

A KATONAI LOGISZTIKAI BIZTOSÍTÁS GYAKORLATA

JAVASLAT A BESZERZÉSI ELJÁRÁSOK TÖRVÉNYI HÁTTEREINEK MÓDOSÍTÁSÁRA A MAGYAR HONVÉDSÉG HÍRADÓ BERUHÁZÁSAI SORÁN

Léránt József¹

*A HM Fejlesztési és Logisztikai
Ügynökség Tudományos Tanácsa
által kiírt pályázatára beküldött ta-
nulmány szerkesztett változat.*

Szerkesztőség

1. Bevezetés



¹ Léránt József mk. őrnagy, HM Fejlesztési és Logisztikai Ügynökség Technológiai Igazgatóság, Rendszertanúsító és Kodifikációs osztály, főtitzt.

A Honvédelmi tárca különös figyelemmel kíséri a Magyar Honvédség híradó és informatikai fejlesztéseit. Ezen figyelem indokolt is, hiszen az informatikai, kommunikáció terén az elmúlt időben hatalmas fejlődés volt tapasztalható. Meg kell felelni az újabbnál újabb kihívásoknak, miközben egy örökölt híradó és informatikai rendszert kell átalakítani úgy, hogy megfeleljen a szervezet igényeinek.

Ezen átalakítási – modernizációs folyamatok a termelői logisztika keretein belül a HM FLÜ hatáskörében történnek. Itt zajlik a műszaki követelmények meghatározása, pontosítása, a beszerzési eljárás bonyolítása.

Azért is választottam ezt a témát, mert azokat a tapasztalatokat szerettem volna feldolgozni, amelyek ezen a területen keletkeztek, hangsúlyozva azokat a törvényi szabályzókat, amelyek megítélése nem egyszerű.

Először nézzük, meg hogy mi is az a terület, amelyeket ezek a beruházások érintenek.

Az Magyar Honvédség hálózatában az állandó telepítésű kommunikációs rendszert a különböző katonai létesítményekben telepített hírközpontok és az azokat összekötő kommunikációs vonalak képzik. A hírközpontok közvetlen kommunikációs kapcsolatban állnak a közcélú távközlő hálózatokkal. A kommunikációs vonalak a közcélú és katonai távközlő hálózatok stacioner jellegű bázisán létesülnek. Az ISDN szolgáltatásokat biztosító digitális központok első sorozata 1999-ben, hazánk NATO tagságával került üzembe helyezésre. A rendszer vezetékes átviteli útjai is elsősorban a közcélú szolgáltatóktól bérelt összeköttetésekkel kerülnek biztosításra, amely mellett mellérendelt, de azzal egyenértékű országos mikrohullámú hálózat működik.

A honvédelmi ágazatra jellemező, hogy szervezetében kissebességű átviteli utat igénylő, egymástól függetlenül működő, lokális és nagytávolságú hálózati erőforrásokat igénybe vevő számítógépes hálózatok üzemelnek.

Az MH hálózatának környezetét vizsgálva megállapítható, hogy – hazánk szövetségi elkötelezettségének megfelelően – külső kapcsolata a NATO ICIS amely a NATO C3 vezetését támogató rendszer.

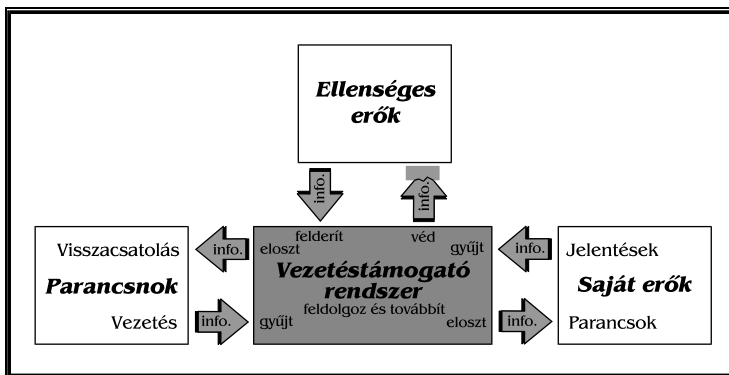
A NATO kommunikációs rendszere alapvetően négy részre osztható:

- Saját tulajdonban levő integrált katonai kommunikációs rendszerre.
- A tagállamok saját tulajdonában levő katonai kommunikációs rendszerre.
- A NATO saját rendszerének és a tagállamok saját rendszerének összeköttetését.
- Támogató közcélú (nemzeti és nemzetközi) kommunikációs rendszerek.
- A különböző tulajdonban levő kommunikációs rendszereket összekötő digitális átviteli infrastruktúra.

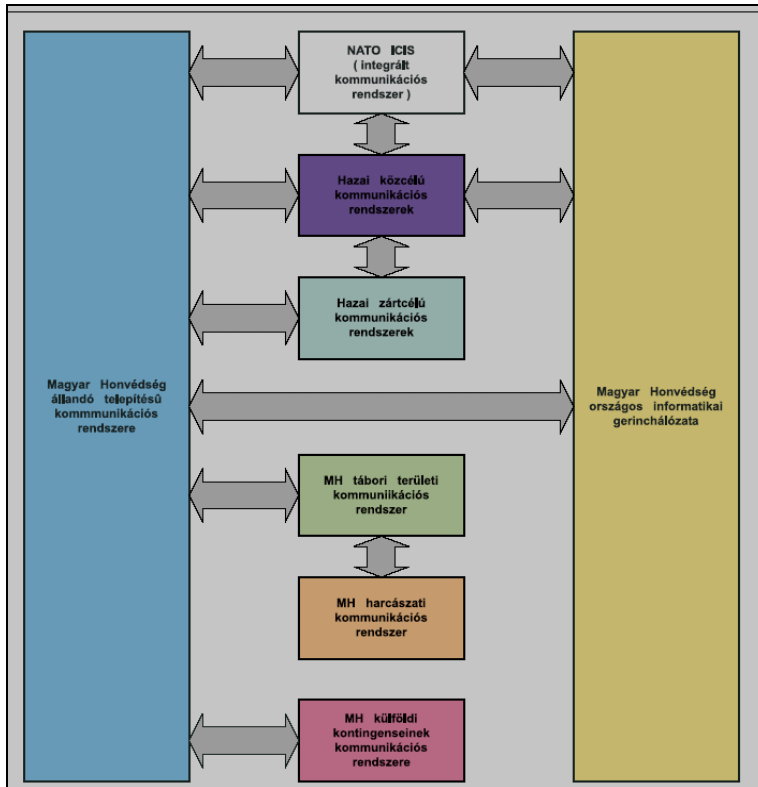
A fentiekben említett kapcsolódásokkor jól látható, hogy bármilyen biztonságot érintő probléma akár országhatárokon is túlnyúlhat.

