Vasvári Géza alezredes:

A KATONAI SZERVEZETEK ELEKTRONIKUS INFORMÁCIÓVÉDELMI KÉPESSÉGEINEK FEJLESZTÉSÉVEL KAPCSOLATOS FELADATOK

ÖSSZEFOGLALÓ: *A vezetés és irányítás feladatait hatékonyan támogató híradó-informatikai rendszerek nagyfokú fejlődésen mentek át az elmúlt időszakban. A digitalizáció és az infokommunikációs rendszerek töretlen fejlődése, az ezekkel járó kockázatok kialakulása az elektronikus információvédelem folyamatos fejlődését követeli meg. A tanulmány célja a katonai szervezetek elektronikus információvédelmi képességeinek kialakításával kapcsolatos feladatok összetettségének érzékeltetése.*

KULCSSZAVAK: *információbiztonság, elektronikus információbiztonság, biztonsági menedzsment, információbiztonsági követelmények*

BEVEZETÉS

Magyarország 1999. évi NATO- és 2004. évi EU-csatlakozását közvetlenül megelőzően, illetve azzal egy időben alapvető követelményként jelentkezett – az új szövetségesekkel való hatékony együttműködés, az úgynevezett interoperabilitás teljesülése érdekében – a Magyar Honvédség vezetés-irányítási és az azt támogató híradó-informatikai rendszereinek felülvizsgálata, kompatibilis eszközök beszerzése, a régi eszközök rendszerből történő fokozatos kivonása, eljárások meghonosítása, létrehozása, megújítása. Mindemellett a 20. század végére a digitalizáció térnyerésével, a számítógépek rendkívüli fejlődésével, az eszközök összekapcsolásával, hálózatba szervezésével soha nem látott távlatok nyíltak az elektronikus adatkezelő rendszerek széles körű alkalmazásában, beleértve a katonai célú felhasználást is.

Az elektronikus adatkezelő rendszerek és eszközök nagyfokú fejlődése és felhasználása, továbbá az ezek működésére információbiztonsági szempontból ható tényezők és cselekmények miatt kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának szavatolása újabb és újabb kihívásokat jelent. Ez jó alkalmat ad a katonai szervezetek elektronikus információvédelmi képességeinek fejlesztésével kapcsolatos feladatok publikálható információkra szorítkozó, önálló írásban való összefoglalásához.

A KATONAI SZERVEZETEK ELEKTRONIKUS INFORMÁCIÓVÉDELMI KÉPESSÉGEINEK FEJLESZTÉSÉRE HATÓ TÉNYEZŐK AZ ELMÚLT IDŐSZAKBAN

Magyarország NATO-csatlakozását megelőző időszakban az információvédelmet megtestesítő nemzeti jogszabályok kifejezetten a minősített adatok, azon belül is leginkább a papíralapú adathordozók védelmét írták elő. Az akkor hatályban lévő, államtitokról és

a szolgálati titokról szóló törvény[1] – ahogy a nevéből is kiderül – két titokfajtát állapított meg. Az egyik a törvény mellékletében meghatározott, az úgynevezett államtitok körébe tartozó adat, a másik a törvény által feladat- és hatáskörében minősítésre felhatalmazott szervezeti vezető által meghatározott adatfajták körébe, az úgynevezett szolgálati titokkörbe tartozó adat volt. A külföldi minősített adatok vonatkozásában az 1995-ös jogszabály rendkívül szűkszavúra sikeredett. A két nemzeti titokfajtát megkülönböztető jogszabály – bár napjainkra már hatályát vesztette – közvetetten mindmáig érezteti kedvezőtlen hatását a külföldi minősített elektronikus adatok feldolgozásához kapcsolódó információvédelmi szakfeladatok végrehajtása során.

Kifejezetten elektronikus információvédelmet leíró nemzeti jogszabály ebben az időszakban nem létezett. A rejtjeltevékenységről szóló kormányrendelet[2] csak a minősített adat kezelésének rendjéről szóló kormányrendeletben[3] előírt rejtjelzési kötelezettség alá eső államtitok és szolgálati titok védelme érdekében rendelt el feladatokat.

A katonai szervezeteknél a híradórendszerek, átviteli utak, illetve csatornák rejtjelző eszközökkel való „zárását", a rejtjeltevékenységet – az akkori értelmezés szerinti elektronikus információvédelmet – a 002/1996. MHPK intézkedés 1. sz. melléklete[4] alapján hajtotta végre a szakállomány. A rejtjeltevékenység mostanra az elektronikus információvédelem részévé vált. A katonai szervezeteknél elvétve alkalmazott számítástechnikai eszközök működtetését – a fenti jogszabályokat időben megelőző Magyar Honvédség Informatikai Szabályzat (Ált/210) alapján, a kezelt adatok minősítési szintjének és a szervezeti sajátosságoknak megfelelő, az adott szervezet vezetője által kiadott számítástechnikai védelmi szabályzat[5] alapján hajtották végre. A Magyar Honvédség felső szintű vezetése és a középszintű parancsnokságok szintjén alkalmaztak – főleg jelentések továbbítására kifejlesztett – számítástechnikai eszközökön futó célalkalmazásokat; az általuk előállított adathalmazt mágneses adathordozón – megfelelő informatikai hálózat hiányában – futárral továbbították. A katonai szervezeteknél a minősített iratokat – jellemzően – leírónapló alkalmazásával, a legtöbbször írógéppel készítették, és sokszorosítással állították elő a kívánt példányszámot. Akkreditált számítógépről, hálózatról mit sem lehetett sejteni ebben az időben.

A teljes jogú NATO-tagságunkat megelőzően a katonai szervezeteknél jobbára orosz, illetve a korábbi Varsói Szerződés tagországai által gyártott és alkalmazott – csakúgy, mint a többi haditechnikai eszköz vonatkozásában – többnyire elavultnak számító, többségében analóg híradó eszközök voltak rendszerben. A kevés kivételt a hazai védelmi ipar képviselői által a Varsói Szerződés megszűnése után, kizárólag nemzeti felhasználásra fejlesztett, illetve a békepartnerségi programban szövetségesektől átvett eszközök jelentették.

A számítógépek és a hálózatépítési képességek fejlettségi szintje, a digitalizáció előtérbe kerülése, az általa nyerhető előnyök felhasználásának egyre erősödő igénye a katonai vezetési és irányítási folyamatokat hatékonyan támogató, korszerű elektronikus adatkezelő rendszerek kialakítását irányozta elő az 1990-es évek második felében. A fejlesztések szükségszerűségét és gyorsítását támasztotta alá a Magyarország NATO-csatlakozásával létrejövő egyfajta együttműködési kényszer, az ebből adódó feladatok hatékony végrehajtását támogató kommunikációs rendszerek létrehozása.

---

1 1995. évi LXV. (VI. 30.) törvény.
2 43/1994. (III. 29.) Korm. rendelet.
3 79/1995. (VI. 30.) Korm. rendelet.
4 A HM és MH rejtjeltevékenységének szabályai.
5 Ált/210. 199. pont.

A NATO civil struktúrában a Nemzetközi Törzsön (IS[6]) belül, az Egyesített Hírszerzési és Biztonsági Osztály (JISD[7]) részeként működik a NATO Biztonsági Hivatala (NATO Office of Security – NOS), mely felelős a biztonság átfogó koordinálásáért, felügyeletéért és a NATO biztonsági politikája megfelelő végrehajtásáért a Szövetségen belül. A NOS feladatai végrehajtását az illető tagország biztonsági hatóságai – Magyarországon a Nemzeti Biztonsági Felügyelet (NBF) – útján, illetve bevonásával gyakorolja.

A NATO-csatlakozás küszöbén törvényben[8] elrendelt módon hozták létre az NBF-t, az Észak-atlanti Szerződés Szervezete (NATO) és a Nyugat-európai Unió (NYEU) Biztonsági Szabályzatában előírt követelmények érvényesítéséért felelős, önálló feladattal és hatósági jogkörrel rendelkező szervezetként. Az NBF az EU minősített adatok vonatkozásában az Európai Unió Tanácsa által határozatban[9] rögzített, az EU minősített adatok védelmét szolgáló biztonsági szabályok figyelembevételével végzi a hatósági feladatait. A csatlakozáshoz még szükséges – a rejtjeltevékenység vonatkozásában az interoperabilitás egyik alappillérét jelentő – NATO, valamint NYEU Központi Rejtjel Elosztó Hatóság (National Distribution Authority – NDA) funkció ellátására a Magyar Honvédség Híradó és Informatikai Parancsnokság, Főhírközpont, Központi Rejtjelző Nyilvántartó Alosztályt jelölték ki.

