HADMÉRNÖK

X. Évfolyam 3. szám - 2015. szeptember

KASSAI Károly
karoly.kassaiv@hm.gov.hu

AZ ELEKTRONIKUS INFORMÁCIÓVÉDELEM FELSŐ SZINTŰ SZERVEZETI ÉS SZAKMAI TÖRTÉNÉSEI A 2005-2015 KÖZÖTTI IDŐSZAKBAN

Absztrakt

A híradó szakterület 2015 júliusában ünnepelte a híradó szolgálat alapításának 70. évfordulóját a Honvéd Vezérkar, Híradó, Informatikai és Információvédelmi Csoportfőnökség szervezésében. A Magyar Honvédségnél a 60. évforduló óta eltelt időszak mozgalmas volt a híradó-informatikai és az információvédelmi szakterületeken szervezeti, üzemeltetési és fejlesztési szempontból egyaránt. A híradó-informatikai szolgáltatások fejlődése tízéves időszak alatt jól értékelhető, így az esemény jó lehetőséget teremt a védelmi szempontú áttekintésre, a kihívások bemutatására. A cikk célja a feladatok összetettségének az egyre bonyolultabb hálózati szintű együttműködés érzékeltetése az elektronikus információvédelem területén.

The military signal service celebrated its 70th anniversary of foundation organised by the Ministry of Defence, General Staff, Communications and Information System (CIS) and Information Assurance Department in July 2015. The period since the 60th anniversary of the CIS and information security fields at Hungarian Defence Forces was eventful from organization, operation and development point of view. The development of CIS services can be evaluated well over ten years so this event a good opportunity for CIS security aspects review, presenting challenges. This article aims to illustrate the complexity of tasks and increasingly complicated network-wide cooperation in field of CIS security.

Kulcsszavak: *információbiztonság, elektronikus információbiztonság, kiberbiztonság, biztonsági menedzsment, információbiztonsági követelmények ~ information security - electronic information security (INFOSEC, CIS Security), cyber security, security management, information security requirements.*

BEVEZETÉS

2015 júliusában a Magyar Honvédségnél a híradó szolgálat fennállásának 70. évfordulóját ünnepelhettük. Az évforduló remek lehetőség a HVK Híradó, Informatikai és Információvédelmi Csoportfőnökség szakterületein belül a fontosabb történések áttekintésére.

Az eseményről a tíz évvel korábbiakhoz hasonlóan korlátozott számú kiadvány jelent meg, ami tartalmazza a fontosabb szervezeti változásokat, szakmai eredményeket. Az elektronikus információvédelem történései az utolsó tíz évben változatosak voltak, korábban nem jelentkező kihívásokat kellett kezelni, melyek megalapozzák a szakterületi rész önálló cikkben történő összefoglalását, természetesen csak a publikus információkra koncentrálva.

2004-2005

A 2005-ös évet megelőzően a NATO csatlakozás idejétől egyre jelentőségteljesebben erősödő *általános elektronikus információvédelem és a rejtjelzés szakmai irányítási és felügyeleti rendje felső szervezeti szinten elkülönült.*

A HVK Híradó, Informatikai és Információvédelmi Csoportfőnökség, Elektronikus Információvédelmi Osztály jogelőd szervezete abban az időszakban a HM Információ és Dokumentumvédelmi Főosztály (HM IDVF), Elektronikus Információvédelmi Osztály volt 2004. 01. 31-ig.

A rejtjelzés szakmai felügyeletét a HVK Híradó-Informatikai Csoportfőnökség, Rejtjelző Osztály látta el. Az MH Központi Rejtjelfelügyelet vezetői feladatokat a csoportfőnök látta el.

Az 1999-es NATO csatlakozáskor nevesített NATO Központi Rejtjelelosztó (National Distribution Authority; NDA) funkciót az akkori MH Híradó és Informatikai Parancsnokság Főhírközpont Központi Rejtjelző Nyilvántartó Alosztály látta el. Szakmai érdekesség, hogy az angol „NDA" kifejezés hazánkban azonnal meghonosodott, annak ellenére, hogy a NATO elosztási és nyilvántartási feladatoknál az alosztály, illetve az országos nyilvántartási rendszer lényegesen szélesebb körű feladatokat lát el, ami napjainkra is érvényes.

A HM IDVF felelősségi köre 2004 februárjában szervezeti átalakítás keretén belül változott és az elektronikus információvédelem szakmai irányítási feladatai átkerültek HM HVK Híradó és Informatikai Csoportfőnökség, Elektronikus Információvédelmi és NATO/NYEU Központi Rejtjelelosztó Osztályhoz. *Szakmai szempontból ez azt jelenti, hogy az akkori nemzeti megfogalmazás szerinti „számítástechnikai titokvédelem" – a NATO megközelítés szerinti általános elektronikus információvédelem – és a rejtjelzés közös szervezeti kereteket kapott.*

Az NDA feladatokat a szervezeti változás nem érintette, az MH Központi Rejtjelfelügyelet vezetői funkciót továbbra is csoportfőnök látta el.

2005-ben haderő átszervezési feladat keretén belül az információvédelem területén kettős változás következett be. Megszűnt a HM IDVF, mint a dokumentumvédelmi szakmai irányításért felelős szervezet, illetve felszámolt a HM HVK Híradó és Informatikai Csoportfőnökség, benne az elektronikus információvédelemért felelős szervezeti elem.

Az „integrált" elektronikus információvédelmi szakterületek felelős szervezeti eleme 2005. 04. 01-től a HM Jogi és Információvédelmi Főosztály, Elektronikus Információvédelmi és NATO/NYEU Központi Rejtjelelosztó Osztály lett, az MH Központi Rejtjelfelügyelet vezetői funkciót az osztályvezető látta el.

Az összetett szakmai feladatok ellátása, a hatékonyság növelése érdekében a rejtjelző és az általános elektronikus információvédelmi szakterületekre egy-egy osztályvezető helyettesi beosztás alakult. A szervezeti megnevezésből is látható, hogy a korábban MH HIP állományába tartozó NDA átkerült az osztály szervezetébe, azon belül elkülönül alosztályként működött.