A vezetéstámogató rendszer (C2SS - Command and Control Support System) az a legtagabb értelemben vett rendszer, amely a parancsnokot támogatja a vezetés és irányítás megvalósításában. A vezetéstámogató rendszert a feladatnak megfelelően biztosított és megszervezett vezetéstámogató (különböző típusú felderítő, híradó, informatikai, tűztámogatás koordináló, légtér-irányító, elektronikai harc, álcázó és megtévesztő, stb.) erők építik ki és működtetik. *A rendszer helyét és szerepét a következő ábrák szemlélteti.*

1. ábra.



A vezetéstámogató rendszer helye és szerepe



***Az MH hálózat kapcsolata más kommunikációs rendszerekkel
(Forrás: Dr. Fekete Károly – Zrínyi Mikós Nemzetvédelmi Egyetem)***

Néhány szóban arról a védelemről, amelyek ezeket a hálózatokat érintik.

A hálózati védelem

A hálózati beléptetés többszintű jelszavas védelemmel van biztosítva, így felhasználói csoportok alakíthatók ki. Minden belépés és az, hogy a felhasználó milyen parancsokat adott ki, a logbuch-ban tárolódik. Ebből szükség esetén kikereshető, hogy honnan, milyen módon, ki hajtott végre bizonyos beavatkozásokat, esetlegesen jogtalan programozásokat.

A rendszerhez az alábbi módokon lehet hozzáférni:

- OHF-en keresztül.
- THF-en keresztül.
- RHF-eken keresztül.
- Teleszervizzel a szervereken keresztül.
- Comtes-sel a központoknál lévő modemeken keresztül.
- Közvetlenül a központra csatlakozva.

Fizikai védelem

A gépekhez, adathordozókhoz stb. csak jogosult személy fér hozzá. Ez csak szervezési probléma.

A felhasználók személyazonosságának és hitelességének megállapítása:

A felhatalmazott személyek szigorú azonosítás után léphetnek a rendszerbe. Az azonosítás lehet gyenge (ekkor valamely begépelte kóddal azonosítja magát), erős (amikor valamely eszköz is kell az azonosításhoz, pl. kártya), vagy háromfaktoros (amikor a felhasználó valamely biológiai tulajdonságával is bejelentkezik, például retina). ***A Magyar Honvédség a kétszintű gyenge azonosítást használja.***

Napjainkban az ***Internetet egyre inkább az üzleti felhasználás jellemzi***, de veszélyforrást jelent az sokszor dicséret nyíltága. Ennek következtében ***új szoftverkategória*** alakult ki, ezek a ***tűzfalak*** (védőgátak).

A tűzfalak feladatai:

- Megvédi egy szervezet belső hálózatát a külső hálózatról érkező nem kívánatos, illetve jogosulatlan hozzáférésekkel szemben.
- Lehetővé teszi a hálózat számára külső hálózat szolgáltatásainak elérését.

A tűzfalak a támadások kivédése mellett használhatók még Internet-szerver funkciók megvalósítására is. Megfelelő biztonságpolitikával tehát alkalmasak két vagy több hálózat (általában Internet és belső hálózat) közötti kapcsolat ellenőrzésére és szűrésére. Arra azért figyelni kell, hogy a tűzfal nem a védelem eszköze (hiszen ez csak a behatolás valószínűségét

csökkenti, a támadás elé akadályt állítva), hanem a védelmi politika egyik fontos kiegészítője.

Ezekon a használt védelmeken túl, szükség van egy olyan funkcionális védelemre, amikor valamilyen szintű leállás, katasztrófa stb. során a feladatokat át kell vennie valamely szervnek.

Ezen célból hozták létre a Tartalék Országos Hálózatfelügyeletet (TOHF).

A Tartalék Országos Hálózatfelügyeletet a Magyar Honvédség digitális kapcsolóelemeit felölelő rendszer biztonsága érdekében hozták létre. A Magyar Honvédségnél "M" állapotban és háborús körülmények között szükséges egy olyan védett objektumban elhelyezett hálózatfelügyelet, mely tarifáláson kívül minden programozási, hibafelügyelési és hibaelhárítási lehetőséggel rendelkezik, mint az **OHF**. Minden konfigurálás, melyet az **OHF** végrehajt 1-2 perces késéssel a **TOHF** szerverén is megjelenik. A hibák szintén mind a két szerverhez befutnak. A **TOHF** tulajdonképpen minden paraméterében és befutott információiban tükörképe az **OHF**-nek.

Békeidőszakban az **OHF** viszi teljesen a felügyeleti stb. funkciókat, a **TOHF**-t csak minimális fenntartó állomány képviseli. Az **OHF** szerverének meghibásodásakor a **TOHF** szervere képes átvenni feladatait minden gond és kiesés nélkül.

A végrehajtott konfigurálások az adott központon végrehajtnak merevlemezis háttértárolóján tárolódnak, a központ konfigurációs állapota a beépített **MOD**-ra letölthető, elmenthető. Központ teljes leállásnál, ha valamilyen katasztrófális konfigurációs hibát vétenek, akkor a **MOD**-on tárolt utolsó mentési adatokkal helyreállítható a központ konfiguráció.

Ugyancsak hardveres biztosítást ad, hogy a **HICOM 350E** központokban lehetőség van egy központi vezérlőt és kapcsolómátrixot is tartalmazó „*meleg tartalék*” kapcsoló egység beépítésére, amit a **Magyar Honvédség** igénybe is vett.

Ebből a rövid leírásból látható, hogy biztonság szempontjából lehet az akár szoftveres vagy funkcionális jellegű - mindent elkövetnek az üzemeltetők, hogy biztosítsák a **MH híradó és informatikai** igényét.

2. Beszerzések és ezek törvényi hátterei

A Magyar Honvédség számára a termelői logisztikán belül a beszerzéseket a HM Fejlesztési és Logisztikai Ügynökség Beszerzési Igazgatósága végzi több Igazgatóság szakembereinek szoros együttműködésével.

A beszerzéseket, a törvényi háttér figyelembe vételével bonyolítják le.

Ezen törvényi hátterek a következők:

- 2003, évi CXXIX törvény
- 228/2004/VII.30 kormányrendelet
- 120/2007 (HK 20) HM utasítás

Így tehát a különféle beszerzések során a beszerzésre kijelölt bizottság feladata az is hogy a törvényesség figyelembevételével meghatározza az eljárás módját.

A Római egyezmény 296 Cikkelye alapján (Common Military List):

A Tagállamok megtehetik az alapvető biztonsági érdekeik védelme érdekében az általuk szükségesnek tartott fegyverek, lőszeres és hadianyagok előállításával vagy kereskedelmével kapcsolatos intézkedéseket.

