ZRÍNYI MIKLÓS
NEMZETVÉDELMI EGYETEM

Kassai Károly mk. alezredes

A MAGYAR HONVÉDSÉG INFORMÁCIÓVÉDELMÉNEK — MINT A BIZTONSÁG RÉSZÉNEK — FELADATRENDSZERE

Doktori (PhD) értekezés

Dr. habil Sándor Miklós nyá. ezds.
témavezető

Budapest, 2007

TARTALOMJEGYZÉK

BEVEZETÉS

A Magyar Honvédség (MH) átalakításának egyik legfontosabb feladata a vezetés korszerűsítése. [1.] A napjainkban tapasztalható fejlődés robbanásszerűen növeli a vezetéshez és működéshez szükséges információk fontosságát és mennyiséget, így az adatokat, és az információs rendszereket egyre bonyolultabb védelemmel kell ellátni. NATO és EU tagságunk is új információbiztonsági kihívásokat és kötelezettségeket jelent.

Az MH-nál a jogszabályoknak és az állami irányítás egyéb jogi eszközeinek megfelelő eszközökkel és eljárásokkal történik a kezelt adatok védelme. Az információvédelmi szakterületért felelős Waplerné dr. Balogh Ágnes jogi szakállamtitkár véleménye szerint „a honvédelmi tárca (…) kezelésében lévő adatok az eddiginél is hatékonyabb védelmet kívánnak, ezért nagy hangsúlyt kapott az információvédelem stratégiája, tárcaszintű koordinálása és felügyelete. Az MH-nál érzékelhető az információ szerepének jelentős növekedése, az információtechnológiai fejlődés, a NATO és EU szinten irányelvként megfogalmazott eltolódás a papíralapú kommunikációtól az elektronikus kommunikáció irányába, ami meghatározza az információvédelem fejlődési tendenciáit is.” [2.]

Munkám kezdetekor megállapítottam, hogy hazánkban az információvédelemre vonatkozó szabályozók *nem ölelnek fel minden területet* (pl. a nemzeti elektronikus adatok védelme), *nem egyformán részletezettek*, illetve *nem pontosan illeszkednek egymáshoz* (pl. a nemzeti és NATO minősített adatok védelmének rendszabályai). Ugyanígy megállapítottam, hogy az MH belső rendelkezéseiben sehol sem szerepel az *információvédelem átfogó értelmezése, területeinek és feladatainak kijelölése*.

A tapasztaltak alapján szükségesnek érzem, hogy az információbiztonság területén is megkezdődjön a feladatok *rendszerszemléletű* vizsgálata, mert *az adatkezelő rendszerek korszerűsítése a védelmi kérdések kutatása nélkül elképzelhetetlen*.

Kutatási célok

Meggyőződésem, hogy az egyre veszélyesebb információs fenyegetések ellensúlyozásaként az információs rendszerek védelmi feladatainak *rendszerszemléletű megközelítésével* megfogalmazható, hogy *milyen területeken, milyen módszerekkel lehet és kell védeni* az MH szervezeteinél kezelt nemzeti és szövetségi (vagy egyéb külföldi) adatokat, és *hogyan kell a védelmi rendszabályokat egységesen menedzselni*. Ennek igazolására a következő kutatási célokat jelölöm ki:

– A magyar stratégiai szintű dokumentumok információvédelemre vonatkozó megállapításainak kimutatása, és az MH szakterületi feladatainak felső szintű

megalapozottságának meghatározása. Az MH összhaderőnemi szempontból legfontosabb doktrínáinak információvédelmi szempontú elemzése, a hiányosságok kimutatása és javaslatok megfogalmazása.

- Az információvédelmi szakterületek általános jellemzése, a nemzeti és NATO, EU védelmi rendszabályok összehangoltságának megállapítása, a fontosabb gátló tényezők feltárása, és általános biztonsági alapelvek megfogalmazása az egységes szintű védelem érdekében.
- Az információvédelmi rendszabályok menedzseléséhez szükséges feladatok jellemzése, a felső szintű jogszabályok hatásainak kimutatása, és az MH információvédelmi szakterület szabályozásának összefogására vonatkozó javaslatok megfogalmazása.

Doktori képzésem előtt tagja voltam a NATO Védelmi Képességek Kezdeményezés végrehajtását tervező vezetési irányítási és információs rendszer munkacsoportnak. 2003-tól részt veszek az adatkezeléssel kapcsolatos jogszabályok véleményezésében, a NATO elektronikus információbiztonsági albizottság munkacsoportjainak tevékenységében, az MH elektronikus adatkezelő rendszerei védelmének tervezésében, ellenőrzésében, a védelmi feladatokat ellátó állomány képzésében és továbbképzésében, ami a doktori képzés mellett jelentős támogatást jelent céljaim eléréséhez.

Az értekezés elkészítése jelentős kihívás számomra, de *nem végcél*, hanem egy folyamat része, ami jó szakmai alapot teremt az információbiztonság egy-egy részterületének további tanulmányozásához, így *azoknak a kérdéseknek a megvilágítását tekintem elsődlegesnek, amelyek gyakorlatban is támogathatják a szakterület fejlődését.*

A vizsgálandó terület körülhatárolása

Az értekezésben információbiztonság alatt a nemzeti, NATO, EU (és egyéb nemzetközi szerződés hatálya alá tartozó) adatok *szükséges mértékű védettségét értem*. *Jelentőségének növekedése és összetettsége miatt az elektronikus adatok és adatkezelő képességek védelmére koncentrálok, de a szoros összefüggések miatt ezt a területet nem vizsgálhatom elkülönítetten; célom a védelmi kérdések átfogó szemlélete.*

Azt a megközelítést tartom helyesnek, hogy egy közfeladatot ellátó szervezetnél *minden szervezeti célú adatot (és információs rendszert) megfelelő szintű (fenyegetettséggel arányos) védelemben kell részesíteni*, így *értekezésemben az „információvédelem" a „titokvédelem" kategóriánál szélesebb területet fed le. A* titokvédelem az MH érvényben lévő meghatározása szerint *a minősített adatok védelmét jelenti*.

A jogszabályok rendje miatt hazánkban kialakult az a gyakorlat, hogy az „adatvédelem” a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló törvény (Avtv.) hatálya alá tartozó adatok védelmét jelenti, míg az egyéb adatok védelme ettől eltérő (más jogszabályok hatálya alá tartozó) tevékenység. Álláspontom szerint az adatok (és adatkezelő képességek) biztonsága szempontjából nem mérvadó, hogy az adott szintű védelemre vonatkozó követelményt melyik jogszabály határozta meg, így *az „adatvédelem” (vagy „adatok védelme”) kifejezés az értekezésben széles körűen, az érzékeny adatok teljes körére, és nem csak a személyes, illetve a közérdekű adatok védelmére értendő*.

Hazánkban a nemzetközi gyakorlattól eltérő az „információ” az „adat” valamint az ezzel kapcsolatos védelemre vonatkozó kifejezések alkalmazása.

Külföldi források (beleértve a NATO, és EU szabályozását is) az „információ” kifejezést használják. Hazánkban az államtitokról és a szolgálati titokról szóló törvény (Ttv.), az Avtv. és más korszerűen fogalmazó jogszabályok „adat”-ot használnak, de a jogszabályok többségében a két kifejezés vegyes alkalmazása jellemző.

Az MH-nál *a személyes adatok védelmére vonatkozó adatvédelmi területtől való megkülönböztetés érdekében a MINŐSÍTETT és a NEM MINŐSÍTETT (de védendő) adatok védelmére az „információvédelem” kifejezés terjedt el* – ezt a honvédelemről és a Magyar Honvédségről szóló 2004. évi CV. törvény 97.§ p. pontja is így határozza meg –, ami az erőforrások tekintetében folyamatosan szűkülő híradó biztonság mellett a titokvédelem, a rejtjelzés, majd az informatikai fejlődés felgyorsulásával párhuzamosan a számítástechnikai védelem (számítástechnikai titokvédelem, adatvédelem, informatikai védelem stb.) halmaza.

Másfél évtizeddel ezelőtt az információvédelem gyakorlatilag csak rejtjelzést jelentett, ami a szervezeti elemek megnevezésében gyakran még ma is tükröződik. Az ezredfordulót követően – szervezeti változások miatt – megjelent az „elektronikus információvédelem”, és elkezdődött az „információvédelem” kifejezés széles körű tartalommal történő használata, valamint a „titokvédelem” kifejezés háttérbe kerülése.

Amíg a terminológiai kérdések nem tisztázódnak, célszerűnek tartom az „információvédelem” kifejezés használatát, de jelzem, hogy szóhasználatom tartalmilag megfelel a szélesen értelmezett „adatvédelem”-nek.

Az értekezésben a „biztonság” állapotot, míg a „védelem” tevékenységet jelöl (a napi szóhasználatban ezek a kifejezések általában vegyesen fordulnak elő). Az adatok, adatkezelő rendszerek esetében ennek megfelelően a „biztonsági követelmény” és ennek teljesítése érdekében a „védelmi rendszabály” kifejezést használom, és jelzem, hogy *a biztonság*

állapota csak aktív, összehangolt védelmi tevékenységek eredménye lehet, és nem kialakult, örökölt adottság, vagy rejtjelzésre, ügyvitelre egyszerűsíthető tevékenység.

Napjainkban gyakran olvasható az „informatikai biztonság (vagy védelem)” kifejezés „információvédelem” tartalmú használata. Tapasztalataim szerint ez a megközelítés károsan szűkíti a szervezetek által kezelt adatok védelmi feladatait. Az értekezésben az informatikai védelmi feladatok az elektronikus információvédelem részét képezik (ami szűkebb kategória, mint az általános, minden szakfeladatot tartalmazó „információvédelem”).

2006. januárjától kezdve a média a minősített adatvédelmi törvényjavaslat kapcsán olyan vélekedéseknek engedett teret, hogy jogszabályok nem gátolhatják az oknyomozó, tényfeltáró újságírást, és (bizonyos esetekben) nem büntethetik, ha egy újságíró munkája során minősített adatot hoz nyilvánosságra. Az indoklás szerint a védelem állami feladat, és annak hiányosságai nem büntethetnek egy állampolgárt, illetve az újságíró feladata, hogy tevékenységével felhívja a közvélemény figyelmét a védelmért felelős állami szerv hibás működésére.

A hasonló vélekedések nélkülözik a szakmaiságot, tévesen értelmezik az információ szabadságot. Az MH szervezetei által kezelt adatok között vannak olyanok, amelyek illetéktelen felfedése emberéleteket veszélyeztethet, állami küldetések sikerét kockáztatja, ellenséges szándék megvalósulását támogathatja, ami *álláspontom szerint nem lehet egyetlen magyar állampolgár célja sem*. *Értekezésemmel a jogszabályok végrehajtását szolgálom, és nem a meghatározott titokkörök tartalmi helyességét, vagy a kötelezettségek alóli kibújási lehetőségeket vizsgálom.*

Az értekezés elkészítése során *kerülöm a minősített vagy nyilvánosan nem megismerhető adatok felhasználását*. Az érzékeny területek, illetve terjedelmi korlátok miatt nem fejtek ki minden feladatkört részletesen, hanem a szakterület illetékeseivel konzultálva azokat a kérdéseket emelem ki, amelyek elsődlegesek, és nyilvánosan említhetők.

Az anyaggyűjtést 2007. május végén fejeztem be, az értekezés ábráit magam készítettem.

Az értekezésben *az információvédelmi szakterületen keletkezett információk más célú alkalmazhatóságát* – bár ezek felhasználhatóságát felismerem – *nem vizsgálom* (pl. információvédelmi feladatok felhasználása megtévesztési műveletekben).

Egy általános vizsgálat nem kötődhet egy, vagy több eszköz (rendszer) működési sajátosságaihoz, vagy az őket támogató irányzatokhoz, termékekhez, cégekhez, így é*rtekezésem technológia és eszköz független.*

A gazdasági, pénzügyi, személyi lehetőségek gyakran keresztezik a szakmai érdekeket, de ennek ellenére *a súlypontot a szakmai szükségletekre helyezem*. A védelmi rendszabályok hatályba léptetése a vezetés felelőssége, ami a javaslatok, körülmények mérlegelése után *az értekezésben foglaltaktól eltérő döntéseket is eredményezhet.*

Az értekezés kidolgozása során felhalmozódott ismereteket folyamatosan felhasználtam napi munkám során, de a pontos értelmezés érdekében leszögezem, hogy *értekezésem megállapításai nem szervezeti, hanem egyéni álláspontot tükröznek*.

Alkalmazott módszerek és erőforrások

A magyar hadtudomány még sok elméleti és gyakorlati kérdéssel adós az információs rendszerek területén, ami az információbiztonság területén is érzékelhető. Meglévő fogalmi rendszer, vagy felállított modell hiányában a téma bemutatására következő sorrendet állítottam fel: MIÉRT kell védeni az adatokat, MILYEN TERÜLETEKEN kell a védelmet kialakítani, és a HOGYAN KELL SZERVEZNI és FENNTARTANI az információs rendszerek, adatok védelmét.

Az értekezés elkészítésekor a nemzeti, NATO és EU információvédelemmel kapcsolatos jogszabályokra, szabályozókra, ajánlásokra, szabványokra támaszkodtam. Figyelemmel kísértem a témával kapcsolatos elkészített és folyamatban lévő értekezések, tudományos diákköri dolgozatok megállapításait, a hadtudományi és műszaki publikációkat, tudományos rendezvényeket és kiállításokat.

Törekedtem a nemzeti (civil és katonai), valamint NATO szaktanfolyamokon, továbbképzéseken, és munkacsoportüléseken elsajátítottak hasznosítására.

A katonai szervezeteknél, háttérintézményeknél és iparbiztonsági cégeknél napi munkám során folyamatosan konzultáltam, tapasztalatokat gyűjtöttem, és az információs rendszerek kialakítása, fenntartása, valamint a védelmi rendszabályok ellenőrzése, felülvizsgálata során szerzett tapasztalataimat felhasználtam a kidolgozáshoz, és a tanfolyamok, továbbképzések anyagainak naprakésszé tételéhez.

Az értekezés felépítése

A doktori iskolára történő felvételhez készített szinopszist ismereteim bővülésével összhangban pontosítottam, és a kutatási céloknak megfelelően a következő tagolást alakítottam ki:

Első fejezet

Bevezetésként néhány külföldi stratégiára és hasonló szintű hivatalos dokumentumra támaszkodva körvonalazom az *információvédelem szükségességét* és az *elsődleges feladatokat*, bemutatom a hasonló szintű nemzeti kormányzati szintű dokumentumok és a legfontosabb katonai doktrínák megfogalmazásait, a NATO haderőfejlesztési elképzelésében az információbiztonság feladatainak megjelenítését.

Második fejezet

Az adatgyűjtés időszakában felkutatott külföldi és hazai modellek, információbiztonsági szakterületeket említő források vizsgálatával kimutatom a leggyakrabban használt védelmi elemeket.

A kezelt adatok minősítési jelzéseinek függvényében a kritikusnak tekinthető területekre és gyakorlati szempontokra koncentrálva vázolom a védelmi rendszabályok kialakításának logikáját.

Harmadik fejezet

A bemutatott szabályok és feladatok nem működhetnek pontosan kijelölt *felelősségi körök* nélkül. A legfontosabb szervezeti kérdések bemutatása mellé kiválasztottam a *szabályozás,* a *felülvizsgálat* és az *ellenőrzés* MH szempontjából lényegesebb kérdéseit, amelyek – mint az információvédelmi feladatrendszer erőforrásai – támogatják az információkezelő rendszerek biztonságos működését.

Összefoglalás, következtetések, tudományos eredmények kimutatása és ajánlások

Az értekezés további részében összegzem megállapításaimat, ismertetem a tudományos eredményeket, és ajánlásokat teszek az alkalmazhatóságra.

1. AZ INFORMÁCIÓVÉDELEMMEL KAPCSOLATOS FELSŐ SZINTŰ MEGÁLLAPÍTÁSOK

1. 1. Magyar stratégiai szintű megfogalmazások, egyéb követelmények

A Magyar Köztársaság *biztonság- és védelempolitikájának alapelveiről* szóló országgyűlési határozat leszögezi, hogy hazánk a biztonságot több tényező együtteseként, *átfogó módon* értelmezi. Megállapítja, hogy hazánkra a tömegpusztító fegyverek és szállító rendszereik elterjedése mellett fokozódó kihívást és veszélyt jelent az *információs rendszerek elleni támadás lehetősége.*[3.]

A *Nemzeti Biztonsági Stratégia* megállapítja, hogy a rendszerek sebezhetősége olyan kockázati tényező, amelynek jellegzetessége, hogy *kis erőösszpontosítás nagy távolságból is rendkívüli kárt képes okozni*. A technológia rohamos fejlődésének korában új feladatként jelentkezik a *korszerű, biztonságos informatikai infrastruktúra kialakítása* és a *kormányzati információs rendszerek védelme*. A kormányzati információs rendszert fel kell készíteni a kibernetikai támadások megelőzésére és kivédésére. A védelem sikere érdekében szoros koordináció szükséges a szövetségesekkel, valamint az informatikai és távközlési szolgáltatók, kutatóközpontok között. [4.]

A Nemzeti Biztonsági Stratégia által meghatározott, az MH szakfeladatainak megalapozása szempontjából fontos *Informatikai és Információvédelmi Stratégia,* valamint a *Katonai Stratégia még készült el* annak ellenére, hogy az ágazati stratégiák elkészítését a Stratégia 2004. szeptember 30-ig határozta meg.[1]

A Katonai Stratégiával kapcsolatos kényszerű helyzetet jól szemlélteti a vezérkari főnök 2004. évi feladatszabó beszéde: „2003. év végén (…) megkezdődött a nemzeti katonai stratégia kidolgozása. A tervezet várhatóan 2004 márciusára készül el. Az első alkalommal elkészülő nemzeti katonai stratégia alapján át kell dolgoznunk a már elkészült katonai doktrínákat és más szabályozókat”.[2] [5.]

Az információbiztonságra vonatkozó más, *átfogó jellegű, hivatalos kormányzati dokumentum nem áll rendelkezésre*. A kormányhatározattal elrendelt, elkészített, publikált, de jogerőre nem emelt Magyar Információs Társadalom Stratégia (MITS) képezhet még alapvető bemenő adatokat az információbiztonságra vonatkozó központi elgondolások bemutatásához.

---

[1] Az előző, 2002-ben kiadott Nemzeti Biztonsági Stratégia erre már előzőleg 2002. december 31-es határidőt tűzött ki.
[2] Hasonló vezérkari főnöki nyilatkozat hangzott el 2007. februárban, a Katonai Stratégia megjelenését 2007. év végére jelezve.

A MITS megállapítja, hogy a fejlődés következtében a kormányzati szektor és a gazdálkodó szervezetek informatikai rendszerektől való *függősége megnőtt*. Ennek ellenére hazánkban az informatikai biztonság súlya, kezelése *nincs arányban a fontosságával*, nem rendelkezünk egységes módszertannal, és nem követjük a nemzetközi irányzatokat. Az előrelépés érdekében – többek között – a *kritikus infrastruktúrák* kiemelt védelmére, az *információbiztonsági tudatosság* és az ismeretek fejlesztésére van szükség. A célok megvalósítása érdekében megfelelő *jogszabályi és intézményi* környezetet kell kialakítani, ki kell dolgozni a *biztonsági követelményeket*, honosítani kell a *nemzetközi szabványokat*, *kockázatkezelési módszereket kell kifejleszteni, biztonságos információs rendszereket* kell kialakítani, támogatni kell fenntartásukat, valamint *részt kell venni a nemzetközi információtechnológiai (IT) biztonsággal foglalkozó szervezetek munkájában.* [6.]

A MITS Informatikai Biztonsági Részstratégia (IBRS) megállapítja, hogy hazánkban az információvédelem területén *nincs központi felügyelet, irányítás*. Több szervezet, különböző hatáskörökkel, zömében csak a minősített adatok védelméért felelős, a *nemzeti adatok védelme dokumentum centrikus.* A részstratégia megvalósítandó céljai a *technikai infrastruktúra stabilitása* (kockázatkezelés, védett alkalmazások és szolgáltatások, a kritikus infrastruktúra kiemelt védelme), az átfogó *biztonsági szemlélet* kialakítása (biztonság-tudatosság, biztonsági szabványok), a *biztonsági tanúsítási rendszer* működtetése, a számítógépes *vészhelyzeteket kezelő sürgősségi csoportok*, és az érintett szereplők *alapvető jogainak védelme*. Ennek érdekében stratégiai célnak kell tekinteni a *hatékony nemzetközi és nemzeti együttműködés* kialakítását, a biztonságos, hatékony kormányzati információs rendszerek működését, a *kritikus infrastruktúrák kiemelt védelmét*, a rendszerekbe és hálózatokba vetett bizalom erősítését és a *biztonsági tudatosság fejlesztését,* valamint az informatikai rendszerek alanyainak tájékoztatását, és a rájuk vonatkozó alapjogok védelmét.

A részstratégia a kormányzati felelősséget két hatóság felállításával centralizáltan tervezi (általános informatikai biztonsági hatóság, minősített adatokat kezelő rendszereket felügyelő hatóság). [7.]

Az említett dokumentumok egyértelműen megfogalmazzák *hazánkban az információbiztonság fontosságát, szerepének növekedését*. A helyzet bemutatására szolgáló megállapítások az MH-nál is kifejtik hatásukat (pl. a dokumentum centrikusság, a széttagolt kormányzati felelősségből adódó többlet nehézségek, a korszerű módszertanok hiánya). Alapvető hiányosságnak tartom, hogy a MITS a fő irányok, kiemelt programok között összefogva, egységesen tárgyalva *nem szerepelteti a védelmi szféra információbiztonságát*. Szenes Zoltán véleménye szerint a nemzetközi szervezetek által definiált veszélyek,

fenyegetések elemzéseken alapuló konkretizálása, adaptálása hazánkban *kormányzati szinten nem jelent meg*. *Hiányzik a nemzeti biztonság komplex felfogásának elmélete és egységes kormányzati gyakorlata*. Az összkormányzati érdekű, biztonságpolitikai feladatoknak nincs önálló költségvetése, eszközrendszere, a döntések a szaktárcák, hivatalok között elhúzódnak. [8.] *Ezeket a védelmi szférára vonatkozó megállapításokat információbiztonsági területen fokozottan érvényesnek, és veszélyesnek tartom.*

Stratégiai szinten kiemelendő területnek, így megfogalmazandónak tartom a kritikus infrastruktúrákra vonatkozó felső szintű követelményeket, a minimális kormányzati kommunikációs szolgáltatások védelmi szükségletét, és a helyreállításra vonatkozó képességeket, prioritásokat, a kockázatok kezelésének rendjét, a felügyeletért és az üzemeltetésért való felelősséget, a nemzeti IT védelmére, a kutatás és fejlesztés támogatására vonatkozó átfogó irányelveket.

Az MH feladatainak egy része közigazgatási jellegű, így az ebből adódó szolgáltatások kialakításakor az e-kormányzat kialakítását célzó nemzeti stratégia kulcsfontosságúnak ítélt feltételeit is célszerű figyelembe venni:

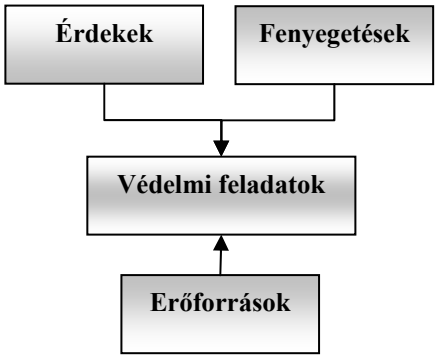
- az állampolgárok biztosak lehessenek abban, hogy működés és ügyintézés közben az adatok nem kerülhetnek illetéktelen kezekbe, illetve
- a személyek, dokumentumok megbízható hitelességgel legyenek azonosíthatók. [9.]

A központi szolgáltatásokra vonatkozó követelmények (a tervezési szakasztól kezdve be kell építeni a *személyes adatok védelmével kapcsolatos feladatokat*, *megbízható azonosításhoz* szükséges infrastruktúrákat és szabályozást kell kialakítani) a honvédelmi tárca egységes kormányzati szolgáltatáshoz csatlakozó rendszerei számára is feladatokat jelentenek. A közszférát és a magánszférát tanácsadással, riasztással és felvilágosítással támogató *hálózat biztonságért felelős központi intézmény felállítására vonatkozó terv összehangolási és együttműködési követelményeket jelent az MH szervezeteinek.*

1. 2. Külföldi megfogalmazások

A nemzeti stratégiai szintű, hivatalos, az információvédelemre vonatkozó megfogalmazások szűkössége miatt célszerűnek tartom a külföldi stratégia szintű dokumentumok információs követelményeire, és ehhez kapcsolódóan az információvédelemre vonatkozó megfogalmazások rövid áttekintését. Célom egy feladatrendszer elemeinek azonosítása, így tudatosan *érdekek*, *kihívások-fenyegetések*,

feladatok és erőforrások szerinti csoportosításban keresem az információvédelemre vonatkozó megfogalmazásokat.



1. ábra: Az információk védelmének befolyásoló tényezői

1. 2. 1. Érdekek

Az Európai Parlament és Európa Tanács megfogalmazása szerint a hírközlési és az információs rendszerek *a gazdasági és társadalmi fejlődés alapvető tényezőjévé váltak*. A számítástechnikai hálózatok a villamos energiához, vagy a vízellátáshoz hasonlóan *mindenütt jelenlévő szolgáltatások. Az információs rendszerek elérhetősége, biztonsága egyre fontosabb a társadalom számára*. [10.]

A területek, állampolgárok védelme mellett alapvető érdekként megjelenik az államok működése szempontjából *kritikus* (egyes megfogalmazások szerint létfontosságú) *infrastruktúrák* megléte és működése (critical infrastructures). [11.] Ez a kategória az energia hálózatokat, pénzügyi és bankrendszereket, a szállítást, vízellátó-, kormányzati és vészhelyzeti rendszereket, valamint az *azokat támogató információs rendszereket* tartalmazza.

Orosz megfogalmazás szerint információs területen nemzeti érdek az alkotmányos állampolgári jogok-, az *információk szabad beszerzésének és felhasználásának* biztosítása, a korszerű *telekommunikációs technológiák fejlődésének* biztosítása, valamint az állami információs források *jogosulatlan hozzáférés elleni védelme*. [12.]

1. 2. 2. Kihívások és fenyegetések

Az EU Biztonsági Stratégia megállapítja, hogy *a kereskedelem, a befektetések, a technikai fejlődés erősítik Európa függőségét* – így sebezhetőségét – az összekapcsolt szállítási, energia, információ és egyéb infrastruktúrákon keresztül. [13.]

A rendszerek összetettsége, a balesetek és hibák, vagy támadások miatt bekövetkezett problémák hatással lehetnek az EU polgárainak jóléte szempontjából kritikus szolgáltatásokat közvetítő fizikai infrastruktúrákra. [14.]

A NATO Stratégiai Koncepció szerint állami és nem állami ellenfelek megpróbálhatják kihasználni a Szövetség függőségét az információs rendszerektől úgy, hogy információs műveletekkel *működésképtelenné teszik a rendszereket*. [15.]

Az észt biztonsági koncepció szerint az elektronikus információs rendszerek használatának növekedése, illetve csatlakozása a globális információs rendszerekhez növeli a *számítógépes bűnözéssel kapcsolatos kockázatokat* és a *nemzeti információs rendszerek sebezhetőségét*. Fenyegetést jelent az alkalmazott elektronikus adatkezelő rendszerek *instabilitása*, *üzemzavara*, a *rendszerek számának folyamatos növekedése*, függőségük a világméretű rendszerektől, a *számítógépes bűnözés növekedése*, valamint az információs rendszerek (beleértve a nemzet biztonsága szempontjából létfontosságú rendszereket) *sebezhetőségének növekedése*. Évente nő azok száma, akik internethez kapcsolódó tevékenységükkel kormányzati adatbázisokat, nyilvántartásokat veszélyeztethetnek. [16.]

Az osztrák biztonságra vonatkozó doktrína szerint a stratégiailag fontos infrastruktúrák ellen irányuló felforgató tevékenység, a terrortámadás, vagy azzal való fenyegetés hatását növelik az új rendelkezésre álló lehetőségek (tömegpusztító fegyverek és IT). *Az ilyen fenyegetések kormányzati és nem kormányzati erőktől, szervezett bűnözök csoportjától vagy egyéni bűnözőktől eredhetnek, és előzetes figyelmeztetés nélkül is feltűnhetnek.* [17.]

Kanadai kormányzati álláspont szerint a *számítógépes támadás és az interneten keresztül történő rosszindulatú tevékenységek* gyakori, súlyos károkat okozhatnak a kritikus infrastruktúrákban és az elektronikus szolgáltatásokban. [18.]

Orosz megfogalmazás szerint fenyegetésnek kell tekinteni a védelmi rendszert és az információbiztonságot szolgáló feladatok hosszú távú *alulfinanszírozottságát*, az *oktatási rendszer hatékonyságának csökkenését,* valamint a *jól képzett szakemberek hiányát, elvándorlását*. [19.]

A litván biztonsági stratégia az előbbieket azzal egészíti ki, hogy a minősített adatok illetéktelen megismerése, vagy az ilyen információk szivárgása *nem csak egyszerűen fenyegeti a nemzet biztonságát, hanem más államok irányában aláássa a nemzet megbízhatóságát*. [20.]

Az orosz koncepció szerint súlyos fenyegetés lehet egyes államok részéről *az általános információs fölényre való törekvés*, az állam (megjegyzés: Oroszország) *kiszorítása a külföldi és belföldi információs piacokról*. Az információs hadviselés különböző koncepcióinak kidolgozása és alkalmazása nehezen felbecsült hatásokat fejthet ki más államok információs rendszereire *az adatkezelő rendszerek működésének akadályozása*, és *az illetéktelen hozzáférések formájában*. [21.]

A növekvő terroristafenyegetést fogalmazza meg az Egyesült Államok Belbiztonsági Stratégiája, mely szerint terrorista csoportok akciók tervezéséhez, anyagi alapjaik növeléséhez, propagandájuk terjesztéséhez, adatgyűjtéshez, valamint biztonságos kommunikációs megoldások kialakítása érdekében *kihasználják az IT és az internet előnyeit*. A terroristák továbbfejlesztik technikai képességeiket, feltérképezik lehetséges céljaikat, így *a számítógépes támadások jelentősen veszélyesebbé válnak*. Folyamatosan keresik az új sebezhetőségeket, és a meglepetés, a megsemmisítő hatás növelése érdekében felhasználják korábbi tapasztalataikat. [22.]

1. 2. 3. Feladatok és erőforrások

Az információvédelemnél tágabb tartalmú, de igen kifejező az EU Biztonsági Stratégia általános követelménye, mely szerint „(…..) a cselekvésre készen kell állni már a krízisek bekövetkezése előtt. A konfliktusok és fenyegetések megelőzését nem lehet elég korán elkezdeni.” [23.]

Az Európai Parlament és Európa Tanács határozata szerint a köz- és a magánszférában egyaránt megfelelő, a „bevált gyakorlat (best practise)” elvén alapuló *kockázatelemzési és menedzselési eljárások kifejlesztése, bevezetése* növeli az európai hálózatok és rendszerek biztonságának szintjét, így a biztonságpolitikákat *jól kialakított kockázatelemzési eljárásokkal kell megalapozni*. *A hálózati és információbiztonsági problémák globális kérdéseknek tekintendők*. Az egységes megközelítés érdekében *felső szintű, szoros együttműködésre van szükség a biztonsági szabványok tökéletesítése, valamint a hálózati és információvédelmi kérdések területén*. [24.]

Az Európai Közösségek Bizottsága a kutatás, a nyitott szabványok kidolgozásának elősegítésével, az érdekeltek párbeszédének támogatásával, illetve szükség szerint kötelező érvényű eszközök alkalmazásával kívánja ösztönözni az „egymással kommunikáló” technológiákat. Cél egy *biztonságos információs társadalmat célzó stratégia kialakítása*, ami egységes rendszerbe foglalja a rendelkezésre álló eszközöket, köztük az *önvédelem szükségességével kapcsolatos tudatosság erősítését*, a *fenyegetések folyamatos figyelését*, illetőleg a *támadásokra, és a rendszerhibákra való gyors és hatékony válaszadást*. Az információs és kommunikációs technológiákra vonatkozó kutatásokba történő befektetések és az innováció megerősítésének területei a *tudás*-, a *tartalom*- és a *kreativitás technológiái* (ideértve a kognitív, a szimulációs és a vizualizációs technológiákat is), a *fejlett és nyitott kommunikációs hálózatok*, a *megbízható szoftverek*, és a *nanoelektronika*. A bizottság állásfoglalása szerint támogatni kell a „beépített” védelemre irányuló kutatásokat, és a

személyazonosság-kezelés megoldását célzó alkalmazások bevezetését, és meg kell fontolni a szabályozás felülvizsgálatát, különösen a magánélet védelme, az elektronikus aláírás, és az illegális és káros tartalom elleni fellépés területén. [25.]

A prágai NATO csúcstalálkozó 2002-ben megerősítette, hogy az 1999-es Védelmi Képességek Kezdeményezés (Defence Capability Initiative; DCI) kiterjesztéseként növelni kell a képességeket a *felderítés*, a *megfigyelés*, a *levegő-föld megfigyelés,* és a *vezetési, irányítási és kommunikációs* területeken. Új elemként jelenik meg, hogy *erősíteni kell a képességeket a számítástechnikai támadások ellen.*

Az isztambuli NATO csúcstalálkozón a Védelmi Tervező Tanács miniszteri szekciójának 2004. június 27-i ülésén *a védelmi miniszterek megerősítették a prágai Védelmi Képességek Kezdeményezés célkitűzéseit.*

A 2006-os rigai NATO csúcstalálkozón kialakított politikai irányelvek szerint a Szövetség működése *hatékony felderítési és információ megosztási képességeket igényel*. Kritikus fontosságúnak kell tekinteni a szövetségi információs rendszerek *számítástechnikai támadások elleni védelmét*. Az időben történő tervezés és döntéshozatal, a gyorsan telepíthető, összhaderőnemi expedíciós erők legnagyobb hatásfokának elérése érdekében növekednek a vezetők, szenzorok és fegyverek közötti kapcsolatok. Emiatt *prioritásként kell kezelni az aszimmetrikus fenyegetések kezeléséhez szükséges képességeket*, az *információs fölényt*. [26.]

Észt megfogalmazás szerint *az új biztonsági kockázatok nemzeti szervezetek közötti összehangolt választ, és széles nemzetközi együttműködést kívánnak. Kiemelt figyelmet kell fordítani a kormányzati adatbázisok és nyilvántartások védelmére*. [27.]

Kanadai kormányzati álláspont szerint feladat egy helyzetjelentés összeállítása az állami kritikus infrastruktúra kulcsfontosságú elemeiről. Emellett a számítógépes támadások előrejelzése és megelőzése érdekében növelni kell a kormányzati képességeket. A magánszektor és a közszféra képviselőiből munkacsoportot kell alakítani a nemzeti informatikai védelmi (cyber-security) stratégia kialakítása érdekében. [28.]

Osztrák megfogalmazás szerint cél *az intenzív és optimalizált gyakorlás, a nemzeti/nemzetközi szintű információcsere* – különösen a terrorizmus és a nemzetközi bűnözés megelőzése érdekében –, az összetett katasztrófavédelmi rendszer kialakítása, valamint az általános biztonságpolitika mellett *ágazati stratégiák kialakítása az infrastruktúrák és információs területeken*. [29.]

A litván biztonsági stratégia szerint feladat *az IT biztonság nemzetközi szabványokkal összhangban lévő jogszabályokkal történő szabályozása*, a létfontosságú információs

rendszerek védelmének erősítése, valamint az IT és adatok védelme érdekében kialakított rendszabályok *megfelelő felügyelete*. [30.]

Az utóbbi években jelentősen növekvő terroristacselekmények hatására az információvédelemre is vonatkozó megállapítások, követelmények jelentek meg.

A NATO Stratégiai Koncepció általános követelménye, hogy *a katonai erőt és infrastruktúrákat meg kell védeni a terrortámadások ellen*. [31.]

Az Egyesült Királyság Védelmi Felülvizsgálatának kiegészítése szerint a terrorizmussal kapcsolatban az a legfontosabb, hogy *pontosan meg kell érteni a fenyegetéseket,* majd objektív módszerekkel felül kell vizsgálni a fejlett demokratikus közösségek sebezhetőségét, és meg kell tenni a megfelelő védelmi lépéseket. [32.]

Az Egyesült Államok Belbiztonsági Stratégiájának megállapítása szerint a gazdasági és kormányzati szféra speciális létesítményeinek terrortámadások általi sebezhetőségének vizsgálatára *projekteket kell kialakítani*. *A védelem kialakításakor ki kell használni a számítógépes elemzés korszerű lehetőségeit.* A mai kor terroristái másképp gondolkoznak, mint régebben, így a védelemnek meg kell ismerni ezt az észjárást. Meg kell tanulni, hogyan alakulnak ki a terroristák hosszú távú tervei, és hogyan történik a célok kiválasztása. A védelemnek a *terroristák képességeinek és elemző módszereinek felhasználásával* kell feltárni a rendszerek sebezhető pontjait és meg kell állapítani a létfontosságú infrastruktúrák kiemelt célpontjainak felkészültségét (Vörös Csoport (Red Team) módszer alkalmazása). A kritikus infrastruktúra egy, vagy több részét érő terrortámadás jelentős károkat okozva egész rendszerek működését béníthatja meg, így *növelni kell az elkülönült elemek és összekapcsolt hálózatok védelmét*. Fontos annak megértése, hogy a kritikus infrastruktúrák, kulcsfontosságú létesítmények védelme nem csak a terrortámadás elleni védelmet szolgálja, hanem csökkenti a természeti katasztrófák-, a szervezett bűnözés-, vagy a hacker támadások elleni sebezhetőséget. [33.]

A bemutatott megfogalmazások alapján megállapítom, hogy *szakmai szempontból a magyar nemzeti stratégiai megfogalmazás korszerűnek tekinthető*. Ugyanakkor megállapítható az is, hogy külföldi megfogalmazások lényegesen szélesebb területeken fogalmaznak meg célokat és feladatokat, mint a magyar, lényegében a fenyegetés érzékeltetésére, az infrastruktúra védelmére történő felkészülés fontosságára, és a koordináció szükségességére mutató stratégia.

A külföldi stratégiai dokumentumokban információvédelmi területen megjelenik a kutatás-fejlesztés, a szabványosítás fontossága, az együttműködés, információcsere

szükségessége a felkészülés és elhárítás kapcsán, a kritikus infrastruktúrák esetében a gyors érzékelési és reagálási képességek kifejlesztésének és karbantartásának szükségessége (beleértve a kockázatelemzés, képzés és gyakoroltatás feladatait is), illetve az ezeket támogató átfogó, központi kormányzati programok fontossága. A különböző súlyú, terrorizmust is tartalmazó fenyegetésekre, sebezhetőség feltárására és kiküszöbölésére történő felkészülés eredményei széleskörűen alkalmazhatók a nemzeti infrastruktúrák üzemeltetése során.

Az állam adatokra vonatkozó védelmi feladatainál megjelenik a nemzetközi kötelezettségvállalások teljesítésének fontossága, ami egyben a nemzetközi bizalom záloga is.

A stratégiai szintű dokumentumok információvédelmi szakterületű vizsgálatán keresztül látható, hogy *a feladatok összetettsége már felső szinten is megkívánja a strukturált megközelítést*. Több nemzeti stratégiai rendszernél jól felismerhető a nemzeti biztonsági-, a védelmi-, a katonai és az információvédelmi szakterületre bontott hierarchia. Ez a hazánkban hiányzó struktúra biztosítja a célok és feladatok szűkítését, és az alkalmazó szervezetek által kialakítandó feladatrendszer pontosabb illesztési lehetőségeit.

A nem tervezett, de véleményem szerint szükséges védelmi-, az információvédelmi-, és a katonai stratégia adhatja azt a felső szintű támogatást, amiből a tárca számára meghatározott feladatok, a katonai sajátosságok figyelembe vételével le lehet bontani az MH-ra vonatkozó információvédelmi követelményeket, és meg lehet határozni a szükséges szakterületi kapcsolódási pontokat.

Az idézett társadalmi stratégia tervezet – bár bemutatott megállapításai helyesek – nem jóváhagyott dokumentum, így a nagyszámú hivatkozás ellenére nem tekinthető az említett hiányzó stratégiák pótlásának. Szakmai szempontból *hátrányként értékelem, hogy a publikált anyag az eltelt majd három év alatt nem fejlődött tovább, nem egészült ki az EU csatlakozásból adódó kérdésekkel, a NATO 2003 óta kiadott állásfoglalásaival*. Az értekezés második és a harmadik fejezetében később láthatóvá válik, hogy a különböző felelősségi körrel felruházott kormányzati szervezetek mennyire veszik figyelembe a dokumentum rendszabályok összehangolására, egységes biztonsági szemléletre és szervezeti integrálásra vonatkozó megfogalmazásait.

Megállapítom továbbá, hogy a stratégia-tervezet az MH szervezeteinek működése és vezetése szempontjából kiemelt fontosságú minősített adatok kezelésével, védelmével kapcsolatos részei nem tekinthetők olyan szinten kidolgozottnak, hogy központilag irányt határozzanak meg a jogalkotók felé, és támogassák a nemzeti adatkezelő képességek egységes kezelését, és a szövetségi képességekhez történő csatlakozását.

1. 3. Az MH doktrínák információvédelemmel kapcsolatos megfogalmazásai

Az összhaderőnemi és funkcionális doktrínákban az információbiztonságra vonatkozó elgondolásoknak átfogóan tükröződnie kell, így szükségét látom az MH doktrinális szabályozói szint rövid áttekintésének.

A jelenlegi doktrínarendszer többlépcsős átalakításon keresztül alakult ki. A 2001-es korszerűsítésekor a vezetési hadviselés a modern törzs felosztás szerinti 6-os blokkból (híradás és informatika) „információs műveletek"-ként átkerült a 3-as blokkba (hadművelet), az elektronikai hadviselés a 2-es blokkba (felderítés).[3] Az Összhaderőnemi Vezetési Doktrína alatt egy híradó, egy informatikai és egy „titokvédelem (biztonság)" megnevezésű funkcionális doktrína volt, amely hármas felosztást a 2004-es doktrínarendszer-felülvizsgálat egy dokumentummal (híradó és informatikai doktrínával) váltott ki.[4]

Az MH Összhaderőnemi Doktrína (MH ÖHD) a NATO, és más nemzetek (pl. amerikai, brit, ausztrál) összhaderőnemi doktrínájához hasonlóan – bár nem teljes fogalmi letisztultsággal –, de *tartalmazza az információs műveleteket és a vezetési hadviselést*. Az információs műveletek az általánosan elfogadott támadó és védelmi területből állnak, nemzetközileg elfogadott (később ismertetett) elemekből kialakítottak, de *logikai hiba, hogy az elemek a doktrína önálló fejezeteiként szerepelnek, és nem eredeti struktúrájuk szerint tagoltak*.

A műveleti biztonságon belül fogalmi keveredés tapasztalható, mert a rendszabályok *aktív rendszabályokra* (a meghatározás szerint ez fizikai megsemmisítésként azonosítható), *vezetési és irányítási hadviselésre* (ez tévedés, mert a vezetési és irányítási hadviselés tartalmazza a műveleti biztonságot és nem fordítva), *megtévesztés és lélektani hadviselésre* (ez szintén tévedés, mert ezek a területek a műveleti biztonságnak mellérendeltek), valamint a *védelmi rendszabályokra* osztottak.

A doktrína a *műveleti biztonság folyamatát* a nemzetközi forrásoknak megfelelően tárgyalja (a kritikus információk azonosítása, a fenyegetettség és sebezhetőség elemzése, a védelmi rendszabályok kiválasztása és alkalmazása).

A védelmi rendszabályok a *személyi állomány biztonságát*, a *fizikai védelmet* (ami tartalmazza a minősített adatok védelmét és a létesítmények támadás elleni védelmét), az

---

[3] A megelőző, 1999-es doktrínarendszerben a törzs 6-os blokkja a katonai vezetés, az összhaderőnemi híradás, informatika, vezetési és irányítási hadviselés, elektronikai hadviselés és titokvédelmi ügyvitel, a 3-as blokkja a hadműveleti vezetés és irányítás témaköröket tartalmazta.

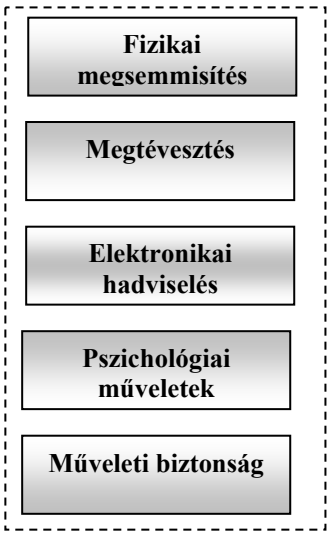
[4] A jól kidolgozottnak tekinthető amerikai, brit, ausztrál, kanadai vagy a NATO doktrínarendszerben szintén nincs önálló vezetési, illetve információvédelmi doktrína.

álcázás és rejtést, valamint nem egyértelműen fogalmazva a *dokumentumok biztonságát*, az *információs biztonságot* és a *számítástechnikai biztonságot* tartalmazzák.