A korszak jellegzetes feladata volt a honvédelmi szervezetek állománytábláinak felülvizsgálata, racionalizálása, illetve a gyakran évek óta húzódó kérdések megoldása, benne a rejtjelzés új kihívásaival. Az egyik legfontosabb megoldandó kérdés a NATO Biztonsági Beruházási Program és más haderőfejlesztés kapcsán a minősített elektronikus adatkezeléshez jogszabályban meghatározott követelmény szerinti rejtjeltevékenységhez szükséges állománytáblás rejtjelző helyek kialakítása és feltöltése.

A 2004. év az EU csatlakozással kapcsolatos utolsó szakmai erőfeszítéseket is jelentette. Az akkori Külügyminisztérium hálózatgazdai és biztonságfelügyeleti irányítása mellett megtörtént az EU BIZALMAS minősítésű adatokat kezelő speciális híradó-informatikai rendszer – a Védett Külügyi Hálózat – központi kiszolgáló szervereinek, rejtjelző megoldásainak kialakítása és feszített tempóban *telepíteni és akkreditáltatni kellett az alkalmazó szervezetek végpontjait*, ami alól a Honvédelmi Minisztérium sem lehetett kivétel.

Az időszak NATO elektronikus információvédelmi területű másik áttörésének tekinthető, hogy *menedzsment és akkreditálási szempontból elkezdődött a két legfontosabb Magyarországon elérhető NATO vezetési és irányítási szolgáltatás* – a NATO magyarországi TITKOS minősítési szintű adatkezelésre feljogosított híradó-informatikai rendszer (WAN); közismert nevén NIAR és a NATO légivezetési és irányítási rendszer (ICC) – *egy hálózatként történő kezelése*. Az éveken keresztül húzódó előkészítés végül sikeres eredményt hozott, a Nemzeti Biztonsági Felügyelet engedélyezte a közös hálózatként történő kezelést.

A kihívást okozó probléma magában a fejlődésben gyökeredzett. Az 1999-es NATO csatlakozáskor NATO technikusok által telepített, NATO tulajdonú eszközökből álló híradó-informatikai rendszer és az évekkel később telepített – de kezdetektől IP alapú – ICC hálózat, közös külföldi csatlakozási pontot használt, *de az alkalmazott technológiát tekintve eltérő volt, illetve az üzemeltetés és biztonsági felügyeletet is más-más katonai szervezet látta el*.

A változás részét képezte a hardver és szoftver platform korszerűsítése, a rejtjelző eszközcsere – mely lépés egyben a központi menedzsment alá szervezett rejtjelző eszközök fejlődésének adott jelentős lökést – a biztonsági dokumentumok és szabályok átszervezése, illetve *mindehhez a hatósági engedélyek megszerzése, beleértve a NATO illetékes biztonsági szervezetének egyetértését is*.

Az egységesítés másik jelentős állomása 2005 elején történt, ami a NATO csatlakozás óta húzódó szervezetek közötti üzemeltetési és biztonságfelügyeleti felelősség megosztást tette helyére. Az addigi rend szerint a NIAR központi üzemeltetési feladatokat a szerverekért felelős katonai szervezet – MH Híradó és Informatikai Parancsnokság – kijelölt szervezeti eleme látta el, míg a központi biztonságfelügyeleti feladatokat a korábban kialakult, nem pontosan értelmezett fontosságra és szakértő állomány hiány miatt a HVK Híradó és Informatikai Csoportfőnökség elektronikus információvédelemért felelős osztály személyi állománya látta el.

A helyzet megérett arra, hogy az üzemeltetői körbe tartozó rendszerbiztonsági felelősi feladatokat és az általános szakmai irányítási és felügyeleti feladatokat szét kell választani, azok egy szervezeti elemnél történő ellátása – mely ráadásul eltér az üzemeltető szervezettől – megoldhatatlan összeférhetetlenségi problémák örökös forrása lesz. A szervezési lépésnek köszönhetően beállt a napjainkban is meglévő „üzemeltetés” és „általános felügyelet” egyensúlya.

A NATO Biztonsági Beruházási Program keretén belül *ebben az időszakban történt meg a rejtjelző szolgáltatással támogatott föld-levegő azonosítási rendszer (IFF) földi helyszínein a szükséges NATO BIZALMAS minősítési szintnek megfelelő kiszolgáló infrastruktúra kialakítása*, a telepítések és a szükséges rejtjeltevékenység megszervezése.

A szárazföldi harcászati tevékenység mobil kommunikációjának biztosítása érdekében megkezdődött a Kronsberg gyártmányú többfunkciós, rejtjelző modullal rendelkező URH rádiók rejtjelző rendszeresítési eljárása, a kulcsgyártáshoz szükséges infrastruktúra telepítése.

2006-2009

2006. 09. 01-től új helyzet állt elő. Az akkori HM Jogi és Információvédelmi Főosztály szervezeti átalakítása során megtörtént a dokumentumvédelmi és elektronikus információvédelmi szakfeladatok kiszervezése. Ezen szakmai irányítási és felügyeleti feladatok átkerültek az újonnan megalakuló HM Informatikai és Információvédelmi Főosztályhoz.

A 2005-2006 évek jellegzetessége, hogy az akkori Zrínyi Miklós Nemzetvédelmi Egyetem, Híradó Tanszék szervezésében és végrehajtásában az elektronikus információvédelmi osztálynál kialakított és a főosztályvezető által meghatározott szakmai követelmények alapján *kialakult az általános elektronikus információvédelem és a rejtjelzés tanfolyami képzési rendje*. A rendszerbiztonsági felelős (később felügyelő), az elektronikus információvédelmi kockázatelemzés, a rendszeradminisztrátori, a kompromittáló kisugárzás elleni védelmi szaktanfolyamok, valamint a rejtjelző alaptanfolyamok és eszközkezelő tanfolyamok az óta is biztosítják a honvédelmi szervezetek és indokolt esetben a közigazgatás más területeiről vezényelt személyek alapfokú szakmai ismereteinek kialakítását.

2007. január elsejével középszintű vezető szerv szinten jelentős változás történt. A légierő, szárazföldi és logisztikai parancsnokságok felszámolásával megalakult az MH Összhaderőnemi Parancsnokság, ami a szakmai irányítási rendben, rejtjelanyag elosztásban jelentős változást okozott. A légierő és a szárazföld híradó-informatikai rendszereinek funkcionális és üzemeltetési sajátosságai, a NATO Biztonsági beruházási Program aktuális feladatai az új szervezeti elem munkáját jelentősen változatossá tették.