Így ezen egyezmény égisze alatt a 228-as kormányrendelet többszöri módosításon esett át, **melyek a következők voltak:**

- 87/2005 (V.5) számú módosítás.
- 384/2007 (XII.23) kormányrendelet.

A 228-as kormányrendelet alapján a beszerzéseket 2 eljárás mód alkalmazásával lehetséges lebonyolítani:

- Tárgyalásos (közzététellel, vagy közzététel nélkül).
- Különleges.

Hirdetmény közzétételével:

A hirdetmény közzétételével történő eljárást a vagy a nyílt eljárás eredménytelensége indokolhatja vagy a beszerzés tárgya pl. kutatásfejlesztés, vagy egyéb feltételek meghatározása pl. ellenszolgáltatás.

Menete:

- Részvételi szakasz (20 nap).
- Ajánlattételi szakasz.

Hirdetmény közzététele nélküli tárgyalásos eljárás:

Főbb esetei:

- Kizárólagosság.
- Rendkívüli sürgősség.
- Bonyolultság.
- Interoperabilitás.
- Előzetes kutatásfejlesztés.
- Országgyűlés vagy a kormány által elrendelt speciális alkalmazás.
- Rendszeresítés.

Menete: csak ajánlattételi szakasz.

Ezen eljárások során „**NATO beszállítói**” cím előírható ekkor nem kell vizsgálni az alkalmasságot, hiszen az alkalmasságot már előzőleg megállapították.

Különleges eljárás:

Fegyveres szervezet alkalmazási keppességét befolyásoló, külföldi kormányok, minisztériumok, egyéb külföldi szervezetek hivatalos felajánlása alapján.

Menete: tárgyalásos szerződéskötés.
(kormány vagy illetékes miniszter döntése az ajánlat elfogadására).

A beszerzéseket bonyolító bizottságnak ezen szabályzók mentén kell kialakítani álláspontjukat az eljárás meghatározása végett.

Az természetes, hogy gyakran az igények és a lehetséges törvényi szabályzók nem állnak összhangban, gyakran jogos felvetések nem kapnak teret, mert a törvény megköti a kezeket.

Számos alkalommal előfordul, hogy a Magyar Honvédség híradó és informatikai hálózatán végzendő munkálatok kapcsán a beszerzési eljárás meghatározása nem egyértelmű mivel a túlságosan sok szabályzó gyakran átfedésekben van egymáson.

A bizottság tagjai gyakran nem tudják értelmezni, hogy mit lehet és mit nem s menet közben előfordul, hogy eljárásmódot kell váltani.

Ezen eljárások egyértelmű meghatározása nem csupán az időtakarékosság gondolatát, de ezen túlmenően a biztonság kérdéskörét is felvetik.

Az időbeliség is egy igen fontos tényező, hiszen mint minden átalakítás gyakran nem egyszerre, hanem a források függvényében történik, így gyakran vízesésszerű modell alapján egymásra épülnek a projektek. (nem indulhat az egyik, míg a másik be nem fejeződik).

A napjainkban történt eset kapcsán is el kell gondolkodnunk, hogy ideje lenne valamit tenni, az eljárásmód egyértelmű meghatározására a híradó és informatikai beruházások terén.

„Olyan speciális az NBH rendszere, hogy csak házon belül lehetett kémprogrammal betörni az informatikai hálózatba, ráadásul annak, aki ezt tette, nagyon ismernie kellett a hivatal operációs rendszerét” - hangzott el az MTV Híradójában.

„Az az életszerű, hogy valaki bement és ott bent betette ezt a kémprogramot és aztán kijött” - nyilatkozta a műsornak Kürti Sándor, az adatmentéssel foglalkozó Kürt Zrt. elnöke.

Forrás: (Index.hu elektronikus média).

3. Esettanulmány

A Magyar Honvédség állandó híradó és informatikai hálózatának fejlesztését érintő, a 2008-as évi Éves Beszerzési Tervben (ÉBT) I/D/55 folyószámon szereplő „Az MH objektumaiban helyi híradó és informatikai hálózatok fejlesztése„ tárgyú beszerzési eljárás jelenleg is folyik az MH FLŰ-n belül.

A KSZF portálon található miniszteri tájékoztatóban az országosan kiemelt termékekre vonatkozó állami normatíva rendszerről a *következő kiemelt termékek szerepelnek a kommunikációtechnológia kapcsán:*

Termék besoroló azonosító	Kiemelt termékek / Termékkategóriák
0100000000	Kommunikációs eszközök és szolgáltatások (1. sz. függelék)
0101000000	Beszédcélú kapcsolók, készülékek és kapcsolódó szolgáltatások
0102000000	Aktív és passzív hálózati elemek
0103000000	Internetszolgáltatás
0104000000	Mobil kommunikációs eszközök és szolgáltatások
0105000000	Zártcélú mobil kommunikációs eszközök és szolgáltatások
0190000000	Kommunikációs eszközökhöz kapcsolódó szolgáltatások
0200000000	Információtechnológiai rendszerek és szolgáltatások (2. sz. függelék)
0201000000	Szoftverrendszerek és elemeik
0202000000	Hardverrendszerek és elemeik
0204000000	Digitális vizuáltechnikai eszközök
0290000000	Szoftverekhez kapcsolódó szolgáltatások
0291000000	Hardverrendszerekhez, kiegészítőikhez kapcsolódó szolgáltatások
0292000000	Digitális vizuáltechnikai eszközökhöz kapcsolódó szolgáltatások

Így ezen fent említett beszerzést a törvényi háttér szerint meg is kezdék a KSZF keret-megállapodás alapján az alábbi termékkörben:

0102000000	Aktív és passzív hálózati elemek
------------	----------------------------------

Hogy a KSZF keret megállapodása mit is ért ez alatt azt a következő műszaki tartalommal jelzi:

Aktív és passzív hálózati elemek

I. Kiemelt termékkör definíciója:

„Az aktív hálózati eszközök olyan, a megfelelő volumenű beszerzési igényt kielégítő hálózati (networking: adat, hang, és képátvitel, valamint kapcsolódó szolgáltatások) feladatokat ellátó hardver-, firmware- (a hardverrel szorosan integrált, azt működtető szoftverréteg) és szoftvereszközök, melyek biztosítják a felhasználói végpontok közötti kommunikációt.”

Származó termékosztályok:

A termékkör az alábbi termékcsoportokra terjed ki:

A lokális hálózaton belül használatos Helyi számítógép-hálózati (LAN) eszközökre (BA: 0102010000), **amelyek lehetnek:**

- Menedzselhető vagy nem menedzselhető desktop switchek (egyes portokra érkezett OSI (Open System Interconnect) modell 2. adatkapcsolati rétegének (Data Link Layer) kereteit továbbítja, vagyis átkapcsolja a megfelelő portra vagy portokra).
- Már különböző funkciókat tartalmazó, menedzselhető és további modullal vagy modulokkal bővíthető moduláris switchek (már akár az OSI modell 3. hálózati rétegének (Network Layer) csomagjaival is foglalkoznak).
- Content Delivery Networking eszközök (OSI modell felsőbb rétegeinek a 4. szállítási rétegtől (Transport Layer) akár a 7. alkalmazási rétegig (Application Layer) információit is fel tudják dolgozni).