A híradó és informatikai rendszerek biztonsága a fizikailag védett környezet, az áramló információk rejtése, a rendszerbe történő behatolás észlelése és kezelése feladatokat tartalmazza *rejtettségre* (a fizikai védelem mellett a híradó és informatikai rendszer része az elektronikus információbiztonság és az informatikai biztonság), és *információvédelemre* bontva. Ezen kívül önálló elektronikus információvédelem címszó alatt gyakorlatilag a rejtjelzés, és az információ megszerzése esetén történő haladéktalan ellentevékenység szerepel. [34.]

A tapasztalt ellentmondások, átfedések miatt szükségesnek tartom annak vizsgálatát, hogy a magyar hadtudományi publikációk hogyan tárgyalják az érintett területeket.

Haig Zsolt 1998-ban bemutatta az információs/vezetési hadviselés alapvető jellegzetességeit, a vezetési hadviselés alapvetően öt, a helyzetnek megfelelően súlyozott elemét (2. sz. ábra). [35.]



2. ábra: Az információs műveletek/vezetési hadviselés főbb összetevői

Más magyar források is ezt az álláspontot fejezik ki, kiegészítve *a felderítés és a híradó és informatikai rendszer támogatásának fontosságával*. [36.] [37.]

Munk Sándor 2002-ben megvilágította, hogy a támadó és védelmi információs műveletek során az elemeknek *egymással párban kell szemben állniuk* (pl. a fizikai megsemmisítéssel szemben fizikai védelem), mivel az ellenség is hasonló elgondolások szerint építi fel műveleteit. [38.] A pszichológiai hadviselés, az elektronikus hadviselés egyaránt része lehet támadó és védelmi műveleteknek, és nyilvánvaló, hogy a különböző műveletekben más-más feladatokat fognak ellátni.

Az öt szakterület Haig Zsolt –Várhegyi István szerint *számítógép hálózati hadviseléssel*, a *polgári-katonai együttműködéssel* és a *tömegtájékoztatással* egészül ki. [39.]

Haig Zsolt említett publikációjában a hadműveleti biztonság feladatának a *kritikus* (az ellenség számára fontos) *információk* azonosítását, valamint ezek alapján a sebezhetőség csökkentését látja, és összetevőként a *felderítés elleni védelmet*, az *információvédelmet*, a *híradás védelmét* és a *fizikai őrzésvédelmet* azonosítja. [40.]

A had*műveleti biztonság* feladatait megvilágíthatja az a megközelítés, amely az információs rendszereket érő fenyegetések szerint csoportosítja a védelmi lehetőségeket. Makkay Imre 1997-ben a rendszerek védelmét a *zavarás*, a *pusztítás* és az *információk felhasználása ellen* kialakított rendszabályokból állította össze. [41.]

A Várhegyi-Makkai szerzőpáros a hadműveleti biztonság hatáskörét a saját csapatok védelmén kívül *kiterjeszette a szövetséges és semleges lakosság védelmére is*.[5] [42.]

Az értekezés vonalától eltérítene az információs műveletek, vagy annak összetevőinek részletes elemzése, így az eddigiek alapján csak annyit szögezek le, hogy a támadó és védelmi információs műveletek során *védeni kell a katonai szervezetek erejét és képességeit, ami a vezetéshez és működéshez szükséges adatok védelme nélkül nem valósítható meg.* Az MH ÖHD az információs műveletek összetevőit pontatlanul azonosítja. Az információvédelemre vonatkozó adatok ellentmondásosak, illetve eltérő szempontok szerint, két helyen szerepelnek (információs műveletek, híradó és informatikai rendszer).

Az MH Légierő Doktrína az információbiztonságot gyakorlatilag nem emeli ki. A doktrínában a „biztonság” fogalmánál közvetetten érzékelhető, hogy az információk védelmére is szükség van (pl. a biztonság, mint alapelv betartásával „csökkenthető a saját erők sebezhetősége…”, valamint „A biztonság elvének természetesen nem csak a védelmi, hanem a támadó jellegű tevékenységek végrehajtásakor is érvényesülnie kell.”). Más megfogalmazások szerint a korszerű technikai eszközökkel vívott fegyveres küzdelmekben „meghatározó jelleggel bír az információvédelem”, és „az ellenség hasonló tevékenységére adott válasz”, valamint „az információs fölény (…) a légi fölényhez hasonlóan meghatározó jelentőségű”.

Az információs műveletek szempontjából pozitívumként értékelem az elektronikai hadviselés hatékony alkalmazásának, és a műveletekbe történő integrálásának említését. [43.]

---

[5] A szerzők szerint a hadműveleti biztonság rendkívül összetett kategória; rendszabályait *felderítés elleni tevékenységre*, *híradásvédelemre*, *elektromágneses zavarás és impulzuscsapás elleni védelemre*, *információvédelemre*, *fizikai őrzésvédelemre* és *kémelhárításra* bontják.

Az MH Összhaderőnemi Logisztikai Doktrína a logisztikai támogatás vezetésének sajátosságainál alapfeltételként említi a *megbízható vezetési rendszert*, valamint a logisztikai támogatás vezetésének alapelvei között a *folyamatosság*, az *operativitás*, és az *interoperabilitás* szerepel, amely fogalmak nem képzelhetők el korszerű információvédelem nélkül. A rejtett vezetési eszközök alkalmazása elősegítheti az erők és eszközök megóvását, a logisztikai támogató rendszerek túlélőképességét.

A többnemzetiségű műveletek logisztikai támogatásának megtervezése és megszervezése szempontjából kiemelendő feladat a vezetési eszközök és eljárási módszerek *szabványosítása*, az *aktív összeköttetés*, az *együttműködés*, a *kiképzés* és a *felkészítés*.

A doktrína nem tér ki a biztonsági funkciókat megvalósító eszközökkel és eljárásokkal kapcsolatos feladatokra, de az életciklus állomások azonosításával helyesen adja meg az ellátás tervezésétől, a rendszerbe állítástól a rendszerből történő kivonásig az általános feladatokat. Az ellátás területén meghatározza, hogy a raktáraknak ki kell elégíteni a különböző hadianyagok tárolásával szemben támasztott *biztonsági követelményeket*. [44.]

A doktrínák tanulmányozása alapján *megállapítom, hogy a magyar hadtudományi kutatások eredményei az információs műveletek nem minden területén jelentek meg.*

- Az MH ÖHD-ban a korszerű magyar hadtudományi eredményekre támaszkodva célszerű megjeleníteni az információs műveleteket/vezetési hadviselést. *Összetevőit szakszerűen formába kell önteni, és egy közös fejezetben, strukturáltan, ellentmondásmentesen kell tárgyalni.* Továbblépés lenne, ha a műveleti biztonság megvalósítását szolgáló folyamat bontásával kiderülnének azok az alapelvek, módszerek, amelyek támogatják ezeket a feladatokat. Az MH vezetéséhez és működéséhez szükséges adatok biztonsága érdekében *a védelmet nem csak a híradó és informatikai rendszer részeként kell kezelni, hanem a komplex fenyegetéseknek megfelelően, egységesen értelmezve az információs műveletekbe beágyazva célszerű kialakítani.*
- Amennyiben az összhaderőnemi doktrínában a hadtudományi forrásoknak megfelelően megjelennek az információs műveletek korszerű összetevői, kiemelt figyelmet kell fordítani az információvédelem és az esetlegesen megjelenő számítógép hálózati hadviselés feladatainak megfogalmazására, mert *a hálózatok védelmére vonatkozó meghatározások, elvek nem fogalmazhatók meg eltérően az elektronikus információvédelem szakterületén belül, valamint számítógépes hálózati védelem (Computer Network Defense; CND) címszó alatt*.

- Az MH Légierő Doktrínában a támogatási tevékenységeknél, a légierővel szemben támasztott alapvető követelményeknél, a vezetési és irányítás alapelvei fejezeteknél célszerű lenne a haderőnemi sajátosságoknak megfelelő, korszerű információbiztonsági követelmények, alapelvek bemutatása.
- A logisztikai szakterület sajátosságainak megfelelő információvédelmi feladatok nem jelennek meg az MH Összhaderőnemi Logisztikai Doktrínában (pl. a logisztikai folyamatok információbiztonsági igénye, az MH információbiztonságával – mint a logisztikai folyamatok egyik tárgyával – kapcsolatos speciális követelmények). Megjeleníthető a műveletek támogatásához szükséges kritikus infrastruktúra fenyegetéssel arányos védelmi szükséglete, a központi logisztikai adatbázisokkal kapcsolatos védelmi rendszabályok (pl. hozzáférés védelem, távoli elérés, felelősség az adatok pontosságáért, adatbázis replikáció), a beruházási és beszerzési folyamatok során a biztonsággal kapcsolatos feladatok meghatározásának követelménye, a hardver/szoftver vagy rejtjelző eszköz beszerzéssel kapcsolatos biztonsági alapelvek, a minősített adatkezelő infrastruktúrák kialakításával és fenntartásával kapcsolatos feladatok.

1. 4. A NATO haderő-fejlesztés és egyéb nemzeti információs követelmények

A bemutatott nemzeti megfogalmazások mellett szükségét látom a haderőfejlesztésre vonatkozó NATO átfogó követelményrendszer információs vonzatainak rövid bemutatásának, ami szövetségi tagságunk által nyilvánvalóan a fejlesztések alapját kell, hogy képezze.

Az elméletet megalapozó cikkben Arthur K. Cebrowski és John J. Garstka kifejtik, hogy a hadviselés új formája a hálózat centrikus hadviselés (Network Centric Warfare; NCW) hozzájárul a *vezetés felgyorsulásához,* és lehetővé teszi az erők *teljes mélységű szervezését és összehangolását.* [45.] Elemei a *nagyteljesítményű hálózat* a szükséges információs források és fegyverek eléréséhez, a *precíziós csapások és nagysebességű manőverek*, az értéknövelt információs folyamatokban megnyilvánuló *vezetési és irányítási rendszer* (Command and Control; C2), valamint az integrált, fegyverirányítással és C2 folyamatokkal összekapcsolt *szenzorhálózatok*. A gyorsabb vezetés alapja az *információs fölény*, az *erők sebességben, precizitásban és reagáló képességben megnyilvánuló hatás alapú alkalmazása* (Effect Based Operation; EBO), és ez által *az ellenség stratégiájának és tevékenységének megzavarása,* ami a mennyiségekben, technológiában vagy helyzetben jelentkező *hátrányok ellensúlyozását teszi lehetővé*.

A NATO Transzformációs Parancsnokság (ACT) megfogalmazása szerint a NATO hálózat által biztosított képesség (NATO Network Enabled Capability; NNEC) célja olyan környezet biztosítása, ahol az adatgyűjtő elemek, döntéshozók, és a szükséges hatásokat kiváltó erők egy hálózatokból álló hálózatba integrálódnak, biztosítva a felhasználók számára a szükséges adatokat bármely helyszínről, a megfelelő formában és szükséges időben. [46.]

A NATO Stratégiai Vízió (The Military Challenge[6]) helyzetértékelésként megállapítja, hogy a Szövetség szélesen értelmezett, számtalan tényező által befolyásolt stratégiai környezetben működik (globalizáció, megoldatlan konfliktusok, radikális ideológia, valamint az egyre bonyolultabb aszimmetrikus kihívások).

A *hatás alapú* megközelítés a Szövetség katonai és nem katonai erejének összetett, integrált, minden vezetési szinten, a konfliktusok teljes skálájánál történő alkalmazása. E képesség eléréséhez fejleszteni kell a *felderítést*, az *adatok megosztását*, az *előrejelzést.* Robosztus és rugalmas híradó és informatikai rendszereken alapuló *hálózat alapú képességeket kell kialakítani a hadműveleti környezet teljes körű ismerete, és a megelőző jellegű beavatkozás érdekében.*

A hatás alapú műveletek az erők és képességek széleskörű integrációját kívánják a *döntési fölény* (Decision Superiority), a *koherens hatások* (Coherent Effects), és az *összhaderőnemi telepíthető és fenntartható erők* (Joint Deployment and Sustainment) érdekében.

A *döntési fölény* kritikusan függ az *információs fölény kialakításától* és fenntartásától, valamint a műveletek minden fázisában a *helyzetismeretre vonatkozó adatok megosztásától*. A döntési fölény alapja a hadműveleti helyzet ellenséghez képest jobb megértése, és a *döntési ciklus napokban mért hosszának órákra, percekre történő csökkenése*. Az új vezetési és irányítási rendszereknek lehetővé kell tennie az információs fölény átalakítását *akcióképes ismeretté*, ez által támogatva a gyorsabb tervezést, a jobb döntéseket, és a döntő hatások elérését. Az erők alkalmazása, a döntési fölény kialakítása egy együttműködő, *globálisan integrált hadműveleti hálózati környezetben képzelhető el*, ahol a hálózat lehetővé teszi a katonai erők, a nemzetközi, nemzeti, és nem kormányzati szereplők azonos elvek szerinti tervező, elemző, és végrehajtást biztosító környezetben történő csatlakozását. Ebben a környezetben kulcsfontosságú tényező az *interoperabilitás*. A hálózat alapú képesség birtokában a műveletek vezetése pontosabb helyzetismereten alapul, bizalmas adatkezelő

[6] The Military Challenge: A Katonai Kihívás.

műveleteket alkalmaz, szorosan felügyelt, közel valós idejű adatgyűjtésre és fúzióra, elemzésre, és gyorsabb döntési képességre támaszkodik.

Koherens hatás akkor érhető el, ha *a katonai erők integrálják képességeiket a Szövetség minden eszközével, erőforrásával és hadműveleti területen a katonai műveletek és nemzetközi, nemzeti, valamint nem kormányzati szereplők erőfeszítései szorosan összehangoltak*. Kritikus az erők elhelyezése, a megfigyelés, az észlelés, a célok azonosítása és követése, a kívánt hatások megtétele, a következmények elemzése, és jobb helyzetismerettel, folyamatos elemzéssel, konzultációkkal támogatva az erők szükség szerinti újbóli alkalmazása.

Az *összhaderőnemi telepíthetőség és fenntarthatóság* lehetővé teszi a Szövetség folyamatos, elosztott, vagy nem folyamatos műveletekre szabott erőinek időbeni alkalmazását, és a műveletek támogatását bárhol, ahol arra szükség van. [47.]

A döntési fölény – és a másik két cél – támogatására szolgáló hálózat alapú képesség kialakítása érdekében több tagállam összefogásával 2004-ben kezdődött kutatás, melynek eredménye a NATO NEC (NNEC) megvalósíthatósági tanulmány (NNEC Feasibility Study).

A tanulmány a hálózatosított információs infrastruktúrára vonatkozó szükségleteket a következők szerint határozza meg:

- *a hálózati képességek kiterjesztése* („bárhol ahol szükséges, bármikor, amikor szükséges”);
- *a kisebb, moduláris rendszerű, többnemzetiségű erők támogatása* (új típusú információ megosztási és biztonsági követelmények, valamint interoperabilitásra vonatkozó elvek szükségessége);
- *a nemzeti elemek rotációjának támogatása, valamint az interoperabilitási követelményeket nem teljesítő, nem NATO nemzetek támogatása* a NATO Reagáló Erők (NRF) kötelékein belül.

A NATO tanulmányban megmutatkozik a hálózat alapú képesség három egymással átfedésben, és szoros összefüggésben lévő dimenziója: a *hálózatok* (hozzáférés, rugalmasság, menedzsment és technikai interoperabilitás), az *információ* (előállítás, hozzáférhetőség, a védelem és a biztonság szükséges szintjének szavatolása) és az *emberek* (egyéni és csoportos oktatás és képzés, team típusú képzés, interoperabilitás).

Az *információvédelmi mechanizmusok* az információs infrastruktúra minden területére beépülve, egymással együttműködve fejtik ki hatásukat. Biztosítják, hogy a megfelelő személyektől, a kellő időben rendelkezésre bocsátott információ valóban megbízható (trusted)

legyen, így megvalósul az elterjedőben lévő információ megosztásra vonatkozó elv (duty to share), kiegészítve a szükséges, hogy tudja (need to know) elvvel. A megosztásra vonatkozó elv alkalmazása lehetővé teszi, hogy a rendszerek tervezésekor, alkalmazásakor a politikák, eljárások tartalmazzák az ehhez szükséges képességeket; ugyanakkor a védelmi rendszabályok alkalmazása biztosítja, hogy *csak a megfelelően felhatalmazott személyek férhessenek hozzá az adatokhoz*.[7] [48.]

A megvalósíthatósági tanulmány után kialakult a NATO hálózat alapú képesség víziója és koncepciója (NNEC Vision and Concept), mely a képesség fontosabb jellemzőjeként három területet azonosít:

- *A tartalomszolgáltatás (information content) fejlesztése*, valamint a kulturális és humán tényezők összehangolása.
- *Azonos interfészek, szolgáltatások kifejlesztése és adaptálása*. Az új követelményeknek megfelelő könnyebb és gyorsabb alkalmazhatóság, valamint a költségtakarékosság érdekében a szervezeti elemek és képességek moduláris, blokk-rendszerű tervezése.
- *Az információ megosztásra vonatkozó képességek fejlesztése, valamint a szolgáltatások bizalmassága szintjének emelése az információvédelem (information assurance; IA)*[8] és a biztonságpolitikák továbbfejlesztése segítségével. A határokon átnyúló, egyre erősödő információ csere területén a „duty to share” elv alkalmazása.

Az NNEC koncepció *a hálózatok, szolgáltatások, és folyamatok föderációjának elméletére* támaszkodik, mely szerint a független alrendszerek, képességek központi menedzseléssel stratégiai szinttől harcászati szintig egyaránt elérhetővé válnak a *hálózati és információs infrastruktúrákon* (Networking and Information Infrasructures; NII) keresztül. Szövetségi szinten az NII szabványosított szolgáltatásokat (pl. továbbítás, tárolás, biztonság, menedzsment) biztosító NATO és nemzeti kommunikációs infrastruktúrák, képességek összességét jelenti. A vízió megvilágítja, hogy a „föderáció” kifejezés tartalmilag eltér az eddig használatos „integráció”-tól, és a „hálózatok hálózata” kifejezést az NII váltja fel.

---

[7] Az említett általános követelmények mellett a vízió konkrét elemeket is tartalmaz, mely szerint az IP (internet protokoll) rejtjelzés, a kulcsmenedzsment infrastruktúra alakvető követelmény megfelelő védelemmel ellátott kommunikáció érdekében. Az egyik legnagyobb kihívás a szövetség szintű telepíthetőség követelményének megfelelő, interoperábilis, megbízható egyedi azonosítással kiegészített PKI (Public Key Infrastructure; nyilvános kulcsú infrastruktúra) rendszer.

[8] A nemzeti terminológiában még nem szereplő információvédelemre vonatkozó kifejezés magyarázata később olvasható (p. 47-48.).

A koncepció megvalósítása *kognitív* és *technikai* területekre bontható. A kognitív képességek feladata a rendelkezésre álló információk átalakítása felhasználható tudássá. Ennek részei az *együttműködés* (az adatbirtokos szervezetek, alkalmazások között), az *információ megosztás* (az elkülönült adatok összeillesztése a szükséges háttér kialakítása érdekében), az *információ feldolgozása* (adatfúzió, melynek eredményeképpen az adat a kívánt helyen, a szükséges tartalom jelenik meg, ahol az alkalmazást megfelelő képzési és gyakorlási háttér támogatja).

Az említettek hatékony információs erőforrás menedzsment, valamint az információkat eredményesen alkalmazó szervezeti elemek és műveletek kialakításával válnak működőképes egésszé.

A *technikai terület* feladata a meglévő képességek hálózat alapú képességgé történő fejlesztése. Ennek részei a hálózat alapú képesség *architektúrájának kialakítása*, a *szolgáltatás alapú megközelítés* (a szükséges szolgáltatások több üzemeltetési környezetben történő alkalmazhatósága), a *moduláris felépítés* (gyors átkonfigurálási lehetőségek, az elemek rugalmas korszerűsítése), az *információbiztonság szintjének szavatolása* (fejlett szintű rejtjelzés és kulcs menedzsment infrastruktúra, objektumok címkézése, a kockázatelemzés hangsúlyosabb alkalmazása, szabványok alkalmazása az információvédelmi rendszabályok területén, interoperabilitás) és a *szolgáltatás menedzsment*. [49.]

Az adatkezelésre vonatkozó átfogó bemutatás alkalmas a szervezeti együttműködés új alapokra való helyezésének érzékeltetésére. A közös célok megkövetelik a civil és katonai szféra szoros együttműködése során az adatok *időbeli, a szükséges partnerek felé történő továbbítását,* egységes, gyors értelmezését, feldolgozását és hasznosítását. Az adatok védelmére vonatkozó „need to know” elv mellett megjelenő „duty to share” elv megköveteli az infrastruktúrák olyan szintű együttműködését, hogy megvalósulhasson az adatok elérése. Ezzel párhuzamosan olyan többszintű védelmi mechanizmus kialakítását teszi szükségessé, ami megvalósítja, hogy az együttműködő szervezet alkalmazásai csak a védelmi szabályrendszer által biztosított adatokat érhesse el.

Ez a megközelítés egyértelműen jelzi az MH-n belüli, esetlegesen eltérő védelmi szintet nyújtó „egy szervezet, és annak működése érdekében egy adatkezelő rendszer” filozófia végét. A szervezeteknek a központilag menedzselt, hálózat által rendelkezésre bocsátott és testre szabott képességet kell használniuk, beleértve a nemzeti és egyéb külső kapcsolatokra vonatkozó igényt. A központilag menedzselt adatkezelő képességeknek olyan üzemeltetés és biztonsági felügyeleti funkciókkal kell rendelkezni, amelyek képesek az eltérő típusú

hálózatok esetében is az összehangolt elvek szerinti üzemeltetésre, és azonos védelmi szint biztosítására.

A MH adatkezelő képességei nem vizsgálhatók a társadalmi információs környezettől elszigetelten így újabb dimenzióként jelenik meg a közérdekből nyilvános adatokra vonatkozó *közzétételi kötelezettség*, *a közigazgatási hatósági eljárások rendjébe történő részvétel*, valamint a szervezeti érdekekből szükséges, *a nyilvánosságot célzó kommunikációs szükséglet.*

Az *elektronikus közzétételi* folyamat kialakításának alapja az elektronikus információ szabadságról szóló 2005. évi törvényben meghatározott általános-, a jogszabályokban rögzített *különös vagy egyedi közzétételi listák összeállítása.*

Az életciklus elméletre támaszkodva a honvédelmi tárca összes szervezetére vonatkoztatva meg kell határozni a közzétételre kötelezett adat megjelenésétől kezdve az engedélyezéshez, közzétételhez szükséges eljárás lépéseit, az adatok honlapon történő megjelenéséhez, helyesbítéséhez, frissítéséhez, eltávolításához és archiválásához szükséges feladatokat a vonatkozó biztonsági követelményekkel és védelmi rendszabályokkal együtt (beleértve az illetéktelen beavatkozás esetén szükséges eljárásrendet, a jelentési kötelezettségeket, és a bizonyítékszolgáltatásra vonatkozó esetleges feladatokat).

Az elektronikus közzétételhez hasonló, az MH-ra is egyre több feladaton keresztül megnyilvánuló általános követelmény a közigazgatási hatósági ügyekre vonatkozó elektronikus formában történő ügyintézés. A hatósági ügyintézés során biztosítani kell az ügyfél betekintési jogát (és másolatkészítési lehetőséget), valamint a folyamatban választási lehetőséget az elektronikus és a hagyományos ügyintézés között. Összetett, több hatóságot érintő ügyintézés esetén az érintett szervezetek adataikat kötelesek egymás felé is szolgáltatni, és nem kötelezhetik arra az ügyfelet (ez adatcsere szolgáltatást igényel az MH egyes szervezetei és az adózással, egészségüggyel, személyi nyilvántartással és nyugdíjjal foglakozó szervezetek között). A hatóságnak gondoskodni kell az eljárás során megismert, törvény által védett titok és a hivatás gyakorlásához kötött titok megőrzéséről, a személyes adatok védelméről. Biztosítani kell az ügyintézési útmutató elérhetőségét, a szükséges formanyomtatványok letölthetőségét, valamint interaktív szolgáltatásként lehetővé kell tennie a határidőkkel, hatályos jogszabályokkal, az ügyfelek jogaival kapcsolatos információk elérését, tájékoztatást kell adni az adatvédelemről, illetékekről, az egyedi azonosító használatáról, illetve az elektronikus ügyintézés technikai szabályairól. [50.]

Az elektronikus közzététellel és a hatósági ügyintézéssel kapcsolatos feladatok nem tartoznak a hagyományosan értelmezett katonai tevékenységek híradó és informatikai szolgáltatásaihoz, de *ezeket a feladatokat a honvédelmi minisztériumnak, mint közigazgatási egységnek szükségszerűen végeznie kell.*

A vázolt követelmények egyértelműen a hálózat alapú képességek szükségességét mutatják már nemzeti szinten is, és jelzik, hogy napjainkban *a hagyományos állandó, vagy tábori kommunikációs képességeket számtalan civil-katonai együttműködés, adatcsere igény gazdagítja. E követelményeket csak akkor lehet teljesíteni, ha az MH információs képességei, és azok védelme a nyilvánvaló katonai igények mellett megfelel a közigazgatási követelményeknek is.*

1. 5. A korszerűsítésre vonatkozó átfogó követelmények, és azok megalapozása

A kutatások gyakorlatba ültetését és a kommunikációs terület fontosságát mutatja, hogy a honvédelmi miniszter 2006. évi irányelvei között haderőfejlesztési prioritást kapott a *híradó és informatikai terület fejlesztése* (úgy, hogy az alapul szolgáljon a kialakítandó hálózat alapú hadviselési képességhez), a *telepíthető vezetési-irányítási rendszer fejlesztése* a műveleti részvételre tervezett szervezetek részére, illetve a haderő professzionális jellegének erősítése érdekében a *vezetési rendszer racionalizálása, fejlesztése*.

Ennek előzményként megemlítendő a MH Védelmi Felülvizsgálat első szakaszának lezárása után készített értékelés, amely szerint a válságkezeléssel (békefenntartás-béketeremtéssel) kapcsolatos feladatok, a terrorizmus elterjedésének veszélye miatt a meglévő katonai kapacitások *korszerűsítésre szorulnak*. A korszerűsítés mellett újabb képességek kialakítására is szükség van, amelynek része a vezetés-irányítás és híradás (C3) modernebbé tétele (a szövetséges hadseregekkel interoperábilis, korszerű, telepíthető és védett vezetési, kommunikációs és információs képesség).

A 2006-os védelmi tervezésnél általános haderő fejlesztési követelményként szerepelt a szövetségi, EU, vagy egyéb koalíciós műveletekben való részvétel érdekében a kompatíbilis vezetési, kiképzési és alkalmazási elvek kialakítása, a bárhol telepíthető tábori híradó-informatikai háttér megteremtése, valamint a minősített időszaki és a békevezetési rend eltéréseinek a legszükségesebb mértékre történő csökkentése. Az új típusú kihívásokkal való lépéstartáshoz elengedhetetlen az adatok gyűjtése, feldolgozása és a felhasználókhoz való időbeni eljuttatása, amelynek érdekében folyamatosan fejleszteni kell az információgyűjtés és feldolgozás hatékonyságát. Emellett prioritást kapott még az MH *hálózat alapú hadviselési képességének* kialakítására vonatkozó terv kidolgozása, melynek során először a repülőgépek

és a légi vezetési-irányítási rendszer közötti kapcsolat elemeit kell kialakítani, majd a képességet ki kell terjeszteni a szárazföldi csapatokra is. [51.]

A közzététel mellett egyre összetettebb feladat a minisztérium (és egyéb szervezetek/szervek) kommunikációs céljait szolgáló adatkezelő képességek biztosítása. *Külső kommunikációként* szükség van a lakossági bizalom és megértés fenntartására, a *műveleti és krízis kommunikáció* területén a missziók kommunikációs támogatására, valamint *belső kommunikációs területen* támogatni kell a hiteles tájékoztatást, a bizalmi légkör kialakítását és fenntartását, valamint a közösségek hatékony működését. [52.]

A tájékoztatás kapcsán fontosnak tartom leszögezni, hogy az újabb és újabb helyzetekről számot adó *tájékoztatási feladatok és a szervezeti érdekből fontos adatok védelme folyamatos együttműködést igényel a tájékoztatási és az információvédelmi szervezeti elemek között*.

Az adatkezelő képességek MH szintű támogatását gyakorlati oldalról tekintve megállapítható, hogy az ezredfordulót megelőzően megkezdődött a rendelkezésre álló távközlő és informatikai hálózatok fejlesztése, lehetséges integrációjuk előkészítése. A korábbi széttagolt, eltérő technológiájú alapokon nyugvó, szigetszerű kialakításokból álló rendszerek nagy része egy *korszerű MH szintű transzport hálózatra csatlakozik*, [53.] és körvonalazódik egy *integrált, korszerű hálózatfelügyelet* alapja.

Az MH Iroda-automatizálási Program beindításával egységes elvek alapján szervezett infrastruktúra szolgáltatások kialakítása kezdődött meg. A tervek szerint a *tábori és az állandó infrastruktúra a felhasználók felé egységes kommunikációs felületet* biztosít, amibe bele kell érteni a megfelelő *csatlakozási képesség biztosítását a mobil felhasználók felé*, illetve a légierő speciális (föld-föld és föld-levegő és levegő-levegő) nyílt és védett kommunikációs igényeinek biztosítását szövetségi viszonylatban is.

A korszerű igények kielégítése érdekében körvonalazódni látszik a minősített adatok elektronikus kezelésére vonatkozó *egységes infrastruktúra* kialakítását célzó vezetői akarat. A felhalmozódott tapasztalatok lehetővé fogják tenni, hogy a nyílt, nem nyilvános adatkezelő képességeket biztosító *zártcélú hálózat transzporthálózatként biztonságosan kiszolgálja a minősített adatok kelezésére feljogosított hálózatot is*.

Megkezdődött a *hitelesítés szolgáltatást nyújtó alrendszer,* az *egységes iratkezelő rendszer* központi, MH szintű szolgáltatásként történő kialakítása, illetve a számítógépes hálózati behatolás érzékelő és az eseménykezelő képesség (Computer Incident and Response Capability; CIRC) megalapozása.

A perspektivikus elképzelések megalapozása minden esetben elméleti vizsgálatok, kutatások formájában kezdődik, ami a magyar hadtudományi kutatásoknál is felismerhető.

Az állandó jellegű híradó hálózat korszerűsítéséről írt értekezésben Fekete Károly körvonalazta a digitális kapcsolóelemek szolgáltatási szintjének kártyákkal történő emelését, javaslatot tett új technológia alkalmazására, honvédségi tulajdonú optikai hálózat kialakítására, ami *szabványos, nagysebességű transzporthálózatként képes a komplex elektronikus kommunikációs igények kielégítésére*.

Szűcs Gáspár kialakította *harcászati szintű adatfeldolgozásra vonatkozó követelményrendszert*, körvonalazta az *adatáramlás rendjét*. A szabványos folyamatok, egységes szemlélet alapján kialakított adatbázisok lehetővé teszik az *együttműködést a különböző kormányzati vagy szövetséges rendszerekkel*, megvalósul az „azonosan látott" harcászati szint.

Rajnai Zoltán az állandó rendszerhez csatlakozó területlefedő, rácsrendszerű tábori kommunikációs rendszer korszerűsítését célzó kutatásával *multimédiás kapcsolókra alapozva* felvázolt egy olyan szabványos, zömében kereskedelmi forgalomból származó eszközöket alkalmazó rugalmas, a katonai szervezetek igényeihez *könnyen átalakítható hálózatot*, ami a szervezetek és egyének kommunikációs szükségleteinek *komplex kielégítését* szolgálja.

Hóka Miklós rádió kommunikációra irányuló kutatásai során *egy integrált, nyílt rendszerű, bővíthető és továbbfejleszthető többfunkciós infrastruktúra harcászati internet jellegű szolgáltatásaként harcászati valós kép kialakítását körvonalazta*, ami multimédiás szolgáltatásokkal támogatja a hatékony információ megosztást és döntés előkészítést, kiemelten kezelve az interoperabilitás különböző technikai és szervezési követelményeit.

Ternyák István az előző kutatók által logikai alrendszerekre bontott egységes infrastruktúra kialakításával kapcsolatosan tett általános megállapításokat, amely a *fejlesztések lépcsőzetességére*, a *nemzeti fejlesztések támogatására,* és az *igény szerinti elemek összeépítésének szükségességére* mutatott rá.

Az említett doktori értekezések jól képviselik az MH szintű adatkezelő képességek korszerűsítésére irányuló elméleti erőfeszítéseket. Megállapítom, hogy az említett kutatások az adatok védelmének fontosságát és szükségességét megfogalmazzák, egy-egy területen megoldásokra is rámutatnak, de kutatási témájuk tárgyalása mellett nem vállalhatták a védelmi kérdések vizsgálatát is, *ami jelzi információvédelmi területen is egy általános vizsgálat szükségességét.*

1. 5. Összefoglalás és következtetések

A bemutatottakon keresztül megállapíthatom, hogy a magyar Nemzeti Biztonsági Stratégia információbiztonsági részei *összhangban vannak a külföldi megfogalmazásokkal, de a feladatok, erőforrások teljes megalapozása a Stratégiában, felső szinten nem történik meg*.

Az információbiztonságra vonatkozó felső szintű feladatok megjelenítéshez, az alapelvek tisztázásához (beleértve a közigazgatási, védelmi szféra információvédelmi feladatainak támogatását) *nagymértékben hozzájárulna egy átfogó Nemzeti Védelmi Stratégia,* és a N*emzeti Információbiztonsági Stratégia kiadása,* illetve a stratégiák általános irányvonalának megfelelő *követelmények, eljárások jogszabályban, korszerű módon történő rögzítése. Ezek hiányában információvédelmi szempontból az MH feladatrendjét nem találom szakmailag alátámasztottnak.* Hiányolom azt a központi szempontrendszert is, ami irányelveket, támpontokat ad a különböző közigazgatási szervezetek nyílt és minősített adatok védelmére vonatkozó információvédelmének egységes menedzseléséhez.

A külföldi stratégiákban megfogalmazottak elemzését és rendszerezését jó kiinduló pontnak találom a nemzeti, stratégiai szintű megfogalmazások támogatásához, a Katonai Stratégiában az MH sajátosságainak megfelelő, információbiztonságra vonatkozó általános alapelvek, követelmények kialakításához. A Katonai Stratégia, illetve a fontosabb honvédelmi tárca szintű stratégiák információvédelmi szempontú támogatása érdekében a rögzítendő kulcskérdéseket a következő keretek között tartom célszerűnek megfogalmazni:

- A társadalom különböző területein az információs szolgáltatások biztosítása az állam alapvető érdeke. Az adatokhoz való hozzáférési lehetőségek biztosítása mellett alapvető érdek a nyilvánosan nem megismerhető adatok-, és az állami funkciók teljesítését szolgáló (beleértve az MH vezetését, működését és együttműködési képességeit) kritikus infrastruktúrák fenyegetéssel és sebezhetőséggel arányos mértékű védelme.
- Az új szolgáltatások, a hálózatok egyre bonyolultabb összekapcsolásai, az internet által biztosított lehetőségek újabb és újabb kihívásokat, és fenyegetéseket jelentenek, mert a gyorsuló ütemű fejlődés *a szolgáltatások támadására, kihasználására alkalmas technológiákat, eljárásokat is támogatja*. A társadalom *egyre jobban függ az információs szolgáltatásoktól*, így a működéssel kapcsolatos problémák (zavarok, meghibásodások, az infrastruktúrák anyagi, technikai, humán és egyéb területű támogatási hiányosságai, a nem megfelelő technológia alkalmazása) halmozott nehézségeket okozhatnak. A véletlenül, vagy szándékosan keletkező negatív hatások *egymást erősíthetik*, és az eltérő területeken jelentkező

információs problémák *lavinaszerű hatásokat válthatnak ki*. Az *ellenséges szándék* (pl. terrorizmus, hírszerzés, számítógépes bűnözés, információs fölényre irányuló törekvések, belső illetéktelen hozzáférési kísérletek) nem csak a fegyveres erőket célozza, hanem térben és időben széttagoltan, aszimmetrikus eszközöket alkalmazva váratlanul támadja a szembenálló felet az *összes lehetséges dimenzión keresztül* (pl. gazdasági előny megszerzése, állami vezetők lejáratására irányuló propaganda, terrortámadás előkészítéséhez tartozó adatgyűjtés, közigazgatási rend hitelének csorbítása).

- A nemzetbiztonság szempontjából érzékeny területeken kiemelten fontos a nemzeti függetlenség, a korszerű technikai lehetőségek kihasználása, a kritikus infrastruktúrák koordinált védelme, mely során a hangsúlyt az észlelésre és a megelőzésre kell helyezni.
- Az információs szolgáltatások, és a rájuk irányuló fenyegetések fejlődésével összhangban folyamatos célszerű fejleszteni a kockázatkezelés eszköztárát, valamint az adatkezelő műveletek rugalmasságát és visszaállíthatóságát.
    - A szervezeti együttműködést szolgáló összekapcsolt információs képességek komplex védelme érdekében hangsúlyos kérdés a szabványosítás, a közös elvek alapján működő tanúsítás, az információvédelem területére is kiterjedő interoperabilitás. Nélkülözhetetlen a társadalom különböző szegmenseinek összehangolása, a nemzetközi együttműködés, a kutatási és fejlesztési folyamatokban történő részvétel, a biztonsági tudatosság erősítése.
    - A terrorizmus és a számítógépes bűnözés elleni védelem érdekében szükség van a támadásra alkalmas technológiák folyamatosan figyelemmel kísérésére, a védendő kritikus infrastruktúra elemek, és a szükséges védelmi rendszabályok folyamatos azonosítására és pontosítására.

A Katonai Stratégia előkészítése napirenden lévő kérdés. A *doktrínák és az egyéb felső szintű dokumentumok információbiztonsági szempontból történő megalapozása érdekében szükségesnek tartom, hogy a Stratégia bevezetésként mutasson rá a katonai erőkre irányuló információs fenyegetések súlyosságára, és a vezetési folyamatok információs szükségletének fontosságára. Alapvető nemzeti érdeknek kell tekinteni a kormányzati és civil szervezetekkel, valamint szövetséges erőkkel kompatibilis vezetési és irányítási rendszer fenyegetéssel, és sebezhetőséggel arányos védelmét, ami nélkül nem képzelhető el döntési fölény. Általános követelmény, hogy az adatkezelő képességek az MH szervezeteinek speciális alkalmazási*

körülményei között is támogassák a szervezetek megbízható vezetését. Ennek érdekében szükség van a kritikus infrastruktúra létfontosságú elemeinek folyamatos működésére, helyreállítási képességekkel támogatva az adatok szabályozott elérési lehetőségének biztosítására, valamint rugalmasan változtatható hozzáférési eljárásokra és megbízható azonosítási mechanizmusokra.

A szerteágazó támadó információs műveleteket gyors és hatékony észlelő, elemző és reagáló képességeket kell ellensúlyozni, és a hasonló szövetségi képességekkel szorosan együtt kell működni.

A vizsgált magyar katonai doktrínákban az információbiztonság tartalmasan nem jelenik meg, de az *információk védelmének szükségessége felismert, a korszerű megfogalmazások kezdetei azonosíthatók.* Összhaderőnemi szinten megjelent az információs/vezetési és irányítási hadviselés, annak nagybani összetevői is azonosítottak. *Az információs műveletek elemeinek ellentmondásmentes definiálása, szabályainak összehangolása, tevékenységgé gyúrása, valamint a műveleti biztonságra, az információbiztonságra vonatkozó megfogalmazások finomítása soron lévő feladatnak tekinthető.*[9] A felsővezetői döntésekben a NATO források által kijelölt iránynak megfelelően megjelent információs fölény - döntési fölény célkitűzése, a hatás alapú műveletek elvének alkalmazási igénye, a vezetést és működést támogató hálózat alapú hadviselés igénye képezik a felülvizsgálat fontosabb szempontjait.

A későbbi, a szabályozási hierarchia alacsonyabb szintjén lévő doktrínák kialakításakor a feltárt hiányosságok további fennállása komoly problémát okozhat, mert a funkcionális doktrínáknak az „általánostól az egyedi felé" haladás logikája szerint támaszkodniuk kell az MH ÖHD-ra. Emiatt az MH ÖHD információbiztonsági szempontból jelentős korrekcióra szorul, a másik két említett doktrínában az információbiztonság pontosabb megjelenítése javasolt.

Távlatokban célszerű figyelembe azt a nyilvánvaló tényt, hogy a kidolgozandó funkcionális doktrínák további, az információvédelem szakterületéhez tartozó kérdéseket fognak érinteni (pl. személyi és egészségügyi adatok, speciális védelmet igénylő adatok (pl. azonosításra, nyomkövetésre alkalmas adatok), és azok megosztása, a nyílt és minősített adatbázisok meta-adatainak védelme, megosztása). Ezeket az információvédelmi kérdéseket

[9] Az MH Szabványosítási és Doktrinális Bizottság a 2006. októberben kezdeményezett felülvizsgálat során véleményem alapján pontosította az információs műveletekre és az információ biztonságra vonatkozó kidolgozói kört, és az értekezésben is említettek alapján elfogadta a szakterületre vonatkozó részek átdolgozásának szükségességét.

nem lehet az MH ÖHD szintjére emelni, vagy egy később kialakítandó funkcionális doktrínában összevontan tárgyalni (pl. a tervezett híradó és informatikai doktrínában), így jelzem, hogy az ilyen szakterületi kérdéseket, egy-egy feladat kapcsán az adott doktrínában kell a szükséges mértékben részletezve megoldani. Az ezzel kapcsolatos egyeztetés, közös kidolgozás igénye egyértel*műen az esetenként felismerhető szervezeti elkülönülési kényszer megszüntetését igényli, mert a doktrínákat az összetartozó feladatkörökhöz kell igazítani, és nem lehet az aktuális szervezeti struktúra szerinti igények szerint darabolni a doktrínarendszert.*

A nemzeti hadtudományi publikációk tanulmányozása alapján megállapítom, hogy a nem kifejezetten információbiztonságot célzó munkák is *felismerik és rámutatnak az információk védelmének fontosságára*. Emellett szükségesnek tartom annak megállapítását is, hogy *az információs műveleteken belül, az adatok védelmére irányuló szakterületi célokat, feladatokat és megoldásokat, a katonai sajátosságokat elemző, bemutató munkák területén hiányosság mutatkozik, a katonai szervezetek sikeres működéséhez szükséges információvédelem napjainkban nem kellően publikált.*

A fejezet végén szakmai summázásként Zrínyi Miklóst idézem:

„Nagy dolog a titok és szükséges a kapitánnak: e nélkül soha semmit véghez nem viszen emberül.” [54.]

2. AZ INFORMÁCIÓBIZTONSÁG SZAKTERÜLETEI ÉS A VÉDELEM KIALAKÍTÁSÁNAK RENDJE

A magyar hadtudomány adós annak kifejtésével, hogy mit kell érteni az információk biztonsága alatt, illetve milyen rendszabályokkal kell ezt az állapotot megvalósítani. Hiányoznak a korszerű védelmi feladatok szakkifejezései, a NATO kifejezések fordításai. Az MH ÖHD tárgyalásakor bemutatott fogalmi keveredések, zavarok olvashatók a katonai lexikonokban is, melynek oka az új és a régi fogalmak ötvözése, illetve az angol kifejezések fordítási és honosítási szándéka.

Az MH-nál egyre kevésbé alkalmazott „titokvédelem” kifejezés a minősített adatok védelmére vonatkozó feladatrendszer megnevezése. Szövényi György 2001-ben publikált adatai szerint a hazai joganyagban több százszor szerepel a „titok” szó, többször használt a „titoktartás” kifejezés is, de a szerző a „titokvédelem” hivatalos meghatározását nem találta meg. [55.]

A „titokvédelem” HM-MH Titokvédelmi és Ügyviteli Szabályzat (1996) szerinti meghatározása a NATO és más nemzetek (pl. Egyesült Államok, Egyesült Királyság) összhaderőnemi, funkcionális doktrínáinak szakkifejezéseihez képest együttesen tartalmazza a *minősített adatok védelmét* és a *megtévesztést*.

Az említett szerző kutatásait folytatva évtizedekkel ezelőtt hatályos jogszabályokban leltem fel legkorábban a „titokvédelem” kifejezést. A joganyagok értelmező rendelkezéseinek hiányában szövegelemzéssel megállapítható, hogy a fogalom a „titkok védelme” (pontosabban a minősített adatok védelme) kifejezésnek felel meg, a jogalkotó megtévesztési feladatokat az említett szabályzathoz hasonlóan nem határozott meg.

Ezzel az állásponttal egyetértve a nemzetközi gyakorlatnak megfelelően célszerűnek tartom a megtévesztést az első fejezetben tárgyaltak szerint önálló feladatként tárgyalni és elkülöníteni az információvédelemtől.

NATO definíció szerint az információbiztonság (information security) az információk védelme a szándékosan, vagy véletlenül bekövetkező illetéktelen megismerés-, másolás-, továbbítás-, változtatás- vagy megsemmisítés ellen.[10] [56.]

Ezzel a definícióval összhangban van az Avtv. meghatározása, mely szerint az adatokat különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen kell védeni.

---

[10] A definíció a védelmet nem korlátozza a minősített adatokra, illetve megfogalmazza, hogy „információ” alatt egyaránt értendő a dokumentum formájú (vagy más tárgyiasult) adat, az elektronikus formában létező adat, vagy az emberi tudatban létező ismeret.