2007-ben a Visegrádi Együttműködés államai védelmi minisztériumainak katonai információbiztonságért felelős szervezetek között szervezett formában – azóta is fennálló – együttműködés kezdődött a szlovák V4 elnökség idején Pozsonyban az elektronikus információvédelmi és a dokumentumvédelmi osztályok szervezésében, melynek lényege az egyeztetés és tapasztalatcsere az információvédelmi képzés, új technológiák fejlesztése és alkalmazása területén.

Az éves szakmai találkozók rendjén kívül közvetlen szakmai támogatás történt már kompromittáló kisugárzás elleni védelmi (TEMPEST), GRIPEN földi híradó-informatikai rendszer felügyelet, NATO légivezetési és irányítási rendszer (ICC) modernizáció, szabályozási keretrendszer területeken. Az évek során egyre hasznosabbá válik a fejlesztési irányok azonosítására, hálózatbiztonsági kérdések megoldására irányuló tapasztalatcsere.

2008-ban hazánk adott Budapesten helyszínt a kétévente rendezett NATO Informális Miniszteri találkozónak. A három szállodából álló civil infrastruktúrára tervezett több százfős rendezvény tervezését 11 hónapos előkészítő tevékenység előzte meg. A híradó-informatikai és információvédelmi biztosítást az elektronikus információvédelmi osztály és az akkor Hadműveleti Főosztály keretében működő Informatikai Osztály képviselője irányította. A katonai irányítással, de civil szolgáltatókkal biztosított rendezvény a zártláncú TV-s közvetítéstől kezdve a sajtó kiszolgáláshoz szükséges speciális kommunikációs igények megoldásán keresztül rejtjelző szolgáltatásokat és a szállodai kapacitásokra ráépített összetett távközlési és irodatechnikai képességeket biztosított, melyre korábbi katonai példa nem hozható.

A 2008-as év a GRIPEN többfunkciós harcirepülők hadrendbe állításával kapcsolatos utolsó erőfeszítések éve is volt, a MIG-29-es harcirepülőktől való feladatátvétel érdekében. A svéd tulajdonú, nemzeti és NATO minősített adatokat kezelő földi kiszolgáló híradó-informatikai rendszer akkreditálása az akkori jogszabályi környezetben nem tartozott az „egyszerű kihívás" kategóriába.

A GRIPEN Program Biztonsági Utasítás a *Nemzeti Biztonsági Felügyelet (NBF) országos hatáskörének meghagyása mellett a katonai információbiztonságért felelős HM szervet már korábban kijelölte kapcsolattartónak és fő felelősnek*. Ebben az időszakban *a jogszabályi*

követelmények elektronikus információvédelem területén hazánkban még nem voltak részletesen kidolgozva, az NBF hatásköre nemzeti és a NATO, EU minősített adatkörön kívülre nem vonatkozott.

A két jelentősen eltérő elektronikus információvédelmi gondolkodásmód, az eltérő svéd és magyar hatósági gyakorlat összehangolásához a NATO elektronikus információvédelmi tapasztalatokra kellett támaszkodni, illetve *ki kellett alakítani egy olyan szoros együttműködést, ami féléves biztonsági munkacsoport ülések és a szakmai kapcsolattartók közötti kommunikációra támaszkodva napjainkban is biztosítja a hálózati, rejtjelző vagy éppen adathordozók adminisztratív védelmével kapcsolatos kérdések megoldását*.

2008-ban megkezdődött a légvédelmi rendszer minősített adatokat kezelő speciális híradó-informatikai rendszer – Mobil Harc és Tűzvezetési Rendszer – akkreditálásának előkészítése, majd két képcsőben, következő évre átnyúlóan a rendszer akkreditálása.

A NATO TITKOS minősítésű adatkezelést tartalmazó tűzvezetési központok és harcoló MISTRAL és SZURN alegységek vezetését kellett megoldani NATO BIZALMAS minősítési szintű rádióhálók kialakításával, illetve a mobil komplexumok információvédelmének teljes körű biztosításával.

Az MH-nál ez volt az az első kialakított és a Nemzeti Biztonsági Felügyelet által jóváhagyott megoldás, ami biztosította a több tucat harc és gépjárműből álló bonyolult rendszer hadműveleti követelmények szerinti rugalmas szervezését, átrendezését, illetve a harci technika és a minősített adatkezelés miatt szükséges tábori elemekből álló beléptetési és felügyeleti rendszert.

2009-ben kétéves előkészítés, nagyszámú egyeztetés és kodifikálás után megtörtént *a honvédelmi tárca információ biztonsági politikájának HM utasítás formájában történő kiadása*. A szabályozó kiadását egy 2005-ös Állami Számvevőszék által végrehajtott ellenőrzés és javaslattétel váltotta ki. A javaslattétel szakmai sajátossága, hogy *abban az időben jogszabály nem határozott meg ilyen tartalmú szabályozó kiadására vonatkozó követelményt,* melynek következménye, hogy a formai és tartalmi elemekre volt közigazgatási követelmény.

A kidolgozás több alkalommal irányt váltott, mert a szervezeti változások, felelősségi körök megosztása hatással volt a szabályozó szakmai tartalmára. A szabályozó végül nem csak elektronikus információvédelmi, hanem általános információvédelmi szakterületi szabályozóvá érett, és meghatározta az általános irányelveket, szervezeti keretrendszert, szabályozási kereteket és a fizikai-, személyi-, dokumentumbiztonsági és elektronikus információbiztonsági általános követelményeket.

Az ügy kapcsán *szakmatörténeti érdekesség, hogy lényegesen később, 2013-ban megjelent a biztonságpolitika kiadására vonatkozó, jogszabályban meghatározott követelmény, de a formai és tartalmi kérdések elrendelése ennél a közigazgatási lépésnél sem történt meg*.[1]

A 2009-es év kihívása volt a NATO Nehéz Légiszállító Ezred – mint NATO feladatokat ellátó nemzetközi szervezet – működéséhez szükséges híradó-informatikai és információvédelmi szakmai támogatás biztosítása Pápán. A nemzetközi szervezet működéséhez szükséges kommunikációs képességek, illetve általánosságban a működés ezer szálon kötődik a magyar katonai repülőtérhez, így a távközlési kapcsolódási pontok kialakítása, a két szervezet közötti együttműködési megállapodás megfogalmazása, illetve a NATO minősített elektronikus adatokat kezelő híradó-informatikai rendszer NATO Biztonsági Hivatal által végrehajtott akkreditálásának közvetlen előkészítése érdekes, egyedi szakmai teljesítmény volt az összes résztvevő részére – beleértve a feladatba bevont Nemzeti Biztonsági Felügyeletet is.