A csatlakozás után elektronikus információvédelmi szempontból mérföldkőnek tekinthető a NATO-eszközök felhasználásával, „NATO TITKOS" minősítési szintű adatkezelésre feljogosított híradó-informatikai rendszer (mely NATO Irodaautomatizálási Rendszer [NIAR] néven került be a köztudatba) – az együttműködéshez minimálisan szükséges számú helyszínen történő – telepítése. A NIAR magyarországi rendszerelemeinek biztonságával és üzemeltetésével kapcsolatos felelősséget és feladatokat honvédelmi miniszteri utasításban[10] határozták meg.

A NATO-csatlakozás, a nemzeti kötelezettségvállalásainkból adódó feladatok végrehajtása, a folyamatban lévő haderőreform, a technikai fejlődés és modernizáció az elektronikus információvédelemi szakterület folyamatos fejlődését irányozták elő. Az új kihívások a jogszabályi környezetben is ösztönözték a változásokat. Többek között ezeknek is köszönhető, hogy a 2003-ban hatályba lépett kormányrendeletben külön fejezetben[11] határozták meg az elektronikus biztonsági alapelveket és követelményeket, megteremtve ezáltal az elektronikus információvédelem jogszabályi alapjait, jóllehet csak a külföldi minősítéssel és jelöléssel ellátott adat elektronikus biztonsága vonatkozásában. Ugyanezen rendelet – egyfajta hiánypótlásként – a Honvédelmi Minisztérium felelősségi körébe utalta a Központi NATO, illetve NYEU Rejtjelanyag Elosztó üzemeltetését is.

Az államtitokról és a szolgálati titokról szóló törvényt hatálytalanító, minősített adat védelméről szóló törvény[12] meghozta az áttörést a nemzeti és a külföldi minősített adatok kezelésében lévő aránytalanságok megszüntetéséért vívott harcban. A törvény nemzeti minősített adatok biztonsága vonatkozásában is az NBF-et azonosította felelősként, és négyszintű, káralapú minősítési rendszert vezetett be. A jogszabály nagymértékben könnyítette ezáltal a nemzetközi együttműködések kapcsán megkötésre kerülő – minősített adatok

[6] International Staff.
[7] Joint Intelligence and Security Division.
[8] 1998. évi LXXXV. törvény.
[9] 2013/488/EU tanácsi határozat.
[10] 82/2002. (HK 26.) HM utasítás.
[11] 179/2003. (XI. 5.) Korm. rendelet, IV. Fejezet.
[12] 2009. évi CLV. törvény.

cseréjére és kölcsönös védelmére vonatkozó – kétoldalú biztonsági megállapodásokban az adatfajták minősítési szint szerinti megfeleltetését, a megfelelő információvédelmi eljárások alkalmazását. A törvény végrehajtására kiadott „elektronikus" kormányrendelet[13] a NATO minősített adat elektronikus biztonságával azonos szintre emelte a nemzeti minősített adat elektronikus biztonsági követelményeit, megszüntetve az eddig fennálló hiányosságot. Későbbi jogszabályváltozás némelyest a nemzeti „Bizalmas!" minősítésű elektronikus adat „kárára", de remélhetőleg a nemzetgazdaság előnyére változtatta az eredeti elektronikus biztonsági követelményeket.

A minősített adatkezelő rendszerek fejlődésével párhuzamosan a nem minősített adatok kezelésére alkalmazott rendszerek is jelentős fejlődésen mentek keresztül a NATO-csatlakozás óta eltelt időszakban. Az 1993-ban kiadott Magyar Honvédség Informatikai Szabályzat szerinti „Számítástechnikai Védelmi Szabályzat" megközelítés helyett nemzetközi szabványok (MSZ/ISO 2700x) alapján kidolgozták és 2012-ben kiadták a Magyar Honvédség általános elektronikus információbiztonsági követelményeit meghatározó[14] HM-utasítást. Ezt a szabályzót a Magyar Honvédség szerteágazó feladatrendszeréből adódóan a szükséges működési és együttműködési feladatok szabályozott végrehajtása érdekében – de törvényi felhatalmazást nélkülözve, mert abban az időszakban jogszabályban rögzített követelmény még nem állt rendelkezésre – dolgozták ki.

A mobil eszközökkel történő kommunikáció és adatkezelés biztonsága érdekében kiadták a mobil kommunikációs eszközök használatával kapcsolatos rendszabályok alapelveiről szóló[15] HM-utasítást, mely alapján az illető katonai szervezet vezetője a helyi sajátosságoknak és a végzett tevékenységnek megfelelően belső rendelkezésben szabályozza a mobil eszközökkel történő kommunikáció és adatkezelés biztonsági követelményeit.

Az állami és az önkormányzati szervek elektronikus információbiztonságáról szóló törvény[16] 2013-ban jelent meg. A törvény rendelkezése alapján a honvédelmi célú elektronikus információs rendszerek biztonsági felügyeletét és a vonatkozó hatósági feladatokat a kormány által kijelölt, a honvédelmi ágazaton belül működő szerv a kormányrendeletben[17] meghatározottak szerint látja el. A törvényben leírt honvédelmi célú elektronikus információs rendszerek közé sorolandó a honvédelemért felelős miniszter által működtetett Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózat[18] (MH KCEHH) is. A 2015-ben módosított törvény végrehajtására kiadott BM-rendelet[19] tartalmazza az elektronikus információs rendszer biztonsági osztályba, valamint az elektronikus információs rendszerrel rendelkező szervezetek vagy szervezeti elemek biztonsági szintbe sorolására vonatkozó követelményeket. A 2012-ben kiadott HM-utasítás szerinti általános elektronikus információbiztonsági követelmények felülvizsgálata – a jogszabályi környezetben történt változások alapján – jelenleg napirenden van.

Az ezredforduló utáni első évtizedben új típusú fenyegetésként jelentek meg a különböző külső kapcsolatokkal rendelkező hálózatokhoz csatlakozó rendszerekben jelentős károkat okozó kibertámadások, melyek akár az egyéni felhasználó, akár egy ország működését

[13] 161/2010. (V. 6.) Korm. rendelet.
[14] 3/2012. (I. 13.) HM utasítás.
[15] 121/2011. (XI. 10.) HM utasítás.
[16] 2013. évi L. törvény.
[17] 187/2015. (VII. 13.) Korm. rendelet, 9. fejezet.
[18] 346/2010. (XII. 28.) Korm. rendelet, 2. melléklet.
[19] 41/2015. (VII. 15.) BM rendelet.

meghatározó kritikus infrastruktúra vonatkozásában idézhetnek elő felbecsülhetetlen károkat. Az új fenyegetés az integrációs szervezetek, így a NATO és tagországai szempontjából is kiemelt kockázatot jelent. Ezért a NATO kibervédelmi politikájával, a végrehajtást célzó dokumentumokkal és a nemzetközi irányzatokkal összhangban azonosították a magyar katonai kibervédelmi stratégiai szintű célokat és feladatokat, majd 2013-ban az MH Kibervédelmi Szakmai Koncepció kiadásáról szóló HM-utasításban[20] meghatározták az MH Kormányzati Célú Elkülönült Hírközlő Hálózat biztonsági szintjének emeléséhez szükséges szakfeladatokat, kiemelten kezelve a hálózati szintű incidenskezeléshez szükséges korszerű, automatizált megoldás kialakítását. A szakterület jelentőségét hangsúlyozza, hogy a 2014. évi walesi NATO-csúcson[21] a kibervédelmi terület bekerült a NATO kollektív védelmi feladatai közé, a 2016. évi varsói csúcson[22] pedig a kiberteret új domainként, új műveleti területként (a közfelfogás szerint helytelenül hadszíntérként) azonosították.

A 2014-ben kiadott MH Informatikai Szabályzat[23] (Ált/39) hatályon kívül helyezte a korábban már említett 1993-as elődjét (Ált/210). Az új szabályzat készítése során üzemeltetői igényként merült fel, hogy az tartalmazzon információbiztonsági követelményeket, függetlenül az információvédelmi szakterületen időközben kialakult szabályozási rendtől. Ez okból a szabályzat egy fejezete tartalmazza – átfogó jellegű megfogalmazásban – a híradó-informatikai rendszerek biztonsága érdekében szükséges személyi, fizikai, adminisztratív és elektronikus információbiztonsági követelményeket.