A Ttv. a minősített adatok védelmét a vonatkozó jogszabályok végrehajtásában, az adatok védelmi rendszerének adminisztratív, személyi biztonsági, technikai, fizikai, kommunikációs, ellenőrzési és felügyeleti elemeken nyugvó kiépítésében és működtetésében határozza meg.

A jogszabályok, hadtudományi publikációk és egyéb források feldolgozása során több mint húsz nemzeti és külföldi megfogalmazást tekintettem át, amelyek az információbiztonságon belüli feladatok kategorizálására vállalkoztak. A legtöbb forrás szerint az információbiztonság *fizikai*-, *személyi*-, *dokumentum*- és *elektronikus információvédelmi* területeken valósul meg.[11] Mráz István publikációjában „információbiztonság”-ot említ „elektronikus információbiztonság” helyett [57.], de a tartalom egyértelműen megmutatja a szakterület elnevezését.

Szakmai érdekesség, hogy az Egyesült Államok Információs Műveletek Doktrína által kialakított rendszer a hasonló gondolatvilág ellenére *nem tartalmazza a dokumentumvédelem* témakörét.

A NATO AAP-31, valamint az EU Biztonságpolitika [57.] e négy elem mellett ötödikként az *eljárás biztonságot* (procedural security) azonosítja, amit a NATO információvédelmét bemutató első magyar honvédelmi kiadvány is említ.[12] [59.] Egy dokumentumban találtam erre magyarázatot, amely a „szervezeti biztonság” kategóriát megalkotva az „eljárás biztonság”-ot a működést szabályozó jogszabályi háttérrel és belső szabályozással azonosította, [60.] de megállapítom, hogy ez nem járható út, mert a jogszabályok (és egyéb szabályozók) alapján történő szabályozás *nem statikus, önálló információvédelmi szakterület*, *hanem a szervezet vezetéséhez tartozó menedzsment tevékenység.*

Esetenként felbukkanó jellegzetesség még a *fizikai védelmi rendszabályok elektronikus információvédelemhez történő sorolása*. [61.] [62.]

Az áttanulmányozott megfogalmazások zöménél felismerhető, hogy nem elégséges az adatkezelő rendszerek védelmét statikusnak tekinthető elemekből felépíteni, *ezek mellett dinamikusnak tekinthető képességek és tevékenységek is szükségesek* (pl. kockázatelemzés, akkreditálás/auditálás, időszakos ellenőrzés). Ugyanígy előfordul a hardver és szoftver

[11] Elfogadott, egységes terminológia hiányában az információ biztonsági részterületek megnevezésénél a „védelem” kifejezést alkalmazom.

[12] Ugyanez olvasható a már hatályon kívüli, a Nemzeti Biztonsági Felügyelet részletes feladatairól és működési rendjéről, valamint az iparbiztonsági ellenőrzések részletes szabályairól szóló 2002-es kormányrendeletben, valamint az EU 2001-es Biztonságpolitikájában (szintén magyarázat nélkül).

védelmi rendszer feltüntetése mellett az észlelés és reagálás, detektálás, dokumentálás és válasz képességek megjelenítése. [63.]

2. 1. Az információbiztonság szakterületei

2. 1. 1. Fizikai védelem

Fizikai védelem az erőforrások szándékos és véletlen fenyegetései ellen irányuló rendszabályok összessége. A rendszabályok a *környezet*, a *védelmi infrastruktúra és technikai rendszer,* valamint az *élőerős védelem* területére koncentrálhatók. A védelmi rendszabályok kialakításának rendje a Sebastian von Vaubantól származó „mélységi védelem" elvén alapul (a védelmi rendszabályokat körkörösen, mélységben tagozva kell kialakítani). Ezt fogalmazza meg a kanadai fizikai védelemre vonatkozó irányelv, mely szerint a „hagymahéj" („gyűrű rendszerű védelem" vagy „bikaszem") koncepció szerint a védendő objektum körül rétegezett védelmi rendszert kell kialakítani.[13] [64.]

A fizikai védelemre vonatkozó nemzeti követelmények nem részletesek, még a minősített adatok védelmére szolgáló rendszabályok is csak általános megfogalmazásúak. A követelményeket megfogalmazó 1995-ös kormányrendelet szerint az államtitoknak minősülő adathordozó őrzésére kizárólag biztonságos zárszerkezettel és biztonsági lakattal (értsd: személyi pecsétnyomóval történő lepecsételésre alkalmas eszköz) védett tárolási megoldás alkalmazható, *lehetőség szerint* gondoskodni kell kombinációs zár rendszeresítéséről is. Minősített adathordozó tárolására, őrzésére lemezszekrényt kell rendszeresíteni, amelynek személyi pecsétnyomóval történő lepecsételésre alkalmasnak kell lennie. A helyiséget a minősített adatok *fokozott védelméhez szükséges technikai, elektronikai eszközökkel* (vasrács, riasztóberendezés, tűzjelző stb.) fel kell szerelni. [65.]

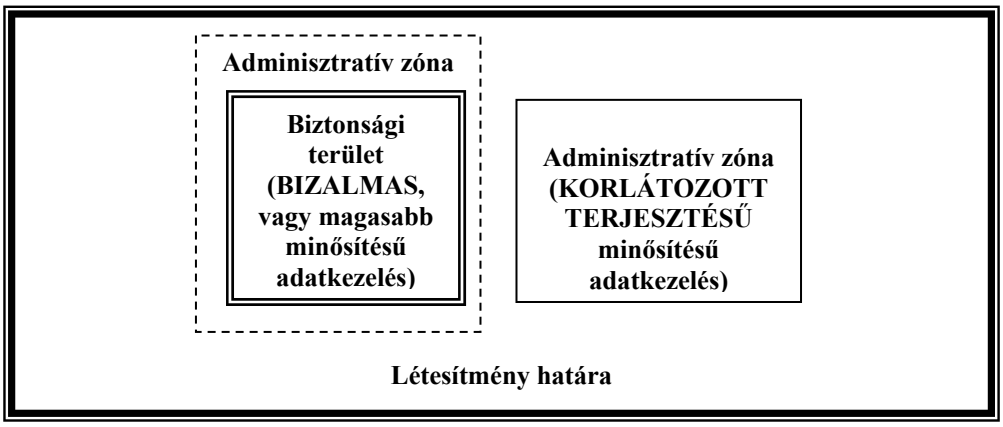
A NATO, EU minősített adatok védelmére szolgáló rendszabályok ennél *lényegesen kidolgozottabbak, és minősítési szintekhez rendelve részletes paramétereket határoznak meg* (pl. rácsvastagság és távolság, rögzítés, biztonsági ajtó és tároló ellenálló képessége és tűzállósága, zártípus, falvastagság, járőrözési gyakoriság, technikai védelmi elemek, illetve ezek komplex alkalmazása). [66.]

Korszerű létesítmények kialakítása esetén célszerű a NATO/EU adminisztratív zóna, illetve BIZALMAS vagy magasabb minősítés esetén az I. és II. osztályú biztonsági terület kategorizálást követni (3. sz. ábra). Különleges funkciók esetén (pl. kiemelt fontosságú

---

[13] A fizikai biztonság területén csak azokkal a feladatokkal foglalkozom, amelyek az adatok, vagy adatkezelő rendszerek védelméhez kapcsolódnak, és megjegyzem, hogy a biztonság érdekében az objektumok védelmének kialakításakor *létfontosságú a feladatok precíz összehangolása*.

hírközpontok, kulcselosztó és tároló központok, hitelesítés-szolgáltató központ elemei) a biztonsági szint speciális szabályokkal tovább emelhető (pl. több személy által felügyelt (no lone zone) helyiségek).



3. ábra: Az adatkezelő helyszínek kialakításának rendje (változatok)

Az *adminisztratív zóna* a normál irodai környezettel egyenértékű (zárható iroda és irodabútor), míg a *biztonsági terület* emelt szintű védelmi rendszabályokat jelent BIZALMAS, vagy magasabb minősítésű adatok kezelése esetén annak megfelelően, hogy a területre történő belépéssel egyidejűleg megtörténik-e a minősített adat megismerése, vagy nem.[14]

A felhasználók mellett a fenntartás, üzemeltetés szerteágazó területein dolgozók is hozzáférhetnek eszközökhöz, adatokhoz, így az említett védelmi rendszabályokkal *biztosítani kell, hogy takarítás, javítás, karbantartás során se történhessen illetéktelen megismerés*.

Tábori körülmények között a különböző vezetési pontokat, objektumokat lehetőleg meglévő épületekhez kell kötni, a védelmet *gyorsan kialakítható védelmi elemek* (mobil kerítések, akadályrendszerek, Hesco-bástyák) és *őrség* kombinációjával kell kialakítani.

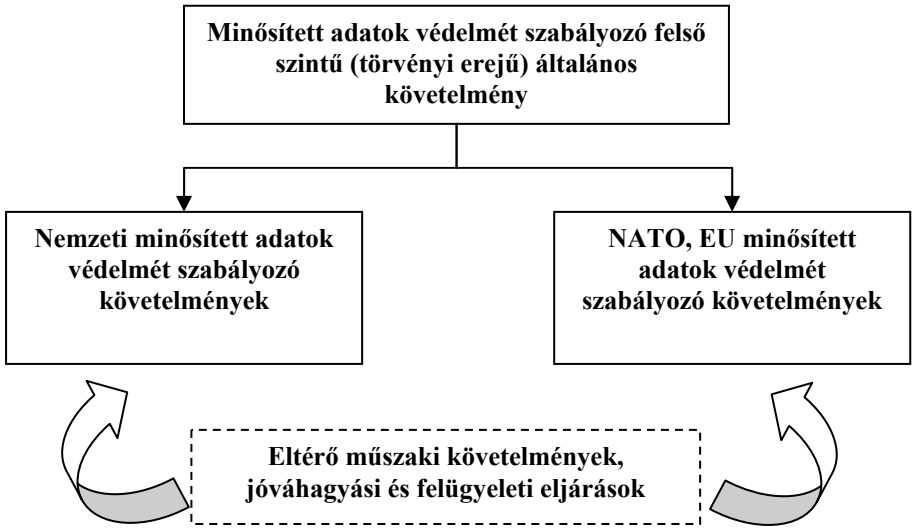
A tábori kommunikációs rendszer elemei más felépítésűek, mint a stacioner rendszer berendezései, így a felépítmények (konténerek, rendszerkocsik) kialakításakor a könnyű szállíthatóság, rövid telepítési idő, a fokozott igénybevételi követelmény mellett a meghatározott biztonsági szint eléréséhez szükséges igényeket is figyelembe kell venni.

Részletesen kidolgozott nemzeti követelményrendszer hiányában a Ttv. 2003-as változtatásakor az MH információvédelmi szakirányításáért felelős szervei *új adatfeldolgozó képességek kialakítása, vagy épületek felújítása során áttértek NATO és EU fizikai biztonsági*

[14] A szakterület fejlődését jelzi, hogy az első külföldi minősített adatok védelméről szóló jogszabály még ettől eltérően definiálta az I. és II. osztályú biztonsági területet, és II. o. biztonsági területen nem engedélyezte a BIZALMAS minősítési szint feletti kezelést.

követelményeinek alkalmazására, amit a 2004-ben megjelent, a minősített adatok egységes kezelésére vonatkozó kormányzati szándék [67.] és a minősített adatok védelméről szóló 2005. évi törvényjavaslat utólag igazolt. [68.]

A fizikai védelmi rendszabályok vizsgálata alapján a nemzeti és NATO, EU követelmények között elkülönítettséget, és egyben összehangolatlanságot állapítok meg. Egy adathordozó, vagy adat cseréje szövetségi és nemzeti szervezetek között úgy, hogy megvalósuljon az azonos szintű védelem, csak akkor valósul meg, ha a nemzeti infrastruktúráért felelős vezető belátás alapján önként kialakíttatja a NATO, EU típusú fizikai védelmet (4. sz. ábra). Erre jogszabály nem rendelkezik, mert NATO csatlakozásunkkor nem történt meg a nemzeti követelményrendszer átalakítása.



4. ábra: A nemzeti és NATO, EU fizikai védelmi rendszabályok egyenértékűsége

2. 1. 2. Személyi védelem

Kanadai meghatározás szerint a *személyi védelem* azon eljárások összessége, amelyek biztosítják, hogy minden személy, akinek érzékeny információhoz van hozzáférési joga, rendelkezzen az erre vonatkozó felhatalmazással és a szükséges szintű hatósági személyi biztonsági tanúsítvánnyal. [68.]

Hazánkban a személyi biztonsági tanúsítvány nemzeti adatkezelés esetén csak korlátozottan intézményesített.

A személyi biztonsági tanúsítványra vonatkozó kötelezettséget NATO BIZALMAS, vagy magasabb minősítésű adatkezelés esetén határozza meg a NATO csatlakozáshoz szükséges információbiztonságra vonatkozó kötelezettségvállalást rögzítő törvény, de a végrehajtást szabályozó jogszabály ezt a követelményt tovább szigorítva már a NATO

KORLÁTOZOTT TERJESZTÉSŰ minősítésű adat kezelését is személyi biztonsági tanúsítványhoz köti.

Nemzeti adatkezelésre vonatkozóan jogszabály csak SZIGORÚAN TITKOS minősítéshez határoz meg nemzetbiztonsági ellenőrzési kötelezettséget.

Az illetéktelen személyek kizárása mellett[15] létfontosságúnak tartom, hogy *a felhatalmazott személyek rendelkezzenek a biztonságos adatkezeléshez szükséges ismeretekkel*. Az illetéktelen megismerést nem csak arra a könnyen felismerhető esetre kell szűkíteni, amikor egy feljogosítással nem rendelkező személy megismer egy rá nem tartozó adatot (pl. elolvassa, lemásolja, jegyzetet készít róla, lefényképezi). *A közvetett információk megszerzése, az információs folyamatok és gyenge pontok kiismerése, személyi tulajdonságok kihasználása* (social engineering) is ugyanilyen veszélyes lehet. *Ugyanígy nehezen, összetett rendszabályokkal kezelhető az MH állományából távozó személyek ismeretében lévő információkkal kapcsolatos védelem.*

A személyi biztonsági tanúsítványra vonatkozó kötelezettség speciális helyzetet teremtett a NATO, EU elektronikus adatkezelés területén. Az MH esetében is érvényesített NATO követelmény szerint [70.] a rendszeradminisztrátoroknak az üzemeltetéshez szükséges rendszer-szintű feljogosítás miatt *a kezelt adatok minősítésénél magasabb szintű személyi biztonsági tanúsítvánnyal kell rendelkeznie.* A követelmény vélhetően felváltható más, kombinált rendszabályokkal is (pl. felelősségi körök felosztása, kétszemélyes szabály alkalmazása), ami azért is javíthat az eredményességen, mert *a rendszeradminisztrátor megbízhatósága önmagában még nem biztosíték a képzetlenség, vagy figyelmetlenségből adódó hiba ellen*.

Humán területen *a védelem a gyakran nem súlyának megfelelően kezelt kiválasztásnál kezdődik*. A feladat egyszerűen megfogalmazható: fel kell tárni a szervezet számára veszélyesnek tekinthető személyiségjegyeket, és szükséges esetben módosítani kell az érzékeny adatok kezelését igénylő megbízást/kinevezést. Máig érvényesek Zrínyi Miklós intelmei: „a részegség kimondatja a titkot”, „a bosszúság (értsd: a bosszú) kimondatja az emberrel a titkot”, vagy „titkot sérthet a nyereség, a félelem” vagy „gyakorta kérdés is megnyitja a titkot” vagy „a magaviseletével és a cselekvésével is elveszti az ember a titkot” vagy „tagadással is kimutathatni a titkot” vagy „asszonyemberek ellophatják az titoknak kulcsát; nincs őnálok titok, az ő szájuk bé nem záródhatik”. [71.]

---

[15] A NATO vagy EU Biztonságpolitika szerinti „szükséges, hogy tudja” alapelv. Az őskeresztényektől eredő „sub rosa” („ami a rózsa jele alatt hangzik el, maradjon titok”) kifejezés is ezt az elvet tükrözi.

Az adatfelkezelésre történő felhatalmazás nem alapulhat kizárólag a nemzetbiztonsági ellenőrzésen. *Ez a nézet a személyi biztonságot a szükséges ellenőrzések, és engedélyek megszerzését célzó ügyintézésre* egyszerűsíti, és háttérbe helyezi a szükséges képességek vizsgálatát.

A személyekre vonatkozó követelmények meghatározásának alapvető eszköze a tevékenységekhez szükséges információs folyamatok kategorizálása, amely alapján a beosztásokhoz r*endelhető a szükséges követelményrendszer* (pl. szaktanfolyamok, nemzetbiztonsági ellenőrzési szint, adatkezelési jogosultságok).

Beosztásba helyezéskor a *védelmi rendszabályok elsajátításának még a munkavégzés megkezdése előtt meg kell történnie*, beleértve azt is, hogy az adott személy hivatalos formában tudomásul veszi, hogy adatkezelése ellenőrzés alatt áll, és a szabályok megsértése esetén tevékenysége szankcionálható.[16]

A minél szélesebb körű megismerési jogosultság nem kiváltság, hanem vezetői tévedés.[17] A parancsnokok (vezetők) feladata a hatáskörök pontos kialakítása, és a szükséges korlátozások érvényesítése. Az adott feladat elvégzése után a megismerési jogosultságok érvényüket kell, hogy veszítsék (beleértve a beosztásból történő felmentést, és a korkedvezményes nyugdíjazás előtti munkavégzés alól történő mentesítés eseteit is).

Az információs műveletek során *veszélyes lehet a szabályok fellazítása* (pl. az információs folyamatokban egymás szabálytalan helyettesítése, a szabályok kölcsönös megegyezésen alapuló megsértése), vagy *a beosztásokhoz kötött felelősségek félreértelmezése* (pl. az adminisztratív beosztott a vezető hozzáférési jogosultságát használja).

Az adatkezelő rendszerek biztonsága érdekében *fel kell tárni a szervezeti és egyéni összeférhetetlenségeket* (pl. biztonságért és üzemeltetését felelős, fejlesztő és üzemeltető, mérést végző és értékelő funkciók), és azokat figyelembe kell venni a katonai szervezetek személyügyi munkája során.

2. 1. 3. Dokumentumvédelem

D*okumentumvédelem* a dokumentumok kezelése (létrehozása, minősítése, nyilvántartása, fordítása, sokszorosítása, csomagolása, továbbítása, módosítása, felülvizsgálata, minősítés megváltoztatása, dokumentumokba történő betekintés

[16] A követelmény az MH-val együttműködő szervezetek tagjaira, tanácsadóira is vonatkoznak.
[17] Surányi Péter, a Nemzeti Biztonsági Felügyelet főtanácsosa az MH 2006. májusi elektronikus információvédelmi továbbképzésén a jelenséget találóan „nice to know”-ként említette.

engedélyezése, irattárazása, levéltárazása és megsemmisítése stb.) során az illetéktelen megismerés elleni védelmi- és a rendelkezésre bocsátást biztosító szabályok érvényesülése.[18]

A „dokumentum” *nem csak papír alapú* rögzített adatot jelent, hanem tartalmazza az egyéb kemény (hard) formában megtestesült adatokat is (magnetofonszalag, film, videokazetta, floppy, merevlemez, memória chip, makett, fénykép, rajz stb.), így az adott szervezetnél a kezelt dokumentumok sajátosságainak megfelelő rendszert kell kialakítani. Az *elektromágneses (optikai és egyéb) adathordozókat* a beszerzéstől kezdve a raktározáson, tároláson, használaton keresztül egészen a megsemmisítésig a dokumentumokra vonatkozó védelmi rendszabályokkal egyenértékűen kell védeni és felügyelni (egyedi azonosítás, minősítés, nyilvántartásba vétel, hozzáférés szabályozása, ellenőrzés). A kezelési szabályok kialakításakor a nyilvánvaló fizikai védelmi kérdéseken túlmenően *figyelembe kell venni az elektronikus adathordozók fizikai tulajdonságaival kapcsolatos igényeket* (mágneses-, hőmérséklet- és páratartalom érzékenység, elöregedés, demagnetizálódás), és a kezelési utasítással történő ellátást is.

Hazánkban a békepartnerségi tagságtól kezdve kezelni kell a NATO minősített adatok védelmének kérdését, ezért a minősítési rendszert össze kellett hangolni a Szövetség rendszerével. Ez a már említett 2000. évi IV. törvényben vállalt kötelezettségvállalás alapján a 2003. évi LIII-as törvény feladata volt.[19] *A „szolgálati titok” kategória hármas tagozássá alakult, de a nemzeti és NATO, EU minősített adatkezelésre vonatkozó védelmi rendszabályok közötti különbség megmaradt, mivel a nemzeti minősítési szintekhez nincsenek hozzárendelve a NATO és az EU biztonsági követelményei*. BIZALMAS és magasabb minősítés esetén *továbbra is eltérőek a nemzeti és NATO, EU fizikai biztonsági követelmények*, így érthető a NATO/NYEU (és EU) nyilvántartók és a nemzeti ügyviteli infrastruktúrák közötti különbségek.

A Ttv. nem rendelkezik NATO, vagy EU minősítési jogról, így a hazánkban más tagállam, vagy NATO, EU szervezet számára készített minősített adat esetében az ügy előzményeként NATO, vagy EU szervezet által meghatározott minősítést lehet megismételni, vagy nemzeti minősített adatot lehet átadni (mely esetben a jelenlegi szabályozás alapján nem garantálható az azonos védelmi szint).

---

[18] A szakterület elnevezése az EU Biztonságpolitikában „security of information”. Az új, minősített adatkezelésre vonatkozó T/18708 törvényjavaslat a szakterületet „adminisztratív biztonság”-nak nevezi.

[19] A törvény megjelenéséig a Ttv. korábbi módosítása alapján a már hatályon kívüli szabályozás szerint az MH-nál a két minősítési kategória mellett megjelenő NATO CONFIDENTIAL (BIZALMAS) és NATO RESTRICTED (KORLÁTOZOTT TERJESZTÉSŰ) minősítésű adatot „titoknak nem minősülő, de védendő adat”-ként, a NATO UNCLASSIFIED (NEM MINŐSÍTETT) jelzéssel rendelkező adatot „nyíltnak minősülő, de a jogosulatlan hozzáférést kizáróan kezelendő adat”-ként kellett kezelni.

Ennél a szakterületnél megemlítendő az *adatok besorolásának gyakran félreértelmezett kérdése*. A besorolás alapvető feladata a besorolási szintekhez védelmi rendszabályok rendelése, a védelmi feladatok tipizálása. Az adatok besorolására vonatkozó általános kötelezettséget nemzetközi szabványok, módszertanok is előírják. [72.] Hazánkban az Informatikai Tárcaközi Bizottság (ITB) 12. ajánlása az *alap*, *fokozott* és *kiemelt* biztonsági osztályokat állította fel. [73.] A kialakításkor korszerűnek tekinthető besorolási rend napjainkban egyrészt *korszerűtlen*,[20] másrészt *az MH szempontjából hátrányos.*[21] A tipizált, biztonsági osztályokhoz rendelt védelmi rendszabályok nem találkoznak az MH gyakorlatával (álláspontom szerint nem megengedett, hogy csak kiemelt osztály esetében tilos külső személy rendszeradminisztrátori alkalmazása, nincsenek hálózatra, illetve azok összekapcsolására vonatkozó részletes követelmények, nem azonosított a besorolás megalapozásához szükséges kockázatelemzés, valamint jóváhagyásra/akkreditálásra vonatkozó követelmény).

Az Informatikai és Hírközlési Minisztérium 2006-ban nyilvánosságra hozott ajánlás tervezete a nem minősített adatokat sorolja az ITB 12. ajánlás szerinti kategóriákba, illetve a közigazgatási hatósági eljárásokhoz szükséges informatikai célrendszereket sorolja az említett biztonsági osztályokba. [74.]

A Központi Elektronikus Szolgáltató Rendszer alkalmazóinak a következő, az ITB ajánlással nem egyező besorolást kell alkalmazni: „különlegesen érzékeny (titkos) adatok”, az „érzékeny adatok”, a „belső adatok” a „nyilvános, közhiteles adatok”, valamint ezek mellett még szerepel a „nem osztályozott adatok” kategóriája. [75.]

Az Egységes Digitális Rendszerhez csatlakozó szervezeteknek a vonatkozó jogszabály szerint a bizalmasság szerint történő besorolás helyett az ITB 12. ajánlás káreseményhez kötött besorolását kell alkalmazni. [76.]

A bemutatott jogszabályok bizonyítják, hogy a jogalkotók nem egységesen értelmezik a biztonsági osztályokba sorolás kötelezettségét, illetve nem érzik kötelező érvényűnek az ITB 12. ajánlás előírásait. A közigazgatási szervezetekre vonatkozó kormányzati ellenőrzések

---

[20] Kétfokozatú minősítési rendszert tartalmaz a 2003-óta alkalmazott négyfokozatú minősítési rendszer helyett, „különösen fontos szigorúan titkos” megnevezést használ. Az ajánlás szerint a hármas felosztást célszerű további finomítani, de az MH esetében *ez nem elégséges*, így az osztályokon belüli további csoportok kialakítása mellett *szükség van az osztályok átalakítására.*

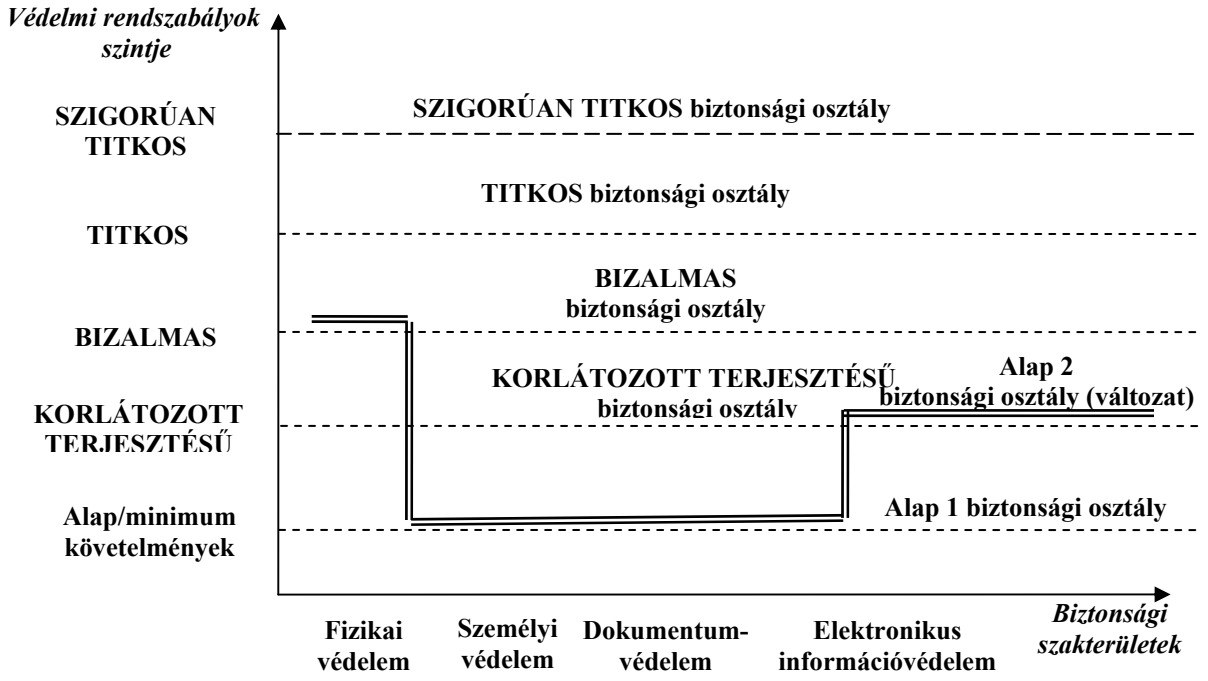
[21] Gazdaságilag nem vállalható, hogy az MH minősített adatok kezelésére feljogosított rendszerei csak a kiemelt osztályba tartozzanak (ez ellentmond a Ttv. titokköri jegyzékének is, mert a közigazgatásban minden szervezetnél azonosak a minősítési szintek). Egyéb esetben az MH-ra vonatkozó emelt szintű követelményt kellene érvényesíteni minden szervezetnél, ahol honvédelmi okból minősített adat kezelése történik.

során tapasztaltam, hogy az ellenőrző szervezetek a nyilvánvaló ellentmondások ellenére is megkövetelik az idézett ajánlás alkalmazását.

Meggyőződésem, hogy a besorolás kialakításánál nem lehet figyelmen kívül hagyni a NATO, EU szabályozás minősítési szintekhez kötött védelmi rendszabályait.

A bizalmasság szempontja szerint vizsgálva a „fokozott" biztonsági osztályban *a KORLÁTOZOTT TERJESZTÉSŰ minősítési szinttől a TITKOS minősítési szintig történő besorolásnak nem mutatható ki gyakorlati jelentősége*.

A besorolást *a minősítési szintekhez kell kötni* (bizalmasság szerinti besorolás), amely alapfelosztást speciális bizalmasságra vonatkozó követelmény, és a sértetlenségre és rendelkezésre állásra vonatkozó igények szerint tovább kell bontani úgy, hogy *az alkalmazandó felosztáshoz külön védelmi rendszabály legyen rendelhető* (5. sz. ábra).



5. ábra: A biztonsági osztályok minősítési szintekhez igazodó védelmi szintjei

A nem minősített biztonsági osztályt legalább két szintre kell bontani, és a funkciójuk, vagy halmozott jellegük miatt fokozottabb védelmet igénylő adatokat külön csoportba kell osztani. Ezeket az adatokat a *minősített adatok védelmi rendszabályaiból összeállított rendben kell védeni* (pl. központi adatbázisokat, kiszolgálókat legalább BIZTONSÁGI TERÜLET típusú környezetbe kell elhelyezni annak ellenére, hogy nem minősített adatok kezeléséről van szó). Az osztály másik csoportjába oszthatók a nem nyilvános, vagy egyéb olyan adatok,

melyek védelmére a bizalmasság, sértetlenség és rendelkezésre állás minimális követelményeit kell kialakítani.

Gyakran félreértelmezett kérdés a dokumentumokra vonatkozó nyilvántartási kötelezettség. A NATO, EU nyilvántartási kötelezettség NATO, EU szervezeteknél TITKOS minősítésnél kezdődik, melynek alapvető oka a hatalmas mennyiségű adat. [76.] Hazánkban a közfeladatot ellátó szervezethez érkezett, vagy általa készített nem minősített dokumentumokat is jogszabály által meghatározott nyilvántartási kötelezettség terheli. A szövetségi előírások a tagállamok nemzeti nyilvántartási kötelezettségét tiszteletben tartják; az elszámolási kötelezettségek közötti különbözőség egyértelműen nemzeti eredetű.

Speciális kérdés az elektronikus, vagy más formában rögzített adatok nyilvántartása. Az elektronikus iratkezelés bevezetéséig is reformra van szükség a fájlok szükséges szintű nyilvántartása érdekében, mert a felhasználói adatokat tartalmazó floppy-k un. „kísérőlap" típusú nyilvántartási mechanizmusa *merevlemezes adattárolók, vagy nagyteljesítményű adathordozók esetében egyszerűen nem alkalmazható*.

Csak az elektronikus adathordozókat érinti az adathordozók minősítési szint szerinti jelölésének problémája. Ez nem minősítés (a Ttv. csak az adatok minősítését határozza meg), de egy olyan nélkülözhetetlen adminisztratív eljárás, ami az adathordozón később minősített adat tárolását teszi lehetővé, *így célszerű ennek az eljárásnak jogszabályban történő szabályozása.*

Említést érdemel a minősített adatokkal kapcsolatos *eltérő nemzeti és hazai gyakorlat* is (NATO, EU szervezetek számára ismeretlen pl. a minősítési javaslat intézménye, vagy a minősítési határidő és a felülvizsgálati kötelezettség együttes alkalmazása), ami eljárási különbséget jelent a nemzeti és a NATO (vagy EU) adatok kezelése során.

Fontos kérdés a nem minősített adatok kezelésére vonatkozó eljárások közötti eltérés. *A NATO, EU nem minősített kategóriájú adat illetéktelen megismerés ellen védendő*. Nemzeti eljárás szerint a nem minősített nemzeti adat *kérésre megismerhető*, *sőt nyilvánosságra is hozható (*mert a megismert adat nyilvánosságra hozatala alkotmányos alapjog), de ez a lehetőség a gyakori vélekedések ellenére nem vonatkozik a NATO, EU nem minősített (UNCLASSIFIED) adat megismerhetőségére.

A nemzeti nem minősített kategóriájú adatok védtelensége problémát jelent, mert pl. egy hálózat védelmi rendszabályainak nagy része ebbe a kategóriába tartozó adat, de ezen adatok nyilvánosságra kerülése nyilvánvalóan ellentétes az MH érdekeivel.

Az egyre nagyobb adatmennyiség az MH-nál is elektronikus iratkezelést igényel. Ennek lényege a szervezet által kapott dokumentumok elektronikus ügyirattá történő alakítása, iratkezelő rendszerben történő azonosítása, rögzítése, az ügyiratok közötti kapcsolati rendszer központi akarat szerint történő kialakítása (beleértve azt is, hogy az ügyintézés során a dokumentumok elektronikus formából papír alapúvá alakuljanak és viszont) az ügyiratok nyomon követése, ellenőrizhetősége és visszakereshetősége. Az iratkezelési folyamatok során biztosítani kell az illetéktelen megismerés/beavatkozás kizárását *a dokumentumok teljes életciklusára vonatkoztatva*. A rendszerben történő kezelési és felügyeleti műveletek folyamatosan rögzítettek, az ezzel kapcsolatos naplózási adatok megváltoztathatatlanok legyenek, illetve a rendszerből kivont dokumentumok tárolása, visszakereshetősége az irattározásra vonatkozó követelmények szerint történjen.

A honvédelmi tárcánál az elektronikus iratkezelésre történő áttérés érdekében 2005-ben megtörtént a kormányzati szférában üzemelő rendszerek tanulmányozása, melynek eredményeképpen az informatikai, ügyviteli és elektronikus információvédelmi szakterületekből álló bizottság az MH Iroda-automatizálási Rendszerbe integrált, portál szolgáltatás alapú elektronikus iratkezelés kifejlesztése mellett döntött (mert az elérhető iratkezelési rendszerek zömében csak részmegoldásokat nyújtanak). A helyzetet bonyolítja, hogy jogszabály jelenleg nem rendelkezik a minősített elektronikus adat készítéséről, nem határozza meg az ehhez szükséges folyamatot, illetve a vonatkozó speciális követelményeket.[22]

Az elektronikus iratkezelés mellett az adatbázisok kezelését lehetővé tevő meta-adatok, a hálózatok címtárai, a hitelesítés szolgáltatáshoz szükséges adatok védelmi és interoperabilitási kérdései mutatják az egyre halmozódó szakterületi feladatokat.

A dokumentumvédelmi szakterülettel kapcsolatos tapasztalatom, hogy *a gyakorlat az MH-nál már több éve meghaladta azt a szintet, ahol az adatkezelés csak papír alapú dokumentumkezeléssel egyenértékű. Emiatt szükségét érzem a szakterület hatáskörének, feladatainak a komplex adatkezelési folyamatokhoz történő igazítását, és felhasználói igények által megkívánt összetett, multimédiás szolgáltatások támogatására történő átállást.*

2. 1. 4. Elektronikus információvédelem

Az *elektronikus információvédelem (NATO terminológia szerint: electronic information security; INFOSEC)* a kezelt adatok-, az elektronikus adatkezelő rendszerek és támogató

[22] A közfeladatot ellátó szervezetek iratkezelését szabályozza ugyan, de meghatározza, hogy a rendelkezéseket minősített iratok esetében a külön jogszabályban rögzített eltérésekkel kell alkalmazni (a külön jogszabály 2005-óta még nem jelent meg).

infrastruktúráik védelme a *bizalmasság*, *sértetlenség* és *rendelkezésre állás* csökkenése ellen.[23]

E biztonsági célkitűzések mellett a különböző dokumentumokban egyéb célok is felbukkannak (pl. a „hitelesség" az EU hálózatbiztonságra vonatkozó ajánlásában, az „elszámoltathatóság" és az „assurance" (a másik négy célkitűzés teljesülésének garantálása értelmezésként) az Egyesült Államokbeli ajánlásban [78.]). Az említett célkitűzések mellett a „azonosítás"-t és a „visszautasíthatatlanság"-ot tartalmazza az Egyesült Államok Védelmi Minisztériumának „information assurance (IA)" meghatározása,[24] [79.] ami detektálási és reagálási képességeket is tartalmaz).

Az Egyesült Államokban, Egyesült Királyságban alkalmazott „information assurance" (IA) kifejezés 2006. közepétől egyre szélesebb körben terjedt el NATO-n belül is, majd 2007. áprilistól az elektronikus információvédelmi albizottság neve INFOSEC-ről „Information Assurace"-ra változott (egyenlőre tartalmi változás nélkül). Tapasztalataim szerint *ez a szövetségi megközelítés felülvizsgálatának közeledését jelzi, így célszerűnek tartom nemzeti szinten is a védelmi feladatok áttekintését, szükség szerinti pontosítását, melynek első lépése értelemszerűen a biztonsági célok újrafogalmazása.*

Az elektronikus információbiztonsági szakterület szabályozására vonatkozó bizonytalanságot, hiányosságokat jelzi, hogy *hazánk NATO-hoz való csatlakozásakor a NATO minősített adatok kezelését szabályozó első, 1999-es jogszabály még nem határozott meg elektronikus információbiztonsággal kapcsolatos követelményeket.*

A szakterület összetett, melynek védelmi feladatai a következőkben olvasható, négy fő területre tagolhatók.

2. 1. 4. 1. Rejtjelzés

Rejtjelezés minden olyan tevékenység, eljárás, amelynek során valamely adatot abból a célból alakítanak át, hogy annak eredeti állapota illetéktelenek számára rejtve maradjon. A rejtjelzés részét képezi a rejtjelzett adat eredetivé való visszaállítása is.[25] [80.]

---

[23] Az elektronikus információbiztonság kifejezés az Egyesült Királyság és az Egyesült Államok dokumentumaiban gyakran „information system security; ISS"-ként (információs rendszerbiztonság) olvasható.

[24] Az „Information Assurance" kifejezésnek nincs hivatalos magyar megfelelője. A szabványokban szereplő magyarázat szerint az „assurance" megfelelője: garancia, biztosíték, biztosítás, illetve a garancianyújtás, vagy bizalomkeltés folyamata.

[25] Az idézett jogszabály sarkalatos pontja, hogy az automatikus rendszerek mérési vagy vezérlési adatainak kódolását akkor sem tekinti rejtjelzésnek, ha az védelmi célokat szolgál (ebben az esetben a földi fegyverirányító rendszerek, vagy a föld-levegő automatikus rendszerek adatfolyamai nem lennének rejtjelzéssel védettek, ami katonai szempontból aggályos).

A szakirodalom a rejtjelzést *algoritmusok* szerint osztályozza. Más megközelítés szerint a rejtjelzéssel végzett védelem megvalósításához *rejtjelzésre* (eszközzel, vagy programmal végrehajtott kódolási és visszaállítási folyamatra), illetve az ezt támogató tevékenységekre *(rejtjeltevékenységre)* van szükség, tehát a védelmi rendszabályoknak lényegesen szélesebb területet kell lefednie, mint a kommunikáció közvetlen védelme (az adat rejtjelzéssel történő továbbítása).

A rejtjeltevékenység bizalmasságának fontosságát szemlélteti Simon Sign, amikor mások kutatásaira hivatkozva leírja, hogy egy rejtjelző eszközt gyártó cég hátsó ajtót (back door) épített eszközébe, amely megoldást átadott egy másik állam kormányának. [81.] A példán keresztül érzékelhető, hogy a szövetségi, vagy kétoldalú nemzetközi megállapodások (pl. a Gripen gépek lízingelése kapcsán a svéd-magyar együttműködés, vagy egy más ország által kifejlesztett eszköz engedélyezése) speciális rejtjelbiztonsági kérdéseket érintenek.

A NATO, EU és nemzeti követelmények szerint rejtjelzést kell alkalmazni minden olyan esetben, amikor a minősített adatok elektronikus átvitele során *a továbbítás átlépi a védett terület határát, vagy tárolás esetén a védelem másként nem biztosítható*.

A NATO TACOM Post-2000 programja jól szemlélteti a hálózatok rejtjelzéssel történő védelmének szélesedő feladatait: az állandó és tábori híradó és informatikai rendszerek átviteli útjainak védelme csoportos rejtjelző eszközökkel történik (bulk encryption), a harcászati és más vezeték nélküli eszközök adatátvitelének védelmét link rejtjelzés valósítja meg (link encryption). NATO KORLÁTOZOTT TERJESZTÉSŰ, vagy magasabb minősítés esetén a védelem egyedi rejtjelző eszközök feladata (end to end encryption). [82.]

Az üzemeltetés könnyítése érdekében megjelent a speciális védelmi elemekkel ellátott, un. CCI (Controlled Crypto Item) eszköz, amely csak meghatározott részegység beillesztése után képes a rejtjelző funkció ellátására.

A rejtjelzés alkalmazási körének bővülését jelzi, hogy a korszerű elektronikus adatkezelő rendszerek biztonsági mechanizmusait kriptográfiai módszerek támogatják (pl. azonosítás és hitelesítés, digitális aláírás, visszautasíthatatlanság, időbélyegzés). E biztonsági mechanizmusokat integráltan alkalmazza az *aszimmetrikus algoritmusú rejtjelzésen alapuló Nyilvános Kulcsú Infrastruktúra* (Public Key Infrastructure; PKI) rendszer.

A technikai fejlődés és a hálózatok szerepének növekedése miatt megjelent az elektronikus kulcselosztás, a távkulcsolás követelménye, ami szintén bővülő feladatokat jelent (pl. rejtjelző kulcs rejtjelzéssel történő továbbítása, kulcs hitelességének megerősítése).

A közérdekű adatok *nem csak minősített adatok*, és az illetéktelen beavatkozás vagy lehallgatás elleni védelem gyakran csak rejtjelzéssel valósítható meg, így *az MH*

rejtjeltevékenységért felelős szervezeti elemeinek a kereskedelmi forgalomból beszerzett rejtjelző eszközök, alkalmazások menedzselésével ki kell egészíteni a hagyományosan értelmezett rejtjeltevékenységet. Ezen a területen megjegyzendő, hogy *a közigazgatásban alkalmazható, a kereskedelmi forgalomból beszerezhető rejtjelző eszközök (alkalmazások) tekintetében nincs iránymutató hazai ajánlás*, így a különböző szervezetek közötti kapcsolatok védelme a partnerek eseti megoldásai szerint kialakítottak. A hiányzó kormányzati szabályozás kialakítását támogatják a Gazdasági Együttműködési és Fejlesztési Szervezet (Organisation for Economic Co-operation and Development; OECD) rejtjelzésre vonatkozó irányelvei: a megbízható rejtjelző eljárások kialakítása, a különböző eljárások közötti választási lehetőség biztosítása, nyílt piaci ösztönzés a rejtjelző eljárások fejlesztésében, szabványok kialakítása, magántitok és személyi adatok védelme, kötelezettségvállalás, a nemzeti rejtjelzésre vonatkozó politika törvényes hozzáférhetőségének biztosítása. [83.]

Az irányelvek érvényesítése érdekében az OECD javasolja az irányelvek szerinti eljárások, rendszabályok és elvek kialakítását, a nemzeti és nemzetközi szintű konzultáció és együttműködés erősítését és intézményesítését, valamint nyilvánosan elérhető, pontosan meghatározott kormányzati felhatalmazások kialakítását. [84.]

Megállapítom, hogy a nyilvánosan hozzáférhető jogszabályok és ajánlások a fentieknek megfelelő általános keretrendszerű irányelvekkel, állásfoglalásokkal nem támogatják a köz és magánszféra adatainak rejtjelzéssel történő védelmét. A nem minősített adatok védelmét rejtjelzéssel megvalósító feladatok kormányzati támogatása jelenleg nem megoldott.

Az érvényben lévő, a minősített adatok védelme érdekében alkalmazott rejtelzést általánosan szabályozó jogszabály gyakorlatilag a hatósági felügyeleti és ellenőrzési eljárást támasztja alá. Szakmai érdekességnek tekinthető, hogy az 1994-es kormányrendelet a NATO és EU csatlakozáskor nem módosult. A szövetségi hatóságokkal való együttműködés, a kutatás-fejlesztés, az engedélyezési eljárásokhoz szükséges kapcsolattartás tartalmazhat olyan feladatokat, amelyeket célszerű lenne a jogszabályban átvezetni.

2. 1. 4. 2. Kompromittáló kisugárzás elleni védelem

Az elektronikus adat nem szándékos, vezetett, vagy sugárzott elektromágneses (vagy egyéb) energia által történő illetéktelen megismerését a *kompromittáló kisugárzás elleni védelem* (Emission Security; EMSEC) rendszabályai is akadályozzák. Az ilyen energia illetéktelen detektálása azért veszélyes, mert *az üzemeltető, alkalmazó szervezetek által*

érzékelhetetlenül képes a kezelt adatok kompromittálására (vagy rendszerinformációk megszerzésére).

A kompromittáló kisugárzás (compromising emanations) elleni védelmi rendszabályok az *elektronikus adatokat kezelő eszközökre* és/vagy az *üzemeltetési környezetre* irányulnak. Az eszközöket olyan aktív és/vagy passzív védelmi elemekkel kell kiegészíteni, amelyek a nem szándékosan kisugárzott jeleket árnyékolják, vagy semlegesítik (a feladatkör hazánkban is „TEMPEST”-ként közismert).