- Telephelyi elérést biztosító útválasztók (access routerek), melyek lehetővé teszik a lokális hálózat eszközeinek összekapcsolását a telephely eszközeivel, illetve hálózatával.
- Nagy csomagáteresztő képességgel rendelkező Gerinchálózati útválasztók (backbone routerek), melyek a gyors forgalombiztosítással lecsökkentik a WAN hálózaton belüli forgalomtorlódást.
- Egy bizonyos szervezet telephelyének védelmére szolgáló Telephelyi tűzfalak, amelyeken keresztül lehet csak belépni az ún. távoli (remote) hálózati számítógépekről a telephelyi hálózatba.

Ezek csupán a részletek voltak a termékkörből, de ha figyelmesen megnézzük a **KSZF portálján** a teljes termékkört, akkor megállapítható, hogy nagyon széles körben kezeli a lehetséges kialakításokat.

Ami azonban jelen beszerzésben fontosabb volt azok a passzív eszközök, melyre az alábbi leírást adja.

A hálózatok Passzív hálózati elemeire (BA: 0102080000), amelyek lehetnek:

- Menedzselhető passzív hálózati elemek.
- Kábelek (Hálózati eszközök).
- Nyomvonal építési anyagok.
- Rack szekrények.
- Rendezők.
- Szerelvények.

A keret-megállapodás azon túl, hogy meghatározza a termékkört - túlmenően külön általános műszaki követelményeket is hozzárendel.

Általános műszaki követelmények:

„A hálózati aktív eszközök az informatika gerincét alkotó hálózatok megvalósításában játszanak döntő szerepet. A hálózatok biztosítják az informatikai rendszerek azon átviteli közegét, amelyek elektronikusan továbbítják az információkat (adatot, képet, hangot) a felhasználók

között, illetve lehetőséget biztosítanak az információcserére számítógépek, alkalmazások között.

A termékcsaládoknak meg kell felelniük a szabványos információ-továbbítási követelményeknek, illetve megfelelő, szakértő tervezési elvek alkalmazásával biztosítaniuk kell az egyedi felhasználói követelményrendszer.

Az eszközök, illetve az általuk biztosított szolgáltatások tegyék lehetővé, hogy a hálózat(ok)ra illeszkedő szerverek, munkaállomások, és egyéb eszközök között a szükséges sebességgel, minőséggel továbbítódjon az információ.

A konstrukció korszerű technológiát képviseljen, ily módon biztosítva a beruházás 3-5 éves időtartamra történő - funkcionális - értékállóságát.

A helyi számítógép-hálózati eszközöknek biztosítaniuk kell az Ethernet szabvány követelményeit, és különböző fizikai szintű szabvány részleteit (réz kapcsolat, optikai kapcsolatok, különböző sebességű kapcsolatok). Az eszközcsalád biztosítson lehetőséget az Ethernettől eltérő szabványú kapcsolatok megvalósítására is, megfelelő eszközök kiválasztásának lehetőségével”.

Összevetve ezen leírást a beszerzés műszaki leírásával és műszaki követelményével elmondható, hogy lefedi a beszerzésünk tárgyát, sőt azon való túlmutatásra is lehetőséget ad.

A szállító vonatkozásában ezen termékkörben a **KSZF** 10 darab szerződést kötött, volt olyan aki egyedül indult volt olyan is aki valamely más céggel közösen.

A Keret megállapodásban szereplő vállalkozók közül többen az **HM híradó és informatikai** hálózatával kapcsolatban semmilyen tapasztalattal nem rendelkeztek, néhányuk pedig teljesen ismeretlen volt az ilyen jellegű projektek során.

Fenti indokoknál fogva a beszerzési bizottság a KSZF keret-megállapodáson belül próbálta szűkíteni a lehetséges vállalkozók számát így a következő szűrőt szeretne volna érvényesíteni:

A Vállalkozó rendelkezzen:

- A műszaki követelményekben meghatározott nagyságrendű hálózatépítési referenciákkal.
- NATO minősített beszállító tanúsítvánnyal.
- AQAP minőségirányítási rendszerrel.
- A minősített adatok feldolgozására, tárolására, nyilvántartására alkalmas helyiséggel, ügyviteli rendszerrel.
- Valamint a vállalkozó menedzsmenete, tervező szakállománya rendelkezzen minimum „B” a kivitelező munkálatokat végző szakállomány minimum „A” nemzetbiztonsági bevizsgálással.

A szűkítésre való igény nem volt egyértelmű, mivel keret megállapodás volt kötve a beszerzés tárgyára.

Ennek folyamodványként a Beszerzési Igazgatóság a KSZF-hez fordult levélben, hogy lehetséges e a keret-megállapodáson belül a további szűkítés.

A 2008. július 1 én a KSZF-től érkezett levél az alábbiakat tartalmazta:

„Hivatkozással a 2008. június 25.-én XXX nyilvántartású levelükre tájékoztatom, hogy tekintettel a KBT 136/B Paragrafus 3. bekezdés b. Pontjára, keret megállapodásos eljárás esetén, az intézmény közvetlen írásbeli ajánlattételi felhívást küld a keret megállapodásban részes valamennyi ajánlattevőnek, amennyiben a keret megállapodás nem tartalmazza az adott közbeszerzés megvalósítására irányuló szerződés valamennyi feltételét.

Tekintettel arra, hogy az Ajánlattevő alkalmasságát gazdasági-pénzügyi illetve műszaki-szakmai (Pl.referencia) szempontból az Ajánlatkérő már az eljárás első szakaszában megvizsgálta, a továbbiakban a verseny újranyitása során, csak a szerződésteljesítéshez szükséges

konkrét feltételek kiegészítésére, pontosítására van lehetőség, azzal kapcsolatban követelmény támasztható.”

A levelet értelmezve, megállapítható hogy ilyen jellegű szűkítés már nem lehetséges.

Felismerve azonban azt a tényt, hogy a *projekt 31 darab MH objektumban mintegy 4000 végpontos hálózatépítési feladatot tartalmaz, amely érinti a Magyar Honvédség szinte valamennyi katonai szervezetét*, s így az ajánlattevőknek lehetősége nyílik a **Magyar Honvédség** szervezeti struktúrájának, katonai objektumainak, valamint híradó és informatikai rendszereinek teljes megismerésére, a bizottság kapaszkodót a **228-as kormányrendeletben** keresett.