Az előzőekben említett szervezetek, szervezeti elemek, szabályzók és követelmények ismerete minimálisan szükséges a katonai szervezetek elektronikus információvédelmi képességeinek fejlesztése során jelentkező feladatok hatékony végrehajtásához, és jelzi azt az ugrásszerű fejlődést, amit szabályozási, szervezési lépésekkel követni, menedzselni kellett.

AZ ADATKEZELŐ RENDSZEREK KIALAKÍTÁSÁVAL KAPCSOLATOS ELEKTRONIKUS INFORMÁCIÓBIZTONSÁGI FELADATOK

A következőkben a minősített, majd a más szempontból érdekes nem minősített adatkezeléshez köthető elektronikus információvédelmi képességek kialakításával kapcsolatos feladatokat mutatom be.

A NATO-csatlakozás után a szövetségesekkel való együttműködés és a kötelezettségvállalásaink teljesítése során felmerülő kezdeti személyi, fizikai és dokumentumbiztonsági kihívások csakhamar és egyre nagyobb mértékben egészültek ki elektronikus információbiztonsági feladatokkal. A hadműveleti feladatok és a közös kiképzések végrehajtása érdekében szervezett itthoni vagy külföldi gyakorlatok és rendezvények során a hadműveleti, illetve az alkalmazói igényeknek megfelelően különböző elektronikus információvédelmi képességek kialakítása, illetve alkalmazása vált és válik szükségessé jövőben is. Az együttműködés szempontjából elengedhetetlen minősített elektronikus adatkezelő rendszerek biztonsági akkreditációs eljárásrendjét csoportfőnöki szakutasításban[24] szabályozták.

[20] 60/2013. (IX. 30.) HM utasítás, 1. melléklet, 6. fejezet.

[21] Wales Summit Declaration, 72., 73. https://www.nato.int/cps/en/natohq/official_texts_112964.htm#cyber (Letöltés időpontja: 2018. 01. 24.)

[22] Warsaw Summit Communiqué, 70., 71. https://www.nato.int/cps/en/natohq/official_texts_133169.htm#cyber (Letöltés időpontja: 2018. 01. 24.)

[23] 39/2014. (HK 7.) HM utasítás.

[24] 13/2016. (HK 7.) HVK HIICSF szakutasítás.

A szakutasítást figyelembe véve a katonai szervezetek minősített adatainak kezeléséhez szükséges elektronikus adatkezelő képességek kialakítását mindig a hadműveleti alkalmazó által pontosan definiált, úgynevezett hadműveleti igény vagy követelmény alapján kell megkezdeni. Az igénynek tartalmaznia kell az alkalmazók körét, az adatkezelés helyszíneit, az elvárt szolgáltatások és alkalmazások felsorolását, a kezelni kívánt adatok típusát, a feldolgozni kívánt legmagasabb minősítési szintű adat minősítési szintjét, biztonsági osztályát és lehetőség szerint a rendszer működésével kapcsolatos rendelkezésre állási követelményeket. Célszerű a kezdetekkor kijelölni a biztonsági menedzsmentet is, melyet az üzemeltető és a biztonságért felelős állomány együttesen alkot.

A következő lépésben kockázatelemzést kell végezni az alkalmazói követelmény alapján megtervezett rendszer üzemeltetésével és elektronikus biztonságával kapcsolatos kockázatok azonosítása érdekében. A hadműveleti követelmények változtatása esetén a kezdeti kockázatelemzés felülvizsgálata szükséges. A már működő rendszer esetében biztosítani kell az üzemeltetési és a biztonsági környezet, továbbá az elektronikus biztonság változásait előidéző tényezőket figyelembe vevő – a honvédelmi tárca információbiztonság-politika[25] által meghatározott gyakoriságú – kockázatelemzést, amely alapján a szükséges beavatkozások azonosíthatók és végrehajthatók, megvalósítva ezáltal a rendszer teljes életciklusra vonatkozó kockázatkezelését.

A kockázatelemzés eredményei alapján – a minősített adatot kezelő szervezet vezetője – kiadja a rendszerspecifikus biztonsági követelményeket meghatározó dokumentumot, mely a rendszer részletes leírásán túl tartalmazza a rendszer által nyújtott elektronikus adatkezelő szolgáltatásra vonatkozó biztonsági követelményeket. Ezzel egy időben jóváhagyja a maradványkockázatokat.

A minősített adatot kezelő szervezet vezetője a vonatkozó szakutasításban[26] meghatározottak alapján – a rendszerspecifikus biztonsági követelmények (SSRS[27]) teljesülése érdekében – kiadja az üzemeltetés-biztonsági szabályzatot[28] (ÜBSZ), mely előírja a biztonsági menedzsment és a felhasználói állomány által betartandó védelmi rendszabályokat. A felhasználói állományra vonatkozó védelmi rendszabályok kisebb terjedelme okán a számukra elegendő rendszabályokat tartalmazó felhasználói üzemeltetés-biztonsági szabályzatot adnak ki, külön a stacioner telepítésű és külön a hordozható minősített elektronikus adatkezelő eszközök vonatkozásában.

Az engedélyeztetési eljárást megelőzően a rendszerspecifikus biztonsági követelményeknek és az üzemeltetés-biztonsági szabályzatnak megfelelően elő kell készíteni a rendszert vagy eszközt a minősített adatok elektronikus kezelésére. Az előkészített rendszeren, illetve eszközön ellenőrzést kell végrehajtani az érvényben lévő követelmények alapján. A feltárt hiányosságok értékelése és kiküszöbölése után – az illetékes hatóság formai követelményeinek eleget tevő kérelem beterjesztésével – kezdeményezhető a rendszerengedély kiadása.

A biztonsági menedzsment közreműködik a hatósági akkreditációs eljárás lefolytatásában. A rendszerengedély kiadásáról szóló határozat kézhezvétele után – a határozatban rögzítetteknek megfelelően – a rendszerspecifikus biztonsági dokumentumokban előírtak szerint végzi a rendszer biztonsági menedzselését, a vonatkozó szakutasítás[29] 1. sz. melléklete

[25] 94/2009. (XI. 27.) HM utasítás, „A kockázatok kezelése” fejezet.
[26] 9/2012. (HK 14.) HVK HIICSF szakutasítás.
[27] System-Specific Security Requirements Statement.
[28] Security Operations; SecOps.
[29] 10/2012. (HK 14.) HVK HIICSF szakutasítás.

szerinti biztonsági ellenőrzéseket, a biztonsági frissítések végrehajtásának ellenőrzését, a változáskezelést, a konfigurációmenedzsmentet, az incidenskezelést, a szükséges felülvizsgálatokat, valamint felkészül a rendszerengedély hosszabbítására, a rendszer újraakkreditálására.

Az előzőekben ismertetett út bejárásával a katonai szervezet minősített elektronikus adatkezelő rendszerhez, eszközhöz jut. Valódi képességgé ez akkor válik, ha a szükséges felhasználói személyi biztonsági feltételeket is megfelelő időben kialakítják, így a rendszerengedély kiadásával egy időben megkezdődhet – a katonai szervezet feladatai végrehajtását hatékonyan támogató képesség – alkalmazásba vétele. Ennek érdekében a rendszer szolgáltatásait és alkalmazásait igénybe vevő felhasználók szükséges felkészítését, illetve képzését a rendszer kialakításának időrendjében tervezni kell, és lehetőség szerint végre is kell hajtani.

A fentiek szerinti rendszerbiztonsági engedélyezési (SA[30]) eljárásrend eredményeként 3 évre érvényes engedélyt adnak ki. A hadműveleti követelmények változatossága, az elvárt szolgáltatások és alkalmazások megvalósíthatóságának előzetes ismerete érdekében a fenti eljárás kiegészülhet további elektronikus információvédelmi feladatokkal, melyeket az alábbiak szemléletesen mutatnak be.