A 2009-es év másik nemzetközi kihívása *a magyar katonai bázison szervezett NATO Egészségügyi Kiválósági Központ kialakításához köthetően a nyílt és a minősített elektronikus*

[1] A jogszabály 2015-ös felülvizsgálata a követelményt megszüntette, így a cikk írásának időszakában ismételten nincs kormányzati követelmény a szakmai politika kiadására.

adatokat kezelő NATO TITKOS híradó-informatikai rendszer létrehozása, a hatósági akkreditálás előkészítése és lebonyolítása. A helyzet érdekessége, hogy a NATO Biztonsági Hivatal a magyar fenntartói felelősség (host nation) alapján a NATO rendszer akkreditálási feladatát delegálta a Nemzeti Biztonsági Felügyelethez. Az üzemeltetési és a védelmi rendszabályok NATO szervezet által történő ellenőrzése egy évvel később megtörtént és az akkreditálást elismerő véleménnyel hitelesítette.

A haderőt érintő változások miatt a Központot 2014-ben költöztetni kellett az MH Honvédkórház telephelyére.

2010

2010-ben újabb átszervezési feladat következett. A HM Informatikai és Információvédelmi Főosztálynál *az általános elektronikus információvédelmi és a rejtjelző szakterület önálló osztályokra vált*. 2010. 05. 01-től megalakult az önálló Központi Rejtjel Felügyeleti és NATO/NYEU Központi Rejtjelelosztó Osztály valamint a Központi Rendszerbiztonság Felügyeleti Osztály, az MH Központi Rejtjelfelügyelet vezetői feladatot a csoportfőnök látta el.

A 2010-es évben megjelent a minősített elektronikus információvédelemre vonatkozó első olyan kormányrendelet [1], ami a nemzeti, NATO, EU és egyéb más, két és többoldalú nemzetközi szerződésen alapuló *minősített elektronikus adatkezelés egységes szabályozását*, az 1994-es rejtjelzésre vonatkozó jogszabály kiváltását [2] és a rejtjelzés elektronikus információvédelemi szakterülethez történő közelítését célozta. A jogszabályban meghatározott követelmény alapozta meg a két központi felügyelet megalakulását. További hiánypótló újdonság, hogy *az NDA-ra vonatkozó, alapvető követelmények meghatározása a NATO csatlakozás óta jogszabályban ekkor történt meg először.*

Az év további jellegzetessége a NATO magyarországi TITKOS minősítési szintű adatkezelésre feljogosított híradó-informatikai rendszer (WAN); közismert nevén NIAR fejlesztése volt.

2010 év az elektronikus információvédelem (benne kibervédelem) területén nemzetközi eredményt is hozott. Több mint két éves nemzetközi egyeztetés, előkészítés és itthoni tervezés-szervezés lezárásaként 2010 júliusában úgynevezett „szponzor nemzet" megnevezéssel teljes jogú tagjaivá váltunk a tallini székhelyű NATO Cooperative Cyber Defence Center of Excellence-nek (NATO Kibervédelmi Kiválósági Központ; CCD COE, mely félreérthető fordítás alatt tartalmilag kutatás-fejlesztési oktatási és tudásközpontot kell értelmezni). A képzés és gyakorlat területű osztályra delegált szaktiszt hazánkban elsőként töltött be e területű katonai beosztást.

A 2010-es évben a biztonságtudatosság és tudományos tevékenység területén is új eredmény született. Az akkori Zrínyi Miklós Nemzetvédelmi Egyetem, Híradó Tanszék és a Csoportfőnökség Elektronikus Információvédelmi Osztály közösen *megszervezte az első Katonai Elektronikus Információvédelmi Konferenciát*. Az azóta minden évben megrendezett szponzoroktól és egyéb külső cégektől függetlenül szervezett konferencia célja, hogy magyar – esetenként meghívott külföldi – *katonák kötetlenül beszélhessenek egymással az elektronikus információvédelem aktuális kérdéseiről, a kihívásokról, tapasztalatokról illetve a jövőt célzó megoldásokról, kapjanak lehetőséget a konzultációra ezen a fórumon is*. A konferencia fő védnöke hagyományosan a Csoportfőnök.

A 2011. évben szoros határidővel kiadott hadműveleti követelmény alapján a missziós tűzszerészbiztosítás támogatás érdekében ki kellett alakítani és missziós területre ki kellett juttatni két COUGAR típusú páncélozott járműből kialakított speciális komplexumot, melyek

egyik legfontosabb információs eleme a NATO TITKOS helyi elektronikus adatkezelést biztosító munkahelyek kialakítása és akkreditálása volt.

A fantáziadúsan elnevezett Afganisztáni Védelmi Ajánlások Tűzszerész Alrendszere (AVATAR) rendszer feladata a tűzszerész képesség és az együttműködők sikeres együttműködésének, kapcsolattartásának biztosítása, az előzetes tervezéshez, értékeléshez és jelentés készítéséhez szükséges támogatás, valamint az eljárásrend elektronikus formában történő helyszíni biztosítása a tűzszerész mentesítéshez.

A kompromittáló kisugárzás elleni védelmi szakfeladatokon kívül megoldandó feladatként jelentkezett a missziós területen lévő eszköz szoftver frissítéseinek biztosítása, illetve a jogszabályban nem részletezett adattárolásra vonatkozó védelem rejtjelzéssel történő megvalósítása, beleértve a külföldi gyártású rejtjelző megoldások rendszeresítésével és akkreditálásával kapcsolatos összes speciális problémát.