Ha megnézzük, a **228-as kormányrendeletet** arra a megállapításra juthatunk, hogy jelen beszerzés tárgya szintén csak nagyban illeszkedik az ott meghatározott termékkörbe.

Íme:

228/2004. (VII. 30.) Korm. Rendelet szerint:

„a védelem terén alapvető biztonsági érdeket érintő, kifejezetten katonai, rendvédelmi, rendészeti célokra szánt áruk beszerzésére, illetőleg szolgáltatások megrendelésére vonatkozó sajátos szabályokról a Kormány a közbeszerzésekről szóló 2003. évi CXXIX. törvény (a továbbiakban: Kbt.) 404. §-a (1) bekezdésének i) pontjában kapott felhatalmazás alapján a következőket rendeli el:

XI. Fejezet

A jelen Jegyzékben másutt nem szereplő, kifejezetten katonai célra tervezett elektronikai berendezések, valamint kifejezetten ezekhez tervezett alkatrészek (ML 11)

Megjegyzés:

1. Jelen fejezet magában foglalja a következőket:

a) Elektronikai ellentévékenység és elektronikai ellentévékenység elleni berendezéseket (úgy mint oda nem tartozó, vagy hibás jeleknek a radar, vagy rádió kommunikációs vevőkbe történő bejuttatására tervezett berendezéseket, vagy amelyek képesek másképpen megakadályozni az ellenséges elektronikus vevőket a hatásos vételben, működésben, be-

leértve azok ellentevékenységi berendezéseit is), beleértve a zavarás és zavarás elleni berendezéseket.

b) Széles frekvenciasávban hangolható elektroncsövek.

c) Elektronikai rendszerek, vagy berendezések, amelyeket elektromágneses spektrum ellenőrzésére és megfigyelésére, katonai hírszerzési vagy biztonsági célokra, vagy az ilyen hírszerzési és megfigyelési ellentevékenység elhárítására terveztek.

d) Víz alatti ellentevékenység eszközei, többek között akusztikai és mágneses zavaróeszközök és csapdák, a szonár vevőkbe zavaró, vagy hamis jeleket továbbító berendezések.

e) Biztonsági adatfeldolgozó berendezés, adattitkosító berendezés, rejtjelzési eljárásokkal ellátott biztonsági távközlési és jelátviteli berendezések.

f) Azonosító, engedélyező és kulcsbetöltő berendezés, valamint a kulcs kezelésére, készítésére és elosztására szolgáló berendezés.

g) Irányítási és navigációs berendezések.

2. számú Megjegyzés:

Jelen fejezet magában foglalja

a) a kifejezetten katonai célra kifejlesztett híradó és informatikai eszközöket, kapcsolás-technikai eszközöket és berendezéseket, adatátviteli eszközöket, kiegészítő készleteket, beleértve a Jegyzék hatálya alá tartozó eszközökbe utólag beépített, illetve leválasztható ilyen eszközöket, berendezéseket is.

b) a speciális elektronikus és mechanikus mérőeszközöket, ellenőrző, kalibráló és hitelesítő berendezéseket is.

Megállapítható, hogy a 228-as kormányrendelet e témakörét pontosítani szükségeltetik, mivel magát a rendszert nem említi, így a rendszerhez történő hozzáférésről sem lehet belőle semmit megtudni.

Könnyen belátható, hogy eszközvásárláson túl szolgáltatásokról is kell beszélnünk, s ilyen jellegű, híradó –informatikával kapcsolatos szolgáltatást, mint pl. strukturált alhálózat kialakítása, szoftvertelepítés stb. a kormányrendelet nem érint. Pedig a hálózaton végzendő munkálatok rengeteg „*szolgáltatással*” járnak.

Ezen kifejezett igényt már több katonai szerv is köztük a HM Hadműveleti és Kiképzési Főosztály is jelezte.

A szükséges változtatást az is indokolja, hogy az 1995. évi LXV törvény 70.pontja értelmében a Honvédelmi Minisztérium, valamint a Magyar Honvédség híradása megszervezésének összesített terve minősített adatnak minősül.

Tekintettel arra, hogy e hálózatépítési feladatok eredményeképpen kialakuló rendszer az összesített terv részét képezi, ezért már maga a műszaki követelmény sem lehet nyilvános.

Továbbiakban az is indokként szerepelhet, hogy a műszaki követelményekben megfogalmazott hálózatépítési feladatok kifejezetten a **VIR (MH Vezetési Információs Rendszerének)** kiterjesztését szolgálják, amely biztosítja mind a béke mind a minősített időszakos vezetés érdekében szükséges kapacitásokat, így már a teljes rendszeren nyílt és minősített adat és hangszolgáltatások is kerülhetnek továbbításra.

Megnyugtató módon az eljárás elindult a **228**-as kormányrendeletbe kapaszkodva ahol már valamiféle szűrést elő lehetett írni.

Ilyen jellegű munkálatoknál még meg kell említeni, hogy vannak az úgynevezett „**konstrukciós időszakok**” amikor nincs igazából hatással az időjárás a munkálatokra - mivel jelentős földmunkával is járhat egy ilyen jellegű beruházás, (amit télen nem mindig lehet elvégezni) ezért egy eljárás csúszása hatással lehet a kivitelezésre is.

A fent említett szűkítési körben egy nagyon fontos területre szeretném felhívni a figyelmet s ez az **AQAP** minőségirányítási rendszer.

4. NATO Beszállítói Rendszer és az AQAP rendszertanúsítás

Ebben a fejezetben szeretnénk összehasonlítani két különálló témát, azonban annak ellenére, hogy a témakörök különállóak mégis valamifajta összefüggést érdemes lenne benne találni már csak azon apropóból is mivel a katonai minőségbiztosítás és a NATO, mint szervezet szoros összefüggésben van.

Röviden ismertetném először a két témát, elősegítve annak jobb megértését, összefüggéseit.

A HM Fejlesztési és Logisztikai Ügynökség Technológiai Igazgatósága (továbbiakban HM FLÜ TI) számára a honvédelmi miniszter feladatul szabta a hadfelszerelést szállítók katonai követelmények (NATO AQAP) előírásai alapján való tanúsítását.

A Nemzeti Akkreditáló Testület a HM FLÜ TI-t minőségirányítási rendszerek tanúsítására akkreditálta. Az akkreditálás kiterjed a NATO AQAP 2110/2120/2130/160 normatív dokumentumok, és/vagy az MSZ EN ISO 9001:2001 szabvány alapján kiépített minőségirányítási rendszerek tanúsítására és felülvizsgálatára.