Azoknak a minősített elektronikus adatkezelő rendszereknek az esetében, melyek az alkalmazásuk során rejtjelzési kötelezettség alá eső minősített adatokat kezelnek, a biztonsági menedzsmentet ki kell egészíteni a rejtjeltevékenységre vonatkozó személyi biztonsági feltételeket teljesítő állománnyal. Az adatkezelő rendszer kialakítását a rejtjelbiztonságra vonatkozó követelmények betartásával kell végezni. Ha a katonai szervezet korábban nem folytatott rejtjeltevékenységet, úgy szükségessé válhat a rejtjeltevékenység fizikai és adminisztratív biztonsági feltételeinek kialakítása is. A minősített elektronikus adatkezelő rendszerben alkalmazott rejtjelző eszköz működtetését a hatóság a rendszerengedély-kérelem alapján kiadott határozatban engedélyezi. A Magyar Honvédségnél bevezetett és fejlesztés alatt álló nemzeti „Titkos!" és NATO SECRET minősített elektronikus adatok kezelésére engedélyezett Védett Vezetés Irányítási Rendszer (VVIR) által használt átviteli utak védelme érdekében – hasonlóan a NIAR-hoz – központi menedzsmenttel működő Internet Protocol- (IP-) alapú rejtjelző hálózat került kialakításra. Ebből következik, hogy a VVIR központi kiszolgáló egységeihez – a rejtjelző hálózaton keresztül – kapcsolódni kívánó minősített adatot kezelő katonai szervezeteknek saját képességük kialakításánál és engedélyeztetésénél a vonatkozó rejtjeltevékenységgel szemben támasztott biztonsági követelményeket is alkalmazniuk kell.

A minősített elektronikus adatkezelő rendszerekre vonatkozó jogszabályok leginkább állandó telepítési körülményekre és általánosnak mondható alkalmazói igényeknek megfelelően állapítanak meg információbiztonsági követelményeket. A több katonai szervezet alegységeiből létrehozandó ideiglenes harci kötelék, zászlóaljharccsoport vezetési és irányítási feladatait támogató minősített harcászati rádió- és minősített elektronikus adatkezelő rendszerek mobil, állandóan változó műveleti környezetre értelmezhető védelmi rendszabályainak és a biztonsági garanciák bemutatása, valamint a rendszerek engedélyeztetési eljárásának lefolytathatósága érdekében 2012-ben a hatóság részére gyakorlótéri környezetben műveleti mozzanatokat mutattak be. A hatóság a bemutató alapján elfogadta a működési sajátosságokból következő alkalmazói igényeket, és határozatban[31] engedélyezte a műveleti tervezést megkönnyítő, modulrendszerűen kialakítható harcászati rádióhálók alkalmazását.

[30] Security Accreditation.

[31] Kassai Károly: Az elektronikus információvédelem felső szintű szervezeti és szakmai történései a 2005–2015 közötti időszakban. Hadmérnök, X. évfolyam 3. szám, 287.

Előfordulhat, hogy a kialakításra tervezett minősített elektronikus adatkezelő rendszer elvárt szolgáltatásai és alkalmazásai funkcionális működése szempontjából elengedhetetlen tesztelés[32] során minősített adatok használata válik szükségessé. Ilyenkor a katonai szervezet kérelmére az engedélyező hatóság – a minősített adat tesztelési céllal történő használatának engedélyezése érdekében készült speciális kockázatelemzés alapján – tesztelési engedélyt (AfT[33]) ad ki legfeljebb három hónap időtartamra, ami igény esetén akár több alkalommal is meghosszabbítható. Több szervezetet érintő tesztelés esetén az illetékes szakterületi elöljáró szerv koordinálja a tesztelési feladatok végrehajtását. Nemzetközi rendszerhez való csatlakozás esetén az akkreditáló hatóság által kiadott megfelelőségi nyilatkozat (SoC[34]) illetékes szervezethez történő megküldésével kell igazolni az összekapcsolással járó információbiztonsági követelményeknek való megfelelést. A tesztelési engedélyezés szükségességét mi sem illusztrálja jobban, mint a NATO Biztonsági Beruházási Program részeként az MH Légi Vezetési és Irányítási Központban (MH LVIK) kialakítás alatt álló légi vezetési és irányítási rendszer (ACCS[35]) – napjainkban is folyamatban lévő – funkcionális és biztonsági tesztjeinek végrehajtása.

Ideiglenes engedély kiadására irányuló kérelem[36] hatósághoz történő benyújtására van lehetőség abban az esetben, amikor a minősített elektronikus adatkezelő rendszer kritikus fontosságú biztonsági követelményei teljesülnek, de a végleges kialakítás szerinti védelmi rendszabályok pontosítása, véglegesítése érdekében szükséges a rendszer üzemeltetésének megkezdése, folytatása, nem utolsósorban a hadműveleti alkalmazás szempontjából kritikus rendelkezésre állás biztosítása. A beterjesztett kérelemben a katonai szervezet biztonsági vezetőjének nyilatkoznia kell arról, hogy a fennálló hiányosságokat elfogadhatónak tartja és hatásaikat ideiglenes védelmi rendszabályok bevezetésével ellensúlyozza. Az ideiglenes engedélyezés (ISA[37]) többnyire a kialakítás vagy átalakítás állapotában lévő minősített elektronikus adatkezelő képességek vonatkozásában alkalmazható. A leggyakrabban alkalmazott metódus a már rendszerengedéllyel rendelkező minősített elektronikus adatkezelő rendszerek – időközben megváltozott TEMPEST-követelményeknek[38] megfelelő – újraakkreditálása. Ha az ideiglenes rendszer engedélyét nem hosszabbítják meg, vagy a végleges rendszer működéséhez előírt követelményeknek megfelelően nem alakítják át, úgy a vonatkozó előírások betartásával meg kell azt szüntetni.

A katonai szervezetnek korlátozott engedélyezési (LSA[39]) eljárás lefolytatására irányuló kérelmet[40] kell az engedélyező hatósághoz benyújtania abban az esetben, amikor a minősített elektronikus adatkezelő rendszert meghatározott feladatra, célhoz kötve, időben behatárolt katonai, illetve válságkezelő feladathoz az eredetileg tervezett üzemeltetési helyszíntől, biztonsági környezettől eltérő feltételek között kívánja alkalmazni. Az MH 59. Szentgyörgyi Dezső Repülőbázis (MH 59. SZD REB.) kijelölt állománya és repülőeszközei 2015 szeptemberétől négy hónapon keresztül balti légtérrendészeti (BAP[41]) feladatokat hajtottak

[32] 13/2016. (HK 7.) HVK HIICSF szakutasítás 1. sz. melléklet 5.2.
[33] Approval for Test.
[34] Statement of Compliance.
[35] Air Command and Control System.
[36] 13/2016. (HK 7.) HVK HIICSF szakutasítás 1. sz. melléklet 5.3
[37] Interim Security Accreditation.
[38] TEMPEST – az elektronikus eszközök kompromittáló elektromágneses kisugárzás elleni védelme.
[39] Limited Security Accreditation.
[40] 13/2016. (HK 7.) HVK HIICSF szakutasítás 1. sz. melléklet 5.3.
[41] Baltic Air Policing.

végre litvániai települési hellyel. A működési feltételek két helyszínen történő egyidejű biztosítása érdekében szükségessé vált a katonai szervezet minősített elektronikus adatkezelő képességei – repülési feladattervező rendszer, elektronikai hadviselést támogató rendszer, műszaki adatkiértékelő rendszer, irodai munkavégzést támogató NATO SECRET/Nemzeti „Titkos!" és NATO CONFIDENTIAL/Nemzeti „Bizalmas!" önálló telepítésű rendszerek számának – átmeneti növelése. Mindemellett biztosítani kellett a minősített elektronikus adatok cseréjét a katonai szervezet kecskeméti telephelye és a repülőgépek gyártói támogatását biztosító svéd fél irányába is. A BAP-feladat végrehajtása során új hadműveleti alkalmazói igény fogalmazódott meg az elfogott repülőgépekről történő légi felvétel készítésére alkalmas kép- és hangrögzítő eszköz használatának engedélyezésére a már hatósági engedéllyel rendelkező Gripen repülőgépek fedélzetén. Az ÜBSZ megfelelő védelmi rendszabályokkal történő kiegészítése után a hatóság hozzájárult a kép- és hangrögzítő eszköz működtetéséhez.