Védendő eszköz alatt nem csak a végberendezéseket kell érteni, hanem minden olyan eszközt (kapcsolók, szerverek, egységeket összekötő kábelek, egyéb kábelek stb.), amelyek részt vesznek az adatkezelésben. Az eszközök védelmének kialakítása *a tervezőasztalon kezdődik* az alkalmazott alkatrészek kiválasztásával (minimális kisugárzott energia), az áramkörök felépítésével (a védendő adatokat kezelő elemek elkülönítésével; un. RED/BLACK elkülönítés[26]), szűrő és földelő elemek, esetleg sugárzó alkatrészek kiválasztásával.

Az üzemeltetési környezet is kialakítható hasonló védelmi rendszabályokkal,[27] így lehetővé válik kereskedelmi forgalomból beszerzett eszközök alkalmazása (pl. szerverterem esetében). A védelem másik módja olyan *biztonsági távolságok* kialakítása, amelyen kívül értékelhető jel detektálása már rendkívül alacsony valószínűségű.

A kompromittáló kisugárzás elleni védelem NATO, EU rendszabályai az adatkezelő eszköz kialakítására és az üzemeltetési környezetre vonatkozó követelményből, a biztonsági távolságból és a minősítési szintből tevődnek össze.

A nemzeti adatok esetében jogszabályban rögzített, kompromittáló kisugárzás elleni védelmére vonatkozó követelmény nincs.

2. 1. 4. 3. Átviteli utak védelme

Az *átviteli utak védelme* (Transmission Security; TRANSEC) az adatok és vezérlő jelek védelmét jelenti az elfogás, az átviteli folyamatba történő beavatkozás, vagy a jogosulatlan felhasználás ellen. Ennek hiányában lehallgatással, forgalomanalízissel olyan adatokat lehet összegyűjteni, amelyek támogatják az információs rendszerek elleni támadást; megtévesztéssel többfajta módon is zavart lehet okozni a hálózatokban, vagy egyéb módon lehet befolyásolni a hálózat működését. Az ITU-T X.800 ajánlás szerint rejtjelző

[26] A „RED” a védendő adatot nyílt formában kezelő részegység, eszköz jelzése, a „BLACK” pedig a rejtjelzett (vagy illetéktelen megismerés elleni védelmet nem igénylő) adatot kezelő részegység, eszköz jelzése.

[27] Annak ellenére, hogy más fenyegetettség ellen nyújtanak védelmet, a létesítmények, illetve eszközök védelmi rendszabályaihoz csatlakoztatható az elektromágnese impulzusok elleni védelem követelményrendszere.

mechanizmusok is támogatják az adatfolyam megfigyelése és/vagy módosítása, a forgalomanalízis, a visszautasítás, a meghamisítás, az engedély nélküli hálózathoz csatlakozás és az üzenetek változtatása fenyegetések elleni védelmet. [85.]

Az adatoknak a meghatározott védelmi szintnek megfelelően a teljes átviteli úton védettnek kell lennie. A híradó és informatikai infrastruktúrában a kommunikációs protokollok és a hálózatfelügyelet összes lehetőségét fel kell használni (pl. jelsorozatok ellenőrző összegei, hibajavító kódolások, térkitöltés, a kapcsolóelemek és átviteli berendezések vezérlésének szigorú kézben tartása).

A korszerű vezeték nélküli átviteli üzemmódok (pl. frekvenciaugratás, szórt spektrum, speciális burkológörbék) is az átviteli utak védelmét látják el, amelyek kiegészíthetők egyéb megoldásokkal (pl. speciális antennák alkalmazása). A NATO egységesített linkjeinek újabb változatai már beépített rejtjelzési képességekkel rendelkeznek (pl. Link 4, 16, 22).

2. 1. 4. 4. Informatikai védelem

Az *informatikai védelem* kormányzati ajánlás szerint „az informatika rendszer azon jellemzője, amely az informatikai rendszerekben kezelt adatok, bizalmassága, hitelessége sértetlensége és rendelkezésre állása, illetve a rendszerelemek funkcionalitása és rendelkezésre állása szempontjából teljes körű, zárt és kockázatokkal arányos biztonságot jelent a szervezet számára”.[28] [86.] Külföldi források (pl. a NATO, az EU, az Egyesült Államok vagy az Egyesült Királyság dokumentumai), vagy információbiztonsággal foglalkozó szabványok ehhez hasonló meghatározást nem említenek, informatikai területen is az elektronikus információvédelemre vonatkozó meghatározást alkalmazzák.

Az elektronikus adatok biztonsága biztonsági funkciókon keresztül valósul meg. Ezeket először az Egyesült Királyságban az Information Technology Security Evaluation Criteria (ITSEC; IT Biztonsági Értékelési Kritériumok) fogalmazta meg, mely szerint nyolc funkció más-más szintje látja el a rendszerek és adatok védelmét,[29] [87.] majd a Közös Követelmények (Common Critéria) több követelményrendszert összegyúrva és továbbfejlesztve alakította ki a biztonsági funkciók jelenlegi rendjét.[30] [88.]

---

[28] A NATO AAP-31 a Computer Security (COMPUSEC) kifejezést használja e szakterületi feladatok azonosítására (újabb NATO kifejezés a számítógép és számítógép hálózat biztonság), ami tartalmilag szinkronba hozható egyre gyakrabban „IT Security”-ként azonosított „informatikai védelem”-mel.

[29] A nyolc funkció: azonosítás és hitelesítés, hozzáférés-felügyelet, elszámoltathatóság, audit, újrahasználhatóság, hitelesség, adatcsere védelem, megbízható szolgáltatások.

[30] Az említett biztonsági funkciók mellett megjelent pl. a felhasználói adatok védelme (User Data Protection), a biztonsági menedzsment (Security Management) személyi azonosítást megvalósító adatok védelme (Privacy), a biztonsági funkciók védelme (Protection of the TOE Security Functions), és az erőforrás-felhasználás (Resource Utilization).

Kormányzati szándék szerint hazánkban is ki kell alakítani az informatikai alkalmazások hiteles tanúsítási rendjét, eljárásait, így *az MH-nak is fel kell készülnie e szabvány alkalmazására*. [89.]

A Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS) 0.95 (publikált tervezet) az informatikai termékek és rendszerek tanúsításához az ITB 12. ajánlásában foglalt kategóriák támogatására a Közös Követelmények EAL 2-4 szintjeit alapul véve azonosított tanúsítási követelményeket.[31] [90.] Ez informatikai területen előrelépést jelent abban az esetben, ha a NATO, EU rendszabályok KORLÁTOZOTT TERJESZTÉSŰ, BIZALMAS és TITKOS minősítéshez EAL-3-as, és SZIGORÚAN TITKOS minősítéshez EAL-4-es szintet rendelnek, *és a magyar nemzeti követelmény nem lazítja fel a Közös Követelmények előírásait*.

Megjegyzem, hogy a többi információvédelmi szakterület rendszabályaival kapcsolatos hiányosságokat e tanúsítási rend bevezetése nem szünteti meg.

A rendszer kialakításakor a besorolásnak megfelelő szintű tanúsítással rendelkező elemek kerülhetnek felhasználásra. Az eszközök életciklusa során az első és az utolsó időszak kritikusnak tekinthető, így kerülni kell a prototípus jellegű eszközök (megoldások) alkalmazását (kiértékelhető üzemidő, karbantartási és anyagellátási háttér hiánya), valamint törekedni kell a korszerűtlen eszközök kiváltása. Emellett biztosítani kell a rendszerek bővíthetőségét és fejleszthetőségét (felfelé való kompatibilitás).

Az *üzemeltetési környezet* kialakításakor a fizikai védelmi elemek mellett szükség szerint biztosítani kell a fűtést és légkondicionálást, a por és egyéb szennyeződésektől való védelmet, a kábelezések védelmét (központok, rendezők, föld alatti és feletti hálózatrészek és elosztópontok, szolgálat hozzáférési pontok), valamint a szükséges villámvédelmet és földelést.[32]

A hálózati elemeket és végberendezéseket *fontosságukkal arányosan* szünetmentes táplálással kell ellátni, vagy az egész rendszer erősáramú betáplálását többszörözni kell, esetleg a létfontosságú rendszereket autonóm áramellátási rendszerrel kell biztosítani.

Gyakori probléma, hogy a rendelkezésre állás érdekében szükséges rendszabályok a köztudatban az MH-nál is gyakran a minősítési szinthez kapcsoltak. Valójában nem azért kell

---

[31] EAL: Evaluation Assurance Level (biztonsági értékelési szint).

[32] Amennyiben a biztonság szintje megköveteli, a létesítmények életvédelmi földelése mellett biztonsági földelési rendszert is ki kell alakítani, amelyet az infrastruktúrához tartozóan kell karbantartani, és időszakos mérésekkel kell hitelesíteni (a földelés ellenőrzésére vonatkozó követelmény a külföldi minősített adatok védelmére vonatkozó kormányrendeletben nem egyértelmű, ami rengeteg félreértést okoz még napjainkban is).

egy számítógépet szünetmentes áramellátással ellátni, mert pl. TITKOS minősítésű adatokat kezel, hanem azért, mert *az adatfeldolgozásra vonatkozó követelmény nem engedélyez kiesést*!

Üzemeltetés területén a rendszer egészéhez az adatkezelő képességek fontosságának megfelelő szerviz hátteret kell kialakítani, és a berendezés fontosságának arányában kell meghatározni a hibaelhárításra vonatkozó követelményeket (helyreállítási eljárások, alkatrészek megelőző jellegű cseréje, kulcsfontosságú javítóanyagok készletezése), ami jelzi, hagy a különböző szolgáltatási szerződéseknek (pl. átalánydíjas javítás, karbantartási, anyagellátási szerződések) több biztonsági vetülete is van.

Az adatvesztés elkerülése érdekében a kezelt adatok fontosságával arányos *biztonsági mentési eljárásokat* kell kialakítani, amelynek a felhasználói adatok mellett ki kell terjednie a szükséges működési paraméterek (pl. felhasználói profilok, konfigurációs adatok) és a naplózási adatok mentésére is.

A *hardver és szoftver védelmet* a rendszerek összetevőinek *védelmi funkcióira*, valamint a rendszerekben kifejezetten a *biztonság érdekében telepített elemekre* lehet bontani.

Illetéktelen beavatkozás ellen az eszközöket szükséges mértékű védelmi mechanizmusokkal kell ellátni (felbontás elleni védelem; tampering). Bonyolultabb esetben a berendezés dobozának felnyitása hálózati riasztást vált ki, míg egyszerűbb esetben ezt a feladatot biztonsági fóliák felragasztása és ellenőrzése is elláthatja.

Az illetéktelen beavatkozások ellen a hardver, szoftver konfigurációt hálózati szinten szoftveres felügyelettel kell biztosítani.

A rendszerprogramok védelmének alapja a szabályos telepítés, a meghatározott biztonsági beállítások teljes körű alkalmazása, és a *használaton kívüli funkciók kikapcsolása*.

Csak sértetlen (szükség esetén teszt környezetben ellenőrzött) kereskedelmi forrásból beszerzett, jogtiszta felhasználói programok, programcsomagok (szöveg és táblázatszerkesztők, böngészők, levelezőprogramok stb.), adatbázis-kezelők, és kiegészítő programok (fájlkezelők, tömörítők, hang és képmegjelenítők stb.), illetve a felhasználói igényekre specializált, *megfelelő körülmények között kialakított egyedi fejlesztésű programok vehetők alkalmazásba*. Az Európa Tanács e-kormányzatról szóló 15/12/2004 számú ajánlása ösztönzi a tagállamokat az információs és kommunikációs technológiák használatára, melynek során a nyílt szabványok és a különböző szoftverek, akár *nyílt forráskódú modellek használatának a lehetőségét is vizsgálni kell, ami nem kerülheti el az MH-t, még a minősített adatkezelő rendszerek esetében sem.* [90.]

A rosszindulatú programok (számítógép vírus, féreg, logikai bomba, trójai program, kémprogramok, fürkészők stb.), kéretlen levelek (SPAM), valamint mobil kódok elleni

védelem egyre összetettebb, már a *minimális védelmi szinten is megjelenő feladat*. A védelem a folyamatos víruskeresésen, sértetlenség ellenőrzésen, tartalomszűrésen, naplózáson, szükség szerinti elszigetelésen alapul. Ugyanígy alapvető követelmény a szükséges mértékű azonosításhoz és hitelesítéshez szükséges eljárások kialakítása.

Összekapcsolás esetén a hálózatok egymás környezetét képezik, ami *biztonsági kockázatot* jelent (pl. csatlakozások más rendszerek felé, eltérő védelmi rendszabályok). A hálózatok védelme érdekében az összekapcsolás szintjének, az adott technológiának és üzemeltetési körülményeknek megfelelő *védelmi mechanizmusokat* kell kialakítani a demilitarizált zónákban elhelyezett tűzfalak (firewall) behatolás detektáló (Intrusion Detection System) és behatolás megelőző (Intrusion Prevention System) megoldások (hardver és/vagy szoftver elemek), virtuális magánhálózat (Virtual Privat Network; VPN) és rejtjelzés formájában. Nyilvános hálózatokhoz történő csatlakozás esetén alkalmazni kell a támadó fél megtévesztésére (és lehetőség szerint azonosítására) szolgáló csapdákat (honey pot) is.

A vonatkozó nemzeti ajánlásban hálózatok összekapcsolásával kapcsolatban általános követelményként szerepel, hogy kétoldalú adatcserét biztosító összekapcsolás csak azonos minősítésű rendszerek között valósítható meg, eltérő minősítési szintek között csak egyirányú adatcsere engedélyezett. [92.] Az Egységes Kormányzati Gerinc (EKG) biztonsági szabályzata rendszer-specifikusan, ennél részletesebben fogalmaz. Meghatározza, hogy az EKG-hez csatlakoztatott rendszer más külső kapcsolattal nem rendelkezhet, összekapcsolás csak a kidolgozott csatlakozó felületeken lehetséges, a csatlakozó szervezet minden szerverét és munkaállomását védeni kell vírusok és rosszindulatú programok ellen, pontosan nyilván kell tartani a csatlakoztatott elemeket, illetve a biztonságos kommunikáció érdekében az EKG tagok között VPN kapcsolatokat kell kialakítani.[33] [93.]

Szövetségi viszonylatban a szervezetek működéséhez szükséges szövetségi-nemzeti, és szövetségi - nem NATO államok, szervezetek közötti adatcserét a hálózatok összekapcsolására szolgáló, az üzemeltetési felelősség szerint kategorizált átjárók (Information Exchange Gateway; IEGW) végzik. [93.]

A hálózatok összekapcsolásánál megemlítendő az adatok megosztásának Szövetség szintű támogatására szolgáló NATO Adat Stratégia (NATO Data Strategy), ami öt cél megvalósításán keresztül támogatja a megosztásra vonatkozó „duty to share” elv

[33] A jogszabály szerint követelmény az MH zártcélú hálózatának és az EKG összekapcsolása. Ez egyes esetekben könnyítést és esetlegesen megtakarításokat eredményezhet (pl. Internet szolgáltatással történő ellátás, kormányzati szervezetekkel történő összekapcsolás az EKG által biztosított szabvány felületeken, hálózati tartalék átviteli utak kialakításának lehetősége), más esetben pedig nehezíti a helyzetet (EKG-n kívüli összekapcsolásokra vonatkozó engedélyezési eljárás).

megvalósítását: *az adatok láthatósága*, *elérhetősége*, *koherenciája*, *a szükséges biztonsági szint szavatolása* (kibocsátó azonosítása, sértetlenség biztosítása, az adat életútjára, biztonsági szintjére és hozzáférésekre vonatkozó adatok elérhetősége), és *interoperabilitás*. [95.]

Az egy szervezet által üzemeltetett és felügyelt hálózatok helyett napjainkban a több szervezetet kiszolgáló összekapcsolt hálózatok kerülnek előtérbe (nemzeti és nemzetközi szinten egyaránt), így a „cracker, hacker" típusú külső támadás feltételezése mellett az *összekapcsolt hálózatokból eredő, és a hálózaton belüli fenyegetéseket az eddiginél hangsúlyosabban kell figyelembe venni*. A kapcsolódó hálózatokat nem szabad automatikusan alacsonyabb biztonságú környezetnek tekinteni, hanem *előtérbe kell helyezni a védelmi mechanizmusok és biztonsági menedzsmentek együttműködésének kérdéseit*.

Szemléletbeli változást igényel, hogy a védelem napjainkban már nem csak különböző védelmi elemek beépítését és felügyeletét, hanem meghatározott szempontok szerint biztonságosnak tekintett *hálózat kialakítását és üzemeltetését jelenti*. Az összekapcsolásra vonatkozó általános követelmények megfogalmazása, a belépési és összekapcsolási pontok szolgáltatási szintek szerinti csoportosítása, specializálása (ezen belül az adott alkalmazásoknak megfelelő részletes feladatok kidolgozása), a meghatározott esetekre korlátozott távoli hozzáférések biztosítása, a központi jogosultságkezelés, fontossága az MH-nál nagyságrendekkel növekszik.

Az elektronikus adatkezelő rendszerek biztonságát időszakosan megismétlődő, többfokozatú behatolás ellenőrző tesztekkel, hálózati szkenneléssel, komplex biztonsági auditok végrehajtásával kell támogatni, ami új humán és technikai területű erőforrások kialakítását és folyamatos fejlesztését teszi szükségessé.

A hálózatok egyre bonyolultabbá válása megköveteli a host és a hálózati érzékelési mechanizmusok együttes alkalmazását, illetve a rendellenességeket jelző, eltérő forrású hálózati adatok összevetésével a biztonsági események és meghibásodások magasabb szintű kiértékelését, megfelelően automatizált riasztási és reagálási mechanizmusok meglétét, ami az MH-nál az egységes hálózat kialakítására vonatkozó új védelmi rendszabályok rendszerbe állítását teszi szükségessé.

Az internet hozzáférés a különböző szolgáltatásokon keresztül (levelezés, böngészés, file transzfer) más-más veszélyt hordoz, és specifikus védelmi rendszabályokat igényel. A katonai szervezeteknek egyre nagyobb mértékben van szüksége a nyilvános hálózatok szolgáltatásainak elérésére, így a védelmi rendszabályok a jövőben át fogják írni a jelenlegi általánosnak tekinthető fizikai elkülönítésre, az azt kiegészítő folyamatos vírusellenőrzésre, a

programok sértetlenségének ellenőrzésére, valamint a felhasználók tudatos viselkedésére épülő eljárásokat.

Az említett védelmi feladatok és az első fejezetben idézett, az internettel kapcsolatos fenyegetések aktualitását legjobban az Észt Köztársaságot ért, interneten keresztül történő támadás (több forrás szerint internetháború) mutatja.

Az eset részletes elemzése nélkül is megállapítható, hogy a szándékos, a hálózatok és szolgáltatások blokkolására, rongálásra szolgáló műveletek egyértelműen EU-s és NATO-s irányelveket, nemzetközi egyezményeket és nemzeti jogszabályokat sértenek. *Ezek a cselekmények egyértelműen elitélendők, mert jogokat korlátoznak, súlyos károkat okozhatnak az államigazgatásnak, a gazdaságnak és egyéneknek*. A nemzetközi médiában megjelenő vélemények, nyilatkozatok már az első napokban felvetették a NATO tagállam megtámadása esetén nyújtandó – eddig példa nélküli – segítésnyújtás szükségességét, amivel általánosságban egyetértek, de annak *formáját kidolgozatlannak tartom*.

Az Egyesült Államok informatikai védelemre vonatkozó mérési irányelve a védelmi rendszabályok elégtelenségének okaként a következőket azonosítja: nem elég hatékony erőforrások (pl. pénzügyi, személyi), képzési hiányosságok (felhasználói vagy telepítéskor, fenntartás során szükséges ismeretek, hiányos adminisztráció), szoftver frissítési hiányosságok, konfiguráció menedzsment problémák, szoftver kompatibilitási problémák, hiányosság a biztonság tudatosság területén, hiányosságok az alkalmazott biztonságpolitika és eljárások területén, rendszer vagy biztonsági architektúra problémák, nem hatékony mérési megoldások. [96.]

A problémák, és azok kombinációjának feltárása, a tényleges sérülések és a külső-belső körülmények pontos ismerete nélkül a helyzet elemezése veszélyes. Szakértői csoportok kiküldése, általános fenyegetések elhárítására irányuló technikai segítség támogathatja az elhárítást, de sajnos nem oldhatja meg véglegesen a biztonsági problémákat. Egy nemzeti infrastruktúra, amely nagymértékben összekapcsolt a nyilvános hálózatokkal, nyilvánvaló veszélyforrás. A megfelelő szintű védelem tervezése, kialakítása és fenntartása a teljes életciklus lefedésével, és folyamatos felügyeleti, felülvizsgálati eljárásokkal biztosítható. *Jelen értekezés fejezetei szemléltetik a védelem összetettségét, a szükséges erőforrások meglétének fontosságát, ami külső támogatással erősíthető, de tartósan nem pótolható.*

A megoldás alapjának az érintett nemzet koordinált, igények szerinti támogatását tartom. A hangsúlyt a további, hasonló eset megelőzésének támogatására, és az azonnali érzékelő és reagáló képességek kialakítására helyezem. Fontosnak tartom, hogy a lehetséges

szakmai fórumokon történjen meg a tapasztalatok értékelése, és a szükséges területeken erősödjön a lehetséges új megoldások felkutatása.

Az adatok megléte mellett speciális kérdés a megsemmisítés, mert a rövid életciklusú adatok felesleges kezelése erőforrásokat von el, és kockázatot hordoz. A technológia fejlődésével egyre komolyabb helyreállítási technikák alakulnak ki, így *az elektronikus adatok, illetve adathordozók szakszerű megsemmisítése is összetett feladattá vált*. Kiemelten kell kezelni azoknak az adatoknak a megsemmisítését, amelyek *más* (esetleg minősített) *adatokhoz biztosíthatnak hozzáférést* (pl. rejtjelkulcsok), valamint a *minősített adatok törlését*. Nemzeti ajánlás vagy jogszabály *nem határoz meg elektronikus adatok törlésére vonatkozó követelményeket,*[34] így az MH szervezeteinél a külföldi tapasztalatokra támaszkodó egyedi megoldások jellemzők.

A rendszerből történő szoftver kivonás, adatok archiválása esetén specifikus feladatként jelentkezik az érintett szoftverek, a működtetésükhöz szükséges hardver környezet megléte, a kezeléshez szükséges dokumentáció tárolása, a hozzáférési jogosultságok meghatározása.

Az informatikai védelmi feladatok áttekintése alapján megállapíthatom, hogy a gyakran hardver, szoftver (és firmver) védelemre egyszerűsített rendszabályok informatikai területen nem képesek megvalósítani a biztonsági célokat.[35] Az informatikai védelmet a kockázatelemzésre támaszkodva, a rendszerek összetevőinél értelmezhető biztonsági funkciók, az üzemeltetési környezetben az egyéb területű információvédelmi szabályok kialakításával és menedzselésével (felelősségi rend, szabályozás, akkreditálás, ellenőrzés, képzés) lehet elérni.

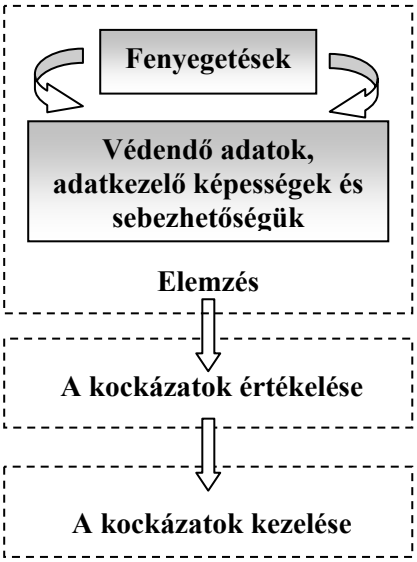
2. 2. A kockázatok kezelése

A biztonsági osztályokhoz rendelt védelmi rendszabályok nem minden esetben elégségesek, ami szükségessé teszi a kockázatok feltárását és a szükséges lépések megtételét (a védelem megerősítése, vagy a kockázatok egyéb formájú kezelése lásd: 6. sz. ábra).

---

[34] Az „X nemzetközi tapasztalattal rendelkező/NATO beszállító cég is ezt a programot ajánlja” vagy az „Y közigazgatási szerv is ezt a megoldást használja” típusú szakértői vélemények gyakran hátráltatják a szakmailag alátámasztott döntések előkészítését.

[35] Ezt a megfogalmazást alkalmazza pl. a nemzetközi szerződés alapján átvett, vagy nemzetközi kötelezettségvállalás alapján készített minősített adat védelmének eljárásairól szóló kormányrendelet, és az elektronikus információvédelemről szóló HM utasítás.



6. ábra: A kockázatok menedzselése

Az általános követelményeket tartalmazó jogszabály alapján a költségvetési szerv vezetőjének kockázatelemzési rendszert kell üzemeltetnie. Objektív kockázatelemzési módszer alkalmazásával fel kell mérni a tevékenységben rejlő kockázatokat, és meg kell határozni a csökkentésükre, megszüntetésükre irányuló intézkedéseket. [97.]

Az *MH (vagy más közigazgatási szerv) adatkezelésével kapcsolatos kockázatfelmérésre és elemzésre vonatkozó részletes kormányzati követelmény nincs.*[36]

Az említett általános követelmények alapján kialakított MH kockázatelemzési szabályzat meghatározza, hogy a kockázatelemzési folyamatokat évente felül kell vizsgálni, és a változásokat a kockázat-nyilvántartásban át kell vezetni. [98.] A kockázatelemzési szabályzat *külső*, *pénzügyi*, *tevékenységi* és *emberi* kockázatokra bontja a vizsgálandó területeket. A szervezeti kockázatokra vonatkozó feladatokon túl *az adatkezelésre vonatkozó kockázatok felmérésére és menedzselésére irányuló feladatrend nincs részletesen kidolgozva*. Az adatkezeléssel kapcsolatos általános kockázatfelmérő és elemző feladatrend kialakításához az említett követelmények mellett még a következők állnak rendelkezésre:

- a közfeladatot ellátó szerveknek az elektronikusan érkezett irat átvételét meg kell tagadni, ha az *biztonsági kockázatot jelent a fogadó szerv számítástechnikai rendszerére* (kockázatelemzésre vonatkozó követelményt a jogszabály nem azonosít); [99.]
- a NATO, EU elektronikus adatkezelő rendszerek biztonsági rendszabályait a NATO (és NYEU), EU biztonsági követelményeire és *a helyszíni kockázat értékelésre kell alapozni* (a jogszabály a kockázatelemzést nem részletezi); [100.]

[36] Csak a Pénzügyminisztérium alakított ki a pénzügyi szférára vonatkozó általános útmutatót.

- a közigazgatási hatóságok iratkezelésére vonatkozó követelménye szerint *az informatikai célrendszer biztonsági kockázatait kétévente felül kell vizsgálni*, és a kockázatokkal arányos védelmet kell kialakítani; [101.]
- a Pénzügyi Szervezetek Állami Felügyeletének ajánlása szerint *a pénzügyi szervezetek védelmi rendszabályai a biztonsági kockázatokkal arányosak legyenek*, a kockázatelemzést legalább kétévente felül kell vizsgálni, melynek során célszerű a COBIT[37] módszertan vonatkozó fejezetét alkalmazni; [102.]
- az ITB 8. sz. ajánlás a CRAMM módszertan[38] alkalmazását javasolja a kockázatelemzéshez. [103.]

A vonatkozó irányelvek, ajánlások és szabványok figyelembe vételével, azokat tapasztalataimmal kiegészítve *az MH-nál az adatkezelésre vonatkozó, a kockázatkezelést megelőző feladatokat* a következőként tartom célszerűnek kialakítani:[39]

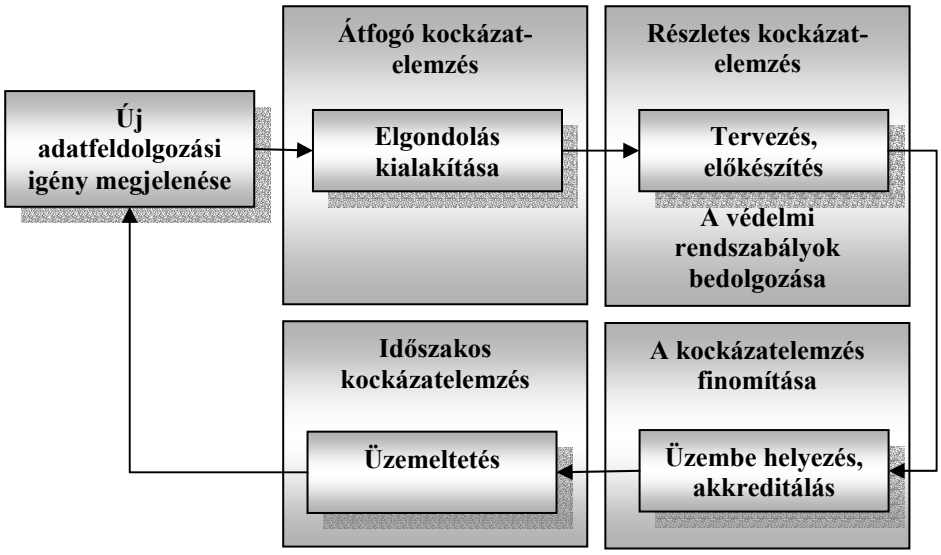
- *A szervezet elé kitűzött feladatok, az ehhez szükséges információs képességek (és a rájuk vonatkozó követelmények) azonosítása.*
- *A védendő objektumok meghatározása és értékelése.* Az információs szempontból fontos objektumok számba vétele: *kommunikációs vagyontárgyak* (hardverek, szoftverek, információk), *személyek* (felhasználók, kiszolgálók és külső személyek), *környezeti tényezők* (épületek, létesítmények) és *tevékenységek* (műveletek). Az anyagi érték szerinti besorolással szemben a bizalmasság, sértetlenség vagy a rendelkezésre állás elvesztésének hatásának vizsgálatát részesítem előnyben (beleértve a helyreállítással kapcsolatos feladatokat is). Az értékeket elégségesnek tartom hármas skála szerint ábrázolni (pl. „alacsony”, „közepes” és „magas”).[40]
- *A fenyegetettség megállapítása.* A fenyegetések felmérése (és előfordulási valószínűségük meghatározása) gyakorlati tapasztalatokra támaszkodó fenyegetés lista alapján, kiegészítve a helyi sajátosságokkal. A valószínűség a *gyakoriság* (tapasztalatok, statisztikák), a *motiváció* (érzékelhető vonzerő és sebezhetőség, a rendelkezésre álló erőforrások) vagy a *földrajzi tényezők* (pl. ipari létesítmények

[37] COBIT: Control Objectives for Information and related Technology (informatikai felülvizsgálatra vonatkozó keretgyűjtemény).
[38] CRAMM: UK Government's Risk Analysis and Management Method (az Egyesült Királyságban alkalmazott kockázatelemzési és kezelési módszertan).
[39] A feladat meghatározása és a *kockázatelemzés feltételeinek megteremtése* (elemző és értékelő csoport kialakítása, munkafeltételek biztosítása) után.
[40] A szakirodalomban találhatók 4-6 fokozatú skálák is, egy ausztrál kockázatelemzéssel foglalkozó kézikönyv pl. 7*6-os mátrixot alkalmaz a fenyegetések és bekövetkezési valószínűségek ábrázolásához.

közelsége, szélsőséges időjárási viszonyok valószínűsége) értékeléséből állítható össze, szintén hármas besorolás szerint.

- *A sebezhetőség felmérése.* A fenyegetésekhez hasonlóan összeállított sebezhetőség listára támaszkodva hármas értékelési skálát alkalmazva a rendszerrel kapcsolatos sebezhető pontok számbavétele.
- *A kockázati szint meghatározása.* A sebezhető pontokra irányuló fenyegetések összerendelésével minden eset kockázati szintjének megállapítása.
- *A meglévő és tervezett védelmi rendszabályok azonosítása.* Azonosítani kell a védelmi rendszabályokra vonatkozó követelményeket, és a továbbfejlesztésre vonatkozó lehetőségeket.
- *Javaslat a kockázatok kezelésére.* Amennyiben a figyelembe vett fenyegetések, és a rendelkezésre álló védelmi lehetőségek között eltérés van, az illetékes vezetőnek dönteni kell, hogy a kimutatott kockázatokat *elfogadja,* vagy *csökkenti* (esetleg valamilyen módon áthárítja, vagy elkerüli). A védelmi rendszabályok által nem ellensúlyozott fenyegetésekre a szervezetnek folytonossági, helyreállítási, szükség esetén vészhelyzeti terveket kell kialakítani.

A kockázatelemzési és menedzselési feladatok számtalan módszertan szerint feldolgozottak, egységesen elfogadott nemzetközi, EU, vagy nemzeti módszertan nincs. Az alkalmazott listákkal, módszertanokkal kapcsolatos részleteket nem tárgyalva csak annyit emelek ki, hogy a kockázatelemzési folyamatnak az életciklust végig kell követnie (lásd 7. sz. ábra), dokumentáltnak kell lennie, a kimutatott kockázatoknak és meghatározott rendszabályoknak az adatkezelésért felelős vezető jóváhagyásával kell rendelkeznie.



7. ábra: A kockázatelemzés beépülése az elektronikus adatkezelő rendszerek életciklusába

Kritikus fontosságúnak tartom *az adatkezelő rendszerek komplex kockázatelemzését* és az üzemeltetésben, alkalmazásban érintett szervezeti elemek között megosztás elkerülését. Ez nemzeti kritikus infrastruktúrák esetében megköveteli *a kockázatelemzésre vonatkozó feladatok, paraméterek részletes kidolgozását és az üzemeltető, alkalmazó szervezetek felé jogszabályban történő megalapozását*.

A nemzeti ajánlás fenyegetésre, és sebezhetőségre vonatkozó listáinak frissítésekor a kezelhetőség, valamint az ismétlődések elkerülése érdekében egységes struktúrába kell önteni a vizsgálati területeket. Célszerű az eltelt időszak alatt keletkezett irányelveket, és más nemzeti ajánlások csoportosításait is figyelembe venni, amit az MH esetében még a katonai sajátosságokkal ki kell egészíteni. A szakirodalom tanulmányozása alapján célszerűnek tartom azt az egyszerű szabályt betartani, hogy *a vizsgált rendszerelemek közé nem szabad még egyszer általános megfogalmazásban biztonsági célokat felvenni* (pl. mint rendelkezésre állás), mivel azok fenyegetése vagy sebezhetősége *önmagában nem, csak valamilyen elemen (vagy azok halmazán) keresztül valósulhat meg, és így ez a hiba átfedéseket okozhat*.

A *listákat (adatbázisokat) időszakosan felül kell vizsgálni*, különben az ITB ajánlásokkal kapcsolatos gyakori érvényességi dilemma ismétlődik meg.

2. 3. Az elektronikus adatkezelő rendszerek védelmének kulcsfontosságú kérdései

A szervezetek, és a nem mindig áttekinthető terepnek tekinthető külvilág közötti határolás (belépő személyek és közlekedési eszközök azonosítása, rakomány ellenőrzése, a szükséges adatok rögzítése) kialakítása mellett *fel kell mérni azokat a negatív hatásokat, amelyek közvetlen befolyással lehetnek az adatkezelő rendszerek üzemben tartására* (pl. javítás, karbantartás, üzemanyag ellátás korlátozása, áramellátás kiiktatása). Az ilyen helyszíneken *megnövekszik a szerepe a környezeti események monitorozásának és a szélesen értelmezett tartalékképzésnek*.

A híradó és informatikai rendszer felügyelet nélküli elemeinek (pl. az állandó kommunikációs infrastruktúra átjátszó, vagy rádiófelvevő pontjai) tervezésekor a *reagáló erők reakcióideje* az elsődleges korlátozó tényező, így a környezeti hatásoknak megfelelő *behatolás-érzékelési* és *megbízható riasztási képességeket kell kialakítani, és a telepített eszközöket önvédelmi képességekkel kell ellátni*.

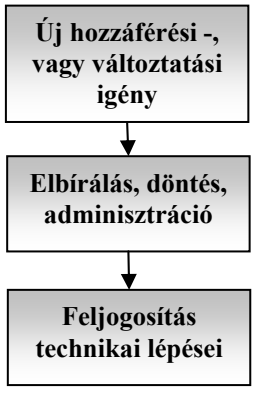
Tábori rendszer esetében a stabil létesítményekre támaszkodó, hordozható elemekkel megerősített védelmi területeken belül *a központi kiszolgálókat, hálózati elemeket, minősített adatkezelő munkahelyeket össze kell vonni*, és körülöttük áttekinthető, a kompromittáló kisugárzás elleni védelem szükséges mértéke szerinti adminisztratív zónát, jól használható

járőrözési útvonalakat, és megfelelő világítási rendszert kell kialakítani. A rendszerkocsik, konténerek csatlakozódobozainál, a rendezőknél biztosítani kell a zárhatóságot, és könnyen áttekinthető kábelezési rendszert kell kialakítani. A vezeték nélküli eszközöknél a csökkentett kisugárzású megoldások, különleges üzemmódok (pl. szórt spektrum, frekvencia ugratás), üzemeltetési adatok csatornán keresztül történő továbbítása, automatikus összeköttetés felvétel és fenntartás, végberendezések és bázisállomások közötti hálózati védelem, központi menedzsment lehetőségek (pl. rugalmas csoportszervezés, forgalomból történő kizárás) mellett az üzemeltetési adatok és rejtjelző kulcsok védelme érdekében *beépített védelmi megoldásokra* (pl. emelt szintű azonosítási követelmények, program és kulcstörlés, processzorok önmegsemmisítő képessége) van szükség.

Nem minősített, vagy KORLÁTOZOTT TERJESZTÉSŰ minősített adatok kezelése esetén a helyi biztonsági környezet kialakítása nem lehet probléma, mert az adminisztratív zónák *katonai objektumok esetében automatikusan rendelkezésre állnak*. Nagyobb szervezeteknél gyakori az „adminisztratív zóna az adminisztratív zónában” megoldás, ahol az azonos szervezeti alrendszerhez tartozók (jellemzően a törzs funkcionális egységei szerint) szervezeten belül is elkülönítettek.

Az ilyen besorolású adatok kezelésére általában kereskedelmi forgalomból beszerezhető eszközök és szoftverek alkalmazhatók a szükséges biztonsági beállításokkal és adminisztratív rendszabályokkal.

MH méretekben korszerű jogosultságkezelés csak jelentős fejlesztésekkel valósítható meg. A *jogosultság kezelést el kell választani az üzemeltetési feladatoktól*, és megfelelő, biztonsági mechanizmusokkal támogatott központi jogosultság menedzselési funkciókat kell kialakítani a szükséges dokumentálási feladatokat együtt (8. sz. ábra).



8. ábra: A hozzáférési jogosultságok menedzselése

A hozzáférések alkalmazásonként történő védelmére az egyedi jelszavas azonosítás nem tekinthető megbízhatónak, a feladatot egyszerűsített bejelentkezési eljárással (Single-Sign On; SSO) célszerű támogatni.

A végberendezések és hálózati eszközök nagy száma szükségszerűen új alapokra helyezi a hardver és szoftver konfiguráció felügyeleti (nyilvántartás, változáskezelés) feladatokat. Az eszközök speciális alkalmazásokkal történő felügyelete az üzemeltetés könnyítése mellett nyilvánvaló hasznokat hajt a biztonság területén is (illegális beavatkozások észlelése és jelzése), így *a változtatási igények azonosítását, elemzését, jóváhagyását vagy elutasítását, illetve a módosítások kivitelezését és a változtatások követését hálózati szolgáltatásként kell kialakítani*. Központi biztonsági szolgáltatásként kell kezelni a vírusok, rosszindulatú programok és mobil kódok elleni védelem, az azonosítás és hitelesítés, a jogosultságkezelés, a behatolás detektálás/megelőzés feladatait, valamint a programfrissítések, javító patch-ek menedzselését (9. sz. ábra).

9. ábra: Az MH hálózati struktúra célszerű változata

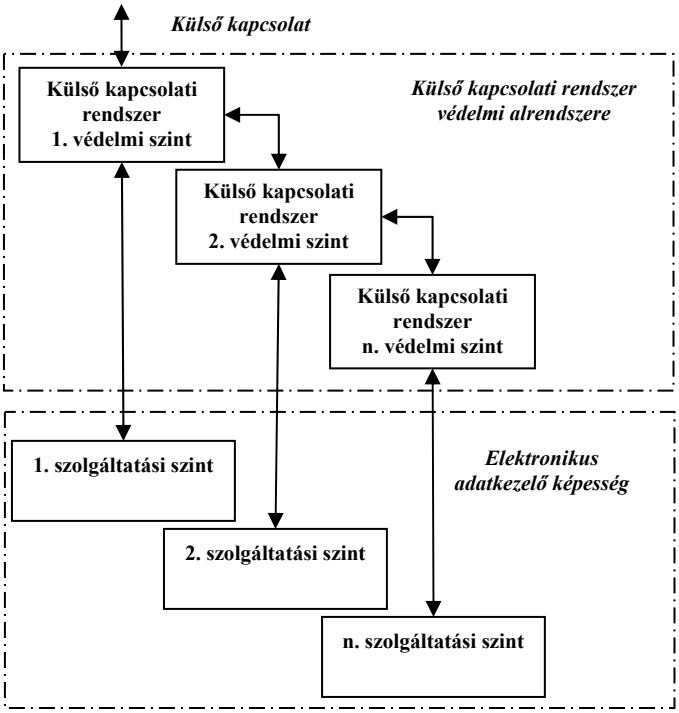
A nyilvános közlésre szánt adatok speciális védelmet igényelnek. A web oldalak könnyen támadás áldozatai lehetnek (pl. honlap tartalmának megváltoztatása, adatok törlése, szolgáltatás megakadályozása), így behatolás-érzékelő, riasztást végző és egyéb védelmi rendszabályokat alkalmazni (fizikai védelem, korlátozott számú hozzáférés engedélyezése, az oldalak automatikus frissítése, gyors helyreállító képességek).[41]

A korszerű munkavégzés távoli bejelentkezési képességeket is igényel, amely esetben *a részletes biztonsági követelmények a felhasználói igények és az alkalmazott technológia függvényében állíthatók össze* (milyen adat, milyen formában történő eléréséről van szó, az igény milyen technikai feltételekkel biztosítható).

Általános követelmény, hogy távoli bejelentkezés körültekintően kiválasztott helyről, fenyegetéssel arányosan kialakított hitelesítési eljárás után történhet (10. sz. ábra). A

[41] Ezek a feladatok az MH szervezetei mellett internet szolgáltatóknál is jelentkeznek, amikor a szolgáltatás rendelkezésre állásával, vagy a közzétett adatok sértetlenségével kapcsolatos követelményeket szolgáltatási szerződésben (service level of agreement; SLA) kell meghatározni.

felhasználó és az adott távoli eszköz azonosításán és hitelesítésén kívül gondoskodni kell a távoli hozzáférést biztosító szolgáltatással (Remote Access Service; RAS) kapcsolatos adatok és folyamatok védelméről (pl. szerver hozzáférési szolgáltatáson keresztüli blokkolás, vagy a cserélt adatok illetéktelen megismerése/módosítása ellen). A kliens oldali védelem alapja a számítógép fizikai védelme (a megbízható tárolás külföldi tartózkodáskor gyakran nehézségekbe ütközik), a megkerülhetetlen jelszavas védelem, az operációs rendszer szabályos telepítése, csak a szükséges alkalmazások megléte és a szükséges biztonsági beállítások alkalmazása, a csatlakozást biztosító elem és tűzfal pontos konfigurálása, csak felhasználói hozzáférési jogosultság engedélyezése és kétfaktoros azonosítás, a mágneses merevlemez rejtjelzése, a vírusok és rosszindulatú programok elleni védelem. [104.] A szerver védelmének alapja az előbbi rendszabályok mellett a fizikai védelem, és a rendelkezésre állás biztosítása (pl. a meghibásodás, áramkimaradás elleni védelem).



10. ábra: Az elektronikus adatkezelő rendszer külső kapcsolatainak központi védelme

Hálózatok összekapcsolásakor általános feladat az érintett felek hatáskörének meghatározása (beleértve a meghibásodások, biztonsági események kezelését), és együttműködési megállapodásban történő rögzítése. Összekapcsolás esetén a kompromittálódás biztonsági kockázatot jelent a csatlakozó hálózat működésére és adatainak bizalmasságára, sértetlenségére, így már kezdeti lépésként szükség van az érintett szolgáltatásokkal kapcsolatos kockázatok felmérésére, és időszakos áttekintésére.

Az összekapcsolás az érintett hálózatok üzemeltetőire és biztonsági állományára új feladatokat határoz meg, így ki kell alakítani a képzéshez és továbbképzéshez szükséges szervezeti, technikai és adminisztratív kereteket. Módosítani kell a meglévő üzemeltetési és biztonsági dokumentumokat (az összekapcsolás előtt az érintett szervezetek önálló folytonossági és helyreállítási tervekkel rendelkeztek), illetve ki kell alakítani, és jóvá kell hagyatni az összekapcsolást megvalósító alrendszer dokumentációját. Az összekapcsolás engedélyezésének feltétele a kialakított csatlakozás műszaki és biztonsági paramétereinek, valamint az üzemeltetési és biztonsági rendszabályok ellenőrzése, szükség szerinti tesztelése.