Az MSZ EN ISO 9001:2001 szabvány követelményei szerint kiépített minőségirányítási rendszerek minősítését a HM FLÜ TI azon szervezetek részére végzi el, amely szervezetek nem rendelkeznek ilyen tanúsítvánnyal, és közös eljárásban kívánják tanúsíttatni a NATO AQAP 2110/2120/2130/160 normatív dokumentum és az MSZ EN ISO 9001:2001 szabvány szerinti minőségirányítási rendszerüket. E szervezetek így közös eljárásban szerezhetik meg AQAP 2110/2120/2130/160 NATO normatív dokumentum, és az MSZ EN ISO 9001:2001 szabvány követelményeinek való megfelelést bizonyító Tanúsítványt.

Az AQAP 2110/2120/2130/160 NATO normatív dokumentum követelményei szerinti tanúsítvány megszerzésére lehetőség van önálló eljárás keretében azoknak a szervezeteknek, amelyek rendelkeznek az MSZ EN ISO 9001:2001 szabvány szerinti tanúsítvánnyal. Ez esetben a Tanúsítvány még legalább 1 évig érvényes kell, hogy legyen az AQAP 2110/2120/2130/160 NATO normatív dokumentum szerinti tanúsítás kérelmezésekor.

Ajánlott a NATO AQAP normatív dokumentumok követelményei szerinti katonai minőségirányítási rendszer működtetésének tanúsítása az alábbi vállalkozások részére:

- Azoknak a hadfelszerelési anyagot előállító és a hadfelszerelési anyagokhoz kapcsolódó szolgáltatást nyújtó vállalkozásoknak, akik a hon- és rendvédelmi szervezetek részére -szerződéses viszony keretén belül- terméket szállítanak, vagy ezekhez kapcsolódó szolgáltatást nyújtanak.
- Az előző pontban részletezett beszállítók alvállalkozóinak.
- Azoknak, akik tanúsított minőségirányítási rendszert működtetnek, vagy kívánnak működtetni és felkészültek arra, hogy beszállítói lehessenek a hon- és rendvédelmi szervezeteknek.

- Azoknak, akik **NATO** tagország részére hadfelszerelési anyagot szállítanak, vagy a hadfelszerelési anyagokhoz kapcsolódó szolgáltatást nyújtanak.
- Az előző pontban részletezett szállítók alvállalkozóinak.
- Azoknak, akik a hadfelszerelési anyagok közbeszerzési eljárásaiban eredményesen szeretnének pályázni.

A tanúsítvány a számtalan előnye mellett a biztonsághoz talán legjobban köthető hogy, hozzáférési jogot biztosít azokhoz a létesítményekhez (telephelyekhez), ahol a vállalkozó a szerződésben rögzített tevékenységeket, résztevékenységeket végzi.

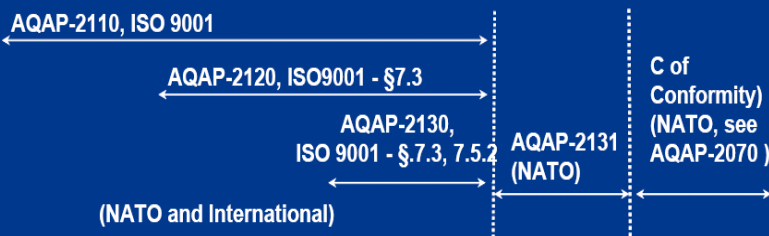
Az **AQAP 2000** sorozat az adott szolgáltatást, termék előállítását a termék teljes életciklusában vizsgálja és a **NATO** minőségpolitikája értelmében nem csupán a terméket magát, hanem a termék előállítással kapcsolatos egész rendszert vizsgálja. Ennek megfelelést bizonyítja az **AQAP** tanúsítvány.

AZ **AQAP** az **ISO** - hoz, képest olyan többlet követelményt tartalmaz, mint a katonai termék előállításához vonatkozó minőségterv, a konfigurációrányítás szabályozása, kockázatelemzés, kockázatkezelés, és a karbantarthatósági és megbízhatósági követelmények szabályozása.

QUALITY ASSURANCE IN NATO

AQAP = Allied Quality Assurance Publication

DESIGN, DEVELOPMENT, PRODUCTION	PRODUCTION	INSPECTION and TEST	FINAL INSPECTION	CERTIFICATE of CONFORMITY
Contractor is responsible for design and development	Complexity of the product requires comprehensive control of quality and of processes	Conformance can only be demonstrated on basis of inspection during manufacturing	Conformance can be demonstrated on receipt of the final product	Need to have the contractor certify that product meets requirements



Minőségbiztosítás a NATO-ban

Mivel az **AQAP** teljes egészében tartalmazza az **ISO** követelményeket (**ISO 9000**) s ezen túlmenően egyéb követelményeket is támaszt ezért minőségbiztosítási szempontból **NATO** beszállításhoz az **AQAP** követelmények teljesítését és nem csupán az **ISO** követelményeket lenne célserű megkövetelni.

A katonai rendszertanúsítási tevékenységet a **HM FLÜ TI Rendszertanúsító és Kodifikációs Osztálya** végzi. A **HM FLÜ TI** katonai rendszertanúsítási tevékenységének függetlenségét a tanúsítási folyamatban érdekelt felek képviselőiből létrehozott **Igazgató Testület** biztosítja.

A HM FLÜ TI katonai minőségirányítási rendszerek tanúsítását a *következő területeken végzi:*

Szakterület száma	AQAP 110/2110/120/2120/130/2130/160 MSZ EN ISO 9001:2001	A szakterület megnevezése
4.	■	Hadi felhasználású textil és textilipari termékek
5.	■	Hadi felhasználású bőr és bőrtermékek
12.	■	Katonai felhasználású vegyipari termékek.
17.	■	Katonai felhasználású nyersfémek és fémipari termékek
18.	■	Katonai felhasználású gépek és berendezések
19.	■	Katonai felhasználású elektromos és optikai berendezések
21.	■	Katonai légi-járművek
23.	■	Máshová nem besorolható katonai felhasználású termékek
28.	■	Katonai rendeltetésű műtárgyak építése
31.	■	Katonai hírközlés
33.	■	Informatika
34.	■	Haditechnikai kutatás-fejlesztéssel kapcsolatos mérnöki szolgáltatások
35.	■	Egyéb katonai jellegű szolgáltatások

NATO Beszállítói Rendszer

A NATO Beszállítói határozat megszerzésének feltételeit *"az Észak-atlanti Szerződés Szervezete Biztonsági Beruházási Programja keretében kiírásra kerülő pályázatokon való részvételi jogosultság feltételeiről, a jogosultság megszerzésével kapcsolatos eljárás szabályairól és az eljáró szervezetről"* szóló 164/2002. (VIII.2.) Kormányrendelet rögzíti.