2011-2015

2011-ben az utolsó átszervezési feladat során HM Informatikai és Információvédelmi Főosztály átalakulásával egyrészt megtörtént *az általános elektronikus információvédelmi és a rejtjelző szakterületek szakmai irányítási funkcióinak egységes szervezetbe történő egyesítése*, másrészt a híradó és informatikai szakmai felelősségek befogadásával kialakult a híradó-informatikai és információvédelmi szakmai feladatokért felelős HM szerv, a HVK Híradó, Informatikai és Információvédelmi Csoportfőnökség. Ennél az átszervezési feladatnál az NDA funkció a HVK-tól 2011. februári határidővel átkerült az MH Támogató Dandárhoz, HVK Támogató Osztály, NATO/NYEU Központi Rejtjelelosztó néven.

Az integrált elektronikus információvédelmi szakmai felügyeleti feladatokért az Elektronikus Információvédelmi Osztály a felelős, az MH Központi Rejtjelfelügyelet vezetői, az MH Központi Rendszerbiztonsági Felügyelet vezetői feladatokat az osztályvezető látja el.

Az időszak jellegzetes szakmatörténeti eredménye, hogy 2011-ben *megtörtént az utolsó rendszerben levő orosz rejtjelző eszköz kivonása* a Nemzeti Biztonsági Felügyelet szakmai támogatásával és segítségével, így a szükséges megsemmisítési feladatok és jelentési kötelezettségek után kijelenthető volt, hogy a rejtjelzés területén is lezárult egy speciális korszak. Az évekig tartó honvédségi szervezési, technikai, ellenőrzési és adminisztratív feladatok mellett markánsan meg kell említeni az Nemzeti Biztonsági Felügyelet által végzett nemzetközi egyeztetéseket is, amelyek megoldották az utolsó problémákat is.

A 2011-es év elektronikus információvédelmi szempontból jelentős erőfeszítéseket igényelt az EU elnökség ellátásához köthetően. EU BIZALMAS minősítésű adatkezelésre feljogosított híradó-informatikai rendszert kellett kialakítani és akkreditáltatni, a Védett Külügyi Hálózathoz kiegészítő elemeket kellett telepíteni, nagyszámú felhasználói munkaállomást kellett csatlakoztatni az akkori Külügyminisztérium által üzemeltetett EU KORLÁTOZOTT TERJESZTÉSŰ elektronikus adatkezelésre feljogosított hálózathoz, illetve megnövekedett forgalom biztosítása érdekében jelentősen meg kellett erősíteni az MH Központi Levelező Szolgáltatás infrastruktúráját.

2012-ben általános elektronikus információvédelmi területen megtörtént a Magyar Honvédség szervezeteire kötelezően érvényes általános elektronikus információbiztonsági követelmény meghatározása, HM utasítás formájában. [3] Ezt követte az MH Kormányzati Célú Elkülönült Hírközlő Hálózatra kiadott hálózatgazdai specifikáció, szakutasítás formájában. [4] A szabályozási lépés az általános elektronikus információvédelmi rendszabályok nemzetközi szabvány (MSZ/ISO 2700x) alapján történő rendezését, az eddigi, informatikai szemléletű „Számítástechnikai Védelmi Szabályzat” [5] felszámolását jelentette. Az egyeztetések, továbbképzések, illetve a végrehajtók fogékonyságának köszönhetően a

honvédelmi szervezeteknél – kis kivétellel – zökkenőmentesen megtörtént a szabáylozók korszerűsítése. A feladat részét képezi az a felismerés is, hogy a több helyőrségben települő katonai szervezeteknél (jellemzően légierő – radar alegység üzemeltetők, MH KCEHH területi üzemeltetők) nem elégséges a törzsben elkészíteni egy szabályzót, hanem a végrehajtó alegységeknél kell helyszíni sajátosság szerint kialakítani az eljárásokat, szabályokat. Az az időszakra visszatekintve megállapítható, hogy a két említett katonai szervezet vezetése, szakmai irányítása és a végrehajtók sikeresen oldotta meg a feladatot.

A következő fontosabb szabályozás lépésként megtörtént a minősített adatokat kezelő híradó-informatikai rendszerekre vonatkozó Üzemeltetés Biztonsági Szabályzat, illetve a tartalmi ellenőrzésére szolgáló ellenőrzési kérdőív kiadása, szakutasítások formájában. [6][7] Ez a lépés a minősített elektronikus adatokat kezelő híradó-informatikai rendszerek üzemeltetői és biztonsági állománya számára nehézséget nem okoztak, az évek során már gyakorlatban finomított, terminológiát tekintve magyarosított NATO követelmény rendszerbe állítását jelentette.

2012. a NATO Biztonsági Beruházási Programon belül a NATO magyarországi légi vezetési és irányítási rendszer (NATO Air Command and Control System; ACCS) gyakorlati kialakításának induló éve. Kezdeti feladatként megtörtént a légivezetési funkciók ideiglenes átköltöztetése Kecskemétre annak érdekében, hogy a leendő beruházások helyszínei felszabadíthatók legyenek Veszprémben.

A többlépéses művelet – benne a visszaköltözés – a Nemzeti Biztonsági Felügyelet helyi ellenőrzése és hatósági engedélyezése nyomán zajlott, illetve ezt követően a napjainkban is folytatólagosan zajlik a korszerű légi C2 kialakítás, benne különböző, változatos funkcionális tesztekkel, szoros együttműködésben a projektet irányító NATO szervezettel, a kivitelezőkkel.

A művelet érdekessége, hogy a NATO légivezetési és irányítási akkreditációs testületben (ACCS Security Accreditation Board; SAB) *a magyar képviseleti feladatokat a Csoportfőnökség elektronikus információvédelmi szakterülete látja el*.

Az ACCS képesség kialakítása a funkcionális és biztonsági tesztek sorozatával napjainkban is folytatódik, így 2015-ben részfeladat NATO *eltérő minősítésű elektronikus adatokat kezelő híradó-informatikai rendszerek összekapcsolási problémáinak megoldása*. A fejlesztési programban résztvevő nemzeteknél erre megoldás még nincs, nemzeti megoldás sem ismeretes, így a NATO támogatással kialakítandó technikai megoldás tesztelésével, biztonsági vizsgálatával és tanúsításával, majd a nemzeti alkalmazásba vétellel kapcsolatos feladatok a Csoportfőnökség és a Nemzeti Biztonsági Felügyelet szoros együttműködése által irányított úttörő feladatként azonosíthatók.