KORLÁTOZOTT TERJESZTÉSŰ, vagy speciális kezelést igénylő külső adatcsere érdekében rejtjelző képességekre van szükség. A szervezeteknél a rejtjelző eszközök üzemeltetéséhez, teszteléséhez és karbantartásához szükséges anyagok, dokumentációk, kulcsok tárolása, nyilvántartása érdekében meg kell, hogy jelenjenek a *rejtjelző nyilvántartó hálózat szervezeti elemei* (ahol bonyolultabb biztonsági rendszabályok (pl. kétszemélyes szabály, vagy a titokmegosztás különböző formái) alkalmazására is sor kerülhet), és az eszközök felügyeletével kapcsolatos feladatok.

Hazánk egyre többször küld külföldre kisebb-nagyobb kötelékeket, ami szövetséges, vagy más nemzet által üzemeltetett hálózatokon keresztül történő kommunikációt igényel (beleértve minősített információk továbbítását is). Ebben az esetben a rejtjelzett kapcsolatokat az illetékes nemzeti hatóság *egyedi esetre vonatkozó követelményei* szerint kell kialakítani, az azonosítási és hitelesítési eljárásoknál emelt szintű követelményeket kell érvényesíteni.

Minősített adatok kezelésére csak az illetékes hatóság által jóváhagyott, szabályosan telepített eszközök, és meghatározott *biztonsági beállításokkal* rendelkező programok alkalmazhatók. [42]

BIZALMAS, vagy magasabb minősítési szint esetében könnyű *épületgépészeti* (pl. a falvastagság nem kielégítő), vagy egyéb problémába (pl. a folyosórészt nem lehet lezárni) ütközni, így gyakran nem járható út, hogy a rendszerek kialakítása alacsony biztonsági

[42] A különböző nemzeti biztonsági szervezetek, független tanácsadók az ajánlott termékek listáját (recommended product list) általában nyilvánosságra hozzák, és időszakonként frissítik. Az MH esetében célszerű a NATO ajánlott terméklistáját elsődlegesként kezelni és a NATO Technikai Architektúra irányelveivel összhangban lévő eszközöket és programokat alkalmazni.

követelmények szerint kezdődik, és *később történik meg a védelmi rendszabályok szintjének emelése*.[43]

A védelem kialakításakor a környezeti védelmi elemek nem hagyhatók figyelmen kívül, különben olyan azonos szintű védelmi megoldások övezik a létesítményt, amelyek közül már a külső védelmi réteg is elégséges lehet.

Ezen a minősítési szinten megjelenik a kompromittáló kisugárzás elleni védelem követelményrendszere, ami már az adatkezelő helyiségek (tábori körülmények között mobil konténerek) kialakításakor speciális feladatokat jelent (pl. kábel nyomvonalak biztonsági távolságai, a kábelek védelme, szűrési és árnyékolási feladatok).[44]

Hazánk kormányzati TEMPEST hitelesítési képességgel nem rendelkezik, így az akkreditáló hatóság más nemzeti hatóságok, vagy NATO szervek tanúsítványait fogadja el. A volt HM Technológiai Hivatal kiemelt feladatként kezelte a kompromittáló kisugárzás elleni védelemmel kapcsolatos mérési képesség kialakítását, [105.] ami *lehetővé teszi az objektumok szakszerű zónázását, az eszközök, hordozó eszközök, valamint egyedi védelmi megoldások mérését*.[45]

Biztonsági területen belül szabályozni kell a szolgálati hordozható elektronikus információkezelő eszközök használatát. A különböző sávokban, üzemmódokban és teljesítményekkel sugárzó eszközök (vagy azok vezérlése) *semmilyen elképzelhető üzemeltetési variációban sem zavarhatják egymást, nem boríthatják fel az elektromágneses környezetben kialakított rendet*.

Egyszerűnek látszó esetekben is (pl. hálózathoz történő csatlakozás a központi nyomtató használatához) a helyi sajátosságoknak megfelelő eljárásrendet, automatikus azonosítási eljárásokat kell kialakítani, különös figyelemmel a napjainkban már alapfelszereléshez tartozó vezeték nélküli felcsatlakozási képességekkel rendelkező eszközökre.

A szolgálati eszköz magáncélú használata, illetve a honvédelmi érdeket szolgáló adat nem megfelelő környezetben történő kezelése miatt a mobil eszközök sebezhetősége magas. A problémák megelőzése csak akkor lehetséges, ha a felhasználók pontosan *ismerik és betartják* az összes védelmi rendszabályt (pl. hordozható memóriák, kisméretű CD-k alkalmazása és elkülönített tárolása, a szállítási szabályok betartása, magasabb minősítésű

---

[43] Régebben gyakori volt a „magasabb minősítésű adatkezelési igények esetén a biztonsági rendszer megerősítése a jelenlegi infrastruktúra bázisán valósítható meg" jellegű megjegyzés a rendszerelgondolásokban, tervekben.

[44] A kompromittáló kisugárzás elleni védelem feladatainak fontosságát erősíti a 2007. 02. 10-én országos napilapban történő híradás, mely szerint az EUROPOL túlságosan nagy kockázatra hivatkozva nem engedélyezte a Nemzeti Nyomozó Iroda Aradi utcai székhelyén a terrorizmus elleni fellépést támogató szoftver alkalmazását.

[45] A mérési képesség a jogutód HM Fejlesztési és Logisztikai Ügynökség Technikai Igazgatóságánál jelenleg is rendelkezésre áll.

anyag küldeményként történő előreküldése), valamint a hordozható eszköz biztonsági funkciói *maradéktalanul kielégítik az adott minősítési szint védelmi követelményeit* (pl. azonosítás és hitelesítés, kompromittáló kisugárzás elleni védelem, rejtjelzés, illetéktelen felbontás elleni védelem).

Biztonsági terület esetében magántulajdonú adatrögzítésre, vagy elektronikus kommunikációra alkalmas eszköz bevitelét *meg kell tiltani*, és e szabály betartását technikai és adminisztratív rendszabályokkal kell érvényesíteni.

BIZALMAS minősítési szintig nemzeti minősített adat is továbbítható NATO, EU rejtjelző eszköz által védve, de *figyelembe kell venni, hogy egy tagállamok által közösen üzemeltetett rendszer használatakor lehetnek olyan esetek, amikor nemzeti érdeket sérthet egy más nemzetiségű személy esetleges illetéktelen megismerése*.

A biztonsági területen elhelyezett eszközök (pl. telefon, fax, számítógép, rejtjelző eszközök) a felhasználók kezelésében vannak, akik *egyénileg felelősek a védelmi rendszabályok betartásáért*. A minősített adatkezelés rendszabályain túl meghatározott mértékig ismerniük kell a rejtjelzéssel kapcsolatos eszközfüggő feladatokat (pl. kulcsbetöltés, váltás, törlés, kulcsellátás), a hibajelenségeket, és a kompromittálódás vagy vészhelyzet esetén szükséges teendőket.

I. osztályú biztonsági területen figyelmet igényel a közösen használt kommunikációs eszközök üzemeltetési rendjének kialakítása, mert az elszámoltathatóság elve minősített adatok kezelése esetén megköveteli az egyedi azonosítást, visszakereshetőséget.

Az eszközök számának csökkentése érdekében hasznos lehet a periféria átkapcsolók (peripheral switch) alkalmazása (pl. billentyű, monitor és egér, vagy nyomtató átkapcsolók), de az átkapcsoló eszköznek ki kell elégíteni *a magasabb biztonságú hálózatra vonatkozó követelményeket*, megfelelő jelölésekkel kell támogatni a felhasználókat, és *ki kell zárni a hálózatok összekapcsolódásának, az adatok keveredésének lehetőségét*.

A központi hálózati elemek, háttérben dolgozó speciális adattárak kiemelt célok lehetnek, így *objektumonként összevonva célszerű kialakítani a biztonságos üzemeltetési környezetet*.[46] Az áramellátás (tartalék áramellátás), a szünetmentes táplálás, a földelési (és biztonsági földelési) rendszer karbantartása, a kommunikációs infrastruktúra (rendezők, kábelcsatornák és alépítmények) menedzselése, a klimatizált környezet biztosítása központosítva könnyebben, és gazdaságosabban megoldható. Ebben az esetben megerősített

[46] 2007. 02. 13-án hajnalban a rendőrség Teve utcai székháza ellen történt gépkarabélyos tüzelés rámutat arra, hogy célszerű újragondolni a középületek fenyegetettségéről alkotott véleményeket, és az agresszív fenyegetésekhez kell igazítani a kritikus infrastruktúrák kialakítását és védelmét.

azonosítási és hitelesítési eljárásokra van szükség (pl. token alapú, egyszer használatos bejelentkezés, vagy kártya alapú, és további jelszavas azonosítással megerősített rendszer). A szolgáltatások elérését el kell különíteni a rendszer szintű hozzáférésektől, és olyan elosztáson alapuló adattárolási módszereket kell alkalmazni, amelyek a várható támadások (vagy meghibásodásokon alapuló kiesések) esetén képesek a rendszer újbóli felélesztésére.

A hálózatba integrált szenzorok adatainak felhasználása érdekében *vezérlési feladatokat* támogató *reagálási képességeket* (pl. elem átkonfigurálása, hálózatból történő kizárás, útvonalak megváltoztatása), *helyreállítási és tartalék kapacitásokat kell kialakítani*. Létfontosságú funkciókat befolyásoló hozzáférések esetén a *feladatmegosztás*, a *műveletek naplózása*, a *kritikus műveletek megkezdése előtti megerősítés kérés*, illetve *automatikus jelentés küldés* jelentik a védelmi rendszabályokat.

Egy hálózat szétzilálásának legbiztosabb módszere a felügyelet kiiktatása, így annak *folyamatos rendelkezésre állása* kritikus tényező. Az aktivizált tartalék felügyeletnek *teljes körű feljogosításokkal kell rendelkeznie a hálózat egészére vonatkozóan*, ami megköveteli a felügyelettel kapcsolatos adatbázisok többszörözését, illetve az összes felügyelettel kapcsolatos információk rendelkezésre állását és *annak megakadályozását, hogy a felügyelet hálózatról történő leválasztásával más elem illegálisan magához vegye a hálózat irányítását*.

A szenzorok által szolgáltatott adatok kizárólag központilag történő elemzése MH méretekben elképzelhetetlen, így *decentralizált elemzési rendet* kell kialakítani a hálózati elemek (pl. csomópontok, átviteli eszközök, csoportos rejtjelző eszközök) és egyéb eszközök védelme érdekében, melynek megvalósítása az un. CIRC (Computer Incident Response Capability) képességek kialakításának formájában történik (*detektálási*, *elemző, reagáló* és a szükséges *helyreállítási műveleteket* kialakítása és folyamatos üzemeltetése).

Az incidenskezelés EU kézikönyve szerint a hálózatok biztonsági céljait támogató fő feladatok: a *detektálás* (detection), az *adatgyűjtés* (collection), a *vizsgálat* (investigation) és a *bizonyítékszolgáltatás* (presentation), [106.] amit a vonatkozó műszaki jelentés alapján a *válaszadással* kell kiegészíteni.

A képesség kialakításakor tisztázni kell az előállított és összegyűjtött adatokért való felelősséget, a hozzáférési módokat és jogosultságokat, a különböző forrású adatok összefüggéseiből adódó bizonyítási lehetőségeket, a tárolási/archiválási és nyilvántartási igényeket, a bizonyítékként történő felhasználás követelményeit. Meg kell vizsgálni, hogy *hol és hogyan történik a személyes adatok kezelése,* és teljes életciklusra értelmezve hogyan

valósítható meg az adatok illetéktelen hozzáférés elleni védelme.[47] Ezután következhet a biztonsági felügyeleti rend technikai, szervezeti és adminisztratív rendszabályainak kialakítása.

A hálózatfelügyelet a menedzsment információk környezettel való cseréjéért, az arra jogosultak számára történő rendelkezésre bocsátásáért, elemzéséért is felelős, [107.] így a felügyeleti rend kialakításakor a szükséges szervezeti kapcsolatokkal is ki kell alakítani. Ez a NATO CIRC (NCIRC) technikai központtal, a NATO *rendszerek hálózatfelügyeleteivel, az* EU hálózatbiztonsági szervezetével történő együttműködés formájában valósulhat meg, az együttműködő szervezetektől, rendszerfelügyeletektől kapott incidens információk, a sebezhetőségre és fenyegetésekre vonatkozó adatok feldolgozása, megosztása formájában.

A háttértámogatás kormányzati szinten a Nemzeti Hírközlési Hatóság által üzemeltetett Főközpont feladata, ami a kommunikációs szolgáltatások állapotfigyelésével, a támogató információk gyors cseréjével és különböző munkacsoportok értesítésével teszi lehetővé a biztonsági eseményekre történő gyors reagálást és az adatbiztonsági fenyegetések gyors kezelését. [108.] Hasonló célú, informatikai területen történő megelőzést és helyreállítást célzó szakmai támogatást lát el a nemzeti CERT (Computer Emergency Response Team; számítógép/hálózati vészhelyzet elhárítást támogató csoport) szervezet is.

A kiszolgáló infrastruktúrák kialakításánál napjainkban szükségszerűen változik a *hálózati elemek elkülönítésének rendje*. Az adott helyszíntől függően a rejtjelző és egyéb RED központi kiszolgálók, valamint a nem minősített adatokat kezelő hálózati elemek elkülönítése jelenik meg a korábban élesen jelentkező nemzeti - NATO elkülönülés helyett. Elektronikus adatok esetében az eszközök (vagy kivehető adattárolók) számának növekedése miatt nem járható út a fizikai elkülönítés, így *erőteljesen fejleszteni és alkalmazni kell a logikai elkülönítési megoldásokat*.

A minősített és a nyílt adatokat kezelő hálózatok menedzselését nem célszerű különválasztani, *a szükséges elkülönítéseket hálózatfelügyeleten belül kell kialakítani.*

A hazánk területén, vagy külföldön állomásozó MH szervezetek vezetéséhez és működéséhez szükséges megbízható információs képességek (pl. katonai üzenetkezelő szolgáltatás, hatósági ügyintézési képesség, közigazgatási rendszerekkel történő együttműködés, elektronikus iratkezelés), és az adatok, adatkezelő képességek védelme érdekében szükség van a *jogszabályok és NATO előírásoknak egyaránt megfelelő hitelesítés*

[47] Az MH szervezetei működéséhez szükséges kommunikációs szolgáltatások szolgálati célt szolgálnak, így amennyiben nem biztosítható a magánjellegű kommunikáció elkülönítése (ami a szolgáltatás igénybevételével kapcsolatos költségtérítés alapja is), a törvényességnek való megfelelés érdekében célszerű a felhasználók írásban történő értesítése arról, hogy elektronikus adatkezelési tevékenységük felügyelet alatt áll.

szolgáltatásra. A hitelesítés szolgáltatásnak *egyaránt támogatnia kell az MH szintű nem minősített és a minősített információs infrastruktúrát,* biztosítania kell a nemzeti és külföldi hitelesítő központokkal történő hitelesítési viszony kialakítását és fenntartását.

TITKOS minősítési szinttel kezdődően a mobil kommunikációs eszközök alkalmazásával kapcsolatos lehetőségek szűkülnek (illetve kifejezett tiltások jelennek meg), illetve az adatok törlésével, minősítésük megváltoztatásával kapcsolatos szabályok is lényegesen szigorúbbá válnak.

A TITKOS és SZIGORÚAN TITKOS minősítésű adatok kezelésének védelmét a már ismertetett szabályok erősítésével lehet elérni. Fizikai védelem területén a nyílászárókra, zárakra és tárolóeszközökre, rácsokra, falakra vonatkozó követelmények, a járőrözés gyakorisága változik. Személyi védelem területén a szükséges nemzetbiztonsági vizsgálat (valamint NATO, EU adatok esetében a személyi biztonsági tanúsítvány) szintje, dokumentumvédelem területén a nyilvántartási és az ellenőrzési feladatok változnak.

Elektronikus információvédelem területén az azonosítási és hitelesítési eljárások, a rendszerek összekapcsolásával kapcsolatos védelmi feladatok összetettebbé válnak, az eszközökre emelt szintű tanúsítási követelmények vonatkoznak, a kompromittáló kisugárzás elleni védelemnél szigorúbb paramétereket kell alkalmazni.

Az információs szolgáltatások tervezése során elsődleges a *biztonsági követelmények és a felhasználóbarát szolgáltatások közötti összhang* megtalálása. A NATO csatlakozás utáni időszakban a NATO minősített adatok kezelésére a NATO nyilvántartók mellett kialakított un. „feldolgozó helyiség" volt az első megoldás, ahol a nyilvántartóból átvett anyagok feldolgozása (tanulmányozása, jegyzetelése) történhetett, ami után a felhasználó maradéktalanul elszámolt a nyilvántartó felé. A számítógépes adatfeldolgozási igény miatt e helyiségekbe kerültek a NATO TITKOS WAN (Wide Area Network; nagy kiterjedésű hálózat) alapszolgáltatásait biztosító munkaállomások is. A gyakorlat bizonyította, hogy ahol nagy a felhasználók száma, vagy folyamatos az adatfeldolgozási igény, vagy a szervezeten belül a munkahelyek széttagoltan helyezkednek el, ez nem jó megoldás. *A szolgáltatásoknak a munkahelyekhez kell alkalmazkodni, így helyben kell telepíteni a biztonsági területeket* (tárolási és adatfeldolgozási lehetőségeket).

MH szinten a tudás jobb menedzselésének feltétele az *elszigetelt fejlesztések megszüntetése*, a *szolgáltatások egységesítése, a nem szabványos megoldások kiváltása*, *valamint az eddigi, külön alrendszerekben történő gondolkozás átalakítása* (pl. közigazgatási és katonai informatikára történő darabolás, a tábori kommunikációs rendszer szolgáltatásainak

kényszerű szervezési és technikai elkülönítése, MH és HM intranetek megkülönböztetése, vagy nemzeti, NATO, EU adatkezelő képességek felesleges fizikai elkülönítése).

A különböző, szervezetileg vagy technikailag elkülönült szolgáltatások, adatbázisok esetében *a hálózatos kiszolgálásra történő áttéréskor esetre menően meg kell megvizsgálni, hogy a független alrendszerekben eddig más módszerrel biztosított biztonsági célkitűzések hogyan valósíthatók meg, a védelmi rendszabályok hogyan korszerűsíthetők*.

A gyakorlati, vagy biztonsági okokból (szűk felhasználói kör speciális adatfeldolgozási szükséglete, vagy kezelési jelzés miatti szeparáció) elkülönített helyi adatfeldolgozó képességeknél alapelvként kell kezelni, hogy *azokat is egység szemlélet alapján – az MH hálózatosított szolgáltatásaival összhangban – kell kialakítani és fenntartani*.

A korszerű adatkezelő szolgáltatások kialakításához *nélkülözhetetlen a felhasználói igények pontos meghatározása*. Rengeteg energiát emészt az egyes feladatokra, rendszerekre kialakított, vagy egyéb eredetű egyedi szemléletű, esetleg külföldi gyártmányú (és más nemzeti szabványra támaszkodó) vezetés támogató megoldások MH szintű alkalmazásba vételének vizsgálata, melynek alapvető oka a központi követelményrendszer hiánya. *Az MH szintű, korszerű vezetéstámogató képességek védelmének kialakítása az egyedi jogszabályi környezet, a szervezeti struktúra és feladatrendszer, valamint a rendelkezésre álló technikai lehetőségek talaján álló követelmények összeállítása és jóváhagyása nélkül nem képzelhető el*.

Az MH szervezeti céljainak támogatása érdekében *perspektivikus követelménynek tartom, hogy az MH adataival és adatkezelő rendszereivel kapcsolatos biztonsági célok, és a kialakított védelmi rendszabályok folyamatosan összehangoltak legyenek a szervezeti célokkal és a külső, belső információs környezettel; a széttagolt rendszereket összefogó, egységes hálózatra való törekvés nem kerülhet szembe a kezelt adatok, adatkezelő képességek biztonsági követelményeivel*.

Az adatkezelésre vonatkozó biztonsági követelményeket az erőforrások biztosítása, illetve a feladatok megjelenítése érdekében be kell dolgozni az MH Védelmi Tervezési Rendszerébe. A tervezés, kialakítás megindításához szükséges projektek szervezése mellett nélkülözhetetlen az üzemeltetéshez szükséges szervezeti és személyi feltételek kialakítása is. Egy-egy adatkezelő képesség kialakítása és folyamatos korszerűsítése (információvédelmi területen pl. az MH szintű eseménykezelő rendszer, a hitelesítés szolgáltatás, a NATO TITKOS adatkezelő rendszer magyarországi alhálózat fenntartása, vagy az elektronikus kulcsmenedzselés) több szakterület többszörös egyeztetésén alapuló folyamat, amit *logikailag összetartozó egységenként, felső szintű szabályozókban rögzített hatáskörökkel és feladatokkal lehet, és kell kézben tartani.*

Az évek óta folyamatban lévő MH szintű korszerűsítési folyamat tapasztalatai alapján *kiemelem a védelmi rendszabályok legkorábbi tervezési szakaszban történő megjelenítésének, és az ehhez szükséges szervezeti kapcsolatok működőképességének szükségességét*. Ennek hiányában az infrastruktúrára, kiszolgálásra, állományra vonatkozó első döntések, a hozzájuk tartozó költségkeretek biztonsági szempontok miatt gyakran felborulnak, aminek gyakran félreértelmezett oka egyszerű: *a védelmi feladatok késve történő beillesztése*.

Ugyanígy hangsúlyozom *az életciklus szemlélet szerinti gondolkodásmód fontosságát, mert az MH nem minősített és minősített adatokat kezelő vezetési és irányítási rendszere nem csak egy adott eszköz, vagy szolgáltatás üzembe helyezéséig fontos*. A hardver, szoftver-frissítések, a szolgáltatások igény szerinti átalakítása/fejlesztése, a karbantartásokhoz és javításokhoz szükséges szolgáltatási háttér biztosítása összetett, szervezeti határokon átnyúló, gördülő tervezést igénylő, folyamatos feladat.

Az MH szintű, komplex fejlesztések esetében nem lehet egy-egy részfolyamatot, vagy rendszerelem/szolgáltatás fontosságát, szerepét rendszer szintű torzulások, hibás vezetői döntések magas kockázata nélkül kiragadni, esetleges szervezeti, vagy egyéni érdekek alapján menedzselni, így a kialakításra vonatkozó rész utolsó és egyben legfontosabb feladataként a *helyes vezetői kommunikációt és szerepvállalást*, a *jól működő egyeztetési és döntési mechanizmust* azonosítom.

A szükséges védelmi megoldások kialakítását bonyolultabb esetben modellezéssel, tesztekkel és szimulációkkal kell segíteni.

2005-ben az akkori MH Híradó és Informatikai Parancsnokság kijelölt állománya a CWID rendezvényre[48] az MH-nál (hatósági engedéllyel) először egy hagyományos operációs rendszerű teszt hálózat köré nyílt forráskódú rendszerre épülő védelmi gyűrűt alakított ki, megerősítve a behatolás érzékelést, monitorozást, és reagálást. A hasonló rendezvények, tesztek, szimulációk nélkül elképzelhetetlen pl. az MH szintű CIRC képesség kialakítása, ezért új lehetőségekkel szolgálhat a NATO szervezetek vagy tagállamok, esetleg más partnerek által kialakított teszthálózathoz, tesztekhez történő csatlakozás, információcsere, közös projektek kialakítása.

[48] Coalition Warrior Interoperability Demonstration (Lillehammer, Norvégia). A rendezvény feladata nemzeti információs rendszerek együttműködését támogató teszthálózat kialakítása, és eljárások, megoldások vizsgálata tesztkörnyezetben.

A fejlesztések, tesztek számára támpont lehet a NATO technikai fejlődést összefoglaló prognózisában [109.] szereplő fontosabb irányok:

- hardver/szoftver konfiguráció felügyeleti feladatok az operációs rendszerek hardver és szoftver megoldásokkal történő támogatásával;
- a vezeték nélküli szolgáltatások vezetékes hálózatokkal egyenértékű védelmi mechanizmusai;
- optikai hálózatok behatolás detektálásának fejlesztése;
- a hozzáférési jogosultságok menedzselése, nyomon követhetősége (Identity Management), egyszerűsített bejelentkezés, illetve személyi azonosítási igény esetén a korlátozott mennyiségű adatokkal történő műveletek;
- szoftver definiált rádiók védelme, és a rádiófrekvenciás azonosítási megoldások;
- a neuronhálózatok alkalmazási lehetőségeinek fejlesztése.

Az EU-ban is hasonlók a fejlesztendő területek. Az információvédelem korszerű megoldásait kereső szervezetek által támogatott szakmai konferencia 2007. évi kiemelt témai a biztonsági menedzsment, a kockázat menedzsment, a jogosultság menedzsment, a személyiségi jogok és adatvédelem, a CERT szervezetek együttműködése és támogatása, a személyi tulajdonságok kihasználása (social engineering), az elektronikus levelezés vagy web szolgáltatás védelme, a hacker és egyéb fenyegetések elleni védelem, a mobil és vezeték nélküli eszközök biztonsága, az azonosítással kapcsolatos menedzsment, a biztonsági tudatosság, a PKI megoldások, a biometria, és a korszerű kártyás azonosítás. [110.]

A NATO információs hálózatainak támogatása érdekében Észt Köztársaság 2006-ban megkezdte az Informatikai Hálózatbiztonsági Fejlesztési és Együttműködési Központ (Cooperative Cyber Defence Centre of Excellence; CCD COE) kialakítását. A központ munkájában résztvevő kutatók a következő területeken javasolják vizsgálatok megkezdését:

- *Mesterséges intelligencia alapú technológiák alkalmazási lehetőségeinek vizsgálata és kifejlesztése az informatikai védelem területein*. Intelligens eljárások (agent) alkalmazási lehetőségeinek vizsgálata a hálózati és számítógép (host) alapú védelmi rendszerben, valamint a válasz reakciók területén; mesterséges intelligencián alapuló megoldások kialakítása a behatolás detektálás (IDS) területén, illetve a szabály alapú védelmi rendszerekben ellenőrzött és öntanuló eljárások alkalmazási lehetőségeinek vizsgálata. [111.]
- *Intelligens szimulációs lehetőségek kialakításának vizsgálata IDS/IPS területen*. Az IT infrastruktúra védelméhez szükséges nagymennyiségű és széles körű adatok elemzéséhez többcélú, rugalmasan skálázható nyílt forráskódú rendszereken alapuló

szimulációs eljárások, platformok kialakítási lehetőségeinek vizsgálata a modell alapú szoftverfejlesztések, a szoftver eljárások automatikus illesztésének támogatása érdekében. [112.]

- *Hálózatok támadási módszereinek szimulációval történő vizsgálata.* Hálózati alapú szimulációval teljes hálózatok, különböző protokollok modellezésével a támadás során keletkező adatok védelmi célú feldolgozási lehetőségeinek vizsgálata. A hálózaton belüli eszközökön (végberendezések, központi kiszolgálók, aktív elemek) zajló folyamatok során keletkezett adatok elemzési lehetőségeinek vizsgálata, megoldások kifejlesztése virtuális számítógép alapú szimulációval. [113.]
- *Esemény összehasonlítási módszerek, adatbányászati eljárások alkalmazása a naplófájlok elemzéséhez.* A hálózat üzemeltetés során keletkező nagymennyiségű, különböző formátumokban érkező adatok analizálásának támogatása nyílt forráskódon alapuló, egyszerűsített eredménykiértékelés módszerének felhasználásával, kiemelten a kritikus események kiszűréséhez szükséges módszerek kidolgozására. [114.]
- *A hálózati védelem jogi szempontjainak vizsgálata.* Az államok szabályozásának, valamint a különböző nemzetközi egyezmények elemzése a szervezeti, nemzeti és nemzetközi együttműködés megalapozásáért a nemzeti kritikus infrastruktúrák védelme érdekében. [115.]

Az említett kutatási témák, fejlesztési irányok egyértelmű jelzések az MH információvédelmi képességeinek fejlesztési és tervezési irányaihoz.

Az együttműködés új formája minősített adatok kezelése területén a Visegrádi Együttműködés államainak katonai információbiztonságért felelős szervezetei között 2007. júniusban Pozsonyban aláírt közös nyilatkozat, ami *egyeztetést és tapasztalatcserét alapoz meg az információvédelmi képzés, új technológiák fejlesztése és alkalmazása, valamint a katonai futárok együttműködése területeken*.

2. 4. Információbiztonsági alapelvek

Az elektronikus információbiztonsági célkitűzések megvalósítása érdekében kialakítandó *rendszer-specifikus, a minősítési szintekhez igazodó védelmi rendszabályok kialakításának támogatásához nincsenek általános érvényű nemzeti biztonsági alapelvek,* illetve hazánkban nincs jogszabályban vagy egyéb módon rögzített, alapelvek kialakítására vonatkozó követelmény.

Az elektronikus adatkezelő rendszerek kialakításának, üzemeltetésének e fejezetben is bemutatott buktatóinak elkerülése, az egységes szemlélet támogatása érdekében a következő, *rendszer független alapelvek kötelező jellegű érvényesítését tartom szükségesnek:*

1) az adatkezelő rendszer kialakítása, üzemeltetési folyamatai és eljárásai megfelelnek a jogszabályok követelményeinek;
2) az elektronikus adatkezelő képességek biztonsági követelményei a rendszer kialakításának legkorábbi szakaszában jelenjenek meg, és a védelmi feladatok épüljenek be a kialakítással és üzemeltetéssel kapcsolatos feladatok közé;
3) az elektronikus adatkezelő képességek kialakításához, átalakításához, és fenntartásához szükséges védelmi rendszabályok időszakosan ismétlődő kockázatelemzési eljárásra támaszkodjanak;
4) a rendszer kritikusnak tekinthető elemei (kiemelten az operációs rendszerek és a biztonsági funkciót megvalósító eszközök, programok) a rendszer biztonsági besorolásának megfelelő tanúsítással rendelkező termékek lehetnek;
5) az elektronikus adatkezelő rendszer szabványos eszközöket, és alkalmazásokat tartalmazzon, kialakítása és üzemeltetési eljárásai szabványos eljárásokon alapuljanak;
6) elektronikus adatkezelő rendszer csak a feladatok ellátásához szükséges szolgáltatásokat biztosítsa;
7) hozzáférés olyan adatokhoz, szolgáltatásokhoz, és ezekkel kapcsolatos infrastruktúrához engedélyezhető, amihez az adott személynek munkája végzéséhez szüksége van, és az ahhoz szükséges jogosultsággal rendelkezik;
8) a rendszer-szintű hozzáférésekkel rendelkező személyek számát a lehető legalacsonyabb szinten kell tartani;
9) A szükséges mértékű rendelkezésre állást a rendszer-specifikus sajátosságoknak megfelelő folytonossági és helyreállítási folyamatok támogassák;
10) A rendszer külső kapcsolatai olyan mechanizmusokkal védettek legyen, amelyek megakadályozzák/jelzik az illetéktelen behatolást (vagy annak kísérletét) és támogatják a hatékony válasz-reakciókat;
11) a rendszer használatba vétele a kezelt adatok fontosságával arányos, előre definiált auditálási és engedélyezési eljárás után történhet;
12) az üzemeltetés (alkalmazás) során szükséges változtatások a biztonsági hatások vizsgálata után, engedélyhez kötötten történhetnek;

13) a fejlesztést, tesztelést és képzést szolgáló infrastruktúrák, adatok, valamint a nyilvánosan elérhető információs szolgáltatások az MH működése és vezetése szempontjából kritikus támogató rendszerektől a szükséges mértékben legyenek elkülönítve;
14) az adatkezelő rendszerekkel kapcsolatba kerülő külső partnerekre (pl. felhasználó, üzemeltető, fejlesztő) vonatkozó biztonsági követelményeket együttműködési megállapodások (szerződések) tartalmazzák, és a szükséges védelmi rendszabályok megismerése biztosított legyen;
15) az adatkezelő képességek üzemeltetői és felhasználói a szükséges rendszer-specifikus ismeretekkel rendelkezzenek, a kialakított képzési és továbbképzési rendszer a védelmi ismeretek frissítését biztosítsa;
16) az adatokhoz történő-, valamint a rendszer szintű hozzáférések elszámoltathatóságát egyedi azonosításon alapuló, szükséges mértékben hiteles folyamatok biztosítsák;
17) a rendszer üzemelése során az incidensek jelentése, kivizsgálása és a tapasztalatok hasznosítása történjen meg;
18) A rendszer biztonságára vonatkozó követelmények teljesülése ismétlődő rendszerű ellenőrzés alatt álljanak;
19) az elektronikus adatkezelő rendszer biztonságát szabályozó dokumentumok időszakosan felülvizsgáltak és szükség szerint pontosítottak legyenek.

2. 5. Összefoglalás és következtetések

Az információbiztonság területeinek áttekintése megvilágítja, hogy a fizikai, személyi, dokumentum, vagy elektronikus információvédelmi szakterület bármelyikének hiányában (vagy hiányossága miatt) megemelkedhet az *illetéktelen* megismerés, vagy az információs műveletekbe történő illetéktelen beavatkozás esélye. A négy védelmi szakterületeket *az információbiztonság alapelemeinek kell tekinteni,* minősítési jelzés és kezelési utasítás szerinti alkalmazásuk megkerülhetetlen. A négy szakterület között *fontossági sorrendet, alá-fölérendeltségi viszonyt nem lehet meghatározni.* Az elektronikus információvédelmen belül *az informatikai védelem rendszabályainak alkalmazása minimum követelmény, a többi szakterület védelmi rendszabályai specifikusan alkalmazandók.*

A megváltozott jogszabályi környezet miatt *az ITB 12. ajánlás szerinti biztonsági besorolást a közigazgatásban nem célszerű alkalmazni, hanem a minősítési szintekhez igazodó ötfokozatú biztonsági osztályozást kell kialakítani* (NEM MINŐSÍTETT,

KORLÁTOZOTT TERJESZTÉSŰ, BIZALMAS, TITKOS és SZIGORÚAN TITKOS). A biztonsági osztályokon belül további bontás célszerű, azonban ennek során nem csak a rendelkezésre állást, hanem *az összes biztonsági célt figyelembe kell venni.* Az értékelési szempontokat nem egymástól függetlenül, hanem *komplexen kell alkalmazni, amelynek célszerű formája a „legalacsonyabb értékelési mutató érvényesítése” elv.*

A nem minősített biztonsági osztályba sorolt adatok esetében is minimum védelmi rendszabályokat kell meghatározni, és meg kell szüntetni a „védelmet nem igényel” típusú megközelítést. Az ebbe a biztonsági osztályba tartozó, de magasabb védelmet igénylő adatok biztonságát specializált védelmi rendszabályokkal kell biztosítani.

A NATO, EU és a nemzeti adatkezelés összhangjával kapcsolatban megállapítom, hogy *a felső szinten elméletileg összehangolt minősítési szintekhez nincsenek egyenértékű biztonsági követelmények rendelve, így nem garantált az adatok és adatkezelő képességek azonos védelmi szintje.* Az adatkezelő rendszerek üzemeltetési környezetének fizikai védelmi elemei eltérők lehetnek, a különböző hozzáférési jogosultságok engedélyezését nem támogatja egységes, a személyi kockázatok kiszűrését célzó hatósági eljárásrend, eltérő a szervezeti célú nem minősített adatok megismerésével kapcsolatos megközelítés. Elektronikus információvédelem területén nincs olyan jogszabályban rögzített szabályozó (keret)rendszer, amely komplexen kezeli a nyílt és minősített adatok védelmével kapcsolatos korszerű biztonsági követelményeket, minimum védelmi rendszabályokat, amely hiányosságok közül *kiemelem a nem minősített adatok rejtjelzéssel történő védelmére vonatkozó kormányzati irányelvek hiányát.*

A hálózat-alapú hadviselés elmélete szerinti civil-katonai, és nemzeti-szövetségi együttműködés a védelmi rendszabályok pontos összehangolását igényli, így mielőbb szükség van a szabályok harmonizálására. Az egységes nemzeti kritikus infrastruktúra védelme a gazdasági szféra, a hatósági szervek összehangolt felügyeleti és koordináló tevékenységét igényli. Információvédelmi szempontból kiemelt fontosságú a fejlesztési irányok meghatározása, a kutatások finanszírozása, a fejlesztés és gyártás felügyelete, a nemzeti számítástechnikai termékek tanúsítása, a rejtjelző eszközök gyártása és tanúsítása, TEMPEST tanúsítási rendszer kialakítása, egységes képzési, auditálási és ellenőrzési modell kialakítása és fenntartása, egységes közigazgatásra vonatkozó kockázatkezelési eljárásrend kialakítása). *A NATO, EU és a nemzeti nem minősített adatok bizalmasságára vonatkozó követelmények közötti különbséget meg kell szüntetni.*

A minősített adatok védelmére szolgáló „titokvédelem” kifejezést nem célszerű „információbiztonság (vagy védelem)” értelemben alkalmazni, inkább törlése indokolt.

Az információvédelmi eljárások hadműveleti körülmények között, vagy terrortámadás esetén önmagukban nem alkalmasak az adatok és adatkezelő rendszerek teljes körű védelmére (pl. nem tartalmaznak elemeket elektronikus felderítés ellen, nem képesek támadás vagy rakétacsapás kivédésére), a kompromittálás következményeinek felszámolására, így *hatékony információvédelem csak a katonai szervezetek tevékenységi rendjébe illesztve, az egyéb szakterületekkel összehangolva képzelhető el*.

A biztonsági követelmények és a védelmi rendszabályok menedzselése szoros kapcsolatban áll a kockázatelemzéssel, mert a minimál jellegű követelményeket rendszer-specifikusan kiegészíti, finomítja. Az adatkezelő képességek kialakításához és fenntartásához nemzeti szinten ki kell alakítani a kockázatelemzéshez szükséges részletezett, az alkalmazók számára egységesen értelmezett feladatrendszert. *Nem engedhető meg, hogy a nemzeti kritikus infrastruktúrához tartozó rendszerek esetében egy üzemeltető, vagy alkalmazó szervezet más vizsgálati módszer, vagy eltérő mértékek alapján eltérő kockázatokat mutasson ki, és eltérő szintű védelmi rendszabályokat alkalmazzon.* A nemzeti kritikus infrastruktúra egységes védelmi rendszabályainak kialakítása és fenntartása érdekében össze kell hangolni a kockázatok elemzésére és menedzselésére irányuló folyamatokat. Az MH-nál ezen túlmenően ki kell dolgozni a katonai alkalmazással kapcsolatos specialitásokat, és az információs rendszerek kockázatelemzését integrálni kell a szervezeti feladatok közé (beleértve a meglévő szabályozás átalakítását).

Az MH ÖHD információs műveletek részében az információvédelem megjelenítését a fejezetben ismertetett szakfeladatok alapján a következőként képzelem el:

A saját erőkre, képességekre, környezetre, ellenséges erőkre vonatkozó adatok biztonsági alapelvek szerinti, kockázatokkal arányos védelme, valamint a rendszabályok folyamatos pontosítása, hatékonyságuk ellenőrzése, a biztonsági eseményekre való gyors és hatékony reagálás, a pontosan meghatározott felelősségi rend, és a hierarchizált szabályozás képezi az információbiztonság alapját.

A kezelt saját, vagy szövetséges erőktől, együttműködő szervezetektől átvett adatok minősítése, kezelési jelölései alapján a jogszabályokban rögzített követelményeknek megfelelő biztonsági szintet a környezet és az aktuális fenyegetettséghez igazodó

kiegyensúlyozott személyi, fizikai, dokumentum és elektronikus információvédelmi összetevőkből álló védelmi rendszer valósítja meg.

A kezelt adatok tömegtájékoztatás, vagy egyéb okból történő nyilvánosságra hozatala előtt felülvizsgálati és engedélyezési eljárás biztosítja, hogy a műveletek sikeréhez szükséges adat ne kerülhessen illetéktelen kezekbe.

A nemzeti, NATO és egyéb szövetséges elektronikus adatkezelő képességeket kiegyensúlyozott kompromittáló kisugárzás elleni védelmi, rejtjelző és számítógépes hálózatbiztonsági eljárásokkal, eszközökkel és alkalmazásokkal kell védeni.

Az első fejezetben foglaltak szerint valószínűsítem, hogy szükségessé válik a doktrínában a számítógép hálózati hadviseléssel kapcsolatos átfogó megfogalmazás megjelenítése, melynek védelmi részét (Computer Network Defense; CND) az információvédelmi részben (indokolt esetben önállóan megjelenítve) a következők szerint képzelem el:

- A katonai szervezetek vezetéséhez és működésének támogatásához szükséges MH szintű nemzeti, NATO, vagy EU nem minősített és minősített elektronikus adatkezelő képességeket az információs fenyegetéseknek és alkalmazott technológiának megfelelően kialakított észlelési, reagálási és helyreállítási képességekkel rendelkező központi eseménykezelő rendszer biztosítja. Az automatizált műveletekre támaszkodó védelmi mechanizmusok segítségével a hálózatokba történő behatolásra, vagy működési rendellenességre utaló jelek elemzése folyamatosan történik.
- A hálózatfelügyeletek információs kapcsolatai biztosítják az együttműködő szervezetek biztonsági menedzsmentjeivel történő összehangolt cselekvést az információs fenyegetettségek, a hálózatok sebezhetőségére és az aktuális helyzetre vonatkozó adatok gyors cseréjével.
- Az adatkezelő rendszerekbe történő illetéktelen behatolások, beavatkozások során szerzett adatok gyűjtése, elemzése megalapozza a jogszabályoknak megfelelő bizonyítékszolgáltatást, és a szükséges válaszlépések megtételét.
- Az állandó és tábori kommunikációs rendszerek üzemeltetése során az információs szükségletek fontosságával arányos helyreállítási műveletek, tartalék eszközök és alternatív megoldások támogatják a szükséges kommunikációs képességek folyamatos fenntartását.

Az adatok mennyiségének ugrásszerű növekedése, a széttagolt adatbázisok egységes kezelésének igénye előtérbe helyezi a *különböző szintű és tartalmú biztonsági mentések technikai és szervezési kérdéseit*, az adatbázisok szükséges szintű rendelkezésre állásának biztosítását, a helyreállításra vonatkozó rendszer-specifikus eljárások kialakítását, tesztelését és rendszerbe állítását. Az adatvagyon MH szintű védelme (adattár), illetve ugyanez a feladat a közigazgatásra vonatkoztatva olyan *egységes szemléletű szervezési és technikai eljárások kialakítását igényli, amelyek képesek az új információs fenyegetésekkel arányos helyreállítási képességeket támogatni*.

A bemutatott biztonsági alapelvek alkalmazása, időszakos felülvizsgálata, és továbbfejlesztése minősítési szinttől és rendszertől függetlenül támogatja a védelmi rendszabályok kialakítását. A korszerűség követelményének megfelelő védelmi rendszabályok érdekében *folyamatosan figyelemmel kell kísérni a szabványok, jogszabályok és ajánlások fejlődését, és a tapasztaltak szerint – a hadműveleti követelményekre alapozva – kell kialakítani a fejlesztési irányokat. Ez a tevékenység információvédelmi területen a jelenlegi kapacitások fejlesztését igényli.*

A miniszteri irányelvekben is meghatározott hálózat-alapú új képességek a jelenlegi helyzettel (erőforrásokkal, szervezeti struktúrával, feladatrendszerrel, technikai háttérrel) történő összehasonlítása megalapozza azt a – nem csak információvédelemre vonatkozó – következtetést, hogy a szükséges változtatások meghaladják a hagyományosnak tekinthető „híradó és informatikai rendszer" kereteit, és a szolgáltatásoknál, az azokat alkalmazó erőknél szélesebb körű változtatások jelezhetők. *A korszerű tartalomszolgáltatás és a magasabb biztonsági szintet nyújtó adatkezelési eljárások új menedzselési eljárásokat igényelnek, amihez éveken keresztül tartó tervezési, szervezési, technikai, képzési és szabályozási folyamatok szükségesek. Ezeket új együttműködési formákkal, stratégiai partnerekre történő támaszkodással, az ipar és a szolgáltatók szoros bevonásával, és az MH érdekeinek érvényesítését szolgáló korszerű garancia rendszer kialakításával kell támogatni.*

Információvédelem területén a dokumentumok, jogszabályok, publikációk és egyéb források (pl. szabványok, ajánlások, kézikönyvek) gyakran eltérő szakkifejezéseket alkalmaznak, mutatva, hogy hazánkban még nem alakult ki egységes nyelvezet. Ugyanez a megállapítás érvényes az MH esetében is; a magyar katonai terminológia *kidolgozatlannak tekinthető*. Az *MH katonai szaknyelv kialakításáért és fejlesztéséért felelős alrendszereknek*

(tanácsok, oktatási intézmények, tudományos testületek), a szakterület képviselőinek jelenleginél hatékonyabban kell támogatni a terminológiai konferenciákat, szakkifejezések összehangolására irányuló törekvéseket, illetve tágabban értelmezve a *katonai nyelvápolást*.

A fejezet befejezéseként az információbiztonságra vonatkozó olyan általános megállapítást idézek, ami világos feladatot szab a tervezők, az üzemeltetők, a felhasználók, és a biztonságért felelős személyek számára:

- a teljes (információs) infrastruktúra biztonsága az alkotóelemek biztonságától függ;
- a fenyegetés és a sebezhetőség szintje folyamatosan emelkedik, így a védelmi rendszabályoknak is legalább ilyen, vagy ennél nagyobb mértékben kell fejlődnie. [116.]

