Architecture Implementation Handbook http://194.7.80.153/website/book.asp?menuid=15&vs=3&page=ihb%2Findex.html
52. A honvédelmi minisztérium szervezeti és működési szabályzata Internet letöltés: http://www.hm.gov.hu/files/9/8778/hm_szmsz_2007_aug01_ok.pdf 2009-01-02
53. Andrew S. Tanenbaum Számítógép hálózatok (Computer Networks) második kiadás Budapest 2004. ISBN 963 545 384 1
54. NATO Handbook ISBN 92-845-0178-4 HB-ENG-0406 © NATO 2006 http://www.nato.int/docu/handbook/2006/hb-en-2006.pdf
55. A Magyar Honvédség hivatalos honlapja: http://www.hm.gov.hu/
56. CERT-Hungary Központ honlapja http://www.certhungary.hu/
57. Informatikai Tárcaközi Bizottság (ITB) 9-s ajánlás: Minőségirányítás. Internet letöltés: http://www.itb.hu/ajanlasok/a9/ 2009. október 11.
58. Közigazgatási Informatikai Bizottság 25. számú Ajánlása: Magyar Informatikai Biztonsági Ajánlások Internet letöltés 2009-12-29 http://www.ekk.gov.hu/hu/kib/KIB-25-2-0_MIBETS_v1_vegl.pdf
59. ENISA honlapja: http://www.enisa.europa.eu/
60. Hadtudományi lexikon Budapest 1995 ISBN 963045226X

Ábrák jegyzéke

Publikációs jegyzék

1. Információk védelme, tanulmány 2006 Szárazföldi Parancsnokság Tudományos Könyvtár Székesfehérvár Zámolyi út 1-2.
2. Rajnai Zoltán-Kerti András Alternatív vezetékpótló lehetőségek Tanulmány 2006 MH Vezérkar
3. Dr. Rajnai Zoltán- Kerti András: Katonai alakulatok információvédő szervei vész-, (veszélyhelyzeti) tervei Kard és Toll 2006/2 p: 181-189
4. Osztályba soroló vizsgáztatás Kard és Toll 2007/2 p: 108-113
5. A vezetés és a hírrendszer kapcsolata Kommunikáció 2006 ISBN 978-963-7060-18-2
6. Dr. Rajnai Zoltán, Kerti András: Az információvédelmi szakállomány továbbképzési rendszere Kommunikáció 2007 ISBN 978-963-7060-31-1 o. 84-89
7. Dr. Rajnai Zoltán, Kerti András: Internetterrorisme Kommunikáció 2007 ISBN 978-963-7060-31-1 o. 116-119
8. Átviteli út biztonság, Hadmérnök II évfolyam 4. szám 2007/4 december http://www.hadmernok.hu/archivum/2007/4/2007_4_kerti.pdf
9. Dr. Rajnai Zoltán mk. alezredes- Kerti András mk. őrnagy: Az ISDN és az IP technológia alkalmazhatósága a Magyar Honvédség kommunikációs rendszereiben (tanulmány)
10. Dr. Rajnai Zoltán mk. alezredes- Kerti András mk. őrnagy: Az ISDN és az IP technológia megvalósíthatósága zártcélú (védelmi) kommunikációs rendszerekben. (tanulmány)
11. Katonai infokommunikációs rendszerszervezés Hadmérnök III. Évfolyam 2. szám - 2008. június
12. Dr. Rajnai Zoltán - Kerti András: Információbiztonság és rejtjelfelügyelet http://www.biztonsagpolitika.hu/userfiles/file/PDF/kerti-rajnai_rejtjelfelugy.pdf
13. Dr. Pándi Erik- Kerti András: Az információ technológiai ágazat sajátosságai Kommunikáció 2008 ISBN 978-963-7060-57-1 o. 66-78
14. A polgári élet és a katonai információbiztonság viszonya Kommunikáció 2008 ISBN 978-963-7060-57-1 o. 102-107
15. Pándi Balázs- Rajnai Zoltán- Kerti András: Structure of The command and information system Hadmérnök IV. évfolyam 3. szám 2009/3 http://www.hadmernok.hu/2009_3_kerti.pdf
16. dr. Rajnai Zoltán- dr. Fekete Károly- dr. Pándi Erik- Kerti András: Infokommunikációs megoldások alkalmazhatósága egy korszerű, mobil biológiai labor esetében (összehasonlító tanulmány), ZMNE, Egyetemi könyvtár, Budapest, 2009. Kv : 572
17. dr. Rajnai Zoltán- dr. Fekete Károly- dr. Pándi Erik- Kerti András: Az MBC System Housing terv keretében kialakítandó rendszer híradó és informatikai alrendszer (tanulmány), ZMNE, egyetemi könyvtár, Budapest, 2009. : Kv : 571