2012-ben hosszas előkészítés befejezéseként megtörtént az MH Védett Vezetési Rendszer (MH VVIR) speciális híradó-informatikai rendszer központi kiszolgáló egységének és első munkaállomásainak akkreditálása a Nemzeti Biztonsági Felügyelet által, így – a meglévő kihívások és további megoldandó technikai és szabályozási feladat mellett – ez tekinthető a nemzeti TITKOS minősítésű korszerű katonai hálózati alapú elektronikus adatkezelésre irányuló erőfeszítés első eredményének.

2012-ben a NATO Kibervédelmi Koncepcióval, a végrehajtást célzó dokumentumokkal, és a nemzetközi irányzatokkal összhangban megkezdődött a magyar katonai kibervédelmi helyzetelemzés és stratégiai szintű célok és feladatok azonosítása. Több mint egy éves kidolgozás egyeztetés, köröztetés és kodifikálás után 2013-ban megszületett az eredmény, és *megtörtént az MH Kibervédelmi Szakmai Koncepció kiadása*, HM utasítás formájában. A lépcsőzetes formában elgondolt képességfejlesztés szakterületi célokra tagolja az MH Kormányzati Célú Elkülönült Hírközlő Hálózat biztonsági szintjének emeléséhez szükséges szakfeladatokat, *kiemelten kezelve a hálózati szintű incidenskezeléshez szükséges korszerű, automatizált megoldás kialakítását*. [8]

2012-ben a Zászlóalj Harccsoport kialakításához köthetően megtörtént az első elektronikus minősített harcászati rádiórendszer Nemzeti Biztonsági Felügyelet által történő akkreditálása NATO TITKOS és nemzeti BIZALMAS, egyes viszonylatokra nemzeti TITKOS minősítési szintű adatkezelésre engedélyezve.

A több katonai alakulat szervezetéből kialakítható ideiglenes kötelék többfunkciós feladatokra tervezhető, így *első lépésben ki kellett alakítani a logikai megközelítést, módszertant, ami az akkreditáló hatóság számára bemutatja a működési sajátosságot, ugyanakkor támogatja az esetleges megalakítás elrendelése során azt a rugalmasságot, ami nem köti meg a Honvéd Vezérkar főnök kezét az adott helyzetre „testre szabható" kötelék kialakításában*. A műveleti tervezés feszített tempójába a Nemzeti Biztonsági Felügyelethez történő adminisztratív kérdőívek benyújtására akkreditálás igénylésére nyilvánvalóan nincs lehetőség. A légvédelmi alegységek rugalmas kötelékszervezést biztosító szervezési elveire építve egy modul rendszerűen kialakítható harcászati rádióhálókból álló rendszert hagyott jóvá az akkreditáló hatóság. A művelet fontosságát jelzi, hogy az engedélyeztetési eljárás szervezési szakaszában a Nemzeti Biztonsági Felügyelet elnöke a Hajdúhadházi gyakorlóterületen tekintett meg szakasz szintű műveleteket tartalmazó gyakorlatot, az információs igények pontos tisztázása érdekében.

A helyi gyakorlati szemléltetés, illetve a helyzet megoldásához szükséges híradó és rejtjelző sajátosságok ismertetésére azért volt szükség, mert a mozgó harcászati környezet igényeihez igazodó rádióhíradásra vonatkozó követelményeket a keretrendszerű jogszabályok talaján kellett bemutatni. Azonosítani kellett azokat a pontokat, ami az üzemeltetés, a helyi biztonsági menedzsment, illetve katonai rejtjelző kulcsgyártás és ellátási rendszerben megadják a szükséges biztonsági garanciákat a hatósági eljárás lefolytathatósága érdekében.

2012-ben szervezeti átalakulás – légierő szervezeti kultúra fejlődési lépcsőváltás – következtében Veszprém helyőrségben más katonai szervezetek részeiből *új szervezetként kialakult az MH Légi Vezetési Központ*. A katonai vonatkozások mellett elektronikus információvédelem szempontjából jelentős feladatot kellett megoldani. A korábbi szervezeti kereteket át kellett szervezni, és a légi vezetési és irányítási rendszerek üzemeltetési és biztonsági feladatok rendjét új alapokra kellett helyezni. *Ki kellett alakítani egy olyan modellt, ahol a híradó-informatikai üzemeltetési feladatokat – beleértve a rejtjelző szolgáltatások biztosítását – és a biztonságfelügyeleti feladatokat két, napi élet szempontjából elszakíthatatlan katonai szervezet látja el úgy, hogy a jogszabályokban és NATO követelményekben megfogalmazott együttműködési és biztonsági szempontból kötelező elkülönítési követelmények megvalósuljanak.*

A szervezési lépéssel megkezdődött a légi vezetés és irányítás szempontjából lényeges lépés, az MH Légivezetési és Irányítási Rendszer (MH LIR) kialakítása. Ennek lényege a korábban külön szabályozott, eltérő érvényességi idejű rendszerengedélyekkel rendelkező elektronikus minősített adatokat kezelő *híradó-informatikai rendszerek egységesítése, funkcionális alrendszerek azonosítása és hatóság által történő elfogadása*.

A 2013-as év a kezdete az MH központi elektronikus információvédelmi szakmai irányító szerv és a kijelölt honvédelmi szervezetek csatlakozásának a NATO (Cyber Colalition) és a NATO Kibervédelmi Kiválósági Központ kibervédelmi gyakorlatsorozatához (Locked Shileds) az évben megfigyelő státusszal majd 2014-től teljes jogú szereplőként.

A folyamat előzmények nélküli, a HM Védelmi Hivatal, az MH kijelölt szervezeti elemek és a Katonai Nemzetbiztonsági Szolgálat képviselői a vezetési és a technikai jellegű gyakorlásokon a meglévő képességekre támaszkodva – a kirakatpolitikát elkerülve –, közösen kezdik megismerni a nemzetközi szakmai kihívásokat.

Az évben megkezdődött a NATO éves válságkezelési gyakorlatokba (Crisis Management Excercise; CMX) a kibervédelmi incidensek megjelenítése és a szövetségi szintű megoldások

gyakoroltatása, melyben a HM Védelmi Hivatal szervezésében kezdetektől fogva részt vesz az elektronikus információvédelmi szakterület.