3. AZ INFORMÁCIÓBIZTONSÁG MENEDZSELÉSE

Az MH-nál az információk biztonságáért *nem lehet egy szervezetet felelőssé tenni*. Az információs követelmények meghatározása vezetői feladat, míg az adatok (és adatkezelő rendszerek) biztonsága a tervezők, kivitelezők, üzemeltetők, felügyelő hatóságok, ügyintézők/felhasználók és biztonságért felelős személyek *összehangolt tevékenységének eredménye*, melynek fontosabb menedzselési kérdéseit a következőkben látom.

3. 1. Felelősség

3. 1. 1. Kormányzati szintű felelősség

Kormányzati feladat a megfelelő jogszabályi háttér, az információvédelmi feladatok felügyeletéhez, támogatásához szükséges szervezetek kialakítása és fenntartása, a nemzetközi szervezetek munkájában való részvétel.

A személyes adatok védelmével és a közérdekű adatok nyilvánosságával kapcsolatos ügyekben az adatvédelmi biztos lát el ellenőrzési, véleményezési feladatokat, illetve elősegíti a jogszabályok végrehajtását. [115.]

A közokiratok kezelésének szakmai irányítását a belügyminiszter (2006. augusztus után a Miniszterelnöki Hivatalt (MeH) vezető miniszter) a Kormányzati Iratkezelési Felügyeleten keresztül látja el. [118.]

Az informatikai védelem ellenőrzése az informatikai és hírközlési miniszter (2006. augusztus után a MeH-et vezető miniszter) hatásköre. [119.]

Az információvédelmi feladatok ajánlások formájában történő meghatározása a 90-es évek közepétől az ITB (2005-től a Kormányzati Informatikai Tárcaközi Egyeztető Bizottság) feladata.

A MeH államtitkára (mint kormánymegbízott) felelős a kormányzati szervezetek benyújtott informatikai stratégiájának, valamint az azt támogató éves fejlesztési és beszerzési tervek áttekintéséért. [120.]

Az elektronikus aláírással kapcsolatos hitelesítési rend felügyelete a Nemzeti Hírközlési Hatóság (2004. előtt Hírközlési Felügyelet) feladata. [121.]

A minősített adatok védelmének szakmai felügyelete 2006-ig a belügyminiszter, ez után a MeH-et vezető miniszter felelőssége.[49] [122.]

---

[49] A MH-nál a minősített adatok védelmének szakmai felügyeletét a MeH-et vezető miniszter és a honvédelmi miniszterrel együtt közösen látja el.

A rejtjeltevékenység felügyeletét a MK Információs Hivatal látja el (a hatósági jogkört első fokon az Országos Rejtjelfelügyelet gyakorolja). [123.]

A NATO, EU és egyéb jogszabályokban rögzített külföldi minősített adatok védelmének felügyeletét a Nemzeti Biztonsági Felügyelet látja el. [124.] Emellett a törvényekben rögzített kétoldalú, minősített adatok védelméről szóló megállapodások gyakran a Belügyminisztériumot (2006. augusztus után jogutódját), vagy a Honvédelmi Minisztériumot azonosítják illetékes hatóságnak.

NATO adatok kezelésével kapcsolatban a honvédelmi tárca országos hatáskörű feladatokat kapott (NATO/NYEU Központi Nyilvántartó és a NATO/NYEU Központi Rejtjelelosztó működtetése, NATO TITKOS WAN magyarországi alhálózat üzemeltetése) így a kormányzati szervezetek mellett az MH képviselői is részt vesznek a NATO szervezetekkel történő együttműködésben.

Az MH adatkezelő rendszereinek üzemeltetésével és védelmével kapcsolatos tevékenységére az EDR hálózatgazda feladatait ellátó MeH-et vezető miniszter, [125.] a közigazgatási nyilvános kulcsú infrastruktúra működtetésére és a biztonsági felülvizsgálaton keresztül az EDR működésére Közigazgatási és Elektronikus Közszolgáltatási Központi Hivatal döntései lehetnek hatással. [126.]

A fentiek mellett az elektronikus hitelesítés szolgáltatás, az elektronikus iratkezelés tanúsítására akkreditált szervezetek, valamint a központi ellenőrző szervek informatikára (és informatikai védelemre) vonatkozó áttekintési és ajánlatok tételére irányuló hatáskörei (Állami Számvevőszék és a Kormányzati Ellenőrzési Hivatal), befolyásolhatják az MH információvédelmi feladatait.

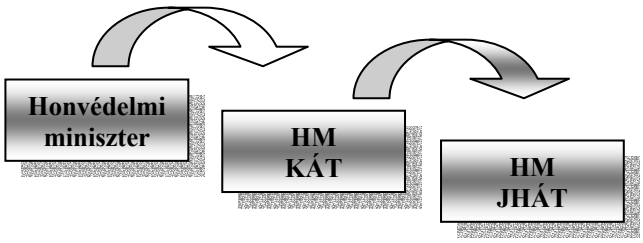
Tapasztalatom, hogy a bemutatott, MH szempontjából felettes szervek szerteágazó felügyeleti tevékenysége horizontálisan nem összehangolt. Esetenként a jogszabályok egyeztetése kapcsán az alkalmazó szervezetek hívják fel a jogszabályalkotók figyelmét azokra az ellentmondásokra, amelyeket fel kell oldani ahhoz, hogy végrehajthatók legyenek a meghatározott feladatok.

3. 1. 2. MH szintű szakmai felelősség

A honvédelmi miniszter információbiztonságért való felelőssége a honvédelemről és a Magyar Honvédségről szóló törvényben rögzített, mely felelősség 2006. júliusig a közigazgatási államtitkárhoz került (az erre vonatkozó szabályozók a *szakirányításért való felelősséget* kötötték a közigazgatási államtitkárhoz), illetve majd a szakirányítási feladatok

„szakmai irányítás”-ként definiált része a HM jogi helyettes államtitkár (JHAT) hatásköre volt.

A JHAT a szakirányítás keretei között „szakmailag irányította” az információk védelmével és a közérdekű adat nyilvántartásával kapcsolatos szabályzók előkészítését, azok végrehajtását, és érvényesülésük ellenőrzését. [127.]



11. ábra: Az információvédelem szakirányításáért való felelősség 2005. április és 2006. július között

Az MH működésére vonatkozó szabályozók nem világították meg a „szakirányítás” és a „szakmai irányítás” közötti különbséget, ami azért fontos, mert ha a szakmai irányítás szűkebb kategória, akkor a szakirányítás „maradék” részének végzésére is a tevékenységnek megfelelő szervezeti elemet kell azonosítani (vagy azt a vezetőnek kell végeznie).

2006. augusztusától a jogi szakállamtitkár kapta meg az információvédelmi tevékenység felügyeletét. [128.]

Az információvédelmi szakirányításának támogatásához szervezeti elemet kell kialakítani a Honvédelmi Minisztériumnál, melyhez szükség van az információvédelemre vonatkozó szakirányítási tevékenység [129.] meghatározására, amit a következőkben látok:

- az MH adatkezelő rendszerei védelmének jogszabályokon-, NATO, EU Biztonságpolitikákon, valamint a támogató direktívákon és irányelveken alapuló normatív rendelkezésekben történő kidolgozása;
- az információvédelmi tevékenységek végrehajtásával kapcsolatban egyedi intézkedések kiadása, valamint döntés (vagy döntés előkészítés) a nem szabályozott kérdésekben;
- az információbiztonságot érintő jogszabályok és egyéb rendelkezések véleményezése, állásfoglalás az MH szervezeteinek információbiztonságát érintő kérdésekben;
- az információvédelmi tevékenység szakirányításához szükséges információk kérése MH-n belül és más szervezetektől, valamint arra jogosult hatóságok, nemzeti, NATO, EU vagy egyéb illetékes szervezetek tájékoztatása;

- az információvédelem szakfelügyelete (a jogszabályok és egyéb központi rendelkezések érvényesülésének ellenőrzése, szükség esetén intézkedés az érvényesítés érdekében);
- az információvédelmi szaktevékenységekre vonatkozó képzési követelmények és a képzés rendjének meghatározása;
- a nemzeti hatóságokkal, kormányzati szervekkel, NATO, EU vagy más nemzetközi biztonsági szervezettel való kapcsolattartás során a MH adatkezelő rendszereit érintő kérdésekben az információbiztonság teljes körű képviselete.

Az információvédelem szakirányításával kapcsolatos feladatokat 2005. áprilisától a HM Jogi és Információvédelmi Főosztály, 2006. augusztusától a HM Informatikai és Információvédelmi Főosztály két osztálya végzi, amelyek – országos szintű szolgáltatásként – ellátják a *NATO/NYEU Központi Nyilvántartó,* és a *NATO/NYEU Központi Rejtjelelosztó* feladatkört is.

Az információbiztonság szakterületeiért való felelősség 2000-2005 között háromszor változott a minisztériumban, és az átalakítások során megosztott volt.[50] A 2005. áprilisban kialakult szervezeti rend az első, amelyben egy kétprofilú főosztály egy részén belüli szervezeti elemeké a felelősség az információbiztonság összes szakterületéért.

Az előző fejezetrészben ismertetett széttagolt kormányzati felelősségi rend, a szerteágazó felhasználói követelmények, és az azokat kielégítő információs infrastruktúra egységesítési szükségessége jelzi, hogy *az MH méretű információs képességek információvédelmi felügyelete eltérő szervezeti célok alapján működő szervekhez rendelve nem valósítható meg*.

A felügyeleti funkció hatósági követelményként elektronikus információvédelmi területen jelenik meg,[51] de a katonai szervezetek adatkezelő képességeinek (valamint az MH szintű rendszereinek) kialakítása, fejlesztése fizikai-, személyi-, és dokumentumvédelem területén is *szakirányítást igényelnek* (pl. nyilvántartó infrastruktúra kialakítása és fenntartása, ügyviteli utaltsági rend karbantartása, szakmai beiskolázások összehangolása).

Külön említést érdemel a NATO/NYEU Központi Nyilvántartó és a NATO/NYEU Központi Rejtjelelosztó felelőssége és hatásköre. Ezek a funkciók a nemzeti hatóságok szakmai felügyelete alatt állnak, de *működéshez szükséges információkat közvetlenül kaphatnak illetékes NATO nyilvántartó szervektől, valamint feléjük tartoznak elszámolási*

[50] Ezen időszak előtt az elektronikus információvédelmi kérdések informatikai, híradó (ezen belül elkülönítetten rejtjelző) szakterületeken jelentek meg, őrzésvédelmi és ügyviteli feladatkörök voltak azonosítva.
[51] A rejtjelzés és a külföldi minősített adatok védelme területeken.

kötelezettséggel. *A két funkciót ellátó szervezeti elem felügyeleti feladataival, működési rendjével kapcsolatosan jogszabály követelményeket nem határoz meg*. Mindkét esetben fő feladatnak tartom az akkreditált nyilvántartó szervek adatainak nyilvántartását, a nyilvántartók működésére vonatkozó szakmai követelmények kialakítását (pl. alkalmazott segédletek, nyomtatványok és eljárások, képzés, belső ellenőrzés, akkreditálási és újra akkreditálási követelmények, a biztonsági események jelentésének tartalma és rendje). A központi nyilvántartóknak támogatni kell a hatóságok akkreditálásra, újra-akkreditálásra, felügyeleti ellenőrzésekre, központi képzések kialakítására vonatkozó tevékenységét, és naprakész adatokat kell biztosítani a nemzeti/NATO hatóságok felé.

3. 1. 3. A közép szintű katonai szervezeti szint információvédelmi feladatai

A katonai szervezetek tevékenységének támogatása, a szükséges feltételek biztosítása területén az elöljáró katonai szervezetnek jelentős feladatai vannak (pl. hadműveleti követelmények, felhasználói igények meghatározása, képzések szervezése, ellenőrzések), így szükség van a *szakfeladatok szervezeti szinteknek megfelelő strukturálására.*

A működőképes közép szintű információvédelmi szakfelügyeleti képességek igénye 2002-2003-ban jelent meg erőteljesen az adatkezelő rendszerek kialakításával és fenntartásával kapcsolatos intenzíven gyarapodó tevékenységek, az összetett hatósági ügyintézés támogatása érdekében.

Elektronikus adatkezelő rendszerek esetében a kezelt adatok *legmagasabb minősítési szintje* és az *alkalmazott védelmi rendszabályok bonyolultsága* a rendezőelv, ami alapján 2004-től kezdődően a *biztonsági követelmények meghatározása*, a rendszer-specifikus *védelmi rendszabályok kialakítása és az akkreditáláshoz történő felkészülés, a különböző szintű ellenőrzések* területein a NATO adatkezelő rendszerek menedzselése során jól működő, strukturált eljárásrend alakult ki az MH szervezeti szintjei között.

Ennél a szervezeti szintnél kulcskérdés annak azonosítása, hogy a védelmi feladatok mely szintjénél kell önálló szakbeosztásokat kialakítani, és melyek azok az információvédelmi feladatok, amelyeket megbízás alapján kell ellátni.[52]

3. 1. 4. A helyi biztonsági menedzsment

A katonai szervezetek elhelyezési és alkalmazási sajátosságai miatt *központilag nem határozható* meg egységesen az információvédelmi szakfeladatokat ellátó szervezeti elemek összetétele. Az *önálló beosztású* (pl. ügykezelő, rendszeradminisztrátor, technikus, rejtjelző

[52] Nem logikus, erőforrás pazarló megoldás, ha a középszintű vezető szervnél szaktisztek helyi biztonsági funkciókat látnak el *az alárendelt katonai szervezetek szakmai támogatása helyett*.

nyilvántartó), vagy *megbízásként ellátott biztonsági funkciók* (pl. titokvédelmi felügyelő, rendszer biztonsági felelős) együtteséből kell egy olyan menedzsmentet kialakítani, ami a személyi védelemnél említett *összeférhetetlenségi követelmények figyelembe vételével* képes az információbiztonsági kérdések teljes körű kezelésére.

Központilag tisztázandó kérdés, hogy az információbiztonság felügyeletére kijelölt személy az *általános vezetői felelősség keretein belül felel a rendszabályok* kialakításáért és fenntartásáért vagy *végrehajtói (és végrehajtást irányítói)* feladatai is vannak. Az ITB 12. ajánlás egyértelműen elkülöníti a vezetői és a végrehajtó tevékenységeket, és *biztonsági vezetői* funkciót, valamint annak szakmai alárendeltségébe *titokvédelmi felügyelőt (és más biztonság funkciókat*) azonosít. Külföldi adatok védelme érdekében a biztonsági megbízott számára jogszabály *kifejezetten végrehajtó típusú feladatokat is meghatároz* (pl. őrzi a tartalék kulcsokat és a belépésre/hozzáférésre feljogosító kódokat), [130.] de általában csak a „gondoskodik" kifejezést alkalmazza, ami *lehetőséget teremt a feladatok strukturálására*.

Jó összehasonlítási alap a kanadai megoldás, mely szerint a kormányzati szervezeteknek biztonsági felügyelőt (Departmental Security Officer; DSO) kell kinevezni, akinek feladata egy olyan biztonsági program kialakítása és irányítása, ami biztosítja a biztonságpolitikával kapcsolatos koordinációs feladatok végrehajtását és a védelmi rendszabályok alkalmazását. Ez az adminisztrációs feladatok (pl. képzés és biztonsági tájékoztatók, továbbképzés, nyilvántartás, kockázat menedzsment), valamint a hozzáférés felügyelettel-, a fizikai védelemmel-, a biztonsági ellenőrzésekkel-, az elektronikus információvédelemmel-, a vészhelyzetek kezelésével-, a helyreállítási tevékenységekkel-, a szerződések biztonsági részeivel és a biztonsági események kivizsgálásával kapcsolatos feladatok menedzselését jelenti. [131.]

A „security officer" más NATO tagállamoknál is ehhez hasonlóan nem felelős vezetőként, hanem olyan *végrehajtó feladatokat is végző személyként azonosított*, aki pontos szakmai ismeretekkel bír, feljogosítással rendelkezik helyi biztonsági kérdésekben (pl. KORLÁTOZOTT TERJESZTÉSŰ minősítési szinten engedélyezi a számítógépek vagy helyi hálózatok üzemeltetését, a helyi sajátosságoknak megfelelően meghatározza a megsemmisítési módokat, ellenőrzi a megsemmisítő eszközök megfelelőségét, nyilvántartásokkal rendelkezik, adatszolgáltatást végez).

A MH-nál kialakult megbízási rend (mely szerint a szervezetek törzsfőnöke (vagy vezető helyettese) a titokvédelmi felügyelő/biztonsági megbízott) inkább általános vezetői felelősséget, és nem szakmai tevékenységet jelent. Emiatt nem logikus a minisztérium egyik vezető beosztású személyét (HM vagy MH) biztonsági megbízottként azonosítani. Egy felső

szintű vezetőhöz végrehajtói feladatok (pl. tartsa nyilván a hozzáférésre jogosult személyeket, őrizze a biztonsági területek tartalék kulcsait) helyett *általános vezetői felelősséget* kell rendelni.

Az információvédelemért felelős vezetők számára jelenleg *nincs központi (kormányzati vagy MH szintű) alapképzés*. *Jogszabály végzettségre vonatkozó követelményt nem határoz meg e feladatkör ellátás betöltéséhez*.[53] Jelenleg az a felelős személy (pl. titokvédelmi felügyelő/biztonsági megbízott, informatikai védelemért vezető), akinek a vezető megbízásából ki kell alakítani a helyi információvédelmi menedzsmentet, és a védelmi rendszabályokból egy összefüggő rendszert kell kovácsolnia, tevékenységét jogszabály ismeretére, gyakorlati tapasztalataira, és a beosztott állomány tudására tudja alapozni.

A kialakult gyakorlatot az MH-nál célszerű felülvizsgálni, és az információvédelmi menedzsment vezetésére olyan, a törzsbe rendszeresített beosztást kialakítani, ahonnan *vezethetők a védelmi rendszabályokért felelős személyek,* és a szervezet vezetőjének (vagy kijelölt vezető helyettesének) irányába *közvetlenül képviselhető az információvédelem*. Ennek támogatására ki kell választani azt az ismeretanyagot, ami az információvédelem szervezeti szempontból lényeges vezetői feladatait tartalmazza (vonatkozó jogszabályok, a szervezetnél alkalmazott információs rendszerek üzemeltetésével kapcsolatos tervezési, ellenőrzési feladatok, változáskezelés, a szervezet szempontjából fontos információvédelmet érintő projektekben való részvétel feladatai, felettes szervekkel való kapcsolattartás/jelentési kötelezettségek) és szervezett formában el kell kezdeni az érintett vezető állomány képzését. A szervezetek információvédelmének irányításáért felelős személyt ennél részletesebben, az elvégzendő szakmai feladatok függvényében kell képezni, a szervezet információvédelmi rendszabályainak kialakításával és fenntartásával kapcsolatos feladatok szervezése és a hatékony szervezeten kívüli szakmai kapcsolattartás érdekében.

A közép és felső szintű szervezetek vezetési feltételeinek biztosítása támogató szervezetek feladata, így ezen esetekben a védelmi rendszabályok csak *szervezetek tevékenységének összehangolásával alakíthatók ki*. Az adatbirtokos szervezet egyértelműen az MH, a védelmi feladatokért első fokon a honvédelmi miniszter felel, aki a védelmi feladatokat szigorú rend szerint ruházza át. A védelmi rendszabályok szervezésekor *nem az a kulcskérdés, hogy a rendszeradminisztrátor, a rejtjelző, vagy a felhasználó kinek az állományában van*, hanem az, hogy az érintett vezetők hogyan tudják úgy összehangolni a tevékenységeket, hogy

[53] A NATO minősített adatok védelméért felelős biztonsági megbízott kinevezésével kapcsolatban az illetékes hatóság egyetértési joga gyakorlatilag formalitásnak tekinthető, mert a személyi biztonsági tanúsítvány megléte esetén nincs alapja a megbízás megtagadásának, így ez a jog gyakorlatilag csak regisztrációs célokat szolgál.

a védelmi feladatok között ne maradjanak rések, és a végrehajtás során nem keletkezzen szervezetek közötti feszültség.[54]

A kezelt adatok védelmének egyik kulcskérdése a szükséges szakértelemmel rendelkező állomány megléte. Váncsa Julianna már 2000-ben említette a szakképzett informatikai munkaerő elvándorlásának problémáját, [132.] ami az eltelt időszakban tovább erősödött, szélesedett. Az átszervezési és létszámcsökkentési feladatok kapcsán egy-egy szervezetnél gyakran hosszú hónapokig visszaeshet a szakmai színvonal, *miközben a vezetői elvárások a korszerűsítési folyamattal lépést tartva emelt szintű követelményeket határoznak meg*.

Bonyolultabb esetben egy szakirányú képzettség megszerzése éveket jelenthet. Az is hosszabb időt vesz igénybe, amíg új igények szerint a képzésért felelős alrendszerek (humán szervek, oktatást és képzést végző intézmények) ki tudják alakítani a szükséges infrastruktúrát, ami központilag menedzselt képzési rend szükségességét jelzi.

Hazánkban a második fejezetben azonosított *információvédelmi szakterületeket lefedő akkreditált Országos Képzési Jegyzékben szereplő komplex képzés nincs*, így a közigazgatás területén a szervezetek egyedi megoldásokat alakítanak ki képzéseikre.

A Zrínyi Miklós Nemzetvédelmi Egyetemen (ZMNE) 2006-ban megtörtént egy rejtjelfelügyelő, és egy rendszerbiztonsági felelős kétéves képzés megszervezése és akkreditáltatása. *Ezzel az iránymutató kezdeményezéssel kapcsolatban kiemelem az elméleti és a gyakorlati ismeretek összhangjának szükségességét*. Létfontosságú, hogy a képzést végrehajtók rendelkezzenek az alkalmazott rendszerekre, eszközökre és eljárásokra vonatkozó gyakorlati ismeretekkel. Ez a követelmény a képzés során szükségszerűen szervezési nehézségeket okozhat, mert az alkalmazott információvédelmi megoldások egy részének oktatásakor jogosulatlan személy MH szempontjából érzékeny adatokat nem ismerhet meg, így *kiemelem a honvédelmi tárca szakirányításért felelős, és az oktatásért felelős szervezeti elemek együttműködésének fontosságát.*

A tanfolyam rendszerű képzés keretén belül az MH-nál a nemzeti és NATO ügykezelők számára háromhetes ügykezelői alaptanfolyamok, elektronikus információvédelem területén a ZMNE Híradó Tanszék bázisán háromhetes rejtjelző, és egyhetes (2007-től kéthetes) helyi rendszer biztonsági felelősi alaptanfolyamok, 2006. őszétől rendszer üzemeltetés biztonsági felelős (rendszeradminisztrátor) tanfolyamok, illetve 2-3 napos kiegészítő szaktanfolyamok támogatják az információvédelmi menedzsmentek tevékenységét.

---

[54] Az országos kiterjedésű hálózatokat üzemeltetése során a rendszer-specifikus biztonsági szabályozás keretei átlépik a szervezetek határait, így *a felelősségi körök kijelölését központi feladatnak kell tekinteni*.

Speciális szakterületeken (pl. kompromittáló kisugárzás elleni védelem, elektronikus adatkezelő rendszerek kockázatelemzése, biztonsági felügyeleti alrendszer üzemeltetése) a szakirányításért felelős szervezetnek meg kell találnia az MH specialitásainak megfelelő képzést (pl. NATO szakiskola, külföldi vagy hazai szaktanfolyamok).

A NATO, EU minősített adatokat felügyelő biztonsági megbízottak továbbképzésére évi egy alkalommal,[55] az ügykezelők, és az elektronikus információvédelemért felelős személyek továbbképzésére egy-két alkalommal történik, melynek során feladat a szükséges alapismeretek fejlesztése és a gyakorlati tapasztalatok feldolgozása, és nem alapismeretek közlése.

A helyi biztonsági menedzsment egyik legfontosabb feladata az ügyintézők, felhasználók elméleti és gyakorlati képzése, ami nem egyenértékű azzal a leegyszerűsített megoldással, hogy új beosztásba került személy elolvassa biztonsági előírásokat. Az érintett személyeknek meg kell tanulni, hogy a kezelt adatokat milyen mechanizmusok védik, és a munkavégzés során kinek milyen feladata, kötelme van. Fel kell ismerni a rendellenességeket, el kell dönteni, *melyek azok az esetek, amelyeket önállóan kell megoldani, és mikor kell segítséget kérni*. Pontosan tudni kell, hogy biztonsági esemény bekövetkezésekor (vagy annak gyanúja esetén) *kinek, milyen tartalmú jelentést kell tenni, vagy vészhelyzet esetén milyen tevékenységet kell megkezdeni*.

A helyi képzésnek támaszkodnia kell az elmúlt időszak tapasztalataira, be kell mutatnia a várható változásokat, azok biztonsági vonzatait. *A gyakoriságot elektronikus adatkezelő rendszer felhasználói számára minősített adatok esetében évi két alkalommal, egyéb esetekben egy alkalommal* tartom szükségesnek.[56]

---

[55] A kialakult gyakorlat szerint a Nemzeti Biztonsági Felügyelet felelősségi körébe tartozó továbbképzés tematikáját a NATO/NYEU Központi Nyilvántartó állománya állítja össze, a felügyelet elnöke hagyja jóvá, majd a képzés a Nyilvántartó szervezésében a minisztérium és a Felügyelet előadói által történik.

[56] A gyakoriságot tapasztalataim mellett a 2005. májusi 2. Regionális Information Assurance szemináriumon történt konzultációkra alapozom. A résztvevők ezt a rendszert a NATO-ban kialakult gyakorlattal indokolták, és a témához tartozónak tartották az általános biztonsági ismeretek oktatását is (pl. terrortámadás, zsebtolvajlás, utazás közbeni trükkös lopás, otthoni munkavégzés).

3. 2. A szabályozás

A HM szintű jogszabályok, és állami irányítás egyéb jogi eszközei körébe tartozó nem minősített szabályozók áttekintése alapján megállapítom, hogy az MH *nem rendelkezik egy olyan hivatalosnak tekinthető állásfoglalással*, ami az információbiztonságra vonatkozó egységes, felső szintű követelmény meghatározásával megalapozza az alacsonyabb szabályozási szinthez tartozó szakterületi feladatokat.

A jogszabályokban meghatározott szabályozók egy csoportja szabályzat formájában áll rendelkezésre (pl. a 79/1995. (VI. 30.) Korm. rendelet végrehajtását szolgálja a HM-MH Titokvédelmi és Ügyviteli Szabályzat és az MH Informatikai Szabályzat információvédelmi feladatokra vonatkozó része, a 43/1996. (III. 19.). Korm. rendelet végrehajtására készült az MH Rejtjelszabályzata, a közszolgálati jogviszonnyal összefüggő adatkezelésre és a közszolgálati nyilvántartásra vonatkozó szabályokról szóló 233/2001. (XII. 10.) Korm. rendelet végrehajtását szolgálja a 42/2002. (HK 16.) HM utasításban kiadott Ideiglenes Közszolgálati Szabályzat).

A belső rendelkezések másik csoportja a *felelősségi rendet, vagy rendszerre, adatkezelési képességre vonatkozó feladatokat* határoz meg (pl. a 169/2000. (HK 19.) MHPK intézkedés a katonai szervezetek biztonsági megbízottainak kijelöléséről, a 33/2002. (HK 13.) HM utasítás az elektronikus információvédelemről, a 12/2006. (HK 4.) HM utasítás a közérdekű adatok közzétételének módjáról), a 47/2003. (HK. 10.) számú honvéd vezérkari főnök intézkedés az MH állandó jellegű híradó és informatikai hálózatának békeidejű üzemeltetési és felügyeleti rendjéről, a 82/2002. (HK 26.) HM utasítás a NATO Iroda-automatizálási Rendszer (NIAR) biztonságával kapcsolatos feladatokról, a 9/2004. (HK 4.) HM utasítás az Európai Uniós nyílt és minősített elektronikus levelezéshez szükséges információs rendszer kiépítéséről, az 58/2006. (HK 12.) HM utasítás a HM költségvetési gazdálkodási információs rendszerről, a 81/1997. (HK 20.) MH PK VKF intézkedés az Internet igénybevételével kapcsolatos titokvédelmi és adatbiztonsági rendszabályok betartásáról).

Az információvédelemre vonatkozó szabályozók *nincsenek egységes rendbe fogva*, *a szabályzatok nem követik naprakészen a szervezeti, technológiai és egyéb változásokat.*

Az elektronikus adatkezelő rendszerek üzemeltetésével, biztonságával kapcsolatos belső rendelkezések a biztonsági követelményeket nem egységes szemlélet alapján határozzák meg. A rendszer-specifikus szabályozáshoz a szabályzatok nem szabnak pontos kereteket, illetve a

technikai lehetőségekhez igazodó szervezet-centrikus szabályozási rend miatt a védelmi rendszabályok nem garantáltan illeszkednek egymáshoz.

A NATO csatlakozás az infrastruktúrák és a rendszabályok területén napjainkban *nehezen finanszírozható párhuzamosságot eredményezett*. Dokumentumvédelem területén e párhuzamosság ellen foglalt állást Király Imre, amikor a helyi szabályozás kapcsán kijelentette, hogy „a katonai szervezetek szintjén nem célszerű külön-külön szabályzatban rögzíteni a nemzeti és a NATO adathordozók kezelésével kapcsolatos helyi eljárási szabályokat", [133.] de a gyakorlat másképpen alakult.

A továbbiakban az említett hiányosságok kiküszöbölése érdekében kialakítandó szabályozási rendszert mutatom be.

3. 2. 1. Az információ biztonságpolitika

Az információ „biztonságpolitika" kifejezésre nincs általánosan elfogadott meghatározás. Értelmezése: a *szervezet vezetésének hivatalos döntése* a biztonsági követelményekkel kapcsolatban (a Közös Követelmények megfogalmazása szerint pl. a biztonságpolitika *szabályok*, *eljárások* és *irányelvek* összessége).[57]

A tömör, fő vonalakat ábrázoló, az összes szereplő számára fontos kérdést tartalmazó, jóváhagyott, és az *MH vezetői által támogatott* dokumentum nem lehet kőbe vésett, mert a különböző szintű stratégiákhoz hasonlóan kezelnie kell a szervezeti célok, az alkalmazott technológia, a nemzeti/nemzetközi jogszabályi-, vagy információs környezet változásait.

Az ITB 12. ajánlás az információ biztonságpolitika tárgyalásakor nem nyújt igazi támpontot, csak az érték- és kockázattal arányos védelmet, a jogszabályoknak való megfelelőséget, az állami szervezetek folyamatos rendelkezésre állási követelményét és a felhasználóbarát védelmi megoldásokat említi. [134.]

Az MSZ ISO/IEC 17799:2006 szabvány ennél pontosabb ajánlásokat tesz (cél meghatározása, vezetőség szándékának kinyilvánítása, szabályozási keretrendszer kialakítása, kockázatelemzés, felelősség meghatározása, támogató dokumentumok azonosítása). [135.]

Az információ biztonságpolitikára vonatkozó megközelítések megértéséhez jó támpont az Egyesült Államokban alkalmazott megközelítés, [136.] ami a biztonságpolitikának három csoportját különíti el:

– szervezeti politika (program policy);

---

[57] A „security policy" kifejezésből a nemzetközi szabványok és egyéb források fordításakor gyakran „biztonsági szabályzat" válik (ez fordult elő pl. Nemzeti Biztonsági Felügyeletről szóló törvényben is). Egy brit szabvány honosításakor pl. az első változat még a „szabályzat", míg a második a „politika" kifejezést alkalmazta. Az MH-nál még előzmény nélküli biztonságpolitikával kapcsolatos félreértelmezés elkerülése érdekében kijelentem, hogy a két dokumentum eltérő célt szolgál, így ezek nem felcserélhető fogalmak.

- egy kiemelt területre irányuló feladat-specifikus politika (issue-specific policy);
- egy rendszerre vonatkozó, un. rendszer-specifikus politika (system-specific policy).

A különböző források politika alatt általában csak rendszer-, hálózat-, vagy IT politikát értenek, de a tartalom vizsgálatakor kiderül, hogy a politikának tartalmaznia kell fizikai-, személyi és dokumentumvédelmi kérdéseket is, így megnevezésként az „információ biztonságpolitika” kifejezést tartom elfogadhatónak (továbbiakban biztonságpolitika), és szükségesnek tartom, hogy az MH szintű politika *fedje le az információbiztonság összes területét.*

Az MH szervezeti típusú biztonságpolitika tartalmi elemeinek összeállításához kiindulási alapnak a nemzetközi/nemzeti szabványokat és az EU Biztonságpolitikát tekintem, amit kiegészítek más nemzeti ajánlásokban foglaltakkal, illetve a nemzeti, NATO és EU rendszerek üzemeltetése során szerzett tapasztalataimmal. A biztonságpolitika általános felépítés ennek megfelelően a következő:

- a biztonságpolitika hatályának azonosítása (alkalmazó MH szervezetek és háttérintézmények itthon és külföldön egyaránt), az információbiztonsági célok kijelölése;
- a biztonságért való szervezeti és egyéni felelősségek meghatározása (szakirányításért való felelősség HM szinten, közép és végrehajtó katonai szervezet/háttérintézmény szintjén való felelősség);
- az adatok besorolásának alapelvei (a második fejezetben foglaltak szerint);
- az adatkezelő rendszerek biztonsági alapelvei (nemzeti, NATO, és EU rendszerekre egyaránt, szükség szerint figyelembe véve a mobil képességeket is);
- a kockázatkezelésre vonatkozó követelmények és a maradvány kockázatok kezelésére vonatkozó eljárások (figyelembe véve a NATO, EU minősített adatkezelő rendszerekre vonatkozó követelményeket, sajátosságokat is);
- a fizikai-, személyi-, dokumentum és elektronikus információvédelem általános biztonsági követelményei (nemzeti, NATO, és EU rendszerekre egyaránt);
- a nemzeti és szövetségi, nemzetközi rendszerek magyarországi alrendszereire vonatkozó akkreditálás, jóváhagyás rendje és az ellenőrzés követelményei;
- a biztonsági események jelentésével, kivizsgálásával kapcsolatos általános követelmények, és a rendszabályok megsértésekor alkalmazandó eljárásrend;
- az információvédelmi képzés és továbbképzés általános rendje, a biztonság tudatosságot célzó programok;

- a biztonságpolitika végrehajtására szolgáló szabályozási rend meghatározása (a kormányzati és a NATO, EU követelményeket egyaránt figyelembe véve);
- a biztonságpolitika felülvizsgálatára vonatkozó követelmények.

A biztonságpolitika megfelelőségének ellenőrzésére a minőségirányításra vonatkozó szabvány, és az erre alapozott információvédelem irányítási rendszer szabvány követelményei szerint kialakított vizsgálatot tartom alkalmasnak. [137.][138.]

A vázolt biztonságpolitika hatáskörét az MH teljes szervezeti kereteire ki kell terjeszteni, így kiadása formailag *miniszteri utasításként* történhet.

3. 2. 2. Az információvédelem stratégiai szintje

Egy stratégia feladata az adott szakterületen a célkitűzések megvalósulási módjának meghatározása. A kellően átfogó stratégia összehangolja a különböző távú beruházási és fejlesztési terveket, illetve a környezeti hatások változásaikor (pl. pénzügyi szigorítások, terrortámadások miatti intézkedések, vagy a Védelmi Felülvizsgálat) segít a prioritások megváltoztatásában.

Közigazgatási szervek részére informatikai stratégia készítése 1993-tól kormányzati követelmény. Az MH-nál 2006-ban kiadott stratégiát megelőző tervezetekben (a tartalomra vonatkozó kormányzati követelmény hiányában) a biztonsági kérdések nem szerepeltek, szervezeti egyetértés hiányában a tervezetek kihagyták az információvédelmet. Ez nézőpont a KIETB 22. ajánlásának megjelenésével tarthatatlanná vált, mert az informatikai stratégiára vonatkozó követelmények között jól azonosíthatók az információvédelem szempontjából lényeges kérdések, mint pl. biztonsági helyzetértékelés, az információvédelemre vonatkozó perspektivikus elképzelés, felelősségi rend, a szabályozás rendje, [139.] így ebben a dokumentumban problémamentesen kidolgozhatók az információvédelem stratégiai szintű követelményei és feladatai.

3. 2. 3. A szabályzatok, szakintézkedések és egyéb szabályozók

Ezen a szabályozási szinten a biztonságpolitika általános követelményeire és alapelveire támaszkodva a védelmi rendszabályokat kell kidolgozni. Az általánosan nem szabályozható kérdések szakutasítás, az eseti jellegű feladatok intézkedés formájában rendezhetők.

A kormányzati szintű, szervezeti és rendszer-specifikus szabályzatokra vonatkozó követelmények a következők:

a) *iratkezelési szabályzat és irattári terv*, beleértve az elektronikus iratkezelés szabályozását; [140.]

b) a személyi iratok kezelésének technikai szabályait tartalmazó *közszolgálati adatvédelmi és az iratkezelési szabályzat*; [141.]

c) *adatvédelmi és adatbiztonsági szabályzat*; [142.]

d) *informatikai biztonsági szabályzat*; [143.]

e) *titokvédelmi szabályzat;* [144.]

f) *rejtjelszabályzat*; [145.]

g) *közzétételi szabályzat*; [146.]

h) NATO, EU minősített adatok védelmére vonatkozó *biztonsági szabályzat*, *intézkedési terv* és *rendszer-specifikus szabályzatok*: *rendszer biztonsági utasítás*, *üzemeltetés biztonsági szabályzat;* [147.]

i) *elektronikus hitelesítés szolgáltatási szabályzat*; [148.]

j) kormányzati fenntartású rendszerekhez (Egységes Kormányzati Gerinchálózat, Központi Elektronikus Szolgáltató Rendszer) csatlakozó rendszerekre vonatkozó *informatikai biztonsági szabályzatok, valamint az* egységes digitális rádió-távközlő rendszerhez (EDR) csatlakozó alrendszerek *üzemeltetését szabályozó belső rendelkezés*.

Az a)-e) pontok szerinti szabályozók tartalmilag több ponton érintenek olyan biztonsági követelményeket, amelyek összevonhatók, egy helyen kifejthetők (pl. illetéktelen megismerés elleni védelem követelményei, a hozzáférések felügyelete és megoldásai, a tárolás, az adatok és megismerésre jogosult személyek nyilvántartására vonatkozó követelmények), és a többi funkcionális szabályozó számára csak idézendők.

A biztonsági szabályzat és az intézkedési terv átfedésben van a nemzeti szabályozási kötelezettséggel (titokvédelmi szabályzat), valamint a NATO, EU követelményeken alapuló rendszer-specifikus szabályozással, amely kettősséget nem célszerű fenntartani.

Egy katonai szervezetnél az ismertetett jogszabályokból eredően (a rejtjelzést és a NATO/EU rendszer-specifikus biztonsági szabályzatokat nem említve) minimum a következő helyi szabályozókat kell készíteni: Titokvédelmi Szabályzat, Biztonsági Szabályzat, Intézkedési Terv, Számítástechnikai Védelmi Szabályzat, illetve Adatvédelmi Szabályzat.

Emiatt elsődleges feladatnak kell tekinteni e szabályozók összevonását, és kezelhetőre formálását. Az erre vonatkozó modernizálás több kormányzati szervet érintő, nemzeti, NATO, EU nyílt és minősített adatokra egyaránt vonatkozó feladat, melynek késlekedése, vagy hibái gátolni fogják a nemzeti hálózat-alapú képességek kialakítását.

A bemutatott szerteágazó védelmi feladatokat MH szinten nem lehet kezelhető méretű szabályzatban kialakítani, így a következő szabályzat-rendszer kialakítása tűnik a legjobb megoldásnak:

- a fizikai-, személyi- és dokumentumvédelem rendszabályai (egy szabályzatban vagy tovább tagolva, de mindenképpen lefedve a jogszabály által meghatározott iratkezelési szabályzatot és irattári tervet);
- MH közszolgálati adatvédelmi szabályzat;
- a közérdekű adat megismerésének szabályai az MH-nál;
- az elektronikus információvédelem általános követelményei (logikailag beágyazva és megalapozva az elkülönítetten kialakítandó rejtjelzésről-, és a kompromittáló kisugárzás elleni védelemről szóló szabályzatot);
- MH Rejtjelszabályzat;
- a kompromittáló kisugárzás elleni védelem rendszabályai.

A szabályozás harmadik szintjét az MH központi szakutasítások (és egyéb intézkedések) képezik, melyekre a következők mutatnak példát (a rejtjelzés és a kompromittáló kisugárzás elleni védelem kivételével):

- a szervezetek adatkezelésére vonatkozó helyi szabályozók tartalmi követelménye és kialakítási rendje;
- az adatkezelő rendszerek életciklusa során alkalmazandó kockázatkezelés rendje (a makro és rendszer-szintű elemzési és értékelési feladatok);
- az adatkezelő rendszerek akkreditálási és jóváhagyási rendje;
- az adatkezelő rendszerek biztonsági követelményeit tartalmazó szabályozó tartalmi és formai követelményei (a rendszer-szintű politika szinopszisa);
- az elektronikus adatkezelő rendszerek védelmi rendszabályait tartalmazó szabályozó tartalmi és formai követelménye;
- adatkezelésre, vagy adatkezelő rendszerre vonatkozó specifikus rendszabályok, eljárások.

Az önálló okmány formájában előzmény nélküli MH Elektronikus Információvédelmi Szabályzatra vonatkozó jogszabályban megalapozott kormányzati követelmény nincs.

Az országos kiterjedésű, a közigazgatásban érintett szervezeteket kiszolgáló rendszerekre vonatkozó szabályozása esetében megkezdődött a nemzeti szabványok részben történő alkalmazása (gyakorlatilag az információvédelmi irányításra vonatkozó szabványokból készített kivonatok kerülnek szabályzatként kiadásra).

A közigazgatási és az MH rendszerek szabályozásának összhangja érdekében az MH elektronikus adatkezelő rendszereire vonatkozó keretszabályozó struktúráját, tartalmi elemeit e tendencia figyelembe vételével kell kialakítani.

A rendszer-specifikus szabályzatokat az MH Elektronikus Információvédelmi szabályzatában megfogalmazott védelmi rendszabályok készletéből kell kialakítani úgy, hogy a különböző szemléletű ellenőrzési módszertanok vizsgálati szempontjai érvényesüljenek, valamint a NATO, EU rendszerekre vonatkozó szabályozók követelményei egyaránt teljesüljenek.

Helyi szabályozási szinten a biztonságpolitikára és a fenti szabályozókra támaszkodva *a Szervezeti és Működési Szabályzatban kell azonosítani az információbiztonságért felelős vezetőt*, és azt a *szervezeti elemet*, amelyik kialakítja/megvalósítja a védelmi rendszabályokat. Meg kell határozni, hogy a katonai szervezet adatkezelő rendszereinek védelmi rendszabályait *milyen helyi szabályozók tartalmazzák*, és mely szervezeti elemek felelőssége a *szabályozók kiadása és naprakészen tartása*.[58]

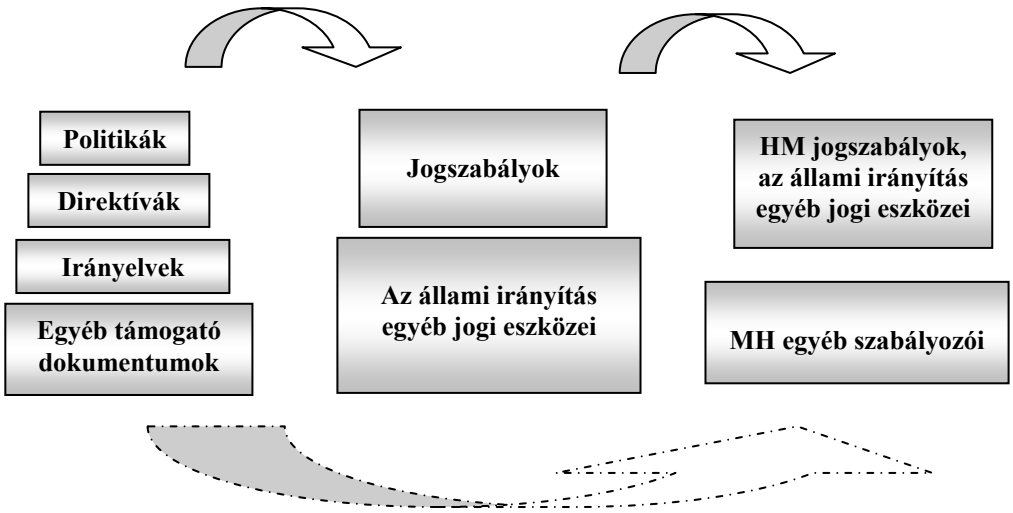
A feladatokat munkaköri leírásokban kell rögzíteni *attól függetlenül, hogy az adott információvédelmi feladat önálló beosztásban ellátott, vagy más beosztás mellett megbízás alapján végzendő*.

A szervezet-centrikus helyi szabályozás nemzeti elektronikus adatkezelés esetében a szervezet vezetőjének hatáskörében van (minősített adatok kezelése esetén is), míg a NATO, EU típusú, minősített adatkezelésre vonatkozó rendszer-specifikus szabályozás hatósági jóváhagyáshoz kötött. *Az eltérés felszámolása alapvető feltétel a nemzeti szintű hálózat alapú műveleti képesség kialakításához, a szövetségi rendszerekhez történő csatlakozáshoz.*

NATO vagy EU minősített adatok esetében a szabályozási környezet összetett. A biztonsági követelmények közvetítése (és a jogrendbe történő beillesztése) a *nemzeti hatóságok felelőssége*. Jelenleg a NATO, EU minősített adatokra vonatkozó biztonsági követelmények meghatározásakor az alkalmazó szervezet „illetékes biztonsági felügyelete” a „hatályos jogszabályok és az érvényes NATO, NYEU, illetve EU szabályok figyelembevételével” jár el, [149.] tehát *az MH központi szabályozóit illeszteni kell a NATO, EU információbiztonsági követelményeihez, irányelveihez is, ami mutatja a szabályozási rend ellentmondásait és összetettségét (12. sz. ábra)*.