A kormányrendeletben az alábbiak találhatóak:

A minősítéseknek való megfelelés feltételeit alapvetően az alábbi szempontok szerinti adatok, információk előírásával határozza meg:

- a) a gazdálkodó szervezet pénzügyi, gazdasági helyzete;*
- b) a gazdálkodó szervezet szakmai felkészültsége, tevékenysége, műszaki-technikai felszereltsége, személyi állománya;*
- c) a gazdálkodó szervezet minőségbiztosítási rendszere;*
- d) a gazdálkodó szervezet referenciái.*

Ezen értékelésnek megfelelően a magyarországi belföldi székhellyel rendelkező, gazdálkodó szervezetek „*NATO Beszállításra Alkalmas*” és „*Minősített NATO Beszállításra Alkalmas*” határozatot szerezhetnek.

Egy gazdálkodó szervezetnek az elnyert beszállítói határozat nem feltétlenül fedi le a teljes profilját, csak azon jellemző tevékenységére, tevékenységeire vonatkozik, melye(ke)t megpályázott. Ennek feltétele, hogy ezen tevékenység(ek)hez a pályázat benyújtásakor érvényes **MSZ EN ISO 9001:2001** minőségirányítási rendszer tanúsítvánnyal, megfelelő **TEÁOR (Tevékenységek Egységes Ágazati Osztályozási Rendszere)** kóddal, és legalább három éves folyamatos szakmai referenciákkal rendelkezzen.

Ezen cím odaítéléséhez már nem csupán **MSZ EN ISO 9001:2001** szabvány meglétét, hanem ezen túlmenően a megfelelő **AQAP** tanúsítványt lenne célszerű előírni, mert külön-külön elveszítik azokat az előnyöket, amelyeket a **HM** számára jelentenek a haditechnikai vagy ilyen célú beszerzések során.

Most egy kicsit nézzünk ki az országhatáron túlra!

A **NAMSA** beszállítói forrásfájlba csak azok a szállítók kerülhetnek be, amelyek megkapják a tagországbeli hivatalos szerv azon bizonyítványát, hogy ilyen jellegű szállításra/ szolgáltatásra alkalmasak.

Azt gondolom, hogy a **NAMSA** beszerzési céglistájára a minősített **NATO Beszállítói** címmel lehet jelentkezni.

A **CNAD (Conference of National Armaments Directors - A Nemzeti Fegyverzeti Igazgatók Értekezlete)** - strukturált betagozódásban jelen levő minőségbiztosítási csoport az **AQAP** minőségirányítási

rendszer, **mint alapvető referenciát** jelöli meg haditechnikai beszerzések területén.

A NATO munkacsoportjainak drasztikus csökkentése előtt levő minőségüggyel foglalkozó munkacsoportról a *következők jelentek meg:*

„Group of National Directors for Quality Assurance - AC/250. This Group publishes Allied Quality Assurance Publications (AQAP) as the basic reference for the enforcement of quality assurance standards for weapon systems and other defence equipment entering the inventory of Alliance forces, as well as for the development of reliability and maintainability guidelines.”

Jelenleg ez a munkacsoport CNAD Life-Cycle Management Group (LCMG) AC/327 csoportjába integrálódott.

6. Megoldások

A kölcsönös összeköttetések növekvő mértéke miatt az információs rendszerek és hálózatok napjainkban növekvő számú és változatosabb fenyegetéseknek vannak kitéve, és sebezhetőségük mértéke és változatosága is megnőtt. Ez új biztonsági kérdéseket vet fel. A kommunikációs és információs infrastruktúrát alkotó technológiák jellege és típusa úgyszintén jelentős mértékben megváltozott.

Az *infrastruktúra*-hozzáférést biztosító eszközök száma és fajtája megsokszorozódott, s ezek tartalmazzák a rögzített, vezeték nélküli és mobil készülékeket, valamint a hozzáférés egyre növekvő százaléka *„mindig bekapcsolt”* csatlakozásokon keresztül történik. Ennek következtében a kicserélt információ jellege, mennyisége és érzékenysége jelentősen megnövekedett. A kölcsönös összeköttetések növekvő mértéke miatt az információs rendszerek és hálózatok napjainkban növekvő számú és változatosabb fenyegetéseknek vannak kitéve, és sebezhetőségük mértéke és változatosága is megnőtt. *Ez új biztonsági kérdéseket vet fel.*

Tudatosítani kell az információs rendszerekre és hálózatokra vonatkozó kockázatokat, valamint az ezen kockázatok kezelésére rendelkezésre álló politikai irányelveket, gyakorlatokat, intézkedéseket és eljárásokat.

Ennek megfelelően a beszerzési eljárások során a **MH híradó és informatikai hálózatát** valamilyen módon kiemelt szerepben kellene kezelni.

Első ütemben a 228.-as kormányrendelet alá kellene vonni az MH híradó és informatikai hálózatát.

Itt konkrétan nevesítve például az alábbiakban:

„ Az MH híradó és informatikai hálózata valamint a hálózatot érintő beruházások.”

Vagy: ugyanilyen címmel, de nevesítve hogy pontosan milyen jellemző beruházásokról van szó a tárgyát a **143/2004. (IV. 29.)** Korm. rendelet alá lehetne vonni.

A **143/2004** kormányrendelet az államtitkot vagy szolgálati titkot, illetőleg alapvető biztonsági, nemzetbiztonsági érdeket érintő vagy különleges biztonsági intézkedést igénylő beszerzések sajátos szabályairól szól.

A rendelet hatálya a Kbt. által ajánlatkérőként meghatározott szervezeteknek a Kbt. szerinti egyszerű közbeszerzési eljárás mindenkor értékhatárait elérő vagy azt meghaladó értékű olyan beszerzéseire terjed ki, amelyek államtitkot, szolgálati titkot, illetőleg alapvető biztonsági, nemzetbiztonsági érdeket érintenek, illetve különleges biztonsági intézkedést igényelnek.

(2) A Kbt. IV. és VI. fejezete szerinti ajánlatkérők esetében a nemzeti közbeszerzési értékhatárokat elérő vagy azt meghaladó értékű (1) bekezdésben meghatározott beszerzésekre a rendelet hatálya akkor terjed ki, ha a beszerzésre az Országgyűlés illetékes bizottsága a Kbt. alkalmazását kizáró előzetes döntést hozott.

(3) Amennyiben a beszerzés a NATO Biztonsági Beruházási Program keretében valósul meg, abban az esetben az arra vonatkozó külön jogszabály rendelkezéseit kell alkalmazni.

A beszerzés tárgya illeszkedhetett volna ebbe a kormányrendeletbe is hiszen:

6. § (1) A beszerzés tárgya árubeszerzés, építési beruházás, építési koncesszió, szolgáltatás megrendelése, illetve szolgáltatási koncesszió. E rendelet alkalmazásában árubeszerzés, építési beruházás, építési koncesszió, szolgáltatás megrendelése és szolgáltatási koncesszió alatt a Kbt. 242. §-ában így meghatározott fogalmakat kell érteni.