2013-ban az elektronikus információvédelemre vonatkozó követelmények végrehajtásának egyik feladataként *egyéves kidolgozás, egyeztetés, a Nemzeti Biztonsági Felügyelettel történő jóváhagyás majd kodifikálás után az MH-nál történő rejtjeltevékenység szabályozása megtörtént az MH Rejtjelszabályzat kiadása*, HM utasítás mellékleteként. [9]

A szabályzat a jogszabályi követelmények végrehajtása mellett a vonatkozó NATO szabályozással is összehangolt, ezzel lezárult a magyar katonai rejtjelzés nemzeti és NATO területekre szabdalt korszaka, a szükséges elkülönítésre vonatkozó ésszerű rendszabályok kialakításával együtt.

A szabályzatban nem lehetett minden kérdést pontosan kidolgozni és meghatározni, így szakmai követelményként megjelent, hogy a részterületként azonosítható kérdéseket szakutasítás formájában kell meghatározni. Emiatt kialakult a rejtjelzésre vonatkozó terminológiai, a rejtjelző szakiratkezelési, a rejtjeltevékenységre vonatkozó ellenőrzési és a biztonsági események jelentésére vonatkozó szakutasítások rendje 2014-ben.

A 2013-as évben a Nemzeti Biztonsági Felügyelet kezdeményezésére megkezdődött a Középeurópai Kiberbiztonsági Platform (Central Europian Cyber Security Platform) kialakítása. A V4 országok és Ausztriai szakmai közösségét mozgósító együttműködés feladata a kibervédelmi tevékenység központi összehangolása, illetve a nemzetközi fórumokon való közös fellépés és érdekérvényesítés lehetőségeinek azonosítása.

Az együttműködés egyik gyakorlati eredménye a Platform tagállamai által végrehajtott nemzetközi kibervédelmi gyakorlat, melynek tervezése 2013-ban, végrehajtása 2014-ben történt. A Platformon belül megkezdődött a katonai együttműködő partnerek azonosítása, a közös érdekek azonosítása, de ennek ellenére a *2014-es gyakorlaton egyedül magyar oldalról történt meg katonai képesség gyakoroltatása*.

Féléves előkészület után 2013 őszén közös gyakorlati programmal megkezdődött a magyar – amerikai kétoldalú katonai kibervédelmi szakmai együttműködés. Az Ohiói Nemzeti Gárda valamint a Csoportfőnökség elektronikus információvédelmi, híradó és informatikai képviselői – megerősítve a központi üzemeltetési feladatokat ellátó katonai szervezet képviselőivel – szakmai találkozón megkezdték azonosítani szakmai eljárásaikat, az általános követelményeket, hogy a közös érdekek mentén ki lehessen jelölni az új szakmai értékek előállítását biztosító együttműködési formát és célokat. A kihívást az akkori jogszabályi környezet, a NATO elektronikus információ biztonsági követelmények, illetve az amerikai szabványok és magyar katonai védelmi rendszabályok összehangolhatósága jelentette. A teljesen eltérően strukturált szakmai szemlélet, az európai és az amerikai szabványok eltérőségének kiismerése, a felismert értékek integrálásának lehetősége a nemzeti katonai gondolkodásba biztató stratégiai szintű és további, erre alapozott technikai lehetőséget, új megoldásokat sejtet. Az egyeztetés 2014-ben ennek megfelelően már szűkített témakörökben folytatódott.

A 2014-es év elektronikus információvédelmi szakterületű, technikai jellegű kihívása jelentősen légierő vonatkozású. A már korábban üzemelő és akkreditált NATO BIZALMAS minősített elektronikus radaradatokat kezelő híradó-informatikai rendszerhez csatlakozó 3D-s radarok az évben hadrendbe álltak. Ezzel párhuzamosan *a NATO illetékes szervei döntöttek a minősítési szint csökkentéséről*.

Feldolgozható előzmények és szakmai tapasztalatok nélkül *az üzemeltető katonai szervezet, az MH Összhaderőnemi Parancsnokság és a Csoportfőnökség elektronikus információvédelmi szakmai irányításért felelős osztálya megtervezte és végrehajtotta a minősítési szint változásával kapcsolatos feladatokat*, felterjesztették a szükséges kérelmet a Nemzeti Biztonsági Felügyelethez, majd megtörtént a szükséges változások átvezetése, mely során

sikerült azonosítani néhány olyan feladatot, melynek megoldását a jogszabályok soros felülvizsgálata során majd célszerű lesz részletesen elemezni.

A 2014-es évben megtörtént a NATO Federációs Missziós Hálózat (Federated Mission Network; FMN) koncepció indítása. A híradó-informatikai rendszer struktúrájának kialakítása, az üzemeltetési rend kialakítása és a szolgáltatások biztosítása, a szolgáltatások igénybevételének szabványosítása alapján kialakítható egy általánosítható modell, ami a jövőbeli katonai műveletek híradó-informatikai kérdéseit szabályozza. Elektronikus információvédelmi szempontból a koncepció kidolgozása, majd ezek alapján egy használható modell kialakítása eddig nem tapasztalható nehézségek megoldását sürgeti.

A NATO erők vezette műveletek mellett – ahol nem lehet kérdés a minősített elektronikus adatkezelésre vonatkozó eljárásrend – a kidolgozók számára nem okozhatnak nehézséget, de azokban az esetekben ahol egy – nem biztos, hogy NATO – nemzet veszi át a művelet vezetését, már komoly szakmai kihívásokat kell kezelni.

Ki kell alakítani az adatkezeléssel kapcsolatos felelősség és információ menedzsment elgondolást, a biztonsági menedzsment megoldási lehetőséget, meg kell oldani a rejtjelző és biztonsági mechanizmusok vizsgálatára, értékelésére és hatósági engedélyezésére vonatkozó eljárásokat, kezelni kell a kockázatelemzési, biztonságfelügyeleti kérdéseket és az incidenskezelésre vonatkozó specifikus- és egyben minden nemzet számára bizalmas tartalmúnak tekintett eljárásokat. Ebből a szempontból megvilágítva érthető, hogy az elektronikus minősített adatkezelés kérdései, a hálózatokkal kapcsolatos szakmai kérdések feldolgozása, illetve a nemzeti célok kialakítása nem tekinthető egyszerű esetnek.