[58] Gyakori félreértést okoz, hogy az MH-nál az SZMSZ-ek tartalmi követelménye központi belső rendelkezésben nem rögzített, így a vezetők gyakran nem értik, hogy az MH szabályozók, intézkedések követelményeinek megfelelő helyi struktúrákat az SZMSZ-ben lehet, és kell meghatározni.

Egy teljes szabályozási hierarchiát (politika, direktívák és irányelvek együttesét) egy törvénnyel és három kormányrendelettel nem lehet lefedni úgy, hogy az adatkezelő rendszerek együttműködése és védelmi rendszabályainak összehangoltsága garantálható legyen. Az egységes eljárások igénye előbb-utóbb részletezett, strukturált kormányzati szabályozást követel a jelenlegi jogszabályokra és eseti hatósági állásfoglalásokra épülő szabályozás helyett.



12. ábra: A szabályozási rend

A NATO, EU szabályozók közvetlen alkalmazása gyakori problémák forrása. A beruházások tervezéséhez, vagy helyi védelmi rendszer kialakításához keret-jellegű szabályozókat, vagy néhány oldalas lényegi fordítást nem lehet a helyi menedzsment, vagy a kivitelezők kezébe adni. A megfelelően részletes kormányzati szabályozás hiányában erre a helyzetre csak egy elfogadható megoldás létezik: *az adott kérdés eseti vizsgálata, és a feladatok szakirányítás rend szerinti meghatározása*.

3. 2. 4. Rendszer-specifikus szabályozók

Az elektronikus adatkezelő rendszerek védelmének kialakítása két fő részre bontható: az üzemeltetési környezet sajátosságaira reagáló *biztonsági követelményekre* (más megfogalmazás szerint rendszer-specifikus biztonságpolitika)-, és az ennek megfelelő *védelmi rendszabályokra.*

A biztonsági követelmények kialakításának a rendszer életciklusa szempontjából a lehető legkorábbi szakaszban kell kezdődnie. A tervezésben érintett szervezetek a kialakítás során *kockázatfelmérésre és elemzésre* támaszkodva beépítik a védelmi rendszabályokat, amelyek így a beruházási, korszerűsítési projektek szerves részévé válnak.

A biztonsági követelményeket tapasztalataim szerint minimum a következő szempontoknak megfelelően kell kialakítani:

- *A rendszer feladatának meghatározása és határolása.* Az elektronikus adatkezelő rendszer adott környezetben valamilyen tevékenységet támogat, melynek környezete, résztevékenységei, sajátosságai vannak, meghatározható elemekkel rendelkezik (közöttük gyakran csak logikai határok és közös erőforrások találhatók), amelyek rögzítése nélkül nem alakíthatók ki a védelmi rendszabályok.
- *A felelősségek meghatározása*. Azonosítani kell a szervezeten kívüli és szervezeten belüli felelősségeket (pl. az üzemeltetés, konfiguráció felügyelet, ellenőrzés, biztonsági események jelentése), a biztonsági menedzsment felépítését, eljárásrendjét.
- *A szükséges mértékű védelmi rendszer*. Az érvényben lévő szabályozók, a helyi sajátosságok, és a kockázatelemzés eredménye alapján fizikai-, személyi-, dokumentum- és elektronikus információvédelmi szakterületeken az arra jogosult hatóság által meghatározott szigorításokkal, kiegészítésekkel a biztonsági követelmények meghatározása.
- *A működés folytonosságra és /vészhelyzeti tevékenységre vonatkozó követelmények*. A reálisnak tekintett külső és belső, szándékos vagy véletlen események hatásainak szükséges mértékben ellenálló üzemeltetés kialakításhoz szükséges *folytonossági tervezés* (continuity planning) alapadatainak meghatározása (minimális szolgáltatások köre, szolgáltatás csökkenésre vagy kiesésre vonatkozó rendelkezések), a helyreállítás tervezéséhez (recovery planning) szükséges prioritások, határidők meghatározása. Vészhelyzetnek tekintett esetekben az erőforrások és a rendelkezésre álló idő függvényében az érzékeny adatok védelmi rendszabályai érdekében (a *védelmi rendszabályok megerősítése*, a minősített anyagok *biztonságos helyre történő szállítása,* vagy *vészmegsemmisítés)* a tervezési követelmények meghatározása.[59]

Szabályozás területén szakmatörténeti érdekesség az egyes NATO minősített elektronikus adatkezelő hálózatoknál a NATO csatlakozást követő időszakban kialakult *angol nyelvű, a NATO formai és tartalmi követelményei szerint kialakított biztonsági dokumentációk gyakorlata*, amit 2005-re sikerült felszámolni.

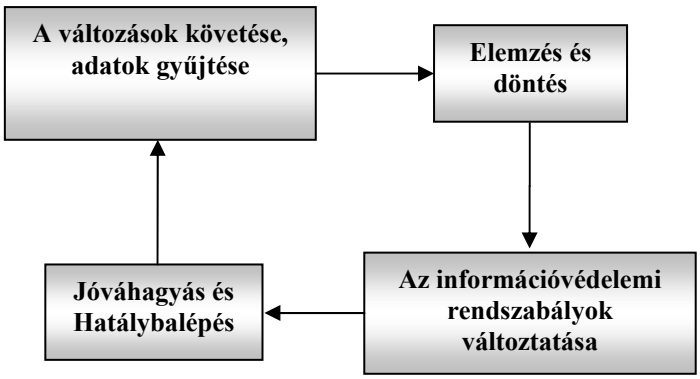
[59] A téma fontossága ellenére a működés folytonosságra vonatkozóan részletes nemzeti követelmény nincs kialakítva.

A helyi/rendszer-specifikus szabályozás speciális eseteként *tábori vagy egyéb ideiglenes adatkezelő rendszereknél is* szükség van a védelmi rendszabályok rögzítésére. Az állandó elhelyezési környezetre kialakított szabályozás valószínűleg nem alkalmazható, így a sajátosságoknak megfelelő rendszabályokat erre az esetre külön ki kell dolgozni.

A szabályozás másik speciális esete a rendezvényekre, gyakorlatokra vonatkozó védelmi rendszabályok meghatározása és kialakítása. Ezen a területen veszélyes lehet a *biztonsági szabályozók más szervezetek képviselőivel történő elkészíttetése* (amit aztán a végrehajtók automatikusan félretesznek, mert nem értik, nem ők készítették, így nem érzik a végrehajtásra vonatkozó felelősséget), vagy egy *másik rendezvény okmányrendszerének másolása.* Az említettek helyett az ideiglenes üzemeltetési helyszín, az alkalmazott eszközök, és a felhasználói kör függvényében kell a szabályozást kialakítani (NATO, EU rendezvény esetén közvetlenül alkalmazva a szükséges direktívákat és irányelveket), bonyolult esetben elöljárói szakirányítással támogatva.

3. 3. A szabályozás felülvizsgálata

Az adatkezelő folyamatok, és azok támadási módjainak *folyamatos változása, fejlődése* miatt ismétlődő rendszerű felülvizsgálat nélkül nem képzelhető el az információvédelem eredményes szabályozása (13. sz. ábra).



13. ábra: A szabályozórendszer felülvizsgálata

A felülvizsgálat feladata a tapasztalatok és környezeti változások alapján annak eldöntése, hogy *a szabályozás megfelel-e a jogszabályoknak, NATO, EU követelményeknek, és megfelelően támogatja-e a szervezeti célokat*. A változtatás szükségességének kimutatása mellett a felülvizsgálat feladata a *fejlesztési lehetőségek értékelése is*. A felülvizsgálat során bemenő adatként figyelembe kell venni:

– az MH rendeltetése, feladatai kapcsán az információs folyamatok változásait;

- az információbiztonságra vonatkozó jogszabályok, nemzetközi és nemzeti szabványok változásait;
- a nemzeti hatóságok, EU, NATO biztonsági szervezetek ellenőrzéseit, javaslatait;
- NATO, EU és egyéb nemzetközi, nemzeti szervezetek kutatási eredményeit, ajánlásait és tapasztalatait;
- az üzemeltetési és biztonsági ellenőrzések tapasztalatait, a biztonsági eseményekből levont következtetéseket, valamint az időszakos kockázatelemzés eredményeit;
- a támadó és védelmi módszereket érintő technikai változásokat.

A felülvizsgálatnak meg kell határozni a változtatással kapcsolatos *adminisztratív teendőket*, és az *egyéb kapcsolódó feladatokat* (pl. tájékoztatás, továbbképzés elrendelése).

Az adatgyűjtés, illetve a szakmai szervezetek információcseréje komoly, nagyméretű adathalmazt eredményez, így tudatosan meg kell határozni azokat az adatokat, amelyek alkalmasak a rendszabályok megfelelőségének bizonyítására. A közép és a felső szintű felügyeleteknél olyan eljárásokat kell kialakítani, amelyek biztosítják, hogy a különböző témájú és formájú dokumentumokból kigyűjthetők legyenek a szükséges adatok.

A MH Információ Biztonságpolitika esetében a felülvizsgálatot évente tartom szükségesnek, egyéb szabályozók esetében szabályozási szinttől és tartalomtól függően 1-3 éves gyakoriság indokolt. Ez a felülvizsgálati rend szigorítja az MH belső szabályozó tevékenységének rendjéről szóló követelményeit (általános érvényű szabályozók esetében kétéves, egyéb szabályozók, szakutasítások 5 évi felülvizsgálati kötelezettség), amit az MH Informatikai Stratégia éves felülvizsgálati gyakorisága, valamint a technikai és szabályozói környezet folyamatos változása indokol. Azonnali felülvizsgálatra van szükség:

- a nemzeti (biztonsági-, információbiztonsági-, esetleges védelmi-, katonai) stratégiák változásakor;
- az összhaderőnemi doktrínák felülvizsgálatakor;
- az információbiztonságra vonatkozó jogszabályok, szabványok vagy kormányzati ajánlások változása esetén;
- NATO, EU Biztonságpolitika, a támogató direktívák és irányelvek olyan változása esetén, amelyek érintik a kidolgozott szabályozókat;
- ellenőrzés során tapasztaltak, vagy olyan biztonsági esemény kapcsán, ami szabályozási hiányosságra vezethető vissza.

3. 4. Az információvédelmi rendszabályok ellenőrzése

Kormányzati szintű ellenőrzési feladatnak a szakterületi felhatalmazással rendelkező szervezetek vizsgálatai tekinthetők, amelyből legfontosabb az Állami Számvevőszék, a Kormányzati Ellenőrzési Hivatal, és a minősített adatok felügyeletét végző szervezetek tevékenysége.

A Kormányzati Ellenőrzési Hivatal ellenőrzéseit a vonatkozó jogszabály megfogalmazása szerint a jogszabályok, és nemzetközi belső ellenőrzési standardok alapján végzi. [150.] Ez az „Informatikai rendszerek módszertani segédlete ellenőrök részére" segédlet alapján a COBIT módszertan szerinti ellenőrzésben nyilvánul meg. [151.]

Az Állami Számvevőszék által alkalmazott „Módszertan az információs rendszerek kontrolljainak ellenőrzéséhez" segédlet a COSO[60] módszertan vizsgálati rendjét tekinti irányadónak. [152.]

Ez azt jelenti, hogy az informatikai rendszerek védelmére vonatkozó, jogszabályban nem rögzített követelmények szerint kialakított szabályozókat (és védelmi rendszabályokat) az említett kormányzati szervek nem biztonsági szemléletű módszertanok alapján vizsgálják. A teljes kép érdekében visszautalok arra, hogy a Miniszterelnöki Hivatal szervei a közigazgatást kiszolgáló rendszereknél az információvédelem szabályozására egy harmadik módszertanhoz igazodó követelményeket határoznak meg jogszabályokban.

A nemzeti minősített adatok és adatkezelő képességekre vonatkoztatott ellenőrzési feladatok jogszabályban nem részletezettek. NATO, EU minősített adatok esetében az illetékes hatóságok az aktuális NATO, EU Biztonságpolitika és a végrehajtásukra vonatkozó alacsonyabb szintű szabályozók követelményei szerint járnak el, de ezek az eljárások jogszabályban szintén nem részletezettek. Emiatt a jogszabályoknak való megfelelés mellett külön szempontként vizsgálni kell a NATO, EU követelményeknek való megfelelést is.

A fentiek alapján megállapítom, hogy nem azonosítható az MH szervezeteinek információvédelmi tevékenységét támogató, egységes szemléletű kormányzati ellenőrzési rend. A szakmai tevékenységet irányító szervezetnek el kell igazodni a különböző módszertanok, és eljárásrendek eltérő fogalmi rendszerében és olyan szabályozási és ellenőrzési rendet kell kialakítania, ami kielégíti az összes, eltérő szemléletű és megfogalmazású követelményt.

Az információvédelmi rendszabályok belső ellenőrzésére irányuló feladatokat az MH általános feladatrendje szerint kell kialakítani. Az érvényes szabályozás szerint a honvédelmi

---

[60] COSO: Comitte of Sponsoring Organisations of the Treadway Comission (Belső Ellenőrök Nemzetközi Szervezete).

szervek rendeltetésével és a szakfeladataik ellátásával kapcsolatos ellenőrzés kiterjed az alaprendeltetési feladatok végrehajtására is, melynek önálló területe az információ és dokumentumvédelem. [153.]

A szakterületi ellenőrzési feladatok kibontására az első szabályozási kísérlet egy komplex ellenőrzési forgatókönyv kialakítása volt egy ideiglenes szakutasítás kiadásával 2003-ban. A kiadmányozói szándék ekkor nem érhette el célját (a dokumentum-centrikus szabályozási szemlélet informatikai védelem területén egy kevésbé használható feladatrendet eredményezett), így *soron lévőnek kell tekinteni az ellenőrzési feladatok kidolgozását* a következők figyelembe vételével.

3. 4. 1. A szabályozottság ellenőrzése

A katonai terminológia szerint az ellenőrzés e típusa a felügyeleti, illetve elöljárói ellenőrzés feladatkörébe illeszthető. Egy több éves időszak átfogó jellegű, működésre vonatkozó vizsgálatakor az ellenőrzési cél a szervezeti működés szabályozottságnak ellenőrzése, és nem egy-egy részterület átvilágítása.

Első feladat az érintett szervezet adatkezelő rendszereinek üzemeltetéséért, biztonságáért, valamint a külső szervezetekkel való együttműködésért felelősség azonosítása (esetenként az ellenőrzés világít rá, hogy egy-egy szakterület nincs megfelelően személyhez kötve, vagy a megbízások között átfedések, ellentmondások, illetve összeférhetetlenségek vannak). Tisztázandó kérdések:

- Az adott kérdést szabályozó dokumentum megfelel-e a felsőbb szintű szabályozók követelményeinek?
- A dokumentumok között nincs-e ellentmondás, illetve nem hagynak-e szabályozatlanul területeket?

A felelősségek azonosítása után a szervezet vezetése számára ki kell mutatni a működési rend megfelelőségét, vagy hiányosságait, melynek alapján megállapítható, hogy a kijelölt felelősségi rend alapján, a kialakított eljárásoktól *elvárható-e az információs műveletek korszerű védelme, vagy nem*.

Helyi szabályozás esetén kezelni kell azt a gyakori problémát, ami a központi (így célszerűen keretjellegű) szabályozások másolásából adódik. Ennek eredménye a helyi sajátosságoknak megfelelő részletes szabályozás helyett egy kivonatszerű, tartalmilag nehezen ellenőrizhető eljárásokat tartalmazó dokumentum. Ugyanígy előfordulhat, hogy központi kialakítású és ellátású rendszer helyi eleme nem szerepel a helyi szabályozókban, „mert az központi”.

3. 4. 2. A védelmi rendszabályok érvényesülése

A védelmi rendszabályok érvényesülésének ellenőrzésekor (ez gyakran félreértelmezett kérdés) nem azt kell vizsgálni, hogy *a rendszer-specifikus vagy egyéb helyi szabályozók előírásainak megfelel-e az adott védelmi rendszabály,* hanem azt, hogy *a központi szabályozók érvényesülnek-e* (amivel kivédhető a helyi szabályozó tévedéseire visszavezethető hiba).

A NATO (és EU) szervezeti kultúrában jól kialakult rendje van a listákra épülő ellenőrzéseknek, de több éves tapasztalatom és civil területen dolgozó auditorokkal való konzultációk alapján megállapítom, hogy *az ellenőrzési listák átvétele és önmagukban való alkalmazása nem hatásos*. Az ellenőrzési listák könnyen ránevelik az ellenőröket és az ellenőrzötteket *a mechanikus, teljesítmény centrikus vizsgálatokra, így könnyen téves reflexek alakulhatnak ki*.[61]

Híradó alegységek vezetése, és információvédelem területén szerzett tapasztalataim alapján a *listákra alapuló ellenőrzés*, a *szervezetek működés közbeni ellenőrzése, valamint a kikérdezéses módszerű ellenőrzés vegyes alkalmazását tartom célszerűnek*. Részletes lista helyett csak egy-egy terület kulcskérdéseit célszerű támpontként rögzíteni, ami biztosítja, hogy fontos területek ne maradjanak ellenőrzés nélkül.

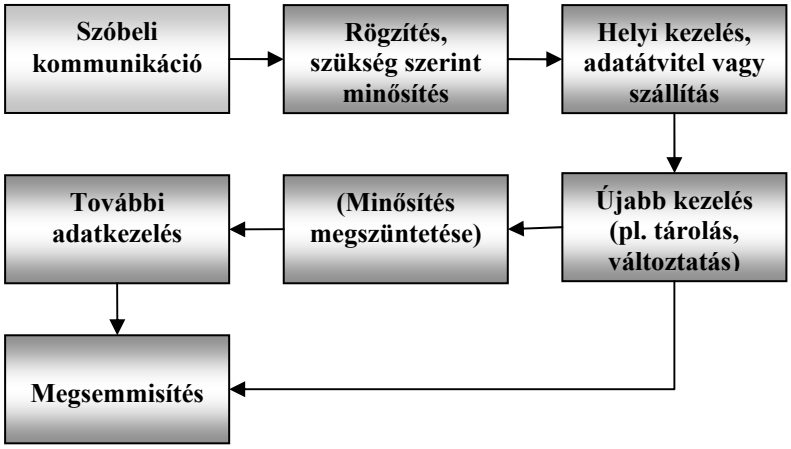
A részletes, lista alapú ellenőrzés *a technikai paraméterek helyességéről való meggyőződés alapvető eszköze* (pl. hálózati eszközök, operációs rendszerek beállításai, biztonsági házirend), ami rendszer-specifikus hardver, szoftver ismereteket igénylő feladat.

Az elektronikus adatkezelés biztonsági kérdéseinek kezelésére vonatkozó korszerű megoldás (incidensek érzékelése, elemzés, értékelés, beavatkozás, szükség szerint többfokozatú újabb elemzés, bizonyíték rögzítése) nem válthatja fel teljesen az eddig említett ellenőrzési feladatot, de hatékonyság, minőség tekintetében nagyságrendeket javít a zömében manuális ellenőrzési módszereken.

Információvédelmi szakterületen a statikusnak tekinthető jelenségek kimutatására helyett *a vezetéshez szükséges kommunikációs folyamatokhoz igazodó komplex ellenőrzési szemlélet* kialakítása tekinthető a legfontosabb kihívásnak (14. sz. ábra). A *szakterületekre vágott ellenőrzési szemlélet gyakran nem hatásos, mert az ügyviteli, híradó, informatikai, rejtjelző szakterületekre szabdalt vizsgálatok között hézagok keletkezhetnek, illetve szemléletbeli különbségek eltakarhatják a védelmi rendszer hiányosságait.*

---

[61] Tipikusnak tekinthető a „ha minden kérdésre megfelelő a válasz, nem lehet biztonsági probléma” vagy „ez nincs az ellenőrzési listán” megfogalmazás.



14. ábra: Adat életciklus (változat)

A célellenőrzést olyan speciális kérdések vizsgálatára kell fordítani, amelyek fontosságuk, bonyolultságuk miatt részletesebb elemzést tesznek szükségessé (pl. elektronikus adatkezelő rendszer esetében: biztonsági mentések megléte, helyreállítási feladatok ismerete, konfigurációmenedzselési feladatok, biztonsági napló ellenőrzés). E feladatok érdekében ki kell alakítani azokat a rendszerek specialitásainak megfelelő vizsgálati módszereket (beleértve a mobil, eszközökkel támogatott képességeket is), amelyek *hitelesen bizonyítják konfiguráció megfelelőségét, a szükséges biztonsági beállítások meglétét* (elemző programok, hálózati és host szkennerek). Az önállóan telepített munkaállomások és adathordozók helyi manuális ellenőrzését hálózati szolgáltatásokkal és központi felügyeleti funkciókkal kell, ha nem is teljesen kiváltani (a helyi üzemeltetési környezetben egyes szabályok betartásának ellenőrzése más módszerrel nem végezhető), de jelentősen megerősíteni.

3. 5. A jóváhagyás/akkreditálás

Kormányzati hatóság jóváhagyási, akkreditálási tevékenységeként nemzeti adatkezelés esetében rejtjelző eszköz engedélyeztetésére, rejtjelszabályzat bemutatására, elektronikus hitelesítés szolgáltatás bejelentésére/tanúsíttatására, illetve elektronikus iratkezelő szoftver tanúsíttatására vonatkozó követelmény azonosítható.

A Központi Elektronikus Szolgáltató Rendszerhez, vagy az EKG-hoz történő csatlakozás feltételeként megszabott szabályozó kialakítására és bemutatásra vonatkozó követelmény tekinthető még rendszer szintű jóváhagyási eljárásnak.

Minősített adatok kezelésére szolgáló nemzeti adatkezelő rendszer használatba vétele az előbbi területek kivételével *nem igényel hatósági jóváhagyást*. *Ez jelzi az országos*

infrastruktúra hiányát, mivel a különböző alkalmazó szervezetek, szolgáltatók, felügyeleti szervek tevékenysége egységes szabályozás és a technikai paraméterek pontos illesztése, illetve e tényezők *használatba vétel előtti ellenőrzése nélkül elképzelhetetlen*.

NATO, EU KORLÁTOZOTT TERJESZTÉSŰ, vagy magasabb minősítés esetén a hagyományos és elektronikus adatkezelő rendszer használatba vétele az *illetékes hatóság* közigazgatási határozatával igazolt akkreditálási eljárásához kötött.[62] [154.] Ennek során kiderül, hogy a kijelölt feladatra kialakított technikai, szervezési és egyéb védelmi rendszabályok alkalmazásával az adott rendszer esetében teljesülnek-e a meghatározott biztonsági követelmények. Az eljárás részletes feladatait hazánkban jogszabály nem tartalmazza, a kialakított eljárásrend gyakorlati úton alakult ki. Minősített elektronikus adatkezelő rendszer esetében az akkreditálási döntés a következő tényezők vizsgálatán alapul:

- *Meghatározott feladat, azonosított minősítési szint, és a meghatározott biztonsági üzemmód.* Az információs műveletek rengeteg specialitást tartalmaznak, így olyan rendszerekre, folyamatokra van szükség, amelyek a szükséges feladatokat a lehető legjobban, biztonságosan szolgálják ki. *A feladatok változása esetén egy addig jól használható eszköz is biztonsági problémák forrása lehet*, amit az ellenfél információs műveletei kihasználhatnak.[63] A minősítési szintekhez rendelt védelmi rendszabályok miatt kritikus lehet az adatfeldolgozásra vonatkozó minősítési szint, vagy a hozzáférési jogosultságok kategorizálására szolgáló biztonsági üzemmódok (elterjedt magyar kifejezés hiányában angol megnevezés szerint: dedicated, system-high, multi-level)[64] téves azonosítása.
- *Azonosított fenyegetések, elfogadhatónak tekinthető kockázat.* Az információs műveleteket megvalósító eszközök, rendszerek kockázatelemezésre alapozva, csak a fontosnak ítélt fenyegetések ellen nyújtanak védelmet. Bonyolult tényezők összesítéseként *a hatóság feladata annak eldöntése, hogy egy rendszer az általa*

---

[62] Ez emelt szintű követelmény az EU eredeti követelményeihez képest. Eredetileg a TITKOS vagy magasabb minősítésű adatokat kezelő rendszereket kell az illetékes hatósággal akkreditáltatni, alacsonyabb minősítés esetén az illetékes biztonsági szervezet jóváhagyja a rendszert.

[63] Pl. az irodai eszközök és a tábori körülmények között üzemeltetett eszközpark közötti eltérés.

[64] A biztonsági üzemmódok jogszabályban nem azonosítottak, de az MH szervezetek által kezelt NATO, EU minősített adatokat kezelő rendszerek ezen felosztás szerint kategorizáltak.
A legegyszerűbb esetben (dedicated) a kezelt adatok legmagasabb minősítési szintjéhez megfelelő személyi biztonsági tanúsítvánnyal rendelkezik az összes felhasználó, valamint érvényes megismerési engedélyük van az összes adatra. A középső esetben a megfelelő szintű személyi biztonsági tanúsítvány mellett nincs mindenkinek megismerési jogosultsága minden adatra. A harmadik esetben a felhasználóknak különböző szintű személyi biztonsági tanúsítványai és korlátozott megismerési engedélyük van, ami miatt összetett szempontú, differenciált hozzáférési rendszert kell kialakítani.

kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása szempontjából biztonságosnak tekinthető-e.

– *A szükséges védelmi szintet garantáló üzemeltetési környezet, a védelmi rendszabályok, és azonosított külső csatlakozások.* A rendszer üzemeltetési engedélyének azonosítania kell a meghatározott minimális védelmi szintet, meg kell határozni az esetleges üzemeltetési korlátozásokat. Az üzemeltetők hatáskörén kívül eső környezetben felmerülő változások, vagy az üzemeltetés feltételeinek jelentős változása olyan tényezők, amelyek az üzemeltetési engedély visszavonását vagy korlátozását eredményezhetik. A csatlakozó rendszernek eltérő céljai, biztonsági környezete és védelmi rendszabályai lehetnek, amely különbségek jelentős biztonsági kockázatokat jelenthetnek, így csak azonosított rendszerekkel, meghatározott rendszabályok teljesülése esetén képzelhető el olyan összekapcsolás, amely nem jelent fenyegetést a kezelt adatok számára.

Az akkreditálási folyamat gyakorlati része az előzőekben ismertetett ellenőrzési feladatkör paneljeiből állítható össze: *a szabályozás megfelelőségének, valamint a védelmi rendszabályok megvalósultságának vizsgálata*. Az akkreditálási eljárás bonyolult rendszer esetében külön műszaki vizsgálatokat igényel (rendszertervnek való megfelelőség, eszközök azonosítása, üzemeltetési és biztonsági paraméterek, sebezhetőség és sérülékenység ellenőrzés).

A nemzetközi rendezvények (gyakorlatok, válságkezelési konferenciák, munkacsoport ülések), a különböző magyarországi elektronikus adatkezelő rendszerek akkreditálási tapasztalatai alapján megállapítom, hogy *a feladatokat tisztázó akkreditálási terv nagyban segíti az üzemeltetők, a biztonsági menedzsment, a hitelesítő hatóságok (és más együttműködők) tevékenységének összehangolását*. A feladatok azonosítása (tesztekre, technikai átvilágításokra, auditokra vonatkozó formai és tartalmi követelmények, szükséges referenciák, határidők, felelősségek, vonatkozó jogszabályok és egyéb szabályozók) lehetővé teszi a hatósági eljárások előkészítéséhez szükséges forgatókönyv kialakítását, a tevékenységek összehangolását. Az akkreditálás ilyen formában történő tervesítése jogszabály szerint nem kötelező, de a feladatok előkészítése, összehangolása megköveteli ezt a gyakorlatot, kiemelten a több szervezet által üzemeltetett hálózatok esetében.

A NATO, EU biztonsági hatóságok hatáskörébe tartozó esetekben a nemzeti hatóság által végzett akkreditálási folyamat kiegészül a szövetségi szervek eljárásrendjével, ami a feladatok szoros összehangolását igényli.

Az MH alaprendeltetéséhez tartozó külföldi küldetések nem minden esetben tervezhetők előre (pl. külföldi misszió során változhatnak az alkalmazási körülmények), így a jelenlegi, gyakorlatilag az állandó üzemeltetési körülményekre kialakított *kormányzati szabályozás rugalmasabbá tételére van szükség.*

Külön esetként kell említeni a külföldi missziók elektronikus adatkezelő rendszereivel kapcsolatos engedélyezési eljárásokat. Ebben az esetben *az előkészítési fázis döntő jelentőségű, mert az egyedi helyzetre kialakított eljárásrend, az ismeretlen együttműködő partnerek, és a dinamikus környezetben történő rendszerbe állítás az átlagosnál több nehézséggel jár.*

A hatóság által kiadott, esetenként időbeni vagy alkalmazási korlátozásokat tartalmazó, lejárati időhöz kötött üzemeltetési engedély a rögzített védelmi rendszabályok, feltételek sérülése esetén automatikusan érvényét veszti. Jogszabály nem tartalmaz az üzemeltetési engedély megújításával kapcsolatos kötelezettséget, de nyilvánvaló, hogy a környezeti változások, a technikai paraméterek szükségszerű változásai, a felhasználói követelmények folyamatos fejlődése olyan tényezők, amelyek indokolják a hatóságok által kiadott engedélyek időszakos felülvizsgálatát.

3. 6. Összefoglalás és következtetések

A kormányzati felelősségi rend, valamint a jogszabályokban meghatározott, az információvédelmi rendszabályok szabályozására vonatkozó követelmények széttagoltságot mutatnak. A hatósági jogköröket ellátó kormányzati szervek elkülönítve menedzselik a NATO, EU és a nemzeti minősített adatok védelmét, és ettől elkülönítetten, de nem összefogottan jelennek meg a nem minősített adatok védelmével kapcsolatos feladatok.

Ezek alapján megállapítható, hogy információvédelmi területen az egységesítési folyamatok alatt álló MH adatkezelő képességeire nem egységes szemléletű kormányzati követelmények hatnak. Az MH elé kitűzött feladatok és a szövetségi vállalások teljesítése csak egységes szemléletű információvédelmi rendszer támogatásával képzelhető el, aminek kulcskérdése a szakterületért való felelősség centralizálása. Széttagolt felelősségi rendben nem képzelhető el egységes szabályozás kialakítása és fenntartása.

A felelősségi rend bemutatása alapján megállapítható, hogy az MH teljes szervezeti hierarchiájában megoldandó kérdés az *információbiztonsággal kapcsolatos általános vezetői felelősség pontosabb megfogalmazása, a felelősség korszerű megosztása*. A katonai szervezeteknél a törzsfőnökre és/vagy parancsnok helyettesre ruházott biztonsági funkciót (jelenleg: titokvédelmi felügyelő és/vagy biztonsági megbízott) át kell alakítani általános

vezetői felelősségé. Az információvédelmi tevékenység irányítására/vezetésére szakbeosztást (szervezeti feladatoktól függően biztonsági felügyeletet) célszerű kialakítani. A jelenleg csak korlátozott, a NATO, EU minősített adatok védelmére szűkített továbbképzési rendet át kell alakítani. A vezetők számára olyan ismeretanyagot kell összeállítani és rendelkezésre bocsátani, amely támogatja a szakmai feladatok végrehajtását (nem a szükséges védelmi rendszabály oktatása, hanem azok kialakításához és fenntartásához szükséges általános menedzsment feladatok, kötelezettségek ismertetése a feladat).

Az országos hatáskörű központi nyilvántartók tevékenysége tárcák szervezeti határain túlnyúló feladatokat tartalmaz. A nemzeti infrastruktúra pontos működése érdekében a jelenleg központilag nem rögzített feladatokat a minősített adatok kezelését szabályozó jogszabályok változásakor célszerű részletesen kidolgozni.

A szakirányításhoz szükséges felső szintű feladatok megfogalmazása alapján megállapítom, hogy hatáskörre, létszámra, szakismeretre, vagy szervezeti kapcsolatokra vonatkozó pontos igények e feladatok rögzítése nélkül nem állapíthatók meg (pl. a közfeladatok ellátásának felülvizsgálatára vonatkozó tevékenység is csak ez után az alapvető lépés után kezdhető). A szakirányításra vonatkozó követelmények tisztázása után válaszolható meg az a kérdés, hogy mely feladatokat szükséges a honvédelmi tárcának végeznie, és melyek azok a szolgáltatások, amelyek más kormányzati vagy egyéb szolgáltató által végezhetők.

Kiemelt kérdésként kezelendő a *képzés korszerűsítése*, melynek során a gyakorlati oldal külön figyelmet igényel. Megfelelő szimulációs és egyéb gyakoroltatási lehetőség nélkül nem lehet szakképzést folytatni, mert az üzemelő elektronikus adatkezelő rendszerek korlátozott gyakorlási lehetőségeket biztosítanak.

Információvédelem területén is szükség van a humán erőforrás gazdálkodás felülvizsgálatára, és rugalmasabbá tételére, mert a korszerű adatkezelő rendszereken megszerzett üzemeltetési tapasztalat, illetve az MH feladatainak átalakulása jelentősen növeli az állomány mobilitását.

A bemutatott jogszabályi környezet, az érzékelhető kormányzati kezdeményezések jól mutatják, hogy az MH adatkezelő rendszerei, információs folyamatai technikailag és jogszabályi szempontból egyaránt *változó környezetben vannak, és új kihívások előtt állnak*. *Az eddig nem összehangolt, egymáshoz nehezen illeszthető kormányzati követelményeket fel kell váltani a nemzeti infrastruktúrára vonatkozó specifikus biztonsági követelményekkel, ami az MH adatkezelő képességeinek védelmére is jótékony hatást fog gyakorolni.*

A szervezeti méretek, struktúra és a vezetési folyamatok bonyolultsága miatt az MH-nál információvédelmi területen a hagyományosan elképzelt „szabályzat” helyett a *szabályozó*

rendszer kialakítása a járható út, amit az MH szintű, információvédelemre vonatkozó szabályozókban a szervezetek, beosztások megnevezésének helytelen gyakorlatának-, a felsőbb szintű szabályozók szövegrészeinek ismétlésének megszüntetésével kell erősíteni. A MH szintű szabályzatoknak – a jelenleg tapasztaltakkal ellentétben – önállóan kialakítva csak azt a területet kell szabályoznia, amire a hatáskör kiterjed, mert a dokumentumok kiegészítései, felülvizsgálatai szakterületenként eltérő gyakoriságot igényelnek.

A szabályozási rend felső szintű szabályozói közé be kell iktatni a biztonságpolitikát olyan tartalommal, hogy az MH információs folyamataiban résztvevők megkaphassák belőle a szükséges szakmai támogatást. Ebben az esetben megszüntethetők a doktrínák területén bemutatott hiányosságok (tartalmi hibák és az összhang hiánya), az alacsonyabb szintű szabályozók eltérő megfogalmazásai, vagy a belső rendelkezések esetében a szabályozókból a hiányzó adatok.

A bemutatott szabályozási rend elemei lényegesen rugalmasabban kezelhetők, mint a jelenleg tapasztalható, központi szabályzat alapú rendszer. Ebben a rendben a szabályzat funkciója szükségszerűen átalakul, és csak technológia és rendszer független követelményeket, rendszabályokat tartalmazza a rendszer-specifikus védelmi rendszabályok kialakításának támogatása érdekében.[65]

A helyi szabályozók területén a *széttagolt szabályozási rendet integrálni kell* (ez akkor is célszerű, ha a jogszabályok ezt az egységesítést a nem követelik meg).

A technikai fejlődés függvényében hálózatok integrálódásával a helyi és a rendszerfüggő szabályozók területén *a helyi (szervezethez köthető) szabályozó szerepének csökkenése, és a nagy kiterjedésű rendszerekre vonatkozó központi szabályozó szerepeinek erősödése várható.*

A rendszer-specifikus szabályozás kétlépcsőssé alakításával a rendszerért felelős vezető belső rendelkezésben meghatározhatja azokat az általános biztonsági követelményeket, hatásköröket és feladatokat, amelyeket a jogszabályok végrehajtása illetve a katonai műveletek sikere érdekében szükséges érvényesíteni. Bonyolultabb rendszer esetében a kockázatelemzés eredményeire támaszkodó részletesebb dokumentum készíthető, amelynek bemutattam egy célszerű változatát. Egyszerűbb esetben ezek a feladatok az üzemeltetésre és biztonságra vonatkozó belső rendelkezésben is megfogalmazhatók. Ez a követelmény adhatja

[65] Az MH-nál még nem terjedt el a cserélhető lapos változatú szabályozatok módszere, de gazdaságosság és kezelhetőség szempontjából ez legjobb megoldás. Egy-egy változtatás esetén gyakori, hogy csak egyes részek változtatására, kiegészítésre van szükség, ami ezzel a módszerrel jól kezelhető.

alapját az éves beruházási/fejlesztési terveknek (az Informatikai Stratégia kötelező mellékletei) vagy a Védelmi Tervező Rendszerben önállóan megjeleníthető feladatoknak.

AZ MH szintű elektronikus adatkezelő rendszer központilag kialakított védelmi rendszabályai szükségszerűen rendszer specifikusak lesznek, centralizált jóváhagyás (minősített adatkezelés esetén akkreditálás) által engedélyezve. Ezzel *megszűnik a katonai szervezeteknél alkalmazott rendszabályok közötti eltérés kockázata*, lehetővé válik a nemzeti és nemzetközi hálózatokhoz történő csatlakozás.

Az MH-nál az információbiztonsági célkitűzések, és a részletes védelmi rendszabályok közül logikailag hiányzik az általánosan megfogalmazott, rendszer és minősítési szinttől független biztonsági alapelv intézménye, így a jelenlegi helyzetnek megfelelően megfogalmaztam azokat. A megfogalmazott alapelvek nélkül a rendszerek kialakításának csak *az anyagi és technikai lehetőségek szabnának határt, amely korlátoknál az információbiztonság szempontja szűkebb keresztmetszetű*.

Az érvényben lévő, nyilvánosan megismerhető szabályozók áttekintése alapján megállapítom, hogy információbiztonság területén az MH szabályzatok kialakult rendje, a rohamos tempójú technikai fejlődés, a haderő átalakítás/fejlesztés a szervezeti változások üteme miatt *a felülvizsgálati rend hatékonysága alacsony*. *A szabályozási rendszer elemeinek a jelenleginél rugalmasabban kell reagálnia a szabályozói környezet változásaira, amelynek érdekében meghatároztam a felülvizsgálatra vonatkozó követelményeket.*

Az információbiztonság szakterületei, valamint a szabályozási és ellenőrzési rend átfogó jellegű áttekintése után megállapítható, hogy a védelmi rendszabályoknak nincs kapcsolatuk a részletes adattartalommal, csak az adatok minősítésével és kezelési jelzésével. *A különböző adatfajták (pl. személyes adat, különleges adat, üzleti adat vagy minősített adat) védelmét az ismertetett védelmi rendszabályok rendjén keresztül kell megvalósítani. Az adatvédelmi felelősnek a jogszabályok szerinti adatvédelmi követelményeket be kell dolgozni az információs rendszerek biztonsági követelményei közé, így megoldódik az eddig függetlenül működő adatvédelmi funkció és az információvédelmi szakterület együttműködése.*

A megváltozott hatáskörök, és a technikai fejlődés eredményeként információvédelmi területén egyértelműen szükség van az ellenőrzési szabályok megváltoztatására, és komplex, az adatkezelő folyamatokhoz igazodó eljárások kialakítására.

Az elektronikus adatkezelésre vonatkozó biztonsági követelmények és védelmi rendszabályok az MH-nál meghaladták azt a szintet, amelyet az ügyvitel-centrikus szabályozói szándék szabályzatban és ellenőrzési forgatókönyvben megjelenített. *Ki kell alakítani a technikai paraméterek ellenőrzésére szolgáló specializált szabályokat, a szükséges humán erőforrásokkal, eszközökkel és eljárásokkal együtt.*

A fejezet befejezéseként Szun Ce szavait idézem:

„Ha ismered az ellenséget és ismered magadat, nem kell félned száz csata kimenetelétől sem.” [155.]

4. ÖSSZEFOGLALÁS, KÖVETKEZTETÉSEK

4. 1. Összefoglalás

Munkám megalapozásaként a nemzeti biztonsági stratégia szakirányú megfogalmazásainak áttekintésére és külföldi biztonsági stratégiák, stratégiai szintű dokumentumok elemzésére támaszkodva *megállapítottam, hogy a nemzeti biztonsági stratégia információvédelemre vonatkozó megfogalmazásai korszerűnek tekinthetők, de nem alapozzák meg kellően az alacsonyabb szabályozási szinten kidolgozandó dokumentumokat*. Megállapítottam továbbá, hogy információs területen a védelem összetettsége, a kritikus infrastruktúra biztonságához szükséges háttérbázis (kutatás-fejlesztés, gyártás, tanúsítás, oktatás, akkreditálás) bonyolultsága *indokolná a széles körű társadalmi kooperáció védelmi stratégiában történő megalapozását, valamint a már többször tervezett nemzeti információvédelmi stratégia kidolgozását*.

Az állami, felső szintű, az információvédelmet egységesen kezelő központi iránymutatást nélkülözhetetlennek tartom a társadalom különböző szereplőinek összehangolt tevékenysége érdekében. Kötelezendően érvényesítendő iránymutatás hiányában nem várható el a felelős kormányzati szervek tevékenységének, a végrehajtás irányításának egységesítése, illetve különböző közigazgatási területeken az azonos elvek mentén történő gondolkozás.

Elemeztem az információvédelmi szempontból meghatározónak tekinthető magyar katonai doktrínákat. *Megállapítottam a legfontosabb szakmai hiányosságokat – beleértve a magyar hadtudományi irodalom eredményeinek mellőzését – és ajánlásokat tettem a hiányosságok felszámolása érdekében.*

Az MH felső szintű szabályozási kérdéseinek egységes támogatása érdekében a nemzetközi trendnek megfelelő csoportosításban összefoglalva *bemutattam azokat az információbiztonsággal kapcsolatos legfontosabb általános témaköröket, megállapításokat és követelményeket, melyeknek kibontásával kidolgozható az adott dokumentumban (jellemzően stratégiában) az információbiztonság általános, felső szintű támogatása*.

A folyamatban lévő, és a tervezett fejlesztések támogatása, perspektivikus információvédelmi követelmények meghatározása érdekében bemutattam a NATO haderőfejlesztési elgondolás fontosabb adatkezelési és védelmi vonzatait.

Nemzetközi és nemzeti forrásokra támaszkodva kimutattam az információbiztonság szakterületeit, *jellemeztem a kulcsfontosságú védelmi feladatokat*, közben a hálózat-alapú hadviselés követelményeit szem előtt tartva *bemutattam a szövetségi és a nemzeti rendszabályok közötti fontosabb eltéréseket*.

Feltártam a jelenleg érvényben lévő nemzeti ajánlás biztonsági besorolásának ellentmondásait és javaslatot tettem a korszerűsítésre. A védelmi rendszabályok vizsgálatánál bemutattam, hogy *a stratégiai szinten hiányzó egységes irányelvek megmutatkoznak a jogszabályok összehangolatlanságán. Bizonyítottam, hogy nemzeti szinten (pl. közigazgatási szervezetek között) illetve a nemzeti és NATO, EU szervezetek közötti kapcsolattartás szintjén az együttműködést nem támogatja egységesen szabályozott védelmi rendszer.*

A védelmi rendszabályok testre szabását szolgáló kockázatkezelés kapcsán *megállapítottam az egységes, jogszabályok által alátámasztott követelmények hiányát, ami nem támogatja a nemzeti, egységes rendszerek kialakítását és a nemzetközi rendszerekhez történő csatlakozást. Az adatcseréhez szükséges egységes védelmi szint megvalósítását csak részletezett, minden résztvevő által egységesen értelmezett azonos módszer és mérték szerint végzett kockázatkezelés támogatja.*

A kezelt adatok minősítési szintjeire támaszkodó besorolásnak megfelelően *bemutattam az elektronikus adatkezelő rendszereknél a védelmi rendszabályok egymásra épülésének logikáját*. A várható trendek alapján megjelöltem azokat az információvédelmi feladatokat, amelyek az MH-nál hangsúlyt kapnak, így kiemelt támogatást és menedzselést igényelnek. NATO, EU források segítségével ismertettem *azokat a kutatási, fejlesztési célkitűzéseket, amelyek iránymutatást adhatnak a MH különböző szervezeteinél az információvédelem tervezésében, fejlesztésben résztvevők számára*. Azonosítottam azokat a legfontosabb szervezeti kapcsolatokat, amelyek támogatják az MH elektronikus adatkezelő rendszereihez szükséges behatolás érzékelő és eseménykezelő képességet.