A NATO integrált légvédelmi rendszer (NATINADS[42]) keretében 2014 októberétől Magyarország is részt vesz a szlovén légtér légtérrendészeti feladatainak ellátásában. A feladatot szintén az MH 59. SZD REB. repülőgépei hajtják végre, Kecskemét helyőrségből. A fedélzetre telepített rejtjelző eszközöknek az ország területéről történő kivitelére és külföldön történő használatára engedélyezési kötelezettség,[43] valamint a fedélzeten működő minősített elektronikus adatkezelő rendszerek és adathordozóik kezelésének szabályozására külön biztonsági eljárásrend kiadása vált szükségessé.

A biztonsági eljárásrend kialakítását nehezíti, hogy a legtöbb szomszédos országgal nincs megállapodásunk arra vonatkozóan, hogy a bajba jutott, esetleg katasztrófát elszenvedett repülőeszköz fedélzetén található minősített adathordozók és elektronikus adatkezelő rendszerek, rejtjelző eszközök és rejtjelanyagok megőrzése érdekében milyen védelmi rendszabályok foganatosítása várható el az illető ország jogosultsággal rendelkező szervezeteitől. Mivel a légtérrendészeti feladat végrehajtása előre nem meghatározható időpontban történik, így az előzetes engedélyeztetési eljárási követelmény nem értelmezhető. Ezért a fegyveres légi készenléti szolgálatot ellátó repülőgépek esetében a feladat megkezdhető, de a végrehajtás elektronikus információbiztonsággal kapcsolatos adatairól – szintén egy erre kidolgozott és a hatóság által jóváhagyott eljárásrendnek megfelelően – jelentési kötelezettsége van a katonai szervezet elektronikus információvédelmi szakállományának.

A minősített elektronikus adatkezelő rendszerek összekapcsolásához szükséges minimum biztonsági követelményeket – a külső csatlakozást megvalósító technikai rendszert és eljárások összességét magában foglaló – rendszerösszekapcsolás-biztonsági követelmények (SISRS[44]) dokumentumban kell meghatározni. Ilyen követelményrendszernek való megfelelés alapján realizálódhatott Lengyelországban az *Anakonda 2016* stratégiai hadműveleti és harcászati szintű, számítógéppel támogatott parancsnoki és törzsvezetési gyakorlaton a – nagyjából 30 eszközt magában foglaló – Hungarian Mission Network (HMN) és a házigazda által üzemeltetett Polish Mission Network (PMN) összekapcsolása. A lengyel fél által meghatározott rendszerösszekapcsolás-biztonsági követelmények és a magyar fél hálózatának rendszerbiztonsági követelményei alapján előkészítették a minősített elektronikus adatkezelő rendszert, melyre az akkreditáló hatóság kiadta a rendszerengedélyt, továbbá a PMN-hez történő csatlakoztatási engedélyt, a lengyel fél irányába pedig a megfelelőségi nyilatkozatot.

[42] NATO Integrated Air Defense System.
[43] 161/2010. (V. 6.) Korm. rendelet, 21. fejezet.
[44] System Interconnection Security Requirements Statement.

Az eset jó például szolgál az adott feladatra és időszakra érvényes, korlátozott engedély kiadására irányuló akkreditációs kérelem benyújtásánál alkalmazandó eljárásra is.

A közelmúltban jelentősen megnövekedtek a szövetségeseinkkel közös kiképzési, műveleti és együttműködési feladataink, melyek során egyre gyakrabban válik szükségessé minősített adat felhasználásával tartandó megbeszélések, konferenciák és más rendezvények szervezése. A rendezvény előkészítésének időszakában a rendező katonai szervezet biztonsági vezetője a feldolgozni kívánt minősített adat minősítési szintjének megfelelő személyi, fizikai, adminisztratív és elektronikus információbiztonsági védelmi rendszabályokat tartalmazó biztosítási tervet készít a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló kormányrendelet[45] alapján. 2017 júniusában – talán az év legjelentősebb ilyen tanácskozásaként – rendezték meg a NATO 4. Északi Régió parancsnoki konferenciáját, melynek az MH Összhaderőnemi Parancsnokság adott otthont. A tanácskozáson az északi régió partnernemzetei, Finnország és Svédország is részt vettek. A NATO SECRET minősítésű adatokat feldolgozó konferencia védelmi rendszabályait ennek megfelelően kellett alkalmazni, biztosítási tervét ennek megfelelően kellett elkészíteni.

A nemzetközi együttműködés nemcsak az integrációs (NATO, EU) szervezetekhez köthető adatfajták, de nemzeti minősített adatok cseréjén és kezelésén is alapulhat. Ilyenkor a felek kétoldalú megállapodásban rögzítik a minősített adatok cseréjéről és kölcsönös védelméről szóló biztonsági szabályokat, mely megállapodást törvényben erősítik meg. A napjainkban hatályos jogszabályok alapján létrehozott megállapodások megfelelően támogatják az elektronikus információvédelmi feladatok végrehajtását. De, ahogy azt korábban említettem, elektronikus információvédelmi szempontból mindmáig erőforrás-pazarlást eredményeznek azok a megállapodások, melyeknek az államtitokról és a szolgálati titokról szóló törvény NATO-csatlakozásunk előtti hatályos változata képezte az alapját. Erre jó példa a Magyar Köztársaság Kormánya és Nagy-Britannia és Észak-Írország Királysága Kormánya közötti megállapodás, mely szerint Nagy-Britannia és Észak-Írország Egyesült Királyságában „RESTRICTED" minősítéssel ellátott információt a Magyar Köztársaságban „TITKOS" minősítésűként kell kezelni.[46] A minősített adat kezelésére vonatkozó elektronikus információbiztonsági követelményeket ennek megfelelően kell alkalmazni, beleértve a TEMPEST – és a címhez ugyan szorosan nem tartozó, de információvédelmi szempontból nem elhanyagolható személyi és fizikai biztonsági – követelményeket is. Az említett megállapodás szerinti elektronikus információvédelmi képesség kialakítása és folyamatos működtetése – a védelmi rendszabályok aránytalansága miatt – az MH 5. Bocskai István Lövészdandár és az MH 25. Klapka György Lövészdandár szakállományát tette és teszi próbára napjainkban is.

A katonai szervezetek mindennapjaiban nem kizárólag a minősített elektronikus adatkezelő képességek kialakításával kapcsolatos tennivalók képezik az elektronikus információvédelemmel foglalkozók feladatait. Új híradó-informatikai rendszer vagy infrastruktúra kiépítése, a meglévő rendszer új összetevőkkel történő kiegészítése, a rendszerben meglévő összetevők módosítása, cseréje, modernizációja esetén érvényesíteni kell az elektronikus információbiztonsági követelményeket a nem minősített adatkezelő rendszerek vonatkozásában is.[47]

[45] 90/2010. (III. 26.) Korm. rendelet, IX. fejezet.
[46] 1999. évi XIX. törvény, 1.2.
[47] 39/2014. (HK 7.) HM utasítás, Ált/39 8.4.

A kormányzati célú hálózatokról szóló kormányrendelet felhatalmazása alapján a Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózatot üzemeltet, melynek rendszerspecifikus biztonsági követelményeit csoportfőnöki szakutasításban[48] adták ki. A honvédelmi célú elektronikus adatkezelő rendszerek üzemeltetése során biztonsági szempontból alapvető cél a nyilvános hírközlő hálózatoktól való fizikai elkülönülés. A fizikai elkülönítés azonban a katonai szervezetek teljes elzárását jelenti a társadalom egyéb szereplőivel való kapcsolattartáshoz és együttműködéshez szükséges elektronikus adatkezelő szolgáltatások igénybevételének lehetőségétől, megnehezítve ezáltal a katonai szervezetek – vezetési és irányítási feladataihoz alapvetően nem kötődő – hétköznapi működtetésével járó más feladatok végrehajtását is. Az együttműködési feltételek megteremtése érdekében az MH KCEHH által nyújtott bizonyos szolgáltatások nyilvános hírközlő hálózat irányába, illetve irányából való igénybevételének lehetőségét – a szükséges védelmi intézkedések bevezetésével egyidejűleg – engedélyezték és feltételeit kialakították.

Elektronikus adatkezelő rendszereink biztonsága magas szinten tartásának egyik záloga lehet a technológiailag megfelelő, fejlett határvédelmi rendszer alkalmazása. A megfelelő határvédelmi rendszer működtetésén túl feltétlenül szükséges, hogy a katonai szervezetek elektronikus információbiztonsági menedzsment személyei naprakész információkkal rendelkezzenek a nyilvános hírközlő hálózatokat feszítő, információbiztonsággal kapcsolatos kihívásokról, és ezekről a szükséges mértékben tájékoztassák a felelősségi körükhöz tartozó felhasználó állományt.