Összegezve: A Híradó és informatikai beruházásokra mind a **228**-as kormányrendeletben történő pontos szerepeltetés mind az idézett **143**-as kormányrendelethez történő folyamodás megoldást nyújthatna.

A tanúsítások területén pedig célszerű lenne a **AQAP** minőségirányítási rendszer feltételként történő beemelése a **NATO Beszállítói Rendszer**-be.

A híradó és informatikai beruházások bevonása a 228, vagy a 143.-as kormányrendelet alá:

Hatások:

Pozitív:

- Egyértelműbb eljárási mód kiválasztásának lehetősége a beszerzésekkor.
- Időtakarékosság az eljárás alatt.
- Szinkronizáltabb összeférhetőség megteremtése a különféle egymásra épülő eljárásokban.
- Ismert jól teljesített, minőségi munkát végző vállalkozások nagyobb fokú megjelenése az eljárásokban (meghívás stb.).

Negatív:

- Részben csökken a verseny.

Az AQAP minőségirányítási rendszer előírása a NATO beszállítói címhez:

Hatások:

Pozitív:

- A NATO beszállítói cím felértékelődése.
- Fejlettebb minőségirányítási rendszer megjelenése a beszállítói oldalon.
- Minőségében emelt teljesítések.
- Biztosabb, jobb pályázatok benyújtása a NATO projektek során a beszállítói oldalon.
- Magyar vállalkozások nagyobb térnyerése a nemzetközi piacon.

Negatív:

- Ideiglenesen csökken a verseny (azon beszállítók, akik nem rendelkeznek AQAP tanúsítással, ideiglenesen kiszorulnának a piacról, ezt egy 1-1,5 éves türelmi idővel lehetne feloldani, ezen időn belül megszerezhetik a tanúsítványt).

7. Befejezés

Már korábban is bizonyosságot nyert, hogy nemcsak a HM-MH az a szervezet, aki az elektronikus információ biztonságával foglalkozik és ennek során különös gondot fordít az információk védelmére, hanem a civil életben is komoly erőforrások állnak rendelkezésre.

Mindenhol előtérbe kerül a biztonság kérdése, ez azonban lehet már megelőző jellegű is, a biztonság – a minőség mindnyájunk közös érdeke, amelyet lehetőleg még a projektek megkezdésekor célszerű a legmagasabb fokon érvényesíteni.

A folyamatos fejlődés is indokolhatja, hogy a különféle törvények, rendeletek tartalma nem életszerű, ekkor természetesen ki kell igazítani.

A problémák, a feladatok hasonlóak, hiszen mindenki szeretné biztonságban tudni az általa kezelt információkat, kiemelten a minősített információkra vonatkozóan, hiszen a **Magyar Köztársaságban** az egyik legnagyobb minősített információhalmazt kezelő szervezet a **HM-MH**.

A Magyar Honvédségben a híradó és informatikai projektek gyakran egymásra épülnek, így egy eljárás elhúzódása más, már sikeresen a végrehajtás szakaszába ért projektek elhúzódását is okozza, ezek szinkronba kerülése a legfontosabb a gördülékeny végrehajtás érdekében.

Érdemes elgondolkodni, hogy a keret-megállapodásokon belül mennyire lehet kezelni a híradó és informatikai beruházásokat.

A téma aktualitását az is kiemeli, hogy a világ az elektronikus ügyintézés, elektronikus adatkezelés irányába halad, és a nem is olyan régi kormányzati- informatikai infrastruktúra elleni támadás is előtérbe helyezte védelem kérdéskörét.

Rövidítések:

Rövidítés	Jelentése
HM FLÜ	Honvédelmi Minisztérium Fejlesztési és Logisztikai Ügynökség
BI	Beszerzési Igazgatóság
TI	Technológiai Igazgatóság
ATKI	Anyagi,technikai és Közlekedési Igazgatóság
PTVI	Program Tervezési és Vezetési Igazgatóság
GI	Gazdasági Igazgatóság
AQAP	Allied Quality Assurance Publication
STANAG	Standardization Agreement
ISO	International Organization for Standardization
RKO	Rendszertanúsító és Kodifikációs Osztály
WAN	Széles kiterjedésű hálózat
TOHF	Tartalék Országos Hálózatfelügyeleti Központ
SNMP	proxy ágens
PM	Forgalomfelügyelet
RHF	Regionális Hálózatfelügyeleti Központ
OHK	Országos Hálózatfelügyeleti Központ
LB	Helyi telepes
HDMS	HICOM Hálózat Menedzsment Alkalmazás
ISDN	Integrált Szolgáltatású Digitális Hálózat
LAN	Helyi hálózat
AQAP	Allied Quality Assurance Publication
TEÁOR	Tevékenységek Egységes Ágazati Osztályozási Rendszere
MOD	Magnetic Optical Driver
ÉBT	Éves Beszerzési Terv
KSZF	Po Központi Szolgáltatási Főigazgatóság
CNAD	<i>Co Conference</i> of National Armaments Directors

Felhasznált irodalom:

1. **Dr. Szűcs Gáspár:** A Magyar Honvédség informatikai helyzete, fejlesztési tervei, problémái. „Kommunikáció 2003.” nemzetközi szakmai tudományos konferencia, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, ISBN 963 86229 6 2, 370–373. oldal, 2003. október 15.
2. **Szöllősi Sándor:** Az új típusú haderő és a súlypont-átrendeződés kérdései a technikai struktúrában. Kommunikáció 2003.” nemzetközi szakmai tudományos konferencia, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, ISBN 963 86229 6 2, 365. oldal, 2003. október 15.
3. **Fekete Károly:** A Magyar Honvédség állandó telepítésű kommunikációs rendszere továbbfejlesztésének technikai lehetőségei. Doktori (PhD) értekezés, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 120–121. oldal, 2003.
4. **Balogh Tamás:** Az ISDN felépítése, ISDN szolgálatok, szolgáltatások és alkalmazásai, - Bp. -PKI-FI Adat és Kommunikációs osztály, 1994.
5. **Dr. Kovács Oszkár:** A Szélessávú ISDN kialakulása és képességei MATÁV PKI Távközlési Intézet 1097. Budapest Zombori u. 1.
6. **Rózsa I. G.-Unghváry F:** Gerinchálózati struktúrák megbízhatósága. MAGYAR TÁVKÖZLÉS 1998/3 (IX. évfolyam 3. szám)
7. 2003.évi CXXXIX törvény.
8. 228/2004/VII.30. Korm. rendelet.
9. 120/2007 (HK.20) HM utasítás.
10. 143/2004. (IV. 29.) Korm. rendelet.
11. NAMSÁ webpage.
12. KSZF portál.