2014-ben szakmai előzmények nélküli katonai képesség aktivizálása történt *a szlovén légtérvédelmi feladatok megkezdésével,* ami speciális szabályozási lépések, hatósági egyeztetések és engedélyezés alapján lehetővé tette a készenléti harcirepülők hadműveleti igényeknek megfelelő alkalmazását és külföldi légtérbe történő átirányítását az elektronikus minősített adatkezelést biztosító számítógépekkel, rejtjelző eszközökkel a fedélzeten, a jogszabályban meghatározott eseti engedélyezés nélkül.

2014-ben megtörtént a korábban már említett MH Informatikai Szabályzat (Ált/210) kiváltása az új Informatikai Szabályzattal, HM utasítás formájában. Informatikai területű szakmai érdekesség, hogy a kidolgozó munkacsoport az MH központi üzemeltető katonai szervezet javaslatát támogatva igényt tartott arra, hogy az informatikai szakterülettől függetlenül kialakult – fentiekben bemutatott – szabályozási rend fenntartása mellett az Informatiaki Szabályzat is tartalmazzon információbiztonsági követelményeket. Emiatt született a szabályzat nyolcadik fejezete, ahol a híradó-informatikai rendszerek biztonsága érdekében szükséges fizikai-, személyi-, adminisztratív és elektronikus információbiztonsági követelmények megfogalmazása történt. [10]

2015-ben a Nemzeti Biztonsági Felügyelet felkérése alapján megtörtént *a NATO minősített elektronikus adatokat kezelő híradó-informatikai rendszerek akkreditálási eljárására vonatkozó követelmények rögzítése és hatósági jóváhagyása*. Az MH Biztonsági Akkreditálási Eljárás dokumentum gyakorlati megközelítésben rögzíti az alkalmazó honvédelmi szervezetek, a szakmai irányításért felelős szervezet és a Nemzeti Biztonsági Felügyelet akkreditálás érdekében történő feladatait, az együttműködés rendjét.

A 2015-ös év első félévének kihívása a *Balti Légvédelmi Készenlét feladatra történő felkészülés*, a kitelepüléssel, valamint a litván katonai repülőtérről történő munkavégzés vezetési és irányítási feltételeinek biztosítása. Ki kell alakítani és üzemeltetni kell a légi feladattervezéshez és légi irányításhoz szükséges helyi híradó-informatikai szolgáltatásokat, valamint biztosítani kell a minősített elektronikus adatcsere lehetőségét az anyarepülőtér és a svéd üzemeltető telephelye felé, a Nemzeti Biztonsági Felügyelet által akkreditált védelmi rendszabályokkal.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Az utolsó tíz év fontosabb történéseinek áttekintése szemléletesen mutatja az elektronikus információvédelmi szakmai feladatok összetettségét.

A katonai sajátosságokhoz igazodó, heterogénnek tekinthető híradó-informatikai szolgáltatások fejlődése jól felismerhető, azonosítható a központosításra, egységesítésre irányuló törekvés. Ezen a tendencián belül körvonalazhatók az elektronikus információvédelem feladatai, szintén a „hálózati" gondolkodásra koncentrálva.

A nemzeti és szövetségi hadműveleti követelmények alapján kialakuló hálózati kiszolgálás egyértelműen felváltja a „pont – pont" típusú kapcsolattartást, mely megállapítás a rejtjelzés területén is egyértelműen jelentkezik.

Az említett jelenségek szervezeti hatásokat is kifejtenek. A hálózatok egységes szintű védelmi igénye egyaránt vonatkozik végpontra, központi kiszolgáló elemre és hálózati utakra, ami helyszínek és szervezetek, illetve üzemeltető és biztonságért felelős közösségek központilag vezérelt együttműködését követeli meg.

Az elektronikus információbiztonsági követelmények NATO szabályozókban és jogszabályokban rögzítettek, kötelező hatósági eljárásokkal hitelesítettek, ami erős szakmai vertikális irányú kapcsolattartást igényel.

A szervezeti változások az elektronikus információvédelmi terület szakmai irányító szervét látható módon érintették. A bemutatott időszakban azonosítható az általános elektronikus információvédelem és a rejtjelzés szakmai elkülönülése, de az utolsó évek szervezeti felépítése már az integrációt mutatja, ami remélhetőleg működőképes modell marad az MH szervezeti rendjében.

Köszönet a nyugállományú és a szolgálatot teljesítő kollégáknak, barátoknak, akik munkájukkal az említett eredményeket elérték, a fejlődési lépéseket megtették és megalapozták a következő fejlődési lépcsőfokokat!

Köszönet mindenkinek, aki segítséget nyújtott a fontosabb, publikálható események összegyűjtésében, kiegészítésében.

A következő tíz év szakmai feladatai vélhetően hasonlóan mozgalmasak lesznek, melyhez sok sikert a szakterületet művelőknek, oktatóknak!

Felhasznált irodalom

[1] 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól

[2] 43/1994. (III. 29.) Korm. r. a rejtjeltevékenységről (hatályon kívül)

[3] 3/2012. (I. 13.) HM utasítás a honvédelmi tárca általános elektronikus információbiztonsági követelményeinek meghatározásáról és a védelmi rendszabályok pontosításáról

[4] A Honvéd Vezérkar Híradó, Informatikai és Információvédelmi Csoportfőnökség csoportfőnökének 20/2013. (HK 12.) HVK HIICSF szakutasítása a Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózatának rendszer-specifikus elektronikus biztonsági követelményeinek meghatározásáról

[5] A Magyar Honvédség Informatikai Szabályzata, Ált/210, 1993, 199. p.

[6] A Honvéd Vezérkar híradó, informatikai és információvédelmi csoportfőnökének 9/2012. (HK 14.) HIICSF szakutasítása a Minősített Elektronikus Adatkezelő Rendszer Üzemeltetés Biztonsági Szabályzatára vonatkozó általános követelményekről

[7] A Honvéd Vezérkar híradó, informatikai és információvédelmi csoportfőnökének 10/2012. (HK 14.) HIICSF szakutasítása a Minősített Elektronikus Adatkezelő Rendszer ellenőrzésére vonatkozó általános követelményekről

[8] 60/2013. (IX. 30.) HM utasítás a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról, 6. fejezet

[9] 75/2013. (XII. 5.) HM utasítás a Magyar Honvédség Rejtjelszabályzat kiadásáról

[10] 39/2014. (05. 30.) HM utasítás a Magyar Honvédség Informatikai Szabályzatának kiadásáról, 1. sz. melléklet, 8. 4. fejezet.