A nyilvános hírközlő hálózatok viszonylatában néhány példa jól mutatja a hírközlő hálózatokhoz kapcsolódó eszközök, rendszerek, alkalmazott fogalmak, az általuk megvalósuló alkalmazások és nyújtott szolgáltatások igénybevételével felmerülő lehetséges kockázatokat. Jelenleg a legtöbb ilyen megoldás a Magyar Honvédségben nincs használatban, de a fejlődés intenzitása és a vonatkozó trendek alakulása kikényszerítheti ezek alkalmazását.

Elsőként, a „Big Data" koncepció kapcsán, óriási mennyiségű – milliárdos nagyságrendű – komplex adatrekordot tartalmazó halmazra kell gondolni, melynek elemzése és feldolgozása hagyományosnak mondható számítási kapacitás alkalmazásával nem kezelhető hatékonyan. Napjainkban másodpercenként több 10 TB-nyi (terabyte; 1 TB nagyjából 220 db egyrétegű DVD-re írható adatot jelent) adat keletkezik a hálózatra feltöltött videófájlok, az elektronikus levelezés, SMS-küldés vagy akár log fájl[49] formájában. A roppant adatmennyiség tárolása és feldolgozása során az elektronikus információvédelmi követelmények közül a rendelkezésre állás biztosítása lehet a legnagyobb kihívás, mivel egy relatíve lassabb adatelérést biztosító tárolási és feldolgozási mód a szükséges adat rendelkezésre állását oly mértékben késleltetheti, hogy az felhasználói szempontból már elfogadhatatlan. A koncepció katonai alkalmazása – a jövőben – döntéshozatali eljárások támogatásában, illetve védelmi rendszerek kialakításának tervezése során realizálódhat.

A felhőalapú számítástechnikai szolgáltatások mindegyikére igaz, hogy – az üzemeltetés részleteinek felhasználó előli elrejtésével – a szolgáltató saját eszközparkján elosztva, virtualizáció alkalmazásával biztosítja azokat. A felhőalapú szolgáltatások szempontjából három csoport különböztethető meg. Az első az infrastruktúra-szolgáltatás, amikor virtuális hardver, tárhely, hálózati kapcsolat és számítási kapacitás biztosítása történik. A második a platformszolgáltatás, amikor az alkalmazás működéséhez szükséges környezetet biztosítják.

[48] 20/2013. (HK 12.) HVK HIICSF szakutasítás.
[49] Naplófájl.

A harmadik pedig a szoftverszolgáltatás, amikor például a böngésző használatával http[50] protokollon keresztül a szolgáltatás tárgyát képező szoftvert lehet használni.

A hozzáférés alapján megkülönböztethető privát, publikus és hibridfelhő. A privát felhőszolgáltatás saját vagy a felhasználó részére kizárólagosan dedikált erőforrások alkalmazásával valósul meg. A publikus felhőszolgáltatás esetén a szolgáltató erőforrásait – a megfelelő izoláció alkalmazásával – megosztják az ügyfelek között. Hibrid szolgáltatás igénybevétel akkor történik, ha a privát felhő használójának átmeneti többletteljesítmény-igénye jelentkezik, és ennek kielégítésére publikus szolgáltatást vesz igénybe. A Magyar Honvédség vonatkozásában a felhőszolgáltatások alkalmazási igénye nem releváns, mivel biztonsági szempontból kizárólag a saját eszközökből felépített privátfelhő-megoldásnak lenne létjogosultsága, viszont a jelenleg üzemeltett infrastruktúra, a nyújtott szolgáltatásai és a biztonsági menedzsment működése garantálja a biztonságos és hatékony munkavégzést.

A „Bring Your own Device”[51] (BYoD) felhívás arra, hogy mindenki használja a saját mobilkommunikációs eszközét vállalati környezetben is. Ez előnyt jelenthet a munkáltatónak abból a szempontból, hogy nem kell céges mobil eszközt biztosítania, illetve jelentősen csökkenthetők az IT-kiadások. A felhasználó komfortérzetében is pozitív változást eredményezhet, ha két mobil helyett egyet kell használnia. Biztonsági kockázatot eredményez azonban az olyan saját eszköz vállalati hálózathoz történő csatlakoztatása, amely ugyanakkor csatlakozik – a gyártók által az utóbbi időben egyre nagyobb népszerűséggel készülékbe integrált – saját felhőszolgáltatáshoz is. Ezeknek a felhőszolgáltatásoknak a legtöbb esetben nem ismert a telephelye, ami adatvédelmi kérdés felmerülése esetén jogi aggályokat eredményezhet. A felhasználók által vásárolt mobil eszközök széles skálája hatványozottan megnövelheti a vállalati rendszer üzemeltetésének biztonsági kérdéseit. Ezért, ha a vállalat vezetése nem a biztonságos és könnyebb tiltó intézkedést választva profitálni szeretne a BYoD jelenségéből, akkor érdemes lehet a biztonsági menedzsment és a vállalati rendszer részéről jelentős többleterőforrás-igényt mellőző termékek engedélyezése és az IT-hálózat ennek megfelelő beállítása. A vállalati hálózat elérésének biztonsági és a mobil eszközön végezhető adatkezelés követelményeit ennek megfelelően kell meghatározni és a felhasználókkal szigorúan betartatni.

A másik megoldás, a saját tulajdonú mobil eszköz vállalati menedzselt eszközkörbe történő bevonása nem életszerű. A katonai szervezeteknél a BYoD-felhívást nem adták ki, de az MH KCEHH szolgáltatásaihoz hozzáféréssel és megfelelő saját tulajdonú mobil eszközzel rendelkező felhasználóknak lehetőségük van a hálózat által nyújtott szolgáltatások korlátozott igénybevételére saját mobil eszköz alkalmazásával, tudomásul véve, hogy a katonai szervezet tulajdonában lévő eszközökre előírt biztonsági követelmények ebben az esetben a saját készülék használatára is mérvadók. A rendszerhez történő csatlakoztatás során a felhasználónak nyilatkoznia kell annak tudomásulvételéről, hogy a központi szerver a mobil eszköz biztonsági szempontból lényeges beállításait felülírhatja. Ennek hiányában a rendszerhez történő csatlakozás nem jön létre. A katonai szervezetek felhasználói ezt a képességet jellemzően irodai környezetben nem alkalmazzák, ezért nem azonosítható teljes mértékben a BYoD koncepciójával.

[50] Hypertext Transfer Protocol.
[51] Hozd a saját eszközödet.

A világban alkalmazott IoT-eszközök[52] darabszáma – a Gartner[53] előrejelzése alapján – a 2009. évi 1,2 milliárdról, 2020-ra 7,3 milliárdra növekszik. Ezek az eszközök kezelői felületet nem feltétlenül tartalmazó szenzorok, melyek képesek az internethez vezeték nélküli kapcsolaton csatlakozva a környezetükre – vagy magát az IoT-eszközt tartalmazó termék működésére – jellemző adatok automatikus továbbítására az adatfeldolgozó rendszer felé. Az évtized végére az IoT-komponensek költségei annyira lecsökkennek, hogy bármilyen terméknek alapfelszereltségévé válhat a hálózati kapcsolódás képessége. A mobiltechnológiák fejlődése, az eszközök méretének csökkenése lehetővé teszi azok biztonságtechnikai rendszerekben való alkalmazásának elterjedését, vagy akár mozgó platformokra történő felszerelését. A beléptető-, azonosító-, behatolásra figyelmeztető, detektáló-, riasztó- vagy akár felderítőrendszerekben történő alkalmazása lehetőséget adhat az IoT-eszközök katonai célú hasznosítására is.[54] Az IoT-eszközök alkalmazásának hasznossága a gazdaság hatékony működése szempontjából vitathatatlan, de elektronikus információvédelmi szempontból közel sem elhanyagolható az a tény, hogy a szenzorok az interneten teljesen nyílt adatforgalmat bonyolítanak a feldolgozórendszer irányába, ami jelentős kockázatot eredményezhet az adatok bizalmassága szempontjából.