Kormányzati követelmény hiányában a védelem kialakításának és fenntartásának vezérlése érdekében *kidolgoztam az összes biztonsági osztályra vonatkozó, minősítési szinttől és kezelési utasítástól független biztonsági alapelveket.*

A szerteágazó kormányzati felelősségi rend bemutatásával információvédelmi területen igazoltam a MITS általános megállapításait. *A bemutatottak egyértelműen bizonyítják, hogy a különböző hatósági szervezeteknek eddig nem sikerült a jogszabályok összehangolása, ezáltal a végrehajtás egyszerűsítése. Napjainkban a hatósági jogkörök szerinti átfedéseket,*

ugyanakkor lefedetlen területeket tartalmazó szabályozás a jellemző. Ebben a helyzetben kiemelten fontosnak tartom az MH-nál az információbiztonság összefogott, centralizált menedzselését, mert az egységes szolgáltatást nyújtó, korszerű védelmi rendszabályok szerint működő adatkezelő infrastruktúra védelme nem képzelhető el a jogszabályok szerint széttagolt, eltérő szemléletű és érdekeltségű szervezeti elemek menedzselésével. Ennek érdekében az általános szakirányítási feladatok kibontásával megfogalmaztam az információvédelem szakirányítási feladatait, ami alapját képezheti a szervezeti erőforrások részletes meghatározásának.

A HM szintű jogszabályok és az állami irányítás egyéb jogi eszközei kategóriába tartozó egyéb MH szabályozók áttekintésével információvédelmi területen megállapítottam a szabályozási hierarchia, illetve az egységes védelmi szemléletet megalapozó alapdokumentum hiányát. Az alacsonyabb szintű szabályozók kialakításához szükséges általános irányelvek meghatározása érdekében a nemzetközi szakirodalom eredményeit felhasználva *kialakítottam az eddig hiányzó MH Információ Biztonságpolitika felépítését*. *A biztonságpolitika végrehajtása érdekében meghatároztam a szükséges szabályozási struktúrát, annak felülvizsgálatához szükséges bemenő adatokat, illetve azokat az eseteket, amikor a felülvizsgálatot soron kívül el kell végezni.* Az általános felülvizsgálatot az érvényben lévő belső rendelkezésben meghatározottnál gyakoribban javasoltam, amit az Informatikai Stratégia éves felülvizsgálati kötelezettsége, a NATO munkacsoportokban folyó, gyakorlatilag folyamatos felülvizsgálati tevékenység, a technikai fejlődés üteme, valamint az összetettnek tekinthető magyar szabályozási környezet indokol.

Elektronikus információvédelmi területen bemutattam a szervezet-centrikus szabályozás helyett a rendszer-specifikus szabályozás előtérben kerülésének fontosságát, körvonalaztam az MH szintű szabályzat kialakításának rendjét.

Munkám összefoglalásánál befejezésképpen megjegyzem, hogy a bemutatott követelmények, szabályok és védelmi feladatok – bár közel sem teljes körűek – *alkalmasak annak érzékeltetésére, hogy az adatkezelő rendszerek biztonsága rendkívül összetett, sok változótól függő állapot.*

Az értekezés segít annak a gyakori problémának a megvilágításában, hogy *hiányos, vagy nem létező felhasználói (hadműveleti) követelmények alapján nem lehet védelmi rendszabályokat kialakítani.*

Ugyanígy segít annak megértésében, hogy mennyire veszélyes elektronikus adatkezelő rendszerek tervezéshez szükséges *általános biztonsági követelmények igénylése a nagybani elgondolás, a technikai jellemzők ismerete és a kockázatok felmérése nélkül.*

4. 2. Tudományos eredmények

1) *Meghatároztam az MK Katonai Stratégia és az MH felső szintű dokumentumaiban megjelenítendő, információbiztonságra vonatkozó általános megállapítások kereteit. Feltártam a legfontosabbnak tekinthető katonai doktrínák információbiztonsággal kapcsolatos megállapításainak hiányosságait, és javaslatokat tettem azok kiküszöbölésére.*
2) Rendszereztem az információvédelmi szakterületek védelmi rendszabályait és *feltártam a nemzeti szabályozásban tapasztalható, a nemzeti és szövetségi szintű hálózat-alapú műveletek támogatását gátló legsúlyosabb hiányosságokat*. Az MH adatkezelő rendszereinek egységes szintű védelme érdekében *meghatároztam a rendszer, és minősítési szinttől független biztonsági alapelveket*.
3) Megállapítottam az MH információbiztonságot érintő szabályozóinak összehangolatlanságát. A hiányosság megszüntetése *érdekében javaslatot tettem az MH Információ Biztonságpolitika felépítésére, a végrehajtást támogató szabályozási rendre, és felülvizsgálatának követelményeire*.

Az értekezés összefoglalásának summázásaként Szun Ce szavait idézem:

„A haditudomány arra tanít bennünket, ne abban bízzunk, hogy az ellenség nem fog jönni, hanem abban, hogy mi készen állunk fogadására; sem annak lehetőségében, hogy nem fog támadni, hanem inkább abban a tényben, hogy pozíciónkat bevehetetlenné tettük.” [156.]

4. 3. Alkalmazhatóság és ajánlások

Az értekezés harmadik fejezetében azonosított MH Információ Biztonságpolitikára vonatkozó követelmények kidolgozása és szakmai köröztetése után javaslom a politika HM utasítás formájában történő kiadását.

Az értekezés második fejezetében azonosított biztonsági alapelveket javaslom megjeleníteni az MH Információ Biztonságpolitikában.

A szakirányításért felelős szervezeti elemek felé az MH szintű szabályozórendszer felülvizsgálatakor javaslom a felső szintű szabályozók és helyi/rendszer-specifikus szabályozókra vonatkozó ajánlásom figyelembe vételét.

Az MH ÖHD felülvizsgálatakor az információvédelemre vonatkozó részek megjelenítésekor a szerkesztőbizottság felé ajánlom az első és második részben foglaltak figyelembe vételét. Az MK Katonai Stratégiában az információvédelmi részek kialakításához javaslom a bemutatott keretrendszer alkalmazását.

Az információbiztonság szakterületi kérdéseit kutatók számára segítségként használható a második fejezetben a kutatás-fejlesztésre vonatkozó elgondolások, valamint az első fejezetben, a NATO hálózat alapú képességekkel kapcsolatos általános követelményeknek tekinthető részek bemutatása. Ajánlom az értekezés részeinek e források által jelzett irányok mentén történő továbbfejlesztését, a megvalósíthatóság rendszer-specifikus vizsgálatát, figyelembe véve a központosított biztonsági megoldásokra vonatkozó igényeket.

Az értekezést javaslom ajánlott irodalomként alkalmazni az MH információvédelmi szakmai tanfolyamain, továbbképzésein.

HIVATKOZÁSOK

[1.] A Magyar Honvédség hosszú távú átalakításának irányairól szóló 61/2000. (VI. 21.) OGY határozat 8. pont; valamint a Miniszteri Irányelvek a védelmi tervezéshez (2007-2016) 10/2006. (HK 4.) HM utasítás 2. §.

[2.] A katonai jogi szolgálat felépítése, interjú; Magyar Honvéd XVII. 36. szám, p. 8.

[3.] 94/1998. (XII. 29.) OGY határozat a Magyar Köztársaság biztonság- és védelempolitikájának alapelveiről, 2. p.

[4.] 2073/2004. (III. 31.) Korm. határozat, a Magyar Köztársaság nemzeti biztonsági stratégiája II. 1. 6. és III. 3. 7. p.

[5.] dr. Szenes Zoltán altábornagy, a HM Honvéd Vezérkar főnökének beszéde a Honvédelmi Minisztérium és a Magyar Honvédség vezetői értekezletén (www. honvedelem.hu/hirek/kiadvanyok/idoszakos/dr._szenes-zoltan-altabornagy_a_hm_honved_vezerkar_fonokenek _beszede.htm.

[6.] Magyar Információs Társadalom Stratégia 2003, (http://www.gkm.gov.hu/data/cms1057440/MITS.pdf), az ágazati stratégiák összefoglalója, informatikai biztonság, minőség fejezetek.

[7.] IBRS, 3. 4. p. szervezeti keretek. IBRS II. 1. 6, III. 3. 7, 3. 4, 5. 1. 3. bekezdések, 5. 2. 3. fejezet, a jövőkép alapelvei fejezet (p. 83.) és a stratégiai célok fejezet (p. 85.)

[8.] Szenes Zoltán: Válaszúton a magyar biztonság politika, Új Honvédsági Szemle 2005/12, p. 67, 68, 72.

[9.] E- kormányzat és akcióterv, 2005, 3. 4. p. és 4. 3. 2. p. (http://www.meh.hu/szervezet/hivatalok/ekk/ekormanyzat/stratismerteto.html)

[10.] Regulation (EC) No 460/2004 of the European Parliament and the Council of 10 March 2004. Establishing the European Network and Information Security Agency, 1. p.

[11.] The National Strategy for Homeland Security, USA, 2002, (www. Whitehause.gov/homeland/book/nat_strat_hls.pdf) „Critical Infrastructure Sectors” fejezet

[12.] 2000 Russian National Security Concept, (www.russiaeurope.mid.ru/russiastrat2000.html), „II. Russia's national interests” fejezet

[13.] A Secure Europe in a Better World, European Security Strategy 2003, (www.consilium. europe.eu/eudocs/cmsupload78367.pdf), a „The global challenges” fejezet

[14.] Regulation (EC) No. 460/2004 of the European Parliament and the Council of 10 March 2004. Establishing the European Network and Information Security Agency, 1. p.

[15.] The Alliance’s Strategic Concept, 1999, „Assessing the Threat” fejezet

[16.] National Security Concept of the Republic of Estonia, 2004, (www.libertysecurity.org.img.pdf.national_security concept_2004.pdf „Foundations and goals of Estonia’s Security Policy”, „Estonia’s security risks, domestic activities” és „Threats in the information technology sphere” fejezet

[17.] Austria Security and Defence Doctrine, 2001, (www.austria.gv.at./2004/4/18.doktrin.e.pdf) „Austria’s security situation” fejezet

[18.] Canadian Government Security Policy, (www.tbs-sct-gc-ca/pubs_pol/gospubs/tbm_12a/gsp-psg_e.asp), 2002 „ Preamble” rész

[19.] Az Orosz Föderáció Információ Biztonsági Doktrínája, Új Honvédségi Szemle 2001/4-5, „az információ biztonságot veszélyeztető fenyegetések fajtái” fejezet

[20.] National Security Strategy of the Republic of Lithuania, 2005, (www3.lrs.lt./pls/inter3/dokpaieska.showdoc_l?p_id=262943), 4. 1. 10. p.

[21.] 2000 Russian National Security Concept, (www.russiaeurope.mid.ru/russiastrat2000.html)„III. Threats to the Russian Federation's national security” fejezet

[22.] The National Strategy for Homeland Security, USA, 2002, (www. Whitehause.gov/homeland/book/nat_strat_hls.pdf) „„Cyber attacks” fejezet

[23.] A Secure Europe in a Better World, European Security Strategy 2003, (www.consilium. europe.eu/eudocs/cmsupload78367.pdf), a „The global challenges” fejezet

[24.] Regulation (EC) No. 460/2004 of the European Parliament and the Council of 10 March 2004. Establishing the European Network and Information Security Agency, 16 és 19. p.

[25.] Network and Information Security: Proposal for A European Policy Approach; COM(2001)298 final, Commission of the European Communities, 2-3. p.
[26.] Comprehensive Political Guidance, Riga, 2006. nov. 29; 10, 16, 17 és 18. p. (www.nato.int/docu/basics.htm).
[27.] National Security Concept of the Republic of Estonia, 2004, (http://web-static.vm.ee/static/failid/432/NSC_RK6-041.pdf), „Estonia's security risks, domestic activities" fejezet
[28.] Canadian Government Security Policy, (www.tbs-sct-gc-ca/pubs_pol/gospubs/tbm_12a/gsp-psg_e.asp), 2002, „Emergency Planning and Management" fejezet
[29.] Austria Security and Defence Doctrine, 2001, (www.austria.gv.at./2004/4/18.doktrin.e.pdf), „Internal Security" fejezet
[30.] National Security Strategy of the Republic of Lithuania, 2005, (www3.lrs.lt./pls/inter3/dokpaieska.showdoc_l?p_id=262943), 6. 2. 2. p.
[31.] The Alliance's Strategic Concept, 1999, 53. i. p.
[32.] A new chapter (The Strategic Defense Review), Public Discuss Paper, MoD, UK, 2002, (www.comw.org.rma/fulltext/0207sdrvol1.pdf),„The Issues" rész
[33.] The National Strategy for Homeland Security, USA, 2002, „Protecting Critical Infrastructure and Key Assets" fejezet
[34.] Magyar Honvédség Összhaderőnemi Doktrína, 2002, 1209, 1611, 1615 és 1103. p.
[35.] Haig Zsolt: Az információs hadviselés, vezetési hadviselés, mint a XXI. Század új hadviselési formája; NEK 1998. 2. évfolyam 2-3. szám II. kötet, p. 241.
[36.] Várhegyi István - Makkai Imre: Információs korszak, információs háború, biztonságkultúra, OMIKK, Budapest, 2000, ISBN 963 593 238-3
[37.] Kovács László: A jövő információs hadviseléséről, Hadtudomány 2001/2, p. 33.
[38.] Munk Sándor: Az információs műveletek típusai és modelljei, Hadtudomány 2002/1, p. 45.
[39.] Haig Zsolt-Várhegyi István: Hadviselés az információs hadszíntéren, Zrínyi kiadó, 2005, ISBN 963 327391 9, p. 198.
[40.] Haig Zsolt: Az információs hadviselés, vezetési hadviselés, mint a XXI. Század új hadviselési formája; NEK 1998. 2. évfolyam 2-3. szám II. kötet, p. 242.
[41.] Makkay Imre: Az elektronika, távközlés, és az elektronikus hadviselés a XXI. Században, Nemzetvédelmi Egyetemi Közlemények 1997/2, p. 267.
[42.] Várhegyi István - Makkai Imre: Információs korszak, információs háború, biztonságkultúra, OMIKK, Budapest, 2000, ISBN 963 593 238-3, p. 195.
[43.] Magyar Honvédség Légierő Doktrína 2002, 112. p, 127, 135. p.
[44.] MH Összhaderőnemi Logisztikai Doktrína, 2002 és 2004, 430, 201, 153, 410, 156, 317, és 316. p.
[45.] Arthur K. Cebrowski, John J. Garstka: Network-Centric Warfare: Its Origin and Future, 1998, (www.act.nato.int/events/documents/nnec/originsandfuture.pdf), „How Can the Military Not Change" fejezet
[46.] Information Superiority & NATO Network-Enabled Capability (Fact sheet); (www.act.nato.int).
[47.] NATO Strategic Vision (The Military Challenge), 2005, 5, 6, 7, 8, 28, 30, 32. p.
[48.] NATO Network Enabled Capability Feasibility Study, 2005, (www.act.nato.int/events/documents/06nnec3/feasibility.pdf) 1. 2. 4. p.
[49.] NATO Vision and Concept, 2006, 8, 18, 25-27. p. (www.act.nato.int/events/documents/06nnec3/visionconcept.pdf)
[50.] 2004. évi CXL törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól (Ket.) 160. §, 30. §. 1-2, 17. §. Ket. 160. §, 30. §. 1-2, 17. §.
[51.] A Miniszteri Irányelvek a védelmi tervezésről (2007-2016) szóló 10/2006. (HK 4.) HM utasítás 2. §.
[52.] 7001/2006. (HK 4.) HM irányelv a Magyar Honvédség kommunikációs feladatairól, II. fejezet, 1-3. p.
[53.] Dobos Attila: Generációváltás a honvédségi távközlésben, Kommunikáció 2005, ISBN 963 7060 11 1, p. 54.
[54.] Zrínyi Miklós: A vitéz hadnagy; 52. Secretum (titoktartás)
[55.] Szövényi György: Biztonságszervezői menedzsment, 2001, PRO-SEC Kft. p. 113.

[56.] NATO Glossary of Communication and Information Systetms terms and Definitions; AAP 31.
[57.] Mráz István: A katonai felső szintű vezetés információs rendszerének korszerűsítése, Új Honvédségi Szemle, 2001/8 p. 118.
[58.] 2001/264/EC, adopting the Council's security regulations és 2001/844/EC, ECSC, Euratom, amending its internal Rules of Procedure (együttesen EU Biztonságpolitika)
[59.] Biztonság és titokvédelem a NATO szabályai szerint; 1999, Honvéd Kiadó, Budapest, ISBN 963 65 47 1
[60.] Informatikai Biztonsági Kézikönyv, Informatikai biztonsági tanácsadó, Verlag Dashöfer Szakkiadó Kft. & T. Bt., első kiadás 3. 5. 2. fejezet
[61.] Information Operations, Air Force Doctrine Document 2-5 (AFDD 2-5), 1998, (www.dtic.mil.doctrine/jel/service/pubs/afdd2_5-pdf)
[62.] Bruce Gabrielson: Typical Government IS Security Course and Handbook http://blackmagic.com/ses/bruceg/bgrpts.html
[63.] Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations (JP 6.0), 1995, USA (www.bits.de/nraneu/others/jp-doctrine/jp6_0(95).pdf) UJ: www.dtic.mil.doctrine/jel/new_pubs/jp6_0.pdf)
[64.] Physical Security Guide Lead Agency Publication; Protection, Detection and Response (G1-025), 2004, (www.rcmp.gc.ca/tbs/pubs/phys-sec/g1-025_e.pdf) „Rings of protection" fejezet
[65.] 79/1995. (VI. 30.) Korm. rendelet a minősített adat kezelésének rendjéről, 27. §. 3-6.
[66.] 179/2003. (XI. 5.) Korm. rendelet a nemzetközi szerződés alapján átvett, vagy nemzetközi kötelezettségvállalás alapján készült minősített adat védelmének eljárási szabályairól, II. fejezet
[67.] 2094/2004. (IV. 27.) Korm. határozat az egységes minősített adatvédelmi rendszer megteremtésével kapcsolatos feladatokról
[68.] T/18708. számú törvényjavaslat a minősített adat védelméről, 2005. december (www. ogy.hu/irományok/T-18708.pdf; archív)
[69.] Threat and Risk Assessment Working Guide (ITSG-04), Canada, 1999, (www.cse-cst-gc.ca/documents/publications/gov-pubs/itsg04.pdf), Annex K
[70.] 82/2002. (HK 26.) HM utasítás a NIAR biztonságával kapcsolatos feladatokról, 7. §. 2. (6).
[71.] Zrínyi Miklós: A vitéz hadnagy, 52. Secretum (titoktartás)
[72.] Best practice for Security Management (ITIL managing IT services), ISBN 0 11 33 00 14 x, 2003, 6. kiadás, UK Stationery Office, 3. 3. 1. p.
[73.] Informatikai Tárcaközi Bizottság (ITB) 12. ajánlás, Informatikai rendszerek biztonsági követelményei, 1996.
[74.] Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatás informatikai célrendszereinek kockázatfelmérésére, biztonsági osztályokba sorolására (tervezet), 2006.
[75.] 84/2007. (IV. 25.) Korm. rendelet a Központi Elektronikus Szolgáltató Rendszer és a kapcsolódó rendszerek biztonsági követelményeiről, 1. melléklet, 4. 2. 1. p.
[76.] 109/2007. (V. 15.) Korm. rendelet az egységes digitális rádió-távközlő rendszerről, 2. sz melléklet, 3. 3. p. 1. 8. rész.
[77.] Tóth Tibor: A külföldi minősített adatok védelmének aktuális kérdéseiről, Új Honvédségi Szemle, 2004/7, p. 110.
[78.] Underlying Technical Models for Information Technology Security, US Department of Commerce, 2001, SP 800-33, (www.csrc.nist.gov./publications/nistpubs/800-33/sp800-33.pdf) p. 2-3.
[79.] USA DoD Directive 8500.1, Information Assurance (IA), 2002, (www.niap-ccevs.org/cc-scheme/policy(dod/d85001.pdf), E2. 1. 17. p.
[80.] 43/1994. (III. 14.) Korm. rendelet a rejtjeltevékenységről, 1. §.
[81.] Simon Sign: Kódkönyv (A rejtjelzés és rejtjelfejtés története), 2002, Park Könyvkiadó, második, javított kiadás, ISBN 963 530 539 7, p. 325.
[82.] NC3TA Vol. 2 v2 Version 2.0 (2000), Annex A NATO TACOM POST 2000 Architecture (archív)
[83.] Guidelines For Cryptography Policy (www.oecd.org/document/1160,2340,en_2649_34255_ 1814731_1_1_1_1,00.html)
[84.] Recommendation of the Council Concerning Guidelines for Cryptography Policy, 27 March 1997 (www.oecd.org/document/34/0,2340,en_2649_34255_1814690_1_1_11,00.html)

[85.] ITU-T: Security architecture for open systems interconnection for CCITT applications X.800, 1991, A. 4. 1. p.
[86.] Informatikai Tárcaközi Bizottság (ITB) 12. ajánlás, Informatikai rendszerek biztonsági követelményei, 1996. p. 17.
[87.] Information Technology Security Evaluation Criteria (ITSEC), Department of Trade and Industry, London, June 1991, (www.bsi.de/zertifiz/itkrit/itsec-en.pdf), 2. 32. p.
[88.] MSZ ISO/IEC 15408-2:2003, Az informatikai biztonságértékelés közös szempontjai szabvány 2-13. fejezetek
[89.] 1214/2002. (XII. 28.) Korm. határozat a Magyar Információs Társadalom Stratégia készítéséről, a további feladatok ütemezéséről és tárcaközi bizottság létrehozásáról, 4. 2. pont.
[90.] Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS) 0.95 verzió, A MIBÉTS általános modellje, általános elvek, a részvevők kötelezettségei és jogosultságai, 2005, 2. 3. p.
[91.] Recommendation (REC) 15/12/2004 of Council of Europe Comittee of Ministers to member states on electronic governance („e-governance)(www.coe.int/T/F/com/presse)
[92.] Informatikai Tárcaközi Bizottság (ITB) 12. ajánlás, Informatikai rendszerek biztonsági követelményei, (www.itb.hu/ajanlasok/a12), 1996. 4. 3. 2. p.
[93.] 50/1998. (III. 27.) Korm. Rendelet a zártcélú távközlő hálózatokról, 10/A §. (1)
[94.] NC3TA Vol2 –v7 p. 18.
[95.] NC3TA Vol2 –v7 p. 29.
[96.] Security Metrics Guide for Information Technology Systems, 2003,USA SP 800-55. 5. 2. p.
[97.] 217/1998. (XII. 30.) Korm. rendelet az államháztartás működési rendjéről, 145/C. §.
[98.] 14/2005. (HK 1/2006.) HM utasítás a folyamatba épített előzetes és utólagos vezetői ellenőrzési rendszer kialakításával kapcsolatos feladatokról, 5. §. (3).
[99.] 335/2005. (XII. 29.) Korm. rendelet a közfeladatot ellátó szervek iratkezelésének általános követelményeiről, 25. §.
[100.] 179/2003. (XI. 5.) Korm. rendelet a nemzetközi szerződés alapján átvett, vagy nemzetközi kötelezettségvállalás alapján készült minősített adat védelmének eljárási szabályairól, 2. §. (15.).
[101.] 195/2005. (IX. 22.) Korm. rendelet az elektronikus aláírást lehetővé tevő informatikai rendszerek biztonságáról, együttműködési képességéről és egységes használatáról, 9. §. (1.).
[102.] 3/2005. sz. PSZÁF útmutató a pénztárak informatikai rendszerének védelméről, 2. p.
[103.] Informatikai biztonsági módszertani kézikönyv, 8. sz. ajánlás, (www.itb.hu/ajanlasok/a8), Budapest, 1994.
[104.] MSZ ISO/IEC 18028-4:2005(E) IT : Security techniques. IT network security. Part 4. Securing remote access elő szabvány, 5. Security requirement, 8. 2. 2. Protecting the RAS client
[105.] www.honvedelem.hu/miniszterium/hm_technologiai_hivatal.htm (archív).
[106.] EU Incident Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries, Study for the European Commission Directorate-General Information Society (2002), 1. 1. p.
[107.] ITU-T M. 3010 Principles for a Telecommunications management network, 1. 5. p.
[108.] 27/2004. (X. 6.) IHM rendelet az informatikai és elektronikus hírközlési, továbbá a postai ágazat ügyeleti rendszerének létrehozásáról, működtetéséről, hatásköréről, valamint a kijelölt szolgáltatók bejelentési és kapcsolattartási kötelezettségéről, 3, 4 és 10. §.
[109.] NATO C3 Technical Architecture v.2, supplement 2: Emerging technologies v.7.
[110.] www.eema.org/downloads/isse2007/isse07_cfp.pdf
[111.] Peeter Lorents: Overview of the CCD COE Project, Research and Development c. előadása 2006. 12. 10. Tallin, NCOE
[112.] Toomas Kaevand Intelligent simulation methods for intrusion detection and prevention c. előadása, 2006. 12. 10. Tallin, NCOE
[113.] Enn Tõugu: Simulation and AI methods in cyberdefence c. előadása, 2006. 12. 10. Tallin, NCOE
[114.] Risto Vaarandi: Event correlation and data mining for event log analysis c. előadása, 2006. 12. 10. Tallin, NCOE
[115.] Eneken Tikk: Cooperative Cyber Defense, Legal Aspects c. előadása, 2006. 12. 10. Tallin, NCOE

[116.] The National Strategy to Secure Cyberspace (Draft), USA 2002 (www.whitehouse.gov.pcipb/cyberstrategy-draft.html)
[117.] 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról, 24. §.
[118.] 150/2002. Korm. rendelet a belügyminiszter feladat és hatásköréről, 8/A §. (8).
[119.] 195/2005. (IX. 22.) Korm. rendelet az elektronikus ügyintézést lehetővé tevő informatikai rendszerek biztonságáról, együttműködési képességéről és egységes használatáról, 5. §. (2).
[120.] 44/2005. (III. 11.) Korm. rendelet a kormányzati informatika koordinációjáról és a kapcsolódó eljárási rendről, 4. §. (1).
[121.] 45/2005. (III. 11.) Korm. rendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással kapcsolatos feladat- és hatásköréről, valamint eljárásának részletes szabályairól
[122.] 160/2006. (VIII. 28.) Korm. rendelet a MeH-t vezető miniszter feladatairól és hatásköréről, 2. §.
[123.] 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról, 4.§. h.
[124.] 1998. évi LXXXV. törvény a Nemzeti Biztonsági Felügyeletről, 5. §.
[125.] 109/2007. (V. 15.) Korm. rendelet az egységes digitális rádió-távközlő rendszerről, 2. §. (1).
[126.] 76/2006. (XII. 23.) Korm. rendelet a Közigazgatási és Elektronikus Közszolgáltatási központi Hivatal létrehozásáról, feladatairól és hatásköréről, 14. és 15. §.
[127.] www.honvedelem.hu/miniszterium/hm_jogi_helyettes_allamtitkari _titkarsag.htm (archív)
[128.] www.honvedelem.hu/miniszterium/hm_jogi_szakallamtitkar.htm
[129.] 2134/2006. (VII. 27.) Korm. határozat a Magyar Honvédség irányításának és felső szintű vezetésének rendjéről, 14. p.
[130.] 179/2003. (XI. 5.) Korm. rendelet a nemzetközi szerződés alapján átvett, vagy nemzetközi kötelezettségvállalás alapján készült minősített adat védelmének eljárási szabályairól, 17. §. (1)
[131.] Government Security Policy, (www.tbs-sct-gc-ca/pubs_pol/gospubs/tbm_12a/gsp-psg_e.asp), 2002, „10.1. Security program” fejezet
[132.] Váncsa Julianna: Az informatikai biztonság menedzsmentjének feladatai a honvédelmi szféra szervezeteiben, Hadtudomány, pályázat, 2000, p. 27.
[133.] Király Imre: A helyi Titokvédelmi Szabályzat rendeltetése, elkészítésének tartalmi követelményei; Új Honvédségi Szemle 2002/9, p. 85.
[134.] Informatikai Tárcaközi Bizottság (ITB) 12. ajánlás, Informatikai rendszerek biztonsági követelményei, 1996, 2. fejezet.
[135.] MSZ ISO/IEC 17799:2006 Informatika. Biztonságtechnika. Az információ biztonság irányítási gyakorlatának kézikönyve szabvány, 5. 1. 1. p.
[136.] An Introduction to Computer Security: The NIST Handbook, (Special Pub 800-12), (www.csrc.nist.gov/publications/nistpubs/800-12), 5. 1-5. 3. p.
[137.] MSZ EN ISO 9001:2000 Minőségirányítási rendszerek, követelmények szabvány 5.6 fejezet
[138.] MSZ ISO/IEC 27001:2006 Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények szabvány 6. fejezet
[139.] Kormányzati Informatikai Egyeztető Tárcaközi Bizottság, A kormányzati intézmények informatikai stratégiájának készítése, 22. számú ajánlás, 2005 (www.meh.hu/szervezet/hivatalok/ekk/kietb/ajanlasok/20050630kietb22.html)
[140.] 335/2005. (XII. 29.) Korm. rendelet a közfeladatot ellátó szervek iratkezelésének általános követelményeiről, 3. §.
[141.] 233/2001. (XII. 10.) Korm. rendelet a közszolgálati jogviszonnyal összefüggő adatkezelésre és a közszolgálati nyilvántartásra vonatkozó szabályokról, 8. §.
[142.] 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról, 31/A §.
[143.] Informatikai Tárcaközi Bizottság (ITB) 12. ajánlás, Informatikai rendszerek biztonsági követelményei, (www.itb.hu/ajanlasok/a12), 1996. II. fejezet
[144.] 79/1995. (VI. 30.) Korm. rendelet a minősített adat kezelésének rendjéről, 3. §.
[145.] 43/1994. (III. 29.) Korm. rendelet a rejtjeltevékenységről 7. §.
[146.] 305/2005. (XII. 25.) Korm. rendelet a közérdekű adatok elektronikus közzétételére, az egységes közadatkereső rendszerre, valamint a központi jegyzék adattartalmára, az adatintegrációra vonatkozó részletes szabályokról, 3. §.

[147.] 179/2003. (XI. 5.) Korm. rendelet a nemzetközi szerződés alapján átvett, vagy nemzetközi kötelezettségvállalás alapján készült minősített adat védelmének eljárási szabályairól, 63, 64. §.
[148.] 3/2005. (III. 18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről, 1-2. melléklet
[149.] 180/2003. (XI. 5.) Korm. rendelet a Nemzeti Biztonsági Felügyelet részletes feladatairól és működési rendjéről, valamint az iparbiztonsági ellenőrzések részletes szabályairól, 13. §. (1)
[150.] 312/2004. (IV. 15.) Korm. rendelet (a Kormányzati Ellenőrzési Hivatalról 9. §. 1.
[151.] Informatikai rendszerek módszertani segédlete ellenőrök részére segédlet (www.1.pm.gov.hu/web/home.nsf/(PortalArticles)/E5E86B3882C77779C1256E860028BB75), 3. 5. p.
[152.] Módszertan az információs rendszerek kontrolljainak ellenőrzéséhez (www.asz.hu//az/modszert.nsf/0/8C1B3D82FE1A910CC12573220040A220/$file/IT_ell_modsz_2004_02.pdf), p. 13.
[153.] 52/2007. (HK 11.) HM utasítás a honvédelmi tárca ellenőrzési rendjéről, 9. §. 2. b)
[154.] 180/2003. (XI. 5.) Korm. rendelet a Nemzeti Biztonsági Felügyelet részletes feladatairól és működési rendjéről, valamint az iparbiztonsági ellenőrzések részletes szabályairól, 11. és 13. §.
[155.] Szun Ce: A hadviselés tudománya, Göncöl Kiadó 2004, ISBN 963 918339 3, III. 18. p.
[156.] U. o. VIII. 11.

ÁBRAJEGYZÉK

RÖVIDÍTÉSEK

ACT	Allied Command Transformation (NATO Transzformációs Parancsnokság)
C2	Command and Control (vezetés és irányítás)
C3	Command, Control and Communication (vezetés, irányítás és kommunikáció)
CCD COE	Cooperative Cyber Defence Centre of Excellence (Informatikai Hálózatbiztonsági Fejlesztési és Együttműködési Központ)
CCI	Controlled Crypto Item (részegységekre osztott rejtjelzési megoldás)
CERT	Computer Emergency Response Team (számítógép/hálózati vészhelyzet elhárítást támogató csoport)
CIRC	Computer Incident and Response Capability (számítógép eseménykezelő és elhárítási képesség)
CND	Computer Network Defense (számítógép hálózati védelem)

COBIT	Control Objectives for Information and related Technology (informatikai felülvizsgálatra vonatkozó keretgyűjtemény)
COMPUSEC	Computer Security (számítógép/informatikai védelem)
COSO	Comitte of Sponsoring Organisations of the Treadway Comission (Belső Ellenőrök Nemzetközi Szervezete)
CRAMM	UK Government's Risk Analysis and Management Method (az Egyesült Királyságban alkalmazott kockázatelemzési és kezelési módszertan)
CWID	Coalition Warrior Interoperability Demonstration (nemzetközi információs hálózatok együttműködési kérdéseit vizsgáló rendszergyakorlat)
DCI	Defence Capability Initiative (NATO Védelmi Képességek Kezdeményezés)
DSO	Departmental Security Officer (szervezeti szintű (információ)biztonsági tiszt)
EAL	Evaluation Assurance Level (biztonsági értékelési szint)
EBO	Effect Based Operation (hatás alapú műveletek)
EDR	Egységes Digitális Rádió-távközlő rendszer
EKG	Egységes Kormányzati Gerinc
EMSEC	Emission Security (kompromittáló kisugárzás elleni védelmi szakterület)
EU	European Union (Európai Unió)
HM	Honvédelmi Minisztérium
IA	Information Assurance (egységes értelmezéssel még nem rendelkező megnevezés az elektronikus információvédelemre)
IBRS	MITS Informatikai Biztonsági Részstratégia
IDS	Intrusion Detection System (behatolás érzékelő rendszer)
IEGW	Information Exchange Gateway (hálózatok közötti átjáró)
INFOSEC	Eectronic Information Security (elektronikus információvédelem)
IPS	Intrusion Prevention System (behatolást megelőző rendszer)
IT	Infomation Technology (információtechnológia)
ITB	Informatikai Tárcaközi Bizottság
ITSEC	Information Technology Security Evaluation Criteria (IT Biztonsági Értékelési Kritériumok)
ITU	International Telecommunication Union (Nemzetközi Távközlési Egyesület)
JHAT	Jogi Helyettes Államtitkár
KIETB	Kormányzati Informatikai Egyezető Tárcaközi Bizottság
MH	Magyar Honvédség
MH ÖHD	MH Összhaderőnemi Doktrína
MIBÉTS	Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma
MITS	Magyar Információs Társadalom Stratégia
MK	Magyar Köztársaság
NATO	North Atlantic Treaty Organisation (Észak-Atlanti Szövetség Szervezete)
NCW	Network Centric Warfare (hálózat centrikus hadviselés)
NEC	Network Enabled Capability (hálózat-alapú képesség)
NIAR	NATO Iroda-automatizálási Rendszer
NII	Networking and Information Infrasructures (hálózati és információs infrastruktúra)
NRF	NATO Reaction Forces (NATO reagáló erők)
OECD	Organisation for Economic Co-operation and Development (Gazdasági Együttműködési és Fejlesztési Szervezet)
PKI	Public Key Infrastructure (nyilvános kulcsú infrastruktúra)
RAS	Remote Access Service (távoli hozzáférési szolgáltatás)
SSO	Single-Sign On (egyszerűsített bejelentkezési eljárás)
TRANSEC	Transmission Security (elektronikus átvitel közbeni védelem)

VPN	Virtual Privat Network (virtuális magánhálózat)
WAN	Wide Area Network (nagy kiterjedésű hálózat)
ZMNE	Zrínyi Miklós Nemzetvédelmi Egyetemen

FELHASZNÁLT IRODALOM

[1.] 24/2006. (IV. 29.) BM-IHM-NKÖM együttes rendelet a közfeladatot ellátó szerveknél alkalmazható iratkezelési szoftverekkel szemben támasztott követelményekről

[2.] A központi közigazgatási szervek szoftverfejlesztéseihez kapcsolódó minőségbiztosításra és minőségirányításra vonatkozó KIETB 24. ajánlás

[3.] Canadian Handbook on Information Technology Security, 1998

[4.] Fekete Károly: A Magyar Honvédség állandó telepítésű kommunikációs rendszere továbbfejlesztésének technikai lehetőségei, Doktori (PhD) értekezés, ZMNE, 2003

[5.] Hóka Miklós: Hadműveleti, harcászati rádiórendszerek alkalmazása béke- és hadműveletekben, valamint a harc támogatására a vezetés-irányítás, az együttműködés és az interoperabilitás tükrében, Doktori (PhD) értekezés, ZMNE, 2005

[6.] ISO/IEC 2000-2 IT - Service Management szabvány

[7.] Joint Doctrine for Information Operations; JP 3-13, USA, 1998

[8.] Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms (2001).

[9.] Károlyi László: Az információvédelem biztonságát növelő, műszaki- kriptoanalitikai támadási módszerek elleni defenzió, értekezés, ZMNE, 1991

[10.] Model Requirements for the management of electronic Records; MOREQ Specification (http://www.cornwell.co.uk/moreq.html)

[11.] Mráz István: a katonai titokvédelem kérdéseiről; Új Honvédségi Szemle, 1999/2

[12.] MSZ ISO/IEC 12207 Informatika. Szoftveréletciklus- folyamatok szabvány

[13.] MSZ ISO/IEC TR 13335-3 Informatika. Az informatikai biztonság menedzselésének irányelvei szabvány

[14.] NISCC Briefing 2006/02. NISCC Briefing 08a/2006, Social engineering against information systems: what is it and how do you protect yourself?

[15.] Rajnai Zoltán: A tábori alaphírhálózat vizsgálata és digitalizálásának lehetőségei egyes NATO országok kommunikációs rendszereinek tükrében, Doktori (PhD) értekezés, ZMNE, 2001

[16.] Schutzbach Mártonné: Az informatikai rendszerek biztonságának kockázatelemzése a védelmi szférában, Doktori értekezés ZMNE, 2003

[17.] Szép József: A NATO új kezdeményezése: a hálózat nyújtotta képesség, Új Honvédségi Szemle, 2004/12

[18.] Szűcs Gáspár: A katonai vezetés harcászati szintű adatfeldolgozásának korszerűsítése, Doktori (PhD) értekezés, ZMNE, 2000

[19.] Ternyák István: NATO tagságunk hatása és következményei a magyar katonai híradásra, Doktori (PhD) értekezés, ZMNE, 2003

[20.] Tom Thomas: Hálózati biztonság; Panem KFT Budapest, 2005. ISBN 963 545 425 2

[21.] Tóth Antal: A titokvédelem (biztonság) komplex értelmezése a NATO csatlakozás után, HVK tanulmány, 2002

[22.] Útmutató a kockázatkezelés kialakításához (www.pm.gov.hu/web/home.nsf/ (PortalArticles)/ E5E86B8382C77779C1256E860028BB75).

A TÉMÁHOZ KAPCSOLÓDÓ PUBLIKÁCIÓK JEGYZÉKE

Cikkek

[1.] A vezetés ellenőrzési funkciójának érvényesüléséről; Hadtudomány ISSN 1215-4121, 1999. 3-4. szám, p. 94-106.

[2.] The difficulties of scope of control duties; Hadtudományi Tájékoztató ISSN1419-7758, 2000/4, p. 93-106.

[3.] A vezetés korszerűsítésének technikai feladatai; Hadtudomány ISSN 1215-4121, 2000. 1. szám, p. 63-71.

[4.] A korszerű rádiókkal kapcsolatos információvédelmi feladatok és lehetőségek, Kard és toll (válogatás a hadtudomány doktoranduszainak tanulmányaiból) Budapest, 2000 ISBN 963 7037 40 3, p. 73-83.

[5.] A fizikai biztonság, mint az adatbiztonság pillére; Katonai Logisztika, 8. évfolyam, 2000/3. szám, p. 154-165.

[6.] A vezetéshez szükséges korszerű információvédelmi feladatrendszer tanulmányozása és az arra történő áttérés fontosabb feladatai; Nemzetvédelmi Egyetemi Doktorandum 2001, ISSN1588-2233, p. 76-86.

[7.] A híradó és az informatikai rendszer korszerűsítése és védelme; Hadtudomány 2001/1, p. 92-98.

[8.] Vezetési és logisztikai műveletek, folyamatok az információvédelmi rendszer hátterében; Katonai Logisztika, 2000/4, p. 23-33.

[9.] A híradó és informatikai rendszer korszerű szolgáltatásainak hatása és az új információvédelmi feladatok; Egyetemi Közlemények, 2001, ISSN 1417-7323, p. 229-239.

[10.] Úton a korszerű híradó és informatikai rendszer felé; Új Honvédségi Szemle ISSN 1585-4167, 2001/4, p. 9-23.

[11.] Biztonságpolitika és információvédelem, Hadtudomány 2001/3, p. 71-76.

[12.] Responsibility for a secure CIS, 2001. Konferencia kiadvány ISBN 963 008819 3, p. 113-117.

[13.] Az információvédelem újszerű megközelítése, Kommunikáció 20001. kiadvány, ISBN 963 008819 3, p. 193- 198.

[14.] Az információvédelem rendszerszintű feladatai, Nemzetvédelmi Egyetemi Közlemények, p. 111- 120.

[15.] A minősített információk és adatok védelme; Hadtudomány 2002/1, p. 64-70.

[16.] A korszerű híradó és informatikai rendszer védelmi szempontú vizsgálatának egyes kérdései Nemzetvédelmi Egyetemi Közlemények, 2002, 6. évfolyam 2. szám, p. 163-170.

[17.] Kassai Károly – Magyar Sándor: A zártcélú hálózat felügyeletének biztonsági kérdései Új Honvédségi Szemle 2002/11, p. 88-95.

[18.] Az elektronikus információk védelmének területei, Hadtudomány 2002/3, p. 95-102.

[19.] Areas and activities for the information (and information system) security; Kommunikáció 2002. kiadvány, ISBN 963 86229 2 X, p. 75-80.

[20.] Az elektronikus információvédelem néhány szervezeti kérdése Kard és toll 2002, ISBN 963 7037 52 7, p. 128-133.

[21.] Az információk és információs rendszerek fenyegetéseinek stratégiai szintű megfogalmazásai, Új Honvédségi Szemle 2003/3, p. 28-36.

[22.] Az információs rendszerek védelméről, Hadtudomány 2003/1, p.119-126.

[23.] Az információk, a híradó és informatikai rendszer eszközeinek védelme, Hadtudomány 2003/3-4, p. 61-68.

[24.] Az információk, valamint a híradó és informatikai rendszer védelmének szabályozása, Kommunikáció 2003. kiadvány, ISBN 963 86229 62, p. 133-140.

[25.] Kassai Károly – Magyar Sándor: A híradó és informatikai rendszer csomópontjainak védelmi kérdései; Felderítő Szemle III. évfolyam 1. szám 2004. március ISSN 1588-242X, p. 128-136.

[26.] Kassai Károly – Kiss József: Információ- és dokumentumvédelem; „A honvédelem négy éve 2002-2006”című kiadvány, HM Zrínyi Kht. 2006. ISBN 963 327408 7, p. 80-81.
[27.] Az elektronikus információvédelmi rendszabályok megalapozásának fontosabb kérdései, Kommunikáció 2006. kiadvány, ISBN 963 7060 18 2, p. 131-143.

Előadások

[1.] Az elektronikus adatkezelő rendszerek védelmének fontosabb tendenciái (kiemelten a szabályozási területtel kapcsolatos feladatok); Kommunikáció 2005, ISBN 963 7060 11 1. p. 161-170.
[2.] Az elektronikus adatkezeléssel kapcsolatos kockázatok kezelésének egyes kérdései, Kommunikáció 2007. kiadvány, ISBN 978-963-7060-31-1, p. 77-82.

TANULMÁNYOK

[1.] Az ellenőrzés negatív jelenségei és az ellenük való védekezés lehetőségei; Magyar Honvédség Tudományszervező Tanács 1999. évi jeligés pályázat
[2.] Az információvédelmi feladatrendszer átalakulásáról (az állandó kialakítású NATO rejtjelző helyiségek általános fizikai biztonsági követelményei) HVK VFCSF TKM, 2000.
[3.] A korszerű, biztonságos híradó és informatikai rendszerkialakításának érdekességei HVK VFCSF TKM, 2000.
[4.] Úton a korszerű híradó és informatikai rendszer felé, Új Honvédségi Szemle 2000. évi jeligés pályázat
[5.] A korszerű információvédelmi rendszer működési környezete, összetevői és az átalakítás feladatai. HVK VFCSF TKM, 2000.
[6.] A NATO minősített - kiemelten rejtjelző - anyagok megsemmisítési rendje és az ezzel kapcsolatos feladatok HVK VCSF TKM, 2001.
[7.] A veszélyhelyzeti tevékenység tartalma és tervezési feladatai az információvédelem területén, HVK VCSF TKM, 2001.
[8.] Az információvédelmi szakterület feladatai kompromittálódás esetén, HVK VCSF TKM, 2001.
[9.] A Magyar Honvédség elektronikus információvédelmi feladatrendszere korszerűsítésének egyes kérdései, Millenniumi Tudományos Keret, 2002.
[10.] Az információvédelmi feladatkör megjelenése néhány állam biztonságpolitikai dokumentumában, a magyar hadtudományi írásokban és az ezekből levonható következtetések, HVK VCSF TKM 2002.
[11.] Az információ biztonság stratégiai szintű fontosabb kérdései, kiemelt figyelemmel a Magyar Honvédség Informatikai Stratégiájának támogatására, és egy korszerű szabályozási rend kialakítására, HM 5. sz. Tudományos Kutatóműhely, 2006.