A már említetteken kívül szót kell ejteni arról is, hogy zsarolóvírusok terjesztése az utóbbi időszakban a kiberbűnözés egyik alapvető módszerévé vált. Leginkább a nem biztonságos webhelyek látogatásával, a letöltésekkel és az elektronikus levél malware[55]-t tartalmazó csatolmányának megnyitásával érkezhetnek ezek a vírusok a felhasználó számítógépére. Az aktiválódás után olyan titkosítási eljárást alkalmaznak a felhasználó adatain, mely a visszaállításhoz szükséges kulcs ismerete nélkül szinte feltörhetetlenné teszi azokat. A kulcsot anyagi ellenszolgáltatásért cserébe hajlandóak átadni a vírus terjesztői. A Cybersecurity Ventures[56] előrejelzése szerint a világon a kiberbűnözés által 2015-ben okozott károk mértéke 2021-re megduplázódik, és meghaladja a hatezer milliárd dollárt, melynek egyre jelentősebb részét a zsarolóvírusokkal okozott károk teszik majd ki.[57] Az előrejelzés rámutat arra, hogy a fenyegetést komolyan kell venni és az elektronikus adatkezelő rendszerek biztonsági szintjének kockázatarányos emelését végre kell hajtani, mindemellett folyamatosan fejleszteni kell a felhasználók biztonságtudatosságát is.

Már a 20. század közepén megkezdődtek a mesterséges intelligencia (AI[58]) kutatásai, de a számítógépek századvégi nagyfokú számítási képességnövekedése tette lehetővé, hogy mostanra egyre több területen alkalmazzák az elért eredményeket. A mesterséges intelligencia lassan mindenütt megtalálható. Elektronikus információvédelmi szempontból jelentősebbnek mondható a keresőmotorokban és az elektronikus levelezés levélszemét-szűrésében való alkalmazása. A jövőre vonatkozóan széles távlatokat nyithat az elektronikus

[52] Internet of Things – a dolgok internete.

[53] Gartner – amerikai kutatási és tanácsadó vállalat.

[54] Előzetes Megvalósíthatósági Tanulmány „Az Internet of Things koordinált fejlesztése és alkalmazásának elterjesztése Magyarországon" tárgykörben. Készítette az Informatikai, Távközlési és Elektronikai Vállalkozások Szövetsége (IVSZ) 2014. június – 2015. május, 17–18. http://ivsz.hu/wp-content/uploads/2016/04/az-internet-of-things-koordinalt-fejlesztese-es-alkalmazasanak-elterjesztese-magyarorszagon-.pdf (Letöltés időpontja: 2018. 01. 22.)

[55] Malicious software, malware – rosszindulatú szoftver.

[56] Cybersecurity Ventures – kiberbiztonsági kutatással foglalkozó amerikai vállalat.

[57] Cybersecurity Ventures, 2017. Cybercrime Report, 3. https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf (Letöltés időpontja: 2018. 01. 24.)

[58] Artificial Intelligence.

adatkezelő rendszerek védelmi képességeinek növelése terén, melyre szükség is lesz, a Cybersecurity Ventures előrejelzése alapján ugyanis csak a zsarolóvírusokkal elkövetett támadások átlagosan 14 másodpercenként fognak bekövetkezni a világon 2019-ben.[59] Ez az adat alátámasztja, hogy a kiberfenyegetések mértéke már túlnőtt azon a határon, amit csupán emberi beavatkozással hatékonyan kezelni lehetne. A fenyegetések észlelése és a reagálás között eltelt idő csökkentésével a bekövetkező kár is jelentősen csökkenthető. A reakcióidő drasztikus csökkenéséhez gyors észlelésre, az elemzési folyamat jelentős lerövidítésére és azonnali automatikus reagálásra van szükség, melyben jó szolgálatot tehet a rendelkezésre álló adatokból és vizsgált folyamatokból állandóan tanuló mesterséges intelligencia. A kutatók azonban a mesterséges intelligencia fejlődésével együtt járó veszélyekre is figyelmeztetnek, melyeket az alkalmazás során ajánlott figyelembe venni.

AZ ADATKEZELŐ RENDSZEREK KIALAKÍTÁSÁVAL KAPCSOLATOS JÖVŐBENI ELEKTRONIKUS INFORMÁCIÓBIZTONSÁGI FELADATOK

Az afganisztáni műveletek tapasztalatai alapján a NATO részéről kezdeményezés született egy olyan képesség – kapcsolt műveleti hálózat (FMN[60]) – kialakítására, amely a jövőbeni műveletek során hatékonyan támogatja a vezetési és irányítási, döntéshozatali folyamatokat, valamint az információk biztonságos megosztását a műveletben részt vevő NATO- és nem NATO-nemzetek, szervezetek között. Az FMN-koncepció kialakítása több mérföldkőhöz kötött, melyek az elektronikus adatkezelő rendszerek, továbbá az általuk kezelt adatok minősítési szint szerinti elkülönítésében különböznek egymástól. A mérföldkövekhez tartozó modellek megvalósítása különböző védelmi rendszabályok kidolgozását követeli meg a biztonsági menedzsmenttől. A műveletekbe felajánlott katonai szervezetek vonatkozásában, a szövetséges erőkkel történő együttműködés érdekében az alapnál magasabb szintű, legalább a részleges önállóságot biztosító – a küldetés szempontjából kritikus szolgáltatásokat nyújtó hálózati elemhez csatlakozni képes – képesség kialakítása indokolt.

A katonai szervezetek elektronikus információvédelmi képességeinek kialakítása – minősített elektronikus adatkezelés vonatkozásában – a VVIR fejlesztésével és kiterjesztésével folytatódik. A képesség kialakításánál a korábban már ismertetett biztonsági akkreditálási eljárásrend, a stacioner minősített elektronikus adatkezelő rendszer engedélyeztetése alkalmazható. A katonai szervezetek feladatrendszerétől függően követelmény lehet a képesség tábori körülmények közötti alkalmazása is, ami a védelmi rendszabályok kiegészítését, esetleg másik műveletek engedélyeztetési eljárásainak lefolytatását is megkövetelheti.

Az EU nagy kiterjedésű hálózati műveletek (OPSWAN[61]) rendszere eredetileg a műveletek tervezésére, az EU Katonai Tanács, a műveleti parancsnokságok (Operational Headquarters; OHQ) és a végrehajtó erő parancsnokságok (Force Headquarters; FHQ) viszonylatában létrehozott legfeljebb EU SECRET minősítési szintű adat kezelésére engedélyezett hang-, adat-, elektronikus levél és faxszolgáltatásokat biztosító elektronikus adatkezelő rendszer. Az EU döntése alapján ezt a rendszert kiterjesztik minden tagország irányába az erőgenerálás és a minősített adatcserék biztonságos végrehajtása érdekében. Mivel az EU-harccsoportok

[59] Cybersecurity Ventures, 2017 Cybercrime Report, 7.
[60] Federated Mission Networking.
[61] Operations Wide Area Network.

(EU BG[62]) rotációjában Magyarország a többi V4-országgal közösen részt vesz, így az érintett katonai szervezetek vonatkozásában a képesség kialakítása a közeljövőben megvalósulhat.[63]

Az MH KCEHH kibervédelmi képességét – az MH kibervédelmi szakmai koncepciójában azonosított kibervédelmi feladatok alapján, az összetettség és a rendelkezésre álló erőforrások okán – fokozatos, folyamat jellegű képességfejlesztési módszer mentén alakítják ki.[64] A katonai szervezetek vonatkozásában a kibervédelmi feladatokat az illető szervezet béke és különleges jogrend szerinti feladatrendszerével összhangban kell meghatározni. A funkciók figyelembevételével azonosítani kell a szervezet kibervédelmi céljainak eléréséhez szükséges szervezeti felelősségeket, szervezeti elemeket.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

A hazánk NATO-csatlakozása óta eltelt időszakban a szakterület követelményeit meghatározó jogszabályi környezet jelentősen átalakult, fejlődött, megfelelő keretet szolgáltatva ezáltal a tárca- és szervezeti szintű szabályzók megalkotásához, melyek biztosítják a katonai szervezetek elektronikus információvédelmi tevékenységének hatékony végrehajtását.

A digitalizáció és a nagyfokú infokommunikációs fejlődés töretlen folytatódása újabb és újabb kihívásokat eredményez az elektronikus információvédelmi szakterületen, ami megköveteli a szabályozási környezetnek az elért eredmények és az információbiztonsági trendek elemzésén alapuló folyamatos felülvizsgálatát.

A katonai szervezetek vezetési és irányítási feladatainak hatékony támogatását központilag támogatott és üzemeltetett, hálózati struktúrában működő, az adatkezelés szempontjából a teljes hálózatban állandó és egységes védelmi szintet biztosító elektronikus adatkezelő rendszerek és az általuk nyújtott szolgáltatások alkalmazásával kell megvalósítani.

Az elektronikus információvédelmi képességek kialakítását és magas szintű fenntartását korszerű technikai megoldások mentén, megfelelően tanúsított termékek és hatékony védelmi rendszabályok alkalmazásával kell megvalósítani, kiegészítve mindezt a biztonságtudatosság célcsoport-specifikus erősítésével a felhasználók, az üzemeltetésért felelősök, a biztonságért felelősök és a döntéshozók vonatkozásában.

A tanulmány áttekintette az elektronikus információs rendszerek védelmével kapcsolatos fontosabb szabályozási lépéseket, és erre támaszkodva bemutatta az érdekesebb védelmi megoldásokat.

Látható, hogy a védelmi rendszabályok kialakulása, a szolgáltatások fejlődése egyre gyorsabb ütemű változásokat generál, melyek hatására a jövőben előtérbe kerülnek az automatikus védelmi mechanizmusok, a pusztán emberi beavatkozást minimalizáló technikai megoldások. Számszerűleg nőni fognak a hálózati típusú megoldások, remélhetőleg kiszorítva az önálló eszközök alkalmazását.

A szövetségi műveletek bonyolultsága ezek mellett megnöveli a közös kialakítású, üzemeltetésű és biztonsági menedzselésű hálózatok világát (lásd FMN), ami a rejtjelzés és annak menedzselése, a biztonsági felügyelet, az auditálás, az ellenőrzés és elektronikus eseménykezelés (incidenskezelés) területén olyan új megoldásokat eredményez, melyek

[62] EU Battle Group.

[63] The European Council and Common Security and Defence Policy (CSDP). http://www.europarl.europa.eu/RegData/etudes/STUD/2016/581416/EPRS_STU(2016)581416_EN.pdf 3.2.2 (Letöltés időpontja: 2018. 01. 25.)

[64] 60/2013. (IX. 30.) HM utasítás 1. sz. melléklet 7. fejezet.

a jelenlegi technikai, szervezési, képzési folyamatok megújítását fogják megkövetelni, beleértve a logisztikai és a pénzügyi folyamatok megújítási szükségességét is.

FELHASZNÁLT IRODALOM

002/1996. MHPK intézkedés 1. sz. melléklet. A HM és MH rejtjeltevékenységének szabályai (hatályon kívül).

10/2012. (HK 14.) HVK HIICSF szakutasítás a Minősített Elektronikus Adatkezelő Rendszer Biztonsági Ellenőrzésére vonatkozó általános követelményekről.

121/2011. (XI. 10.) HM utasítás a mobil kommunikációs eszközök használatával kapcsolatos rendszabályok alapelveiről. https://net.jogtar.hu/jogszabaly?docid=A11U0121.HM&timeshift=fffffff4&txtreferer=00000001.TXT

13/2016. (HK 7.) HVK HIICSF szakutasítás a Minősített Elektronikus Adatkezelő Rendszerek biztonsági akkreditációs eljárásrendjéről.

161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól. https://net.jogtar.hu/jogszabaly?docid=a1000161.kor

179/2003. (XI. 5.) Korm. rendelet a nemzetközi szerződés alapján átvett, vagy nemzetközi kötelezettségvállalás alapján készült minősített adat védelmének eljárási szabályairól (hatályon kívül).

187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról. https://net.jogtar.hu/jogszabaly?docid=a1500187.kor

1995. évi LXV. (VI. 30.) törvény az államtitokról és a szolgálati titokról (hatályon kívül). https://mkogy.jogtar.hu/jogszabaly?%20docid=99500065.TV

1998. évi LXXXV. törvény a Nemzeti Biztonsági Felügyeletről (hatályon kívül). https://mkogy.jogtar.hu/jogszabaly?docid=99800085.TV

1999. évi XIX. törvény a Magyar Köztársaság Kormánya és Nagy-Britannia és Észak-Írország Egyesült Királysága Kormánya között a minősített védelmi információk kölcsönös védelméről szóló, Londonban, 1998. szeptember 7-én aláírt Megállapodás megerősítéséről és kihirdetéséről. https://net.jogtar.hu/jogszabaly?docid=99900019.tv

20/2013. (HK 12.) HVK HIICSF szakutasítás a Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózatának rendszerspecifikus elektronikus biztonsági követelményeinek meghatározásáról. http://www.kozlonyok.hu/kozlonyok/Kozlonyok/13/PDF/2013/12.pdf

2009. évi CLV. törvény a minősített adat védelméről. https://net.jogtar.hu/jogszabaly?docid=a0900155.tv

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról. https://net.jogtar.hu/jogszabaly?docid=a1300050.tv

2013/488/EU EU tanácsi határozat az EU minősített adatok védelmét szolgáló biztonsági szabályokról. https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32013D0488&from=HU

3/2012. (I. 13.) HM utasítás a honvédelmi tárca elektronikus információbiztonsági követelményeinek meghatározásáról és a védelmi rendszabályok pontosításáról. http://www.kozlonyok.hu/kozlonyok/Kozlonyok/13/PDF/2012/2.pdf

346/2010. (XII. 28.) Korm. rendelet a kormányzati célú hálózatokról. https://net.jogtar.hu/jogszabaly?docid=a1000346.kor

39/2014. (HK 7.) HM utasítás a Magyar Honvédség Informatikai Szabályzatának kiadásáról.

41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről. https://net.jogtar.hu/jogszabaly?docid=a1500041.bm

43/1994. (III. 29.) Korm. rendelet a rejtjeltevékenységről (hatályon kívül). http://www.codel.hu/documents/Kepek/Dokumentumok/Torvenyi/43per1994evi.pdf

60/2013. (IX. 30.) HM utasítás a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról. https://net.jogtar.hu/jogszabaly?docid=A13U0060.HM&getdoc=1

79/1995. (VI. 30.) Korm. rendelet a minősített adat kezelésének rendjéről (hatályon kívül). http://codel.hu/documents/DOKUK/Torvenyek/1995_evi_79_VI_30_korm_rend.pdf

82/2002. (HK 26.) HM utasítás a NATO Irodaautomatizálási Rendszer (NIAR) biztonságával kapcsolatos feladatokról.

9/2012. (HK 14.) HVK HIICSF szakutasítás a Minősített Elektronikus Adatkezelő Rendszer Üzemeltetés Biztonsági Szabályzatára vonatkozó általános követelményekről. http://www.kozlonyok.hu/kozlonyok/Kozlonyok/13/PDF/2012/14.pdf

90/2010. (III. 26.) Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről. https://net.jogtar.hu/jogszabaly?docid=a1000090.kor

94/2009. (XI. 27.) HM utasítás a honvédelmi tárca információbiztonság politikájáról. http://www.kozlonyok.hu/kozlonyok/Kozlonyok/13/PDF/2009/18.pdf

Ált/210. a Magyar Honvédség Informatikai Szabályzata, 1993 (hatályon kívül).

Cybersecurity Ventures, 2017 Cybercrime Report. https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf

Előzetes Megvalósíthatósági Tanulmány „Az Internet of Things koordinált fejlesztése és alkalmazásának elterjesztése Magyarországon" tárgykörben. Készítette az Informatikai, Távközlési és Elektronikai Vállalkozások Szövetsége (IVSZ) 2014. június – 2015. május, 17–18. http://ivsz.hu/wp-content/uploads/2016/04/az-internet-of-things-koordinalt-fejlesztese-es-alkalmazasanak-elterjesztese-magyarorszagon-.pdf

Kassai Károly: *Az elektronikus információvédelem felső szintű szervezeti és szakmai történései a 2005–2015 közötti időszakban.* Hadmérnök, X. 3. (2015) http://hadmernok.hu/153_23_kassaik.pdf

The European Council and Common Security and Defence Policy (CSDP). http://www.europarl.europa.eu/RegData/etudes/STUD/2016/581416/EPRS_STU(2016)581416_EN.pdf

Wales Summit Declaration. https://www.nato.int/cps/en/natohq/official_texts_112964.htm#cyber

Warsaw Summit Communiqué. https://www.nato.int/cps/en/natohq/official_texts_133169.htm#cyber